Risk, Loss and Security Spending in the Financial Sector: A SANS Survey

Copyright SANS Institute
Author Retains Full Rights
Risk, Loss and Security Spending in the Financial Sector: A SANS Survey

A SANS Analyst Survey

Written by G. Mark Hardy
Advisor: John Pescatore

March 2014

Sponsored by
Blue Coat, FireEye, ForeScout, Raytheon, Sourcefire and Tenable Network Security

©2014 SANS™ Institute
Introduction

Financial institutions are struggling with internal threats, the means to protect financial accounts from spearphishing and other endpoint attacks, and lack of resources, according to the SANS Financial Services Security Survey.

The purpose of this nonscientific survey was to understand the drivers for security-related spending in the financial services industry. We also wanted to identify the techniques organizations are adopting to mitigate threats associated with an ever-expanding threat landscape. In this survey, SANS identified key areas in which employees and endpoints were most at risk, with direct losses resulting from internal abuse, spearphishing and botnet infections.

Respondents also reported a lack of visibility into their losses and a need for more resources to manage risk in their environments.

Resources and resource planning are critical for security managers and incident responders. Attackers are constantly adapting their tactics based on what works and will drop ineffective efforts to try new, unanticipated techniques. On the other hand, for IT professionals, mitigation is cost driven, which, in turn, requires quantification of the cost of the risk in order to procure resources for protection. Unfortunately, as survey results show, mitigation can be as formidable of a challenge as identifying the risks.

But the news is not all bad. The outlook for increased budgets to address security concerns is good. Smaller IT security budgets (from 1–3% of IT spending) are on the decline—this was the budget range for 21% of respondents in their previous fiscal year (FY), 15% for the current FY budgets and only 11% in the next FY, an overall improvement of 10%. Meanwhile, security spending (from 11%–25%) is on the rise—from 7% in the previous FY to 13% in the current FY and to 15% in the next FY.

These and other findings will be discussed more fully in the following pages.

Internal Threats to Accounts

Survey respondents reported the most losses resulting from the following types of attacks:
- Abuse or misuse by internal employees or contractors (43%)
- Spearphishing emails (43%)
- Malware or botnet infections (42%)

Of those who suffered a breach, 44% of respondents experienced “Direct losses against impacted financial accounts.”

Lack of Visibility, Resources

- Only 16% felt very prepared to fend off intrusions aimed at financial accounts.
- Of those who have detected intrusions, quantification of losses is a major challenge. Only 21% of all respondents could quantify losses that occur as a result of attacks.
- Approximately 36% of the respondents who were breached experienced denial of service resulting in lost business.
- A similar proportion (36%) cited regulatory or legal issues as a result of an incident.
- Some 32% spend 25% or more of their security budget on meeting or providing compliance mandates.
About the Participants

The 293 professionals who took this survey between January and February 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, as important, what's not working and what could use improvement.

Participating Organizations

The greatest number of survey respondents (38%) came from the retail or commercial banking sector. Just over 24% work in other financial industry segments. See Figure 1.

The distribution of industry categories is about what we expected. The large number of “Other” participants (38%) includes the following, in descending order:

- Consultants
- Government agencies
- Financial services firms (supporting financial organizations)
- Insurance companies
- Investment fund and pension management firms
- Health care organizations
- Mortgage and loan services companies
- Legal firms

Figure 1. Respondent Industry Representation
What this tells us is that multiple industries are dealing with financial applications in their environments. For example, health care billing departments and government agencies accept payments from the public. Others are managing their ACH accounts—their internal clearinghouse accounts—which are also primary targets of spearphishing attacks. This cross-section of government agencies and businesses also provides an extended view of security with respect to the financial systems they’re protecting and the types of countermeasures in use.

**Wide Range of Organizational Sizes**

The survey targeted IT professionals across a wide range of organizational sizes. Nearly 31% came from workforces greater than 10,000 people, while on the opposite end, 44% came from workforces less than 1,000, as shown in Figure 2.

Smaller organizations are most likely consulting, legal and other entities serving financial clients, whereas the distribution across sizes greater than 1,000 suggests a mix of local, regional and national financial institutions, as well as government agencies.
International Representation

Although a large majority (71%) of respondents indicated that they operate in the United States, many also operate in other countries or regions, as illustrated in Figure 3.

