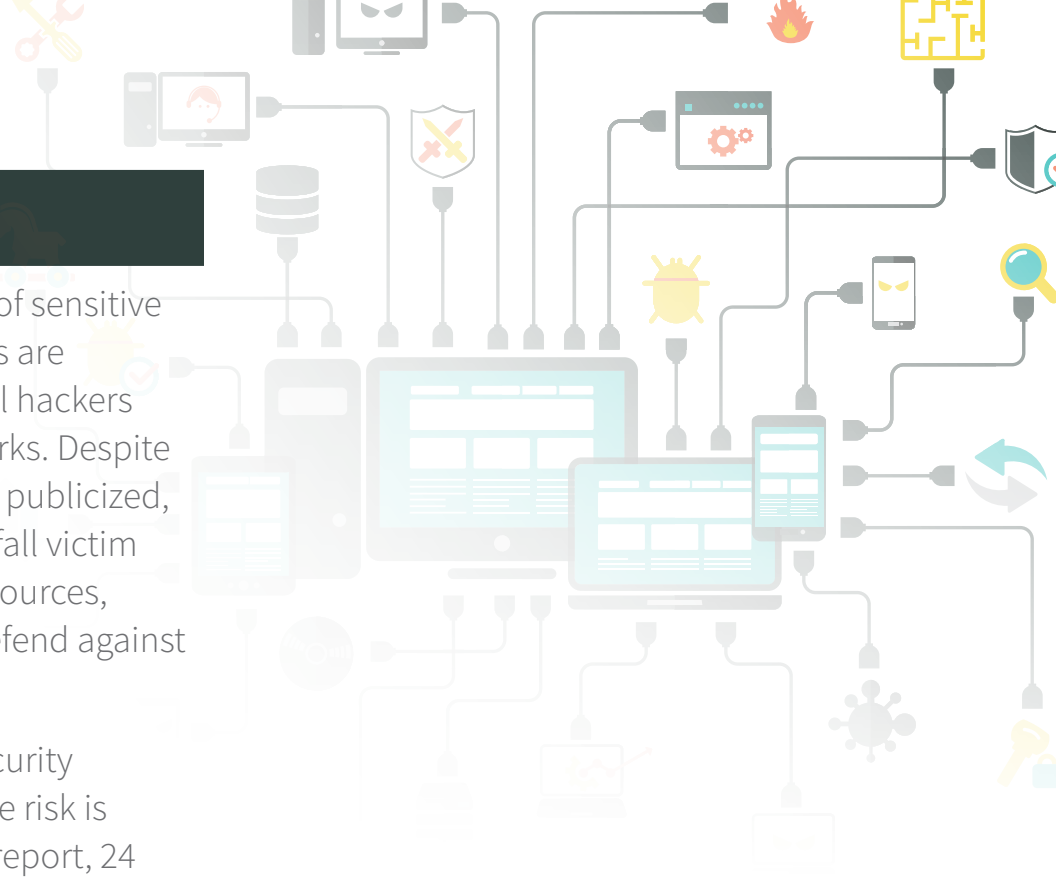
Information Security
IN THE DIGITAL ERA

POWERED BY eMoney

Introduction



Because they hold a wide variety of sensitive data, financial services companies are primary targets for both individual hackers and sophisticated criminal networks. Despite the fact that cyberattacks are well publicized, financial services companies still fall victim to them because they lack the resources, infrastructure, or experience to defend against the range of possible threats.

The consequences of lax cybersecurity protocols are often severe. And the risk is increasing. According to a recent report, 24 percent of financial services firms suffered a breach in 2017, up from 19 percent in 2016.[1]

This white paper outlines the risks and the data-security strategies that financial advisors, home-office executives, and wealth management enterprises should consider to better protect their clients and their businesses.

The Threatscape

Attacks on sectors such as retail and government often attempt to gather personal data to sell online. Threats to financial services companies, on the other hand, focus mainly on fraud as attackers attempt to steal money or data directly from the company or its customers. To carry out these cyberattacks, hackers employ a variety of methods.

BUSINESS EMAIL COMPROMISE (BEC)

The most brazen attack is the business email compromise (BEC), in which a criminal persuades a company executive or agent to send funds to a fraudulent account. These attacks are classic confidence tricks, combining research, persuasion, and a contrived sense of urgency to build trust before asking the individual to transfer funds.

