www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

CIO
BUSINESS TECHNOLOGY LEADERSHIP
CSO
BUSINESS RISK LEADERSHIP

Financial Services

Key findings from The Global State of Information Security® Survey 2014

April 2014

pwc

Compliance is not enough as threats advance faster than security.

- The results of The Global State of Information Security® Survey 2014 show that financial services companies are spending more on information security than ever before and have improved many of their security practices.
- Our research indicates that regulatory compliance is still a significant driver of security spend in the industry. Yet incidents continue to occur as a result of unprecedented attacks, ranging from distributed denial of service to advanced persistent threats (APTs).
- Why is this happening? We believe most organizations are defending yesterday, even as their adversaries exploit the threats of tomorrow.

38%

of financial services respondents say complex, rapidly evolving, and sophisticated technologies such as high-frequency trading systems pose a "significant challenge" for the future success of their organization's information security.

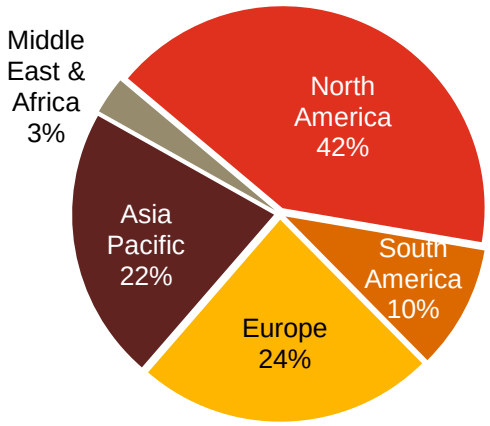
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

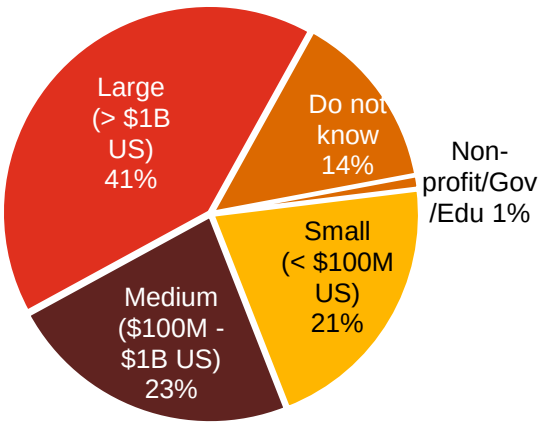
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 993 respondents from the financial services industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

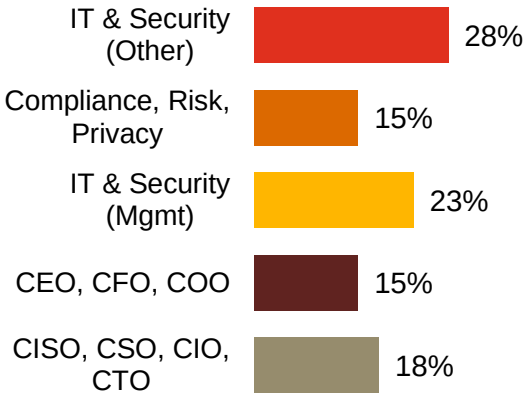
Financial services respondents by region of employment