Most of the respondents (73%) were from organizations headquartered in the United States, and 13% were based in Europe, as shown in Figure 4.

1 Note that percentages do not add up to 100% because respondents were allowed to select all countries or region in which they operated.
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 being considered 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.

Roles and Responsibilities

Responses to the survey came from a wide cross-section of roles and positions within participating organizations, which breaks down to a near equal mix of administrative-level and managerial-level professionals, as shown in Figure 5.

Global Banking Systems

The United States has a large number of independent banks within its borders. According to the Federal Deposit Insurance Corporation (FDIC), there are 6,891 FDIC-insured banks in the U.S. today,\(^2\) down from over 18,000 30 years ago.\(^3\) This is more than the entire European Union combined (5,846).\(^4\) In the United Kingdom, there are only 40 domestic banks\(^5\) and just 29 in Canada.\(^6\)

The Bankers Almanac identifies four of the top five largest banks in the world as European and four of the top ten largest banks in the world as Chinese.\(^7\) The largest U.S. banks, JPMorgan Chase and Bank of America, are numbers 12 and 18 in the world, respectively.

---


\(^3\) [http://online.wsj.com/news/articles/SB10001424052702304579404579232343313671258?mod=ITP_pageone_0](http://online.wsj.com/news/articles/SB10001424052702304579404579232343313671258?mod=ITP_pageone_0) (Note: Subscription required for access.)


\(^7\) [www.accuity.com/useful-links/bank-rankings](http://www.accuity.com/useful-links/bank-rankings)
Just over 29% of respondents identified themselves as CIO, IT manager or director (12%) or CSO, CISO, IT security manager or director (17%). An additional 29% identified themselves as either a security analyst (27%) or a forensics analyst (2%). Respondents choosing “Other” (12%) included consultant and security engineer, as well as chief privacy officer and e-commerce director.

This wide sampling of different perspectives and levels of responsibility for financial security is very important in that it provides viewpoints from nearly all positions directly associated with financial security. This diversity means that survey responses include answers to questions where management may see issues differently from nonmanagement positions.
Most attacks start from within, either through abuse or misuse—or by employees falling victim to spearphishing emails. Malware, botnets and vulnerable unpatched or misconfigured devices are other effective attack vectors.

**Endpoints and Insiders**

We asked participants to rank the top three most prevalent causes of security incidents in their organizations. Interestingly, three items were statistically more prevalent than others:

- Abuse or misuse by internal employees or contractors (43%)
- Spearphishing emails (43%)
- Malware or botnet infections (42%)

These numbers support the school of thought that insider threats can cause the greatest damage. They also show that even a nonmalicious insider can be a threat by means of drive-by infection or an attacker spearphishing them into giving away access to protected systems or even Automated Clearing House (ACH) account information.¹⁸

Spearphishing emails almost 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. User education and endpoint monitoring, 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*).

We found it interesting that exploits against unpatched/misconfigured devices were a somewhat distant fourth (24%) among their concerns. The Critical Security Controls (CSCs)⁹ recommend continuous vulnerability assessment and remediation for all endpoints, servers and critical systems as an effective means to identify and rectify endpoint compliance issues. Either these organizations are all well configured, or they are not making this the priority it needs to be.

---

¹⁸ Useful online resources for ACH fraud prevention here: https://treasuryinsights.wellsfargotreasury.com/?elqPURLPage=1587

⁹ www.sans.org/critical-security-controls
See Table 1 for the top security incidents respondents selected.

