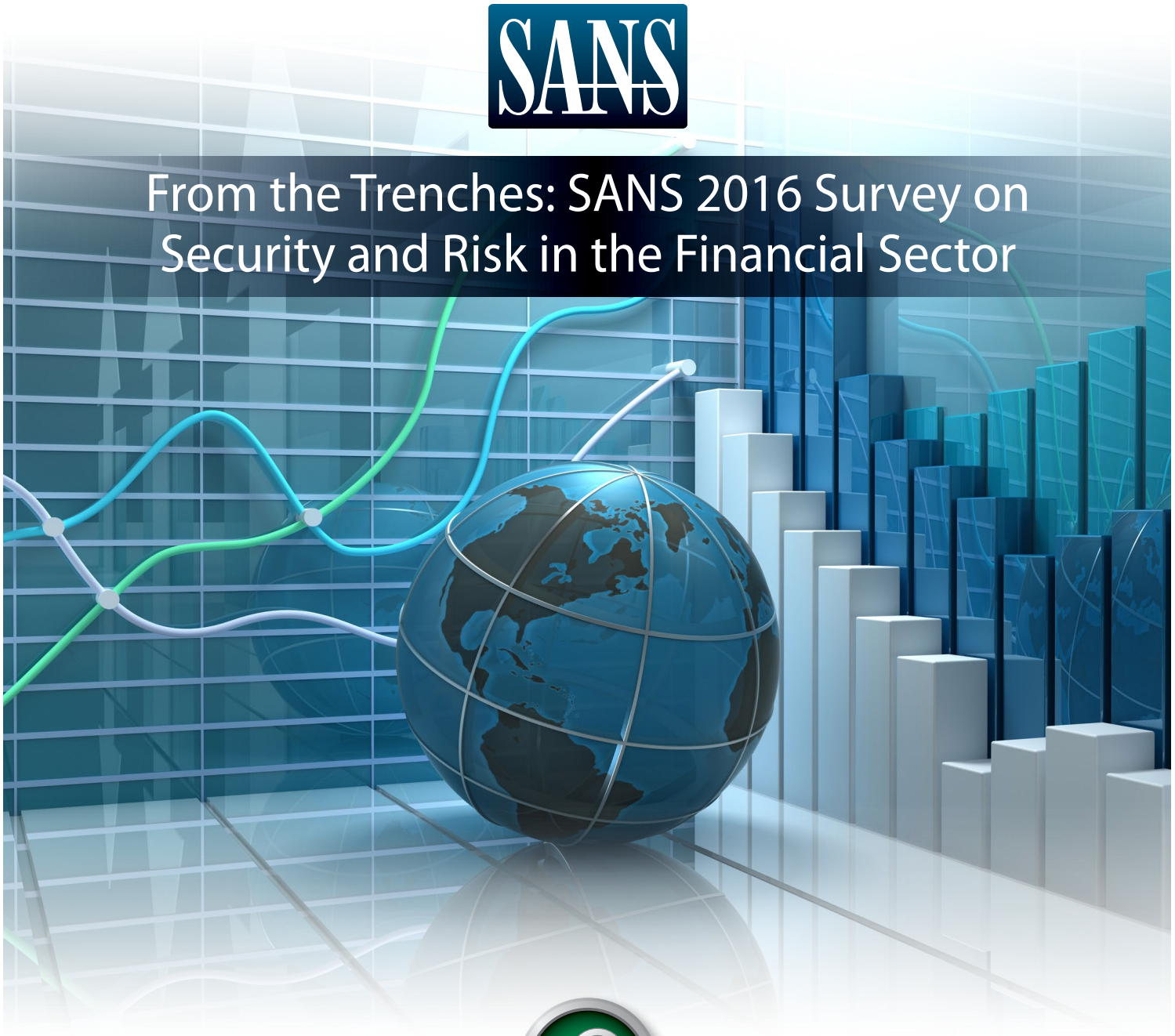
Interested in learning more about security?

# SANS Institute InfoSec Reading Room



## From the Trenches: SANS 2016 Survey on Security and Risk in the Financial Sector

The financial services industry is under a barrage of ransomware and spearphishing attacks that are rising dramatically. These top two attack vectors rely on the user to click something. Organizations enlist email security monitoring, enhanced security awareness training, endpoint detection and response, and firewalls/IDS/IPS to identify, stop and remediate threats. Yet, their preparedness to defend against attacks isn t showing much improvement. Read on to learn more.



# From the Trenches: SANS 2016 Survey on Security and Risk in the Financial Sector

**A SANS Survey**

*Written by G. Mark Hardy*

*Advisors: Stephen Northcutt and Matt Bromiley*

October 2016

*Sponsored by*

*Arbor Networks, ForeScout Technologies, Guidance Software, NSFOCUS, and WhiteHat Security*

# Introduction

**Top Vectors**

Ransomware attack (e.g., CryptoLocker)

Spearphishing or whaling

Advanced attacks/Advanced persistent threats (APTs)

DoS attacks

The financial services industry is under a barrage of ransomware and spearphishing attacks that are rising dramatically, according to the 2016 SANS survey gauging the state of risk and security in the financial sector. In it, 34% of respondents had or suspected they had impactful breaches, while 11% didn't know. Among those that had experienced a breach, 68% of respondents feel impactful events are on the rise, with 18% saying events are rising significantly.

Ransomware and phishing attacks are causing them the most harm. Of those that were able to quantify their losses, the largest group (32%) reported losses between $100,001 and $500,000.

It's important to note that the top two vectors identified by respondents both rely on the user to click something. Add to that the perniciousness of ransomware, which gets more convincing every day. The recently released "Fantom" ransomware, for example, is difficult to distinguish from a legitimate Microsoft Windows Update.[1] So, it's not surprising that organizations are enlisting email security monitoring and enhanced security awareness training to protect against phishing and ransomware. They are also using endpoint detection and response to more quickly identify, stop and remediate threats that penetrate the network, which they consider their most effective control, along with firewalls/IDS/IPS.

**Most Effective Overall Controls**

Advanced firewalls, IDS and IPS

Endpoint protection

Employee awareness training

Log management

The good news is that 23% of organizations believe they had a decrease in impactful incidents during the past 12 months, which indicates these controls are helping.

This result ties to their growing ability to quantify losses, which they can use to drive improvements. This year, 73% were able to quantify losses from impactful events, as opposed to only 25% in the SANS 2015 survey on financial services risk and security.[2] This shows significant growth over the past 12 months.

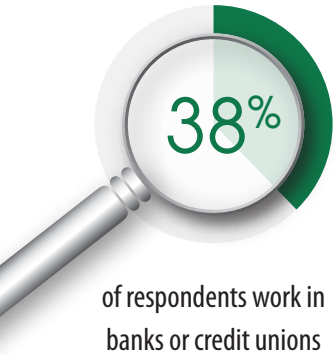
Their preparedness to defend against attacks, however, isn't showing much improvement. In our 2016 survey, 57% of respondents felt prepared or very prepared to fend off attacks compared to 55% in 2015. New alternative payment programs for mobile and online payments, such as Apple Pay and PayPal, are also already in use among 29% of respondent organizations, further testing respondents' preparedness to deal with new threats tied to these new payment methods.

This report discusses these and other findings more fully in the following pages.

[1] www.darkreading.com/attacks-breaches/new-fantom-ransomware-poses-as-windows-update/d/d-id/1326774?_mc=RSS_DR_EDT

[2] "Security Spending and Preparedness in the Financial Sector: A SANS Survey," www.sans.org/reading-room/whitepapers/analyst/security-spending-preparedness-financial-sector-survey-36032

# About the Participants




of respondents work in banks or credit unions


of respondents are from financial industry service providers

The 238 professionals who took this survey (conducted between January and February 2016) represent the front lines of IT security in the financial sector, responsible for defending against attacks. They are also constantly defining and rewriting the security requirements of their organizations as attacks evolve. Their input into this survey serves to educate the IT community about what's working in the defensive battle IT pros find themselves in—and, equally important, what's not working and what could use improvement.

## Participating Organizations

Service providers to financial institutions represented the largest group of respondents at 16%. Another 14% of respondents worked for credit unions, and 22% worked for retail, commercial, and investment banking. The remainder of respondents came from a variety of lines of business, including payment processors, accountancies, vendors and payment card companies. See Figure 1.