Financial services respondents by company revenue size



Financial services respondents by title

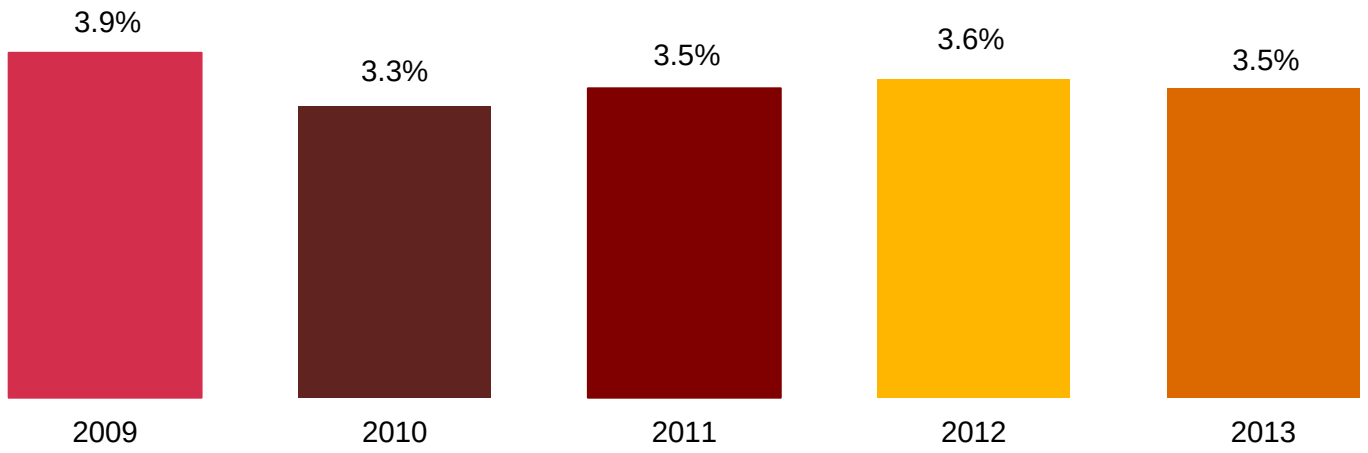


(Numbers reported may not reconcile exactly with raw data due to rounding)

The share of IT budget has held steady, but as overall IT spending has increased, security budgets have also expanded.

As illustrated below, security's share of IT spend has held constant at approximately 3.5% in recent years. As overall IT budgets have recovered from post-financial crisis lows, however, spending on information security has increased in tandem.

Percent of IT budget spent on security

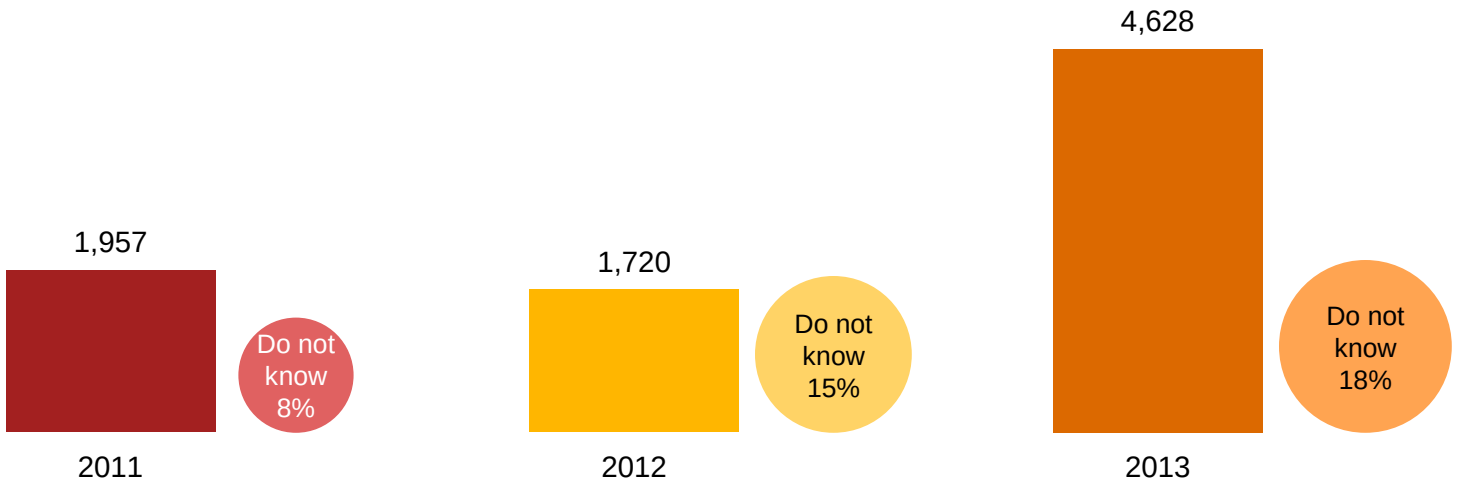


Question 7: "What is your organization's total information technology budget for 2013?" Question 8: "What is your organization's total information security budget for 2013?"

*Financial services respondents are detecting significantly more security incidents.**

The average number of detected incidents increased by 169% over last year, evidence of today's elevated threat environment and perhaps respondents' improved ability to identify incidents. Average total financial losses have increased significantly over 2012, which is not surprising given the cost and complexity of responding to threats.

Average number of security incidents in past 12 months



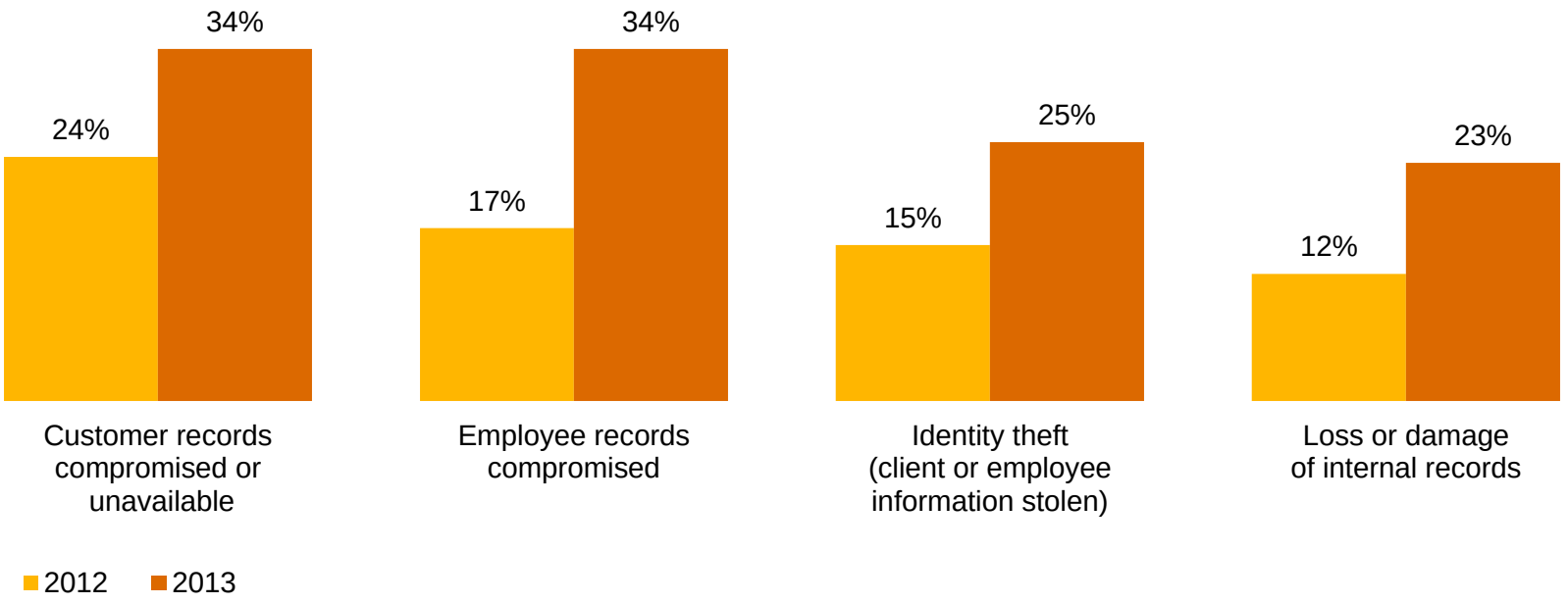
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents.

Financial services respondents report a significant increase in data loss as a result of security incidents.

Compromise of employee and customer records remain the most cited impacts, potentially jeopardizing an organization's most valuable relationships. Also significant: Loss or damage of internal records almost doubled over 2012.

Impact of security incidents

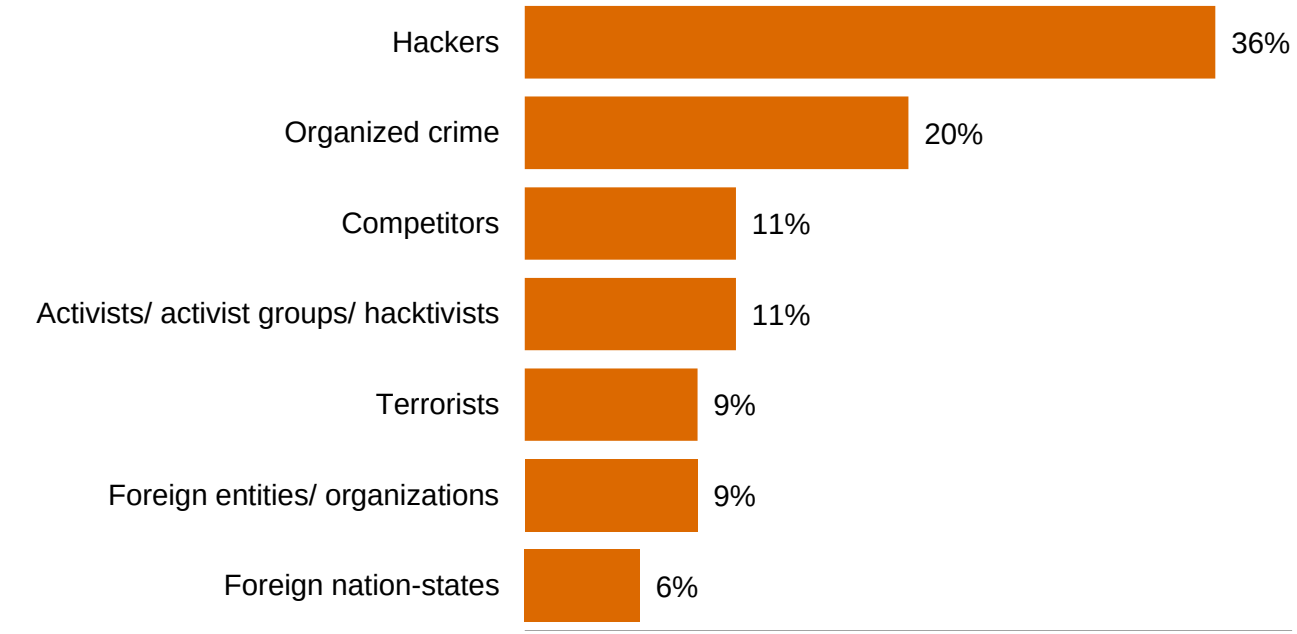


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

While attacks backed by nation-states make headlines, financial services firms are more often hit by other outsiders.

Only 6% of financial services respondents report security incidents perpetrated by foreign nation-states. Hackers and organized crime pose a much more likely danger.

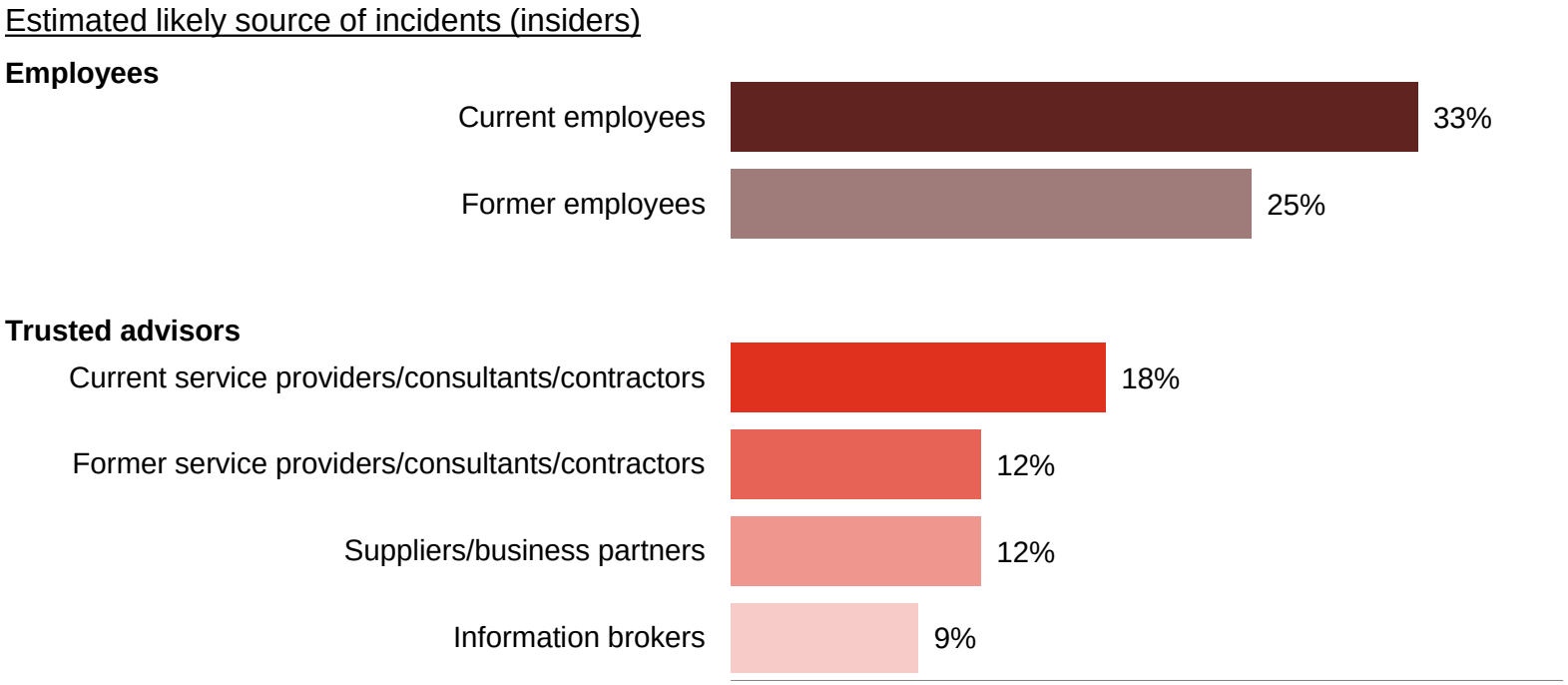
Estimated likely source of incidents (outsiders)



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most financial services respondents.

It's the people you know—current and former employees, as well as other insiders—who are most likely to perpetrate security incidents.

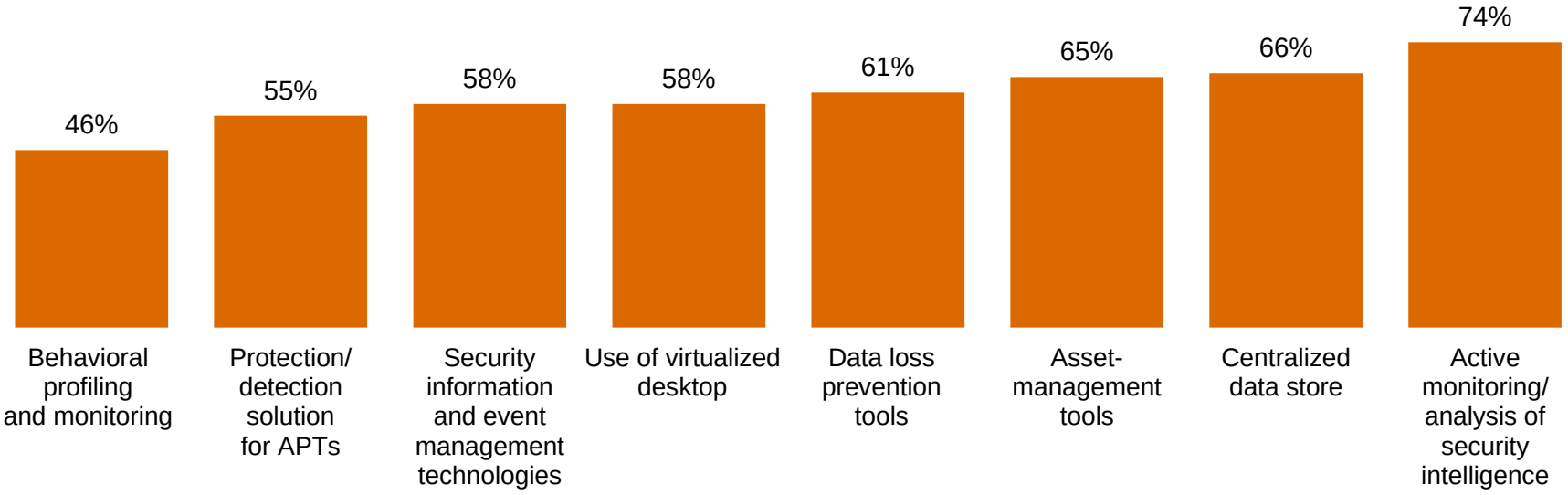


Question 21: "Estimated likely source of incidents" (Not all factors shown.)

Respondents have not fully implemented technologies and processes that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place than traditional "block and tackle" security. The types of tools below—behavioral profiling and safeguards against APTs, in particular—can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Security safeguards currently in place



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

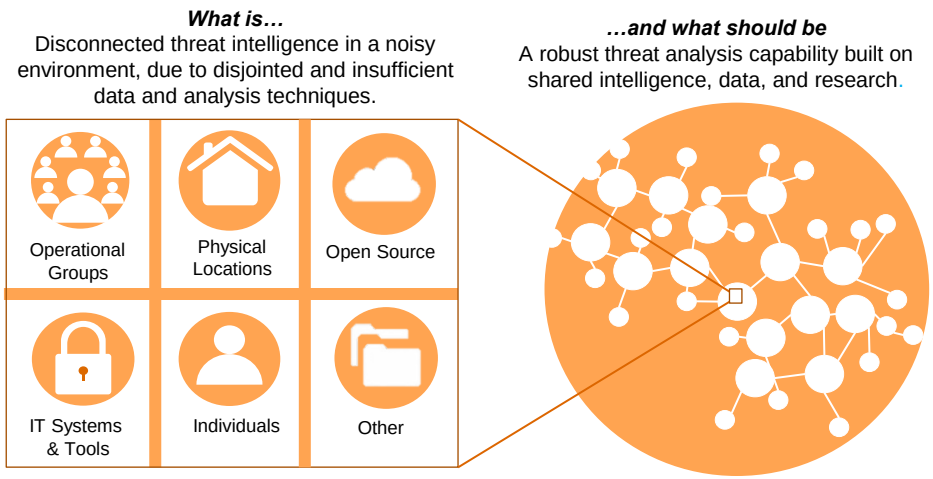
As they work to upgrade their defenses against cyber attacks, financial institutions should focus on these key areas:

