EQUIPMENT LEASING & FINANCE FOUNDATION
Your Eye on the Future

CONNECT WITH THE FOUNDATION

JOURNAL OF EQUIPMENT LEASE FINANCING

Articles in the Journal of Equipment Lease Financing are intended to offer responsible, timely, in-depth analysis of market segments, finance sourcing, marketing and sales opportunities, liability management, tax laws regulatory issues, and current research in the field. Controversy is not shunned. If you have something important to say and would like to be published in the industry's most valuable educational journal, call 202.238.3400.

The Equipment Leasing & Finance Foundation
1625 Eye St NW,
Suite 850
Washington, DC 20006
202.238.3400
www.leasefoundation.org

EDITORIAL BOARD

VOLUME 36 • NUMBER 3 • FALL 2018

Inflation, Interest Rates, and Equipment Finance: Anticipating and Adapting to a Changing Economic Environment

By Jeff Jensen, Elizabeth Rust, and Serena Mackool

Over the last decade, the equipment finance industry and the U.S. economy have operated in a climate of low interest rates and low inflation. How will the industry respond in the face of rising interest rates and inflationary pressures? Here are three scenarios, with ideas on how industry leaders might adjust their business operations in response.

After an extended period of decent growth, low inflation, and low interest rates, the economic environment is changing. As of August 2018, unemployment is historically low at 3.9%; job growth remains strong, averaging 185,000 jobs per month for June through August; and economic growth is accelerating, estimated at 4.2% in the second quarter of 2018.

At the same time, some economists worry that the combination of rising aggregate demand, a years-long buildup of "easy money," and rapidly rising deficits could send inflation on a tear. If these worries prove correct, the Federal Reserve may raise interest rates faster than the market currently expects in order to combat inflation. If so, it is unclear whether businesses and consumers are adequately prepared.

This article explains how a world of rising inflation and interest rates may affect the equipment finance industry, including customer demand, portfolio performance, spreads, and the propensity to finance. It explores three distinct scenarios for inflation and interest rates over the next one to three years, describes the likely and potential scenario-specific ramifications, and provides insights into ways industry leaders could consider adjusting their business operations in response.

For a more detailed examination of the topic, please refer to the Equipment Leasing & Finance Foundation's new study developed by Keybridge LLC titled "On the Rise: How Inflationary Pressures and Rising Interest Rates Could Impact the Equipment Finance Industry."

LIKELY SCENARIOS FOR INFLATION AND INTEREST RATES

The potential for near-term inflation is rising. As the current business cycle matures and wage and inflation pressures build, the Fed is likely to push ahead with its plans to normalize interest rates. However, while most economists agree that the current environment of ultralow interest rates and inflation is unlikely to persist, there are multiple scenarios for inflation and interest rate levels that could conceivably develop.

Each scenario is likely to affect the equipment finance industry differently and will consequently require a different firm-level response. These scenarios revolve around (1) the pace at which interest rates and inflation rise and (2) the way in which these two measures move in relation to one other (i.e., whether inflation outpaces nominal interest rates and drives the real interest rate — that is, the nominal interest rate adjusted for inflation — downward, or vice versa).

This point can be illustrated using a matrix that describes four different environments for rising interest rates and inflation (Fig. 1). The matrix's x-axis represents the pace of interest-rate hikes, ranging from little to no acceleration on the left (e.g., 25 to 50 basis points per year) to fast acceleration on the right (e.g., 125+ basis

Editor's note: This article is based on a Foundation research report titled On the Rise: How Inflationary Pressures and Rising Interest Rates Could Impact the Equipment Finance Industry, *published in June 2018. It is available at www.leasefoundation.org.*

Alternatively, the Fed may correctly interpret evidence of a buildup in inflationary pressures but decide to raise interest rates faster than inflation for other reasons, such as a desire to normalize interest rates.

Figure 1. Four Different Environments

points per year). The y-axis represents the pace at which inflation accelerates, ranging from a theoretically slow, gradual increase on the bottom to rapid increases at the top.

Together, the relative speed of interest rate and inflation increases creates four different market environments, each represented by a numbered quadrant in the matrix.

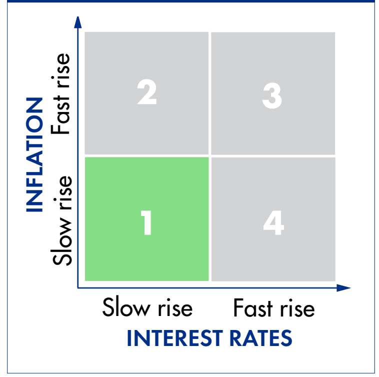
- **Quadrant 1** represents an environment of slow increases in both inflation and interest rates. Although inflation and interest rates may rise, they do so gradually and predictably. This quadrant should feel familiar to the industry, as it corresponds to the state of the U.S. economy over the last three years.
- **Quadrant 2** represents an environment where inflation begins to accelerate rapidly, but nominal interest rates do not rise quickly enough to keep inflation in check. Here, an unexpected surge of inflation — caused by mounting wage growth, an oil price shock, or other factors — either occurs so quickly that it takes the Fed and the market by surprise, or the Fed intentionally adopts a dovish posture and delays action to avoid harming the labor market.
- **Quadrant 3** represents an environment of rapidly mounting inflation combined with fast increases in nominal interest rates. In this environment, inflationary pressures remain strong, but an aggressive response from the Fed and proportionate market reaction results in interest rates rising quickly in an effort to prevent inflation from accelerating further.
- **Quadrant 4** represents an environment in which nominal interest rates rise more rapidly than inflation. This situation often arises due to a mistiming or misstep on the part of the Fed, which anticipates breakout inflation and raises interest rates to preempt the acceleration. Alternatively, the Fed may correctly interpret evidence of a buildup in inflationary pressures but decide to raise interest rates faster than inflation for other reasons, such as a desire to normalize interest rates to allow for more policy flexibility during the next economic downturn.

It remains reasonably likely that a shift from quadrant 1 (where the U.S. economy has stood for the last three years) to another quadrant will occur in the next one to three years. Three potential scenarios are described below.

