Cyber Risk and Security in the Equipment Leasing and Finance Industry

EQUIPMENT LEASING & FINANCE
FOUNDATION
Your Eye on the Future

EQUIPMENT LEASING & FINANCE
FOUNDATION
Your Eye on the Future

Established in 1989, the Equipment Leasing & Finance Foundation is a 501c3 non-profit organization dedicated to inspiring thoughtful innovation and contributing to the betterment of the equipment leasing and finance industry. The Foundation accomplishes its mission through development of future-focused studies and reports identifying critical issues that could impact the industry.

Foundation research is independent, predictive, and peer-reviewed by industry experts. It is funded solely through contributions. Contributions to the Foundation are tax-deductible. Support the Foundation by making a 100% tax-deductible gift today at **www.LeaseFoundation.org**.

Equipment Leasing & Finance Foundation
1625 Eye Street, NW • Suite 850
Washington, DC 20006
www.leasefoundation.org
202-238-3429
Kelli Jones Nienaber, Executive Director

Table of Contents

Executive Summary

Technology is impacting the way businesses function in degrees not seen since the industrial revolution. The previous generations' tools fade more quickly than ever as the word processor replaces the typewriter, and the word processor is replaced by the voice assistant on a smartphone. Each stage of technology adoption has a brief usability window before being replaced by the next stage. The dizzying pace of technology adoption has become one of the most significant drivers of competitive advantage and gains in operational efficiency for equipment leasing and finance companies.

Businesses are not the only groups rapidly adopting technology. Criminal organizations have discovered new ways to commit fraud with far less risk and expense. Ransomware has become one of the most successful of criminals' methods to monetize their activities while staying anonymous. State-sponsored actors can exfiltrate trade secrets directly from organizations and even target communications and power grids in military actions. There is no need to send intelligence agents into harm's way to collect information when it can be acquired covertly over the internet.

It has become clear that the adoption of new technology involves accepting increased cyber risk.

Governments and industries have developed compliance standards and regulations to tame this wild-west environment. This has led to an incomprehensible mix of laws and requirements that most companies have trouble understanding, much less implementing. The well-intentioned regulations have become so numerous that security teams spend a large portion of their time and budget attempting to comply while potentially neglecting more practical security activities. Management can also make the mistake of correlating compliance with a false sense of security. Compliance requirements can be an excellent initial driver for developing a security program but can also become a bureaucratic burden for those security programs that are well established.

Successfully managing organizational cyber risk requires constant vigilance to understand the environment's threats and adopt an agile risk management methodology while balancing compliance requirements. The pressure to perform has never been higher as more organizations learn the hard way through a data breach or ransomware attack. This is an impossible task for the security team alone and requires a total organizational commitment to information security goals and practices.

Cybersecurity is a monumental challenge for equipment leasing and finance companies regardless of their size. This study provides observations and insights on how to build effective cyber-defenses in this everchanging world of digital transformation. Organizations that effectively manage their cyber risk will gain competitive advantage and protect against unexpected losses due to security incidents. Organizations that continue to ignore the dramatic rise of cybercrime may lose consumer confidence, market share, and be mired in regulatory fines and legal action.

The goal of this study is to provide guidance to equipment leasing and finance companies across the vast subject of cybersecurity. This includes:

1. An analysis of the current and future industry threat environment from experts in the cybersecurity industry.

2. A summary of the most impactful cybersecurity regulations and trends in compliance.

3. Analysis of current cyber defenses in use by other equipment leasing and finance companies acquired through original research.

4. Practical advice for securing any size organization, including recommendations on technologies and policies.

5. A real-world ransomware case study with analysis of potential defenses and lessons learned.

Introduction

The role of technology in business continues to grow at an exponential rate. Equipment leasing and finance companies are looking to technology to drive innovation, improve efficiencies, and create closer connections to their customers. This digital business transformation movement has not gone unnoticed by criminals and state sponsored actors. The interconnectivity of the internet that makes it so beneficial for digital transformation also benefits a new breed of criminal. The lack of proximity to a bank or office is no longer a limiting factor as criminals now extend their reach across the globe.

Most equipment leasing and finance companies have some form of cybersecurity defenses in place. Larger organizations have an advantage in that they have invested in formal information security programs. Smaller organizations are less fortunate and may not be aware of the risks involved in the acquisition and use of technology. Both organizations are still vulnerable to cyberattack due to the rapidly advancing tactics and techniques used by modern attackers.

Well-funded criminal organizations and nation-states now have access to tools and capabilities that can penetrate even the best defended organizations. The SolarWinds supply chain compromise at the end of 2020 affected at least seven different branches of the federal government as well as tech company elites, including Cisco, Microsoft, and VMWare. Ransomware attacks increased 98.1% in the United States through the third quarter of 2020, according to a study conducted by Check Point Research. The same study claims that there is a new victim of ransomware every 10 seconds worldwide.

Governments have reacted to the dramatic increase in cyberattacks by passing additional legislation. The European Union enacted the General Data Protection Regulation (GDPR) which can result in fines of €20 million or 4% of the organization’s worldwide annual revenue from the preceding financial year, whichever amount is higher. The California Consumer Privacy Act (CCPA) used GDPR as a template for establishing the most stringent U.S. privacy act. All 50 states including the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted data breach notification legislation. The compliance landscape for equipment leasing and finance companies has never been so complex.

Industry Threat Assessment

The movie "War Games," starring Matthew Broderick, came out in 1983 and became wildly popular. Most information security professionals remembered this quintessential moment where they realized that technology was fallible and the potential impacts of malicious actions. The movie told the fictional story of how a teenage hacker used a modem to dial through all the possible phone numbers looking for a game company but found the famous NORAD ICBM launch facility by mistake. He unknowingly activates an artificial intelligence that does not realize that the game the hacker starts playing, "global thermonuclear war," is only a simulation and attempts to win the game by launching an actual nuclear attack. Artificial intelligence learns the cold war inspired message at the last minute that there was no way to win when playing the game of nuclear war.

The rumor is that the current President of the United States, Ronald Reagan, and members of the military began investigating if this entirely fictional story could be possible. Real-life hackers had adopted the movie's tactic where phone numbers were tested for modems and called it "war dialing." Several large companies had been compromised using this technique, reinforcing the government investigation. However, the security experts came back to the President and explained that NORAD's systems were wholly self-contained and could not be accessed remotely. There was no way for staff to use modems on standard phone lines to access these critical systems.

The number of threats faced by modern organizations has increased exponentially since the "war dialing" attacks of the 1980s became a national concern. However, this is an example of the early use of threat modeling based on the attacks prevalent at the time. The internet was in the early stages of development and not yet accessible by the public. Almost all remote access was conducted over the phone lines with simple passwords. Organizations analyzed the threat and developed techniques to monitor these remote connections and alert on potentially malicious actions. The times have changed, and the number of potential threats to businesses has skyrocketed due to the modern reliance on interconnected systems and public networks. However, the idea of threat modeling is still relevant today as companies attempt to build defenses for their information systems.

A significant factor in any modern threat modeling discussion is how business processes are irrevocably linked to technology and automation, making them vulnerable to interference by threat actors. Businesses ' competitive nature has significantly contributed to these threats by driving the adoption of insecure technology and processes to be first to market. Technology has exposed previously internal business processes to public networks and systems that must be understood to be defended. Threat modeling must take these processes into account as it can be easy to only focus on threats generated through technical vulnerabilities.

Social Engineering

One common threat that is still used today is called social engineering. This technique involves using some trick to gain a target's trust to harvest confidential information. This is no different than the conmen of old that used sleight of hand to take advantage of their victims. The difference is that modern social engineering usually involves using technology to gain that trust. This technique is still used because hacking human behavior is easier than targeting technology. Calling an employee and asking for their password posing as an internal IT employee is easier than finding a 0-day vulnerability in the company's firewall, for example.

The equipment leasing and finance industry is no different than any other industry in that it is vulnerable to social engineering attacks. Banks and finance organizations, in general, tend to be higher priority targets for social engineering given their primary business is to store and distribute funds. They have more processes to exploit that involve monetary transactions, making them more vulnerable to social engineering. There is a blurred line between what is defined as social engineering and what would constitute simple financial fraud as they both involve using fake information to gain trust or financial resources. However, technology has enabled financial fraud on a global scale using social engineering over interconnected public networks like the internet.

The other target for social engineering that is not as obvious in the equipment leasing and finance industry is the amount of confidential information stored by the individual organizations. Direct financial gain may not be the primary goal of an attacker. The equipment leasing and finance industry works with many customers in verticals that could be interesting to several potential threat actors, both criminal and state-sponsored. These actors may target a customer or vendor working with the finance organization to gather financial positions, account numbers, equipment inventory, or other types of confidential information. This could include personal data from the target company to be used in additional social engineering attacks or to gather intelligence into the customer organization's operations.

Dan Nowak is the CEO and founder of Celsus Advisory Group, a firm specializing in threat intelligence. He provided insight into the rapidly changing threat environment that companies now face, given the changes in technology and the impact of COVID on operations. His firsthand experience offered additional insight into the motivation of threat actors where the primary goal of their operations may not be financial gain. Attacks may be conducted for various reasons against the equipment leasing and finance industry that are political, competitive, or even military in nature.

Supply Chain Attacks

Nation-states are becoming more involved in cyber activity to achieve specific political and military goals. A nation-state may implement a ransomware attack for coverage for other activity types. The NotPetya ransomware attack in June 2017 is an example of a state-sponsored attack targeting a specific geographic region for political goals that ended up doing over ten billion dollars of collateral damage to other organizations. NotPetya came out shortly after the WannaCry ransomware attack in May 2017 and used similar exploits leaked to the public from the National Security Agency in March of 2017. The big difference was that NotPetya was intended to look like ransomware but was actually developed to destroy data.

The typical ransomware attack involves a threat actor gaining access to an organization's internal network through social engineering or software vulnerability. The threat actor will perform reconnaissance to identify data locations and target backups for destruction. They will then force encryption of all data stored throughout the organization and hold the encryption key for ransom. The organization is usually given a sample key to test the recovery of a few files. The threat actor then sends instructions to the organization for submitting the payment in some form of cryptocurrency to recover their encrypted data.

NotPetya mimicked a ransomware attack by encrypting the data and leaving behind a ransom note complete with payment instructions. However, the organizations that submitted their payments through cryptocurrency as instructed never heard back from the attacker and could not recover their data. These organizations had to resort to manual procedures and disaster recovery plans, including the recreation of information systems and data without backups. There was some conjecture that the ransomware operators had failed to create the recovery keys or did not have sufficient infrastructure to respond to many successful attacks. No one suspected that the threat actors had achieved all of their goals through the distribution of NotPetya except for a few threat intelligence groups.

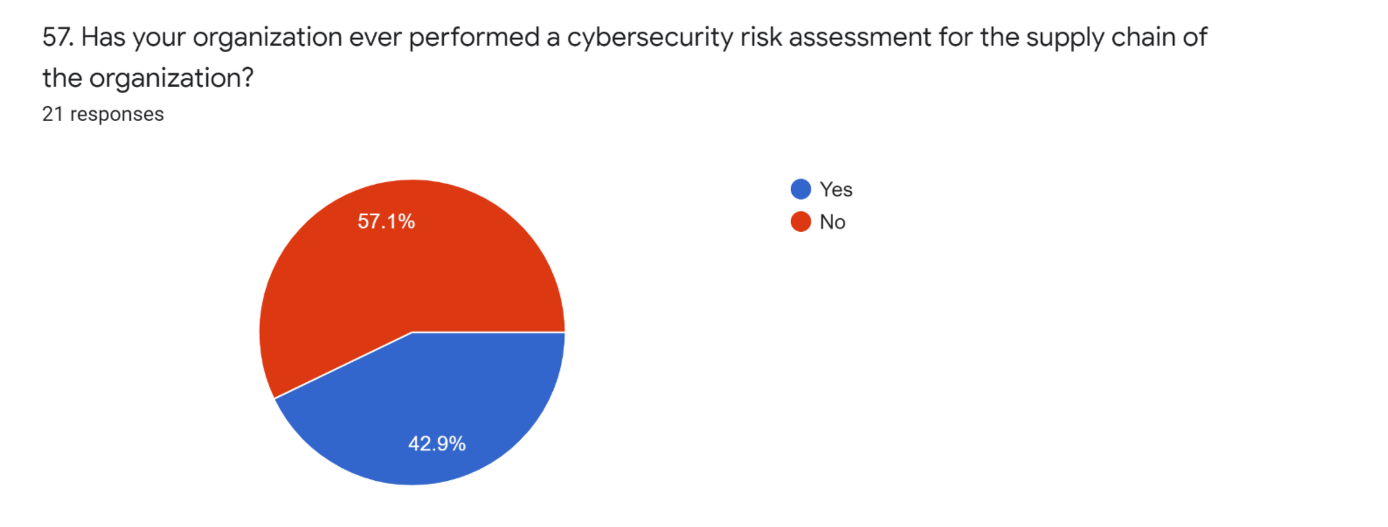
The Linkos Group is a technology firm that currently owns M.E.Doc, a widely used accounting software system in Ukraine. This software contains links to the Ukrainian tax systems, making it highly successful. It is similar in functionality to TurboTax or QuickBooks, which is used in the United States. Most organizations operating in Ukraine were utilizing the accounting software at the time of the NotPetya attack. The M.E.Doc software used an automatic update feature that allowed for the distribution of software fixes to their customers.

Russia has had a long history of conflict with the Ukraine, which has been carried out in cyberspace as well as on the battlefield. They saw the opportunity to severely impact businesses in Ukraine using the recent WannyCry ransomware as a cover for their true intentions. They compromised the M.E.Doc software update engine and configured it to deploy NotPetya to all businesses using the software. The Russian objective was to send a clear message to companies doing business in Ukraine. “If you do business in Ukraine, bad things are going to happen to you.”

NotPetya successfully attacked and destroyed the majority of Ukraine’s technology infrastructure. The list of casualties included hospitals, power companies, airports, and over 22 banks. This type of threat went under the radar of all of these companies who implicitly trusted the software update service for the M.E.Doc account software. Companies in equipment leasing and finance use many software applications with similar update functionality. These applications could use this type of functionality to download changes in interest rates, currency exchange rates, or other data-based exchanges, as well as software features and fixes.

Most organizations have not recognized this type of threat and do not have controls to prevent a future NotPetya style attack. It would be difficult since most software vendors provide updates in the same manner. A thorough due diligence risk assessment of these software vendors involved in the supply chain may uncover potential security threats. A whole industry has evolved to certify that organizations have the appropriate security controls such as the SOC, ISO 27000 series, CMMC, and HITRUST certification. However, this does not guarantee that an organization will not be compromised in the future. This is especially true if the attacker is a nation-state like Russia, as was the case in the NotPetya attack.

A supply chain attack like that used by NotPetya is the modern equivalent of the fabled trojan horse. It is even more difficult to detect in the digital world due to the interconnectivity required for modern business. This type of attack is still as viable as it was in 2017 and will probably occur again in the future. Organizations should still perform vendor supply chain assessments and consider restricting automatic data feeds and software updates were possible. Most of the equipment leasing and finance companies that participated in the survey conducted as part of this research have not performed a supply chain risk assessment.



57. Has your organization ever performed a cybersecurity risk assessment for the supply chain of the organization?
21 responses

Source: ELFF 2020 Cybersecurity Survey

The United States Department of Justice announced on October 19, 2020, that "a federal grand jury in Pittsburgh returned an indictment charging six computer hackers, all of whom were residents and nationals of the Russian Federation (Russia) and officers in Unit 74455 of the Russian Main Intelligence Directorate (GRU), a military intelligence agency of the General Staff of the Armed Forces." This statement confirmed the Russian government's involvement in NotPetya, although it offers no insight into the motivation behind the attacks. NotPetya was only one of the attacks confirmed in the statement, along with attacks against the French Elections in 2017 and the 2018 Winter Olympics. Organizations can no longer ignore the threat of state-sponsored activity, which must be considered in any threat assessment. The full listing of charges from the October 19 announcement against the Russian officers includes attacks on the:

- "Ukrainian Government & Critical Infrastructure: December 2015 through December 2016 destructive malware attacks against Ukraine's electric power grid, Ministry of Finance, and State Treasury Service, using malware known as BlackEnergy, Industroyer, and KillDisk;

- French Elections: April and May 2017 spear-phishing campaigns and related hack-and-leak efforts targeting French President Macron's "La République En Marche!" (En Marche!) political party, French politicians, and local French governments before the 2017 French elections;

- Worldwide Businesses and Critical Infrastructure (NotPetya): June 27, 2017, destructive malware attacks that infected computers worldwide using malware known as NotPetya, including hospitals and other medical facilities in the Heritage Valley Health System (Heritage Valley) in the Western District of Pennsylvania; a FedEx Corporation subsidiary, TNT Express B.V.; and a large U.S. pharmaceutical manufacturer, which together suffered nearly $1 billion in losses from the attacks;

- PyeongChang Winter Olympics Hosts, Participants, Partners, and Attendees: December 2017 through February 2018 spear-phishing campaigns and malicious mobile applications targeting South Korean citizens and officials, Olympic athletes, partners, and visitors, and International Olympic Committee (IOC) officials;

- PyeongChang Winter Olympics IT Systems (Olympic Destroyer): December 2017 through February 2018 intrusions into computers supporting the 2018 PyeongChang Winter Olympic Games, which culminated in the Feb. 9, 2018, destructive malware attack against the opening ceremony, using malware known as Olympic Destroyer;

- Novichok Poisoning Investigations: April 2018 spear-phishing campaigns targeting investigations by the Organization for the Prohibition of Chemical Weapons (OPCW) and the United Kingdom's Defense Science and Technology Laboratory (DSTL) into the nerve agent poisoning of Sergei Skripal, his daughter, and several U.K. citizens; and

- Georgian Companies and Government Entities: a 2018 spear-phishing campaign targeting a major media company, 2019 efforts to compromise the network of Parliament, and a wide-ranging website defacement campaign in 2019."

The most significant supply chain cyber-attack in modern history was unfolding as this research paper was being written. The attack's effects are very different from NotPetya but potentially more damaging in the long run. This attack was so severe that it has been labeled the cyber equivalent of the Pearl Harbor attacks on December 7, 1941 and will be a watershed moment for information security. The very definition of an open internet may well have to change to prevent attacks like this in the future.

SolarWinds is a technology company located in Austin, Texas, involved in this attack. The company is very well known within IT professional circles but not with those unfamiliar with backend IT operations. SolarWinds produces a software suite called Orion for monitoring technology infrastructure, including networks, servers, and databases. The software has been wildly popular in this specific niche market with over 300,000 customers due to affordable pricing and lack of competition. SolarWinds Orion was installed into the heart of these companies' information systems and often trusted with full administrative access. There was no more perfect target for a supply chain attack than SolarWinds.

SolarWinds advertised many customers on their website along with their logos which included most U.S. Government agencies and most of the Fortune 500. The customer listing was taken down in December 2020, shortly after the attack hit the news. However, this listing was probably a factor in the attacker's decision to target the company. The successful insertion of malicious code into SolarWinds Orion would let the attackers into the heart of U.S. Government and major corporation data centers unnoticed. The operation would have to be covert as the stakes were high if the attackers were caught in the act. The temptation was just too much to resist.

There is speculation into how the attackers gained initial access into the SolarWinds network and, ultimately, the build engine for their software. They thoroughly reviewed the Orion source code to gain a detailed understanding of how the software was built. They needed to make sure that their modifications would go unnoticed. They tested their backdoor, which looked for specific operations being performed during the build process. The backdoor would then inject their own test software into the source code while it was being compiled. The SolarWinds build software then cryptographically signed the completed binary code with their own certificate. The test was successful, and SolarWinds did not notice the modification.

The attackers had learned enough about the SolarWinds software build process to deploy the real payload. They changed their test process to include a software trojan in the Orion software. SolarWinds posted the software updates on their support portal, unaware of the trojan back door inserted in March 2020. Over 18,000 customers downloaded updates for SolarWinds Orion between March and December 2020, and not one had detected the trojan backdoor. The attackers allegedly gained access to the systems of many branches of the U.S. Government, including:

1. Department of State
2. Department of Homeland Security
3. National Institutes of Health
4. The Pentagon
5. Department of the Treasury
6. Department of Commerce
7. Department of Energy, including the National Nuclear Security Administration.

The attackers infiltrated organizations in multiple sectors, including finance, healthcare, and high-tech. Specific corporations including Intel, Cisco, VMWare, and Microsoft have confirmed using the compromised versions of the Orion software. Microsoft has stated that the attackers viewed source code for both its Windows and Office products, although they deny any code was stolen. Microsoft also stated that the attackers were targeting their Office 365 product once a company had been compromised to gain access to email and other sensitive documents in the cloud.

The U.S. Department of the Treasury confirmed that their Microsoft Office 365 system had indeed been compromised using the technique Microsoft had documented. This was not due to a weakness in Office 365 but a result of the privileged position the attackers had in each network. The attackers moved stealthily using stolen administrative accounts from the Orion software. Their attacks blended in with normal activity in order to go unnoticed. They targeted the system that synchronized internal network accounts to Office 365 and gained complete control. It has been confirmed that the attackers were reading emails from the Department of the Treasury and Department of Justice early in the investigations. There will undoubtedly be additional findings where the attackers gained access to more government agencies and commercial companies as these investigations continue.

The Cybersecurity & Infrastructure Security Agency (CISA) has released the following alert that indicates this attack was successful against several commercial and government targets.

"ALERT – APT Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

CISA is tracking a significant cyber incident impacting enterprise networks across federal, state, and local governments, as well as critical infrastructure entities and other private sector organizations. An advanced persistent threat (APT) actor is responsible for compromising the SolarWinds Orion software supply chain, as well as widespread abuse of commonly used authentication mechanisms. This threat actor has the resources, patience, and expertise to gain access to and privileges over highly sensitive information if left unchecked. CISA urges organizations to prioritize measures to identify and address this threat.

Pursuant to Presidential Policy Directive (PPD) 41, CISA, the Federal Bureau of Investigation (FBI) and the Office of the Director of National Intelligence (ODNI) have formed a Cyber Unified Coordination Group (UCG) to coordinate a whole-of-government response to this significant cyber incident."

The cybersecurity firm FireEye finally detected the attack. They had been doing an internal investigation as they noticed that the security software they use in penetration tests had been stolen. It has not been confirmed if the SolarWinds hack was the cause of this breach, but it was during the investigation that FireEye noticed artifacts in their Microsoft Office 365 accounts. The attacker attempted to maintain persistence and needed to add multifactor authentication to their account to meet FireEye's security requirements. The activity was flagged as unusual and tipped FireEye off that their system had been compromised. They sounded the alarm on December 13, 2020, and released the technical details of the compromise publicly on their website.

FireEye attributed this attack to a Russian government-backed group called APT29 by comparing the attackers' tactics and tools. U.S. intelligence agencies confirmed later that the attack was "likely" to be orchestrated from Russia but did not name specific individuals or groups. The motive for these attacks remains elusive but is believed to be an intelligence-gathering effort. Russia has continued to deny any involvement in the attack. Many governments perform espionage operations, including the United States, often overlooked.

Organizations in the equipment leasing and finance industry were undoubtedly affected by this attack. The attackers could have been looking for information on specific customers, including defense contractors or healthcare companies researching COVID 19, for example. The information included in leasing contracts could help state-sponsored actors determine an organization's current operations, the status of product development, financial situations, and even identify vendors for additional supply chain attacks. This makes the organizations in the equipment leasing and finance industry targets for these types of operations in the future.

Both examples of supply chain attacks mentioned in this report were wildly successful. The NotPetya attack was so successful that it escaped from networks initially targeted to come back and infect networks in Russia. The impact of the SolarWinds Orion supply chain attack is yet to be understood but was a phenomenal success for the attackers given the number of organizations we know were compromised. Success breeds imitation and innovation. Supply chain attacks are not only here to stay but will become more invasive and numerous in the future.

Insider Threats

There are much easier ways for well-funded criminals or state-sponsored actors to access an organization's information systems. Attacking a software supply chain will take a considerable amount of time to execute. The attacker must identify the target's software and determine any potential vulnerabilities. The culmination of the final attack may take months to reach a payoff. However, an attacker could just simply look for an insider to pay off or even a customer to get them inside much more quickly. Criminal organizations are so well funded that payoffs and blackmail are effective options. These attacks can be just as damaging as supply chain attacks and even more challenging to detect.

The age of social media has provided the attackers with a wealth of information about the people that work for an organization. They will often try to connect with people on LinkedIn or Facebook using fake accounts to access contacts and work experience. An attacker searching for specific positions within the company to target can act as a job recruiter to gain an employee's attention. Information about what technology is in use at the organization can be found by looking through the IT staff's LinkedIn accounts.

An attacker can also use information gained from other data breaches to target employees with financial problems or those with blackmail potential. Breaches that include financial information about a target that could come from a bank or credit monitoring agency are extremely useful for identifying those who might be open to financial fraud. Healthcare data breaches can include information about substance abuse or other emotional issues that could lead to a blackmail situation. Employees who use web services for pornography or other morally questionable activity may also be targets if a criminal organization gains access to these types of data breaches.

Organizations can use canaries to attempt to discover where their insider breaches are. This is a highly effective yet inexpensive approach. A basic example would be to create a fake document and put it in an email message in the CEO's inbox. The document could be something fictitious about closing a division or launching a new product. The insider will access the file and trip the monitoring alarms because there is no reason that these fake files would ever be accessed for legitimate purposes. The information may also leak to a competitor or the press. However, the culprit will most likely be identified in the process.

The insider risk is real and can have catastrophic impacts on companies through cyberattacks and business espionage. Organizations need to integrate their current political and business knowledge to build defenses against these types of attacks. It is important to understand critical processes and develop strong segregation of duties along with the appropriate audit controls. The security industry keeps focusing on tools and technologies while not addressing these fundamental issues. Organizations that chase the silver bullet through technology spending to address the insider threat will not be successful.

Evolution of the Attacker

This section started with the description of the hacker from the movie War Games as defined by 1980's pop culture. The impression of the socially inept outcast that spends time in their basement in a black hoodie is woefully outdated and outright dangerous today. Today's attackers are well funded, and their operations are run as a professional business in most cases. These groups' leaders are more likely to have an MBA and be reading Barron's or the Wall Street Journal than the stereotypical image of playing video games and skipping high school classes. Organizations continue to underestimate this new class of informed and intelligent adversaries.

These criminal organizations hire staff with employee benefits, vacation time, and have regular company meetings. The staff tends to work standard office hours and feel the same apathy towards their job as any other modern cubical worker. The organizations are usually run under an unassuming name like the internet Research Agency to reduce suspicion. They are interested in direct cyberattacks and will work to understand business processes, financial flows, and political nuances to achieve their objectives.

The United States indicted 13 Russian citizens and 3 Russian entities in February 2018, including the internet Research Agency for interfering in the 2016 U.S. Election. The internet Research Agency employed over 1,000 staff in 2015 and had direct ties to Russian intelligence agencies. They are experts in mining social media sites like Facebook and planting stories meant to change opinions or divert attention from other types of intelligence operations. They have been known to interfere in sensitive political situations and business relations worldwide. This group is just an example of many operational with state sponsorship or are conveniently ignored by the state. These types of attackers have the potential to do far more damage than the stereotypical rebellious teenager in a black hoodie. Organizations have to understand this type of adversary to build appropriate defenses.

Information Operations

The internet Research Agency is engaging in a different type of cyber activity than just what is commonly thought of as hacking. They are engaging in what is referred to as information operations. This technique utilizes offensive hacking operations and social media to attempt to reshape opinions and change perspectives. The targets could be as broad as a political election and as focused as breaking up M&A activity to give a more favored company a competitive advantage. This type of interference in international business deals becomes more common where one of the organizations involved has some level of state-run ownership.