Prioritize and protect the "critical information storage / transactions"

- PwC's 2014 GSISS survey indicates that only 24% of financial services respondents classify the business value of data. Financial institutions will need better processes for the inventory, assessment, and valuation of the organization's data to prioritize the defense of these data assets. These priorities, in turn, determine the appropriate allocation of the organization's resources.

Harness the power of collaboration

According to GSISS 2014, 55% of financial services respondents say they collaborate with others to improve security. However, many still resist sharing data with outsiders, because they do not want to draw attention to their own weaknesses.



While these concerns are legitimate, the threat intelligence that can be gathered and shared from collaboration with law enforcement, federal agencies, and other private partnerships often prove invaluable in enabling financial institutions to gain insight into emerging threats.

Develop a robust threat analysis capability

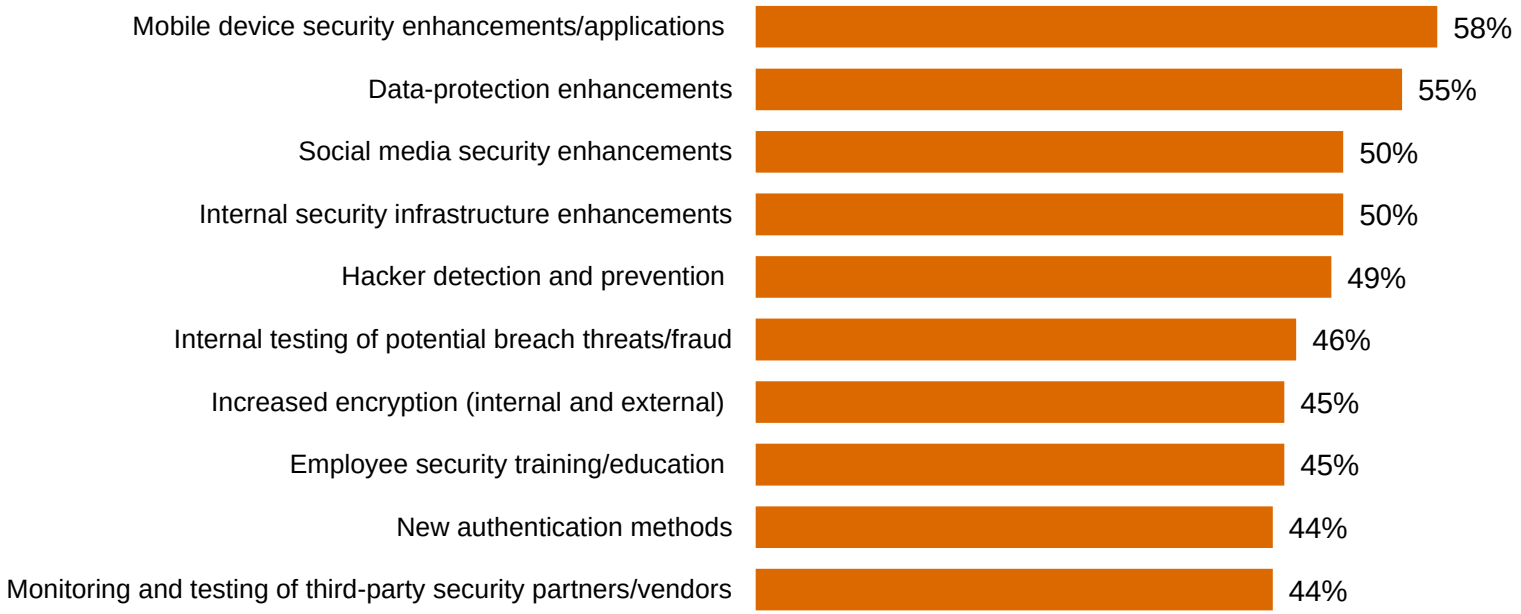
Most institutions' threat analysis efforts suffer because they inhabit a disjointed environment that is spread across several functions, physical locations, and systems. In our view, institutions should establish a robust threat analysis capability that is built on shared intelligence, data, and research from internal and external sources. This capability should address:

- Governance and operations–the roles and responsibilities that various security functions have, and how they should interact.
- Collaborative analysis—processes for digesting internal data and external threat intelligence feeds.
- Analytics tools—investment in big data technologies to enhance monitoring of security threats and improve fraud detection across business lines.
- Communication protocols—processes for disseminating actionable intelligence across the organization, enabling security functions to prevent, detect, and respond to threats.

What business imperatives and processes will financial services respondents prioritize over the next 12 months?

Some of the highest priorities include enhanced security for mobile devices and social media.

Over the next 12 months, organization will increase spending for:

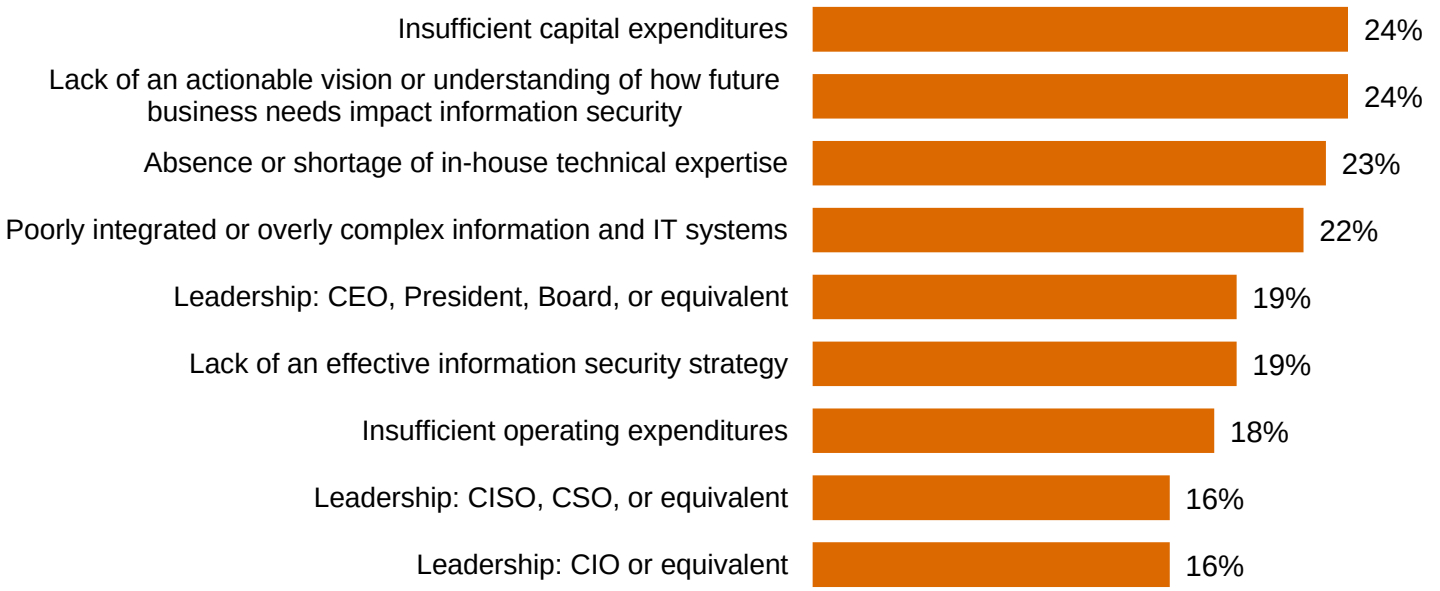


(Asked only of financial services respondents.) Question 3: “Please indicate whether your organization will increase or decrease spending on information security over the next 12 months for?” (Not all factors shown.)

More money and an actionable vision are needed to overcome obstacles to advancing security.

This is critical because effective security requires an adequate budget that is aligned with future business needs, as well as the support of top executives.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Leading security practices for financial services companies.

Security is a board-level business imperative	
Advance your security strategy and capabilities.	• An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge. • You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
Board and CEO drive security governance.	• Security risks are operational risks and should be reviewed regularly by the board. • Strong support and communication from the board and CEO can break down traditional silos, leading to more collaboration and partnerships.
Strong multi-party governance group should manage security risk.	• An executive with direct interaction with the CEO, General Counsel and Chief Risk Officer should lead security governance. • Security governance group should include representatives from legal, HR, risk, technology, security, communications, and the lines of business. • The cybersecurity governance group should meet regularly (monthly or quarterly) to discuss the current threat landscape, changes within the organization that impact risk levels, and updates to remediation programs and initiatives.
Security threats are business risks	
Security program is threat-driven and assumes a continuous state of compromise.	• Security risks are among the top 10 operational risks. • Adopt the philosophy of an assumed state of compromise, focusing on continuous detection and crisis response in addition to traditional IT security focus of protection and mitigation. • Security risks include theft of intellectual property, attacks on brand, and social media. • You should anticipate threats, know your vulnerabilities, and be able to identify and manage the associated risks. • Focus on your adversaries: who might attack the business and their motivations.
Ensure cooperation among third parties.	• Proactively make certain that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Leading security practices for financial services companies (cont'd).