In many cases, they also involve a direct attack on the client, compromising an individual's email account and reading their correspondence with their advisor. Once they learn the target's financial workflows and communications styles, attackers will often pose as the client, demanding a quick transfer of funds to deal with a fictional emergency.

Tillage Commodities Fund vs. SS&C Technology

In 2016, the U.S. investment firm Tillage Commodities Fund sued SS&C Technology, an investment management software and services provider. Tillage alleged that SS&C had been duped by a BEC after scammers requested the firm send Tillage funds to overseas bank accounts. According to the claim, Tillage lost six million dollars.[2]

RANSOMWARE

Ransomware is malicious software, or "malware," that encrypts a user's data so that it's impossible to access. Often, the organization must pay the hackers a ransom to restore its data. According to Verizon's 2018 Data Breach Incident Report (DBIR), ransomware has become a pervasive threat.[3] In fact, in 2017, ransomware was used in around 40 percent of malware-related cases. The Securities and Exchange Commission (SEC) also highlighted ransomware as a particular threat for smaller investment management firms in its May 2017 Risk Alert.[4]

PHISHING

Ransomware and BEC schemes alike often arrive via phishing attacks, which are especially prevalent in the financial sector.[3] In these attacks, an email persuades an individual to log in to a fraudulent website, to open an attachment, or to visit a link that then infects their computer with malware. The higher the target's value, the more sophisticated the attack. Because larger firms have more potential areas of weakness, they are often more vulnerable to attack than smaller firms.

Phishing threats that target financial services companies and their clients are likely to increase [3] as hackers mount attacks through a growing range of channels. Verizon's Data Breach Investigations Report identified phishing as a leading threat vector with at least one in three hacks on financial services companies involve this form of cyberattack.[3] High-risk channels include social media networks because many users willingly post compromising information that exposes them or their companies to attack.

GROWING SOPHISTICATION OF ATTACKS

Cyberattacks are almost commonplace because of the increasing sophistication of attackers. In the early days of computing, hackers were often amateurs targeting companies for fun. Soon after, "hacktivists" started targeting financial institutions in order to make ideological points. To overwhelm networks, disrupt operations, and corrupt data, hackers often employ distributed denial of service (DDoS) attacks.

More recently, though, the financial industry has been the target of shadowy, organized criminal networks for whom hacking is a profitable business. They attack wealth management firms and other financial institutions in well-planned campaigns that can be difficult to detect.

According to industry surveys, criminal organizations are increasingly targeting high-value firms and individuals. Thales Security found that 24 percent of U.S. financial companies reported a breach in 2017, up from 19 percent the previous year.[1] Incidents of fraud, whether online or offline, have grown by over 130 percent in the past year, according to PwC.[5]

Because of the threat to investment advisors and wealth management companies, the SEC is more closely scrutinizing IT security. According to a 2017 assessment of cybersecurity practices, registered investment advisors (RIAs) are particularly vulnerable targets. The commission identified "areas where compliance and oversight could be improved."[6] For example, the SEC found that more than a quarter of investment management firms did not conduct periodic risk assessments of critical systems to identify security vulnerabilities.[6]

Attacks on Tillage **[see Page 3]** and others show that while wealth managers and investment advisors may be aware of the threats to cybersecurity, they are ill-prepared to defend against them. A 2016 cybersecurity report by the Financial Planning Association found that 81 percent of the 1,015 advisors surveyed identified cybersecurity as a high risk; however, fewer than one in three felt adequately prepared to manage and mitigate the threats.[7]

The Risk

The risks associated with a data breach in the financial sector include the three Rs: **revenue, regulatory compliance, and reputation**. Advisors and firms that fail to take cybersecurity seriously could find themselves paying significant costs in each of these areas.

REVENUE IMPLICATIONS

The 2017 Ponemon Institute report The Cost of a Data Breach estimates the average cost of a breach in the financial services sector to be $245 per record. [8] Trailing only healthcare, finance was the second most costly sector for data breaches. These costs add up. In the U.S. alone, the average number of records lost per data breach is 28,512.[8] As a result, a single breach in the financial services industry can cost a firm nearly seven million dollars from both direct and indirect sources **(see Figure 1)**.