Scenario 1: Status Quo

The first potential scenario for interest rates and inflation is a continuation of the status quo, with the U.S. economy remaining firmly in quadrant 1 of the matrix (Fig. 2). Although inflation and interest rates may rise, they would do so gradually and predictably.

Figure 2. Scenario 1: Status Quo



This scenario is the likeliest outcome if U.S. gross domestic product reverts to a modest or moderate pace in the next six to 12 months (i.e., 1.5% to 2.5%). If this scenario materializes, wage pressures are likely to remain muted despite a generally healthy labor market, as (1) slower revenue growth would cause businesses to be more cautious about raising wages, and (2) stagnant labor productivity growth would hinder employee efforts to command higher salaries. As a result, the Fed would have little rationale to raise interest rates more than once or twice per year (i.e., 25 to 50 basis points).

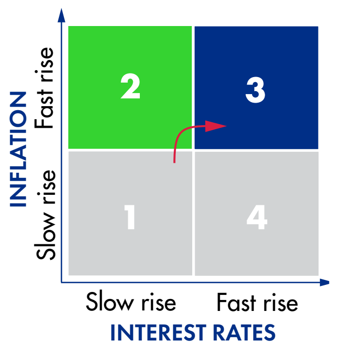
This scenario should feel the most familiar to equipment finance professionals, as the same trends that have characterized inflation and interest rates over the last several years would likely continue, including weak investment demand, favorable lease-versus-buy conditions, and an ambiguous (though likely marginal) effect on spreads.

Scenario 2: Breakout Inflation Prompts Strong Fed Response

Under this second scenario, the U.S. economy would initially slide up into quadrant 2 of the interest rate-inflation matrix, where an acceleration in inflation outpaces interest rates (Fig. 3). However, a rapid response from the Fed and corresponding reaction in the credit markets would quickly pull the economy over into quadrant 3.

In other words, a sudden, unanticipated surge in inflation prompts the Fed to accelerate its rate hike schedule, leading to

Figure 3. Scenario 2: Sudden Surge in Inflation



five or more nominal interest rate increases (125+ basis points) per year. The real interest rate would fall initially, but, as nominal interest rates rise to catch up to rapid inflation increases, it would soon return to more familiar levels.

This scenario would likely arise due to some combination of tighter labor markets, rising energy prices, and rising inflation expectations.

Scenario 2 entails the U.S. economy passing through two separate market environments: first, moving briefly through quadrant 2 as inflation accelerates, and then shifting quickly into quadrant 3 after the Fed responds. Each quadrant would likely present distinct effects on the equipment finance industry.

While in quadrant 2, the industry would be likely to experience rising labor costs, a decline in the real value of loan and lease payments, and higher residual values (which may have implications for leases that have end-of-term purchasing options).

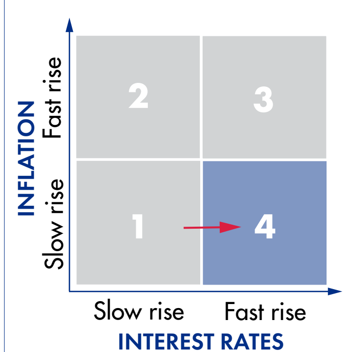
As the economy moves into quadrant 3, the industry should expect to experience increased demand for investment, increased customer demand for longer-term and fixed-rate leases, added complexity in loan and lease valuation and negotiation, and a decline in portfolio values.

Scenario 3: Interest Rates Rise Faster Than Inflation Justifies

Under this third scenario, the U.S. economy moves directly from quadrant 1 to quadrant 4 (Fig. 4). In this scenario, the Fed would move forward with raising interest rates at a moderate or even accelerated pace, despite a weak inflationary environment. Depending on the speed and duration of the rate hikes, the U.S. economy would likely slow and could contract.

Even though inflationary pressures appear to be building, this scenario could nonetheless arise, given that (1) the Fed has committed to a policy of interest rate normalization in the interests of "reloading" for the next recession, even if inflation remains subdued; (2) unwinding the Fed's policy of quantitative easing may exert stronger-than-expected upward pressure on bond yields, which could drive interest rates higher even in the absence of inflation; and (3) the Fed is likely to take a more hawkish approach to monetary policy under the leadership of Jerome Powell than it pursued under Janet Yellen.

Figure 4. Scenario 3: Rising Rates and Weak Inflation



A pronounced rise in interest rates in an environment of relatively muted inflationary pressures poses different implications for the equipment finance industry from the other two scenarios. The effects are likely to include compressed spreads, deteriorating portfolio performance, and falling demand for equipment investment.

WHAT EACH SCENARIO MEANS AND HOW LEASING FIRMS CAN ADAPT

The most successful equipment finance firms are able to adjust their business strategies and operations in anticipation of and response to changing macroeconomic conditions, and the prospect of increasing inflation and/or interest rates is no exception.

The Keybridge–Foundation report offers several concrete actions that individual firms should consider under each scenario, and some of these recommendations are presented in tables 1, 2, and 3. These actions are not intended to be exhaustive, nor are they likely sufficient to ensure profitability if inflation and/or interest rates rise.

As always, industry leaders are best positioned to know how to successfully manage their own businesses. However, these recommendations provide a starting point for industry firms to consider how to adjust their business strategies and should spur additional ideas for discussion in strategic planning sessions.

> The most successful equipment finance firms are able to adjust their business strategies and operations in anticipation of and response to changing macroeconomic conditions.

In addition to reviewing the full report, equipment finance professionals are also encouraged to consult with the Foundation–Keybridge *Applied Economics Handbook*, first published in 2016 and updated in summer 2018. It offers tips for how equipment finance firms can make better business decisions by incorporating economic data into their strategies and tactics.

For a complete list of firm-specific actions to consider

Table 1. Firm-Specific Actions to Consider Under Scenario 1: Status Quo

Anticipated industry effects	Firm-specific actions to consider
Ambiguous effect on spreads	**Consider shifting toward a borrow-long, lend-short mind-set.** Gradually rising interest rates could allow some leasing firms to operate on a longer time horizon and increase profitability by borrowing long and lending short. While a more traditional matched-funds approach is generally associated with lower risk, a borrow-long strategy may be viable for some firms, particularly given that portfolio performance would likely remain strong. This approach may not be appropriate for all lenders, but it is something to consider if the status quo operating environment persists.
Weak investment demand	**Achieving new business volume targets could require a higher tolerance for risk.** Relatively weak demand for equipment investment means that the number of equipment leasing opportunities grows more slowly or potentially stagnates. As a result, equipment lessors should expect to see a continuation of strong industry competition as firms vie for market share. To meet new business volume targets, some firms may need to accept a higher tolerance for risk and/or thinner profit margins. Company forecasts for new business volume growth may need to be revised downward. Senior leadership should discuss the implications on firm operations in quarterly and annual planning discussions.

Table 2. Firm-Specific Actions to Consider Under Scenario 2: Breakout Inflation Prompts Strong Fed Response

Anticipated industry effects	Firm-specific actions to consider
Decline in real value of loan and lease repayments	**Include inflation hedges in loan and lease terms.** Declines in the net present value of a lease or loan due to rising inflation will be exacerbated for deals with fixed rates and long terms. Leasing firms should consider pursuing variable rate agreements or including excise payment provisions to offset the risk of higher-than-expected inflation. Firms may also hedge against inflation risk by adopting shorter terms.
Increased complexity in loan/lease valuation and negotiation	**Incorporate a rate lock fee or related provision to offset risk of interest rate increases during negotiations.** Every capital investment that a business undertakes involves making explicit or implicit assumptions about the level of inflation and interest rates that will prevail over the investment's life. In a rapidly rising interest rate environment, interest rates may rise substantially during the lock period (e.g., 90 days). To protect against this increased risk, leasing firms should consider charging a fee for the rate lock, shortening the rate-lock period, indexing the offered rate to LIBOR, or requiring a higher margin on rate-locked transactions.

Table 3. Firm-Specific Actions to Consider Under Scenario 3: Aggressive Fed Action While Inflation Lags

Anticipated industry effects	Firm-specific actions to consider
Compressed spreads	**A borrow-long, lend-short strategy could increase profitability, but timing is critical.** Some leasing firms could gain a competitive edge by borrowing long and lending short, as short-term interest rates will likely rise faster than long-term rates. However, such a strategy would carry more risk, as an overly aggressive Fed could trigger an economic downturn that would presumably lead to a rapid reduction in the federal funds rate once it becomes apparent that the Fed acted inappropriately. As such, the success of a borrow-long strategy will depend on a lessor's ability to time interest-rate movements correctly.
Deteriorating portfolio performance	**Prepare to tighten lending standards as delinquencies and defaults rise.** Interest rates rising faster than economic conditions warrant will result in many firms struggling to make their loan and lease payments. Lenders and lessors should closely monitor their delinquency and default rates, particularly for more recent deals that have higher interest rates. Firms should consider imposing more stringent loan and lease approval requirements to avoid being overextended in the event of an economic downturn.
Falling demand for investment	**Lower expectations for new business volume growth.** If the Fed raises rates too quickly, it will likely deter capital expenditures, particularly among small businesses. Equipment lessors and lenders should prepare themselves for the possibility that investment demand could slump suddenly, despite relatively strong growth in recent quarters. If this scenario appears to be unfolding, firms should hold more frequent strategic planning meetings, closely monitor internal performance metrics, and consider reducing their risk tolerance (at least temporarily) to avoid becoming overextended in the event of a recession.

under each scenario, read the full report.

CONCLUSION

Every capital investment that a business undertakes involves making explicit or implicit assumptions about the level of inflation and interest rates that will prevail over the investment's life. If these assumptions turn out to be wrong, certain types of investments could be at risk and business performance could suffer. As such, understanding the key drivers of inflation and interest rates and how they affect the economy is a critical part of making sound business decisions.

Over the last decade, the equipment finance industry and the U.S. economy have been operating in a low-interest-rate and low-inflation setting. Although this environment has contributed to increased competition within the industry, it has also provided a relatively stable climate for investment in equipment and software. Equipment finance firms have become accustomed to this low-rate environment, and many may be ill-prepared for the possibility of a more rapid rise in inflation and interest rates in the near future.

However, change is in the air, and uncertainty abounds. The industry is sure to face new challenges and opportunities in the years ahead, and a key factor to watch will be how it responds in the face of rising interest rates and inflationary pressures. The new report produced by Keybridge and the Foundation is designed to help industry leaders understand the risks and opportunities presented by increasing inflationary pressures and rising interest rates.

Jeff Jensen

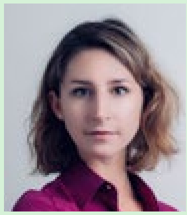
jjensen@keybridgedc.com

Jeff Jensen is a senior director at Keybridge Research LLC in Washington, DC. He has experience in energy policy, flood insurance markets, Medicare fraud, equipment investment, credit card markets, and federal regulation. Before joining Keybridge, Mr. Jensen spent four years as a senior analyst at the U.S. Government Accountability Office, where he focused on homeland security issues and analyzed federal programs on aviation and mass transit security, including the Transportation Security Agency's Secure Flight, CAPPS I, and behavior detection programs. He also analyzed U.S. government efforts to ensure the safety of imported food, increase preparedness for domestic outbreaks of avian influenza, and improve the environmental footprint of the U.S. Postal Service. Mr. Jensen holds a bachelor's degree in economics from Carleton College in Northfield, Minnesota, and master's degrees in public policy and environmental management from Duke University, Durham, North Carolina.

Elizabeth Rust

erust@keybridgedc.com

Elizabeth Rust is an economist at Keybridge Research, where she focuses on macroeconomic analysis and forecasting, economic policy analysis, and economic modeling. She holds a master's degree in international economics and European studies from Johns Hopkins University's School of Advanced International Studies (SAIS) in Washington, DC, and a bachelor's degree, magna cum laude, from Cornell University, Ithaca, New York.



Serena Mackool

smackool@keybridgedc.com

Serena Mackool is a senior analyst at Keybridge Research, focusing on macroeconomic and public policy analysis. She holds a master's degree in international economics and political economy from Johns Hopkins University's SAIS, and a bachelor's degree, summa cum laude, from Columbia University in New York City.

The Business Guide to Improving Information Security

By Joseph Granneman

The continuing increase in large-scale cybersecurity breaches has businesses searching for solutions to reduce their risk. Despite an explosion of new information security products and services, no single tool can reduce risk. Equipment financing companies must build a formal information security framework, complete with policies and procedures.

2018 has seen the continuing trend of cybersecurity incidents and large-scale data breaches across every industry. Companies continue to utilize technology to gain efficiency and productivity, only to find that these same tools can be used against them.

Online systems that store or process any type of financial data become targets of the modern-day criminal. Intellectual property or trade secrets become the target of a new type of industrial espionage performed using technology. Companies that do not even believe they have anything of interest to criminals suddenly find all their computer systems crippled and held for ransom.

The truth is that all businesses are so hyperconnected through technology that there is no business that is truly not at risk of cyberattack. The very existence of the technology creates a potential opportunity for exploitation by an adversary.

There are common threads among most of the successful cyberattacks and data breaches that have been reported. These common threads involve basic failures in understanding the risks involved with the use of technology. Basic controls such as strong passwords, multifactor authentication, and vulnerability management programs would have prevented many of these cyberattacks.

The problem is that many companies lack a formalized program with the expertise necessary to understand and mitigate these risks. The employee making a risk-based cybersecurity decision for the business is too often unware of the potential risks. The rationale is that this decisionmaker does not know how to breach the security of the system, so why would anyone else? This lack of mature risk management is one of the main reasons that businesses continue to make the same mistakes in cybersecurity.

Business is about profiting from risk. Leasing and financing businesses have their industry- specific risks that are professionally managed by knowledgeable staff. A business that used staff untrained in these types of risks would eventually fail due to a lack of understanding.

Managing the cybersecurity risk of the business with untrained staff will deliver the same outcomes. Businesses that can apply their existing risk-management experience to cybersecurity can successfully avoid becoming yet another data-breach headline.

There is no silver bullet to managing cybersecurity. Contrary to popular belief, there is no singular product like an operating system, firewall, or specific antivirus version that can reduce cybersecurity risk. To have any impact on cybersecurity risk, these tools must be orchestrated with the appropriate policies and procedures. That is why this article contains a framework for building a formal risk-based information management program instead of offering specific product or technical recommendations.

SECURITY AS A BUSINESS IMPERATIVE

Businesses that successfully implement a formal information security risk-management

TERMS USED IN THIS ARTICLE

GDPR – The European Union's General Data Protection Regulation, effective May 2018.

GLBA – The Gramm-Leach-Bliley Act, also known as the Financial Modernization Act of 1999. Congress passed it to control the ways that financial institutions deal with the private information of individuals.

HIPAA – The Health Information Portability and Accountability Act of 1996. It defines the privacy and security requirements for healthcare providers and payers to protect patient information.

Lean – A formalized approach to reducing waste in manufacturing and business processes to improve efficiency.

Network Drawing – A technical document that shows both the physical and logical locations of network electronics. It includes the communications flows that occur between different nodes on the network.

NIST – The National Institute of Standards and Technology, a U.S. government agency. It defines information security standards and controls that can be used by any organization.

PCI – Or PCI DSS, the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data.

PII – Personally Identifiable Information, which is defined as a minimum of name, address, and account number. This information is the basis for all privacy regulation and may include other specific information elements, depending on the scope of the legislation.

Six Sigma – A formalized approach to eliminating defects through business process optimization.

SOX – The Sarbanes-Oxley Act, enacted in 2002. It established auditing and financial regulations for public companies. The intent was to protect shareholders, employees, and the public from accounting errors and fraudulent financial practices. The Securities and Exchange Commission enforces SOX.

program recognize that cybersecurity must be a business priority. This means that information security risk has been interwoven into every technology initiative.

It is important for organizations to realize that they must build security processes into technology solutions early in the adoption phase. Security controls that are applied after a system or process is already in production are not nearly as effective.

Businesses looking for motivation to build a formal information security program need only to look at the increase in regulatory and commercial penalties for data breaches. Regulations such as HIPAA, GLBA, SOX, and GDPR (see sidebar) are increasing financial penalties and civil liabilities. Commercial requirements for simply accepting a credit card are enforced through PCI (see sidebar), which specifies its own penalties.

Other businesses are awakening to the potential risks involved with third-party data hosting as well. Companies that host any type of personally identifiable information (PII, see sidebar) are now being thoroughly scrutinized through due-diligence processes and contractual obligations.

It is important to note that these regulations and requirements do not apply only to technology companies. Leasing and finance companies are storing, processing, and transmitting this type of information as a part of normal business operations, using technology while not being a technology company.

The Cost of Major Breaches

Motivation to build a formal information security management program can also come from the potential impacts of a data breach. History has shown that the impacts vary widely, depending on the industry and the size of the breach. Target was forced to pay $18.5 million in damages and suffered a temporary reduction in stock price for its 2013 credit card breach. Small businesses may not be able to absorb the expenses associated with a major breach, including managing brand damage that in turn results in loss of revenue and potential insolvency.

Examples of negative business impacts are easy to find and well documented in the news. There are also less-well-known business opportunities to be found in building an information security program. Companies that develop software or services will find that they can use the discipline of information security to increase the quality of their offerings. Information security programs can be used to gain competitive advantage over other companies in the same space.

Information security can also be used to increase efficiencies and reduce costs. Processes and procedures need to be reviewed or created to build a formal information security program. These business process reviews can be integrated with Lean or Six Sigma optimizations (see sidebar) to increase operational efficiency while improving security-risk posture.

Information security programs thrive on standardization of processes and procedures, rendering them a perfect match for process optimization projects.

BUILDING A FORMAL RISK-BASED INFORMATION SECURITY PROGRAM

First Step: The Leader

The first step in building an information security program is to recruit a leader with security expertise to direct it. This is a key requirement for helping the company understand its true cybersecurity risk profile. This position is usually titled "chief information security officer" (CISO), and he or she becomes a member of the executive team.

This position needs to report at the same level as other executive officers of the company and should not report to the CIO or CFO. The CISO is a type of audit function that needs to have segregation of duties from IT operations to be effective. The driving motivation for the CISO should not be based solely on cost, which can happen if the position reports to a CFO. In other words, to build an independent, value-based information security program, the CISO should report to the CEO and the board of the company.

The next step is to develop a funding strategy for the information security program. The CISO cannot be effective without the additional staff and tools to build the program. There is no predefined rule for the amount of funding that will be required. Financial institutions have been known to spend 15% of their IT budgets on information security, while healthcare institutions lag at around 3%.

The amount of funding depends on the industry (industry vertical), size of the organization, and the level of technical debt that has been incurred. Technical debt refers to the number of outdated or unsupported systems that must be addressed, and it dramatically affects required funding levels.

It is important to consider that spending will increase moderately over the life of the security program, as shown in Figure 1. Determining a funding strategy early on will help to define the options available during the planning phase.

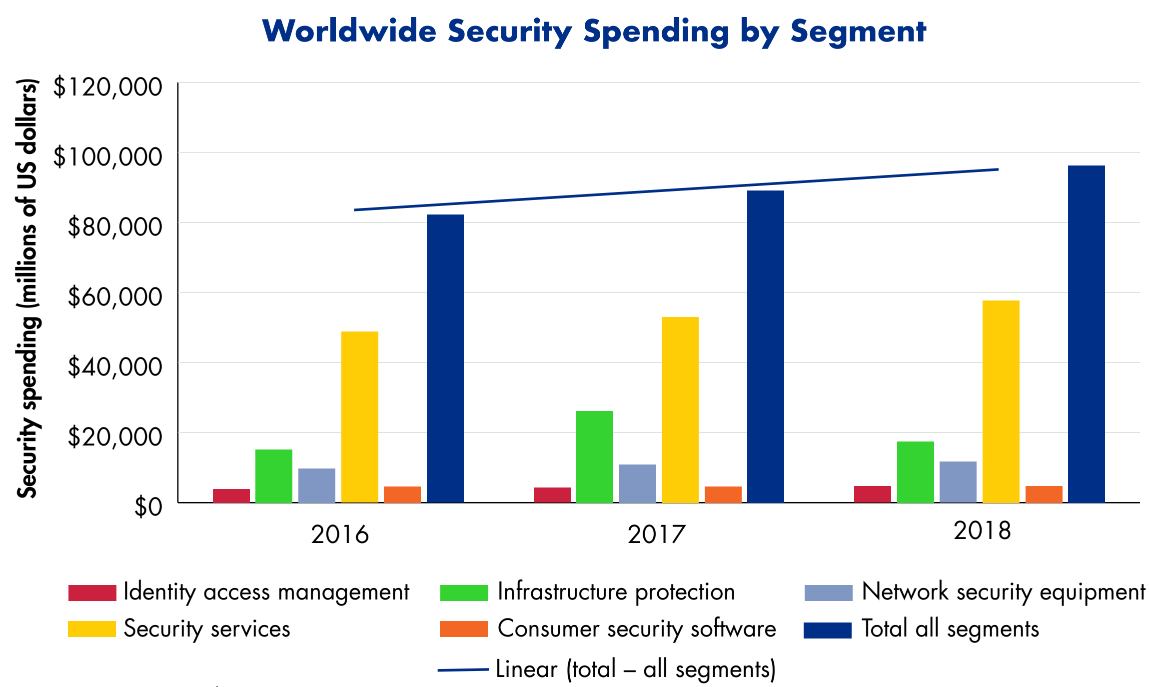
The CISO cannot personally lead all the process changes required to implement a formal information security program. Progress ultimately depends on the organization's support of the information security program. This is best accomplished through creation of an information security governance committee. This formal group is made up of representatives from different departments within the organization.

This committee provides the platform for the CISO to present strategies and opportunities for changing organizational processes. Committee representatives can discuss, approve, or modify the proposals before implementation and provide feedback from the business unit perspective. The information security governance committee will own the security strategy decisions, which helps prevent the perception that the CISO is making decisions from a silo.

The CISO should chair the information security governance committee, which should report to a board-level audit committee. Accountability at the board

> The information security governance committee will own the security strategy decisions, which helps prevent the perception that the CISO is making decisions from a silo.

Figure 1. Worldwide Security Spending Trends



Source: Gartner, December 2017.

The charter should keep the committee focused on high-level initiatives and out of the technical details. Subcommittees or project workgroups can meet more frequently and address these technical issues.

level is crucial to the success of the program.

The committee needs a formal charter that defines both the accountability and the authority to act on information security related issues. The charter should include the ability to identify risk, define strategies and priorities, and assign organizational ownership to security initiatives. The charter should keep the committee focused on high-level initiatives and out of the technical details. Subcommittees or project workgroups can meet more frequently and address these technical issues.

Once this committee is in place, the information security program should develop specific goals. Regulatory compliance, despite its often negative connotations, can be a good starting point for any business to begin building a formal security program. Information security regulations define the base required capabilities of the organization's information security program and can be used to identify quick wins in reducing compliance risk.

Increasing Penalties

Penalties continue to increase for noncompliance with information security regulations. When credit cards are breached, the payment card industry (PCI, see sidebar) can fine a company between \$5,000 and \$10,000 per month, going back to the initial date of noncompliance.

HIPAA can fine up to \$1.5 million for a breach of identifiable patient information. HIPAA has also been used to bring civil lawsuits stating that patient privacy is a basic expectation of patient care.

The European Union's new General Data Protection Regulation (GDPR), effective in May 2018, has penalties of €20 million, or 4% of global revenue, whichever is higher for breaching the personal information of EU citizens. These penalties can provide the necessary motivation to build an information security program and help justify the required investment.

Leasing and financing companies could be affected by these regulations and not even be aware of the requirements. An organization's marketing and leasing equipment to EU citizens could be covered by the GDPR, for example.

Organizations that are processing payments through credit cards, either online or through the use of card readers, fall under PCI requirements. Organizations that lease equipment to healthcare organizations may find themselves required to sign a business associate agreement that binds the organization to HIPAA compliance.

Any organization in the United States that allows personally identifiable information to be breached is subject to Federal Trade Commission penalties and the breach notification requirements enacted by all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. Information security compliance is now just a cost of doing business in the 21st century.

Compliance can become complex when dealing with multiple requirements — for example, in the case of an organization that must comply with GDPR, PCI, and HIPAA. Information security frameworks can be used to build out general security requirements that can be mapped to other compliance regulations. This allows the company to build a single set of policies and technical security controls, instead of generating unique controls for each compliance requirement, thereby reducing expense and complexity.

In short, information security frameworks will help to reduce overall security risk, whereas compliance requirements tend to be more focused on providing documentation.

The Role of NIST

There are many security frameworks available, but the most commonly used ones were developed by the National Institute of Standards and Technology and are available for free. NIST Special Publication 800–53 is one of the older frameworks but is still as current as when it was first published.

This document was used as a template for compliance regulations including HIPAA and GLBA. However, it contains a large set of controls that may be overwhelming for smaller businesses. NIST SP 800–171 contains a subset of the controls defined in SP 800–53; thus, it may be more appropriate for these organizations.

The NIST SP 800–171 framework has become more popular lately due to becoming a requirement for U.S. government manufacturing subcontractors. NIST has recently created other resources that may be easier to navigate, including the NIST Cybersecurity Framework and NISTIR 7261. The latter focuses specifically on small business information security.

ASSESS AND ANALYZE CURRENT ORGANIZATIONAL INFORMATION SECURITY POSTURE

Once the information security leadership, governance structure, and security framework have been created, the organization can assess its security posture. This begins by creating an inventory of information assets ranked by their business value. Applications that house key business processes or confidential information should be ranked higher.

A best practice is to classify the types of data used by the organization into three or four categories based on this system ranking. These classifications could be "Confidential," "Financial," "Ephemeral," and "Public," for example.

Security controls can now be mapped from the security frameworks to each one of these categories. These controls will include items such as authentication requirements, encryption requirements, authorization protocols, and audit requirements for each data classification type.

Technical Documentation

The inventory of information assets should also include technical documentation, such as system configurations and network drawings for both internal and internet-facing systems. Network drawings (see sidebar) should include traffic flows to record how confidential data is transmitted across the environment. System configurations should include age of the operating system, security patching schedule, and antivirus capabilities.

Network infrastructure, cloud-based applications, mobile devices, and removable media must also be included in this inventory. Although this amount of data collection may seem rudimentary, many organizations will have trouble finding basic network documentation. However, this information is key to building an accurate risk model. It is impossible to defend systems that are unknown to the organization.

With the inventory complete, a thorough risk analysis of the core technologies and business operations of the organization can begin. The technical assessments include implementing regular commercial vulnerability scanning to gain a baseline understanding of the environment.

The value of the assets, as assigned during the inventory phase, can be overlaid with the results from the vulnerability assessment to determine the high-risk assets. A third-party penetration test can then be used to validate these findings and discover any other potential security flaws in the internal, external (internet-facing), and wireless network-based systems.

Policies and Procedures

Policies and procedures require creation or review to conform to the security framework selected earlier in the program. Security policies play a key role in any information security program: they define the requirements and standards to manage overall risk.

Security policies will cover technical requirements such as encryption standards and password complexity requirements. They also define the processes for provisioning user accounts and assigning the minimum necessary permissions. These policies are the basic building blocks of the information security program.

Documentation of critical business processes must be created or reviewed to understand the technical interdependencies of current applications. Many organizations mistakenly believe that the priority of each application to business operations is fully understood. Priorities are often overstated for applications that may not have direct revenue impacts, while some critical applications can go unnoticed because staff takes them for granted.

Mapping out these processes using a Lean or Six Sigma approach will help pinpoint these critical applications as well as opportunities for process improvement. The results of this process mapping will also provide the necessary information to develop a business impact analysis for building a disaster recovery plan.

Supply chain management is a specific business process that needs to be reviewed for potential information security risks. The U.S. government will not use equipment or components from specific companies in certain parts of the world. It has become common for state intelligence agencies to intercept shipments of computers, phones, or networking equipment and install backdoors or hidden accounts to perform surveillance on the intended customer. Vendors for any critical infrastructure must be reviewed in light of the origin of their equipment and any potential government ownership. Vendors can then be selected based on the risk tolerance of the organization.

> The inventory of information assets should also include technical documentation, such as system configurations and network drawings for both internal and internet-facing systems.

The Security Culture

In addition, the chief information security officer must gauge the information security culture of the organization. This includes reviewing the IT staff security skill set and measuring the general security awareness of all employees. Information security is most effective when it is interwoven into standard business and IT processes.

Subjective by nature, the measurement of these cultural aspects of information security can be challenging. However, driving change through a culture shift will yield the most benefits.

Using all of the collected information, the CISO can begin to design a formal strategy for information security initiatives. The strategy should span no more than three years.

This is especially true for IT staff, who are usually responsible for implementing and maintaining company infrastructure and applications.

Culture can be measured using various tools and techniques. Surveys and questionnaires can provide the security program with interesting insights into the organizational culture and technical knowledge. Valuable information can emerge from questions about difficulty with password changes or the risks involved with using mobile devices.

IT staff members can be interviewed regarding their strategy for implementing a DMZ (internet-facing servers) or their current process for handling removable media like USB drives. Training programs can then target problem areas in which technical knowledge is found lacking or where the resistance to change may be the strongest.

Risk Tolerance

By way of comparison, executive-level surveys should target larger cultural issues that affect overall information security strategy. The security program must incorporate an understanding of the organization's risk tolerance level, for example. A security program is a function of organizational risk management and must be compatible with the organizational business model.

Information security risk tolerance will be very different for a company hosting websites with marketing material, when compared to a bank website with online transactions. These organizations share certain risks associated with having a website on the internet. However, the risks for the bank website are considerably higher than those for the marketing firm.

The organization may decide to join an information sharing and analysis center (ISAC) to share threat information and gain a better understanding of the risks in its specific vertical. ISACs are industry-specific groups whose many company members share cyberthreat information and best practices. Moreover, these groups share technical details about the viruses their members have encountered and disseminate warnings about scams targeting their specific vertical.

The Financial Services Information Sharing and Analysis Center (https://www.fsisac.com) may best fit the needs of the equipment leasing and financing industry.

BUILD AND IMPLEMENT THE PLAN

Using all of the collected information, the CISO can begin to design a formal strategy for information security initiatives. The strategy should span no more than three years, given that security threats change too rapidly for longer plans to be valid.

Budgets and resource commitments essential to the desired results must be part of the strategy, based on the initial funding decisions. Staffing requirements for both internal and outsourced positions are also vital to the strategy. Threat intelligence gained from internal assessments and through ISAC membership should help shape the strategy and identify areas of risk.

The CISO should present the complete formal strategy to the information security governance committee. He or she can focus on opportunities for reducing expenses or opportunities for additional revenue or competitive advantage, based on security initiatives.

The risks identified in the assessment need to be presented to the committee along with multiple options for remediation. Potential quick wins should be identified to bolster short-term support for the adoption of the long-term plan.

To build organizational ownership of the security strategy, the CISO presents only the options with recommended actions. However, the CISO does need to take organizational risk tolerance into account while developing these options.

The Implementation Team

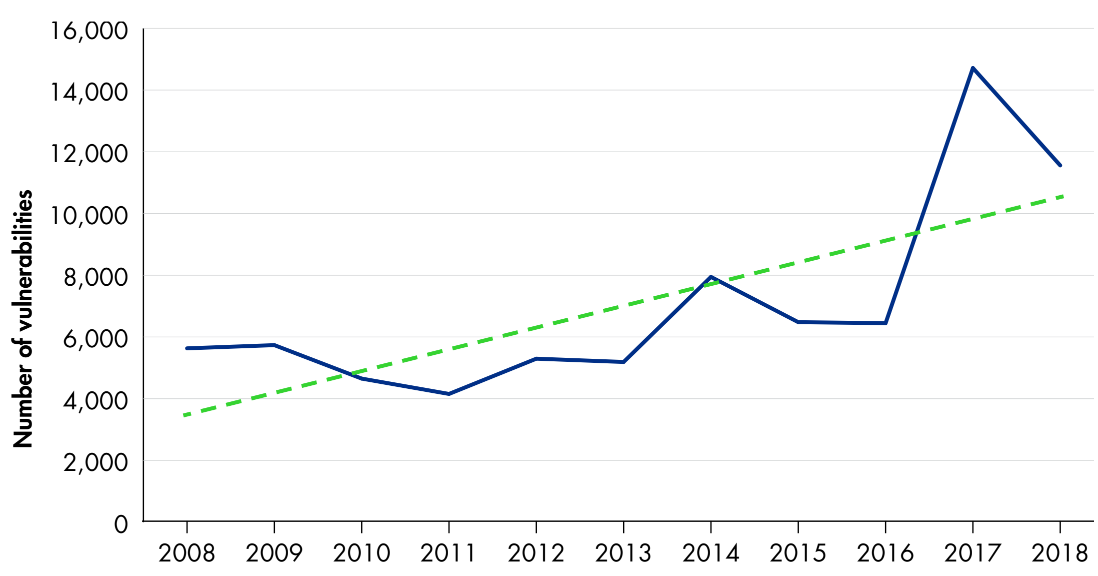
Once the information security governance committee has adopted the formal security strategy, the next task is to build the team that will implement it. Many organizations skip over this step, mistakenly believing that simply hiring a CISO is enough to manage information security risk. This is equivalent to hiring a football coach without the team and expecting to win championships. Information security is also a team effort, involving people with different skill sets to effectively manage risk, just as a football team requires players at different positions to play the game.

The essential information security roles to be filled are similar in all organizations. Roles can be combined based on the size and complexity of the information technology environment. They can also be assigned outside of the information security department and fulfilled by existing IT staff. Table 1 presents

Table 1. Common Information Security Roles and Activities

Role	Activity
Identity management	Adding, creating, and removing access to employees based on job roles
Asset management	Maintaining a list of all equipment and locations of high-priority organizational data
Disaster recovery	Maintaining the capability to restore the technical environment after a disaster
Compliance	Auditing current processes and documentation to maintain compliance with required regulations such as PCI, HIPAA, GDPR, and SOX
Configuration management	Maintaining and monitoring the secure configuration of workstations, servers, and other devices
Monitoring and alerting	Reviewing system activity for anything suspicious or out of the ordinary and escalating to Incident Response when appropriate
Vulnerability management	Monitoring and regularly applying software security patches to all systems
Incident response	Responding to security events, preventing damage and preserving evidence
Penetration testing	Assessing technical systems using tools and techniques commonly used by attackers

Figure 2. Software Vulnerabilities Reported by Year



Source: "CVE Details by Date," MITRE Corp.

examples of common information security roles and their typical activities.

Vulnerability Management

Vulnerability management is one activity that can generate a quick win in implementing the security strategy. Vulnerabilities are software defects or misconfigured systems that allow an attacker to bypass security controls. The number of reported vulnerabilities continues to increase each year, as shown in Figure 2, but the risk can be mitigated by applying software patches and changing default passwords.

The WannaCry ransomware outbreak of 2017 was caused by those organizations failing to apply a security patch released by Microsoft two months before the attack started. The Mirai botnet that disrupted internet access on the East Coast of the United States in October 2016 was powered by systems using default credentials. The botnet continually scanned the internet for devices that would allow a login using a username of "admin" and password of "admin" to propagate the attack.