Information operations include any cyber activities meant to disrupt competitors and are often blamed solely on nation-states. However, U.S. companies have also engaged in these types of attacks. Ticketmaster agreed to pay a $10 million fine over hacking their competitor. They had hired an employee from a competitor that knew internal passwords and used them without authorization to collect business intelligence. The two employees involved were fired in 2017 and not condoned by Ticketmaster, but the damage had been done. This incident demonstrates why these types of attacks are so attractive to adversaries as they can be easy to perpetrate.

Other types of information operations attacks have involved sowing disinformation through other fake sources. Attackers will appear to be legitimate businesses with sales intelligence data that happens to be fabricated. The organization purchases the data and makes the wrong business decisions that benefit its competitors. The attackers may have been financed directly from the competitor or state-sponsored with more political agendas.

Information operations can also be used for intelligence and surveillance activities. An equipment finance organization providing funding for a company developing a new product could be a target for information operations. A competitor could attempt to gain access to the metadata included in the financial transactions to determine more about the product being developed. This could be information about additional suppliers that specialize in manufacturing specific products and the dates of shipments, and the associated payments. The competitor can then use the metadata to piece together a complete picture of the product being developed.

Ransomware and Offensive Hacking Operations

The explosive growth of Ransomware continued in 2020 as criminal organizations improve their tactics and refine their operations. Ransomware continues to be one of the most common types of attacks given the profitability and the ease of converting technical vulnerabilities into revenue. According to a study conducted by Check Point Research, ransomware attacks increased 98.1% in the United States through the third quarter of 2020. The same study claims that there is a new victim of ransomware every 10 seconds worldwide. Organizations located in the United States are the most targeted by attackers.

Emotet was suspiciously missing for about five months in 2020 but came roaring back as the most popular malware used for ransomware attacks. Emotet started as a banking trojan that would target a victim's login credentials to their banks and financial accounts. It spreads primarily through email attachments such as Adobe PDFs or macro-laden Microsoft Word documents. The victim opens the attachment, usually sent from a compromised partner or vendor, and unknowingly installs the trojan backdoor into their network. The original operator of the Emotet attack then sells the compromised network to a ransomware group that carries out the final attack. It is common for the bank accounts of the victims to be targeted at the same time the ransomware is deployed.

There is a complete business ecosystem that has evolved to support ransomware operations. The sale of compromised credentials and networks on the dark web has become a booming business. Attackers that don't possess the technical skills or infrastructure necessary to carry out the ransomware attacks can use Ransomware-as-a-Service (RaaS) models. These services will carry out the attack and provide the customer support necessary to help the victims convert cash to Bitcoin for a percentage of revenue. This business ecosystem is the primary reason that ransomware attacks are continuing at such a rapid pace.

Ryuk is one of the most devastating types of ransomware seen in the last few years. This ransomware can be deployed through a trojan and often pairs with Emotet for the initial compromise. The attackers will often hire contract hackers to exploit the victim's network. They will move silently through the network, acquire administrative credentials, and identify targets. They are well-versed in enterprise backup solutions like Veeam, which many organizations use. They will destroy these backups and remove shadow copies from all of the Windows machines to give the victims no choice but to pay up. They deploy the ransomware to all network systems at once using scripts and scheduled tasks on the target machines.

Ransomware attackers are using new techniques to prevent attribution. Security researchers used to be able to identify an attacker by the evidence left behind. Every programmer has a different style which could be identified if the researcher can review enough artifacts. This is similar to being able to identify an artist after looking at multiple paintings because of similarities in style and technique. However, attackers have adopted a technique called "red sourcing" to prevent being identified by their programmatic artifacts. Red sourcing is simply using off-the-shelf software for attacks that cannot be attributed to anyone. This includes the use of security tools like Metasploit and Cobalt Strike, for example.

Another technique for avoiding identification and attribution is called living-off-the-land or LOL. Microsoft Windows offers many different tools for automation and remote administration. These tools were intended to be used by system administrators for managing Windows systems. Attackers use these tools because they are always allowed by antivirus and blend in with legitimate system administration activity. Microsoft

PowerShell and tools like WMIC (Windows Management Interface Command Line) and Remote Desktop are built in Windows components commonly abused by ransomware attackers.

Ransomware attackers have adopted a cloud-first model for their infrastructure, just like any other business. The cloud enables them access to unlimited cheap resources that will blend in with other legitimate cloud traffic. Attackers are known to look through source code hosted on websites like GitHub looking for hard-coded logins to cloud platforms like Amazon. This allows them to scale up quickly using a stolen account that cannot be traced back to the attackers. Victims monitoring their network will just see traffic from an Amazon host that cannot be decerned from any legitimate business traffic until it is too late.

2020 saw a change in tactics where ransomware attackers take copies of the victim's data before performing the encryption. This gives the attacker more leverage with the victim as many organizations must comply with breach notification regulations. The ransom amount increases if the victim does not pay and then ultimately leads to the attackers dumping the data on a public website. The combination of business interruption and a data breach can be lethal to an organization that has become a victim. This change in tactics has also led to much higher monetary demands from ransomware attackers.

Future Threats

Cybersecurity threats evolve so quickly that they can be almost impossible to predict accurately. Cybersecurity's operational tempo will continue to increase and strain already thin information security departments. The use of contracted hackers and "hands-on keyboard" professionals will continue to increase and target smaller organizations with fewer defenses. Ransomware will predictably spread to infecting IoT devices and PLC systems that could impact human lives. There may even be successful attacks against the power grid or other critical infrastructure. It is going to be a very difficult time for defenders.

There will be a continued fusion of criminal and state-sponsored activity, increasing the complexity and severity of attacks. Several countries already look the other way when a criminal organization located in their borders targets businesses in other countries. Strategic displacement of business processes must be recognized as targets along with the traditional technical attacks of the past. Organizations will need to be both highly technical and understand the global political and business environment. It will be critical to target the attackers' motives instead of just focusing on technological tools to build a better organizational defense.

The bar will continue to rise for information security spending to keep up with these threats in the future. Startups or smaller organizations will find it increasingly difficult to absorb these expenses. Attackers will target those organizations with the weakest defenses making these organizations prime targets. Cybersecurity could become a barrier to entry for businesses in the future that cannot afford to invest in the appropriate personnel and resources and remain viable.

Case Study – Phishing and Ransomware Example

It was getting close to 5:00 PM, and Shannon watched many of the staff leave the office. She was packing up her laptop to work at home as she was still finishing the budget for next year. Shannon was used to being one of the only people left in the office late at night. She works as the CFO for a small firm with only about 20 employees, so she is used to having multiple responsibilities. She oversees many operational aspects outside of her CFO duties, which the company's owners appreciate.

One of those responsibilities that she doesn't get enough time to address is Information Technology. She has seen the value of using Information Technology to increase efficiencies and has implemented several new software packages, including a small-business Enterprise Resource Planning system. She pulled the company through this implementation, eliminating the paper and spreadsheets that made up their business processes in the past. This project demonstrated the value of Information Technology to the company's owners. The implementation of this significant project enhanced the future growth of the organization.

The company has not had the resources to employ a full-time IT professional and outsources all PC desktop and server maintenance. This has worked out well for the company as they have been able to keep their spending low on Information Technology. They did purchase new server equipment for the Enterprise Resource Planning System, but the rest of the PCs and network infrastructure are older technology. Their outsource provider did recommend upgrading the older PCs to Windows 10, which saved the company the cost of purchasing new desktop computers.

She had read about the increasing ransomware threats online. Her company had made sure to do basic security measures, including using the built-in antivirus in Windows 10. She had read that it worked well, especially for the cost. They had implemented a SonicWall firewall several years ago, and it seemed to be doing the job. Their passwords were fairly simple because it was just too difficult to get everyone in the office to change them. These passwords were only used on internal systems, so her IT Support company didn't feel it was an extreme risk. She was reassured that hackers would probably target larger companies anyways due to their deeper pockets.

She continued to shut down her laptop and turned to her desktop computer to make sure she was closed out of the files she would want to access from home. This was when she noticed the error messages on her screen. Her desktop computer reported that it could not access a critical file. The only option she was given was to click "ok," which was then replaced with another error message. She attempted to open files on her desktop but noticed they all had a strange file extension on them. She realized that something was very wrong.

She ran into the tiny server closet right across from her office to shut down the new servers running the new Enterprise Resource Planning system and hosted their shared files. She quickly pulled the power plugs of the back of the servers and reassuringly heard the loud cooling fans spin down. She pulled the network cable out of the back of the Network Attached Storage unit that housed their backups. She then sprinted down the hallway, unplugging desktop computers as quickly as possible. She then picked her iPhone, noticing how dark and quiet the office was after 5:00 without computers running, and dialed her outside the IT Support company.

What she could not have known was that the owner had received a phishing email earlier in the day. The email did not appear suspicious as it came from a reliable vendor that the owner recognized. The owner did not know that the vendor's email account had become compromised and was being used to distribute phishing emails. The email stated that he needed to verify an invoice attached as a Word document. He opened the attachment in Word on his Windows 10 workstation and was greeted with a message that he needed to enable macros to view the file's contents. He had not needed to do this in the past with this vendor, but he still did not realize the file's malicious nature.

He enabled the macros within Microsoft Word, and nothing appeared to happen. He didn't see the invoice that was supposedly attached to the file. This seemed odd, but the invoice file could have been corrupted. He sent an email back to the vendor stating that he could not open the file and could they please resend it. He continued to work the rest of the day and logged into several banking systems to validate deposits and any investment-related activity. There were no clues that he had just given control of his system over to a criminal.

The malicious program that was now running on his computer was collecting his passwords from memory and by monitoring his keystrokes. Each time he logged into the banking system, they could steal the authentication information to the company accounts. The malicious code was able to bypass all of the security features in the fully updated installation of Windows 10, including the Windows Defender Antivirus. They began accessing his accounts as soon as he left his office for another meeting.

The owner started receiving phone calls from his bank in the afternoon leading up to the ransomware attack. The criminals had attempted to make a sizeable fraudulent wire transfer overseas, and the bank had caught it. The bank recommended that he change all of his passwords on his financial systems, which is probably how they gained access to his accounts. He thanked them and left his accounts frozen until he got out of his meeting and could change his passwords. He had been lucky that the bank had caught the attack, and the company suffered no financial losses.

The criminal organization that planted the malware called Emotet realized that they made a mistake trying to pull out so much money at a time. This always set off red flags, but they only had a certain amount of time to reuse the owner's credentials before the session token on the website would expire. This didn't mean that they couldn't still profit from the intrusion that they just spent several days planning. They could use the access they had acquired to the company network to install ransomware. They installed the Ryuk ransomware on the owner's desktop computer and began to infiltrate the company's network.

The criminal group called in their black-hat hackers as the owner's username and password only got them so far. A successful ransomware attack relies on gaining full administrative privileges to the target network. This is where the hackers come in to elevate their privileges and launch the attack. They first steal all of the passwords from the owner's system, including the administrator account. A script is uploaded to the owner's computer that enumerates all of the network's desktop and server systems as initial reconnaissance.

They noticed that the administrator account password from the owner's computer worked on other computers throughout the company. However, it doesn't work on the company servers. They search for other locations where a full network administrator account is logged in using the same local administrator password. They were successful because the administrator account was used on a workstation that was acting as an interface to send and receive financial information. They pull the network administrator password from memory on the target computer and now have control over the entire network.

The attackers uploaded their encryption tool and several other administrative tools to the workstation to begin the distribution. They used the file that contained all of the computer names on the network to automate a script to distribute their files. They were trying something new this time to use the task scheduler built into Windows to launch their attack. This had several advantages in that all of the computers will begin encrypting simultaneously, and a rebooted computer will resume encrypting files after a reboot. They used their administrative tools to set all of the computers on the network to execute the ransomware at 5:00 PM. Knowing that most people would be leaving for the day gave ample time for the encryption process to complete overnight.

The ransomware executed as scheduled and began to encrypt files across all of the machines on the network. The old Network Attached Storage (NAS) unit holding the backups was the only hold-out as it was so outdated that the task scheduler did not function correctly. The virtual servers were attacked from two sides as the host encrypted the virtual disks and the virtual servers encrypted the files they contained. The Primary Domain Controller, which performs all of the authentications on a Windows network, was encrypted along with all of the data in the new Enterprise Resource Planning system. The CFO pulling the power managed to save one of the Domain Controllers, but not before it replicated the authentication data from the infected Domain Controller corrupting all user accounts and passwords.

This had the effect of rendering the network inoperable as even internet browsing was not working on the company network. The CFO was able to at least communicate through the guest wireless network provided through the cable modem. However, she had to resort to using her personal email account because her company account was no longer functioning. Her organization ground to a halt as the majority of the work done by the company on the computer was no longer possible.

The first person on the scene was the outside consultant who provided support for the ERP system. He arrived early the next day after the initial to determine the damage and begin recovery. He reviewed the integrity of the ERP backups, which had been stored on the NAS, and copied them offsite for testing back at his office. However, there was no were to recover the backups to the company network as all of the servers were unusable. He worked with the CFO to try and understand the extent to which criminals were still in the network and quickly found that type of work was outside of his expertise. He recommended that the CFO bring in an information security specialist to diagnose, contain, and help bring the company systems back online.

The CFO contacted someone she knew previously and received a Statement of Work for emergency recovery operations. The company did not have any pre-existing relationship with a security company for incident response services. The hourly rate for this type of response was 50% higher than their standard rate given the short notice and the after-hours support requested. She had no choice but to move forward to get her company back up and operational. The cost of the organization being down far outweighed the costs of bringing the security consultant onsite. The CFO didn't feel that the option of paying the ransom made sense as there was no guarantee that they would recover their files. The ransom that the criminals demanded was far more than her company could afford, even if they wanted to pay it.

The security specialist arrived on a Thursday afternoon and began to triage the available evidence. Discussions with the owner revealed the initial entry point of the infection. The owner's computer was encrypted, but the attack email was found in his email inbox. The attachment was analyzed and quickly identified as the Emotet trojan, which was known for stealing banking credentials and dropping additional payloads. The document files on the computers had new file extensions of .RYK instead of the standard .DOC, .XLS, or .PPT showing that they had been encrypted. Each folder of documents also contained a new file called "RyukReadMe.txt". The contents of that file are shown below with the original misspellings.

> "Your network has been penetrated.
>
> All files on each host in the network have been encrypted with a strong algorithm.
>
> Backups were either encrypted
>
> Shadow copies also removed, so F8 or other methods may damage encrypted data but not recover.
>
> We exclusively have decryption software for your situation.
>
> More than a year ago, world experts recognized the impossibility of deciphering any by means except the original decoder.
>
> No decryption software is available in the public.
>
> Antiviruse companies, researchers, IT specialists, and no other persons cant help you encrypt the data.
>
> DO NOT RESET OR SHUTDOWN – files may be damaged.
>
> DO NOT DELETE readme files.
>
> To confirm our honest intensions.Send 2 different random files and you will get it decrypted.
>
> It can be from different computers on your network to be sure that one key decrypts everything.
>
> 2 files we unlock for free.
>
> To get info (decrypt your files) contact us at
>
> redacted@protonmail.com
>
> or
>
> redacted@tutanota.com
>
> You will receive btc address for payment in the reply letter
>
> Ryuk
>
> No system is safe"

The security specialist was able to identify this ransomware variant as Ryuk quickly. This ransomware was responsible for many public attacks, including municipalities, school districts, healthcare organizations, and financial institutions. They always ask for payment in Bitcoin, a cryptocurrency that anonymizes their identity, although not their transactions. However, the ransomware operators are savvy and know how to hide their tracks by using multiple throw-away email accounts and many different Bitcoin addresses for payment. Ryuk operators netted over 705.80 BTC across 52 known transactions for a total current value of USD 3,701,893.98 in the first four months of operation. The Ryuk operators may use many more Bitcoin addresses. The table below shows the Bitcoin addresses and values at the transaction time.

BTC Address	Total Received	No Received	Total Value (USD)
12vsQry1XrPjPCaH8gWzDJeYT7dhTmpcjL	55	3	$221,685.46
1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY	182.99	10	$734,601.91
1FtQnqvjxEK5GJD9PthHM4MtdmkAeTeoRt	48.25	4	$188,974.93
14aJo5L9PTZhv8XX6qRPncbTXecb8Qohqb	25	2	$113,342.70
1E4fQqzCvS8wgqy5T7n1DW8JMNMaUbeFAS	0.001	1	$6.47
1GXgngwDMSJZ1Vahmf6iexKVePPXsxGS6H	30	3	$132,654.91
1Cyh35KqhhDewmXy63yp9ZMqBnAWe4oJRr	0	0	$0.00
15LsUgfnuGc1PsHJPcfLQJEnHm2FnGAgYC	0	0	$0.00
1CbP3cgi1Bcjuz6g2Fwvk4tVhqohqAVpDQ	13	2	$82,917.49
1Jq3WwsaPA7LXwRNYsfySsd8aojdmkFnW	35	1	$221,979.83
129L4gRSYgVJTRCgbPDtvYPabnk2QnY9sq	0	0	$0.00
1ET85GTps8eFbgF1MvVhFVZQeNp2a6LeGw	3.325	1	$12,661.74
1FRNVupsCyTjUvF36GxHZrvLaPtY6hgkTm	38.99	3	$246,893.95
1CW4kTqeoedinSmZiPYH7kvn4qP3mDJQVa	24.077	2	$152,727.13
13rTF3AYsf8xEdafUMT5W1E5Ab2aqPhkPi	0	0	$0.00
17zTcgKhF8XkWvkD4Y1N8634Qw37KwYkZT	0	0	$0.00
14dpmsn9rmdcS4dKD4GeqY2dYY6pwu4nVV	0	0	$0.00
17v2cu8RDXhAxufQ1YKiauBq6GGAZzfnFw	0	0	$0.00
1KUbXkjDZL6HC3Er34HwJiQUAE9H81Wcsr	10	1	$63,358.27
12UbZzhJrdDvdyv9NdCox1Zj1FAQ5onwx3	0	0	$0.00
1NMgARKzfaDExDSEsNijeT3QWbvTF7FXxS	0	0	$0.00
19AE1YN6Jo8ognKdJQ3xeQQL1mSZyX16op	25	1	$164,774.21
1L9fYHJJxeLMD2yyhh1cMFU2EWF5ihgAmJ	40.035	4	$259,478.16
18eu6KrFgzv8yTMVvKJkRM3YBAyHLonk5G	30	1	$198,651.35
1C8n86EEttnDjNKM9Tjm7QNVgwGBncQhDs	30.0082	2	$194,113.76
12N7W9ycLhuck9Q2wT8E6BaN6XzZ4DMLau	0	0	$0.00
162DVnddxsbXeVgdCy66RxEPADPETBGVBR	0	0	$0.00
1ChnbV4Rt7nsb5acw5YfYyvBFDj1RXcVQu	28	2	$175,177.98
1K6MBjz79QqfLBN7XBnwxCJb8DYUmmDWAt	1.7	2	$12,455.95
1EoyVz2tbGXWL1sLZuCnSX72eR7Ju6qohH	0	0	$0.00
1NQ42zc51stA4WAVkUK8uqFAjo1DbWv4Kz	0	0	$0.00
15FC73BdkpDMUWmxo7e7gtLRtM8gQgXyb4	0	0	$0.00
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk	10	2	$64,990.62
1CN2iQbBikFK9jM34Nb3WLx5DCenQLnbXp	15	1	$92,934.80
1LKULheYnNtJXgQNWMo24MeLrBBCouECH7	0	0	$0.00
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj	50.41	3	$326,477.83
1KURvApbe1yC7qYxkkkvtdZ7hrNjdp18sQ	0	0	$0.00
1NuMXQMUxCngJ7MNQ276KdaXQgGjpjFPhK	10	1	$41,034.54
Totals	**705.7862**	**52**	**$3,701,893.99**

Table 1 - BTC Addresses Identified by CrowdStrike - https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

The CFO had no intention of paying the ransom, so the security specialist recommended rebuilding all of the workstations and servers from scratch. This included installing Windows 10 and Windows Server from the original media on the appropriate hardware. The entire Windows network infrastructure had to be rebuilt, and user accounts recreated with new passwords. The security specialist built out a security-hardened configuration for the Windows computers to prevent the attacks from occurring in the future. The default Windows installation was not secure enough for corporate use without these additional configuration changes.

The ERP consultant determined that the application backups were usable and began to restore the application onto the rebuilt servers. The old Windows NAS ended up saving the organization as it wouldn't execute the ransomware correctly. The attackers did try to delete all backups from the computers by removing Shadow Copies. This is when Windows maintains previous versions of files that can be restored easily. However, the old Windows NAS did not support the Shadow Copy commands that the attackers sent to remove any older files. The existence of this unsupported old Windows NAS was the primary reason for the organization's rapid recovery.

The security specialist continued to review the network's security capabilities to prevent these attacks from occurring in the future. The built-in Microsoft Defender was replaced with a cloud-based antivirus product that provided alerting and daily reporting of threats. The old SonicWall firewall that was in place was also unsupported, and the subscriptions for malware protection had expired. The firewall had logged the inbound ransomware email as a potential threat but did not block it due to the lack of an adequate configuration. A new SonicWall was put in its place with the added security subscriptions configured correctly to better respond to inbound threats.

The team worked through the weekend and had a functioning system just a week after the initial incident. The recovery effort took over 150 manhours to rebuild the small-business network with a usable backup. The company was able to recoup the expense of both consultants under their cyber liability insurance policy. This incident could have been far worse, but the CFO's quick action and the luck of running an outdated NAS system that was not compatible with the ransomware gave the organization a fighting chance to recover. It would have been a far different story had the ransomware group had longer to work on attacking the NAS and destroying the backup.

Lessons Learned

Invest in email security tools that filter malicious content.

Email continues to be the primary attack point for most ransomware and fraudulent scams. An updated email security system could have caught and prevented this attack from starting. These systems should not only flag malware through matching signatures but also flag messages based on behavioral factors and other indications of compromise. The Word document that was attached to the email that was sent to the owner contained a macro that is out of the ordinary. This should have been a red flag for any email security system to quarantine the message.

Review the need to allow older versions of Microsoft Office attachments

The macro that was contained in the Word document, in this case, was using the old file format of .DOC that was replaced in Word 2007 by .DOCX. Criminals prefer the .DOC format because it is binary, making it easy to hide any macros from the analysis. The newer .DOCX version is based on XML and easily scanned for malicious content as it is text-based. All versions of Office since 2007 can use the new format, so the interruption to the business is minimal for the amount of protection blocking the old formats can offer. This block should include all older Office formats, including .DOC, .XLS, and .PPT.

Always have "Defense in Depth"

Security professionals refer to Defense in Depth as having more than one security control in place in case the other one fails. This company was relying only on the base install of Microsoft Defender to defend their company against ransomware. They had no additional protection once the attacker bypassed this software. The firewall could have had the ability to scan for any potentially malicious software, such as another email security product. The attackers would then have to break through three different systems to deploy their ransomware successfully.

Get and maintain cyber liability insurance

The company did have cyber liability insurance in place, which covered the expenses involved in recovering from the incident. Recovery from this type of security incident could cost anywhere from $20,000 to over $2,000,000, depending on the severity. According to a leading cyber liability insurance company, the average ransom has increased 47% in Q2 of 2020 to $338,669. The company in this case study would have had to pay a ransom if the backups had been destroyed, which could have been catastrophic for the business.

Monitor and maintain infrastructure and security tools

The outdated firewall and security subscription service contributed to the success of this attack. The firewall should have been replaced with an updated security subscription earlier. However, most small businesses do not have local IT resources to monitor their inventory's health. This can be solved by hiring an IT consultant to review your infrastructure periodically and maintain this inventory. The cost will be a minimal impact on the budget and could literally save the organization.

Acquire and Implement end-point protection software

Current antivirus software is a must-have in the current security environment. However, basic antivirus software does not protect against unknown threats. Antivirus software must have seen the malicious software previously to detect it and prevent it from running. Most new malware is generated automatically and customized for each target to bypass these old antivirus techniques. Modern end-point protection software uses other techniques such as monitoring behaviors of software to prevent critical operations from occurring. A program should not need to connect directly to memory to attempt to capture passwords, for example. These newer end-point protection tools provide much more in-depth protection against threats from malicious software.

Analysis of Recommended Cybersecurity Measures

Much of this study has been spent on discussing the potential cyber threats and business impacts to companies in the equipment leasing and finance industry. The general message has been that the threats are getting more sophisticated and challenging to defend against. The attackers are well funded and targeting businesses for economic gain, espionage, and even competitive advantage. Presenting this type of information is difficult as it is often labeled as targeting fear, uncertainty, and doubt. However, businesses need to get comfortable with discussing these cybersecurity risks to build more robust defenses. Businesses will never successfully defend their networks if they do not understand their adversaries and their tactics.

The reality of the situation is that any network connected to the internet is already at high risk of compromise. No business in the equipment leasing and finance industry has the unlimited resources to protect their networks from state-sponsored actors. This doesn't mean that businesses shouldn't utilize internet-connected technology to increase efficiencies. It means that businesses need to understand and manage the risks associated with the use of internet-connected technologies. Any technology initiative's value must be realistically considered against the cybersecurity risks, so the business is not blindly stepping into a chasm.

The good news is that there are approaches to identifying and managing the risks of adopting and operating technology in the equipment leasing and finance business. Some vendors can provide excellent technical solutions to help defend your equipment leasing business from common cyber-attacks. However, there is a common misconception that acquiring these technological solutions is a silver bullet. The best security defenses must address not only the technology but also people and processes. Any solution that does not address all three areas is destined for failure.

Information security is a constant process of reevaluation to understand threats and reposition defenses based on updated threat intelligence. There is no "one size fits all" solution that can be adopted by all businesses unilaterally in the equipment leasing and finance space. However, there are some general recommendations that can help to improve the cyber resiliency of any business. Examples of these recommendations are included below from all three categories of controls, including people, processes, and technology. These recommendations are included to help businesses improve their defensive posture but are not a replacement for a full risk assessment and security remediation plan.

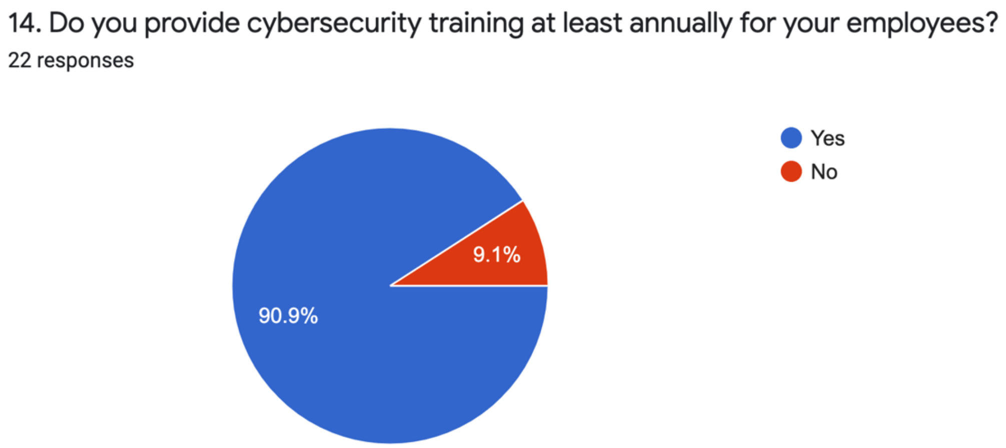
People (Culture Development and Training)

People are the number one target for cybercriminals as they are often the easiest to exploit. Through fraudulent phone calls, email phishing, and physical intrusions, social engineering attacks are far easier than discovering a new flaw in a commercial firewall. Therefore it is critical to build a culture of security within the organization. Employees need frequent reminders that they are critical to the company's cyber defense. They need the knowledge to make good security risk-based decisions during their daily routine as well as during the acquisition of new technologies. The security risk is reduced considerably when everyone in the company understands their role.