**What is your organization's role in the financial industry or involvement in financial services?** ***Select the most appropriate.***

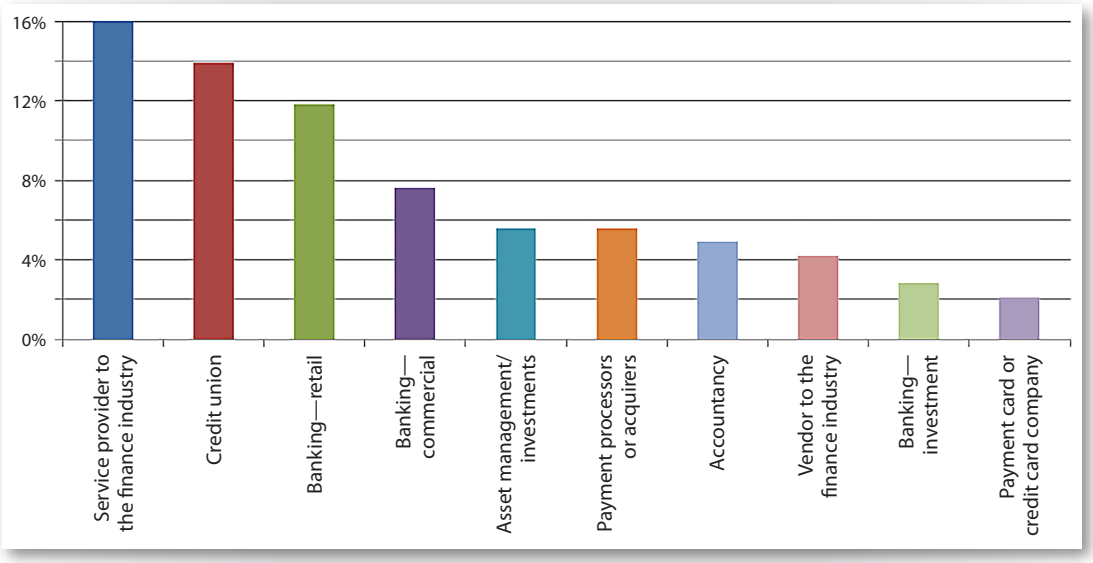



*Figure 1. Top 10 Respondent Industries*

*Financial applications are a factor for multiple industries beyond the banking and financial industry, including insurance, healthcare and government, among others.*

Spearphishing

An attack that targets specific individuals in an organization, such as chief financial officers, for their direct access to accounts, or others, such as human resources personnel, with authorized access to employee databases

Industries represented, but not included on Figure 1, include lenders, online banking and online alternative payment systems, each selected by 1%. The distribution of industry categories is about what we expected. The 22% that selected "Other" consist of the following, in descending order:

- Insurance companies
- Healthcare organizations
- Education and training organizations
- Government agencies
- Telecommunications
- Consultants

This suggests that financial applications are a factor for multiple industries beyond banks and service providers. Insurance companies face significant reporting requirements. Healthcare firms and government agencies accept payments, and educational institutions deal with student loans and related financial information. Other, nonfinancial organizations are managing their ACH (internal clearinghouse) accounts, which are also primary targets of spearphishing attacks.

## Wide Range of Organizational Sizes

The survey targeted IT professionals across a wide range of organizational sizes. Nearly 29% came from workforces greater than 10,000 people, while on the opposite end, 42% came from workforces of less than 1,000, as shown in Figure 2.

**What is the size of the workforce at your organization, including employees, contractors and consultants?**

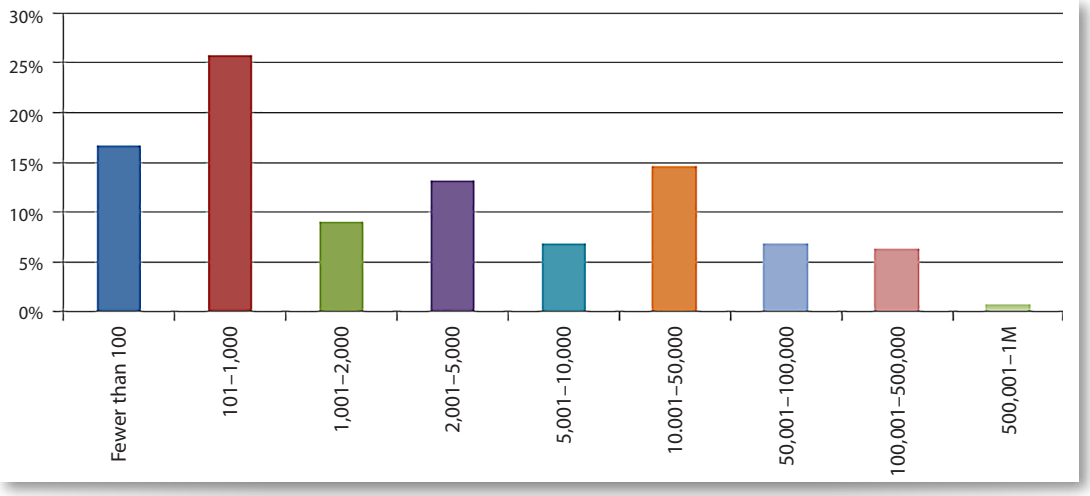
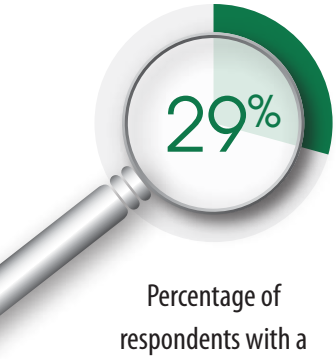



*Figure 2. Workforce Size*

Smaller organizations include credit unions, consulting, legal and other entities serving financial clients. The distribution across sizes greater than 1,000 workers suggests a mix of local, regional and national financial institutions, as well as the service providers that work with them.



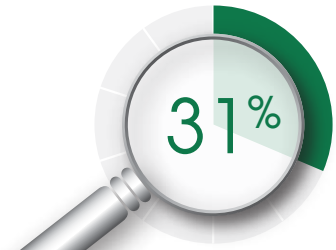

Percentage of respondents with a workforce larger than 10,000

## International Representation

A large majority (79%) of respondents indicated that they operate in the United States, 31% operate in Asia and 31% in Europe, while 67% are from organizations headquartered in the U.S., and 13% are from organizations headquartered in Europe, as illustrated in Table 1.

**Table 1. International Representation**

| Country/Region | Conduct Operations | Headquarters |
|---|---|---|
| United States | 78.5% | 67.4% |
| Asia | 31.3% | 5.6% |
| Europe | 31.3% | 13.2% |
| Canada | 25.0% | 4.2% |
| South America | 22.9% | 3.5% |
| Middle East | 19.4% | 2.1% |
| Australia/New Zealand | 16.0% | 0.7% |
| Africa | 15.3% | 0.0% |




Percentage of respondents that report operating in Asia. An equal percentage operate in Europe.

By drawing on this diverse set of respondents, the survey should also provide some insight into global best practices. For example, the regulatory and legal framework used by most respondents is U.S.-centric. That said, some security frameworks are international in scope, for example the ISO 27000 series, and are considered germane to organizational efforts, which we'll examine later in the "Security Frameworks" section of this paper.

### Global Banking Systems

According to the Federal Deposit Insurance Corporation (FDIC), there are 6,122 FDIC-insured banks in the U.S. today,[3] down from 6,891 two years ago, and down from more than 18,000 30 years ago.[4] Even with this reduction, the U.S. is home to more independent banks than the entire European Union combined (5,249).[5] In the United Kingdom, there are only 116 banks and building societies that have permission to accept deposits (i.e., domestic banks)[6] and just 29 in Canada.[7]

The *Bankers Almanac* identifies the top four largest banks in the world as Chinese (significant change over last two years), and three of the top 10 largest banks in the world are European.[8] The largest U.S. banks, JPMorgan Chase and Bank of America, rank sixth and 12th in the world, respectively.

[3] www.fdic.gov/bank/statistical/stats/2016mar/industry.pdf

[4] http://online.wsj.com/news/articles/SB10001424052702304579404579232343313671258?mod=ITP_pageone_0 [Subscription required for access.]

[5] "Number of Monetary Financial Institutions: June 2016," www.ecb.europa.eu/stats/money/mfi/general/html/mfis_list_2016-06.en.html

[6] www.bankofengland.co.uk/statistics/Pages/reporters/institutions/default.aspx

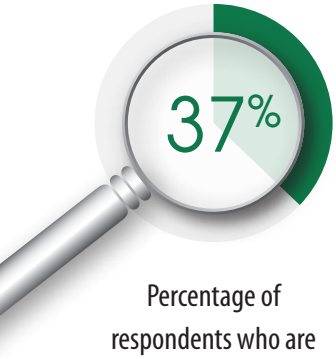
[7] www.osfi-bsif.gc.ca/Eng/wt-ow/Pages/wwr-er.aspx?sc=1&gc=1&ic=1#WWRLink111

[8] "Bank Rankings—Top Banks in the World," https://accuity.com/resources/bank-rankings/

Responses to the survey came from a wide cross-section of roles and positions, thus providing viewpoints from nearly all positions directly associated with financial security. Participant roles break down to a near equal mix of administrative-level and managerial-level professionals:

- 19% security managers or directors
- 10% C-level or VP-level security experts
- 18% security administrators or analysts
- 10% IT managers or directors
- 7% system administrators
- 6% "other," which includes analysts, risk managers and penetration testers

Auditors, compliance officer/risk managers and security architects each represented 5% of survey takers.




Percentage of respondents who are security managers, directors, administrators or analysts

## Spending Trends

The largest group of respondents indicated they either did not know or were unsure about the budgets for the current (32%) or the future fiscal year (38%). This may be because many respondents are not responsible for IT security budgeting and may not have good visibility into their IT spending.

Spending on IT security varies, with the largest group (14%) reporting spending between 2% and 3.9% of their IT budgets on security, while 13% were spending 9% to 10.9% of their budgets on security.

The shift in spending appears to be tilting upward, as the peaks in the spending curve move up from 3% and 10% in FY2016 to 5% and 12% in FY2017. The percentage in the 1% or less range dropped from 13% to 10%, as shown in Table 2.