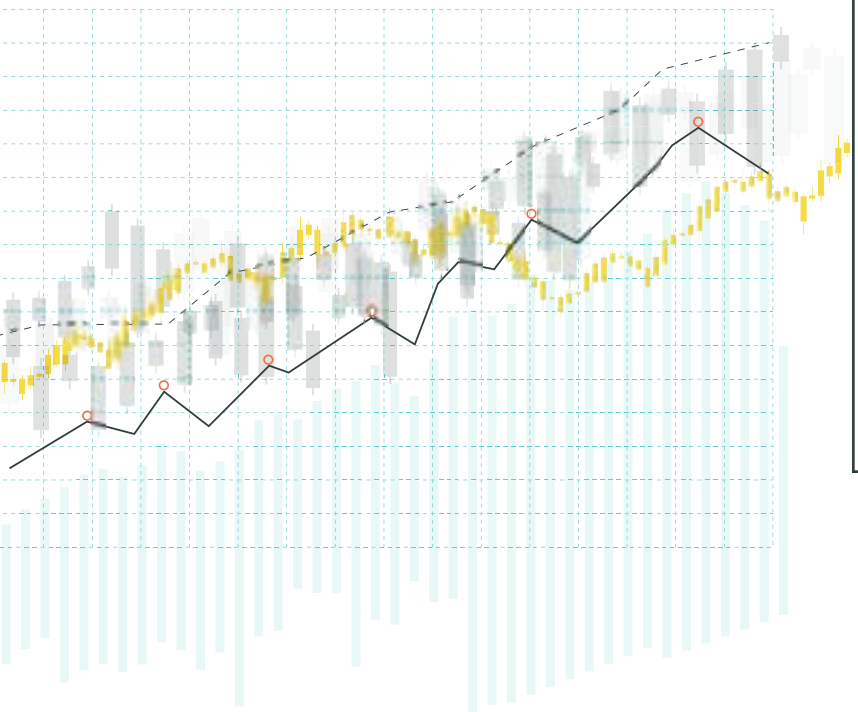


Figure 1: Costs associated with a data breach for a financial services company

DIRECT COSTS

- Investigating the cause of the breach
- Determining the probable victims and notifying them
- Organizing—and often hiring—an incident response team
- Recovering from company-system downtime
- Implementing additional call center support resources
- Engaging in communication and public relations outreach
- Offering free or discounted services to victims of the breach
- Settling legal fees and regulatory fines

INDIRECT COSTS

- Company time dedicated to breach resolution
- Internal communications and additional training
- Value of customer loss
- Diminished customer acquisition rates
- Ongoing reputational and brand damage

Source: Ponemon, eMoney Advisor

GROWING REGULATORY PRESSURE

The additional costs experienced by the financial services industry are unsurprising as heavily regulated industries tend to pay more for breaches than industries that are lightly regulated. In fact, the cost of cybersecurity failures in the industry was nine percent higher in 2017 compared with the four-year average.[8]

One factor contributing to the increase in costs is growing regulatory scrutiny. Not only is it time consuming and costly to compile and report breach information to regulators, but potential fines may be expensive. In 2014 the SEC Office of Compliance Inspections and Examinations (OCIE) conducted its first cybersecurity review of the broker-dealer and financial advisory industry. This review culminated in a February 2015 report that criticized the sector for failing to prevent cyberattacks. As a result, the SEC issued guidance on how firms should improve data security. Since then, fines have become more commonplace. These may range from $75,000 for incorrectly storing customer records with a third-party service to up to a million dollars for serious breaches in which large numbers of records are stolen.[9] [10]

UNDERSTANDING REPUTATIONAL DAMAGE

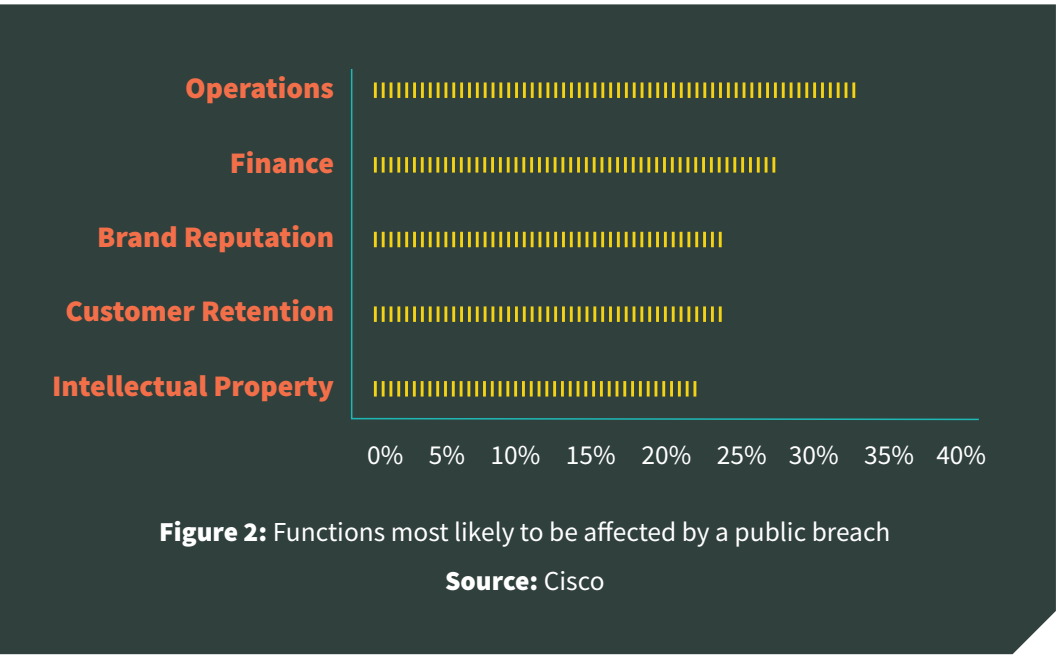


Figure 2: Functions most likely to be affected by a public breach

Source: Cisco

Indirect costs, which affect company brands and reputations, can also impact financial services companies. Cisco's 2017 cybersecurity survey found that brand reputation and customer retention suffered as a result of data breaches. Twenty-six percent of companies cited indirect costs as a significant factor.[11]

Financial services firms are particularly susceptible to adverse publicity regarding security breaches. At 5.7 percent, the industry has the highest abnormal churn rate—the expected loss of customers following a security breach beyond the expected rate of attrition—in the U.S. economy.[8] This figure is unsurprising as financial services companies are charged with protecting the sensitive customer data they hold. And consumer trust plays a large role in their success.

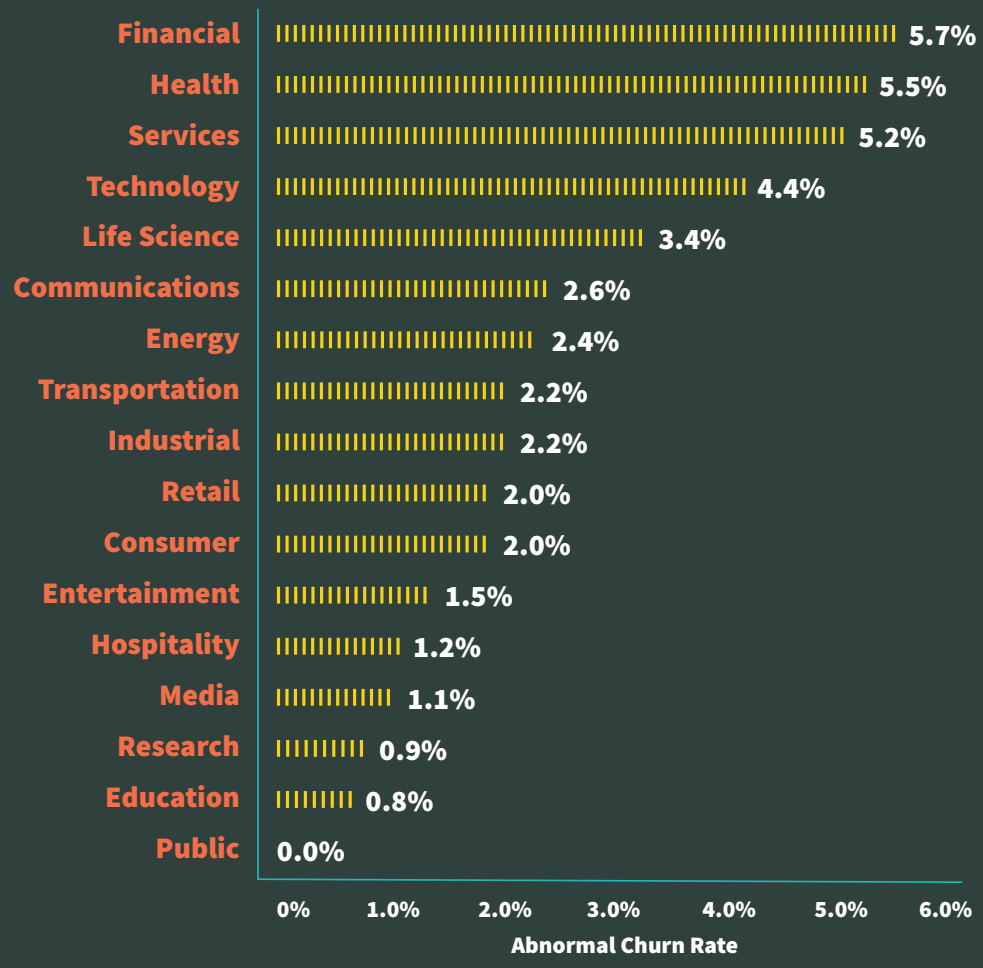


Figure 3: Abnormal churn rate by industry after cybersecurity breach

Source: Ponemon

BREACHES ARE INCREASINGLY PREVALENT

Unfortunately, as the cost of a breach in financial services increases, so does its prevalence. A 2017 Thales Security survey of more than 1,100 senior security executives worldwide found that 42 percent of financial services organizations had experienced a data breach at some point in the past, with 12 percent suffering multiple breaches. The rate of compromise also seems to be increasing. Twenty-four percent of financial services companies suffered a data breach in the last year alone, up from 19 percent in the previous year.[1]

The risks associated with poor cybersecurity in the financial services industry is increasing and can have severe consequences for the short- and long-term health of an organization.

Protecting Your Firm

Financial companies both large and small are at risk of data breaches. So how can they protect themselves? Although no company is 100 percent secure, those that invest in systems, partners, and processes that follow proven data and cybersecurity measures can reduce their vulnerability.

These considerations are particularly important when evaluating technology providers, especially those that process client data. Not only must you ensure your practices safeguard your business from potential breaches, you must also ensure your providers do the same.

TWO-FACTOR AUTHENTICATION (2FA)

One of the most effective measures for protecting access to user accounts is two-factor authentication (2FA). Traditionally, financial services companies have used passwords to protect access to sensitive files. But passwords are limited because people tend to use simple, easily-memorized phrases. Fifty-two percent of users reuse passwords between different services, making them more vulnerable to attack.[12] In response, some systems require users to set complicated passwords that are difficult to remember. Although this solves the simplicity problem, it creates another; users tend to write down these passwords to remember them.

Two-factor authentication (2FA) augments passwords by requiring a second, variable PIN that is delivered to a device in the user's possession. When a user tries to log into a 2FA-enabled system, they must provide the time-sensitive PIN, as well as their password. Without both, they are unable to log in to the system. This method prevents a hacker from accessing user accounts through brute-force attacks or password theft.

ENCRYPTION

While 2FA makes it more difficult to compromise an account, it won't stop intruders who gain direct access to system files by hacking a network or snooping on an insecure connection or device. For added protection, financial advisory firms should encrypt data at rest and in transit. There are several encryption options: If data is stored in a cloud-based service, the provider should encrypt the data on its servers. The provider should also be able to show how it secures the digital keys used to encrypt and decrypt the information. Financial advisors who store files locally on their systems should use full-disk encryption on local servers, endpoints, and networked storage.

BACKUPS

Encryption will not protect advisors from ransomware, which is one of the most prevalent forms of modern cyberattack facing professional services firms.[3] Ransomware can render legitimately encrypted files inaccessible. To protect against ransomware attacks, firms should regularly back up locally held data to offline storage. With this approach, firms have a safe copy of data that can be restored in the event of attack.

CYBERSECURITY HYGIENE

The phrase “cybersecurity hygiene” can describe several fundamental security measures. These are essential steps that can help protect systems from attack:

- **Regularly update operating systems and applications.** Install the latest software patches to reduce their attack surface.
- **Use anti-malware tools.** These software and appliances may not stop all malicious software—particularly zero-day attacks—but they will reduce the risk of compromise by identifying many malicious files.
- **Whitelist applications.** Rather than merely scanning for malicious software on the network, use a whitelist that allows users to only run approved applications. A whitelist will help IT control and protect the software running on its endpoints.
- **Minimize privileges.** Financial services firms can reduce the risk of erroneous or malicious system activity by granting system users only the privileges they need to do their jobs.