Training is the most obvious solution that should be considered, but not all training is considered equal. Companies often use web-based solutions that provide prebuilt training modules to save time. They can also provide for reporting to demonstrate compliance with regulations that require employee training. However, these templates may not be overly effective in communicating the necessary skills, and often staff just click through the questions to meet the requirements. There are good security training classes available online, but it will require extra time to review and select solid training programs.

An effective online training program should include multiple types of media and interaction with the students. The training material should be continually updated with information on current threats to the organization. Security policies and procedures also need to be included, so staff is aware of requirements for passwords, incident response, and encryption requirements. It is critical that the training includes material on the business impact of these threats and not just technical details. Online classes also need to be supplemented with other forms of training, including live demonstrations, staff meetings, newsletters, and company intranets. Practical security training should be approached more like an advertising campaign than traditional compliance classes using multiple mediums and frequent messaging.

The survey conducted as part of this research paper showed that many equipment leasing and finance organizations are already heavily involved in training their employees. Over 90% of the organizations that answered the survey are already providing cybersecurity training at least annually for their employees. 40% of these organizations are training their staff quarterly and even monthly. 63% of the companies also include contractors and temporary employees in their training programs which are best practices. These organizations will be reaping the benefits of having well-informed staff help defend against cyber-attacks.

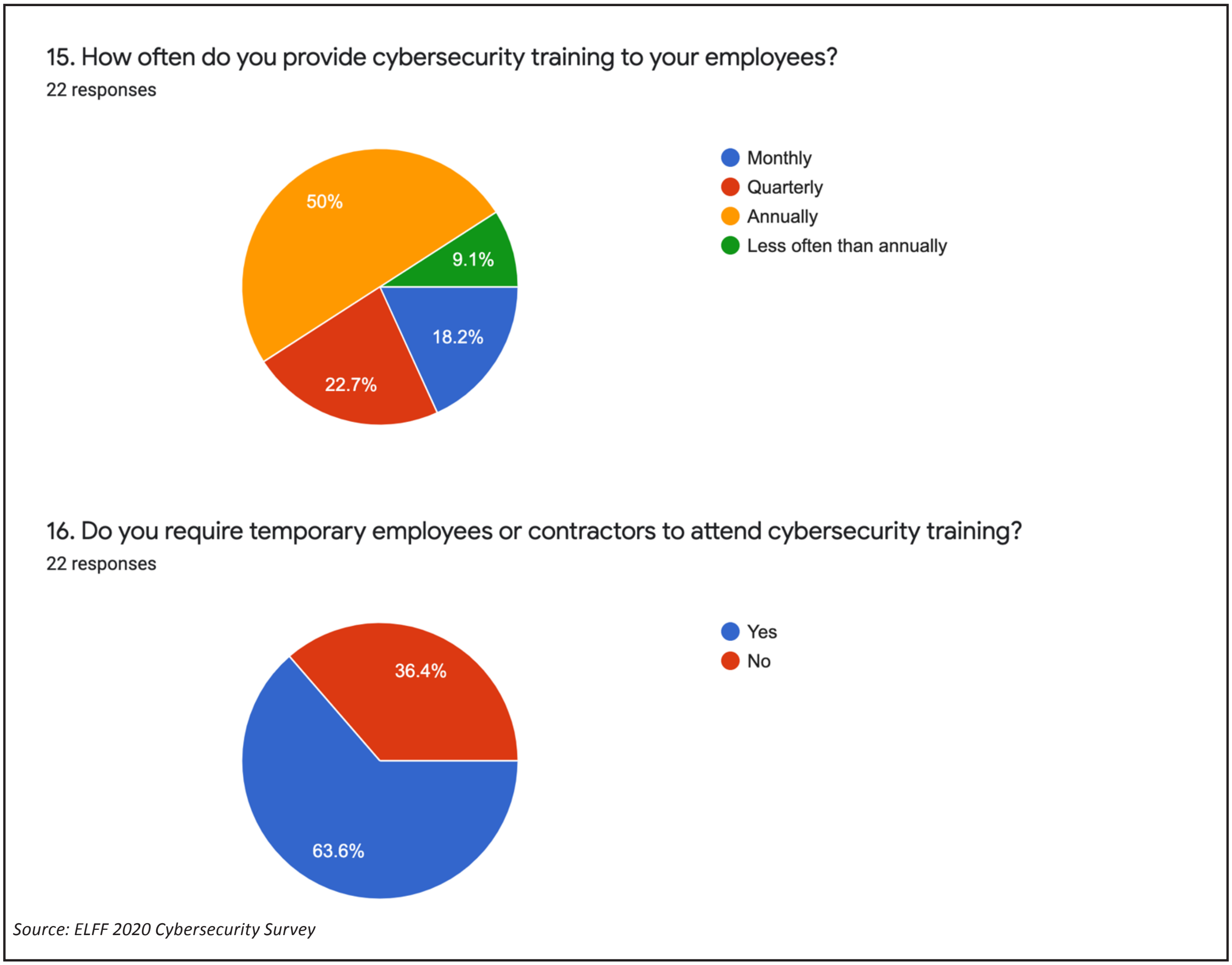


14. Do you provide cybersecurity training at least annually for your employees?

22 responses

Source: ELFF 2020 Cybersecurity Survey

One of the most effective forms of training is performing phishing training. This involves the organization sending out fake phishing messages using common techniques used by attackers to educate staff. Employees that click on a link included in the fake phishing test message are redirected to a training website that shows them how to detect similar phishing messages in the future. The company can get a report on the staff that failed the test and provide additional targeted training. There are many third-party companies providing these types of services, and it is included in the higher Microsoft M365 plans.



15. How often do you provide cybersecurity training to your employees?

22 responses

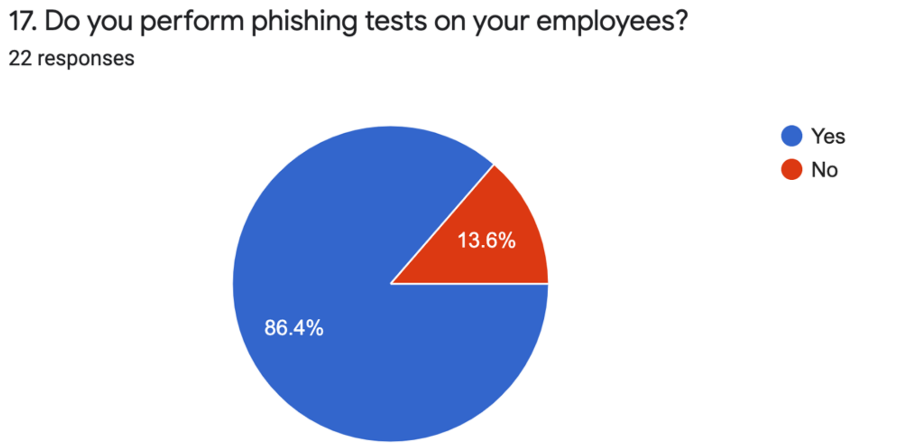
16. Do you require temporary employees or contractors to attend cybersecurity training?

22 responses

Source: ELFF 2020 Cybersecurity Survey

There is some controversy in using phishing testing for training staff. Employees can feel like the organization is targeting them specifically or setting them up to fail. This situation can be made worse if the organization uses disciplinary action for employees who fail the phishing tests. Phishing testing needs to be used as a training tool and not a form of punishment to be effective. The information security culture build will be much more difficult if employees are suspicious of the organization's motives. However, phishing testing is one of the best overall methods to reduce risk in one of the most common attack vectors. Most of the companies that answered the survey are using phishing testing in their cybersecurity training programs.

Additional training on other forms of social engineering attacks should be considered by companies in the equipment leasing and finance industry. There are numerous occasions where employees interact with customers over the phone or through email and discuss sensitive financial information. This creates more opportunity for a social engineer to convince an employee to release information or change a financial transaction's details. Employees need to be familiar with social engineering techniques like pretexting, where the attacker provides incorrect information, and the staff corrects them with information after gaining trust. Many third-party organizations can provide these training programs through in-person testing or online courses.

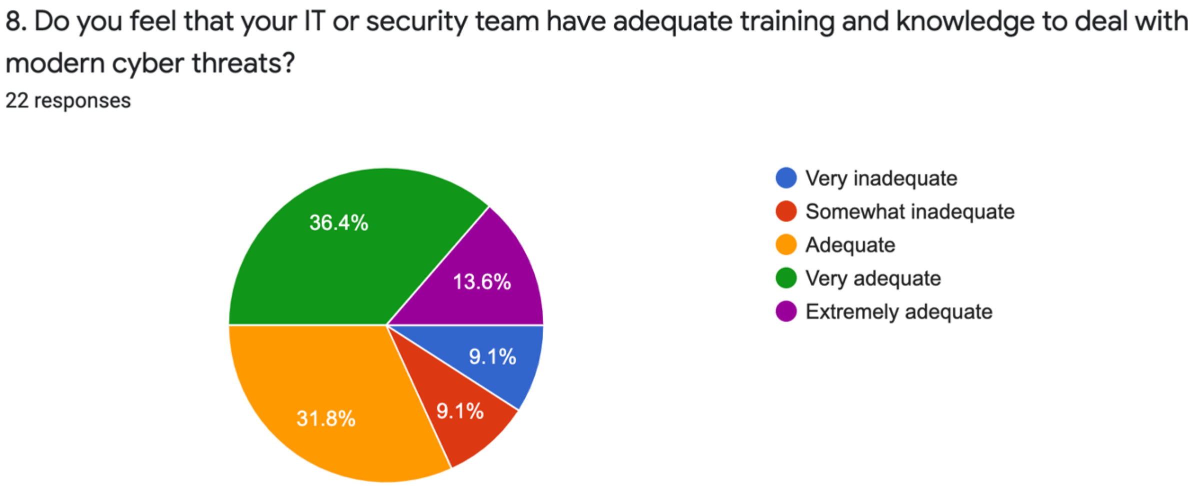


17. Do you perform phishing tests on your employees?
22 responses

Source: ELFF 2020 Cybersecurity Survey

The use of remote workers has exploded during the COVID-19 pandemic due to necessity. Many organizations quickly sent their staff home with a computer and a few instructions. This has created a new vulnerability in that these staff could be more vulnerable to specific cyberattacks. Remote staff should be trained on the physical security of their environments along with the technical risks and requirements. WIFI security, software updates, and antivirus all need to be addressed in remote worker training programs. Third-party training sources may not yet be available, so organizations will need to develop customized training for these employees.

Most organizations do not realize that their IT staff are not cybersecurity experts. IT staff are traditionally focused on providing system stability and customer service. They may not recognize that the decisions they make every day in the course of their duties can impact the security of the organization. This is why it is critical to provide security training to operational IT staff. They need to understand the potential threats to the organization and how to mitigate them. This type of training is primarily technical and can be expensive, but it is worth the investment. Third-party companies like SANS (sans.org) are great resources for training IT and IT security staff.

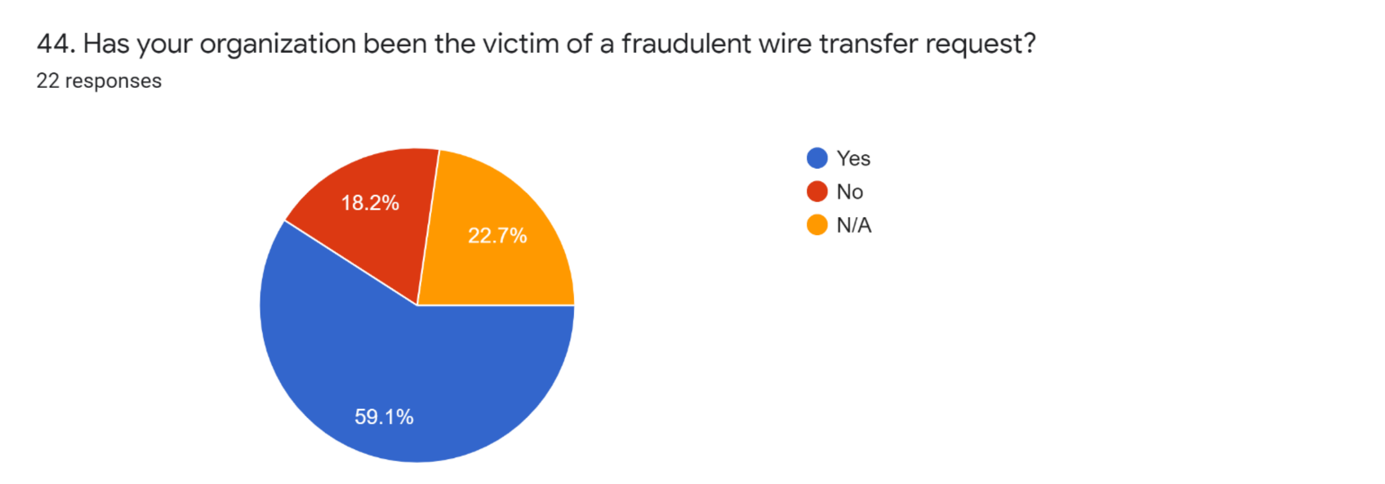


8. Do you feel that your IT or security team have adequate training and knowledge to deal with modern cyber threats?
22 responses

Source: ELFF 2020 Cybersecurity Survey

Processes (Administrative Controls)

Attackers have shifted their attacks to target specific processes within equipment leasing and finance organizations. These have included common procedures such as performing fraudulent ACH transfers, unauthorized direct deposit bank account transfers, unauthorized changes to vendor payment information in accounts payable, and fraudulent loan applications. Many organizations use email communications to authorize changes for financial transactions. The attackers will either spoof or use a compromised email account to help legitimize their fraudulent requests. Attackers may even spoof an entire company, including their email addresses, phone numbers, and websites. Our survey results show that almost 60% of the organizations polled have experienced this type of fraud.



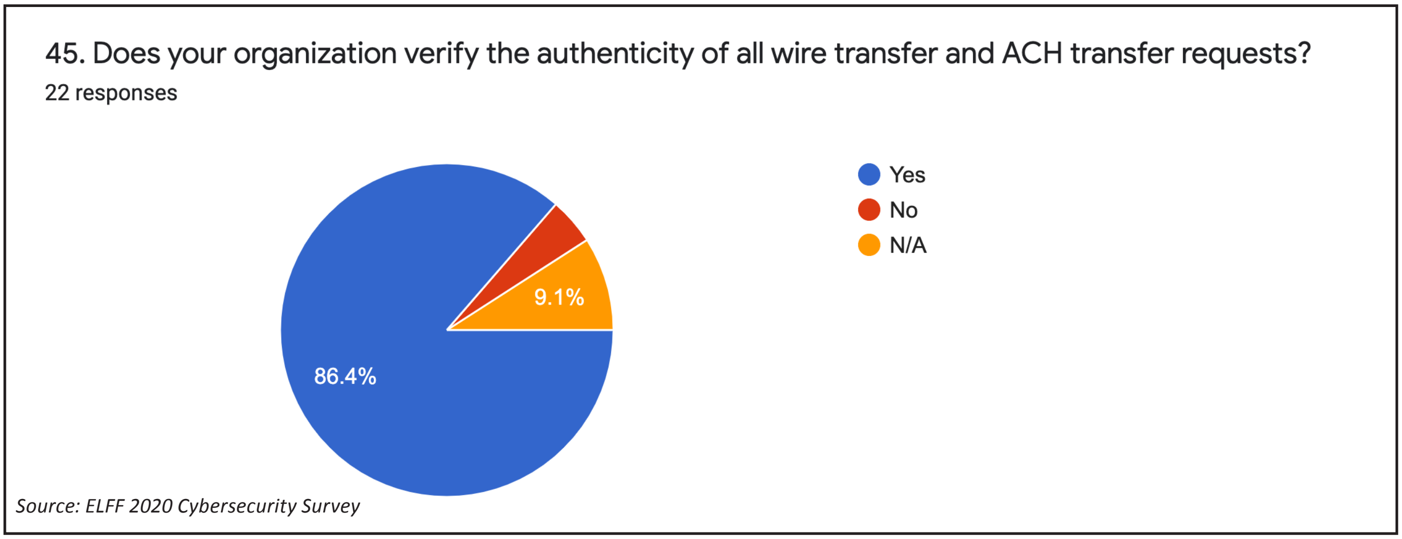
44. Has your organization been the victim of a fraudulent wire transfer request?

22 responses

Source: ELFF 2020 Cybersecurity Survey

Business processes must be hardened to include approval processes that require non-electronic verification. Direct deposit change requests should be verified with the employee with a phone number already on file. Any requested change to vendor payment information must be verified by contacting the vendor directly using their direct phone number and not one provided in an email. Manual approval for wire transfers or ACH same-day transactions can help prevent these types of fraud. Some organizations have moved to using virtual card payments for vendors with prespecified amounts. This involves using separate virtual credit card numbers for each vendor to prevent loss if a single vendor is compromised and the card number stolen.

There are many more processes that may need manual review to find weaknesses that could lead to financial fraud. Organizations in the Equipment Leasing & Finance sector are especially vulnerable given the number of transactions that occur through various departments. A risk assessment that includes all processes where financial transactions are conducted will help identify the weak areas that need to be reinforced. Manual approval processes may slow the efficiency of automated transactions, but the cost of fraud will outweigh these efficiency gains. The majority of the organizations included in the survey have addressed these risks in wire and ACH transfers.

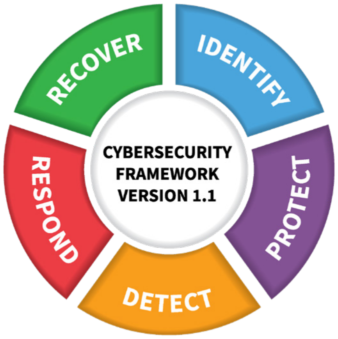


Source: ELFF 2020 Cybersecurity Survey

Processes should also be used to reduce the technology risks of the organization. These can vary widely based on the business's size and its technology infrastructure. The overall goals are the same, but the path to reducing risk will be different. Larger organizations have more exposure due to larger numbers of employees and systems but offsetting these risks with larger investments in technology and people. Smaller organizations have reduced risk due to their size. However, they may not even be aware of their level of security risk and may not have the financial resources to remediate that risk.

Midsize and larger organizations can benefit by implementing a formal risk-based information security program. An executive-level leader should be brought in to oversee the information security program and provide visibility into outstanding risks for the business. There are several frameworks available to help shape that program and define the controls that need to be put in place. The National Institute of Standards and Technologies (NIST) developed a Cybersecurity Framework (CSF) after an executive order in 2013 to protect U.S. critical infrastructure. This framework is available for free and provides the guard rails to create a formal risk-based information security framework.

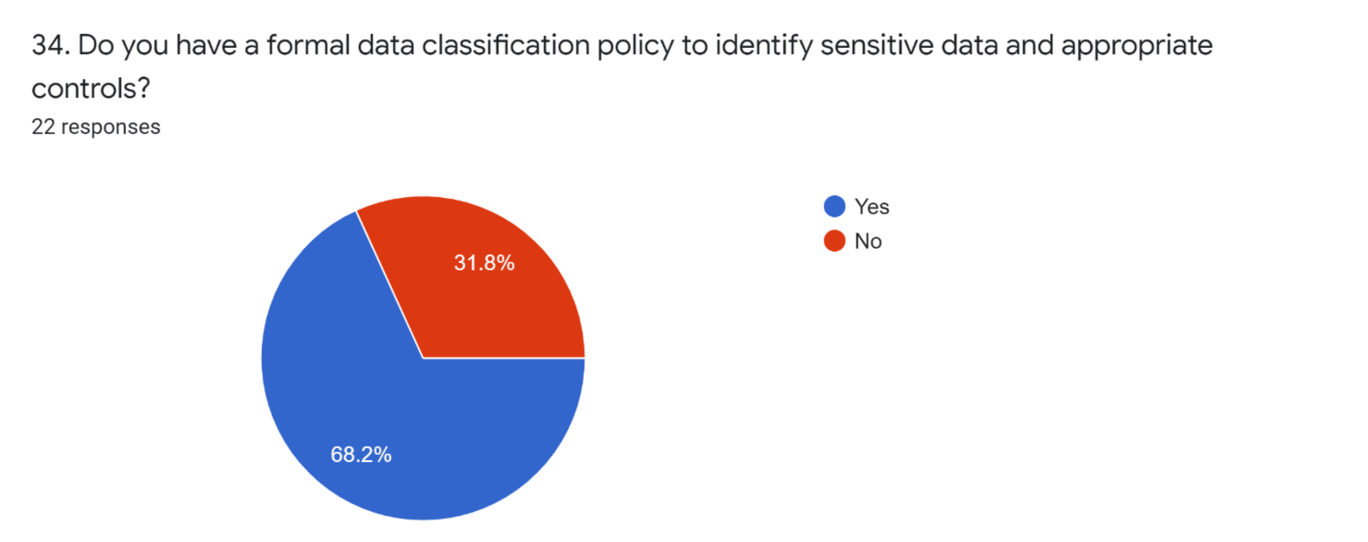
The NIST CSF has an advantage over other information security frameworks in that it is easy to understand and explain to people outside of IT or information security. The five functions that make up the NIST CSF are named after the actions that need to be taken: Identify, Protect, Detect, Respond and Recover. The framework structure can be quickly summarized and presented to executives and the board of directors with minimal explanation. The specific details, including the development of procedures and technical controls, follow each function. The NIST CSF requirements can be easily converted into KPIs for reporting progress and fostering transparency in organizational risk.



The NIST Cyber Security Framework can be scaled down depending on the organization's size. However, it may not be practical for small companies where the number of policies and procedures would outnumber the employees. There are still processes that can be implemented that address the higher risk areas and improve overall organizational security. Many of these processes are addressed within the NIST CSF and would allow the company to grow into the formal framework when appropriate. The following recommendations are included as areas that smaller companies may want to address specifically. This is not an all-inclusive list as each company's risk profile is unique due to its business and technology architecture.

An accurate and updated inventory of all equipment, software, and data is mandatory in any security program. Asset management is one of the first steps in the NIST CSF "identify" function. This inventory should include hardware information like the model number, serial number, location, physical security controls, technical security controls, and primary use case. It is crucial to record all the hardware, including network infrastructure, multifunction printers, and wireless access points in the hardware inventory. The software inventory should look similar but include purchase date, support agreement status, and information on getting security updates for each product. The most important step is to then identify the data stored on each system and classify it by sensitivity. Marketing information will not have the same sensitivity as personnel records.

The combination of these elements can provide insight into making better security decisions. The use of a laptop in a remote location should be assessed based on the provided controls and the type of information being accessed, for example. Information that is deemed confidential or too sensitive to be on a mobile device, laptop, or PC can be restricted to prevent potential data breaches. Loan application information from customers or detailed credit card transactions are examples of data that should not be stored on mobile devices. This same information should not be stored in an application that lacks security controls such as auditing and encryption. Loan application information would never be safe in a "notepad" but could be used on a Windows desktop computer running Excel with file-based encryption or information rights management controls.



34. Do you have a formal data classification policy to identify sensitive data and appropriate controls?

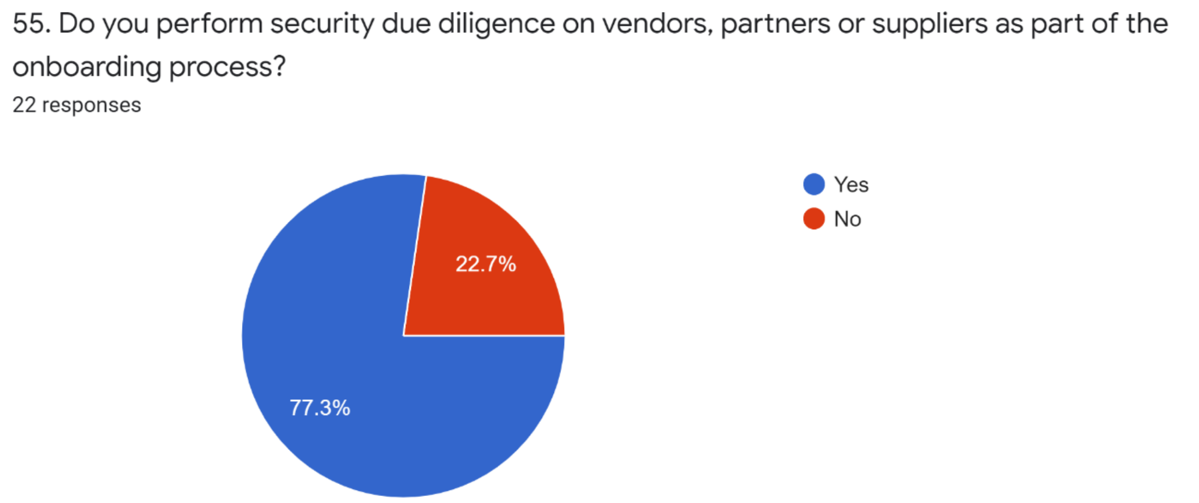
22 responses

Source: ELFF 2020 Cybersecurity Survey

Data retention policies are also an important piece of the overall information security strategy. Storage is inexpensive, and many cloud services offer essentially unlimited email and file storage plans. It may not be beneficial to save every piece of information forever about the organization. This is especially true in business email compromises where attackers take over a cloud-based email account. A single spreadsheet stored in an email inbox used by companies in Equipment Leasing and Finance could contain thousands of records requiring data breach notification in multiple states and countries.

The impact of a data breach can be reduced significantly by setting the data retention policy for email down to just a year. There are optional archival systems that would allow employees to go back further if necessary but not provide it directly in the inbox. This helps the organization meet compliance obligations while limiting the amount of data available in the case of a breach. The business requirements for data retention will vary between applications, but this can be documented in the preceding data inventory phase.

Organizations often look inward when assessing their organization's security risk when third parties are the ones who introduce new risks through M&A activity, outsourcing services, joint ventures, and cloud-based applications. A security risk assessment should be conducted on all third parties before the acquisition and annually thereafter. Many cloud-based providers offer independent audits of their services that can be reviewed online. These types of assessments are provided for free and can be accessed by anyone to validate the security controls of the cloud service. Microsoft, Google, Amazon, and Salesforce all offer full compliance centers where these reports can be reviewed, for example.



55. Do you perform security due diligence on vendors, partners or suppliers as part of the onboarding process?

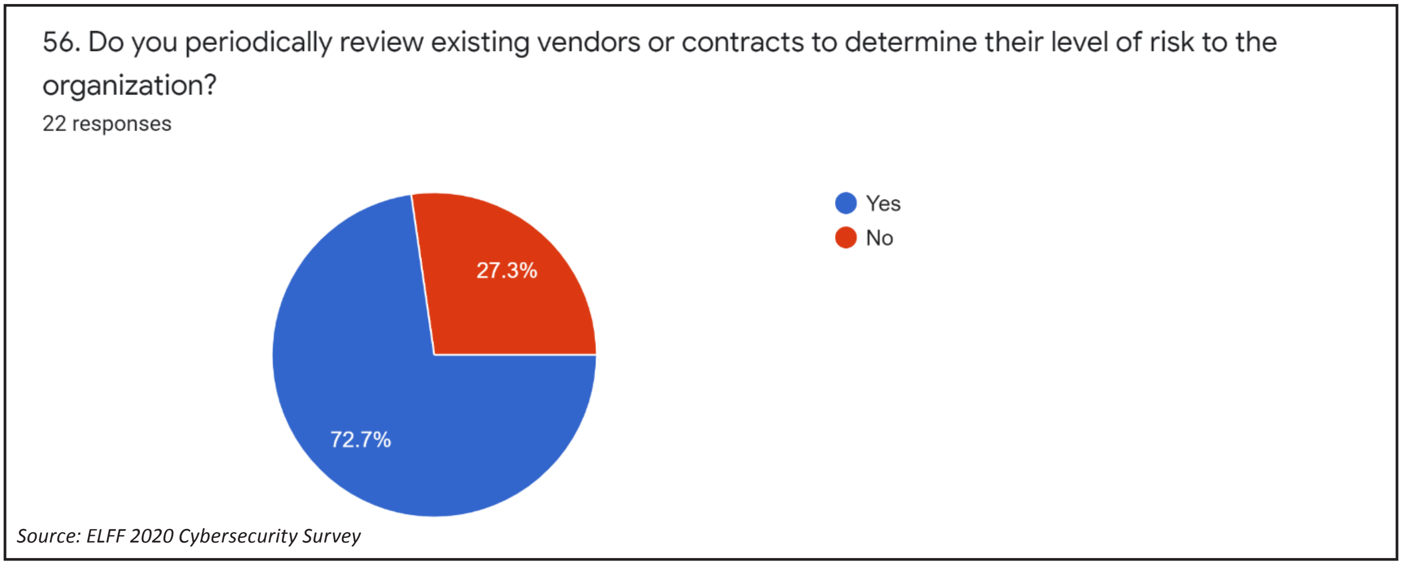
22 responses

Source: ELFF 2020 Cybersecurity Survey

The most prevalent independent report on a service provider is the SOC 2, overseen by the AICPA. These reports are conducted by CPA firms that are authorized by the AICPA as they started as audits against service organizations that could affect the financials of an organization. They have grown to encompass many different information security controls as the SOC 2 has matured over time. They can apply to all types of service organizations and not just technology-based platforms. The SOC 2 Type 1 audits the controls presented by the organization but does not test them for effectiveness. The SOC 2 Type 2 is more desirable from an auditing perspective because it tests the effectiveness of security controls over a more extended period of time.