**Table 2. Security as a Percentage of IT Budget for Fiscal Years 2016 and 2017**

**What percentage of your organization's IT budget was allocated to security in FY2016?**
**What percentage of the IT budget will be devoted to security in the FY2017?**

| % of budget | Unknown/ Unsure | Less than 1% | 1% | 2%–3.9% | 4%–6.9% | 7%–8.9% | 9%–10.9% | 11%–25% | More than 25% |
|---|---|---|---|---|---|---|---|---|---|
| **FY2016** | 31.8% | 7.5% | 5.6% | 14.0% | 7.5% | 9.3% | 13.1% | 9.3% | 1.9% |
| **FY2017** | 38.2% | 4.9% | 4.9% | 5.9% | 16.7% | 4.9% | 8.8% | 12.7% | 2.9% |

The good news is that 55% of respondents say that they did not have a significant event resulting in loss of business or personal data in the past 12 months, as shown in Figure 3.

**In the past 12 months, has your organization suffered one or more incidents that significantly affected your operations, including sensitive, financial and personal data, their systems or availability?**

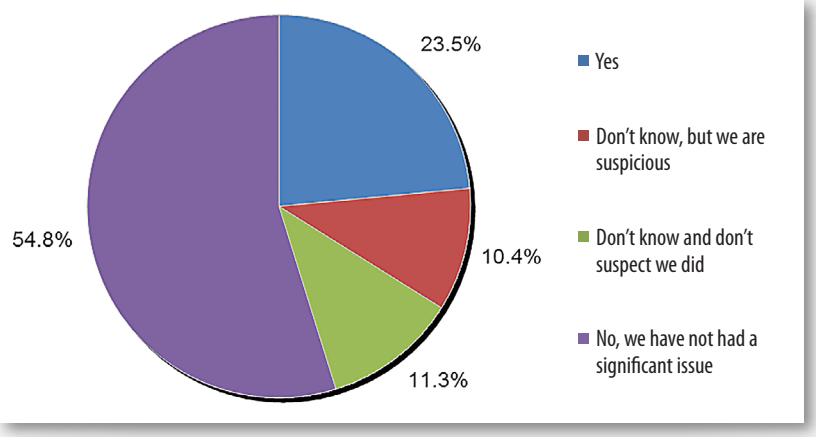



*Figure 3. Attack Prevalence*

However, 24% of respondents indicated that they suffered one or more incidents that significantly affected operations, while the remainder didn't know.

Considering that financial institutions are a primary target for fraud, it would be surprising that two-thirds of these organizations went unscathed. It is important to remember that you can't know what you can't detect. Indicators of the increasing number of attacks are illustrated in Figure 4, wherein 68% of respondents feel impactful events are on the rise, with 18% of those suspecting a significant increase.

**Increase or Decrease in Number of Incidents Significantly Affecting Organizations**

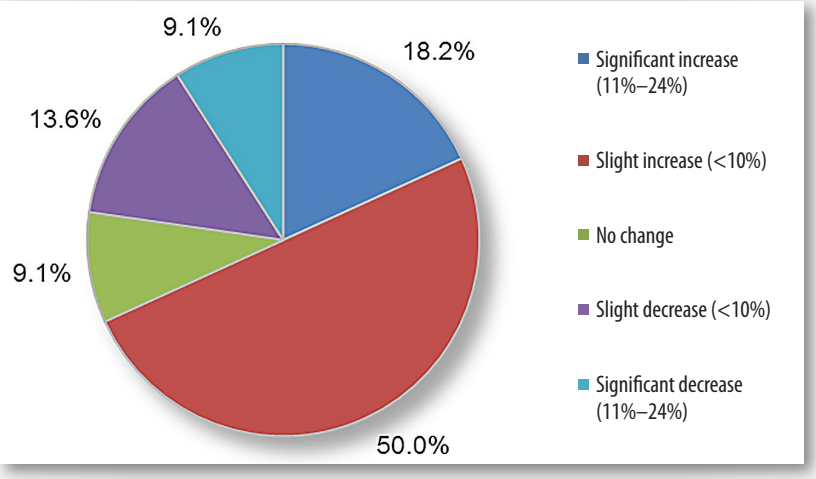



*Figure 4. Number of Incidents Increasing*

It is interesting to consider that 23% of organizations believed they had a decrease in impactful incidents. There are some rational explanations for this. One may be that countermeasures, security technologies and increased user training and awareness are working. Or, as noted previously, another possibility is that the attackers are not being noticed.

## Attack Vectors

Ransomware emerged as the most identified type of attack for those organizations that had experienced a breach. In SANS' most recent report, the SANS 2016 Threat Landscape Survey published in September, ransomware was the second most significant form of adverse event after phishing/spearphishing.[9] In a matter of months, ransomware rose to the top, showing just how fast the ransomware threat is growing. In our 2015 financial services survey, ransomware was barely on the radar.

### Ransomware How To

Ransomware usually starts with phishing-type email attachments or web URLs embedded in messages or documents. In addition, "malvertising" (advertisements on legitimate websites that contain hostile content) may be an infection vector for ransomware, but rarely do victims realize or recognize when this occurs.[10]

The top defenses against ransomware are:

- Provide user awareness training and inoculation (friendly testing) to reduce the human attack surface.
- Use comprehensive patch management programs that keep all systems up-to-date to reduce the endpoint attack surface.
- Limit user privilege and network drive connectivity to the minimum essential for job requirements.
- Conduct frequent backups and store them offline (newer ransomware variants spread through drive shares and even reconnect disconnected shares).
- Use network segmentation that requires authentication (i.e., user types in password) to traverse the network to reduce the network attack surface.
- Use current threat intelligence to block inbound and outbound traffic to known ransomware command-and-control sites, thus preventing users' ability to download hostile tools or upload encryption keys and credentials.
- Know how to obtain Bitcoin in advance of an attack (or purchase some as a hedge; you might even make a small profit).

For a comprehensive discussion of ransomware and recommended defenses, see Shafqat Mehmood's whitepaper in the SANS Reading Room.[11]

[9] "Exploits at the Endpoint: SANS 2016 Threat Landscape Survey," www.sans.org/reading-room/whitepapers/firewalls/exploits-endpoint-2016-threat-landscape-survey-37157, Figure 4, p. 6

[10] http://images.wellsfargotreasury.com/Web/WellsFargo/wfb4632-ransomware-infographic.pdf

[11] "Enterprise Survival Guide for Ransomware Attacks," www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-ransomware-attacks-36962

The top five vectors in 2016 were:

- 55% Ransomware attack (e.g., CryptoLocker)
- 50% Spearphishing or whaling
- 32% Advanced attacks/Advanced persistent threats (APTs)
- 32% DoS attacks
- 27% Web application attacks

Tools to launch ransomware and denial of service (which today are usually distributed denial of service, or DDoS) attacks are generally available on the dark net, essentially as malware-as-a-service (MaaS), making these attacks easy to perpetrate en masse with very little skill. These attacks are also multifaceted, with adversaries using DDoS to launch APTs, for example, or web app attacks aimed at the back-end financial database. Figure 5 identifies the types of attacks used in impactful attacks against respondent organizations.

**What types of attacks were involved?** ***Select all that apply.***

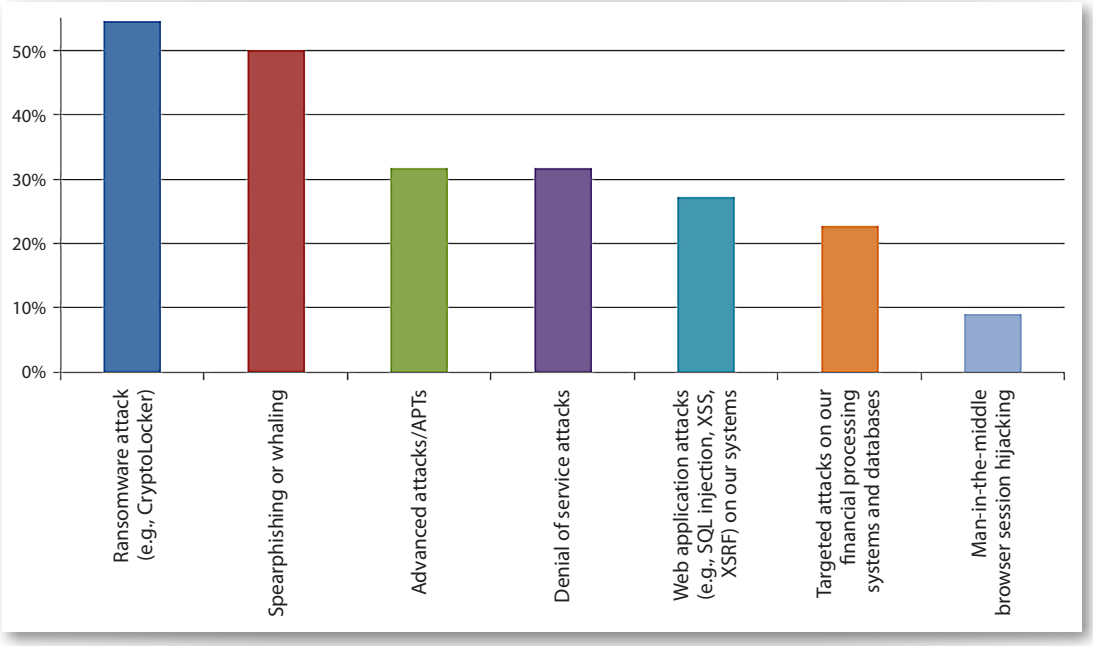



*Figure 5. Types of Attacks Identified*

Web application attacks against financial systems remain popular as attackers take the easiest route. Most attacks exploit known vulnerabilities, such as SQL injection and cross-site scripting (XSS), where patches have often been available but organizations have not prioritized these vulnerabilities for remediation.