Protect the information that really matters	
Identify your most valuable information.	• Know where these "crown jewels" are located and who has access to them. • Allocate and prioritize resources to protect your valuable information.
Establish and test incident-response plans	
Incident response should be aligned at all levels within the organization.	• Incident response should integrate technical and business responses. • Response is aligned at all levels by integrating the technical response (led by IT) and business response (led by business with input from legal, communications, the senior leadership team, and HR).
Security incident response should be tested using real-world scenarios.	• Improve planning and preparedness through table-top simulations of recent industry events and likely attack scenarios. • Frequently conduct table-top simulations. • Response to various attack scenarios and crisis should be pre-scripted in a "play book" format.
Gain advantage through Awareness to Action	
Security is driven by knowledge, an approach we call Awareness to Action.	• All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring. • Organizations should create a culture of security that starts with commitment of top executives and cascades to all employees. • Organizations should engage in public-private collaboration with others for enhanced threat intelligence.

A framework for response

Putting cyber in the security architecture

Know your enemy

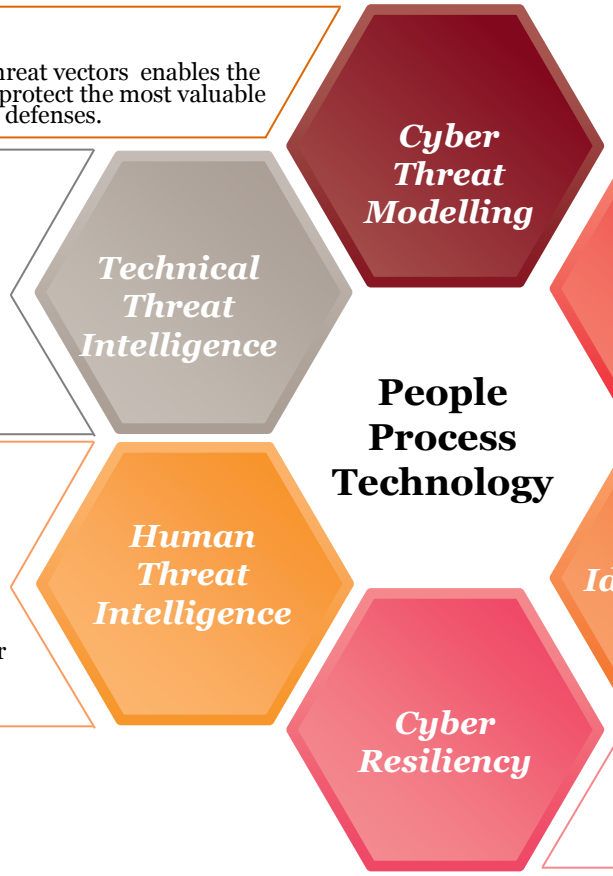
Understanding threat actors and threat vectors enables the organization to design defenses to protect the most valuable assets and identify gaps in current defenses.

Keep abreast of changes

The threat landscape is continuously changing and evolving. Technical Threat Intelligence collects information, analyzes, normalizes and makes available to other processes for situational awareness

Don't forget the human element

Non-technical threats can also affect the organization from insider threat to employee e safety.



Managing exposure

Security monitoring & Intelligence enable the enterprise to identify potential or actual attacks on the environment and engage response.

Securing systems

Identity assets and the data contained on these systems. 'Right-sizing' the protection level based on the asset value and the data stored on the system.

Managing Availability

The organization's reputation and servicing of customers and clients relies on available systems. Cyber Resiliency focuses on architecting systems to resist attack and ensure available systems

For more information, please contact:

Financial Services IT Security & Risk Contacts

Joe Nocera
Principal
312.298.2745
joseph.nocera@us.pwc.com

Shawn Connors
Principal
646.471.7278
shawn.joseph.connors@us.pwc.com

Andrew Toner
Principal
646.471.8327
andrew.toner@us.pwc.com

Christopher Morris
Principal
617.530.7938
christopher.morris@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

PwC