<table>
<thead>
<tr>
<th>Causes</th>
<th>Rank 1</th>
<th>Rank 2</th>
<th>Rank 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abuse or misuse by internal employees or contractors</td>
<td>23%</td>
<td>12%</td>
<td>9%</td>
</tr>
<tr>
<td>Spearphishing emails</td>
<td>16%</td>
<td>16%</td>
<td>11%</td>
</tr>
<tr>
<td>Malware/botnet infections</td>
<td>16%</td>
<td>15%</td>
<td>11%</td>
</tr>
<tr>
<td>Exploits on unpatched/misconfigured systems and devices</td>
<td>8%</td>
<td>7%</td>
<td>9%</td>
</tr>
<tr>
<td>Lost devices (laptops/phones)</td>
<td>7%</td>
<td>6%</td>
<td>10%</td>
</tr>
<tr>
<td>Denial of service attacks</td>
<td>7%</td>
<td>9%</td>
<td>6%</td>
</tr>
<tr>
<td>Web application attacks (SQL Injection, XSS, XSRF)</td>
<td>4%</td>
<td>6%</td>
<td>6%</td>
</tr>
<tr>
<td>Advanced targeted attacks (APTs)</td>
<td>4%</td>
<td>6%</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
<td>4%</td>
<td>6%</td>
</tr>
<tr>
<td>Employee-owned devices (BYOD)</td>
<td>3%</td>
<td>3%</td>
<td>7%</td>
</tr>
<tr>
<td>Attacks on financial processing systems and databases</td>
<td>2%</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>Password exploitation</td>
<td>2%</td>
<td>2%</td>
<td>6%</td>
</tr>
<tr>
<td>Partner access exploitations</td>
<td>1%</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>Attacks on collaboration (data sharing) applications</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Despite the reports and fear around employee-owned device risks, bring your own device (BYOD) was cited only rarely as a top cause of security incidents.

A recent SANS Survey on BYOD\(^\text{10}\) suggests that many organizations are allowing BYOD, although not many employees per organization actually use their own devices for work. This implies that the low level of concern on this survey may be either because responding organizations are not allowing very many employees to use their own devices at this time or that the methods to defend against this new attack vector are not yet a core competency and attacks are not yet being detected. More employees will demand use of their own devices for business applications, and many may already be using these devices for tasks like email without the knowledge of their IT departments. Before implementing BYOD policies, organizations must ensure they can protect themselves from emerging threats in this space.

\(^{10}\) www.sans.org/reading-room/analysts-program/fear-loathing-byod-survey
Quantification of Losses

One of the challenges facing security professionals is developing cost-justification criteria for investing in countermeasures. Imagine hearing this statement: “Last year we gave you money for security, and nothing happened. Why should we give you more next year?”

“Well . . . because nothing happened.”

Security managers face difficulties in demonstrating a link between expenditures and savings, so return on investment (ROI) may not be a valid metric.

Rather, organizations should consider using a cost-avoidance metric. The savings are huge when the cost of a breach and the cost of prevention are compared. But organizations need to be able to quantify losses when they do occur.

Of those who reported experiencing the incidents (as detailed in Table 1), close to 80% of respondents either cannot quantify losses from attacks or do not know if their organizations can quantify them (see Figure 6).

![Figure 6. Ability to Quantify Losses with Attacks](chart.png)
Why are losses so difficult to quantify?

There are multiple aspects of risk, each with its own loss indicator: financial, legal, reputation and regulatory. In some cases the impact of a breach may not be fully quantified for months or even years due to inadequate and incomplete remediation, delays in discovering intrusions, brand erosion or slow-moving litigation.

There are references available that offer methodologies to begin formalizing a risk or loss measurement process, including some at the SANS Reading Room website.¹¹

Impacts on Financial Accounts and Services

Of those who suffered a breach and who could quantify their losses, 44% admitted to suffering “Direct losses against impacted financial accounts.” An additional 36% of respondents experienced denial of service resulting in lost business. A similar proportion cited regulatory or legal issues as a result of an incident.

Account breaches resulted in significant costs to the business and its impacted partners. According to the most recent Ponemon Institute cost of a data breach report,¹⁵ the average cost of a data breach in the U.S. was $188 per compromised record. In the financial industry, that cost was 14% higher—or $215 per record.

References and Methodologies for Assigning Risk

First determine the high-value targets for a cyber attacker and then enable the ongoing defense of those systems and endpoint targets through more secure processes.

This involves several key steps included in the CSCs, including assessment and inventory of hardware and software, network controls, and management of servers and endpoint devices.¹²

The COBIT (an acronym derived from Control Objectives for Information and Related Technology) framework includes a control objective for “establishment of risk context.”¹³

Federal government IT professionals can consult The National Institute of Standards and Technology’s “Guide for Applying the Risk Management Framework to Federal Information Systems.”¹⁴ That approach starts by categorizing IT assets, then selecting, implementing and assessing security controls, authorizing the system for use, and monitoring the security controls.