The SOC 2 Type 2 is easy to read and will contain a listing of the controls that were tested towards the back of the report. There may be exceptions that were noted by the auditor that should be reviewed. The company being audited will respond with details on their remediation efforts in the section afterward. The fact that exceptions were found while reviewing the SOC 2 report should not be a deal-breaker. A good auditor should find exceptions that need to be addressed by the organization. How the company responds to the exceptions is more important than the exceptions themselves.

Security risk assessments for other types of business activities such as joint ventures, mergers, and acquisitions are more labor-intensive. These will require internal security or external consulting resources to perform the necessary due-diligence assessments. There are no standard reports that can be used in these audits. Examples of documents that should be reviewed during the audit include penetration testing results, vulnerability scanning results, security incident reports, and security policies. There are third-party services that will scan externally available information to build a risk profile on a target company, but those may not be very reliable.



56. Do you periodically review existing vendors or contracts to determine their level of risk to the organization?

22 responses

Source: ELFF 2020 Cybersecurity Survey

Security risk assessments should also be used whenever the organization acquires a new application. The results of these assessments can then be added to the inventory of hardware, software, and data. The organization should use a standard questionnaire to classify the type of data that will be stored by the application and the security controls provided by the vendor. Most of the questions will be focused on areas where the vendor is stepping away from security best practices. Examples of questions for a new application risk assessment include but are not limited to:

1. What type of data will be stored on this system?
2. Can the application run without local administrator permissions?
3. Are there any antivirus restrictions that need to be put in place to allow the application to run?
4. Can security patches for Microsoft Windows be applied normally, or will they affect the application?
5. Can the built-in Windows firewall be used while running the application?
6. Does the application encrypt data between the workstation and server?
7. Does the application encrypt data stored on the server?
8. Does the application provide for individual user accounts for auditing?

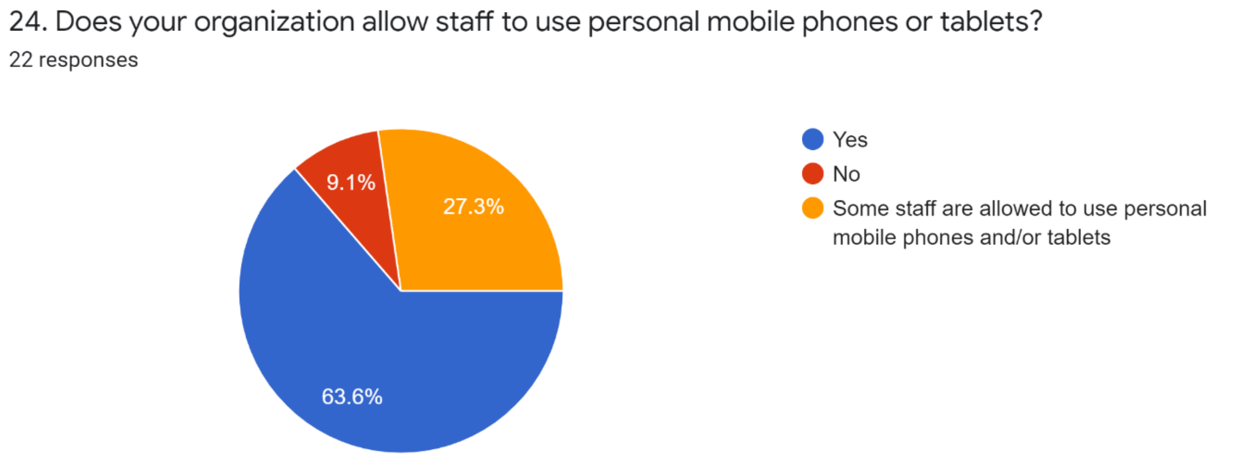
9. Does the application utilize strong authentication like complex passwords or multi-factor authentication?
10. Does the application audit access confidential information for later review?
11. Are there any non-standard permissions that must be granted for the application to run?
12. How does the company test its software for security vulnerabilities?
13. How does the company provide remote support?

Many vendors will have exceptions with even this limited list of questions. The organization can use the results of this assessment to choose another vendor or implement additional security controls to compensate for any identified security deficits. A Windows-based system that cannot receive timely security patches poses a threat to the organization and should be considered a high priority risk. The organization can choose to isolate this system from the rest of the network or even restrict internet access to reduce the overall risk to an acceptable level, for example. There are almost always options to help mitigate risk, but they may take time to identify and implement.

Another common but neglected area of security risk is the lack of processes around the use of personal devices. This is commonly referred to as "Bring Your Own Device" or BYOD. The use of BYOD has exploded with the rapid consumer adoption of smartphones. Some companies have taken BYOD further and provide stipends for the employee to purchase their own equipment. The lack of security policies and procedures around the use of personal equipment can quickly change BYOD to mean "Bring Your Own Data breach."

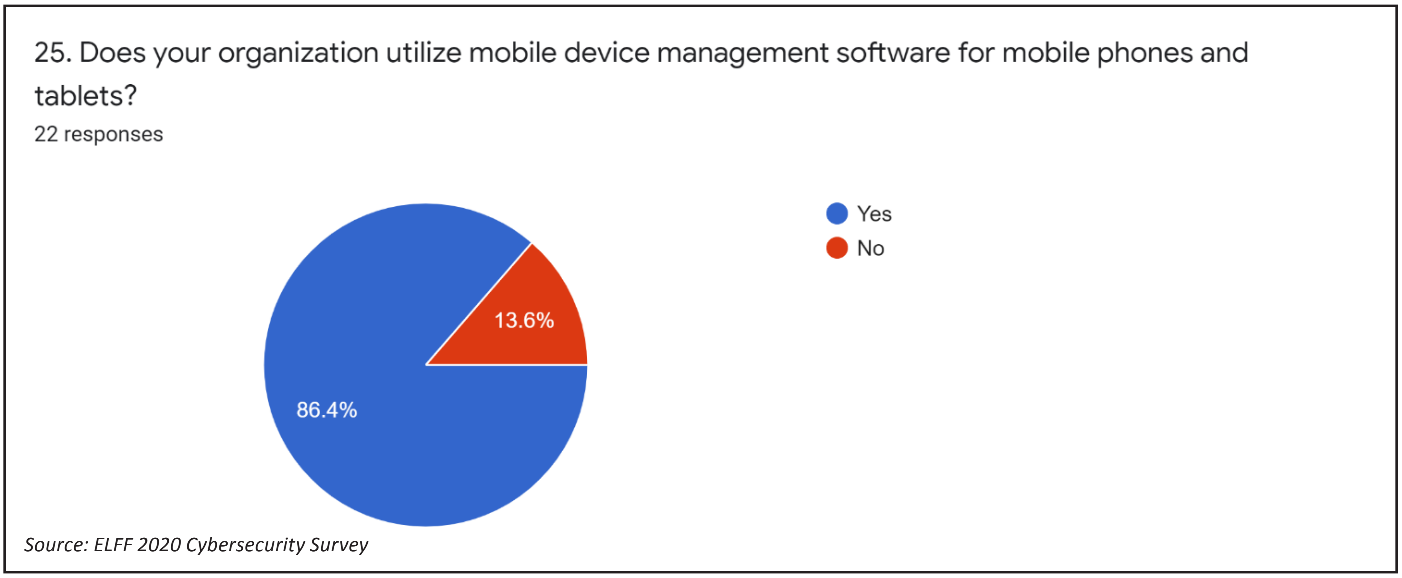
Personal devices may not have appropriate security controls, including encryption, timeouts, password strength, or even security updates. Employees may inadvertently install applications that compromise the security of their devices. Organizations need to define the usage of the devices and enforce technical controls that configure appropriate security controls. Devices that do not meet the requirements should be restricted from accessing confidential data. Organizations with lower risk tolerance may want to simply limit the use of any personal devices. Corporate-owned devices are cheap compared to the costs of a potential data breach.

The majority (63.6%) of the organizations that completed the survey are allowing the use of personal mobile devices. However, most (86.4%) of those organizations are protecting those personal devices using mobile device management policies with technical enforcement. The remaining organizations are exposed to the risks identified above.


24. Does your organization allow staff to use personal mobile phones or tablets?

22 responses

Source: ELFF 2020 Cybersecurity Survey



25. Does your organization utilize mobile device management software for mobile phones and tablets?

22 responses

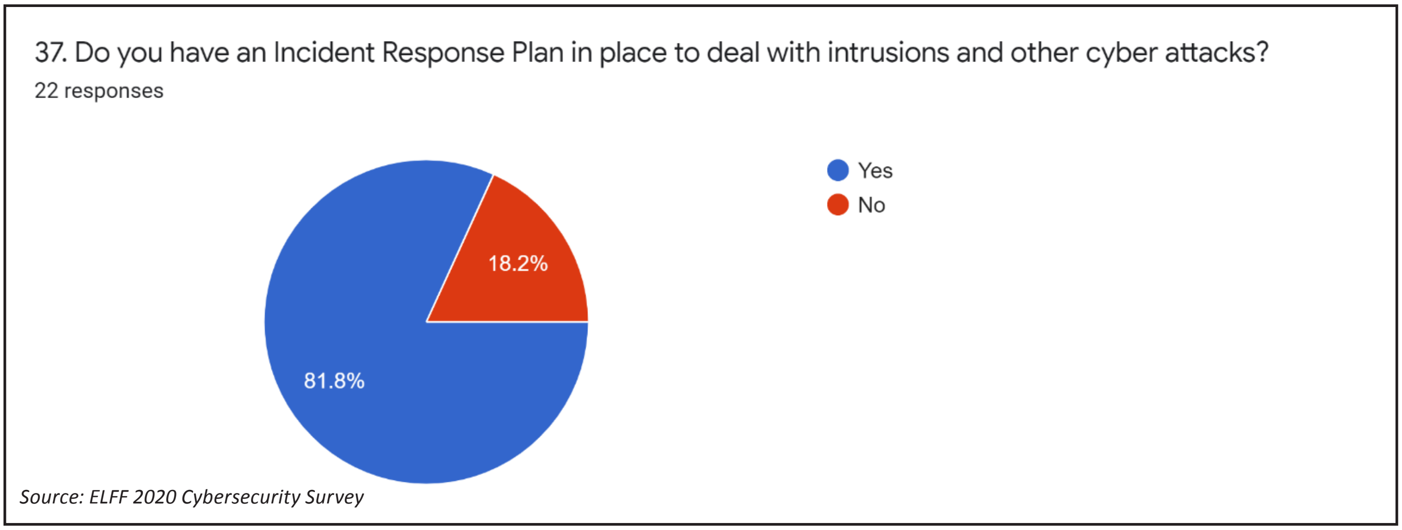
Source: ELFF 2020 Cybersecurity Survey

Many new cyber-attacks are being developed every day targeting the equipment leasing and finance sector. Organizations must stay updated on these new attacks through threat intelligence. Many commercial offerings have been introduced in the last few years that could provide this type of insight. One of the best sources for threat intelligence often comes through Information Sharing and Analysis Centers or ISACs. These are industry-specific associations that share threat intelligence among the members. The Financial Services ISAC provides detailed information on threats to financial organizations depending on the membership level.

The information gained from an ISAC can be invaluable to understanding the threats faced by similar organizations. They will provide information on malware that has been seen by member organizations along with information for remediation, for example. ISACs may find stolen company credentials in password dumps for sale on the dark web and notify member organizations that could be affected. They will also issue alerts coordinated with law enforcement when the member organizations are specifically targeted. Threat intelligence provided by ISACs will provide insight that could prevent a cyber-attack.

The best defenses can still fail as cyber-attacks have become more frequent and sophisticated. The response to these incursions can make the difference between a simple incident and a successful ransomware attack. A security incident is not unlike any other disaster where anxiety and chaos quickly take over decision-making. Organizations need to have a predefined Incident Response Plan to provide a calm, organized response. The incident response team structure, including leadership, technical, financial, legal, and communications roles, should be clearly defined. Incident response plans should include detailed communications plans that define customer and press notification processes.

Many organizations include legal representation in their incident response team to protect internal communications about the incident through attorney-client privilege. Some organizations have decided to provide transparent updates through various media sources as the incident progresses. It may be necessary to contract with other technical or forensic specialists if the organization lacks these skillsets internally. These decisions must be made before an incident occurs to provide the best defense possible to reduce both the organization’s financial and technical damage.

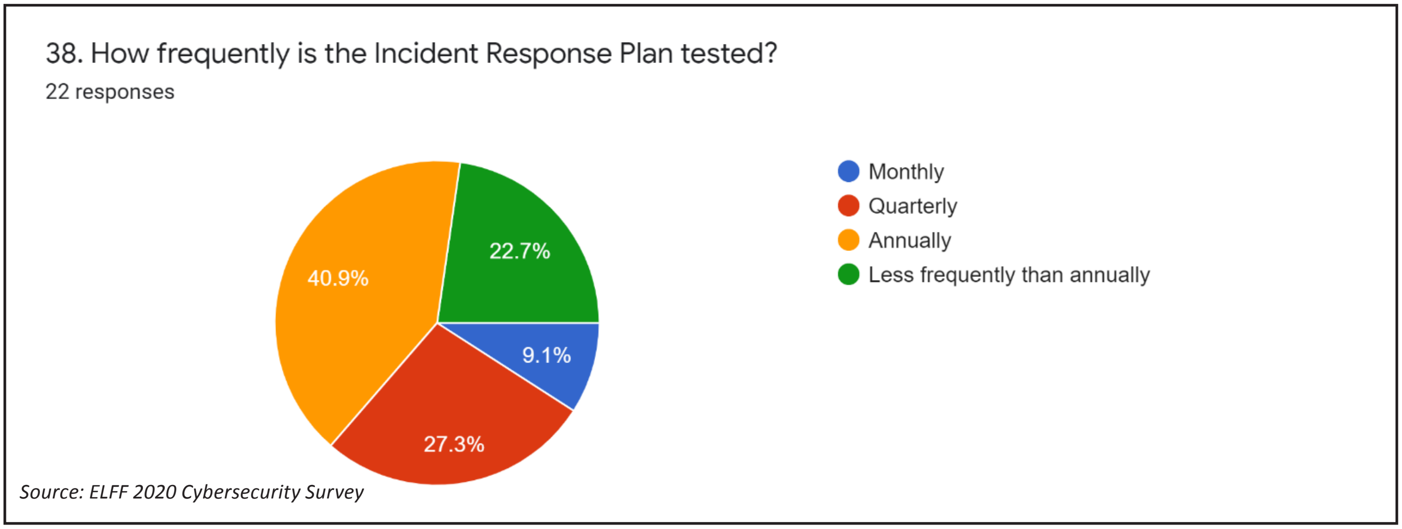


37. Do you have an Incident Response Plan in place to deal with intrusions and other cyber attacks?

22 responses

Source: ELFF 2020 Cybersecurity Survey

An incident response plan that has not been exercised will not be effective in the event of a cyber-attack. Therefore, organizations must test their incident response plans at least annually to reinforce familiarity with the plan and identify any weaknesses that should be addressed. These tests can be conducted as tabletop drills to increase the frequency of the tests and limit the time required for planning and participation. The individuals assigned critical roles in the plan need to know how to execute their responsibilities efficiently. External resources included in the plan need to be tested to understand their response times in the event of an actual cyber-attack.



38. How frequently is the Incident Response Plan tested?

22 responses

Source: ELFF 2020 Cybersecurity Survey

A critical piece of any incident response plan should be cyber liability insurance. Many insurance plans will provide the resources necessary for legal representation and forensic investigations. They can provide bulk mailing services and call centers to breach notify affected customers. They can also provide data mining services to identify the information involved in the breach. Some of the plans will even assist in working with ransomware actors to negotiate lower ransoms and convert to a specified cryptocurrency. Cyber liability insurance may also cover any regulatory fines issued as the result of a data breach.

The limits and deductibles for these plans vary greatly and can drive the overall cost. Most plans will have deductibles for each service required along with separate limits. It is important to match the insurance coverage with any gaps in resources available internally. Cyber liability insurance applications have begun requiring that the organization have security controls in place before granting coverage. A security incident involving a lost laptop that was not encrypted would be exempt from coverage under the majority of plans, for example. The use of cyber liability insurance is not a replacement for a formal information security program.

Technology

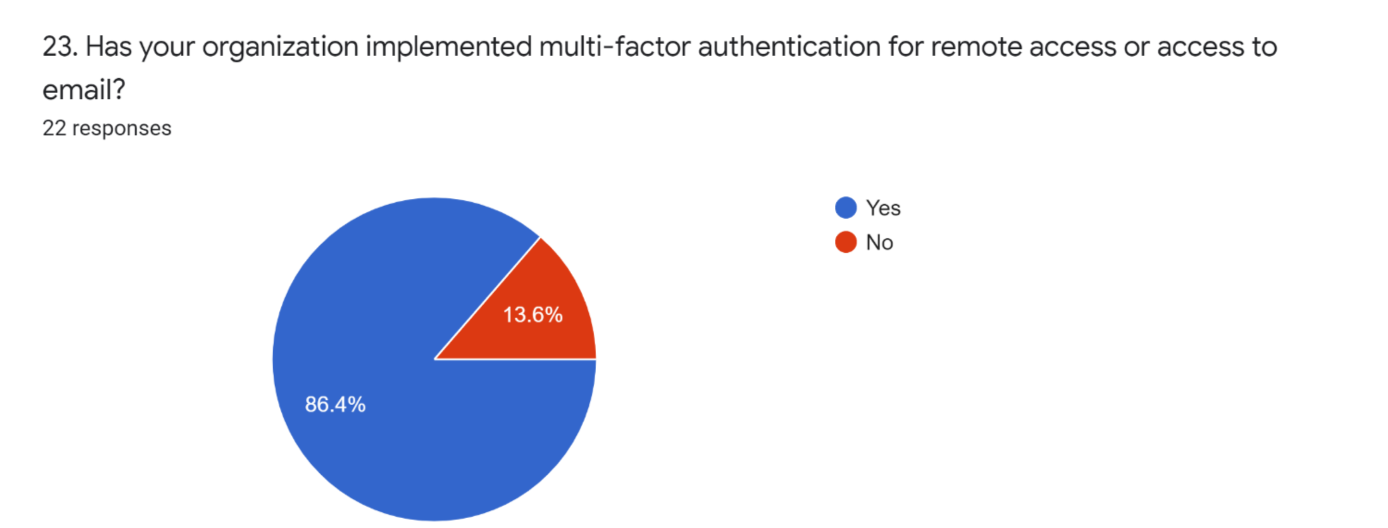
Business email compromise has become one of the most common cyberattacks. The attacker just needs to compromise one employee's credentials, and the results can be catastrophic. These credentials could be acquired through phishing, other data breaches, or through the use of simple passwords. Attackers can then go after additional credentials for financial fraud, target customers or employees with further phishing attacks, or begin a ransomware attack. A business email compromise is a very profitable endeavor with lots of options for revenue generation. It is also very preventable.

Multifactor Authentication (MFA) has existed for a long time. The concept is that the user has something they know and something they possess or something they are (biometrics) to gain access to a system. An attacker that gains access to the username and password will be missing the other portion of the authentication. Modern forms of MFA include sending an SMS text message to a predefined phone number to authenticator apps that generate one-time verification codes.

Microsoft and Google both provide MFA capabilities and authenticator apps for smartphones for no extra cost. There can be resistance from employees when MFA is rolled out, as it does complicate the authentication process. However, MFA must be viewed as a standard requirement in 2021 and not just an option for organizations looking for the highest levels of security. It is essential to communicate the risk of account compromise to employees to garner support. However, the implementation of MFA may be the most cost-effective way to reduce the organization's security risk.

MFA must be implemented on all remote access points to the organization. Microsoft Office 365 and Google Workplace have built-in capabilities for MFA, so it is easy to implement with these services. VPN access to the network needs to be protected with MFA as well. Any access to virtual desktops through VDI, RDS, or Citrix-based technologies must include MFA. Third-party websites used by the organization for financial services also need to be MFA enabled. Attackers will continue to test each access point and naturally gravitate to the weakest link in an organization's defensive security. The application inventory identified early on in this section can be used to identify everywhere MFA should be applied.

One of the other reasons for the rise in business email compromise is the rapid adoption of Microsoft 365. This system's popularity has enabled attackers to target one location that could compromise millions of corporate networks. This economy of scale provides a high return on investment for the attackers. Microsoft Exchange was the previous favorite of attackers but has fallen out of favor due to the customization from each locally installed server. Microsoft 365 offers far more information than Microsoft Exchange as it incorporates new data storage services like SharePoint and OneDrive. The system is also very complex to configure securely, leaving customers unaware of the risks to their information.



23. Has your organization implemented multi-factor authentication for remote access or access to email?

22 responses

Source: ELFF 2020 Cybersecurity Survey

Organizations need to review hardening advice for Microsoft 365 or find a consultant with the knowledge to perform the necessary hardening tasks. Microsoft is continually adding features to the product, so it can be challenging to maintain a secure environment without assistance. There are many online guides for securely configuring Microsoft 365, including one from **Microsoft** directly. The Center for internet Security provides excellent **recommendations for hardening Microsoft 365** as well as other services. Examples of basic M365 hardening recommendations include:

1. Enforce MFA for all user accounts
2. Restrict basic authentication (unencrypted)
3. Restrict legacy authentication forms such as IMAP, POP3, and ActiveSync
4. Limit Global Administrators and using administrative role-based access
5. Reduce the authentication timeout from 90 days to a week or less
6. Limit public sharing from SharePoint and OneDrive
7. Restrict users from allowing external applications direct access to M365
8. Prevent automatic forward of all email from accounts
9. Limit PowerShell access to M365 to administrative users only

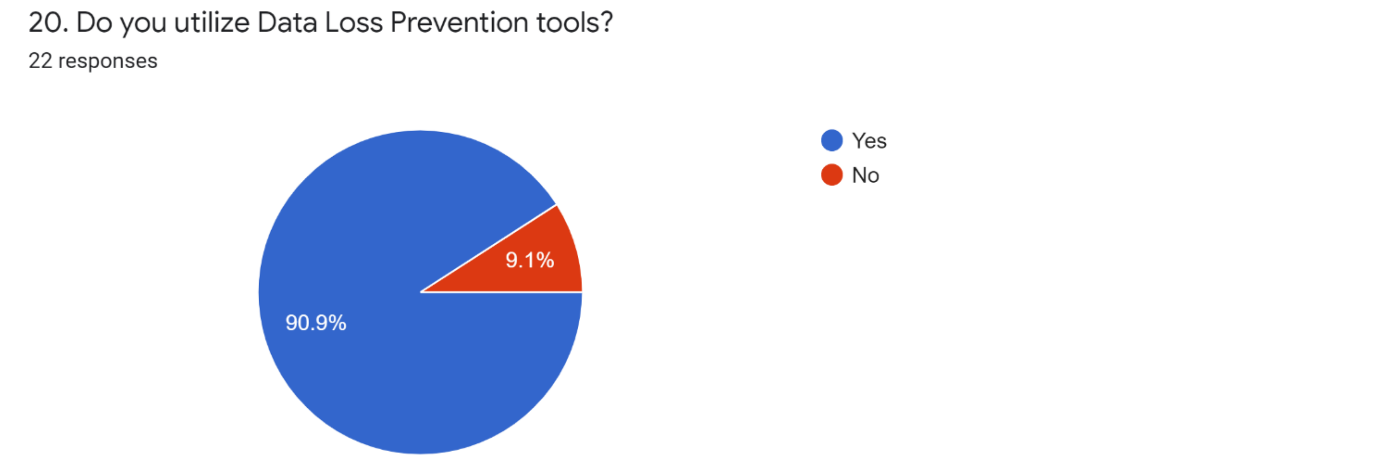
Microsoft 365 licensing is difficult to understand for even the most experienced IT professional. Unfortunately, the least expensive licensing options provide little in the way of security controls to protect the cloud environment. This fact may not be apparent when first purchasing a basic subscription. Audit logs are retained for 30 days or less. Login attempts from foreign countries cannot be blocked. Multiple sign-ins for the same user from two different locations are allowed without alerts by default.

Microsoft does provide additional features beyond simple hardening that can turn Microsoft 365 from a liability to a one-stop security solution with the more expensive subscriptions. Conditional Access is one of the key security tools in the upgraded plans that can provide role-based access to the company M365 tenant. It can block access from international locations or from systems that the company does not manage.

It can force multifactor authentication or even a password change if a user attempts to log in from multiple geographic locations at the same time. M365 will generate alerts based on these events and provide a centralized audit log. These features and more are available in the E3-E5 subscription levels and should be reviewed by anyone using Microsoft 365.

Data Loss Prevention (DLP) is one of the features available in the higher-end subscriptions of Microsoft 365 that some organizations may already have in place. DLP is software or a service that combs through all the unstructured data in a company like Word documents, Excel spreadsheets, and email attachments and identifies potentially confidential information. Organizations can assign rules to protect this information using encryption, restrict printing, restrict download, and restrict email forwarding. DLP has been available for years from other providers, but implementations were often unsuccessful due to the decentralized storage of these documents.

The aggregation of all this unstructured data in the Microsoft 365 cloud eliminates the need to search through many potential locations where data could be stored. The data that used to be stored in shared directories on servers scattered throughout the organization is stored within SharePoint and OneDrive in the Microsoft cloud, for example. This simplifies the implementation of DLP even though the DLP capabilities included in Microsoft 365 may not compare to other commercial solutions. The Microsoft 365 DLP solution continues to mature and offers capabilities that may have been out of reach of smaller organizations in the past.



20. Do you utilize Data Loss Prevention tools?

22 responses

Source: ELFF 2020 Cybersecurity Survey

Microsoft offers email security tools in Microsoft 365 as well. However, many other third-party solutions can be used with Microsoft 365 or any other email system. The features of these third-party systems go way beyond the simple spam filters of the past. These systems utilize machine learning and crowdsourced threat intelligence to protect an email system. Other features that organizations should look at in an email security solution include VIP spoofing protection, URL link protection, and attachment detonation.

Spoofing protection will analyze emails that appear to have been sent from the CEO and block suspect messages, for example. This has become a common attack technique as employees will respond to the CEO's request. URL Links within the emails that could lead an employee to a malicious site should be replaced by email security systems and analyzed before allowing the user to visit the website. URL Link protection is not perfect as attackers try multiple techniques to bypass reputation filters. However, these filters are updated frequently, and the email security system would alert the information security team if an employee accessed a link that has since been deemed malicious. File attachments should be analyzed for potential malware and tested by the email security systems in a sandbox for malicious activity.

