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.

Financial Services

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

September 2013

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 look to exploit the vulnerabilities of tomorrow.

Sophisticated intruders are bypassing traditional perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives or key customers.

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.

Gain advantages with an evolved approach to security

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

To be effective, security should move beyond compliance and be aligned with the business—and championed by the CEO and board—to emphasize threat awareness, asset protection, and motives of opponents. Security risks, including evolving cybersecurity threats, should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels, similar to how credit losses are managed.

In this new model of information security, knowledge is power. Seize it.

The new realities of cyber threats

Disappearing boundaries: Cyber threats destroy or dissolve boundaries, making attribution or legal action very difficult.

Shrinking cost and effort: The cost of developing and launching cyber campaigns is decreasing drastically, making them easily scalable and customizable.

Cheap and easy intelligence: Accessible 24/7, socially connected networks provide a rich source of data and an easy attack platform.

Far-reaching impact: Attack profiles and targets have matured to impact brand, reputation, intellectual property, and the bottom line.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

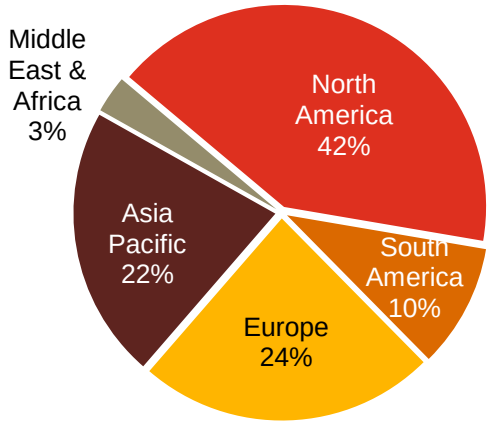
A global, cross-industry survey of business and IT executives

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.

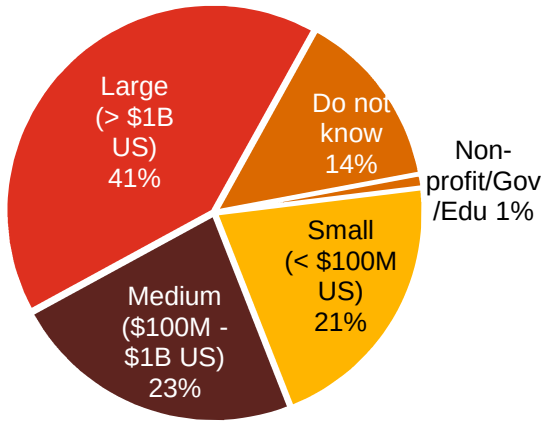
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions 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

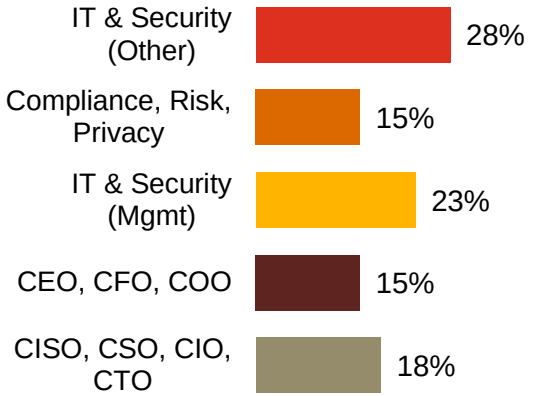
Financial services respondents by region of employment



Financial services respondents by company revenue size



Financial services respondents by title



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

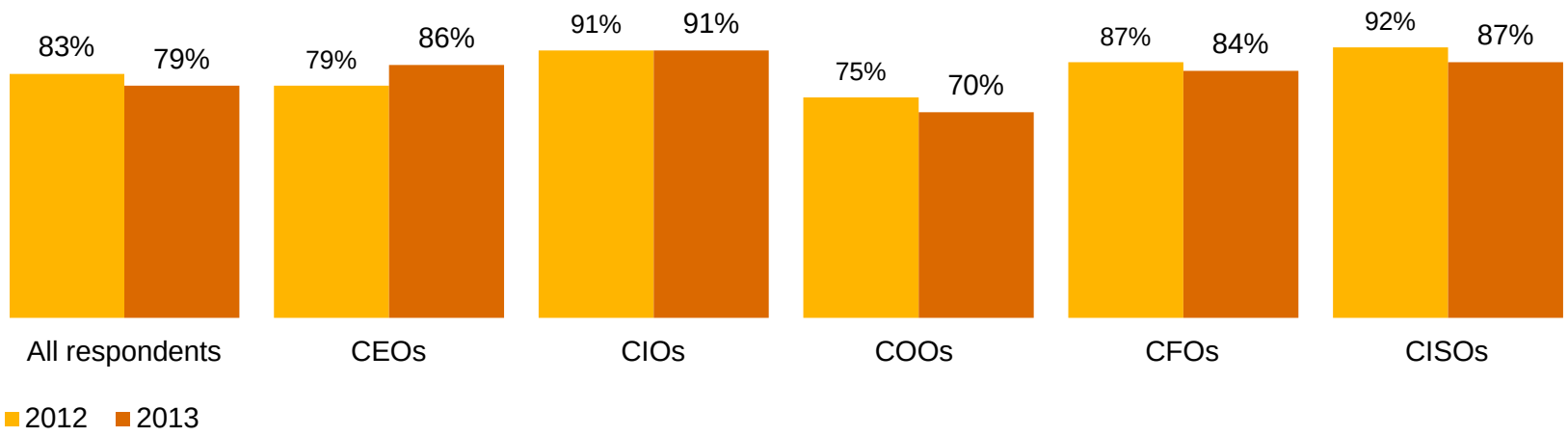
Section 2

Confidence in an era of advancing risks

79% of respondents say their security activities are effective, a decline of 5% over last year.