It will take time to develop such a process, which will also need continual refinement over time.

¹¹ www.sans.org/reading-room/whitepapers/leadership/quantifying-business-information-security-33149
¹² www.sans.org/critical-security-controls
¹³ www.isaca.org/Groups/Professional-English/po9-2-establishment-of-risk-context/Pages/Overview.aspx
See Figure 7 for detailed results concerning the outcome of incidents.

In our survey 26% of respondents reported damage to brand reputation simply as a result of reporting the incident. This implies that complying with the law can result in loss of brand reputation, which is a common reason businesses hesitate in reporting breaches. A smaller percentage (16%) indicated that their brand was damaged as a result of subsequent spearphishing attacks on their customers.

One way to reduce such losses would be to encrypt all sensitive data in storage, in transit and on endpoints, including mobile endpoints. With most data-protection laws, encrypted data is exempt from reporting requirements. And it would be much more difficult for attackers to use stolen data to launch spearphishing attacks if the data were encrypted in all phases. Sophisticated attackers will not target data at rest or data in motion, but data in use. So in addition to encryption, strict controls on operating environments, robust patch management and whitelisting are technologies that can reduce this dangerous vulnerability.
Almost 16% of respondents say they are spending more than 50% of their security budgets on compliance. The same percentage (16%) say they spend 26%–50% on compliance, as shown in Figure 8.

Yet compliance does not ensure security—compliant systems are hacked all the time. Compliance represents a minimum standard, and organizations with the best security programs far exceed these minimums. Yet the law is often inflexible, requiring a diversion of scarce security dollars away from meaningful countermeasures and into generating compliance reports.

Compliance and avoiding breaches are the largest drivers for IT security, with 69% saying that demonstrating regulatory compliance and avoiding data breaches are their top priorities. A majority also cited reducing risk (64%) and improving overall risk posture (51%) as program drivers. In this answer set, respondents were able to select all drivers that apply. The complete results are presented in Figure 9.
From these results it’s clear that reducing data breaches and risk is competing for resources with meeting compliance mandates. This is worrisome because organizations cannot “graduate” from compliance reporting and redirect funds toward where they need to be to improve defenses. Recall, 51% cited protecting institutional or brand reputation as a driver, which is closely tied with the cost of reporting a breach and following compliance mandates.

Savvy security managers need to convince management that investments in cybersecurity will address many, if not all, of those concerns—reducing risk, protecting against breaches, providing quick response capabilities, reducing costs and demonstrating compliance. Organizations need tools and resources that reduce the time and effort to achieve these goals, while providing ongoing monitoring and remediation for new risks and compliance violations that arise.
Compliance with Multiple Regulations

Most organizations are complying with multiple mandates, which could also explain why so much of their budgets are being spent on compliance. Maintaining these compliance requirements requires automated tools to help identify overlaps in compliance reporting requirements as they monitor against multiple frameworks. See Figure 10 for the list of mandates respondents comply with.

Payment Card Industry Data Security Standard (PCI DSS), a requirement for processing credit cards, was cited by 50% of respondents as a mandate they adhered to. Other key mandates included Sarbanes-Oxley Act of 2002 (SOX, P.L. 107-204), a requirement for publicly traded companies (49%), and Gramm-Leach-Bliley Act, the Financial Services Modernization Act of 1999 (GLBA, P.L. 106-102; 47%), a requirement for financial institutions.

What security regulations and mandates does your organization adhere to?
Select those that most apply.
Approximately 37% adhere to the Bank Secrecy Act, 35% to Federal Financial Institutions Examination Council (FFIEC) and 32% 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).

The tangle of legal requirements for security compliance is complex—especially for the 44% who must also comply with a variety of state, regional and/or provincial laws. For example, many respondents cited the Health Insurance Portability and Accountability Act of 1996 (HIPAA, P.L. 104-191), the National Credit Union Administration (NCUA) mandates and the Family Educational Rights and Privacy Act of 1974 (FERPA, 34 CFR 99) in the “Other” category.