There are simple email security improvements that organizations can make to reduce their email security risk. The most important is blocking common malicious attachment filetypes that attackers use. Many businesses have difficulty implementing the file attachment blocks due to potential legitimate business use. However, some filetypes are only used for executing code locally on a Windows workstation. These filetypes are seldom used by the business and can safely be blocked without any communication interruption.

These filetypes include:

.386, .ace, .acm, .acv, .ade, .adp, .adt, .ani, .app, .arc, .arj, .asd, .asp, .avb, .ax, .bas, .bat, .boo, .btm, .cab, .cbt, .cdr, .cer, .chm, .cla, .cmd, .cnv, .com, .cpl, .crt, .csc, .csh, .css, .dll, .drv, .dvb, .email, .exe, .fon, .fxp, .gms, .gvb, .hlp, .ht, .hta, .htlp, .htt, .inf, .ini, .ins, .iso, .isp, .its, .jar, .job, .js, .jse, .ksh, .lib, .lnk, .maf, .mam, .maq, .mar, .mat, .mau, .mav, .maw, .mch, .mda, .mde, .mdt, .mdw, .mdz, .mht, .mhtm, .mhtml, .mpd, .mpt, .msc, .msi, .mso, .msp, .mst, .nws, .obd, .obj, .obt, .obz, .ocx, .ops, .ovl, .ovr, .pcd, .pci, .perl, .pgm, .pif, .pl, .pot, .prf, .prg, .ps1, .pub, .pwz, .qpw, .reg, .sbf, .scf, .scr, .sct, .sfx, .sfx, .sh, .shb, .shs, .shtml, .shw, .smm, .svg, .sys, .td0, .tlb, .tmp, .torrent, .tsk, .tsp, .tt6, .url, .vb, .vbe, .vbs, .vbx, .vom, .vsmacro, .vss, .vst, .vsw, .vwp, .vxd, .vxe, .wbk, .wbt, .wlz, .wk, .wml, .wms, .wpc, .wpd, .ws, .wsc, .wsf, .wsh

Other filetypes should be considered for blocking but could be impactful to the business. These include the legacy Microsoft Office filetypes of .DOC, .XLS, and .PPT which were superseded by .DOCX, .XLSX, and .PPTX in Office 2007. These old filetypes are favorites for ransomware threat actors as they can easily hide malicious macro code in these binary formats. Security tools cannot completely parse the binary format leaving organizations vulnerable to attack. The newer Office filetypes are XML based, allowing for much more scrutiny from security tools. These old filetypes have been depreciated for fourteen years, and most people can save their files in the newer formats.

The use of cloud-based services has become ubiquitous for consumers and enterprises. The growth of Microsoft 365 is an example of how organizations are flocking to the cloud for what used to be internal IT solutions. However, it has also allowed for the creation of shadow IT services where employees use unapproved cloud solutions for company work. Many consumer-focused cloud services are not compatible with corporate privacy or regulatory requirements. The employee may not utilize strong authentication and cause a data breach that puts the organization unknowingly at risk. Free accounts on Dropbox or consumer versions of Google services are examples of shadow IT that employees commonly use without management approval.

Organizations must be aware of these shadow IT services and create controls to manage the potential risk. A Cloud Access Security Broker (CASB) is a security solution that can discover and manage access to cloud-based services. They can utilize network traffic logs from a firewall and locally installed agents on corporate systems to identify usage of cloud-based services. They will also allow the organization to define policies for using these applications, including forcing authentication using company credentials.

There are several different CASB solutions on the market, but organizations that are already using Microsoft 365 may opt to use their solution. Microsoft provides the Cloud App Security portal with the higher-end licenses of Microsoft 365. It is not yet the market leader, but it could already be included in the company's Microsoft 365 subscription. It offers integration with other Microsoft 365 security controls such as Conditional Access and Data Loss Prevention. The cloud application reporting and associated dashboard will help organizations locate and secure any unauthorized shadow IT activity.

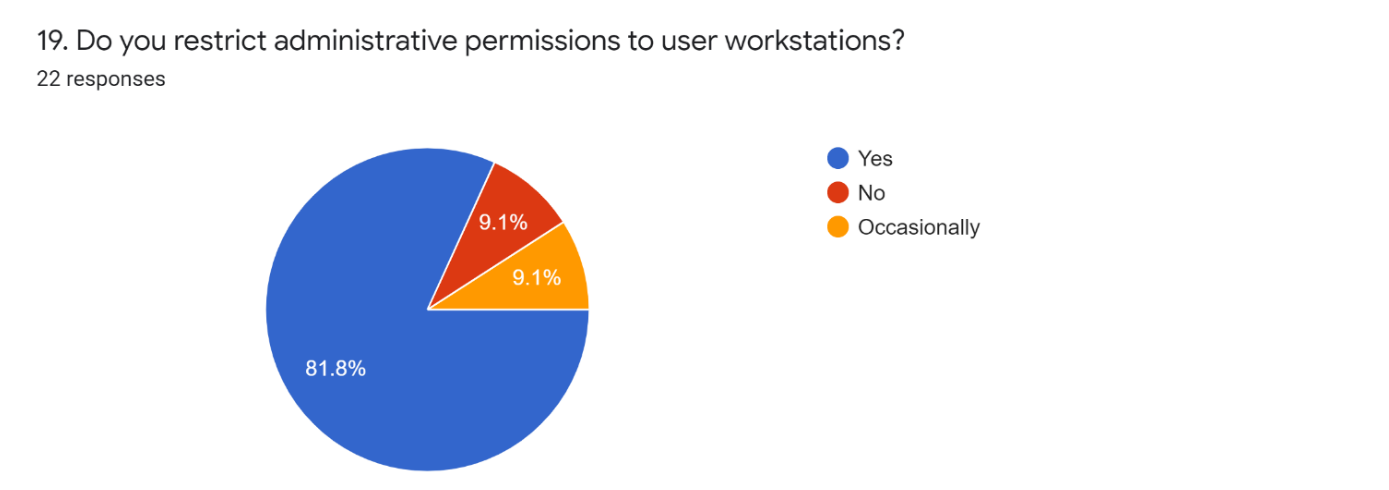
The risks of consumer cloud-based consumer storage services go beyond just the potential of leaking proprietary company information. Attackers utilize these services as well through phishing attacks to distribute malware. An employee would receive an email with a link from a free Dropbox account, for example. The email itself and the link are not malicious and will not get flagged by an email security filter. The employee clicks on the Dropbox link and executes the malware letting the attacker into the company network.

Organizations that cannot implement a CASB due to cost or complexity should consider blocking these consumer-based file-sharing services at the firewall. This can be difficult as all legitimate cloud-based file services need to be inventoried and whitelisted before implementing a block. The organization should also choose an officially supported business-class solution for employees to use as an alternative. This will ease the transition as consumer-grade services are cut off and lessen the impact on any business operations. It will also provide centralized management, auditing, and compliance giving the organization the required visibility to manage risk properly.

There are multiple options for secure file transfer and storage solutions available both in the cloud and locally hosted. Many of the consumer-based solutions like Dropbox and Box.com offer plans for businesses that include the necessary security and compliance features. Some services are focused only on secure file transfer options for businesses like Citrix ShareFile. Organizations that want to host their own secure file sharing solution can opt for using Secure File Transfer Protocol (SFTP), which is included in most Linux distributions and available on Windows. Unencrypted file transfer options like legacy FTP services cannot be used securely and must be avoided.

A simple security change that all organizations can make to improve their security posture is to limit local administrator rights to workstations. The fact is that most malware will not run correctly if running with regular user permissions. A user who opens a malicious Word document would only be exposing assets where they have permissions. This can slow down an attacker because they need full administrative rights to gain further access to the network and deploy ransomware payloads. An attacker running with local administrative rights should be able to compromise the entire organization in less than an hour. The same attacker without local administrative rights may take double that time, giving the information security team time to detect the attack.

Users do not need to have local administrator rights to perform any standard Windows functions. Many IT organizations that run into application issues will simply add the user to the local administrators' group to quickly solve the problem. It does take time and effort to determine application compatibility and grant the appropriate granular permissions. These often include granting write permissions to Windows system folders or specific registry keys. However, the long-term security benefits far outweigh the quick fix of adding users to the local administrators' group. Organizations need to support their IT departments and allow the time and resources necessary to test and install applications using appropriate permissions or suffer the consequences. The majority of the organizations (81.8%) that participated in the survey have already implemented this control.



19. Do you restrict administrative permissions to user workstations?

22 responses

Source: ELFF 2020 Cybersecurity Survey

One of the most effective security controls to further prevent the execution of malicious code on workstations is through application whitelisting. The concept is that only applications approved to run in the environment are allowed to execute on company workstations. This provides a much higher level of protection than the blacklisting approach used by traditional security products like antivirus. Whitelisting is very resource-intensive to configure because it requires the organization to document each application that needs to run in the environment. Ongoing maintenance can be resource-intensive as well because each new application or upgrade must be approved as well. However, this is a very effective control that can be used in high-security environments.

Microsoft has an optional feature called AppLocker in Windows 10 Enterprise that provides application whitelisting capabilities. It is not supported on standard versions of Windows 10 Pro or Home, so it will not be applicable for smaller companies. The configuration of AppLocker is done using standard Group Policies in traditional Active Directory environments. The AppLocker policies can also be deployed through Microsoft 365 Endpoint Manager once defined in Active Directory. Attackers can bypass AppLocker if the configuration is not well managed, so organizations need to plan to resource the project appropriately for maximum defensive effectiveness.

AppLocker is just one feature that should be considered in on overall system configuration management strategy. A default installation of Windows is vulnerable to several attacks and exploits. This is by design as Microsoft provides a compatible out-of-the-box installation to address most customers' needs. However, the configuration of Windows workstations and servers needs to be hardened against known security vulnerabilities and to provide enhanced logging for incident response. This is true for all other operating systems, including Linux, Macintosh, and network hardware.

The Center for internet Security (CIS) offers detailed guides for hardening all types of operating systems for free. The documentation they provide is very detailed and provides insight into why each configuration change is being made and potential application compatibility issues. They are excellent resources for IT professionals to learn the internals of how operating systems function and their specific security vulnerabilities. CIS sells tools to help organizations automate and monitor these configuration changes to ease implementation requirements.

Microsoft provides its own tools for system management and configuration to harden Windows systems and monitor for deviations. Most of the hardening configuration for Windows systems can be done with Group Policies included with Windows Server. Larger organizations may have additional options, such as using Microsoft Endpoint Configuration Manager to monitor for deviations from hardened configurations. Microsoft has bundled Endpoint Configuration Manager (Previously called Intune) into Microsoft 365, which can provide hardening and monitoring for small businesses as well.

Another hardening recommendation that organizations should implement to reduce their security risk profile is to limit the use of Microsoft Remote Desktop Protocol (RDP) in their networks. This service is built-in to the Windows operating system going back to Windows XP and enabled by default. Any user with administrative access can access all the computers on a corporate network using one username and password. Attackers utilize RDP to deploy malicious code once they gain access to a single username and password. Disabling RDP where not necessary can slow the attacker’s progress and allow more time for detection.

Microsoft PowerShell has become an essential tool for administrating Windows networks and Microsoft 365 cloud environments. It utilizes .NET to expose core operating system functionality to the scripting language. Attackers have become extremely adept at using PowerShell in their attacks because it is provided on all Windows systems and will not be detected by standard antivirus. The popularity of using PowerShell for attacks has prompted some attackers to rename it the Microsoft “post-exploitation scripting language.” Many automated attack tools and frameworks are available for PowerShell simplifying these styles of attacks even further.

The use of PowerShell must be restricted and logged on a corporate network. Many attackers will attempt to use the older versions of PowerShell to bypass security protections. These older versions can be restricted or uninstalled. Group Policy can be used to force the restriction of execution on PowerShell scripts to only those signed with a cryptographic security key. PowerShell commands can also be centrally logged to detect any malicious use or for forensic investigations. Microsoft offers additional guidance on securing PowerShell that all organizations should review to reduce the malicious use of this very powerful tool.

One of the fundamental challenges in system management is providing software security updates to all corporate-owned systems. Microsoft releases its patches on the second Tuesday of every month. However, they offer tools that allow system administrators to manage the deployment of these patches. The biggest management issue comes from software not provided by Microsoft that also requires security updates. Oracle Java, Adobe Acrobat, and Mozilla Firefox are examples of third-party applications that can introduce critical security vulnerabilities into the environment.

Organizations that are using Microsoft Endpoint Configuration Manager can package third-party updates to be deployed to all corporate systems. This platform is expensive and can be complex to manage, requiring dedicated IT resources to be effective. Several easier-to-use systems can be just as effective in smaller businesses like BatchPatch or PDQ Deploy. Third-party software updates can also be deployed directly through Group Policy for free but may require a serious time investment to become fully operational.

The COVID-19 pandemic has driven many organizations to move office workers to home offices. These initially temporary solutions will most likely become permanent in the future as organizations have saved on office expenses. The use of Virtual Private Networks (VPN) has increased as a result and is an effective control for remote workers. A correctly configured corporate VPN solution can protect the remote workstation as well as the company network.

One of the biggest corporate VPN configuration mistakes is the use of split tunneling. The most secure use of a corporate VPN is to send all network traffic from a remote system, including internet requests through the corporate network. Some organizations utilize split tunneling, which allows the remote system to bypass the corporate network for local network resources and internet browsing. This effectively exposes the remote system to internet-based threats as corporate web security systems are bypassed. This also allows any other system on the home user network to access the remote system. A personal computer used by another family member that is infected with malware could find a path into the corporate network through the remote system.

Many employees that have become familiar with the security offered by corporate VPN solutions believe they must implement a personal VPN solution. The marketing for these personal VPN solutions offers promises of privacy and protection when using a public WIFI network. However, these solutions can present other security risks when used to access corporate-owned information systems.

Personal VPNs aggregate all the network traffic from the remote system, and many sell advertising based on usage. They have also been found to be maintaining logs of network traffic even if they do not sell the data for advertising. These logs provide detailed insight into the corporate data being sent and could capture any inadvertently unencrypted information. The security protocols used by many personal VPN systems are lacking and provide an easier attack vector for threat actors. Personal VPNs also disguise the geographic source of data transmission, which can cause compliance issues for regulated corporate data transmission outside of the United States. Organizations should block any access to corporate information systems using personal VPNs.

There are so many security technologies available that it can be easy to forget about the fundamentals. Increasing the strength of basic security controls like passwords can add significant improvements to the organizational security risk posture. The outdated guidance that is still proliferated through auditors and compliance frameworks is that a complex eight-character password changed every 90 days is considered secure. The reality in 2021 is that a complex eight-character Windows password can be brute-forced offline in less than a minute using standard PC hardware once an attacker is able to acquire the password hashes.

As directed by NIST, modern password guidance defines the use of longer passphrases that are changed less frequently. A passphrase is defined as a series of random words chained together and used as a password. This approach can create passwords that are over 26 characters long but still memorable by the user. NIST also recommends that these passphrases not be changed unless they are considered compromised. This provides much stronger passwords that are much easier for employees to adopt.

Password management becomes a serious problem as passwords get longer and more complex. People tend to reuse passwords for multiple systems to simplify password management. Attackers are aware of this practice and will use a username and password found in a data breach from another site against corporate systems in a password spray. Password managers have become necessary to prevent these types of attacks and make passwords even stronger. Password managers allow the user to generate long random series of impossibly strong characters while easing the process for users.

Enterprise password managers like LastPass can also provide additional security benefits. The information security team can receive reports about password reuse or passwords for sites that have been compromised. The reports will also provide a score for the complexity of user passwords for auditing and remediation. The inventory of sites and user accounts can also be passed on to a new employee easing the transition and eliminating the risk of leaving access to corporate systems after employment ends.

The most important passwords to manage in an organization are those for administrative access. They are used infrequently for system configuration or troubleshooting and often need to be shared between multiple IT departments. It is not uncommon to find IT staff sharing simple text files or Excel spreadsheets that contain all of the administrative logins for the corporate systems to perform their jobs. These IT departments often manage hundreds of these administrative accounts ranging from network hardware to administrative portals for cloud applications.

Privileged account management systems can be a powerful tool to manage all administrative logins. These platforms are similar to enterprise password management systems but offer additional security features for these highly sensitive accounts. Each time an administrator account is used, the activity is logged for future audits. They can scan the network for accounts with administrative privileges and automatically add them to the system. They can even provide password changes for embedded administrative accounts like those used to run services so that these passwords are never stale.

Many administrative accounts are associate with vendors that require remote access for support and maintenance of corporate applications. A huge number of web-based products can be used to gain remote access inside a network, including TeamViewer, GoToMyPC, and LogMeIn, for example. However, these platforms also allow attackers to trick employees into providing remote access to the corporate network. The uncontrolled use of these remote services can also lead to unauthorized changes and the lack of visibility into who is accessing the network. This is both an information security and compliance risk that must be managed.

Organizations must adopt a single centralized solution for remote support that provides strong authentication and logging. All other consumer-grade remote support solutions need to be blocked at the firewall. This can be difficult to implement as many vendors will only support a single remote access solution. They may even threaten that the restriction of remote solutions interferes with their ability to provide support. However, they must recognize that this attack vector is just too simple to exploit. The organization may want to survey their vendors to find common solutions that may be used. The remote access solution should then be included in any future contract negotiations with vendors to eliminate future contention.

Not all firewalls have the technical capabilities to block specific applications like web-based remote access sites. Nextgen firewalls have been around for several years and offer far more protection than the simple firewalls of the past. A Nextgen firewall can inspect network traffic and analyze the application use and any potentially malicious content. Organizations can then restrict specific types of websites like social media or protocols used for instant messaging. These firewalls can also use threat intelligence feeds to update reputation lists to prevent users from accessing malicious sites. Palo Alto was one of the first entries into this market segment, but almost all vendors have a NextGen solution available.

NextGen firewalls have limited capabilities since encryption was more widely adopted on the internet after the Snowden revelations in 2013. Encryption prevents the Nextgen firewall from decoding the network traffic to identify the application being used. The firewall will then act like a traditional firewall, only forwarding network traffic based on ports and IP addresses. Threat actors utilize encryption just like every other legitimate website, so encrypted attacks will go undetected. Nextgen firewalls can decrypt internet traffic, allowing the application inspection capabilities to be fully utilized.

Many organizations struggle with the politics of decrypting traffic and the associated visibility that is gained by logging all website activity. There are concerns that employees accessing personal sites with usernames and passwords could be exposed along with other private information. There is little risk that an attacker could access the cleartext information if the decryption occurs within the same firewall hardware. However, there is a slight risk that unencrypted information could be inadvertently captured into a security log. Organizations where this is a concern, can choose not to decrypt information from specific application categories where personal information may be collected.

The firewall has become the symbol of information security as it has been a primary control used since corporate networks were first connected to the internet. Firewalls can also be a useful security control inside the corporate network and not just at the internet perimeter. The typical network allows for fully unrestricted communication between all connected systems. This legacy configuration benefits attackers who only need to compromise one system to access the entire network. They can target the most vulnerable IoT-based device like a lightbulb and pivot to accessing critical business information systems.

Networks should be logically segmented from each other using firewalls to restrict communication between zones. Segmentation designs can be implemented based on several factors, including device type, data classification, or separation of business processes. When designing a network segmentation plan, the most important concept is maintaining the minimum necessary standard. The goal is to design a segmentation plan that restricts any communication that is not completely necessary to support business operations.

IoT devices are an excellent example of where segmentation can be used effectively to reduce risk. These inexpensive devices often lack basic security capabilities and are difficult to patch. They can be run on a separate network that restricts communication to only the necessary endpoints. Segregation can also prevent access to a core application from departments that have no business need for access. Marketing may not need access to transactional financial systems, and accounting may not need access to the CRM. Segmentation can also be used when vulnerable legacy systems running outdated software must be kept in production. A Windows 2008R2 server that is still in production to help collect accounts receivable from potential bad-debt accounts is an example where segmentation could be applied.

Segmentation does not have to be achieved through additional hardware firewalls alone. All major operating systems, including Windows, Linux, and Macintosh, provide software firewall capabilities. An organization can configure software firewalls in the same way to prevent unnecessary communication. A software firewall could prevent RDP access, as recommended earlier in this paper. They will slow down an attacker attempting to jump from one host to another. Firewalls included with operating system software can be a much more cost-effective solution for smaller organizations, although maintenance can become resource-intensive.

One area where segmentation can be used to bolster ransomware resilience is in segmenting backup data and systems from the rest of the network. Ransomware attackers will target backups if they successfully gain access to the network. Many organizations use online disk-to-disk-based backup technologies with the backends hosted on network-attached storage systems. Attackers may target the backup software or the network-attached storage system to destroy company data and increase the chances that the ransom will be paid.

Some organizations utilize network segmentation to only allow access to the backup system during the primary backup window. This reduces the time that the systems are exposed but still poses a risk if the organization is attacked during the backup window. Another strategy is to create an additional copy of the backup data that is only kept offline. These backup copies may not be as frequent as full backups but are meant to provide a starting point if all data from the first backup is destroyed. Offline backups require duplication in hardware which can be expensive as well. However, this is the only true ransomware recovery strategy that does not involve converting dollars to bitcoins.

Backup software companies are adapting to ransomware attacks and building in additional controls to prevent the destruction of data. The new capabilities include immutable backups that can be written once and never altered. The prevents an attacker from deleting backups even if they compromise the administrative password to the backup system. The immutable backups are usually retained for a predetermined time so that newer backups can be created. However, there should always be at least one immutable copy of the backup data to prevent unauthorized data alteration.

Cloud-based storage providers have also been adding immutable storage to their service offerings. Cloud-based storage was previously an easy target for attackers as they only had to locate an administrative account within the target network to wipe out the backup data. The addition of immutable storage makes the cloud-based storage providers an attractive solution for ransomware restoration that should be less expensive than purchasing additional hardware. Amazon offers an S3 Glacier Vault Lock that lets the customer define a data modification policy that cannot be changed once created.

No ransomware defense strategy would be complete without the deployment of Endpoint Protection and Response (EDR) tools. These products were originally designed to be used for incident response to provide detailed technical visibility into every operation of a compromised computer system. They have since matured to provide this same level of detailed visibility during normal situations to detect advanced attacks. They are similar to a black box recorder in an airplane that gathers telemetry data from every source in real-time. The EDR client is loaded onto all desktop and server systems to provide as much visibility into the monitored network as possible. Most EDR systems send this data to cloud-based analytics platforms, where it is categorized using machine learning algorithms and human review.

The endpoint has become the battleground as ransomware attacks typically start with a single end-user. The attackers gain their beachhead through a phishing email or compromised attachment and then gather credentials to move to other systems. Traditional antivirus is only looking for malicious code that has been seen previously. Ransomware actors typically utilize functions built-in to Windows that will not be detected by antivirus software. EDR instead looks for behaviors and activities that could be malicious and will catch the ransomware attack that traditional antivirus will miss.

There are some potential issues with the implementation of EDR systems that organizations need to address. These systems generate mountains of data that need to be analyzed quickly. This creates a huge resource problem for an already stressed information security team. Most of the EDR solutions can also be paired with a service offering to provide the resources necessary for monitoring the platform. This adds additional expense to an already expensive EDR solution that may price some organizations out of the market.

Operational issues that need to be addressed with an EDR deployment include dealing with false positives and performance impacts. The behavioral analysis used by EDR clients may not distinguish between a PowerShell script run by a system administrator or a malicious actor. EDRs will generate alerts that require some type of human triage before action is taken. Some EDRs impact system performance by as much as 20% due to huge amounts of data being collected for behavioral analysis. Organizations need to review their hardware inventory and determine the business impact of the performance loss imposed by EDR.

The following are an example of EDR products available on the market. This list is only provided for comparison and is not considered an exhaustive list of all providers, nor does it infer any type of endorsement. Organizations must conduct their own analysis of potential EDR solutions to meet their specific business and technical requirements.

Carbon Black was one of the early players in the EDR marketplace. The Carbon Black Response system has been used in many incident response scenarios. This platform provides the most thorough data collection from managed endpoints, but it comes at a performance impact. The system also requires a large commitment of resources from the information security team to analyze the data collected. Carbon Black is often paired with third-party monitoring services to alleviate the monitoring impact on the organization.

Microsoft offers an EDR solution as part of the highest-end Microsoft 365 license called Microsoft Defender for Endpoint. The codebase for the Defender client is already included in Microsoft Windows, making deployment as simple as enabling a checkbox. Microsoft includes clients for Macintosh and Linux systems, although they do not offer the same capabilities as the Windows client. Microsoft Defender for Endpoint utilizes playbooks for automating responses to specific events to reduce the monitoring burden. However, it still requires heavy resources from the information security team to be effective.

Crowdstrike is a newer entry into the EDR space with the Falcon Complete product and service. The Crowdstrike agent is lightweight and has less impact on performance than most other EDR solutions. Crowdstrike is one of the few EDR solutions that provide “hands-on keyboard” response services along with the software solution. They will actively prevent an attack as long as the organization has authorized them to act. They are confident enough in their software and services to offer a unique million-dollar breach warranty to their clients.

EDR tools enable additional security capabilities that organizations should utilize when the system is operational. Active threat hunting one of these capabilities. Threat hunting a process where security specialists proactively utilize EDR systems to scan through the network, looking for indications of compromise. This technique is much more effective than waiting for a security alert where it may be too late to act. Organizations with threat hunting capabilities may have found indications of the SolarWinds attacks before they were broadly identified, for example.

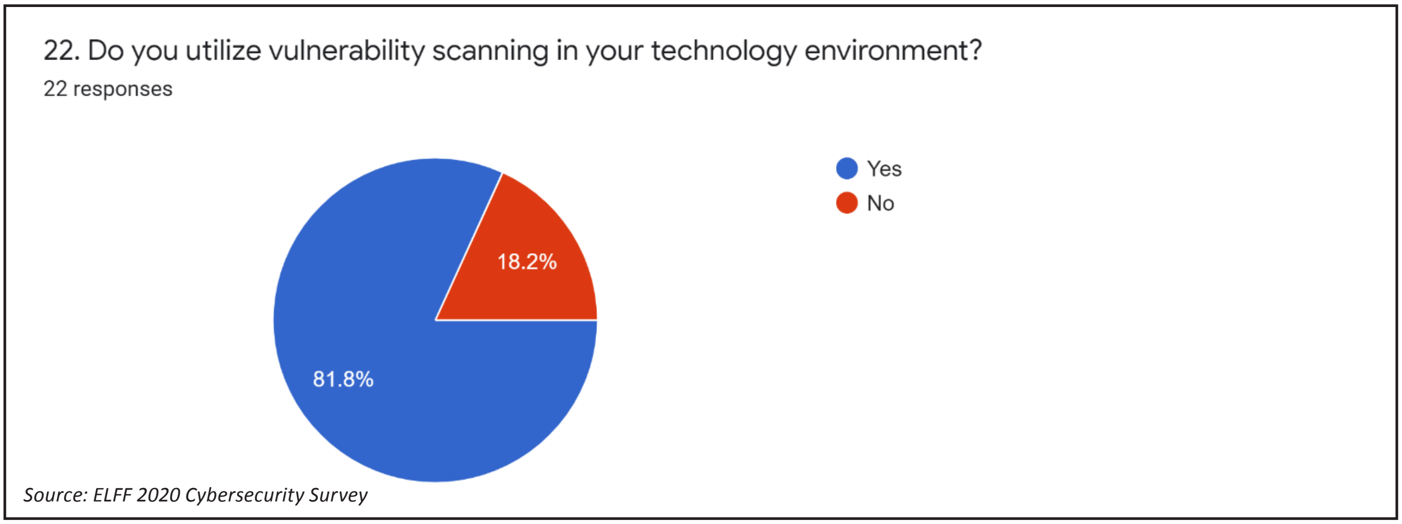
Threat hunting requires a unique skill set that is difficult to recruit and retain, especially in smaller organizations. There are service offerings through EDR vendors and partners that can provide skilled threat hunting for those organizations that cannot afford or recruit the required talent. Threat hunting is an expensive proposition regardless of internal or outsourced resources. It can be hard to show a return on investment to management when there are limited findings. However, the cost of threat hunting could be offset by detecting a single ransomware attack.

Additional third-party options can be used to fill the gaps in an organizational security strategy. Managed Security Service Providers (MSSP) offer multiple services beyond EDR and threat hunting. MSSPs typically utilize a managed Security Information and Event Management (SIEM) tool to aggregate logs for analysis. This could include logs from firewalls, IDS/IPS systems, antivirus software, Windows event logs, Syslog from network equipment, and even application activity logs. This provides a comprehensive view into the network operations that can help detect malicious activity across the organization. The MSSP can then operate as a Security Operations Center (SOC), relieving the burden of analyzing all of this information from the organization and become an extension of the internal information security team.

A SIEM can be a very useful tool for information security teams providing insight into all aspects of security. Organizations can choose to run their own SIEM instead of utilizing an MSSP for management. Many organizations have difficulty implementing a SIEM as it is a complex and resource-intensive undertaking. The first impulse is to send all logs unfiltered into the SIEM without a plan. This leads to increased expense as most SEIMs are licensed by data throughput, performance problems due to index issues, and no progress in converting logs to actionable intelligence. Organizations must commit positions dedicated to implementing and maintaining the SIEM to make the most of their investments. This is why MSSPs are a good solution for organizations without large security teams and dedicated SEIM engineers.

Organizations that want to take on the challenge of running their own SIEM have several choices. Licenses for a commercial SIEM can be expensive and become cost-prohibitive for smaller organizations. This is true whether the SIEM is hosted locally or in the cloud. There are some excellent open-source options that are available for free that may work well for organizations that cannot afford the commercial options. Graylog is a commercial SIEM product that offers an open-source version, for example. Another similar option is Wazuh, where they offer a commercial and open-source version. Both platforms are built on the open-source Elasticsearch data management platform and very capable. The downside to using these open-source solutions is that they take more time to build, and there is minimal support. However, these solutions can keep pace with a commercial solution if an organization has information security talent to build and maintain the platform.

An organization must also include a strategy for scanning their networks for vulnerabilities. These could include missing security updates, misconfigured systems, or the use of default credentials. The organization must be aware of these vulnerabilities before an attacker can exploit them. There are many solutions available in a wide range of prices from Qualys, Tenable, and Rapid7, to name some examples. They offer cloud-based and locally hosted scanning options. They can utilize passive network traffic analysis, locally installed agents, or active network scanning to identify vulnerabilities. Passive scanning and local agents can be used on a network where the potential noise of active network scans can be disruptive.



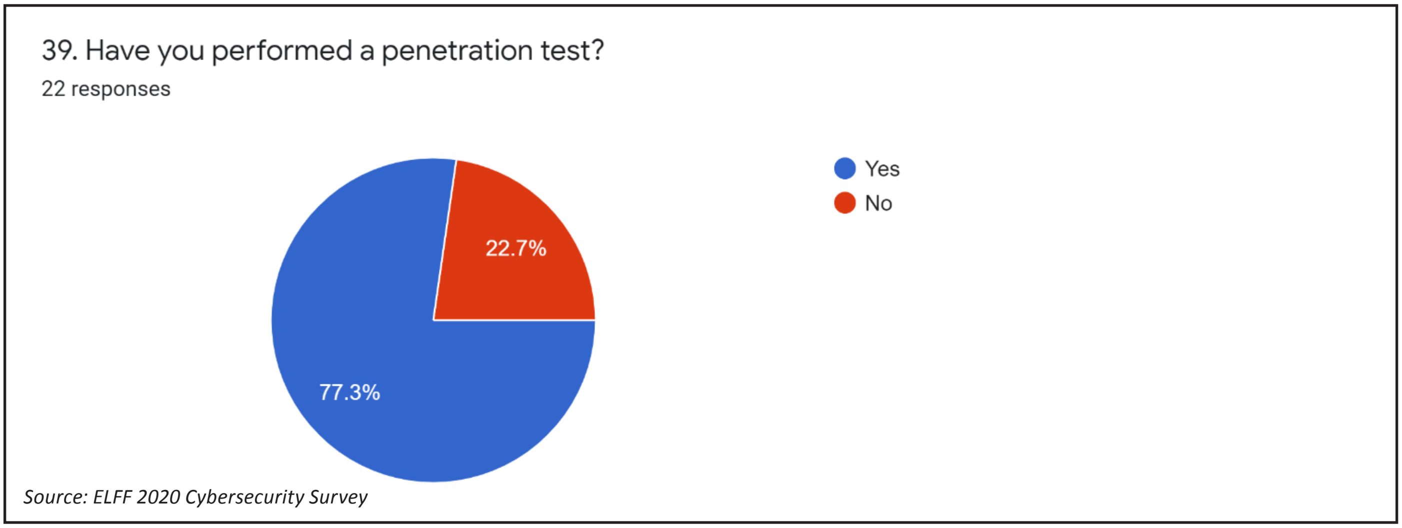
22. Do you utilize vulnerability scanning in your technology environment?

22 responses

Source: ELFF 2020 Cybersecurity Survey

Vulnerability scanning can also be provided through an MSSP if the organization lacks internal expertise. There are efficiency gains in the integration of vulnerability scanning with incident response and threat hunting services. The MSSP can use information from vulnerability scans to determine if a specific attack would be successful against the intended target. An exploit of the WannaCry vulnerability (MS17-010) launched by an attacker would not be successful against a fully patched Windows server, for example. This allows the MSSP to concentrate their attention on the highest priority attacks that could have a significant impact.

Vulnerability scanning provides a high-level view of the technical security risks inherent in a corporate network. However, it does not simulate the real-world impact an attacker could have using these vulnerabilities. Organizations need to be performing penetration tests on their networks to gain insight into potential attack paths and the effectiveness of their network monitoring and defenses. A penetration involves the combination of automated and manual testing by experts in technical information security. The goal is to identify weaknesses in security posture so the organization can remediate any findings.

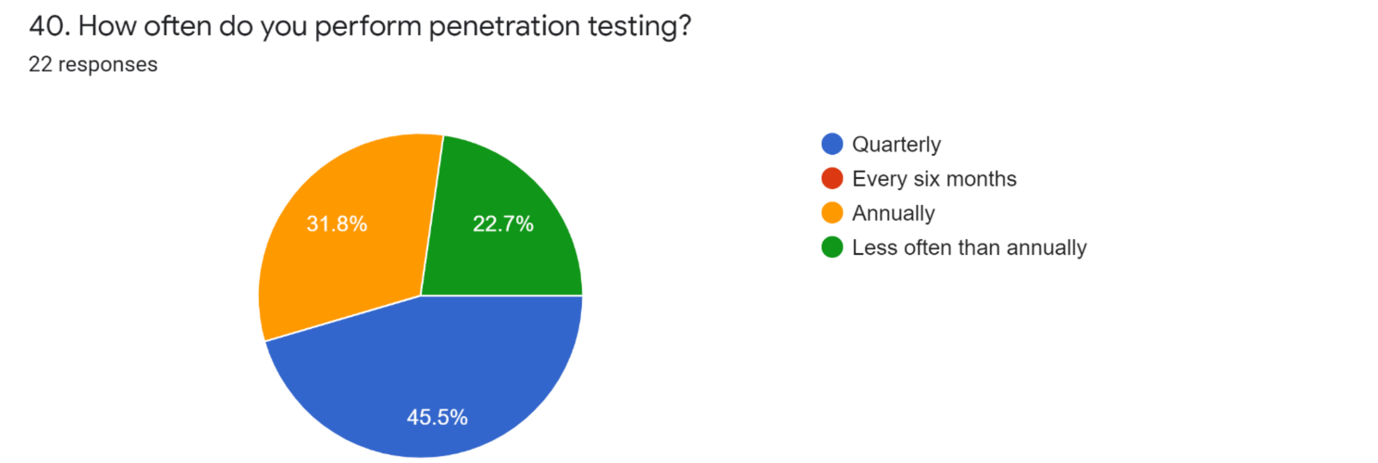


39. Have you performed a penetration test?

22 responses

Source: ELFF 2020 Cybersecurity Survey

Penetration testing is a highly technical field and requires very specific skillsets and years of previous experience. Many penetration testing companies will offer cheap rates because they are only using automated vulnerability scans without the expertise of seasoned professionals. Their reports are often full of false positives and unverified vulnerabilities. These types of tests are not only a waste of time and resources but also create a false sense of security. Organizations need to be very selective in their choice of penetration testing firms to get maximum value from the service.


40. How often do you perform penetration testing?

22 responses

Source: ELFF 2020 Cybersecurity Survey

The downside to penetration testing is that it is usually a time-constrained engagement. The penetration testers are under pressure to complete their technical work and report their findings in a short amount of time. A typical penetration tester will usually spend at least 70% of the time scheduled for the engagement writing the final report. Attackers are not limited by time, nor do they have to write a report on their activities. This makes a penetration useful but not an accurate predictor of attacker behavior and defensive capabilities.

This is why some organizations have adopted the concept of red teaming from military training. A red team engagement stimulates the activity of known threat actors. They will use the same types of tools and techniques as these threat actors to attack the corporate network. The blue team is charged with detecting these attacks and responding appropriately. The red team will then share any successful tactics and techniques back to the blue team to make improvements before the next exercise. This form of technical wargaming within the corporate is one of the best methods to drive organizational security improvements.

Thus far, the majority of the recommendations have been focused on technical security controls. The physical security of the organizational technology assets must also be addressed. A top-tier antivirus solution will not prevent a data breach from the computer from being stolen from an unlocked office. Physical access controls must also be in place as well. This includes the use of locks, card access controls, security cameras, and visitor escorts. A physical security plan must be developed and implemented after a thorough physical security audit.

Physical security testing can help determine where the weak points are in physical security controls. Many security firms offer these types of assessments and can often be combined with a technical penetration test. A physical test may use social engineering to determine if they can get in through a secured entrance into the building. They may also try to pick locks, climb through the drop ceiling, and hijack security camera surveillance systems. The results of these tests can be enlightening as most organizations assume their physical security measure work as intended. It can be uncomfortable for an organization to undergo these types of tests, but they are invaluable for improving physical security.

Physical attacks can take many different forms and are only limited by the attacker's creativity. An attacker that gains physical access into a business can gain access to technical assets through several different methods. They may insert a USB drive into an unmanned computer and retrieve information or install malicious code. They can also leave behind USB devices that intercept keystrokes to capture passwords and confidential information. They can install a network tap that intercepts all network communication stripping out passwords or financial information. Some will even attach a small device using a cellular radio to the network to provide remote access without any detection.

There are technical controls that can improve physical security or reduce the impact of physical security intrusions. USB drives should not be allowed for use in a corporate network. Some organizations will provide corporate-approved USB drives that offer encryption and restrict all other USB drives from functioning correctly. Organizations with highly sensitive networks have used hot glue guns to seal the USB ports off completely. This unorthodox approach effectively prevents any types of USB-based attacks but can impact productivity. This is an organizational risk-based decision that must balance the threats and potential for business process interruption.

Microsoft Windows includes several security features that can be used to increase physical security. User sessions can be locked after a period of inactivity to prevent an attacker from gaining access to an unattended workstation. Microsoft includes BitLocker encryption for both hard drives and USB drives in Windows 10 Professional. This prevents an attacker from accessing data even if the device is lost or stolen. Group policies can be applied to force all removable USB drives to be encrypted before data can be written to them. Windows 10 Pro computers protected with BitLocker will detect if an attacker attempts to decrypt the drive-through brute force and lock it until a recovery key is provided. These capabilities are included in Microsoft Windows and should be implemented by all organizations regardless of size.

Compliance and Regulatory Updates

California passed Proposition 24, The Consumer Privacy Rights Act, during the general election on November 3, 2020. This new law adds additional privacy protections to the existing California Consumer Privacy Act that just went into effect on January 1, 2020. Proposition 24 is focused on limiting the amount of tracking that can be performed by any organization operating in California. This law is not intended to target financial institutions directly. Still, it is the latest in a long line of increasing legislation and compliance requirements attempting to stem the overwhelming tide of data breaches and privacy violations. However, it is an example of how increasingly important it is for all organizations to understand this increasingly complex legal and compliance environment or face significant financial penalties or revenue loss.

There are laws and regulations across almost every industry being enforced by state, federal, and industry groups. The United States does not yet have a federal level privacy law which has created a patchwork of state solutions, further increasing complexity. The Gramm Leach Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) are examples of industry-specific federal laws targeting financial institutions and healthcare providers, respectively, which have been around since the 1990s. The U.S. is releasing final revisions to the Cybersecurity Maturity Model Certification (CMMC) in 2020 to increase the defense industrial base's cybersecurity posture for new contracts starting in 2021. American organizations doing business in Europe also have to consider compliance with the European Union's General Data Protection Regulation (GDPR).

The following is a brief review of some of the regulations that could affect leasing and finance organizations. This is not a full list of every potential law or industry requirement that could affect an organization but some of the most common. Organizations will need to perform a full compliance review to build an appropriate risk management program to discover and manage compliance with all of the appropriate regulations that could apply. However, the requirements of many laws overlap, and organizations can develop crosswalks to show compliance with multiple regulations.

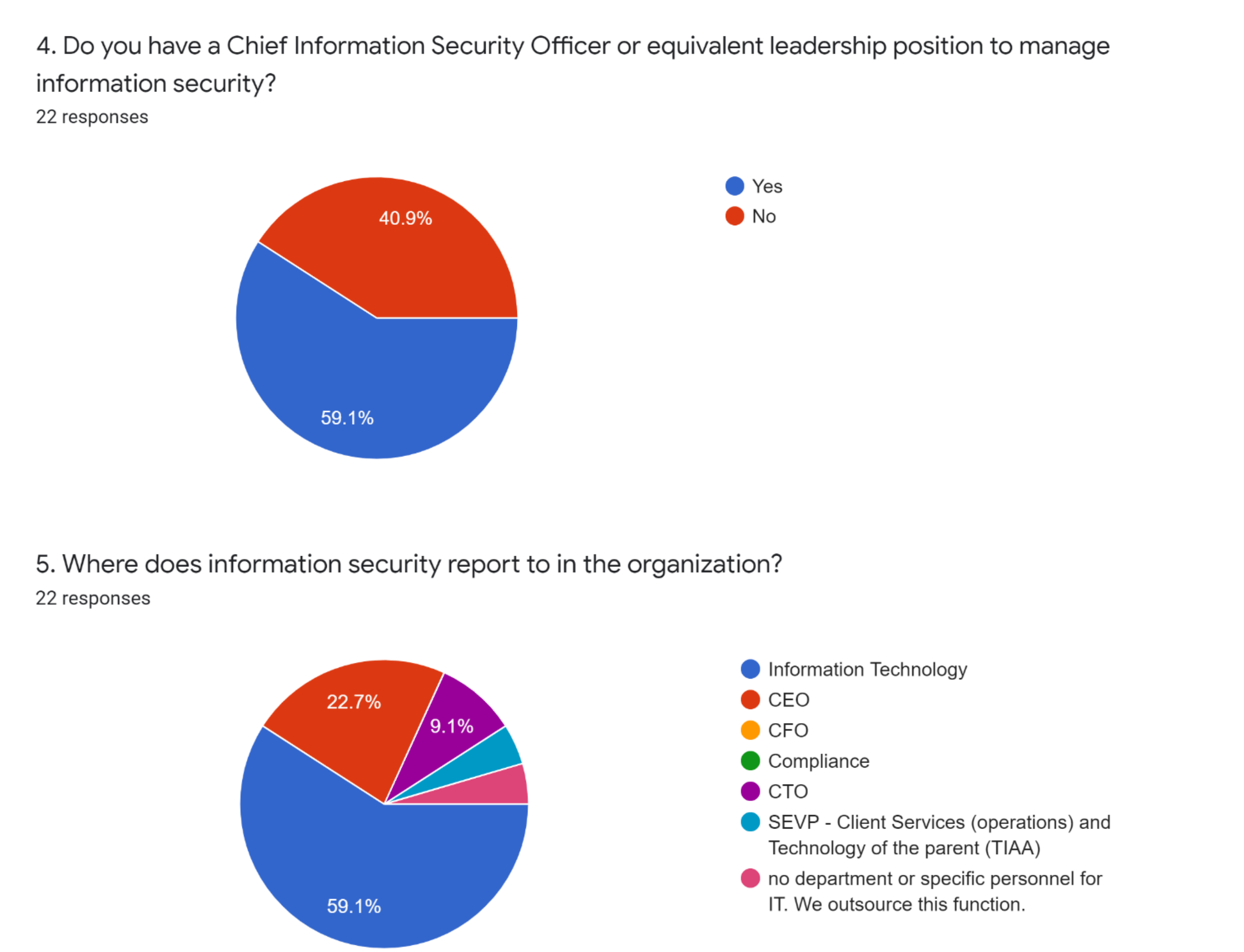
1999 Gramm Leach Bliley Act (GLBA)

The Gramm Leach Bliley Act (GLBA) was passed in 1999 to repeal part of the Glass-Steagall Act of 1933. This legislation's primary focus was to allow mergers and acquisitions between banks, securities companies, and insurance companies that the Glass-Steagall Act previously forbade. However, this bill also contained language to control the collection, disclosure, and privacy of customer personal financial information by financial institutions that are still enforced today. The Federal Trade Commission is charged with the enforcement of the GLBA, and it is worth reviewing some of their more prominent cases for insights into compliance.

The GLBA is divided into three separate sections regarding privacy and information security. The first section is the Financial Privacy Rule which requires that the financial institution publish their privacy policies. These policies need to describe what information is collected about the customer, how the information is shared with other institutions, and how the information is kept private. It also must allow the customer to opt-out of the sharing of their personal information at any time. The financial institution must also maintain contracts with any third-party vendors that require them to maintain the privacy of the customer's personal financial information while in their possession.

The second section of the GLBA is the Safeguards Rule requires that the financial institution assign an employee to manage the security program. This is typically referred to as the Information Security Officer, although many organizations have elevated this position to a Chief Information Security Officer or CISO. GLBA requires that this individual create a documented information security program to monitor and test the mitigation strategies put into place. The security program must utilize formal risk analysis and management techniques to identify and manage potential issues with handling this protected information when created, stored, or transmitted.

During this study, the majority of organizations surveyed do have a CISO in place to address information security and potentially GLBA compliance. There is no standard to where the CISO should report within the organization, and there are multiple models. The most effective CISO should report to the CEO to be part of the overall business strategy. A CISO reporting to Information Technology may be focused only on technical information security solutions and not fully integrated into business processes. This CISO may also lack the political power necessary to implement necessary business process changes. The majority of the organizations included in the study that have a CISO position have it reporting to Information Technology, limiting their overall effectiveness.



4. Do you have a Chief Information Security Officer or equivalent leadership position to manage information security?

22 responses

5. Where does information security report to in the organization?

22 responses

22.7%
9.1%
59.1%
● Information Technology
● CEO
● CFO
● Compliance
● CTO
● SEVP - Client Services (operations) and Technology of the parent (TIAA)
● no department or specific personnel for IT. We outsource this function.

Source: ELFF 2020 Cybersecurity Survey

The final section of the GLBA is called Pretexting protection. This section is fairly unique to GLBA and not specifically addressed in other regulations. Pretexting is the act of trying to acquire personal financial information illegally by impersonating someone with appropriate access to the information or the person. Pretexting is part of an overall Social Engineering technique where a criminal uses non-technical means to con the information out of the victim. An example of pretexting would be receiving fake credit card emails requiring the receiver to enter their account numbers.

General Data Protection Regulation

The European Union has developed a very conservative view on the protection of personal information. Some speculate that this conservative view was formed out of the events surrounding World War II, where personal information from the census was used to persecute different ethnicities and members of religious groups. This led to a European Convention on Human rights in 1950, which stated, “Everyone has the right to respect for his private and family life, his home and his correspondence.” This statement is reflected in the data privacy legislation that followed in 1980 and contrasted sharply with the view of privacy in the United States.

The changing political climate in Europe in the late 1980s and the fragmentation of privacy laws made it apparent that the European Union needed a new unified standard in the 1990s. The rapid development of technology and, ultimately, the privacy challenges that came with the internet made creating a new law imperative. This is why the predecessor to GDPR, the European Union Data Protection Directive 95/46/EC of 1995, went into effect in 1998, and versions of it were adopted into 27 separate national data protection regulations across Europe.

It quickly became evident as companies that built business models around collecting personal data and more companies moved transactions online that tougher regulations than the Data Protection Directive were required. Banks moved to use online services, and credit card transactions began running across the internet. The meteoric rise of social media sites like Google and Facebook in the early 2000s made personal information more valuable than ever. The existing Safe Harbor requirements for transferring data outside of the EU to countries like the U.S. were not sufficiently stringent to provide adequate protection for the data of EU Citizens. The EU Data Protection Directive of 1995 no longer encompassed the controls necessary to enforce the spirit of the law and uphold the privacy values in the EU.

The General Data Protection Regulation was passed in 2016 and was effective on May 25, 2018. This law is the most stringent privacy legislation enacted by any government up to this point. It encompasses the European spirit of privacy protection and enacts serious penalties for those found non-compliant. Organizations worldwide that do business in the EU or market to EU citizens now find themselves needing to comply with GDPR or face stiff penalties. Organizations operating in the U.S. may come under increased scrutiny due to the European view that the U.S. has insufficient privacy regulations in place to protect its citizens.

There are many specifications in the 119 pages of GDPR that will take major organizational initiatives to meet the compliance requirements. However, there are two major issues that organizations will want to understand right away. The first is that the breach notification requirement with GDPR is only 72 hours. This is a different type of notice than prevalent in U.S. privacy law, where the notice is made to the authorities as well as the individuals within several weeks to two months. However, an organization must notify a supervisory authority that enforces GDPR without delay and not later than 72 hours of becoming aware of the breach.

The challenge in providing the breach notification in 72 hours is that many forensic investigations take much longer to uncover a security incident's details. The GDPR notification timeframe does not leave sufficient time to investigate the full nature of the breach unless an organization possesses the resources to perform the investigation rapidly. These resources can be costly to maintain, whether in-house or provided through a managed security service provider. The details that must be included in the data breach notification follow from the GDPR text:

a) describe the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

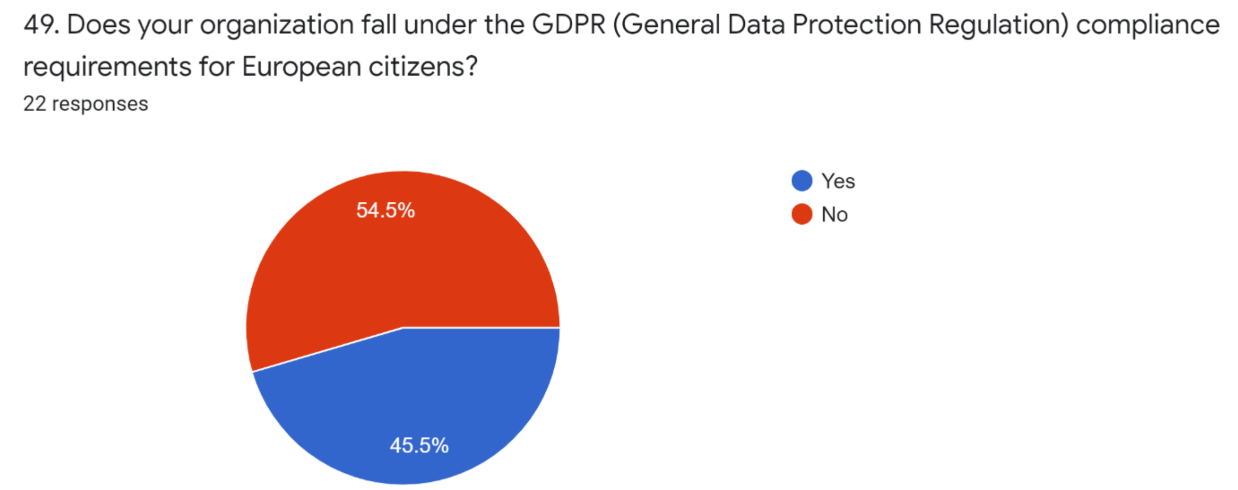
b) communicate the name and contact details of the data protection officer or other contact points where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The second major issue that organizations need to understand about GDRP is the number of fines for non-compliance. The most serious infractions can result in fines of €20 million or 4% of the organization's worldwide annual revenue from the preceding financial year, whichever amount is higher. The EU has learned that privacy regulations without serious penalties just become a cost of doing business for large organizations. The amount of the potential GDPR fine should get the CEOs' and boards' attention they were intended to impress. The EU has followed through on the threat of these fines, having levied over €177 million since the beginning of GDPR enforcement in 2018.

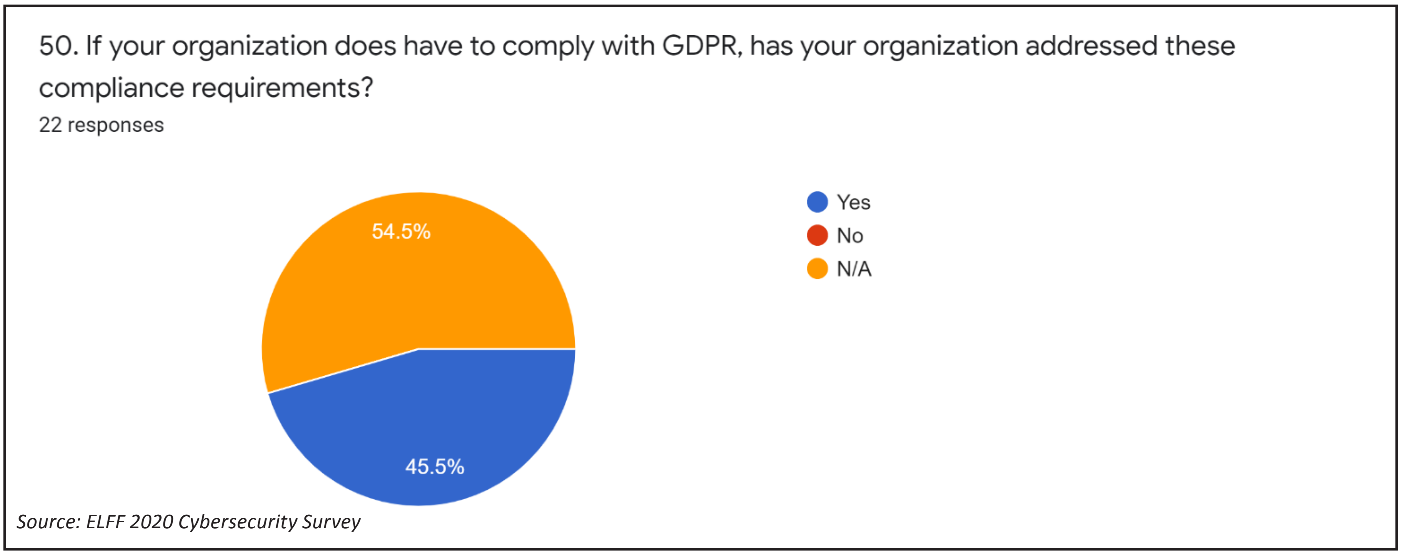
The equipment leasing and finance organizations surveyed through this research have taken note of the serious nature of GDPR enforcement. 56.3% of the organizations surveyed did have compliance obligations under GDPR. 100% of these organizations have developed security programs to maintain compliance with GDPR without exception. This point demonstrates that the EU was correct in its assertion that considerable fines would raise awareness and ultimately drive compliance with GDPR.



49. Does your organization fall under the GDPR (General Data Protection Regulation) compliance requirements for European citizens?

22 responses

Source: ELFF 2020 Cybersecurity Survey



50. If your organization does have to comply with GDPR, has your organization addressed these compliance requirements?

22 responses

Source: ELFF 2020 Cybersecurity Survey

The primary target initially for GDPR enforcement was the large tech companies like Google and Facebook. However, enforcement has been occurring across other sectors, including banking and finance. Bulgaria's DSK Bank was fined $569,930 for a data breach in 2019 by the Bulgarian Commission for Personal Data Protection which enforces GDPR in Bulgaria. The interesting point of this case was that there was never any evidence of a hacking incident. A former convict was found in possession of personal data on 33,492 people who had received loans from the bank. The personal data discovered in this breach seemed to indicate an insider threat as the data included copies of ID cards and property deeds along with account numbers. The actual source of the incident was never discovered, yet a significant fine was assessed against the bank under GDPR.

Cybersecurity Maturity Model Certification (CMMC)

The cyberattacks against the Defense Industrial Base have increased dramatically as the design and development of weapons and support systems move into the digital realm. U.S. Department of Defense development projects involves very long supply chains that pass through large prime contractors to medium-sized subcontractors to very small specialty manufacturing and machining shops. State-sponsored actors have been very successful in attacking organizations throughout the supply chain. However, the larger prime contractors have been developing mature information security practices while it is "business as usual" for the medium to small subcontractors.

A case study from FireEye, a prominent cybersecurity incident response company, states that these organizations have been targeted specifically by China-based actors to gain intellectual property to aid their own defense initiatives. These attacks are very different than the ransomware attacks that plague other industries as they are stealthy, and the company is usually unaware that their systems have been compromised. FireEye discovered at least seven systems at one defense manufacturer that had been compromised through phishing emails, for example. They also discovered that a China-based actor had infiltrated over 300 systems at another defense contractor and evidence that they had been in the system for several years. The attacks in both cases were aimed at acquiring intellectual property on the design and manufacturing of weapon systems. The categories of data that were compromised in the attacks investigated by FireEye are listed below.

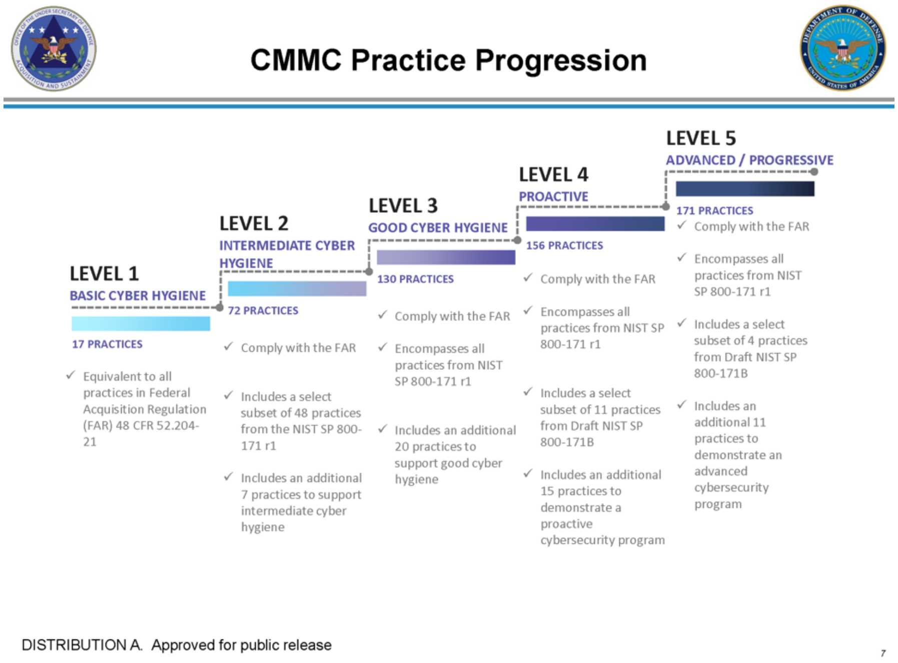
Data Stolen from Aerospace & Defense Organizations

- Budget Information
- Business Communications
- Equipment Maintenance Records
- Specifications
- Organizational Charts
- Company Directories
- Personally Identifiable Information
- Product Designs/Blueprints
- Production Processes
- Proprietary Product or Service Information
- Research Reports
- Safety Procedures
- System Log Files
- Testing Results & Reports

The Defense Federal Acquisition Regulation Supplement (DFARS), administrated by the U.S. Department of Defense (DoD), developed clause 252.204-7012 to counteract these attacks against the Defense Industrial Base. This regulation required all contractors and subcontractors to develop an information security program in line with the requirements outlined in the National Institution of Standards and Technologies (NIST) Special Publication 800-171 by December 31, 2017. NIST has a long history of developing these types of security requirements, and SP 800-171 provided a simplified framework that could scale from small to large organizations.

The lack of enforcement of DFARS clause 252.204-7012 was the primary reason why the NIST SP 800-171 standards were not adopted by many of the Defense Industrial Base organizations. This is because clause 252.204-7012 did not define exactly which organization was responsible for ensuring that organizations were compliant. The responsibility finally fell onto the prime contractors who had to specify the NIST SP 800-171 requirements in their contracts with the subcontractors. These prime contractors did not have the resources or the motivation to deny contracts based on missing information security requirements. It could directly affect their ability to deliver on major contracts for the DoD. This left the entire Defense Industrial Base open to attack from very capable adversaries as most organizations simply ignored the requirements.

It became apparent to the DoD that the original intent of NIST SP 800-171 was being ignored. The Office of the Under Secretary of Defense for the Acquisition & Sustainment (OUSD(A&S)) began working with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Development Centers (FFDRC), and the industry to develop a replacement called the Cybersecurity Maturity Model Certification (CMMC). This new requirement would start from the NIST SP 800-171 origins and scale up and down depending on the organization's type and size. Smaller subcontractors would need only a subset of the security controls required by a larger organization, for example. CMMC contains five different levels better to match the organization's size and security risk.



CMMC Practice Progression

LEVEL 1
BASIC CYBER HYGIENE
17 PRACTICES
- ✓ Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

LEVEL 2
INTERMEDIATE CYBER HYGIENE
72 PRACTICES
- ✓ Comply with the FAR
- ✓ Includes a select subset of 48 practices from the NIST SP 800-171 r1
- ✓ Includes an additional 7 practices to support intermediate cyber hygiene

LEVEL 3
GOOD CYBER HYGIENE
130 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes an additional 20 practices to support good cyber hygiene

LEVEL 4
PROACTIVE
156 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 11 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 15 practices to demonstrate a proactive cybersecurity program

LEVEL 5
ADVANCED / PROGRESSIVE
171 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 4 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 11 practices to demonstrate an advanced cybersecurity program

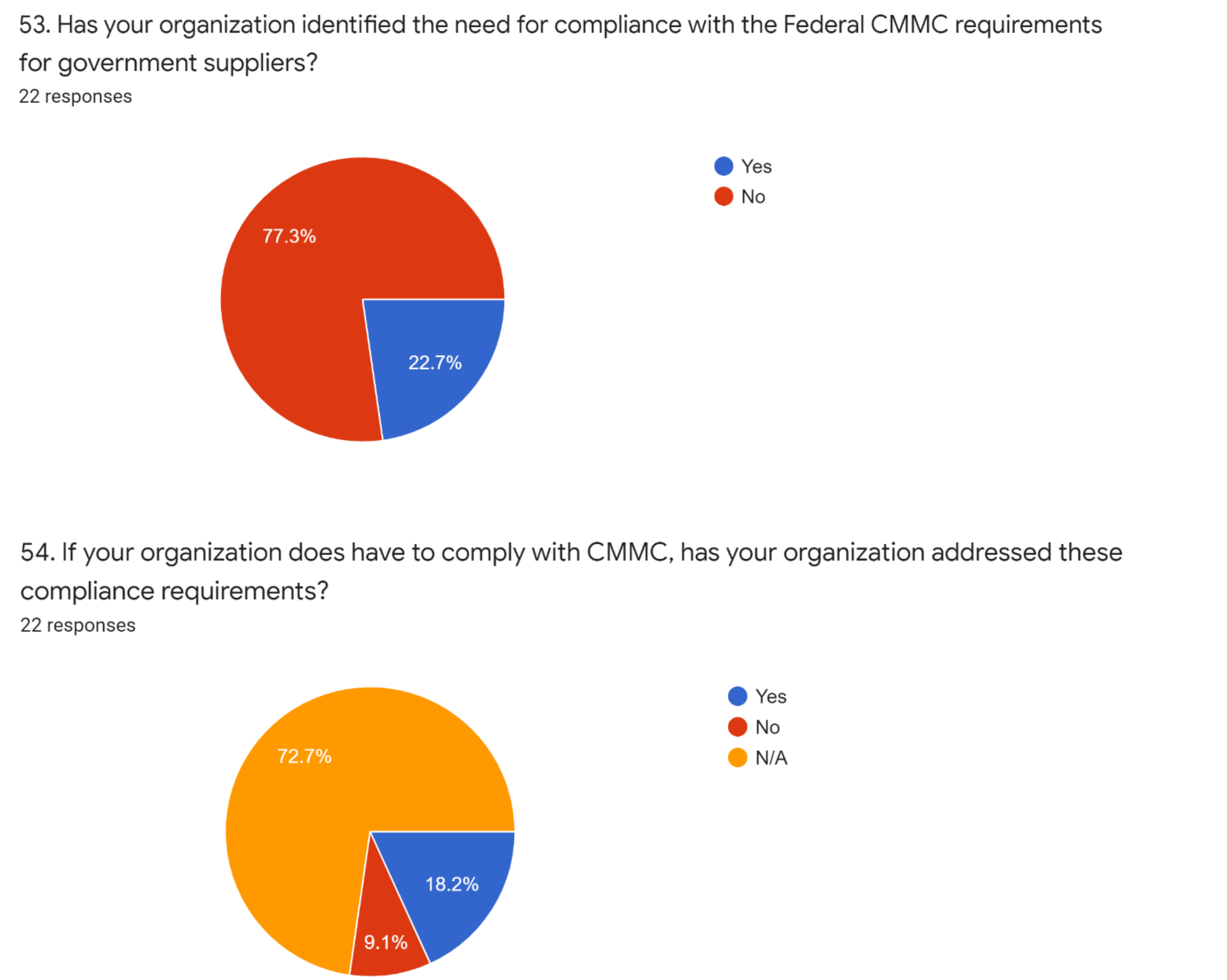
DISTRIBUTION A. Approved for public release

7

The biggest change made in CMMC was that it would be enforced through independent certification. Auditors have been trained and certified to produce audits for contractors and subcontractors in the Defense Industrial Base. These organizations will have to submit their certified audit results and any bid responses to receive work from the U.S. DoD. This takes the responsibility from the prime contracts who lacked the resources and incentives to perform the audits for NIST SP 800-171 compliance. The first contracts requiring CMMC certification are being released in 2021, and the DoD expects all contracts to require CMMC certification by 2024. The organizations that had already started on NIST SP 800-171 compliance have a head start and a competitive advantage.

CMMC will have a massive impact on the Defense Industrial Base, driving up costs and forcing consolidation of smaller contractors that cannot make the investments in information security. However, it may not be immediately clear how CMMC will affect the equipment leasing and finance industry. CMMC relies on the classification of data as Controlled, Unclassified Information (CUI) as defined in NIST SP 800-171. The definition of CUI is much broader than the data protected by any other security/privacy regulation. It covers multiple data categories, from critical infrastructure and defense details to procurement and acquisition of products. This definition of CUI could force some organizations in the equipment leasing and finance industry to adopt CMMC requirements to provide finance for contractors and subcontractors in the Defense Industrial Base.

A survey conducted through this research showed that many responders from equipment leasing and finance organizations (75%) have determined whether they need to comply with the CMMC requirements. A small number (12.5%) of these organizations have determined they must comply with CMMC but have not addressed the requirements. This is probably because CMMC is fairly new, and only a select number of contracts will require full compliance with the regulation. The number of non-compliant organizations should drop over the year as CMMC begins to mature.



53. Has your organization identified the need for compliance with the Federal CMMC requirements for government suppliers?

22 responses

54. If your organization does have to comply with CMMC, has your organization addressed these compliance requirements?

22 responses

Source: ELFF 2020 Cybersecurity Survey

Notable State Privacy and Security acts

All 50 states, including the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have enacted data breach notification legislation. These laws are similar yet have variations on specific points such as the definition of Personally Identifiable Information (PII), including SSN, Drivers License, and other account information. The definition of what constitutes a data breach and whether there was harm to the person that suffered the breach are also differences in these state laws. The breach notification timeframe also varies considerably, with Florida, Colorado, and Washington tied for the shortest at 30 days post-discovery. Most of these state laws will defer to Federal laws where notification is required. However, it is critical that any organization that operates in multiple states have legal counsel review the specific state notification requirements.

These data breach notification laws did little to stem the tide of data breaches and only made customers aware that their data had been compromised. They provided no framework for protecting personal data and limited penalties for when a breach occurred. This led the states to enact privacy protection laws to expand upon the existing data breach notification laws. Bills were introduced in at least 30 states in 2020, although the COVID-19 pandemic has delayed many. The bills that have been proposed have all adopted some form of the requirements found in GDPR as it has become a template for data privacy legislation. This includes some of the key elements of GDPR, such as the "right to be forgotten," where companies must delete customer data upon request and the right to request corrections for data elements that are deemed erroneous.

A detailed analysis of the numerous laws and proposed bills could be a research project unto itself. This paper will focus on some of the first laws passed and those with unique requirements. This includes the Illinois Biometric Information Privacy Act (BIPA), the California Consumer Privacy Act of 2018 (CCPA), and the New York Stop Hacks and Improve Electronic Data Security Act (SHIELD). Future bills will undoubtedly be based on these laws and should provide a preview of potential Federal privacy legislation.

Illinois Biometric Information Privacy Act (BIPA)

Illinois became the first state to pass a law that protected biometric data in 2008. Washington and Texas are the only other states that have followed up with their own variations on this law. The Illinois law is unique in that it is the only one that allows the individual to file a civil claim against an organization for potential violations. The amount of the claims are $1,000 for each violation and $5,000 for each intentional or "reckless" violation. The law also allows for the claimant to recover fees for the attorneys and any expert witnesses.

The law defines a biometric identifier as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." This type of data collection was not commonplace in 2008 as many organizations could not capture or store this information. Systems in place in 2008 included time and attendance systems where timeclocks used fingerprints to identify employees when they punched in.

However, the collection of video and audio biometrics has expanded dramatically since the passing of this bill. Inexpensive video surveillance systems can now track faces, and voice recording software can analyze audio for intent and identification. Commercially available products like Ring video doorbells can be used for facial recognition, and Amazon Alexa can identify voices and accidentally record private information. These advances in technology have made BIPA more relevant than when it was first passed in 2008.

The law is simple compared to other state privacy laws and only has three main provisions for the protection of biometric information. The three provisions from the law are as follows: An organization "cannot collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information unless it first:

1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

These requirements summarize that the person must first be informed that their biometric data is being collected. They must then be told how the biometric data is used and how long it will be stored. The final requirement is that the person must provide a written release for the organization to use the biometric data for the specified purpose. However, there are additional requirements for the organization once the release has been signed, including the prohibition of the sale of biometric information and list the requirements for disclosure of biometric information. The specific requirements from the law are:

a) "No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

b) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

   a. the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

   b. the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

   c. the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

   d. the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction."

The primary focus of BIPA is informed consent for the use and disclosure of biometric information. There is very little language in the law about how the organization should protect biometric information while stored. It states that the consumer should be informed about the retention period of biometric information while not offering any guidance to organizations on retention timeframes. There is no definition of data destruction requirements after retention timeframes expire. There is only a broad requirement for the organization to protect biometric data while being stored and in transit with the same or better protection as other confidential and sensitive information.

The combination of the broad language and civil penalties has caused over 40 class action lawsuits since 2017 in Cook County alone from various industries. An Illinois-based health care system was sued due to their use of biometric identification without notification for electronic timeclocks, for example. Another complaint was filed against Six Flags Amusement Parks for collecting guests' thumbprints in the park. Complaints have also been filed against major social media platforms in California for using algorithms to identify individuals in uploaded images. Many of the complaints have been dismissed as there has been a lack of agreement on the damages incurred by the plaintiffs bringing the lawsuits.

The impact of BIPA on the equipment leasing and finance industry is difficult to determine. The type of biometric information being processed and stored by the industry is probably limited in scope. However, the main complaints that arise from BIPA include using fingerprints for electronic timekeeping, which could be an issue if the organization conducts business in Illinois. The use of video surveillance systems in banks and other financial institutions in Illinois could also come under scrutiny if people are identified in the videos. The main takeaway from BIPA for the equipment leasing and finance industry may be that it will become the template for future legislation regarding biometric data privacy.

California Consumer Privacy Act of 2018 (CCPA)

The California Consumer Privacy Act of 2018 (CCPA) is currently the most stringent privacy law in effect in the United States at the time of this paper. The law is like GDPR in many ways but did not spend as much time in the development phase. The law was written in response to the proposed bill from a California citizen who had collected enough signatures to place a more restrictive bill on the November 2018 ballot. Legislators worked quickly to develop their alternative bill, which became the CCPA, in exchange for dropping the more restrictive bill originally proposed. It was approved on June 28, 2018, and went into effect on January 1, 2020, but enforcement was delayed until July 1, 2020.

The primary focus of the CCPA is to attempt to apply privacy requirements to the tech industry giants like Google, Facebook, and Apple. These companies are headquartered in California, and this bill is a direct shot at their business model of collecting and selling personal information for directed advertising. There have been direct changes to the Apple iPhone operating system iOS 14 to comply with CCPA, including requiring permission from users for ad tracking and monetization as a result. However, the CCPA requirements will have ramifications across all verticals, including equipment leasing and finance organizations.

The CCPA differs from most security and privacy legislation by stating specific business size requirements for covered organizations. The CCPA does not impact small businesses or non-profit organizations that may still be collecting and selling personal information. The CCPA impacts organizations that do not have headquarters in California but are meeting the other size requirements. The law states that it specifically applies to organizations that:

1. A legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners
2. Has annual gross revenues above twenty-five million dollars. ($25,000,000)
3. Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices
4. Derives 50 percent or more of its annual revenues from selling consumers' personal information
5. Does business in the State of California

The CCPA contains much broader definitions of personal information than other privacy laws. It overlaps with BIPA in that it covers the protection of biometric information but adds additional data elements, including DNA and exercise data, to the definition of personal information. Even a broad definition covers the way a person looks, sounds, smells, and body temperature. The CCPA also defines vague data references such as "tendencies" and "inferences" made by analyzing personal information and purchase history as personal information. This makes compliance more difficult for those organizations affected as these may not be concrete data elements and may be generated by automated algorithms.

A full listing of personal information as defined by the CCPA:

1. Internet Protocol (IP) address. This is the unique address provided to your device that allows it to communicate across the internet. It will usually change as addresses are usually dynamically allocated but can be used in the short term to identify all device activity.

2. Any records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

3. Biometric information is defined as an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, the imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

4. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet Web site, application, or advertisement.

5. Geolocation data. The precise location is derived from GPS coordinates or other telemetry data.

6. Audio, electronic, visual, thermal, olfactory, or similar information.

7. Non-public professional or employment-related information.

8. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act.

9. Inferences are drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

The impact of this broad definition of personal information cannot be underestimated. Internet of Things (IoT) devices like Amazon's Alexa and Google Assistant are creating personal information covered by the CCPA. Web server logs could also create personal information covered by the CCPA as they contain IP addresses and specific web browsing history. The CCPA definition of personal data covers even opinions about personal traits created by organizations. Organizations operating under CCPA must spend the time and money to build an accurate inventory of the data elements they are producing as well as capturing to ensure compliance.

The privacy protections defined within the CCPA are described as a consumer privacy bill of rights with justification based on current technology trends and examples of inappropriate use of personal information. The introduction to the law provides several examples of the personal information collected by businesses about consumers, including how many children they have, how fast they drive, their personality, and their sleep habits. The law also references the March 2018 data breach by Cambridge Analytica, where Facebook data was collected and misused to influence user behavior. These facts are then used to justify and define the five consumer privacy rights in the CCPA.

The five privacy rights as defined by the CCPA are:

1. "The right of Californians to know what personal information is being collected about them." Businesses need to be transparent about what data they are collecting and notify the consumer. This is like the requirement in BIPA but broader given the wide definition of personal data in CCPA.

2. "The right of Californians to know whether their personal information is sold or disclosed and to whom." This requires businesses to be transparent with consumers about business operations involving the transfer of or sale of personal information. Consumers must be kept informed whenever personal information changes hands.
3. "The right of Californians to say no to the sale of personal information." This is a requirement that may have major impacts on organizations that have based their business models on advertising revenue. Consumers must have the ability to opt-out of the sale of any personal information to a third party.
4. "The right of Californians to access their personal information." Businesses must be able to provide copies of all information collected on a consumer, including all of those defined as personal information. The business also needs to allow for the deletion of this data upon request of the consumer unless there are extraordinary conditions that require data retention.
5. "The right of Californians to equal service and price, even if they exercise their privacy rights." This requirement could also have major impacts on organizations if a consumer has opted out of the sale of their personal information. The business cannot deny access to the service or artificially increase the price of service just because the consumer has opted out of the sale of their data. However, they can adjust the service price based on the offset of the revenue that would have been collected through the sale of personal information.

The Attorney General of California is responsible for enforcing CCPA in the initial version of the law, which is like the enforcement of privacy and security legislation in other states. The potential state penalties that can be assessed for violating CCPA are very large, with $2,500 per violation up to $7,500 per violation for intentional disclosures. The CCPA also includes civil penalties of $100 per violation to $750 violation for intentional disclosures.

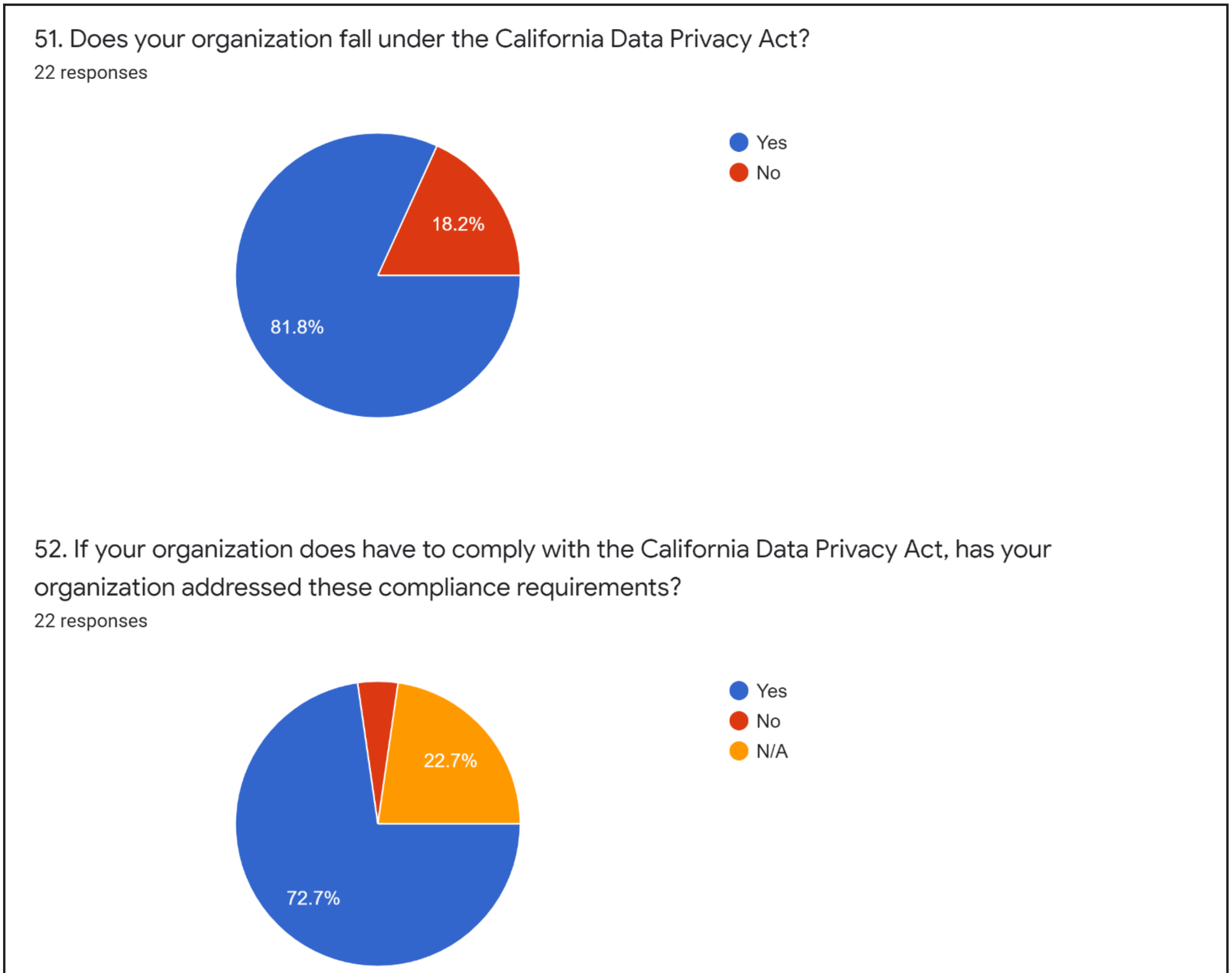
These penalty amounts may seem low compared to the GDPR penalties of €20 million or 4% of annual revenue at first glance. However, the difference is that there is no cap on the penalty amounts under CCPA compared to the caps defined in GDPR. The combined penalty of an unintentional data breach of only 10,000 records would exceed €20 million, while the combined penalty of an intentional breach would take less than 3,000 records under CCPA. No penalties have been assessed at the time of this research, so the actual financial amounts that will be enforced under CCPA are still unknown.

CCPA does include a provision that the civil penalties will only be assessed when a data breach occurs. Individuals cannot be entitled to the $100 - $750 per incident penalties based solely on a complaint. The organization must also be provided 30 days to cure any infraction before a penalty is assessed. This provision provides a limited exception for businesses to prevent abuse and potentially frivolous lawsuits, as seen in Illinois with BIPA.

CCPA does not specify any data breach notification requirements, unlike GDPR, which requires notification in 72 hours. This is because breach notification is already addressed in the California Data Breach Notification Law. This law states that notification must be performed "in the most expedient time possible and without unreasonable delay" but does not define any other timeframe requirements. This means that organizations must thoroughly document the reasons they have not yet notified customers during forensic investigations or legal delays. It does not mean that organizations should wait to notify or hold back information that could impact customers’ privacy or security.

The applicability to the equipment leasing and finance industry is well defined in the CCPA. The law specifies that financial organizations and their information will be regulated by GLBA if there is a conflict. However, only financial information as defined in GLBA is considered outside of the jurisdiction of the CCPA. Personal information used for targeted advertisements would still fall under the CCPA. A financial organization that collects personal information through their mobile app would still have to comply with CCPA, for example. Organizations in the equipment leasing and finance industry must create a strong data classification policy to determine the compliance obligations of both types of data.

The survey conducted as a part of this research confirmed that surveyed ELFA member organizations have confirmed that they must comply with the CCPA. Only one of the organizations that stated it must comply with CCPA has not already addressed the requirements. The breakdown of the responses is shown in the attached charts.



51. Does your organization fall under the California Data Privacy Act?

22 responses

52. If your organization does have to comply with the California Data Privacy Act, has your organization addressed these compliance requirements?

22 responses

Source: ELFF 2020 Cybersecurity Survey

2020 California Proposition 24 Updates to the CCPA

The CCPA was written and passed quickly, which created the need for additional revisions and amendments since 2018. The latest change called Proposition 24 was passed in November 2020, which added some unique provisions not found in other privacy laws. The enforcement of the CCPA was originally the responsibility of the Attorney General of California. Proposition 24 created the California Privacy Protection Agency, which is now taking over enforcement duties. This new agency is an unprecedented step in the enforcement of state privacy laws that could be adopted across the country if successful.