Targeted attacks against financial systems, a somewhat distant sixth at 23%, usually require significant reconnaissance and intelligence to mount effectively. It appears that attackers aren't bothering with all that when targets of opportunity—through ransomware and spearphishing—yield better results.

## Users Still the Weakest Link

Ransomware and phishing usually originate from outside the organization and involve some form of social engineering that convinces and co-opts the user into careless or dangerous behavior that allows the attacker to gain a foothold in the enterprise. Spearphishing emails, for example, nearly always originate from outside the organization, but they universally require some user action to be effective, making them as much an insider threat as an external threat.

As such, email security monitoring and enhanced security awareness training lead the list of controls that organizations use to protect against phishing and ransomware, whether in-house, through a cloud security provider or through a managed security service provider (MSSP). See Figure 6.

TAKEAWAY:

User education, endpoint monitoring, and access and configuration controls are essential in driving down the effectiveness of spearphishing attacks. In addition, all organizations should invest in training and periodic testing of users (a practice known as *inoculation*).

**What controls (tools and techniques) do you feel are most effective in specifically protecting against spearphishing and ransomware?**

***Indicate whether these protections are managed in-house, by a cloud provider/MSSP or both.***

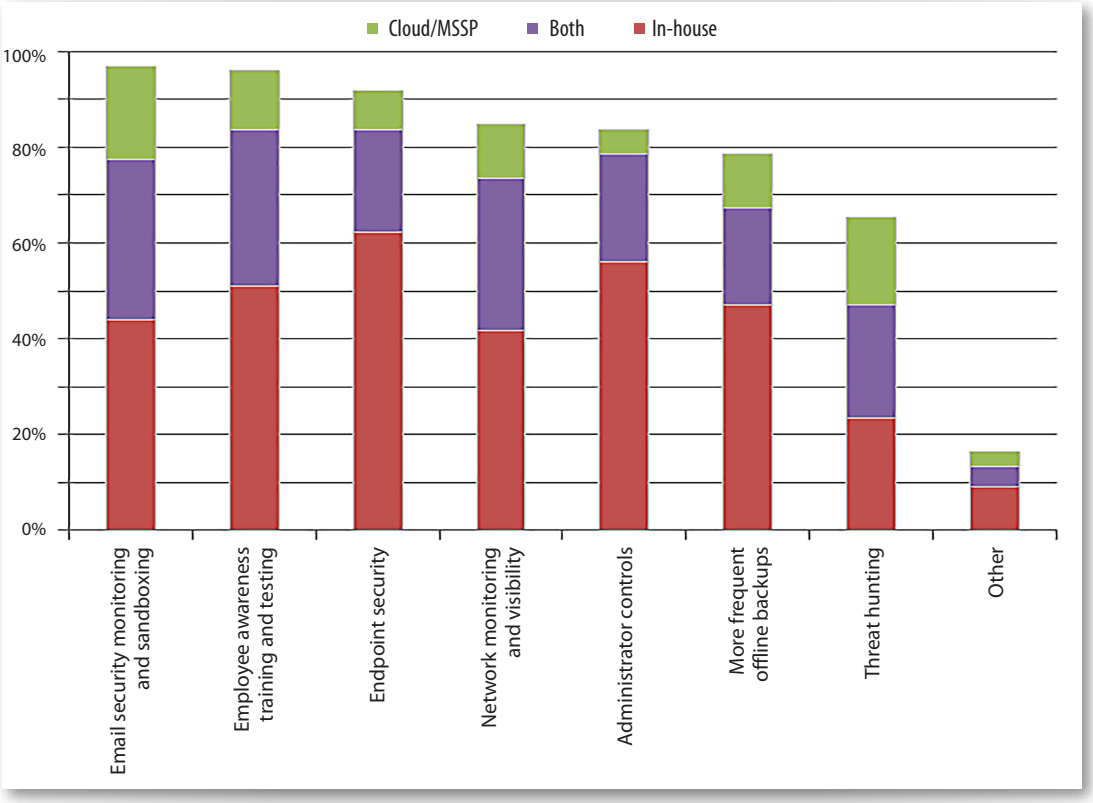



*Figure 6. Controls and Techniques to Combat Phishing and Ransomware*

## Future Vectors

Alternative payment systems are an industry disruptor that organizations need to address from a risk perspective. Although a few years ago technologies such as Apple Pay, Samsung Pay and other digital forms of payment did not exist, they are emerging in force today. Some researchers cited as much as a 6,000% increase in fraud in the first few weeks of Apple Pay, once thieves figured out how to exploit weak provisioning controls.[12]

In this survey, 29% of respondents indicated that their organizations utilize alternative payments, with 4% not knowing. Increased consumer demand for these services, gaining competitive advantage and gaining an approved, documentable security program from the provider are the top three demands organizations have before they want to adopt these systems. See Figure 7.

**What would have to occur to make alternative payment instruments more acceptable to your organization?** ***Select all that apply.***

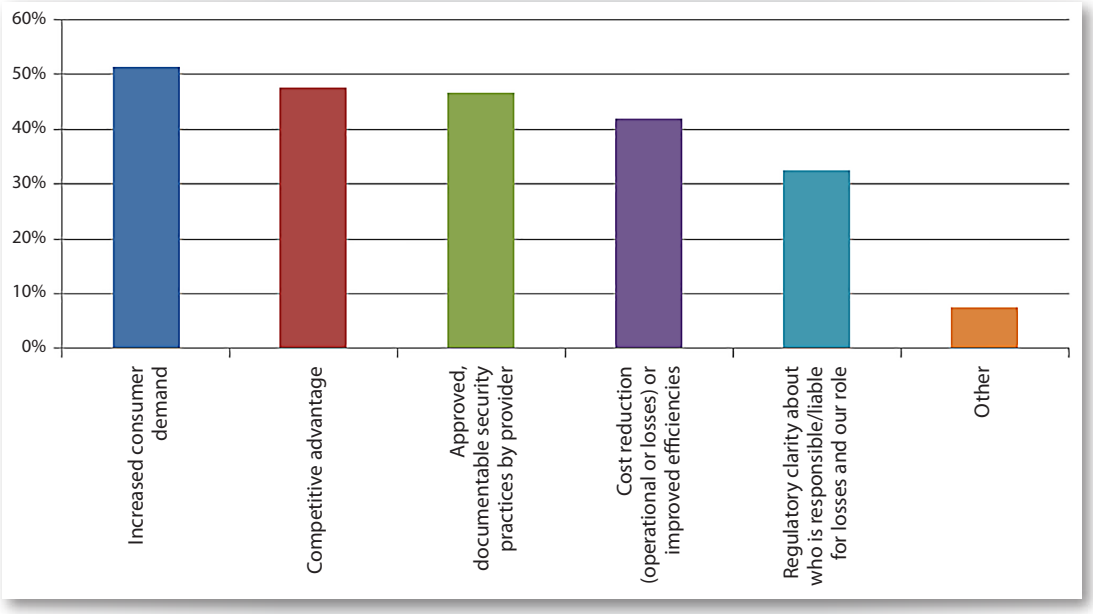



*Figure 7. Drivers of Alternate Payment System Adoption*

Ambiguity about responsibility and liability also act as a drag on innovation and implementation of such programs. Another concern may be surprises in technical security weaknesses that are exploitable by criminals.[13] IT security professionals will need to monitor developments in these technologies and their security profiles in the coming years.

[12] Cherian Abraham, "Rampant: Explaining the Current State of Apple Pay Fraud," 22 February 2015, accessed at www.droplabs.co/?p=1231

[13] Andrew Ross Sorkin, "Pointing Fingers in Apple Pay Fraud," 16 March 2015, accessed at www.nytimes.com/2015/03/17/business/banks-find-fraud-abounds-in-apple-pay.html?_r=0

## Quantification of Losses

When viewed in comparison to the financial resources being protected, the costs of most security countermeasures are miniscule. However, their positive impact can be tremendous in the event of a potentially serious breach.

Of those who reported experiencing the incidents, 73% quantified their losses or gains (in 5% of cases, their gains) resulting from impactful breaches over the past 12 months. In 2015, 41% could not quantify losses, while 35% didn't know whether they could, a significant improvement.[14]

TAKEAWAY:
Quantifying losses is important for a number of reasons—preparing insurance claims, meeting compliance-reporting criteria for breach notification and for justifying funding for improved countermeasures and increased security resources.

In our 2016 survey, 23% of losses fell under $10,000; however, 36% experienced losses over $100,000. Figure 8 shows detailed results for 2016 responses.