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\textsuperscript{16} revealed 78 different bills or resolutions before the current Congress.

**Security Frameworks**

Survey respondents also use a range of security frameworks and standards. The top two (49% each) were the ISO 27000 Series and PCI DSS for securing card payments. The ISO 27000 Series,\textsuperscript{17} 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). Previously known as ISO 17799, this was derived from the British Standard (BS) 7799. Organizations seek ISO certification for a number of reasons, including contractual requirements, government regulation, corporate governance and supply chain pressure.\textsuperscript{18}

\textsuperscript{16} \url{www.govtrack.us/congress/bills/subjects/computer_security_and_identity_theft/5954}
\textsuperscript{17} \url{www.27000.org}
\textsuperscript{18} \url{http://bhconsulting.ie/securitywatch/?p=953}
Credit card processors require card issuers and merchant banks to be compliant with PCI DSS as well as to use only service providers that also demonstrate compliance. In November 2013, the PCI Security Standards Council released PCI DSS version 3.0. Another common security framework is COBIT. Published by the Information Systems Audit and Control Association (ISACA), it is a business framework for the governance and management of enterprise IT. The latest version, COBIT 5, was issued in May 2013 and can be downloaded from ISACA for a fee.

Interestingly, although this is a financial services survey, respondents also selected federal agency guidelines they were following. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 is written to provide standards for federal information systems to comply with the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. 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. Note that although 25% of respondents indicated they adhere to NIST SP800-53, which was designed to facilitate FISMA compliance, only 17% of respondents cited a FISMA compliance requirement.

See Figure 11 for a look at the security frameworks commonly used by our survey takers.

19 www.pcisecuritystandards.org
20 www.isaca.org/COBIT/Pages/default.aspx
The “right” framework from a compliance perspective is the one that leads to the greatest degree of overlapping mandated compliance for an organization. The ISO 27000 series\(^\text{23}\) is a family of standards that is recognized internationally. Although they may represent best practice, they are not a panacea for compliance reporting.

Many organizations are also adopting the CSCs to augment FISMA, Sarbanes-Oxley and other requirements.\(^\text{24}\) According to the SANS 2013 survey on the CSCs, 17% of respondents represented the financial industry (just 3% shy of the 20% representing government agencies).\(^\text{25}\)

**Prepared, but Not Very**

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

The majority (42%) felt “Prepared” to fend off attacks directed at their financial systems and accounts, while only 16% felt “Very prepared.” That may seem reasonable, but the other 39% felt only “Somewhat prepared” or “Not prepared” to fend off such attacks (see Figure 12).

Organizations clearly need better tools and processes to reduce their risk and fend off such attacks. First, let’s examine their spending.

---

\(^{23}\) [www.iso.org/iso/home/standards/management-standards/iso27001.htm](http://www.iso.org/iso/home/standards/management-standards/iso27001.htm)

\(^{24}\) [www.sans.org/critical-security-controls](http://www.sans.org/critical-security-controls)

When asked what percentage of respondents’ IT budgets are being spent on security year-over-year, an average of 40% indicated they either did not know or were unsure about the budgets. This is because many respondents are not responsible for IT security budgeting and may not have good visibility into their IT spending.

While 1–3% is the most common amount of the IT budget earmarked for security in 2013, a significant percentage (13%) was in the 6–10% bracket of spending. It looks like we’ll see the most dramatic change in the next fiscal year, when 15% plan 11–25% of their IT budgets for security, while fewer (11%) fall into the 1–3% range. Figures 13–15 illustrate the year-over-year spending comparisons.

When past, present and future budget projects are compared, the results show that:

- The number of organizations with smaller IT security budgets (from 1–3% of IT spending) is on the decline—from 21% in the previous FY to 15% in the current FY and to 11% in the next FY.
- The number of those with higher security spending (from 11–25%) is on the rise—from 7% in the previous FY to 13% in the current FY and to 15% in the next FY.
Budget Plans by Size of Organization

Spending also correlates to size of organization: Companies with fewer than 5,000 employees are spending a larger percentage of their budgets on security and are planning the most growth in spending. See Figures 16–18.

Figure 16. Comparison of Previous Year Security Spending for Organizations of Different Sizes

Figure 17. Comparison of Current Year Security Spending for Organizations of Different Sizes

Figure 18. Comparison of Future Year Security Spending for Organizations of Different Sizes
Spending by the larger enterprises (more than 5,000 employees) appears relatively steady year-over-year, with trends not as clearly apparent from our results. This may be because larger organizations have a more mature security function, and costs have stabilized as investments move from product acquisition to maintenance.

Who’s Driving?

Technologies, practices and spending are, ultimately, driven from the top down according to survey results: For the clear majority of organizations (48%), security practices are driven by the CSO, CISO or director of information security, as shown in Figure 19. However, we do see risk and compliance managers taking oversight for information security in nearly 10% of organizations. Other business functions—board of directors (8%), CEO/COO (6%) and CFO (2%)—also make up a significant portion (16%) of non-IT persons responsible for driving security practices.

Oversight—and accountability—is important and should be firmly planted in the IT and operational sides of the organization.
Outside Services

Respondents indicated their organizations rely mostly on internal staff, while deploying consultants primarily for event response. In this survey 44% of respondents turn to outsourcers for security event management. Another 27% outsource security architecture, and 26% outsource compliance management. See Figure 20.

The “Other” responses (19%) include services such as penetration testing, threat intelligence, forensics and distributed denial of service (DDoS) mitigation.

Inversely, nearly 56% of organizations handle their security event management and response internally, and 73% develop and maintain their own security architecture. The systems built by the financial sector can often be proprietary, and compliance is taking a large chunk out of their budgets, which is largely reflected here: They’re keeping most of these skills and functions in-house.

On the other hand, the tendency for organizations of any size is to outsource incident response and forensics makes sense: They need to augment skills and capacity during a stressful time. Digital forensics experts are highly skilled in particular system and device investigations to the degree that an internal response team may not equal, even at a large organization with resources.

For which of the following do you rely on outside services?
Check all that apply.

Figure 20. Reliance on Outside Services
Protection Technologies in Use

As we pointed out earlier in this survey, endpoints (via malicious user or loaded malware) represent the largest threat vectors. In this survey we list 13 technology options, and the clear winners in terms of frequency of use are vulnerability scanning and continuous monitoring (80%) and advanced firewalls and intrusion detection or prevention systems to protect internal systems (80%). Following these are data protections (69%) and real-time monitoring (68%). See Figure 21.

This was another “Select all that apply” answer set.
Also strongly represented were data protection/encryption, monitoring for anomalies, log aggregation, strong authentication and secure configuration. These technologies, which were selected by more than 60% of respondents, apply to the endpoint. We anticipate that this is an area where services—either mobile device management (MDM), cloud-based and/or network access control (NAC)-based—management functions will become increasingly critical.

A strong percentage of respondents also use whitelisting or blacklisting (49%), strong authentication for customer-facing sites (44%), endpoint visibility (43%) and malware analysis (41%), with fewer using third-party real-time threat intelligence (39%) and in-house security analytics (34%).

**Effectiveness in Question**

The technologies respondents believed were the most effective, in general, aligned with those they say they are using. The interesting exception is strong authentication—although it ranked sixth and ninth in use for employees/partners and customer-facing sites (respectively), it rose to second and fourth in terms of effectiveness. In addition, vulnerability scanning, ranked first in terms of use, scored only fifth in terms of effectiveness (see Figure 22).
Advanced firewall, IDS and IPS are ranked very effective, perhaps because they generate alerts when attacks are detected and are perceived as being more important. It’s curious to see the lower rating on continuous monitoring and vulnerability scanning, and configuration best practices, which, if implemented effectively, reduce the attack surface and improve risk scoring for endpoints and internal systems. Real-time intelligence by third parties and security analytics conducted in-house, along with malware analysis systems, seem to have not yet gained wide acceptance in the marketplace.

**Customer-Facing Apps**

For protecting external-facing customer systems, respondents ranked multifactor authentication, continuous monitoring and secure application development as most effective, as shown in Figure 23.

Fraud detection (44%) was considered almost as effective in protecting external-facing customer systems. Three of the “Other” responses included web application firewalls. Note that 50% of respondents cited their main driver as compliance requirements with PCI DSS, under which requirement 6.6 specifies web-application firewalls for public-facing web applications.