Confidence is still high in the C-suite*, with 86% of CEOs saying they believe their security program is effective. Across all respondents, however, confidence dropped 5% over last year, likely a result of today's enhanced threat environment. In fact, for the first time, the OCC has ranked cyber threats as a major factor heightening banks' operational risks.[1]

Executive confidence in effectiveness of security activities (somewhat or very confident)



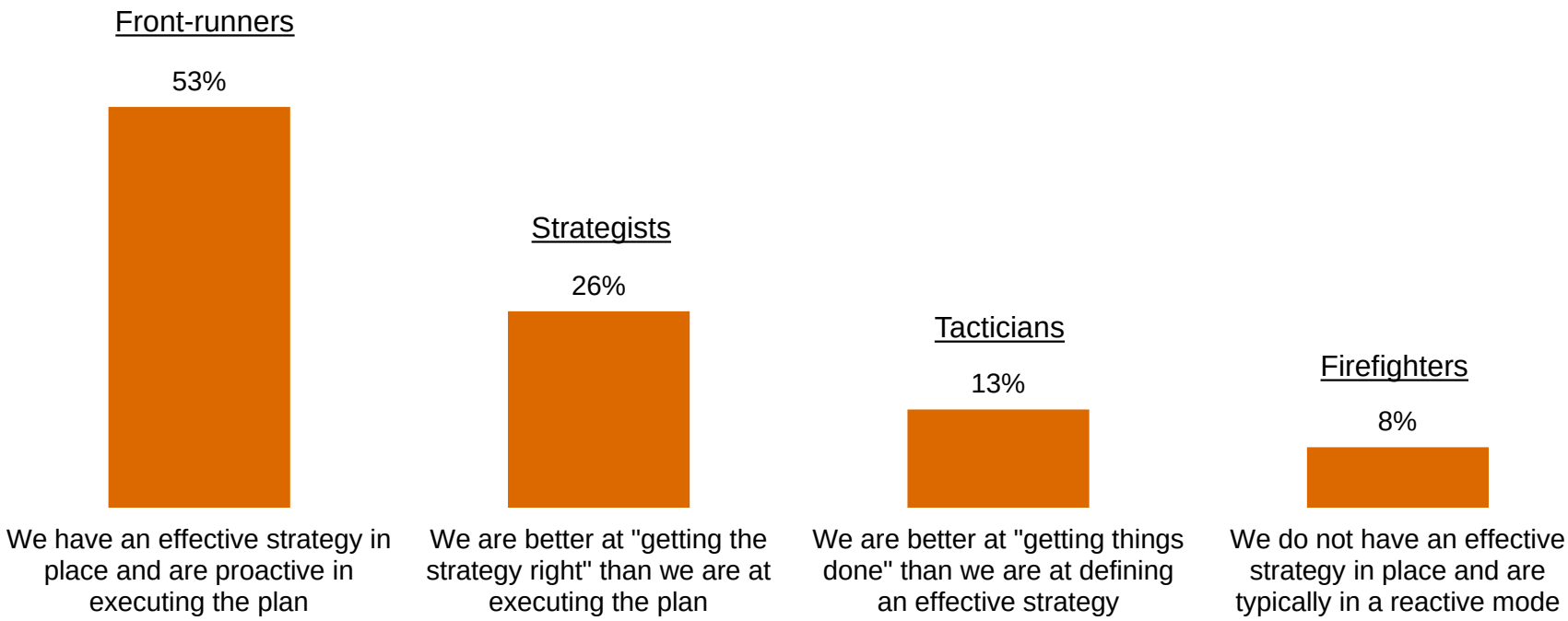
* CEOs, CFOs, and COOs

[1] Office of the Comptroller of the Currency, Semiannual Risk Perspective, Spring 2013

Question 39: "How confident are you that your organization's information security activities are effective?" (Respondents who answered "Somewhat confident" or "Very confident.") Question 1: "My job title most closely resembles"

53% of respondents consider themselves "front-runners," ahead of the pack in strategy and security practices.

More than half of financial services respondents say they have an effective strategy in place and are proactive in executing the plan. About one in four (26%) say they are better at getting the strategy right than executing the plan.

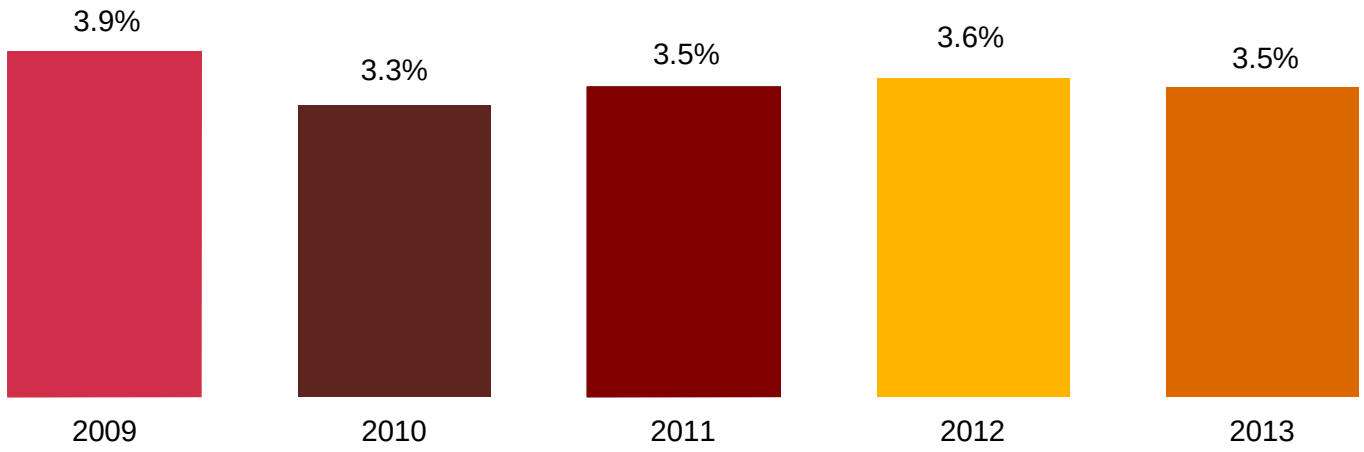


Question 27: "Which statement best characterizes your organization's approach to protecting information security?"

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?"