**For all significant incidents in the past 12 months combined, what was the overall financial cost to your organization?**

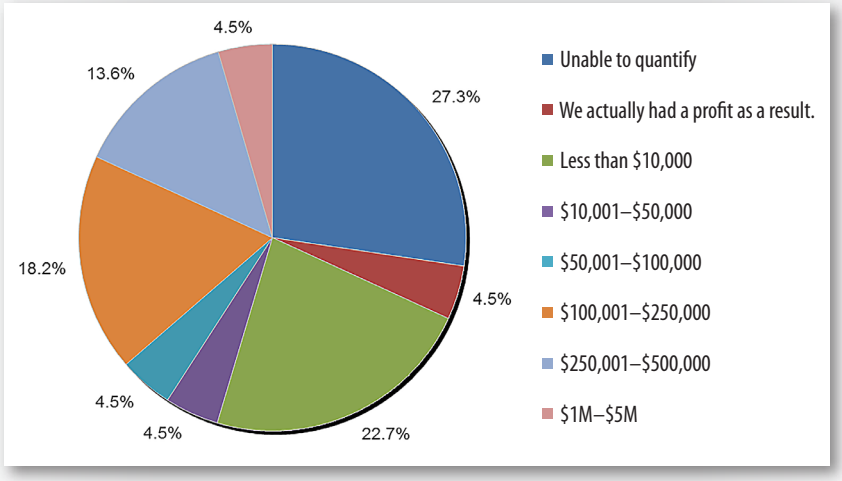



*Figure 8. Overall Financial Cost of Breach to Organization*[15]

The significant increase in ability to quantify losses (from 21% in 2014[16] to 73% over two years' time) suggests that valuable methodologies are working in many organizations.

[14] "Security Spending and Preparedness in the Financial Sector: A SANS Survey," www.sans.org/reading-room/whitepapers/analyst/security-spending-preparedness-financial-sector-survey-36032

[15] No respondents indicated incurring a cost of $500,000 to $1M or over $5M.

[16] "Risk, Loss and Security Spending in the Financial Sector: A SANS Survey," www.sans.org/reading-room/whitepapers/analyst/risk-loss-security-spending-financial-sector-survey-34690, Figure 6, p. 9.

## Assigning Risk

Methodologies vary, but assigning risk always starts with assessment: First determine the high-value targets for a cyber attacker, and then assess risk and apply countermeasures to protect high-value systems. Plan to invest significant time to develop and continually refine such a process. Some resources to get you started include:

- **The CIS Critical Security Controls, version 6.1.** Specifically, assessment and inventory of hardware and software, network controls, and management of servers and endpoint devices.[17]
- **COBIT (an acronym derived from Control Objectives for Information and Related Technology) Control Objective PO9.2: "Establishment of Risk Context."** Provides a means for establishing risk context based on the risk, value and guidance provided by its corresponding control practices.[18]
- **The National Institute of Standards and Technology's "Guide for Applying the Risk Management Framework [RMF] to Federal Information Systems."** Federally focused approach that can be applied to the financial industry starts by categorizing IT assets, then selecting, implementing and assessing security controls, authorizing the system for use, and monitoring the security controls.[19] Training is available on the RMF.[20]

[17] www.cisecurity.org/critical-controls.cfm [Registration required.]

[18] www.isaca.org/Groups/Professional-English/po9-2-establishment-of-risk-context/Pages/Overview.aspx

[19] http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[20] http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/rmf-training

## Impacts of Breaches

Of those that suffered a breach and could quantify their losses, 48% indicated that the incident resulted in unplanned and unbudgeted deployment of new technologies, while another 38% spent additional funding on augmenting their teams. Both expenditures are valuable if they result in improved processes and in reduced risk and number of breaches. See Figure 9.

**What was the outcome of your significant incidents?** ***Select all that apply.***

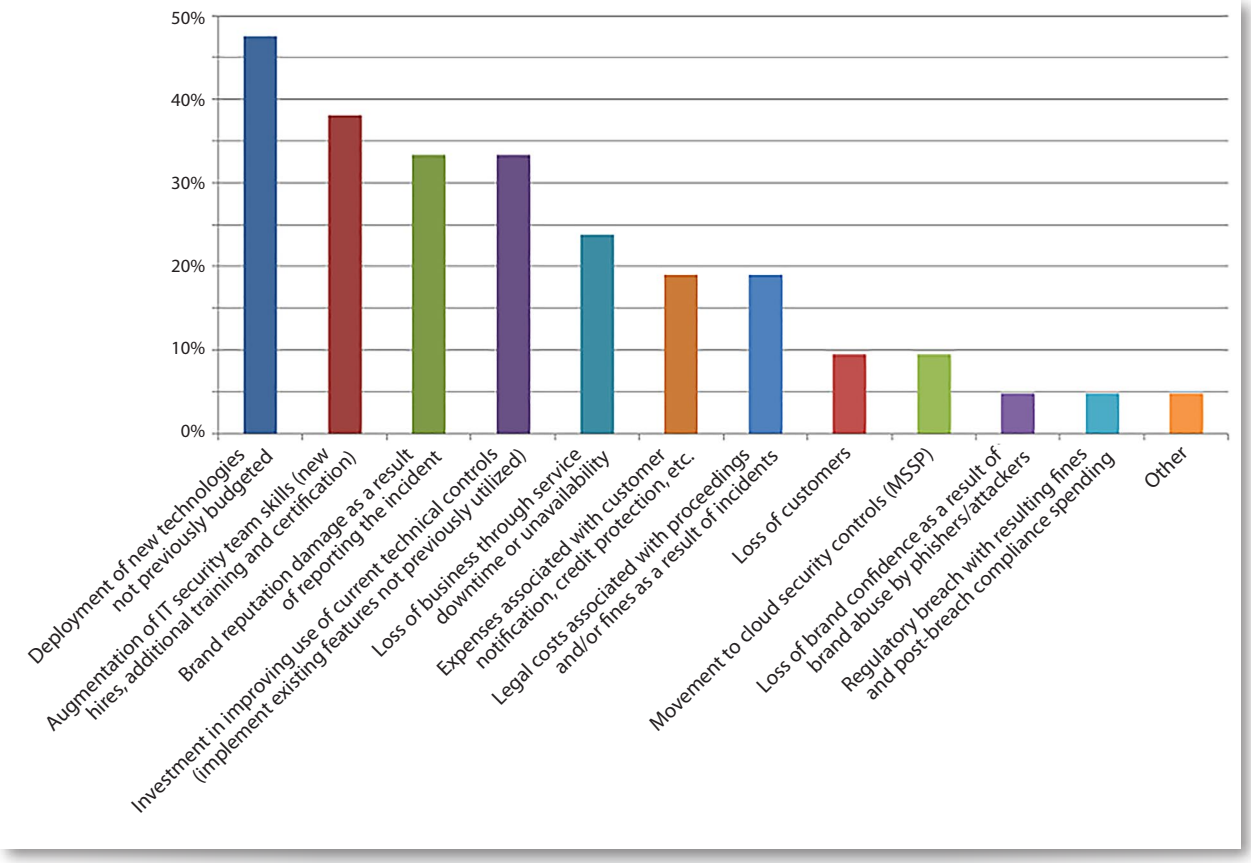



*Figure 9. Outcome of Significant Incidents*

### Higher Costs in Regulated Industries

According to the 2016 Ponemon Institute cost of a data breach report,[21] the average cost of a data breach in the U.S. was $158 per compromised record. In the financial industry, that cost was 40% higher—or $221 per record.

Real damage to brand affected 33% of respondents' organizations, which implies that complying with the law and reporting incidents can result in loss of brand reputation, which is why many businesses hesitate to report breaches. A smaller percentage (19%) incurred legal costs associated with proceedings and/or fines as a result of incidents.

Ironically, one of the most effective ways to protect sensitive information—encryption—is also a weapon adversaries use in their ransomware attack vectors. Although encrypted data is exempt from reporting requirements under most data-protection laws, new reporting guidelines for HIPAA and the Affordable Care Act[22] pertaining to ransomware attacks are a game-changer. Specifically, if personal health information (PHI) is encrypted by ransomware, it must be reported as a breach. The rationale is that if malware could access the information to encrypt it, it also could have exfiltrated it. That may not be the case, but in the absence of more specific rules addressing proof of containment (e.g., data loss prevention [DLP] logs), ransomware encrypting employee or patient data now counts as a privacy breach.

[21] "Ponemon Institute 2016 Cost of a Data Breach Study: Global Analysis," June 2016 [Registration required.]

[22] For a discussion of these changes, see www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

# Improving Risk Posture

Risk =
Threat x Vulnerability x Asset Impact

It's well known that the act of compliance doesn't make organizations more secure. Yet, 80% of respondents indicated that compliance efforts did, indeed, improve their overall risk posture, with 31% noting a "significant improvement."

The interesting question is: How does one value improvement in risk posture? Risk is a product of threat times vulnerability times asset impact, meaning risk is reduced if one of these factors is reduced. In this equation, vulnerabilities represent the vectors through which threats interact with assets.

The results illustrated in Figure 10 indicate that compliance represents an important part of the overall security and risk management program.


Percentage of organizations that indicated compliance efforts led to at least moderately improved overall risk posture

**To what extent have your compliance efforts improved your overall risk posture?**

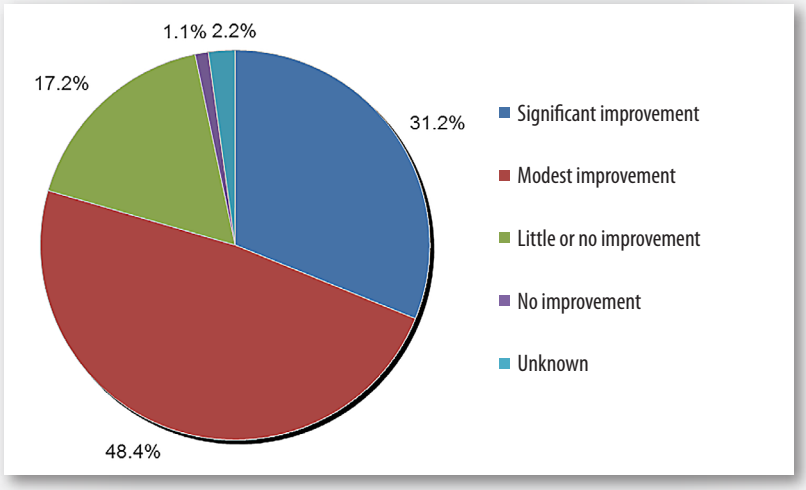



*Figure 10. Improvement in Risk Posture Attributed to Compliance Efforts*

Compliance seeks to reduce vulnerabilities, but it still does not equal security.