Each of these technologies applies to different stages of a system lifecycle (access, operations and development), and all can be used together to significantly increase security. This suggests that organizations could benefit greatly by integrating security throughout all of the stages of their application lifecycle program.
Information Sharing

Sharing threat, vulnerability and remediation information along with obtaining security education are some of the benefits to participating with groups established for this purpose. There are a number of resources available for sharing this type of information, and it’s clear from our survey responses that financial organizations are using them.

Nearly half of respondents (49%) belong to the SANS Internet Storm Center (https://isc.sans.edu), and 46% use the United States Computer Emergency Readiness Team (US-CERT, www.us-cert.gov) or regional CERTs. About 36% mentioned local or regional peer groups, and 35% use the FBI/private sector partnership known as Infragard (www.infragard.org). Approximately 30% use educational and training groups and boards. Additional responses are listed in Figure 24.

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

Figure 24. Information and Education Groups Used
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 in 2014 and 2015.

**On Their Wish Lists**

According to our survey, nearly 49% of organizations intend to invest more heavily in IT security over the next two years, as shown in Figure 25.

Almost as many expect their security investments to remain the same (48%), and only 5% (9 respondents) expect to decrease their investment. These results are promising.

In a write-in answer at the end of the survey, respondents are asking for more forms of multifactor authentication for their users, enforcement of separation of duties, website access controls or restrictions by proxy. There were also multiple requests for endpoint detection and management. Others want to replace out-of-date noncompliant systems, as well as improve security on and receive more funding for incident response.

Respondents clearly understand that there is danger in complacency. Just because a tool is familiar does not mean it is effective. Attackers continuously evolve their attack tools, and it is prudent for organizations to evolve with them.
Financial institutions represent, perhaps, the most protected business segment in the private sector. They are also the most targeted.

In spite of a range of preparations and defenses, attacks still get through. A big contributor to this is malicious and manipulated insiders. Attackers circumvent technical defenses by preying on human gullibility and weakness.

In addition to using appropriate security tools, it is essential that proper screening, monitoring and education of employees and contractors be implemented. Yet, according to our survey, the IT and managerial staff in charge of security lack the visibility they need to protect against endpoint risks, including insider threat and malware on the devices, which are the most prevalent cause of security incidents reported in this survey.

Of those who could quantify losses, their most common losses were financial account data, but denial of service and regulatory issues figured prominently in outcomes. A likely emerging category of significant loss will become civil lawsuits filed by customers, partners, financial entities or governments. Class-action suits may take years to wend their way through courts, making accurate calculation of losses extremely difficult to anticipate.

Growing numbers of regulations are attempting to control the potential losses in the financial services industry. The amount organizations spend on meeting regulatory requirements is huge—and is getting bigger. But, for every dollar spent on completing a regulatory form, there is one less dollar available for actually making systems more secure. There is room for legislative reform to move mature organizations away from being compliance driven to focusing on reducing attack surfaces, minimizing vulnerabilities and defending against threats.

The good news is that security spending is trending upward. However, money is wasted if it is not spent effectively. Managers must ensure that their security investments meet their needs and are deployed appropriately to gain every possible advantage from their available resources.
**About the Author**

**G. Mark Hardy** is president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for more than 30 years and is the author of more than 100 articles and presentations. He serves on the National Science Foundation’s CyberWATCH Advisory Board and is a retired U. S. Navy captain. A graduate of Northwestern University, he holds a BS in computer science, a BA in mathematics and master’s degrees in business administration and strategic studies. Hardy holds the GIAC Security Leader Certification (GSLC) and is designated as a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).

---

**Sponsors**

*SANS would like to thank this paper’s sponsors:*

![Blue Coat](image1)

![FireEye](image2)

![ForeScout](image3)

![Raytheon](image4)

![Sourcefire](image5)

![Tenable Network Security](image6)
# Upcoming SANS Training

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

<table>
<thead>
<tr>
<th>Event Name</th>
<th>City, Country</th>
<th>Date Range</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NIH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>Online TXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>

---

*Last Updated: March 21st, 2015*