TRAINING USERS

Even with the best technology controls, poorly educated users can still accidentally create vulnerabilities. Many attacks persuade users to click on malicious links or open infected attachments. To mitigate the risk, it’s important to properly educate staff of the dangers and to outline safe practices in a formal security policy. A sustained cybersecurity awareness campaign should be a core part of any IT security program.

TESTING SECURITY

These technical measures don’t exist in a vacuum. People, processes, and IT infrastructures change over time, making it essential to regularly test their effectiveness. Security audits can help to ensure that data is protected in the future. Consider auditing staff awareness. Several vendors offer phishing services to test users and to identify those who regularly fall victim to spoof emails so that they can be educated further.

CHECKING YOUR VENDORS

Thoroughly vet your vendors to ensure that they have taken measures to protect your data. Compliance with the AICPA Service Organization Control 2 (SOC 2) standard is a good starting point for evaluating the security, processing integrity, and privacy of personal information offered by vendors of cloud-based software and services.[13] Regulators recognize the value of SOC 2 certification.

For a deeper dive, companies can use the Cloud Security Association's Consensus Assessments Initiative Questionnaire (CAIQ) in conjunction with its Control Matrix for an itemized set of questions concerning cloud security.[14] A site visit can reassure advisors about a service provider's levels of security.

Technical experience is only half of the story, however. Few financial technology (Fintech) companies have practical experience managing the complexities and nuances of financial services regulations and commercial practices. When looking for a software and technology services partner, advisors should look for vendors who have experience with regulated companies, and whose staff include dedicated security personnel who understand cybersecurity issues in finance.

PREPARING FOR THE WORST

Financial advisors must accept a fundamental reality of cybersecurity; even with the best controls in place, an attack may still succeed. Preparing for this possibility is a critical step in any cybersecurity preparedness initiative, which is why it's important to develop an incident response plan.

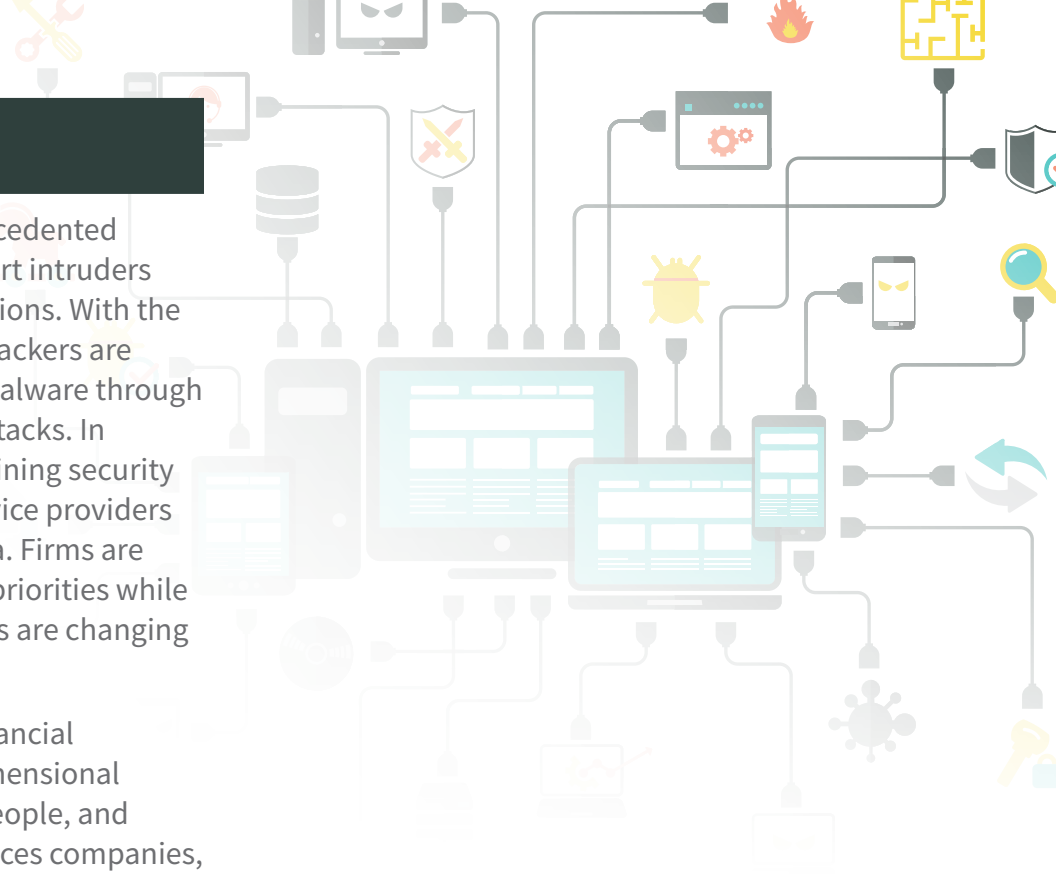
National Institute of Standards and Technology's (NIST) incident response plan outlines four steps:[15]