## Drivers for Programs

Protecting private and sensitive data from breach or exposure is one of the top three drivers for information security programs, as cited by 69% of respondents. Half of the respondents selected demonstrating compliance, while 43% are seeking to improve overall risk posture. The complete results are shown in Figure 11.

**What are the primary drivers behind your information security program?**
***Select your top three drivers, not in any specific order.***

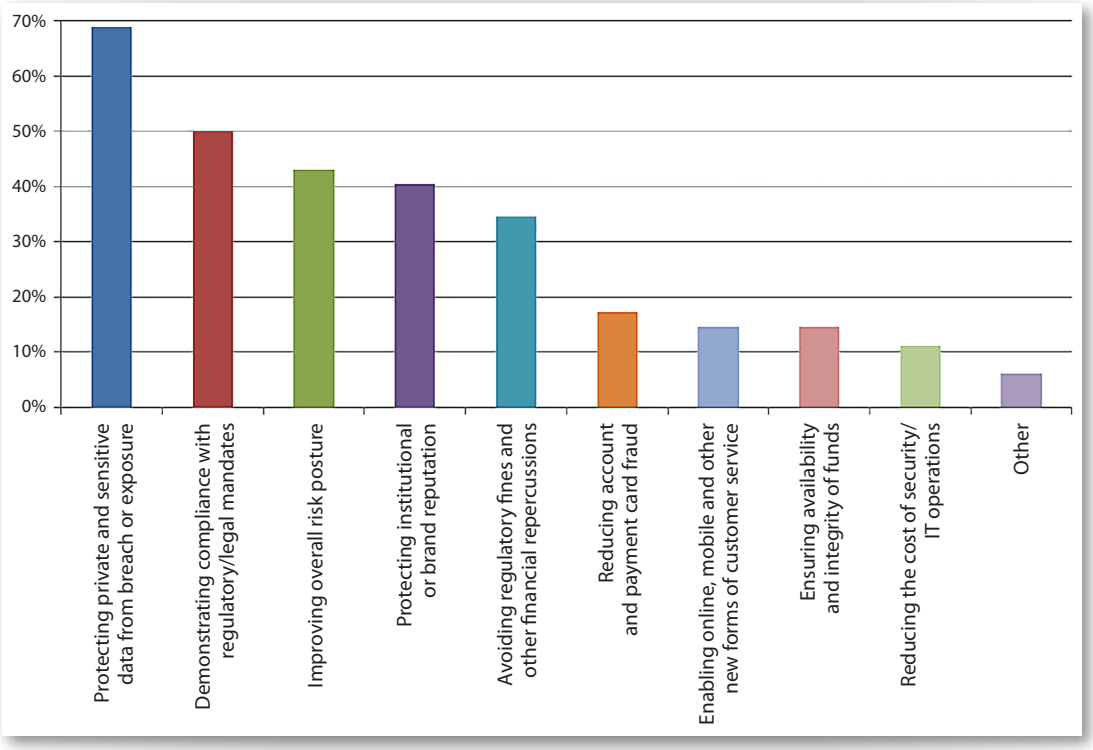



*Figure 11. Primary Drivers Behind Information Security Program*

TAKEAWAY:

Those that spend only to comply, rather than to improve security and risk posture, become the attackers' low-hanging fruit—ripe with targets of opportunity.

Protecting institutional or brand reputation (41%), and avoiding regulatory fines and other financial repercussions (35%) rounded out the top five. These results indicate that protecting data from breach or exposure may be competing for resources with meeting compliance mandates.

## Regulatory Compliance

Regardless, regulatory mandates are often a non-negotiable line item in security budgets, and this survey shows that financial institutions have multiple compliance mandates. The largest group, just over 50%, cited the Payment Card Industry Data Security Standard (PCI DSS), a requirement for processing credit cards, as a mandate they follow. Other key mandates included the Gramm-Leach-Bliley Act, the Financial Services Modernization Act of 1999 (GLBA, P.L. 106-102), selected by 44% of respondents, while 42% selected the Sarbanes-Oxley Act of 2002 (SOX, P.L. 107-204), a requirement for publicly traded companies.

TAKEAWAY:

Where there are multiple regulatory requirements, use frameworks and tools to manage, monitor and report across compliance rules, as well as to track efforts.

Approximately 41% adhere to Federal Financial Institutions Examination Council (FFIEC), 33% to the Bank Secrecy Act, and 30% to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, better known as the USA PATRIOT Act (P.L. 107-56).

As results show, the tangle of legal requirements for security compliance is complex—especially for the 39% who must also comply with a variety of state, regional and/or provincial laws. For example, 33% of respondents cited the Bank Secrecy Act, and 32% selected the Health Insurance Portability and Accountability Act of 1996 (HIPAA, P.L. 104-191), while 30% also cited the Financial Industry Regulatory Authority (FINRA).

The need to comply with multiple regulations is likely to get more complex in the years ahead. A recent check on the page for bills related to computer security and identity theft on GovTrack.us[23] revealed more than 200 different bills or resolutions before the current Congress as of this writing (up from 78 in the last Congress).

[23] www.govtrack.us/congress/bills/subjects/computer_security_and_identity_theft/5954

## Security Frameworks

Survey respondents also use a range of security frameworks and standards to help them meet compliance and security targets. These include:

- **ISO 27000 Series.** Used by 51%, the ISO 27000 Series,[24] published by the International Organization for Standardization (ISO), provides best-practice recommendations on security management in the context of an information security management system (ISMS.) Organizations seek ISO certification for a number of reasons, including contractual requirements, government regulation, corporate governance and supply chain pressure.[25]
- **PCI DSS.** The choice of 41% for securing card payments, PCI DSS includes a framework for securing payment card systems.
- **CIS Critical Security Controls.** Utilized by 37%, the critical controls are an industry-agnostic list of 20 practical technical controls that emphasize automation and closing the loop around inventory assessment, vulnerability management, security, response and repair/continuous improvement.[26] Adoption of the controls is up significantly from 17% two years ago.[27]
- **National Institute of Standards and Technology (NIST) Special Framework for Improving Critical Infrastructure Cybersecurity.** Used by 36%, this framework represents a very useful tool for organizing security efforts for protecting critical infrastructures. The Department of Homeland Security (DHS) has designated the financial services sector as one of 16 critical infrastructures for the U.S.[28]
- **COBIT.** Chosen by 32%, this business framework for the governance of enterprise IT is published by the Information Systems Audit and Control Association (ISACA).[29] The latest version, COBIT 5, has been in force more than three years and is available for download from ISACA for a fee.
- **Federal Information Security Management Act of 2002 (FISMA).** Used by 21%, is a government standard for continuous improvement, showing yet again the crossover between federal systems and financial systems.
- **NIST SP800-53.**[30] Selected by 20%, SP 800-53 addresses multitiered risk management, security control structure, baselines and designations, external service providers, and assurance and trustworthiness. It also includes a "Security Control Catalog" listing more than 200 pages of controls, enhancements and guidance.

[24] www.27000.org

[25] http://bhconsulting.ie/securitywatch/?p=953

[26] www.cisecurity.org/critical-controls.cfm [Registration required.]

[27] "Risk, Loss and Security Spending in the Financial Sector: A SANS Survey," www.sans.org/reading-room/whitepapers/analyst/risk-loss-security-spending-financial-sector-survey-34690, Figure 11, p. 16

[28] www.dhs.gov/critical-infrastructure-sectors

[29] www.isaca.org/COBIT/Pages/default.aspx

[30] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

## Prepared, but Not Very

Do these compliance mandates and frameworks make financial organizations more prepared to fend off attacks? The answer to that question is mixed.

The largest percentage (39%) felt "Prepared" to fend off attacks directed at their financial systems and accounts, while only 18% felt "Very Prepared." That may seem reasonable, but 42% felt only "Somewhat Prepared" or "Not Prepared" to fend off such attacks and 1% didn't know (see Figure 12).

**How prepared is your organization to fend off attacks aimed at gaining access to your financial systems and accounts?**

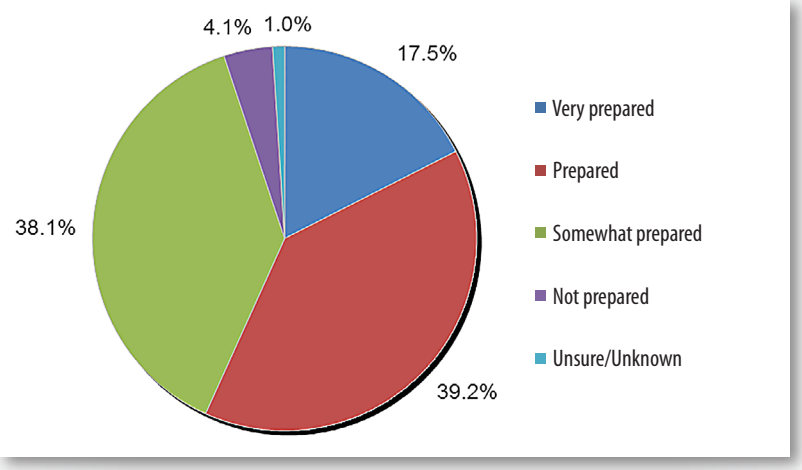



*Figure 12. Preparation to Fend Off Attacks*

Although this is a slight improvement over 2015,[31] when only 55% felt prepared or very prepared, organizations clearly need better tools and processes to reduce their risk and fend off such attacks.