Another quick win can occur by implementing a phishing awareness program. According to the 2018 Verizon Data Breach Investigations Report, phishing was used in 98% of the social attacks and 93% of the reported security breaches. Email was used 96% of the time as the attack vector of choice in these incidents.

Criminals use phishing because it is the easiest way to bypass firewalls and other technical controls and gain access to credentials or to spread ransomware. Organizations can use services to phish their own users or to train them to identify suspect messages. A well-managed internal phishing program can dramatically reduce the risk

Criminals use phishing because it is the easiest way to bypass firewalls and other technical controls and gain access to credentials or to spread ransomware.

of falling victim to a real phishing attack.

The solution is to build a formal information security program based on a standardized framework to identify assets, develop policies, assess vulnerabilities, and manage overall risk.

Continual Measurement

It is important to continually measure the progress of the information security strategy and program metrics. The CISO should issue status reports on the major initiatives and regulatory compliance to the governance committee as well as give current program statistics. Security incidents should be one of the key metrics analyzed and reported, because the program's direction may need to change to mitigate a related vulnerability.

Progress in remediating the risks identified during the assessments should be reported as well. The cost of these specific remediations should be tracked and reported to verify that the expenses do not exceed the risks being addressed.

SUMMARY

The continuing increase in cybersecurity incidents has businesses searching for solutions to reduce their risk. There has been an explosion in information security products and services marketed to address this growing need. However, no simple solution or single product can actually reduce organizational security.

The solution is to build a formal information security program based on a standardized framework to identify assets, develop policies, assess vulnerabilities, and manage overall risk. The current business technology environment is too complex for ad hoc security solutions. Organizations that ignore security risk management, assuming that their antivirus or firewall alone will save them, will become the data-breach headlines of the future.

References

Abrams, Rachel, "Target to Pay $18.5 Million to 47 States in Security Breach Settlement," New York Times, May 23, 2017, https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.

Badshah, Nadeem, "Facebook to contact 87 million users affected by data breach," The Guardian, April 2018), https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach.

"CVE Details by Date," MITRE Corp., https://www.cvedetails.com/browse-by-date.php.

"Framework for Improving Critical Infrastructure Cybersecurity," version 1.1, National Institute of Standards and Technology, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

"Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017," Gartner news release, December 7, 2017, https://www.gartner.com/newsroom/id/3836563.

"HIPAA Administrative Simplification Regulations: The HIPAA Security Rule," 45 CFR Part 160 and Subparts A and C of Part 164, U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/security/index.html.

Paulsen, Celia, and Patricia Toth, "Small Business Information Security: The Fundamentals," NISTIR 7621, revision 1, National Institute of Standards and Technology, November 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf.

"PCI Noncompliance Consequences," Focus on PCI: A Data Security Standards Guide, http://www.focusonpci.com/site/index.php/pci-101/pci-noncompliant-consequences.html.

Peretory, Frank, Robert L. Hornby, Michelle A. Schaap, and Brigitte M. Gladis, "Cybersecurity: The Increasing Obligations and Exposure in the Age of State Regulation," Journal of Equipment Lease Financing, Fall 2017 (vol. 35, no. 3), https://www.store.leasefoundation.org/cgi-bin/msascartdll.dll/ProductInfo?productcd=JELF2017FALLSECURITY.

Ragan, Steve, "Here are the 61 passwords that powered the Mirai IoT botnet," Salted Hash – Top Security News, CSO, October 3, 2016, https://www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html.

Regulation (EU) 2016/679 of the European Parliament and of the Council, "General Data Protection Regulation," document 32016R0679, April 27, 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Ross, Ron, Kelley Dempsey, Patrick Viscuso, Mark Riddle, and Gary Guissanie, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," Special Publication 800–171, Rev. 1, National Institute of Standards and Technology, Computer Security Resource Center, planning note, June 7, 2018, https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final.

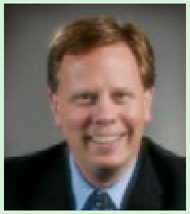
"Security and Privacy Controls for Information Systems and Organizations," initial public draft: NIST Special Publication 800–53, revision 5, Joint Task Force Transformation Initiative, National Institute of Standards and Technology, August 2017, https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf.

"Security Breach Notification Laws," National Conference of State Legislatures, March 29, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

"Security Update for Microsoft Windows SMB Server (4013389)," Microsoft Security Bulletin MS17–010, last updated October 11, 2017, https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.

"Verizon 2018 Verizon Data Breach Investigations Report (DBIR)," Verizon, https://www.verizonenterprise.com/verizon-insights-lab/dbir/.

Vossen, Britt, Sjoerd van der Zee, and Egbert de Jong, "Managing the Impact of Compliance on Life Cycle Management," DLL Financial Partner Solutions, May 2018, https://www.dllgroup.com/en/press-homepage/overviewhomepage/dll-publishes-new-research-and-insights-on-the-impact-of-compliance.



Joseph Granneman

jgranneman@illumination.io

Joseph Granneman is CEO of illumination.io in Cherry Valley, Illinois. He founded the cybersecurity company in 2013 following more than 20 years of experience as an executive IT leader in healthcare and financial trading institutions. He is an expert in penetration testing in the banking, manufacturing, and healthcare vertical markets; incident response; and forensic analysis as well as regulatory compliance with HIPAA, PCI, and NIST security frameworks. He has worked closely with the FBI and Secret Service on behalf of his clients who have been victims of cybercrime. Mr. Granneman has written articles for Information Security and CIO/CSO magazine and publishes online with TechTarget at http://searchsecurity.techtarget.com. He is an adjunct professor of IT strategy for the MBA program at Northern Illinois University's College of Business in De Kalb, where he also received an MBA in 2011. He is involved in developing as proposal for secure healthcare data exchange for the state of Illinois. In addition, he helped develop security standards for emergency medical responders as part of serving on the Certification Commission for Health Information Technology Security Working Group. Mr. Granneman received a BS from Millikin University, Decatur, Illinois, in 1993 and also holds the CISSP (certified information systems security professional) credential.