Proposition 24 also made a major change to the penalties defined in the CCPA. Consumers still must be involved in a data breach to file a claim under Proposition 24. However, the 30-day cure period that allowed a business to correct security issues and avoid the financial penalties has been removed. This will allow the consumer to move directly to penalty assessment and increase the number of penalties awarded under the CCPA. The addition of a new dedicated agency with an annual cost of approximately $10 million and something to prove along with the removal of the cure period will drive a dramatic increase in the penalties assessed.

New York Stop Hacks and Improve Electronic Data Security Act (SHIELD)

New York has joined a growing number of states that have expanded existing data breach notification laws into stringent rules for managing information security. The Stop Hacks and Improve Electronic Data Security Act (SHIELD) was passed in July 2019 as a reaction to the increasingly large number of data breach notifications being sent to New York residents. The new law specifies that businesses must create and maintain a formal information security program similar in size and scope to GLBA to protect the personal information of state residents. The law's effective date was March 21, 2020, providing just over six months for businesses to build up their information security programs.

The impact of the SHIELD Act is wide-ranging as New York followed the template laid out by California with the CCPA. The original data breach notification law only applied to New York businesses and residents. The SHIELD Act radically expanded covered entities to include "any person or business which owns or licenses computerized data which includes private information of a New York State resident." This requirement is like the CCPA, which protects the personal information of California residents regardless of the location of the data. The difference is that the CCPA specifies that businesses must have some presence in California to be covered under the law. The New York SHIELD Act does not specify the business's location, which theoretically means that all organizations that store personal information about New York residents are under its jurisdiction.

The SHIELD Act followed the CCPA in redefining personal information that should be protected as well. However, the SHIELD Act does not repeat the vague definitions contained in the CCPA, such as "intent" or "inferences" that were directly targeting the ad-tech industry. The data elements defined as personal information in the SHIELD act are more focused on financial fraud or identity theft. Biometric information is included under the law though not as thoroughly as it was defined in the CCPA.

The definition of personal information as specified by the SHIELD Act is:

"Personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted or is encrypted with an encryption key that has also been accessed or acquired:

- Social Security Number
- Driver's license number or non-driver identification card number
- Account number, credit, or debit card number, in combination with any required security code, access code, password, or other information that would permit access to an individual's financial account
- Account number, credit, or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password
- Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity
- A username or e-mail address in combination with a password or security question and answer that would permit access to an online account."

The structure of the SHIELD Act is very similar to the GLBA Safeguards Rule. Both laws specify that organizations must implement Administrative, Physical, and Technical Safeguards to protect personal information. These same safeguards are also used in The Health Insurance Portability and Accountability Act of 1996 (HIPAA) to protect patient information. The SHEILD Act versions of these safeguards are not as detailed as GLBA or HIPAA and cover the protections at a broader level. However, the SHIELD Act was patterned after these two preceding Federal laws. This is also why organizations covered by either HIPAA or GLBA are considered compliant with the SHEILD Act.

The SHIELD Act contains language that scales compliance to the business's size. A small business is defined as having fewer than 50 employees and less than three million dollars in gross annual revenue or less than five million dollars in total year-end assets. The SHIELD Act does not exempt small businesses but requires them to apply appropriate administrative, physical, and technical safeguards. This requirement might be difficult for small businesses to interpret and apply as "appropriate" safeguards could have multiple definitions. The SHIELD Act does attempt to offer some guidance on the creation of these safeguards.

1. Safeguards should be consistent with the size and complexity of the business.
2. Safeguards should consider the nature and scope of the small business's activities.
3. Safeguards should address the sensitivity of the personal information the small business collects from or about consumers.

The definition of a data breach changed with the passing of the SHIELD Act. The previous New York breach notification law stated that a breach occurred when an unauthorized individual or entity acquired the information. The SHIELD Act changes this definition to include information accessed by an unauthorized individual or entity. This means that an attacker only gains access to an email account to be defined as a data breach where previously they must download the contents of the email account.

The SHIELD Act maintained a provision from older data breach notification laws that seems incompatible with the law's intent. An organization is not obligated to provide notification of a breach if the exposure of personal information was to an authorized individual, which seems appropriate. However, the organization can also avoid notification if there is a reasonable determination that the breach "will not likely result in misuse of such information or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials." Organizations must maintain any documentation about a decision not to notify after a data breach for five years. There is no other definition of "reasonable determination" in the law, so organizations will surely have broad interpretations of this clause by trying to avoid breach notification.

A major difference between the CCPA and the SHIELD Act is that it offers no civil right to action for New York residents involved in a data breach. It does provide for damages based on actual costs or losses incurred for data breach notification violations if it was deemed as "not reckless or knowing." These damages can also include consequential financial losses incurred because of the breach. However, a deemed knowing and reckless violation will face the greater of $5,000 or up to $20 per instance with a cap of $250,000. Organizations can also face penalties for violations of the safeguard requirements of not more than $5,000 per violation but with no cap on the total penalty assessed.

The SHIELD Act is enforced by the New York State Attorney General, which is like other state privacy acts. There have been no penalties assessed under this new law, probably due to the COVID-19 pandemic occurring simultaneously. The law has broad jurisdiction and impactful financial penalties, making every organization take notice. However, the impact on the equipment leasing and finance industry should be minimal due to the GLBA compliance exception noted earlier.

Doing Business in the Age of Compliance Requirements and Privacy Regulation

The privacy and security laws discussed in this paper are just a fraction of those that apply to the equipment leasing and finance industry. The promise of technology was supposed to include increased productivity and greater efficiency. The reality of technology is that productivity and efficiency have improved but are offset somewhat by the increased risk and costs associated with managing that risk. Our information systems' security must now be accepted as a cost of doing business that can no longer be ignored. The financial incentives continue to increase for criminals as more systems are interconnected and play a more valuable role in modern society. The cost of defending organizational information systems will continue to increase and may become a barrier to entry for small businesses.

Organizations that struggle with compliance with multiple laws and regulations have options to help them reduce complexities and costs. The best approach is to target compliance with an information security framework instead of a specific law or regulation. Frameworks are useful as they define a standard set of controls, both technical and administrative, that can be used to define an information security strategy. These controls can then be mapped to all the different laws and regulations that apply to the organization, greatly reducing the amount of time spent on compliance activities. The most popular framework currently is the National Institution of Standards and Technologies Cybersecurity Framework (NIST CSF), which is available for free on their website.

Laws and regulations like those addressed here are ways for society to force the adoption of information security management programs in reaction to the dramatic increase in cyber incidents. These well-meaning intentions continue to have serious impacts on businesses that must invest substantial resources just to show compliance with all the nuances of the various laws. The dirty secret is that basic compliance with privacy and security laws does not equate to secure information systems. However, regulatory compliance can be used as a foundation for building a risk-based security program that will provide a competitive advantage for the organization in the future for those with the foresight to embrace the spirit of the laws.

Conclusion

The increase in regulatory compliance and technical security requirements will not slow the adoption of technology in the Equipment Leasing and Finance sector or business generally. Companies will continue to look for technology solutions that provide productivity improvements or opportunities for competitive advantage. Technology has become ubiquitous in business as well as in our personal lives. The first iPhone was introduced as recently as 2007, starting a wave of smartphone adoption for both personal and business use that we take for granted today. The first mainframes led to personal computers and the internet, leading to dramatic improvements in business efficiency and profitability in the Equipment Leasing and Finance industry.

Technology has had many positive impacts on both business and our personal lives. However, a darker side of our technology addiction has become clear in recent years. The implementation of technology and specifically Internet connectivity has made many systems we use targets for criminal or state-sponsored activity. A twenty-first-century criminal no longer must take the physical risk of robbing a bank when they can use a software flaw in a website to steal funds instead. A foreign government no longer must send in agents to acquire state secrets when they can compromise a cloud-based system where they are stored. Propaganda can spread without consequences through social media to influence the opinions of millions.

Companies in the equipment leasing and finance sector have been facing attacks attempting financial fraud and theft for some time as they were obvious first targets. Modern cybercriminals are looking beyond these short-term financial gains at other types of opportunities. Business disruption and industrial espionage are becoming much more frequent motives for attacks. The information stored and processed by the equipment leasing and finance sector may be more valuable in the long run than a single fraudulent transaction. A nation-state may want to know details of an equipment lease for a defense contractor or interfere with finance by attacking the lender, for example. These new threat models must be considered while organizations build out their information security programs.

Technology adoption in the United States has outpaced many other nations, making it one of the more vulnerable. Almost every aspect of our business operations and personal lives involves technology. Electrical power grids, water processing plants, financial transactions, and even the opinions we share on social media have become targets as a result. State-sponsored actors and large criminal organizations have noticed and migrated their operations online. Small countries that could not compete on the world stage militarily find that the playing field is now level, thanks to the power of cyber-attacks.

There are best practices that organizations can adopt to reduce the risk and impact of these cyber-attacks. These include using the NIST Cybersecurity Framework (CSF) and adopting a formal risk-based information security management program. The adoption of technical controls, including patch management, endpoint detection and response, next-generation firewalls, and email security tools, has become necessary. Multifactor authentication and encryption are included in all cloud-based office productivity platforms and operating systems simplifying their implementation. Strong passwords still play a leading role in protecting information assets, although the definition of "strong" continues to evolve.

Privacy and security compliance are becoming more complex and stringent as the threat landscape evolves. GLBA, HIPAA, CMMC, and PCI just some examples of both federal and commercial regulatory requirements facing organizations in the leasing and finance industry. The European Union has raised the bar for privacy requirements with the passage of GDPR, which has inspired additional privacy legislation in the United Stated States. The recent California Consumer Privacy Act was built on GDPR and added 'how a person smells' and many other attributes to the list of data protected by this law. New York is not far behind California with the passage of the SHIELD act, which can penalize a company outside of New York if data on New York residents was involved in a security incident. Many other states are preparing similar legislation, and they are talks of a national privacy act along the lines of GDPR.

The information security hurdle is raising every day, creating problems for small lenders. Large firms with information security staff and resources to acquire modern security tools should be able to adapt to new threats more easily. A small lender may not have the resources to invest in a security program to protect their information assets adequately. The level of technical, legal, and compliance expertise needed to navigate through information security risk in 2021 continues to increase. These smaller organizations may be left vulnerable and become targets of opportunity for threat actors.

Information security spending could become a barrier to entry in the equipment leasing & finance sector due to rapidly increasing expenses. Start-up companies will need to amass much more capital to meet information security technical and regulatory requirements. This could limit new competitors in the space while also driving consolidation of existing smaller lenders. Data breaches experienced by smaller lenders could also lead to consolidation as the incident's expenses and brand damage could be difficult to overcome.

There have been calls for government intervention in helping defend businesses from cyber-attacks. The legislation that has been passed so far seems to punish the company that experienced the breach regardless of if any negligence was identified or not. Companies will receive very little proactive assistance to prevent breaches before they occur. The regulations seem hypocritical as the federal government has suffered its share of serious data breaches. The uncomfortable truth is that it may not be possible to defend future information systems from state-sponsored actors or well-funded criminal organizations without government assistance. How this would be accomplished without stepping on individual privacy has yet to be determined.

Organizations that adopt a formal information security program that addresses best-practices will still effectively reduce their overall risk and impact of cyber-attacks. Small lenders will need to be creative in finding security resources to secure their information systems. Large lenders will need to continue to improve their defenses as attackers adapt and modify their techniques. The continual battle between new offensive measures and improved defensive tactics will continue with the balance never permanently favoring one side or the other. Information security must recognize these changes and make improvements in people, processes, and technology.

Information security is a team sport that every employee must play to win. Technology decisions are made throughout the organization around acquiring new products and establishing business processes. Information security teams cannot supervise every decision or process in the organization, nor would they possess the expertise necessary. Well-trained and empowered employees will have a much greater effect and encourage participation in the information security program. Companies that face cybersecurity risks as a team will be successful in protecting their information system assets.

Technology still offers great promise for lenders of all sizes. The improvements in communications, efficiency, and competitive advantage are still available to organizations that effectively leverage their technology investments. However, it may be necessary to be more diligent about information technology decisions that can impact information security. It is very difficult to add information security into an existing platform or product as an afterthought. Information security is most effective when engineered directly into the platform or product as it is being built or implemented. The future of information security should be about enabling the organization by implementing technology.

Works Cited

Benway , Kathleen. “FTC Announces Settlement with Mortgage Broker for Publishing Personal Information about Consumers.” *JD Supra*, Alston & Bird, 15 Jan. 2020, **www.jdsupra.com/legalnews/ftc-announces-settlement-with-mortgage-98917/**.

Marini, Alice, et al. *Comparing Privacy Laws: GDPR v. CCPA,* DataGuidance/Future of Privacy Forum, 26 Nov. 2018, **iapp.org/resources/article/comparing-privacy-laws-gdpr-v-ccpa/**.

“The 2020 Cybersecurity Stats You Need to Know.” *Fintech News*, 19 Dec. 2020, **www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/**.

740 ILCS 14/ Biometric Information Privacy Act., Illinois General Assembly, **www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57**.

“AB-375 Privacy: Personal Information: Businesses.” *Bill Text - AB-375 Privacy: Personal Information: Businesses.*, State of California, 29 June 2018, 4:00, **leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375**.

Aerospace & Defense Cyber Security Report | FireEye. FireEye, 6 June 2016, **www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-aerospace.pdf**.

Alper, Andrew K. “Preventing Equipment Fraud.” *Monitordaily*, 2014, **www.monitordaily.com/article-posts/preventing-equipment-fraud/**.

“Art. 33 GDPR – Notification of a Personal Data Breach to the Supervisory Authority.” *General Data Protection Regulation (GDPR)*, Intersoft Consulting, 29 Mar. 2018, **gdpr-info.eu/art-33-gdpr/**.

Asokan, Akshaya, and Ron Ross. “Interpol Busts Massive Nigerian BEC Gang.” *Data Breach Today*, 26 Nov. 2020, **www.databreachtoday.com/interpol-busts-massive-nigerian-bec-gang-a-15466**

“Attackers Finding New Ways to Exploit and Bypass Office 365 Defenses.” *Help Net Security*, 26 Oct. 2020, **www.helpnetsecurity.com/2020/10/26/exploit-and-bypass-office-365-defenses/**.

Belani, Gaurav. “5 Cybersecurity Threats to Be Aware of in 2020: IEEE Computer Society.” *IEEE Computer Society 5 Cybersecurity Threats to Be Aware of in 2020 Comments*, **www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020**.

“Biometric Privacy Litigation: The Next Class Action Battleground.” *Winston & Strawn*, 12 Jan. 2018, **www.winston.com/en/thought-leadership/biometric-privacy-litigation-the-next-class-action-battleground-1.html**.

Brumfield, Cynthia. “New York’s SHIELD Act Could Change Companies’ Security Practices Nationwide.” *CSO Online*, CSO, 23 Mar. 2020, **www.csoonline.com/article/3533455/new-yorks-shield-act-could-change-companies-security-practices-nationwide.html.**

“California Consumer Privacy Act (CCPA).” *State of California - Department of Justice - Office of the Attorney General*, 2 Feb. 2021, **oag.ca.gov/privacy/ccpa**.

Cesaratto, Brian G. “The New York State ‘Stop Hacks and Improve Electronic Data Security Act’ (SHIELD Act) Becomes Effective March 21, 2020: Is Your Organization Ready to Achieve Compliance?” *The National Law Review*, 6 Feb. 2020, **www.natlawreview.com/article/new-york-state-stop-hacks-and-improve-electronic-data-security-act-shield-act**.

Cimpanu, Catalin. “Ransomware Accounted for 41% of All Cyber Insurance Claims in H1 2020.” *ZDNet*, ZDNet, 10 Sept. 2020, **www.zdnet.com/article/ransomware-accounts-to-41-of-all-cyber-insurance-claims/**.

Consult Hyperion. “GDPR: Banks, Breaches and Billion Euro Fines Are Financial Institutions Ready for the 72-Hour Notification Challenge?” *Report - Are Financial Institutions Ready for the 72-Hour Notification Challenge?*, AllClear ID , June 2017.

CoreView. “GDPR Fine Tracker - Updated List of Enforcement Actions.” *CoreView*, 12 Jan. 2021, **www.coreview.com/blog/alpin-gdpr-fines-list/**.

“Cybersecurity Framework.” NIST, 14 Dec. 2020, **www.nist.gov/cyberframework**.

Cybersecurity Maturity Model Certification (CMMC). United States Department of Defense, 31 Jan. 2020, **www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf**.

“Data Breaches.” *Chronology of Data Breaches,* Privacy Rights Clearinghouse, **privacyrights.org/data-breaches**.

De Groot, Juliana. “The History of Data Breaches.” *Digital Guardian*, 1 Dec. 2020, **digitalguardian.com/blog/history-data-breaches#:~:text=Data%20Breaches%20Have%20Become%20Larger%20in%20Number%20and%20Impact&text=In%20 2014%2C%20783%20data%20breaches,1%2C579%20reported%20breaches%20in%202017**.

Deo, Rema. “The Gramm-Leach-Bliley Safeguards Rule: 4 Lessons Learned from Equifax.” *24by7security*, 17 Sept. 2019, **blog.24by7security.com/the-gramm-leach-bliley-safeguards-rule-4-lessons-learned-from-equifax**.

“FTC Announces Settlement for Venmo’s Alleged Violations of the GLBA’s Privacy and Safeguards Rules.” *Privacy & Information Security Law Blog*, Hunton Andrews Kurth LLP, 5 Apr. 2018, **www.huntonprivacyblog.com/2018/03/02/ftc-announces-settlement-for-venmos-alleged-violations-of-the-glbas-privacy-and-safeguards-rules/**.

“Global Surges in Ransomware Attacks.” *Check Point Software,* 9 Oct. 2020, **blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/**.

“Gramm-Leach-Bliley Act.” *Federal Trade Commission*, **www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act**.

Granneman, Joseph, and Dan Nowak. “Current Threat Actor Trends in Information Security.” 7 Nov. 2020.

Greenberg, Pam. *2020 Consumer Data Privacy Legislation*, **www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx**.

Hanel, Alexander. “What Is Ryuk Ransomware? The Complete Breakdown.” *CrowdStrike*, 28 Feb. 2020, **www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/**.

Harding, Elizabeth. “CCPA – Enforcement Is Coming, Ready or Not.” *The National Law Review*, 26 June 2020, **www.natlawreview.com/article/ccpa-enforcement-coming-ready-or-not**.

Hautala, Laura. “Russia Has Allegedly Hit the US with an Unprecedented Malware Attack: Here’s What You Need to Know.” *CNET*, 3 Feb. 2021, **www.cnet.com/news/solarwinds-hack-officially-blamed-on-russia-what-you-need-to-know/**.

Hays, Tom. “Ticketmaster to Pay $10 Million Fine over Hacking Charges.” *Chicagotribune.com*, Chicago Tribune, 30 Dec. 2020, **www.chicagotribune.com/business/ct-biz-ticketmaster-fine-hacking-charges-20201230-rwwhe5kgvzfhdf7elb2ttv4tya-story.html**.

History of Privacy Timeline, University of Michigan, **safecomputing.umich.edu/privacy/history-of-privacy-timeline**.

Holmes, Aaron. “California Just Passed a Major Privacy Law That Will Make It Harder for Facebook and Google to Track People and Gather Data.” Business Insider, *Business Insider*, 4 Nov. 2020, **www.businessinsider.com/prop-24-privacy-california-data-tracking-facebook-google-2020-11**.

"Is the CCPA's Definition of 'Biometric Information' Broader than the Definition Used by Other States?" *JD Supra*, Bryan Cave Leighton Paisner LLP, 13 Apr. 2020, **www.jdsupra.com/legalnews/is-the-ccpa-s-definition-of-biometric-64996/**.

Johnson, Joseph. "U.S. Data Breaches and Exposed Records 2020." *Statista*, 25 Jan. 2021, **www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/**.

Lazzarotti, Joseph J., et al. "New York SHIELD Act FAQs." *The National Law Review*, Jackson Lewis P.C., 11 Mar. 2020, **www.natlawreview.com/article/new-york-shield-act-faqs**.

Mangion, David. "Biggest GDPR Fines of 2019." *Skillcast*, **www.skillcast.com/blog/biggest-gdpr-fines-2019**.

MITRE ATT&CK®, **attack.mitre.org/**.

"Mortgage Broker That Posted Personal Information about Consumers in Response to Negative Yelp Reviews Settles FTC Allegations." *Federal Trade Commission*, 7 Jan. 2020, **www.ftc.gov/news-events/press-releases/2020/01/mortgage-broker-posted-personal-information-about-consumers**.

Nato. "Collective Defence - Article 5." *NATO*, 3 Dec. 2020, **www.nato.int/cps/en/natohq/topics_110496.htm**.

"The New York SHIELD (Stop Hacks and Improve Electronic Data Security) Act." *IT Governance*, **www.itgovernanceusa.com/ny-data-security-act**.

"NY State Senate Bill S5575B." *NY State Senate*, 25 July 2019, **www.nysenate.gov/legislation/bills/2019/s5575**.

Oksanen, Sofi. "Indifference Is a Green Light for Hatred and Violence - The Northern European." *UpNorth*, 10 Sept. 2020, **upnorth.eu/indifference-is-a-green-light-for-hatred-and-violence/**.

Ramos, Gretchen A., and Darren Abernethy. "Additional U.S. States Advance the State Privacy Legislation Trend in 2020." *The National Law Review*, Greenberg Traurig, LLP, 27 Jan. 2020, **www.natlawreview.com/article/additional-us-states-advance-state-privacy-legislation-trend-2020**.

Reuters Staff. "OTP's Bulgarian Unit Fined for Data Breach Affecting over 33,000 Clients." *Reuters*, Thomson Reuters, 28 Aug. 2019, **www.reuters.com/article/us-otp-bank-bulgaria-fine/otps-bulgarian-unit-fined-for-data-breach-affecting-over-33000-clients-idUSKCN1VI22X**.

Rippy, Sarah. *US State Comprehensive Privacy Law Comparison*, 4 Feb. 2021, **iapp.org/resources/article/state-comparison-table/**.

Ryan, Vincent. "Scammers Target ACH Transactions." *CFO*, 11 Apr. 2019, **www.cfo.com/applications/2019/04/scammers-target-ach-transactions/**.

Sanger, David E., and Nicole Perlroth. "Microsoft Takes Down a Risk to the Election, and Finds the U.S. Doing the Same." *The New York Times*, The New York Times, 12 Oct. 2020, **www.nytimes.com/2020/10/12/us/politics/election-hacking-microsoft.html**.

Schouwenberg, Roel. "NotPetya Ushered In a New Era of Malware." *VICE*, **www.vice.com/en/article/7x5vnz/notpetya-ushered-in-a-new-era-of-malware**.

Schwartz, Mathew J., and Ron Ross. "GDPR: $126 Million in Fines and Counting." *Bank Information Security*, 21 Jan. 2020, **www.bankinfosecurity.com/gdpr-126-million-in-fines-counting-a-13630**.

Shields, Ronan. *Apple's Latest Privacy Announcement Could Be More Impactful than CCPA or GDPR*, Adweek, 23 June 2020, **www.adweek.com/programmatic/apples-latest-privacy-announcement-could-be-more-impactful-than-ccpa-or-gdpr/**.

"Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." *The United States Department of Justice*, 19 Oct. 2020, **www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and**.

"State of New York, Bill S5576B." *Open Legislation - SHIELD ACT*, 7 May 2019, **legislation.nysenate.gov/pdf/bills/2019/S5575B**.

"States Continue to Expand Breach Notification Requirements in 2019." *Perkins Coie*, 27 June 2019, **www.perkinscoie.com/en/news-insights/states-continue-to-expand-breach-notification-requirements-in-2019.html**.

Stephens, John. "California Consumer Privacy Act." *American Bar Association*, 14 Feb. 2019, **www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/**.

Stiehl, Jason P., et al. "New Biometric Information Privacy Cases Reveal Breadth of Potential Exposure for Companies." *Lexology*, 5 Mar. 2018, **www.lexology.com/library/detail.aspx?g=80888745-6cd4-4d2f-bdf0-979969911feb**.

"Supervisory Authority (GDPR)." *Thomson Reuters Practical Law*, **uk.practicallaw.thomsonreuters.com/w-014-8205?transitionType=Default&contextData=%28sc.Default%29&firstPage=true**.

"Supplier Payment Fraud: How It Happens And How to Avoid It." *Sharespace.digital,* 5 May 2020, **sharespace.digital/article/supplier-payment-fraud-how-it-happens-and-how-avoid-it**.

"Supply Chain Compromise." *Cybersecurity and Infrastructure Security Agency CISA*, 13 Dec. 2020, **www.cisa.gov/supply-chain-compromise**.

Thomas, Brian. "Hackers Target Defense Contractors in an Effort to Reach the Pentagon." *BitSight*, 13 Mar. 2020, **www.bitsight.com/blog/hackers-target-defense-contractors-in-an-effort-to-reach-the-pentagon**.

Vaughan-Nichols, Steven J. "SolarWinds: The More We Learn, the Worse It Looks." *ZDNet*, ZDNet, 4 Jan. 2021, **www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/**.

Vlamis, Kelsey. "Here's a List of the US Agencies and Companies That Were Reportedly Hacked in the Suspected Russian Cyberattack." *Business Insider*, Business Insider, 19 Dec. 2020, **www.businessinsider.com/list-of-the-agencies-companies-hacked-in-solarwinds-russian-cyberattack-2020-12**.

"What Is GDPR, the EU's New Data Protection Law?" *GDPR.eu*, 13 Feb. 2019, **gdpr.eu/what-is-gdpr/**.

Acknowledgements

We would like to acknowledge the support of the Equipment Leasing & Finance Foundation and Steering Committee Volunteers including, Andrew Cotter, Jeffry Elliott, Julia Gavrilov, Jim Johnson, Jennifer Martin and Tom Ware.

About the Author

Joseph Granneman has more than 20 years of technology experience, primarily focused in health care information technology. He is an active independent author and presenter in the health care information technology and information security fields. He is frequently consulted by the media and interviewed on various health care information technology and security topics. He has been focused on compliance and information security in cloud environments for the past decade with many different implementations in the medical and financial services industries. Granneman is also a past contributor to the J*ournal of Equipment Lease Financing* having authored "The Business Guide to Improving Information Security" in 2018.

Granneman has been active in many standards groups, including the developing the early frameworks for Health Information Exchange as part of the Health Information Security and Privacy Security Working Group for Illinois. He was also a volunteer for Certification Commission for Health Information Technology (CCHIT) Security Working Group, which developed the information security standards for ARRA certification of electronic medical records. He is currently a member of the Metropolitan Chicago Healthcare Council HIE Planning & Technology committee. He also continues to be involved in InfaGard and the Chicago Electronic Crimes Task Force. Granneman has a B.S. in Music Business from Millikin University and an MBA from Northern Illinois University.

The Equipment Leasing & Finance Foundation

WHY GIVE? INVESTING IN THE FUTURE

BENEFITS OF VALUED DONORS

- Early access to industry-leading research and resources
- Recognition among peers in the industry
- Relationship-building with industry thought leaders
- A voice in creating new industry research
- Opportunities to author industry-related studies and articles
- Connect with the next generation workforce through the
- Guest Lecture Program and online Internship Center
- Free digital library to access insightful, in-depth industry resources

YOUR SUPPORT IS VITAL TO THE INDUSTRY

The Foundation is funded entirely through generous donations from corporations and individuals. These donations provide the necessary funding to develop key resources and trend analyses, maintain our grant program, and support the research products published by the Foundation. We value our donors and recognize contributors in print, online, and at a distinguished awards presentation.

Make a lasting impact and donate today at www.leasefoundation.org.

JOIN THE CONVERSATION

EQUIPMENT LEASING & FINANCE
FOUNDATION
Your Eye on the Future

EQUIPMENT LEASING & FINANCE
FOUNDATION
Your Eye on the Future

1625 Eye Street • Suite 850
Washington, DC 20006
www.leasefoundation.org
202-238-3429