[31] "Security Spending and Preparedness in the Financial Sector: A SAN Survey," www.sans.org/reading-room/whitepapers/analyst/security-spending-preparedness-financial-sector-survey-36032

## Effectiveness of Controls

Overall, advanced firewalls, IDS and IPS tied with endpoint protection for the most effective overall controls for mitigating risk, with 95% selecting that answer option. They also highly value employee awareness training and log management, with 93% selecting each. See Figure 13.

**What controls (tools and techniques) do you feel are most effective overall in protecting your organization?** ***Select all that apply and indicate whether the protections are managed in-house, by a cloud security provider/MSSP or both.***

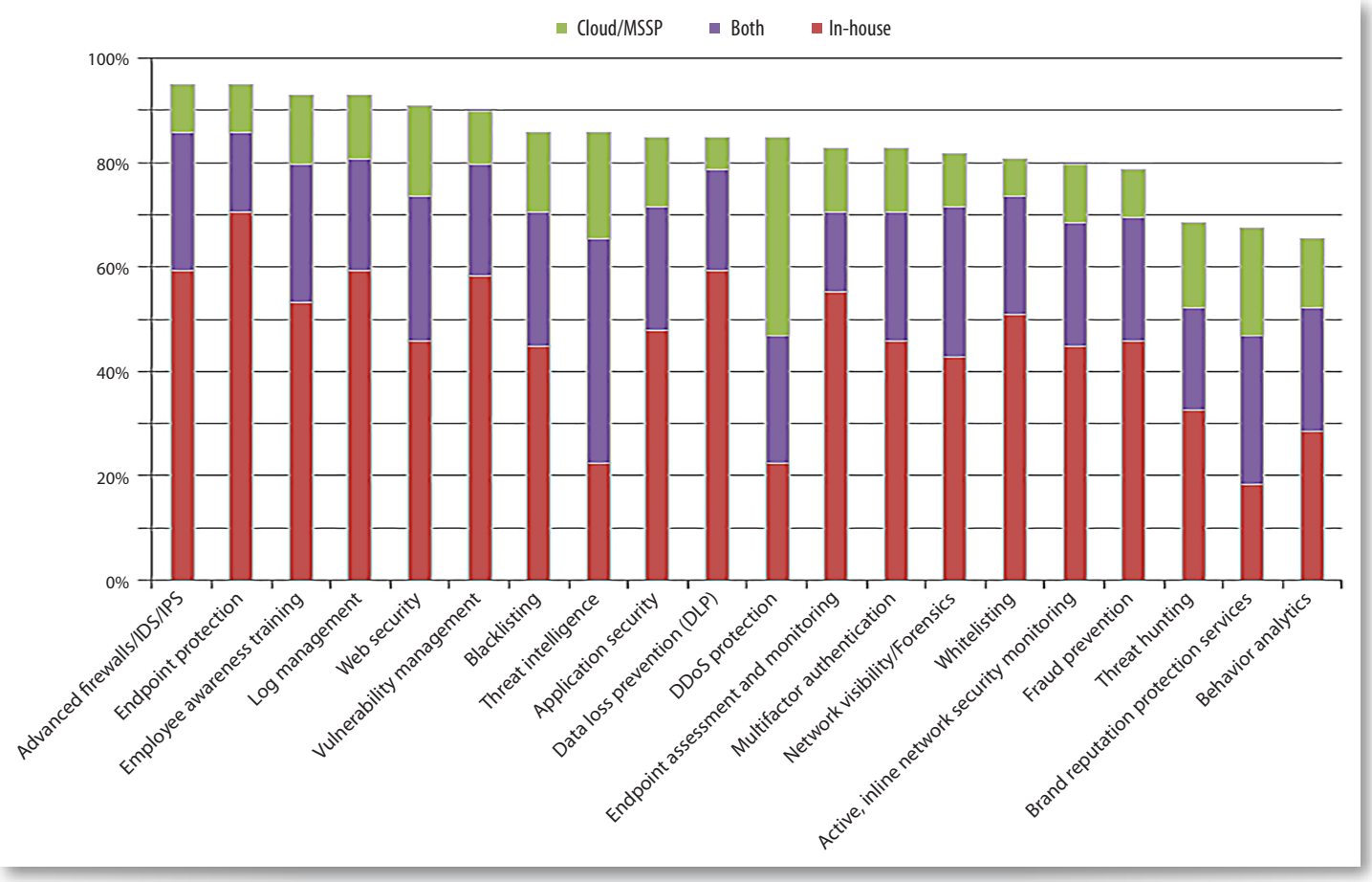



*Figure 13. Effectiveness of Controls Used In-House, in the Cloud or Both*

When evaluating in-house implementation only, the most effective controls included:

- Endpoint protection, 70%
- Advanced firewalls/IDS/IPS; Log management; and DLP, 59% each.
- Vulnerability management, 58%
- Endpoint assessment and monitoring, 55%

TAKEAWAY:
Only 22% evaluated in-house interpretation of threat intelligence as effective, suggesting that third-party resources may be needed.

Interestingly enough, only eight of the 20 in-house controls were deemed effective by more than 50% of respondents (see red bars in Figure 13.) Thus, organizations rely on cloud providers and MSSPs to improve the effectiveness of most technologies—in some cases significantly. For example, 22% of respondents evaluated threat intelligence and DDoS protection as effective in-house, but evaluations from all sources reached 86% and 85% effectiveness, respectively. Thus, "do-it-yourself" security solutions seem to leave quite a bit to be desired, requiring staff to configure, manage and verify the results so they can follow up on real threats rather than chasing false positives. Further, employees may not keep up with mastery of an increasing array of in-house tools. Considering the industrywide shortage of qualified security professionals, turning to third parties that can afford to attract and retain top talent may be a continuing trend as management accepts the fact that it cannot effectively defend its enterprise with organic assets.

## Visibility and Response

Investigations are an essential element of effective security management and provide a structured means for addressing security incidents. So, one would expect that most artifacts would be available to investigation teams, but the highest-ranked item, Windows Registry, was fully visible to only 45% of the respondents.

Endpoint sessions, user activity and network activities were the only others with significant visibility, where 40% said they had full visibility into these activities. Six areas also ranked above 50% in the partial visibility category, suggesting that some investigation teams are accessing some or most of the information they need to conduct investigations. It also shows they are hindered in their ability to diagnose and identify problems due to lack of primary forensic data. See Figure 14.

**During investigations, how much visibility do you have into the following areas?**

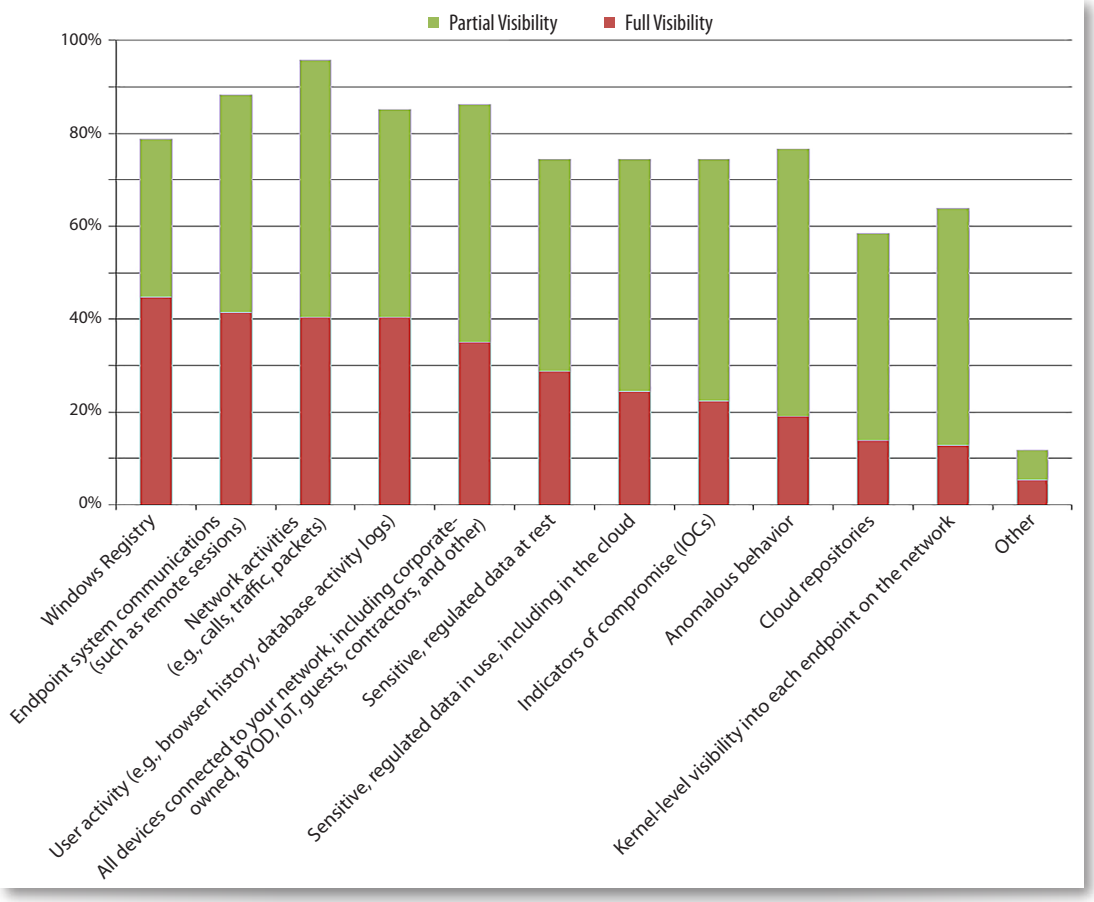



*Figure 14. Visibility into Systems and Assets*

TAKEAWAY:

Visibility continues to be an issue that IT security professionals must address to improve security of financial environments.