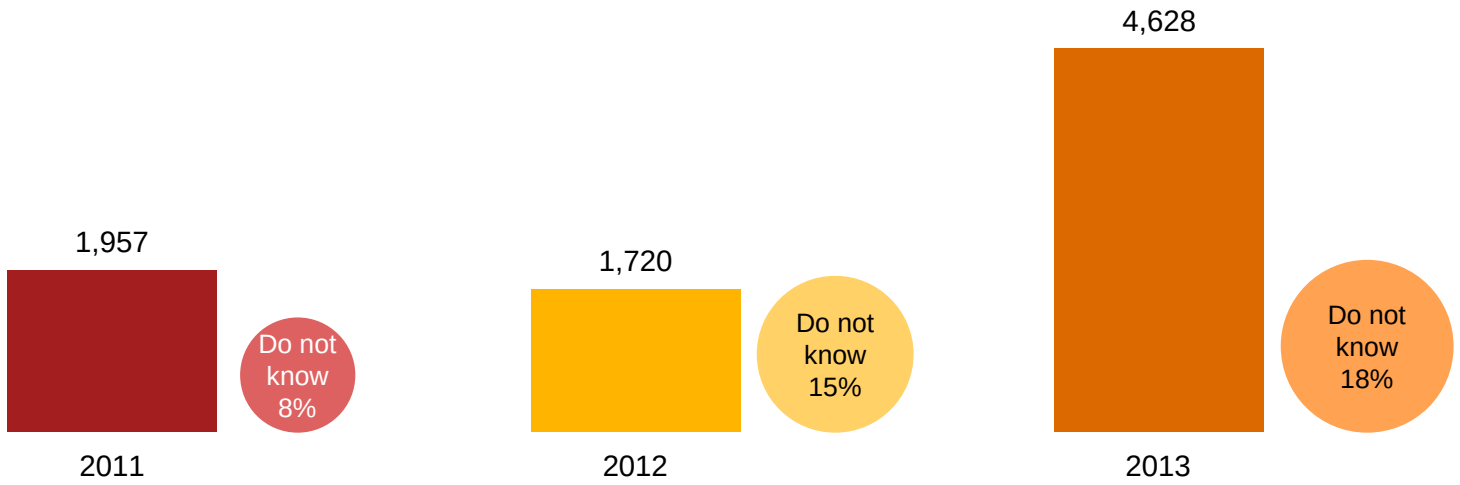
Section 3

Today's incidents, yesterday's strategies

*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.

The constantly evolving cyber-threat landscape is driving the increase in security incidents.

The marked increase in the number of detected incidents, in our view, is likely driven by the changing cyber-threat landscape. As the digital channel in financial services continues to evolve, cybersecurity has become a business risk, rather than simply a technical risk.

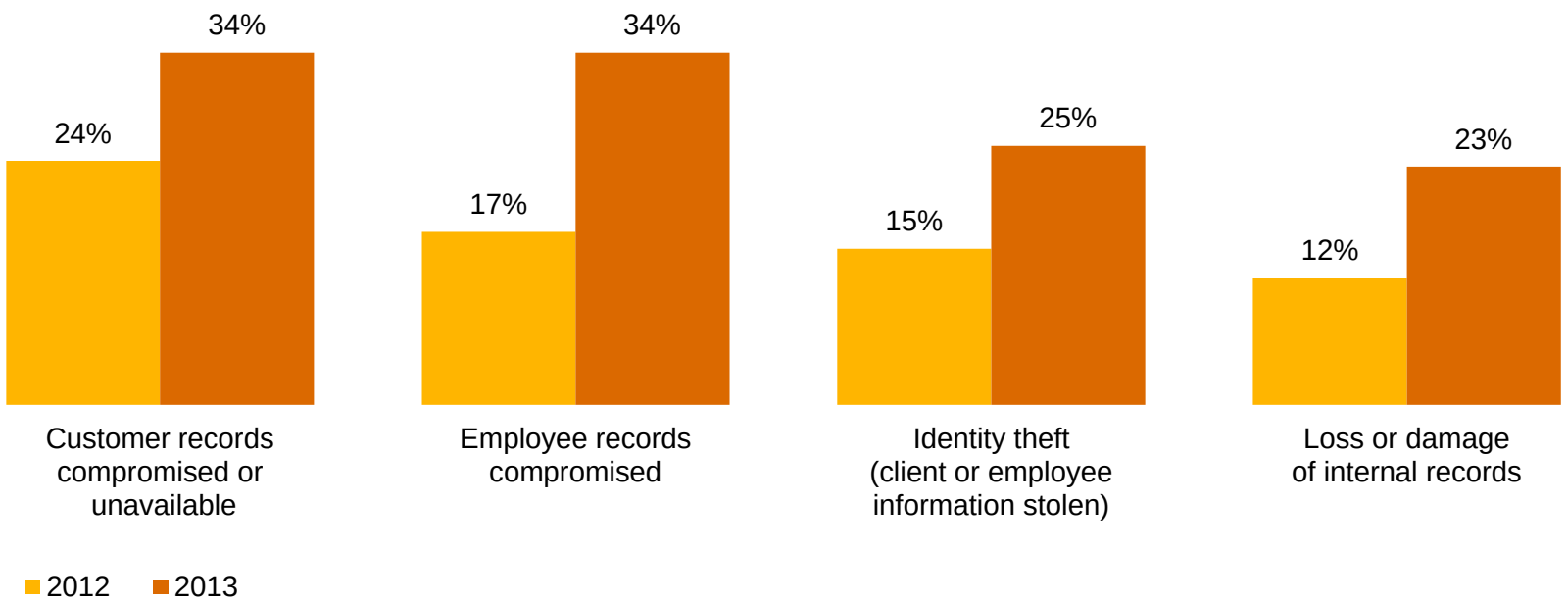
Lines between the threats are blurring

	Motivators	Threat vectors	Impact
Nation-states	• Global competition • National security • Fraud	• Targeted, long-term cyber campaigns with strategic focus • Insider • Third-party service providers	• Loss of intellectual property • Disruption to critical infrastructure • Monetary loss • Regulatory
Cyber criminals	• Illicit profit • Fraud • Identify theft	• Individual identity theft • Data breaches and intellectual property theft • Insider • Third-party service providers	• Loss of identity • Monetary loss • Intellectual property loss • Privacy • Regulatory
Cyber terrorists/ individual hackers	• Ideological • Political • Disenfranchised • Malicious havoc	• Opportunistic vulnerabilities • Insider • Third-party service providers	• Destabilize, disrupt and destroy cyber assets of financial institutions • Regulatory
Hacktivists	• Political cause rather than personal gain • Ideological	• Targeted organizations that stand in the way of their cause • Insider • Third-party service providers	• Disruption of operations • Destabilization • Embarrassment • Public relations • Regulatory

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

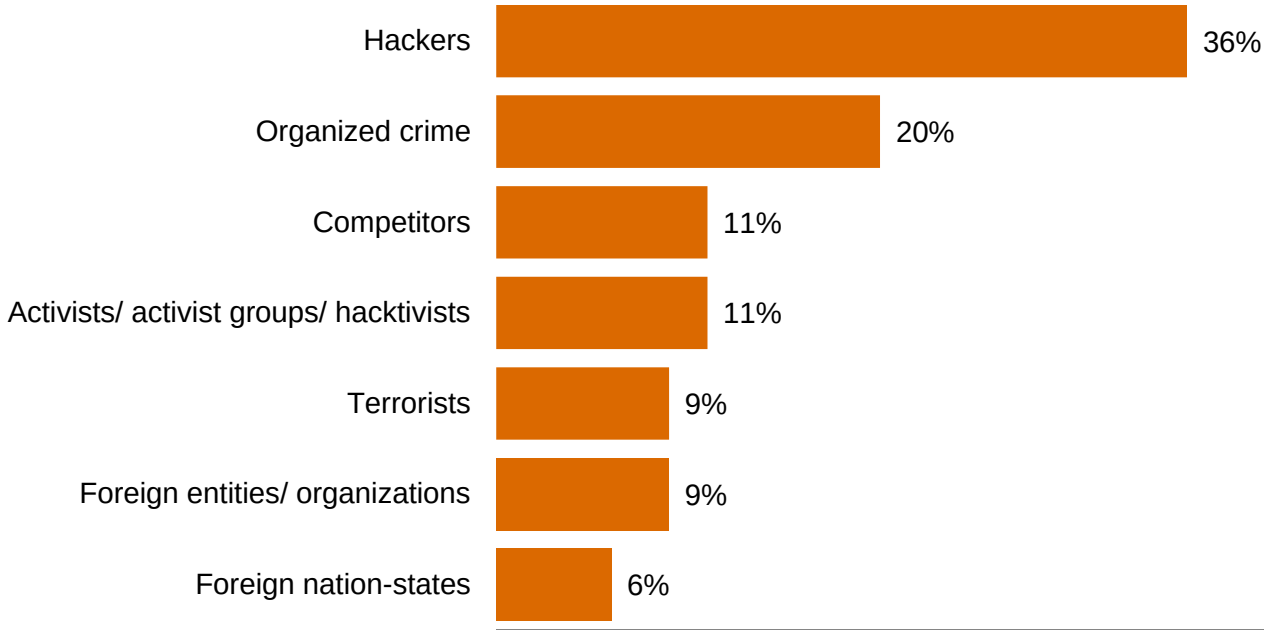


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

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.

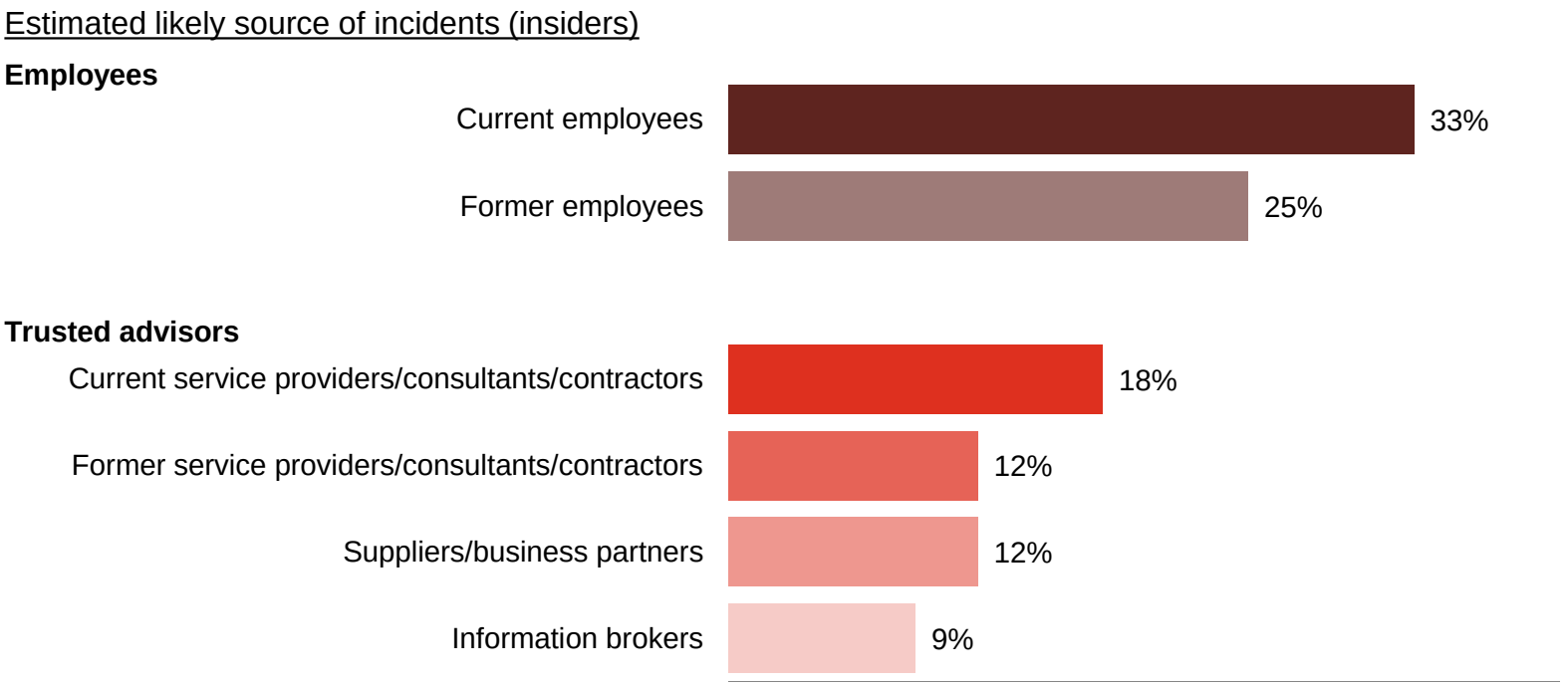
Estimated likely source of incidents (outsiders)



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.)

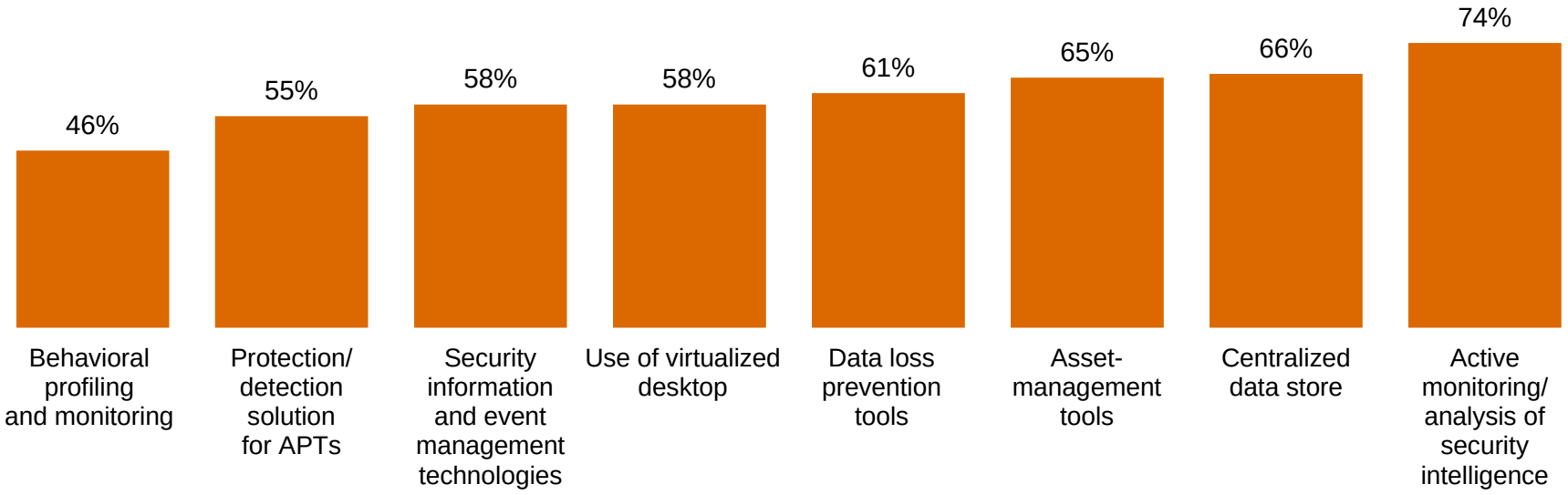
Section 4

A weak defense against adversaries

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

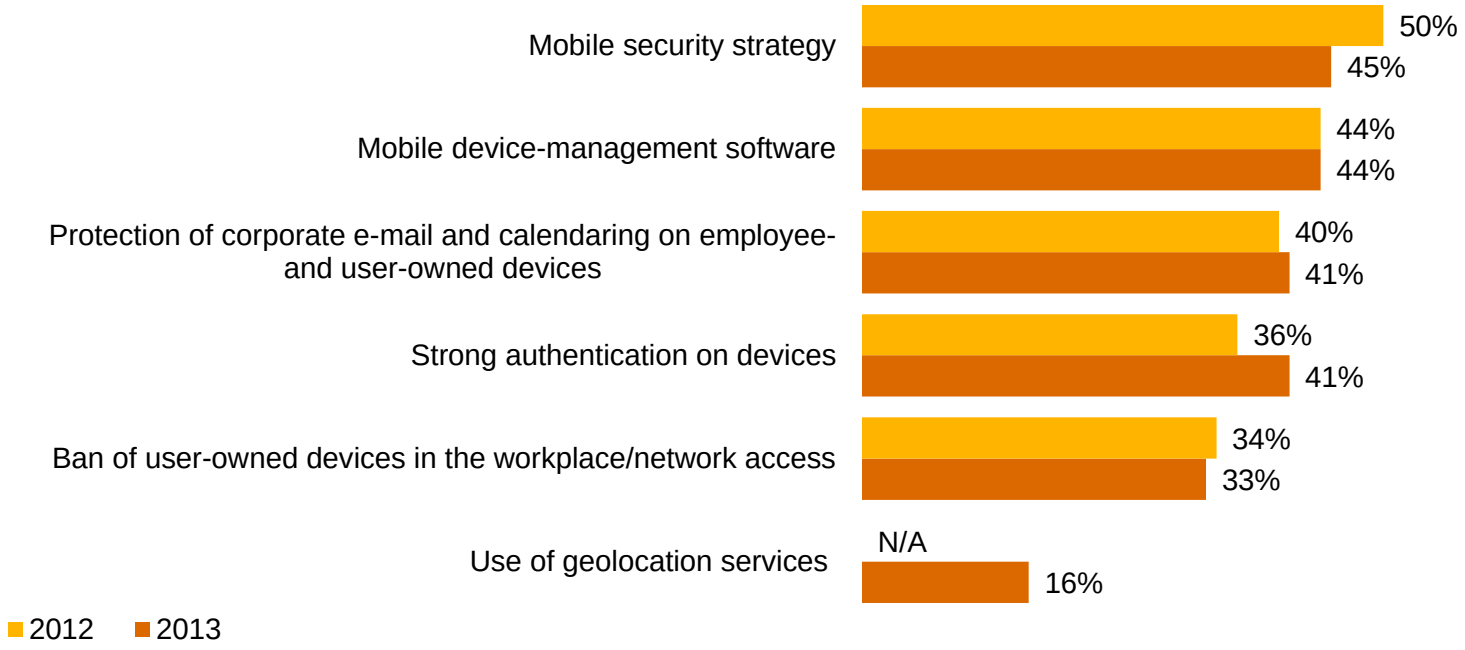


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet financial services companies' efforts to implement mobile security do not show significant gains over last year, and continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

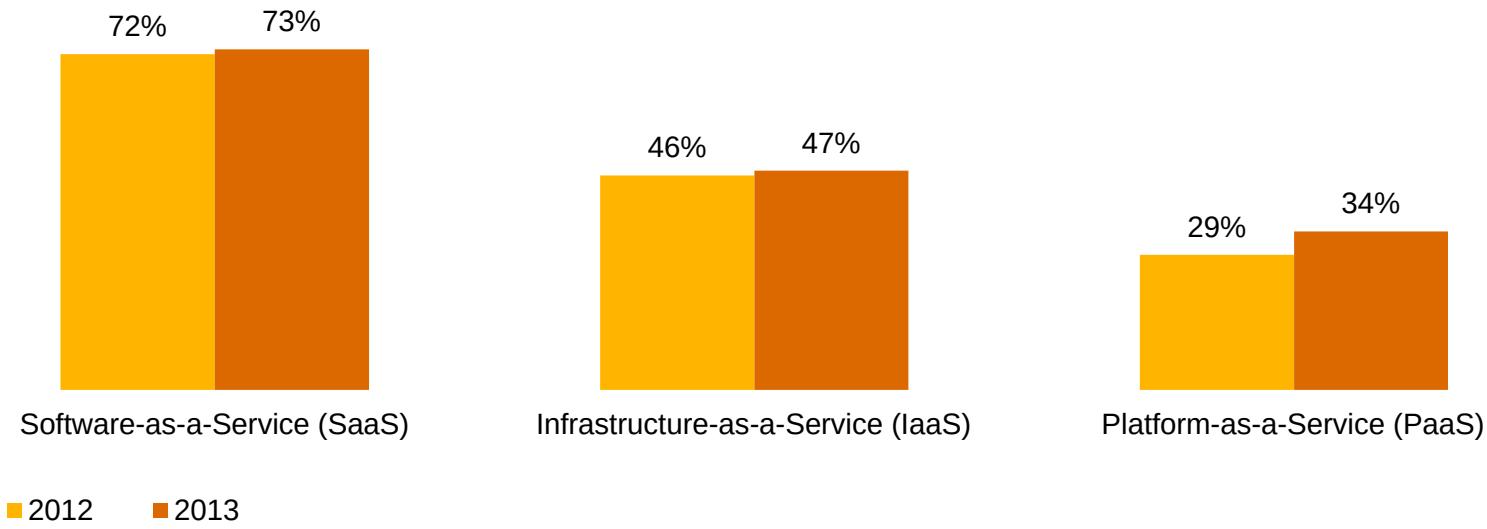


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Almost half of respondents use cloud computing, but they often do not include cloud in their security policies.

While 46% of financial services respondents use cloud computing—and among those who do, 53% report better security—only 18% include provisions for cloud in their security policy. SaaS is the most widely adopted cloud service, but PaaS shows growth.

Type of cloud service used

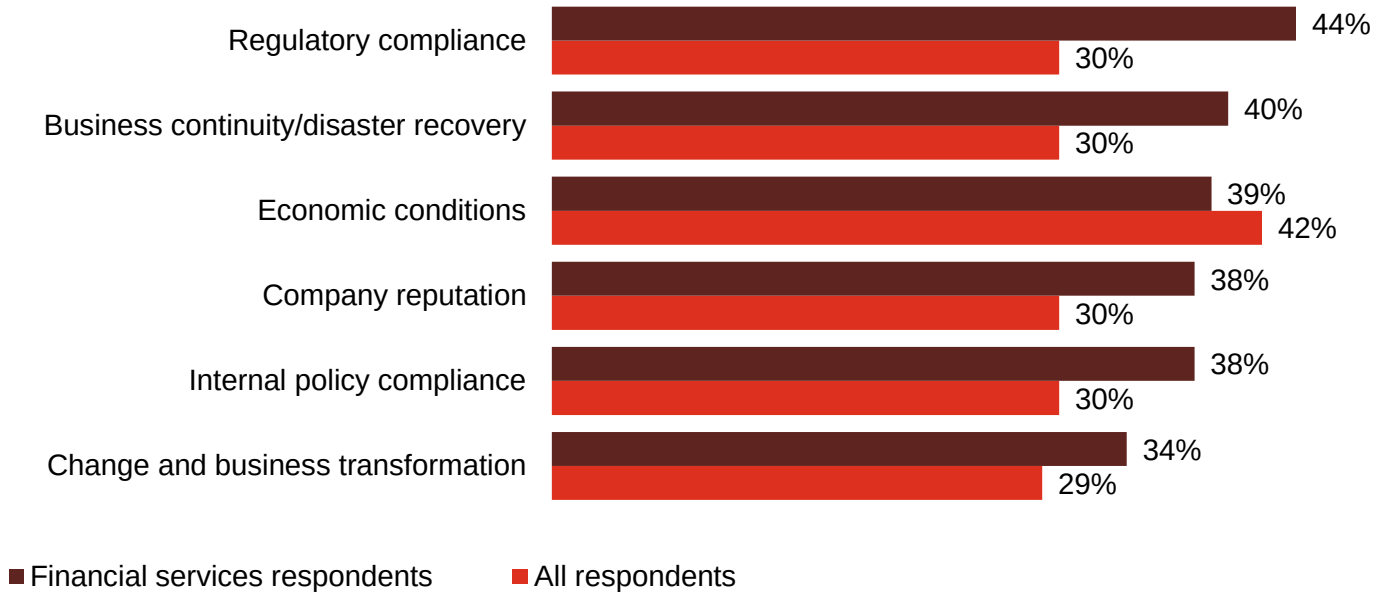


Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

Regulatory compliance remains the top driver of security spending for financial services respondents.

Compared with other industries, financial services respondents prioritize regulatory compliance as a driver for security spending. That's not surprising in a highly regulated industry, but a security model centered on existing compliance standards may not adequately address today's evolving security threats.

Drivers of information security spending



Question 35: "What business issues or factors drive your company's information security spending?" (Not all factors shown.)

Section 5

Preparing for the threats of tomorrow

Respondents rank evolving technologies and third-party standards as significant challenges to security.

Complex technologies such as high-frequency trading systems are a top concern among financial services respondents.

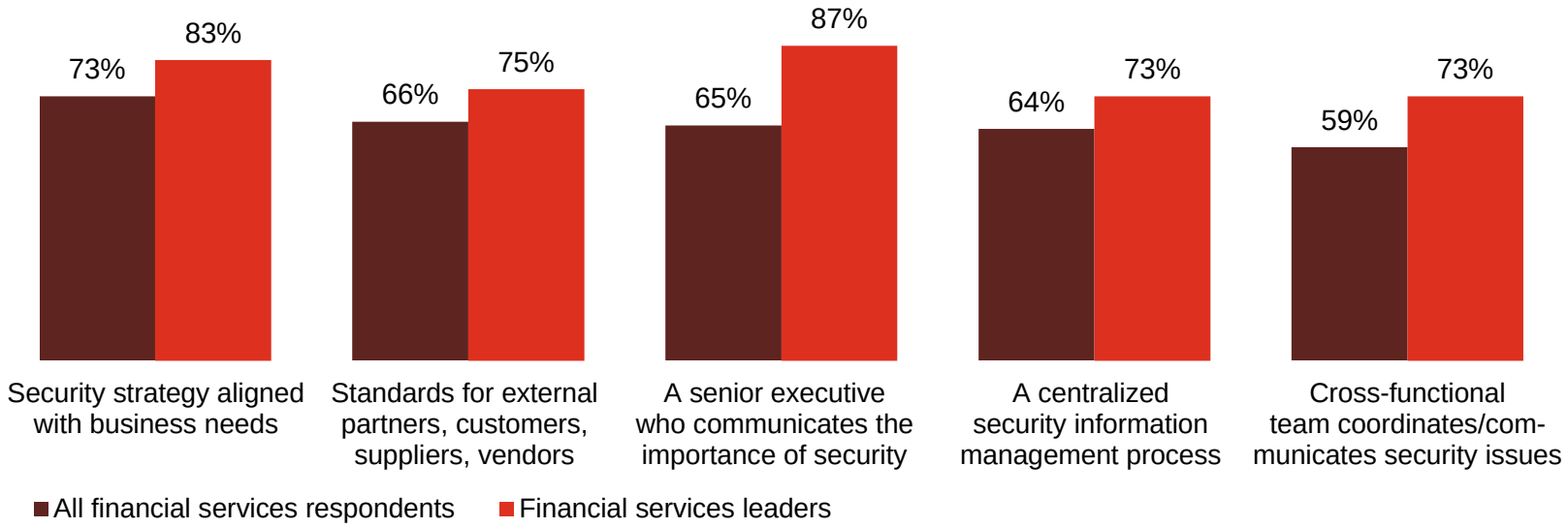
Top challenges to information security

(Asked only of financial services respondents) Question 4: “Please state the degree to which the following are challenges for the future success of your organization’s information security efforts?” (Respondents who answered “Significant challenge”) (Not all factors shown.)

Leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT challenge.*

Aligning security with business needs, setting standards for external partners, and improving communications show leaders, in particular, are rethinking the basics of security.

Security policies and safeguards currently in place: All respondents vs. leaders



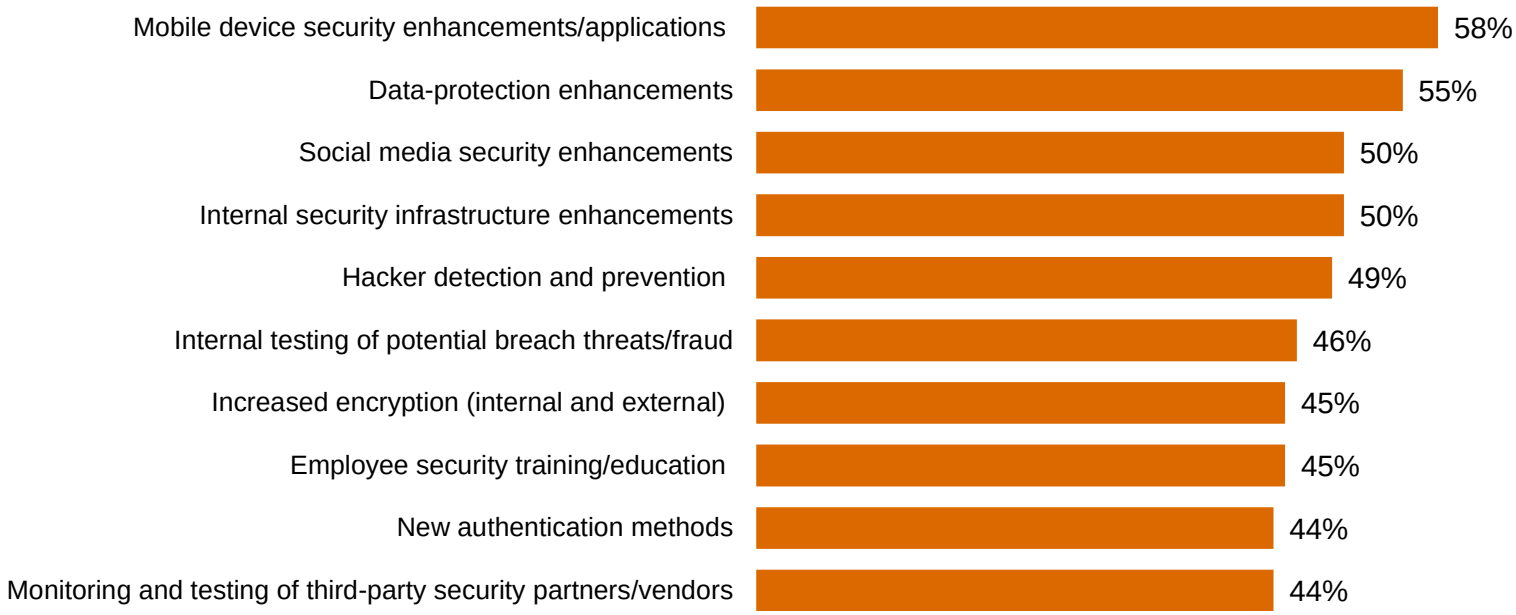
* We define leaders by the following criteria: Have an overall information security strategy; employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel; have measured and reviewed the effectiveness of security within the past year; and understand exactly what type of security events have occurred in the past year.

Question 14: "What process information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?"

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:

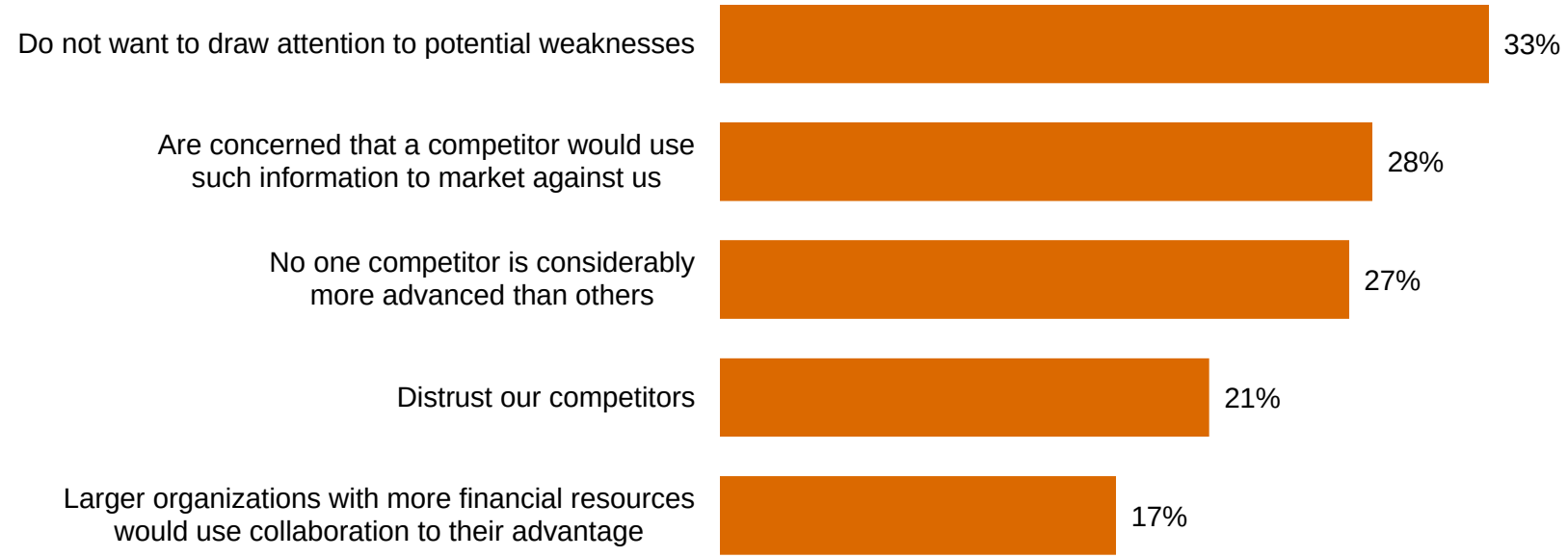


(Asked only of financial services respondents.) Question 3: “Please indicate whether your organization will increase or decrease spending on information security over the next 12 months for?” (Not all factors shown.)

55% of respondents collaborate with others to improve security, leveraging a powerful tool.

Compared with other industries, a higher percentage of financial services firms report they collaborate with others to advance security and better understand the threat landscape. Some, however, remain hesitant to share information, and that can impede security.

Reasons for not collaborating on information security

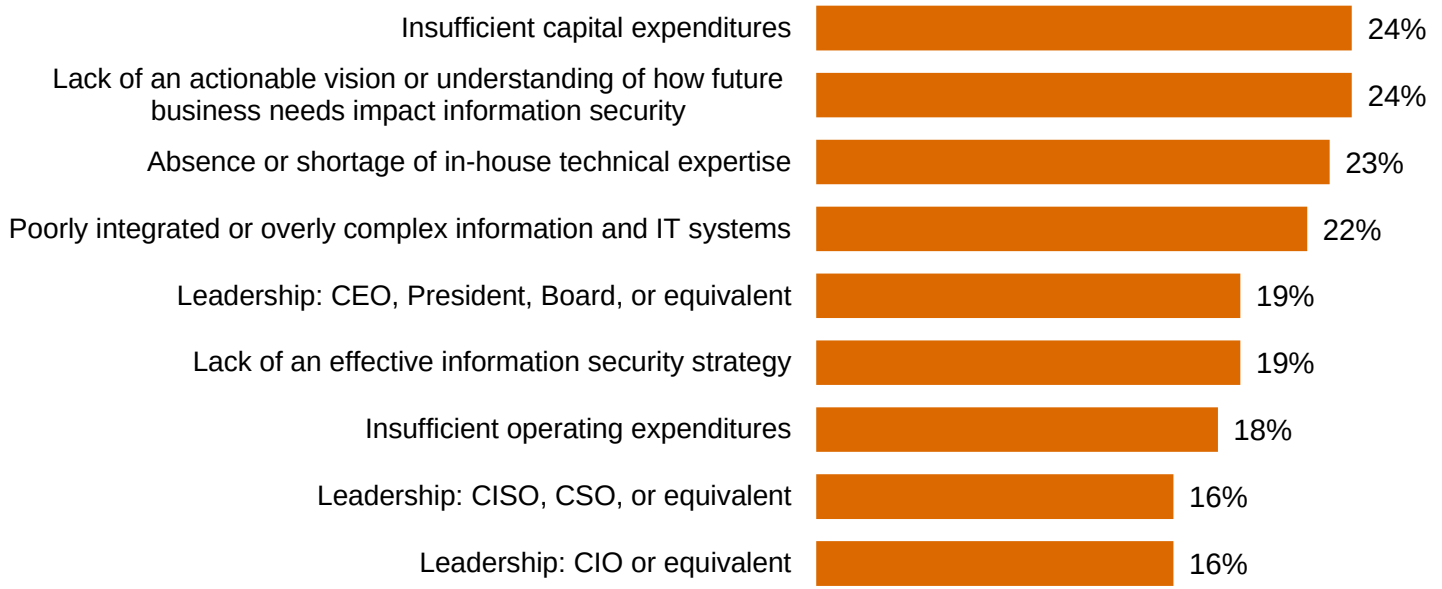


Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (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?"

Effective security also demands that organizations align policies and spending with business objectives.

This year, more financial services respondents say security policies and spending are aligned with business goals. This suggests they are starting to understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?" Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are 10 key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

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.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

US Financial Services 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