- **Preparation.** This stage involves assembling a response team with the appropriate expertise. These include technical skills as well as legal knowledge and communications expertise so that the team can update stakeholders about the security event efficiently and accurately.
- **Detection.** The detection phase includes analysis and reporting of security breaches to understand the causes and consequences. This prepares the team for its next step.
- **Containment, eradication, and recovery.** The incident response team must coordinate its response, share information about the breach, and communicate the business impact to senior executives. It must also isolate the attack from the rest of the system, neutralize it, and recover the company's systems and data where possible.
- **Post-incident activity.** This stage closes the loop by using data gathered during the event to expand the organization's knowledge base and reassess security measures. By drawing valuable lessons from the event, financial companies can enhance their defenses against similar attacks in the future.

Conclusion

Financial services firms face an unprecedented set of challenges as they work to thwart intruders while complying with industry regulations. With the possibility of large financial payoffs, hackers are deploying technically sophisticated malware through a wide variety of social engineering attacks. In response, regulators are closely examining security measures to ensure that financial service providers protect their customers' sensitive data. Firms are challenged to meet these competing priorities while serving customers whose expectations are changing in a fast-moving industry.

To defend against security threats, financial advisory firms must adopt a multi-dimensional strategy that combines technology, people, and processes. Yet for many financial services companies, cybersecurity is not a core competency. To promote client engagement and growth, while protecting themselves and their customers, firms must select technology partners with experience in both financial services and cybersecurity.



Learn more about the features and practices that can protect your customer data.

References

[1] Thales, *'Thales Data Threat Report'*
Available at: https://goo.gl/YQAPV4. Accessed April 2018.

[2] Trend Micro, *'$6M Lost in Another BEC Scam: Who Is the Weakest Link?'*
Available at: https://goo.gl/F4RVew. Accessed April 2018.

[3] Verizon Enterprise, *'Tales of dirty deeds and unscrupulous activities'*
Available at: https://goo.gl/JX3RtG. Accessed April 2018.

[4] SEC, *'Cybersecurity: Ransomware'*
Available at: https://goo.gl/wCwaHm. Accessed April 2018.

[5] PWC, *'Top financial services issues of 2018'*
Available at: https://goo.gl/KBnqH7. Accessed April 2018

[6] SEC, *'Observations from cybersecurity examinations'*
Available at: https://goo.gl/Uk6L4e. Accessed April 2018.

[7] Financial Planning Association, *'Is your data safe?'*
Available at: https://goo.gl/UNTUU1. Accessed April 2018.

[8] Ponemon, *'2017 Cost of Data Breach Study'*
Available at: https://goo.gl/fa33ev. Accessed May 2018.

[9] *SEC.* Available at: https://goo.gl/J7n9Ur

[10] *SEC.* Available at: https://goo.gl/82BR9A

[11] Cisco. *'Cisco 2017 Annual Cybersecurity Report'*
Available at: https://goo.gl/fJySWw. Accessed May 2018.

[12] Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart and Gang Wang Department of Computer Science, Virginia Tech
'The Next Domino To Fall: Empirical Analysis of User Passwords across Online Services'
Available at: https://goo.gl/57NFw1. Accessed May 2018.

[13] AICPA, *'SOC 2® - SOC for Service Organizations: Trust Services Criteria'*
Available at: https://goo.gl/f6457B. Accessed May 2018.

[14] Cloud Security Alliance, *'Consensus Assessments Working Group Downloads'*
Available at: https://goo.gl/fidGqp. Accessed May 2018.

[15] National Institute of Standards and Technology, *'Computer Security Incident Handling Guide - SP 800-61 Rev. 2'*
Available at: https://goo.gl/bXZHdy. Accessed May 2018.