In general, some information is ALWAYS available (e.g., Windows Registry), unless a system is wiped completely clean. Other activities require some advance preparation (e.g., having scanners set to watch network traffic, for which 96% have full or partial visibility).

The cloud, unfortunately, represents a frontier into which organizations have yet to gain any helpful level of visibility. In our survey, only 14% had full visibility into cloud repositories, and 32% of respondents reported no visibility. And, despite their emphasis on endpoint controls, 31% had no kernel-level visibility into endpoints.

## Information Sharing

One way to improve visibility is through shared intelligence. A number of resources are available for sharing threat, vulnerability and remediation information, and it's clear from our survey responses that financial organizations are using them.

In the survey, 43% of respondents say someone in their organizations belongs to local or regional peer groups, and 41% utilize the FSISAC (Financial Services Information Sharing and Analysis Center). The same number also utilize US-CERT (United States Computer Emergency Response Team) or other regional CERTs for new threat information. In addition, 40% participate in InfraGard,[32] a partnership between the FBI and the private sector involving people from business, education, law enforcement and other areas sharing information to prevent hostile acts.

Educational or training groups and boards are used by 34%, FFIEC (Federal Financial Institutions Examination Council) by 28%, and 24% utilize communication channels established through vendor partners. Note that the FICO [Fair Isaac Corporation] Fraud Alert Network[33] is an "invitation only" site that allows for the liberal exchange of threat intelligence among financial organizations.

Educational groups are a great place to share security intelligence information. It is from many groups like this, including the FS-ISAC, that participating members learn of advanced attacks.

However, exchanging ideas is not enough. Defense improves dramatically when targets can share intelligence and reconfigure dynamically to block active threats. This "back plane" can exist either among groups or through innovative applications that adapt in real time. Automating information sharing may be one area in which IT groups decide to increase spending from 2016 to 2017.

[32] www.infragard.org

[33] https://community.fico.com

## Improvements Possible

There were 69 write-in responses to the question about what would improve ability for innovation. Seventeen mentioned education or training in some form, and eight cited user awareness training as being particularly important. Some ideas presented include:

- "Less encryption and more tokenization" (meaning that information can be viewed and analyzed without violating PCI-DSS or other security requirements)
- "Adoption of cloud security controls" (Does the cloud service provider not offer them, or are they available only for an additional fee?)
- Configuring existing technologies by emphasizing the CIS Critical Security Controls (CSCs)[34] before purchasing new technology

Some recommendations from an organizational perspective include better integration of IT and information security into business strategy and planning; implementing a strategic plan for governance, risk and compliance (GRC); and changing the bank's culture.

Finally, a few respondents cited limited staffing or gaps in personnel and the need for existing staff to acquire additional skills, while others wanted a move from in-house to managed service providers for some security services. This suggests that each organization has unique requirements, and no "one-size-fits-all" solution is possible with respect to staffing or oversight.

[34] "CIS Critical Security Controls," www.cisecurity.org/critical-controls.cfm [Registration required.]

# Conclusion

Results indicate that those working in the trenches of IT security and response need more resources, awareness and tools to protect and store their clients' money. They need to work closely with their physical security departments and their business units, and to evaluate thoroughly the risks of new payment programs such as Apple Pay or Samsung Pay before implementing them for customers.

More important, all financial organizations should continually work to improve their security, risk management and response capabilities, whether the solutions are internal staffing or turning to a growing array of services. Ultimately, they need visibility into threats and vulnerabilities across their environments, particularly with regard to their users, who are activating ransomware and falling victim to targeted phishing attacks.

Organizations partially address these and other issues with tools and processes. However, ongoing learning, information and intelligence sharing, as well as improving overall risk posture, will be key issues that IT security teams must face sooner rather than later.

# About the Authoring Team

**G. Mark Hardy**, SANS analyst and certified instructor, is an internationally recognized expert in information security planning and policy development, management of security assessment and penetration teams, data encryption and authentication, software development and strategic planning for e-commerce. He has spoken at more than 250 events worldwide and has served government, military and commercial clients for more than 30 years. Founder of National Security Corporation and CardKill, Inc., G. Mark is a retired U.S. Navy Captain whose credentials include bachelor's degrees in computer science and mathematics, master's degrees in business administration and strategic studies, and the GSLC, CISSP, CISM and CISA certifications.

**Stephen Northcutt** founded the GIAC certification and served as the founding president of the SANS Technology Institute, an accredited graduate school focused on cyber security. He maintains the SANS Leadership Laboratory, leads the Management 512 Alumni Forum and is the lead author/instructor for a variety of SANS Institute courses. Stephen is the author/co-author of *Incident Handling Step-by-Step*, *Intrusion Signatures and Analysis*, *Inside Network Perimeter Security (2nd Edition)*, *IT Ethics Handbook*, and *Network Intrusion Detection (3rd Edition)*. He was the original author of the Shadow intrusion detection system before accepting the position of chief for information warfare at the Ballistic Missile Defense Organization.

**Matt Bromiley**, a SANS GIAC Advisory Board member who holds the GCFA and GNFA certifications, is an up-and-coming forensics instructor. A senior consultant at a major incident response and forensic analysis company, he has experience in digital forensics, incident response/triage and log analytics. His skills include disk, database and network forensics, as well as memory analysis and network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, sharing with others and working on open source tools.

# Sponsors

*SANS would like to thank its sponsors:*

ARBOR NETWORKS

ForeScout

GUIDANCE SOFTWARE

NSFOCUS

WhiteHat SECURITY

Last Updated: October 27th, 2016

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Sydney 2016 | Sydney, AU | Nov 03, 2016 - Nov 19, 2016 | Live Event |
| SANS Gulf Region 2016 | Dubai, AE | Nov 05, 2016 - Nov 17, 2016 | Live Event |
| DEV534: Secure DevOps | Nashville, TNUS | Nov 07, 2016 - Nov 08, 2016 | Live Event |
| SANS Miami 2016 | Miami, FLUS | Nov 07, 2016 - Nov 12, 2016 | Live Event |
| DEV531: Defending Mobile Apps | Nashville, TNUS | Nov 09, 2016 - Nov 10, 2016 | Live Event |
| European Security Awareness Summit | London, GB | Nov 09, 2016 - Nov 11, 2016 | Live Event |
| SANS London 2016 | London, GB | Nov 12, 2016 - Nov 21, 2016 | Live Event |
| Healthcare CyberSecurity Summit & Training | Houston, TXUS | Nov 14, 2016 - Nov 21, 2016 | Live Event |
| SANS San Francisco 2016 | San Francisco, CAUS | Nov 27, 2016 - Dec 02, 2016 | Live Event |
| SANS Hyderabad 2016 | Hyderabad, IN | Nov 28, 2016 - Dec 10, 2016 | Live Event |
| MGT517 - Managing Security Ops | Washington, DCUS | Nov 28, 2016 - Dec 02, 2016 | Live Event |
| ICS410 @ Delhi | New Delhi, IN | Dec 05, 2016 - Dec 09, 2016 | Live Event |
| SANS Cologne | Cologne, DE | Dec 05, 2016 - Dec 10, 2016 | Live Event |
| SANS Dublin | Dublin, IE | Dec 05, 2016 - Dec 10, 2016 | Live Event |
| SEC560 @ SANS Seoul 2016 | Seoul, KR | Dec 05, 2016 - Dec 10, 2016 | Live Event |
| SANS Cyber Defense Initiative 2016 | Washington, DCUS | Dec 10, 2016 - Dec 17, 2016 | Live Event |
| SANS Frankfurt 2016 | Frankfurt, DE | Dec 12, 2016 - Dec 17, 2016 | Live Event |
| SANS Amsterdam 2016 | Amsterdam, NL | Dec 12, 2016 - Dec 17, 2016 | Live Event |
| SANS Security East 2017 | New Orleans, LAUS | Jan 09, 2017 - Jan 14, 2017 | Live Event |
| SANS Brussels Winter 2017 | Brussels, BE | Jan 16, 2017 - Jan 21, 2017 | Live Event |
| Cloud Security Summit | San Francisco, CAUS | Jan 17, 2017 - Jan 19, 2017 | Live Event |
| SANS Las Vegas 2017 | Las Vegas, NVUS | Jan 23, 2017 - Jan 30, 2017 | Live Event |
| Cyber Threat Intelligence Summit & Training | Arlington, VAUS | Jan 25, 2017 - Feb 01, 2017 | Live Event |
| Pen Test HackFest Summit & Training | OnlineVAUS | Nov 02, 2016 - Nov 09, 2016 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |