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.

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

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries exploit the threats of tomorrow.

Consequently, sophisticated intruders can bypass perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents increase in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Budgets are rising and confidence continues to climb.

But while many organizations have raised the bar on security, their adversaries have done better.

This year's survey shows that detected security incidents have increased, as has the cost of breaches. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few organizations have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"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."

This evolved approach requires that organizations identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

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

Agenda

Section 1

Methodology

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

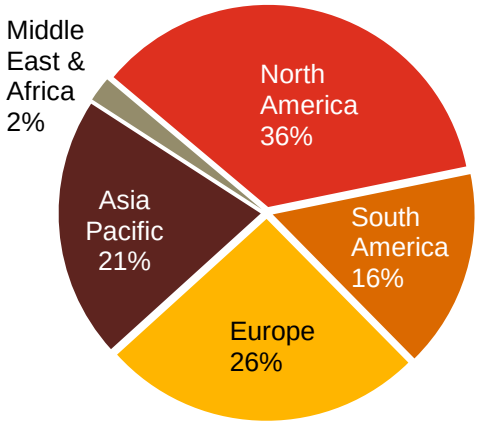
The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

- 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
- Margin of error less than 1%; numbers may not add to 100% due to rounding

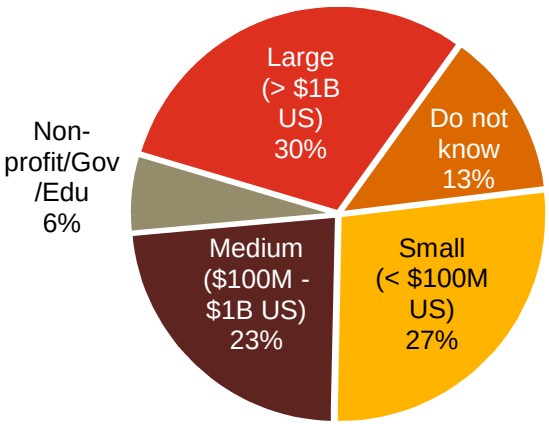
Demographics

30% of respondents work for large organizations (more than $1 billion in revenue), an increase of 22% over last year.

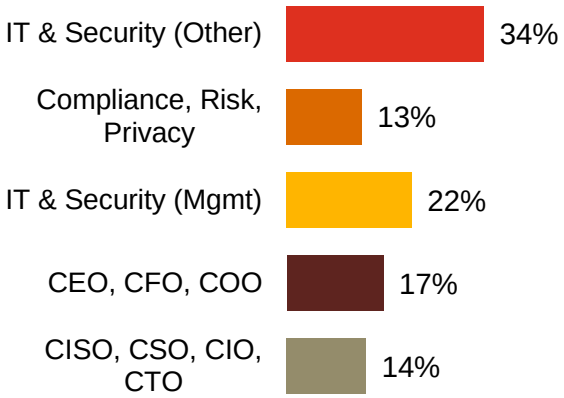
Respondents by region of employment



Respondents by company revenue size



Respondents by title



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

Survey response levels by industry

Number of responses this year	
Technology	1,226
Financial Services	993
Retail & Consumer	820
Public Sector	694
Industrial Products	671
Telecommunications	456
Healthcare Providers	398
Entertainment & Media	221
Automotive	209
Aerospace & Defense	193
Power & Utilities	143
Oil & Gas	107
Pharmaceutical	74

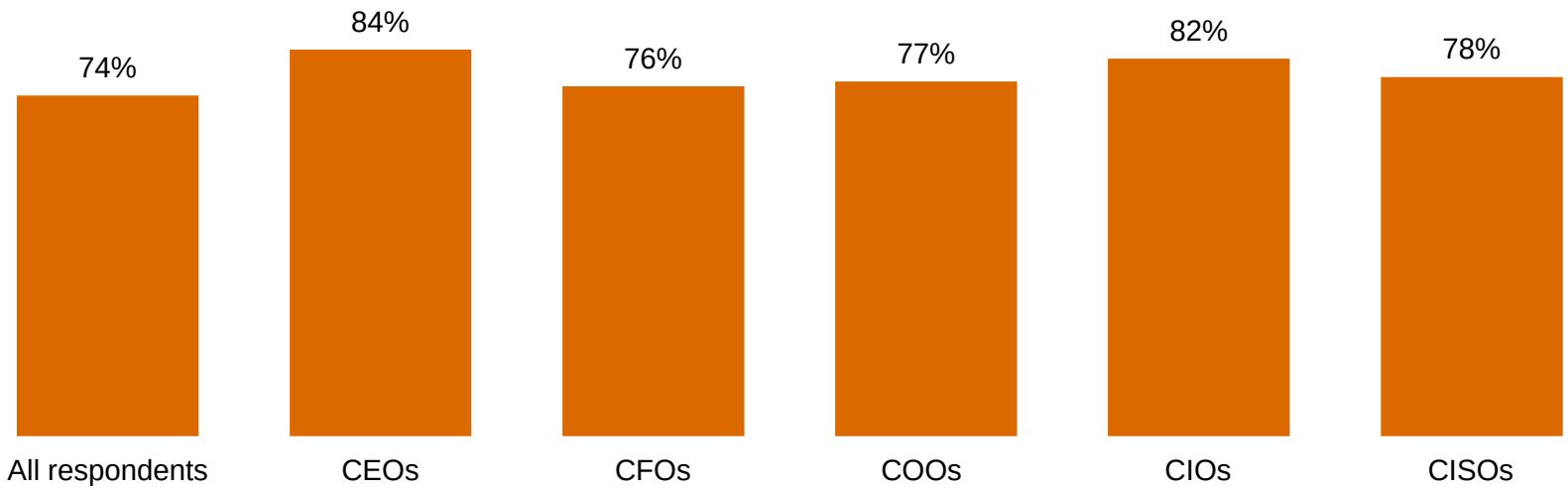
Section 2

Confidence in an era of advancing risks

Confidence is high: 74% of respondents believe their security activities are effective, with top execs even more optimistic.

In the C-suite,* 84% of CEOs say they are confident in their security program. Note that CFOs are the least confident among executives.

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

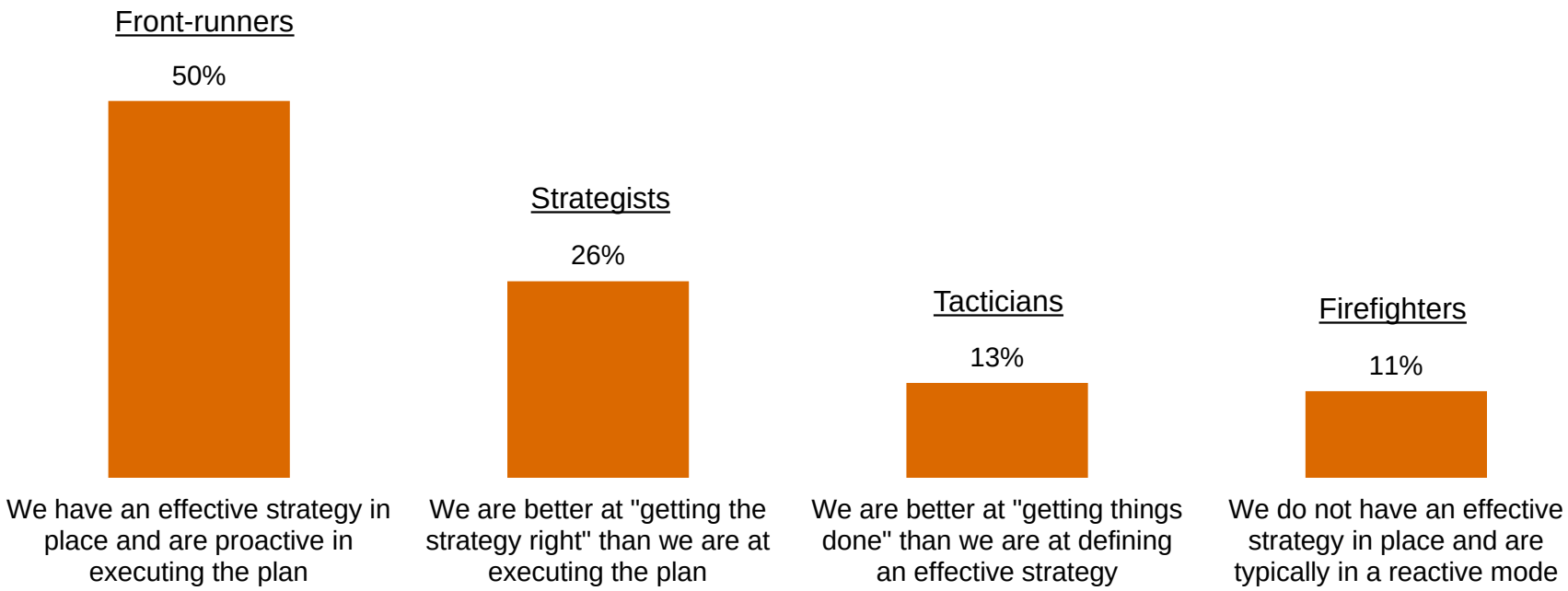


* CEOs, CFOs, and COOs

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”

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

50% say they have an effective strategy in place and are proactive in executing the plan, a 17% increase over last year. 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?"

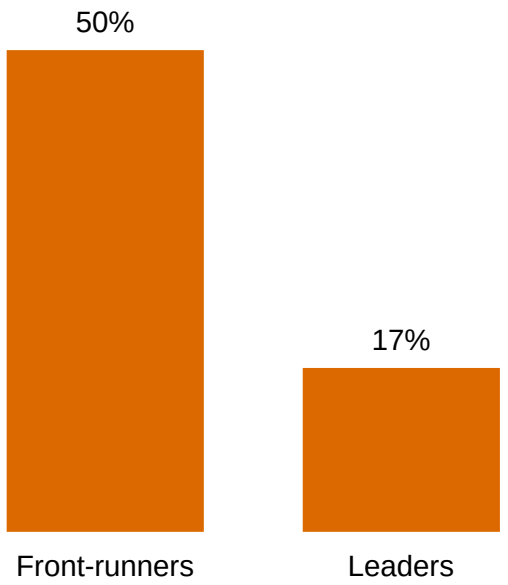
But closer scrutiny reveals far fewer real leaders than front-runners.

We measured respondents' self-appraisal against four key criteria to filter for leadership.

To qualify, organizations must:

- 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
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are still significantly fewer real leaders than self-identified front-runners.

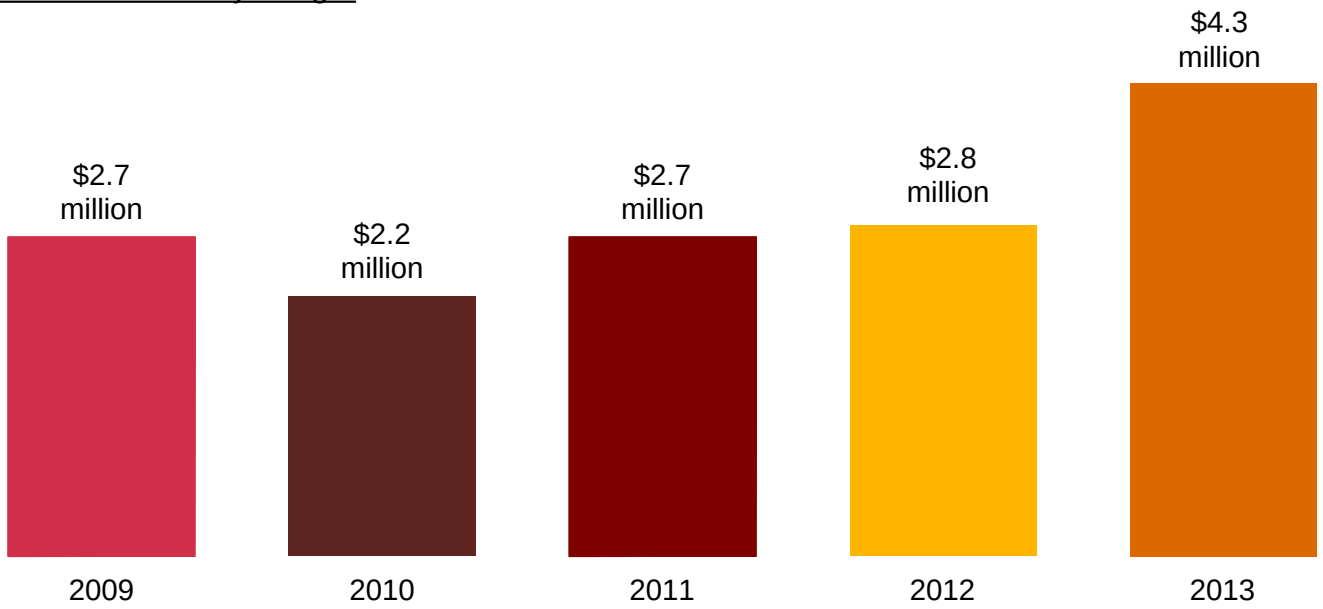


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Information security budgets increase significantly.

Security budgets average $4.3 million this year, a gain of 51% over 2012. Organizations understand that today's elevated threat landscape demands a substantial boost in security investment.

Average information security budget



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

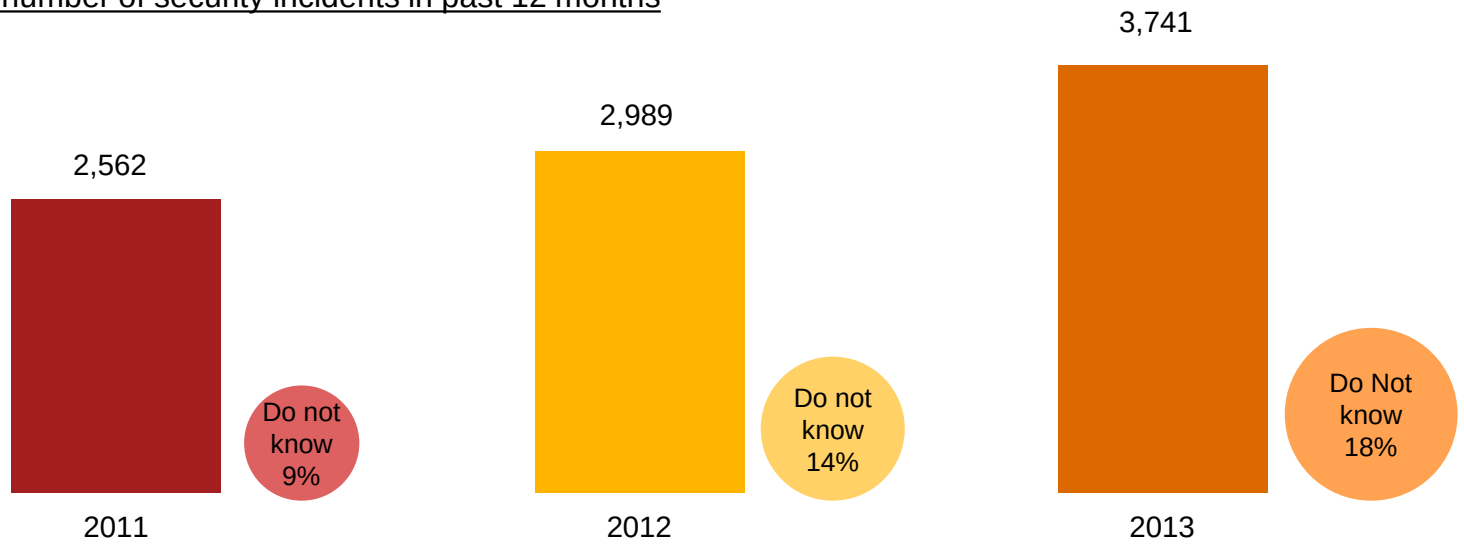
Section 3

Today's incidents, yesterday's strategies

*Respondents are detecting more security incidents.**

The number of incidents detected in the past 12 months increased by 25%, perhaps an indication of today's elevated threat environment. It is troubling that respondents who do not know the number of incidents has doubled over two years. This may be due to continued investments in security products based on outdated models.

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?"

A US-only survey shows that, even when in place, security technologies and policies often do not prevent incidents.

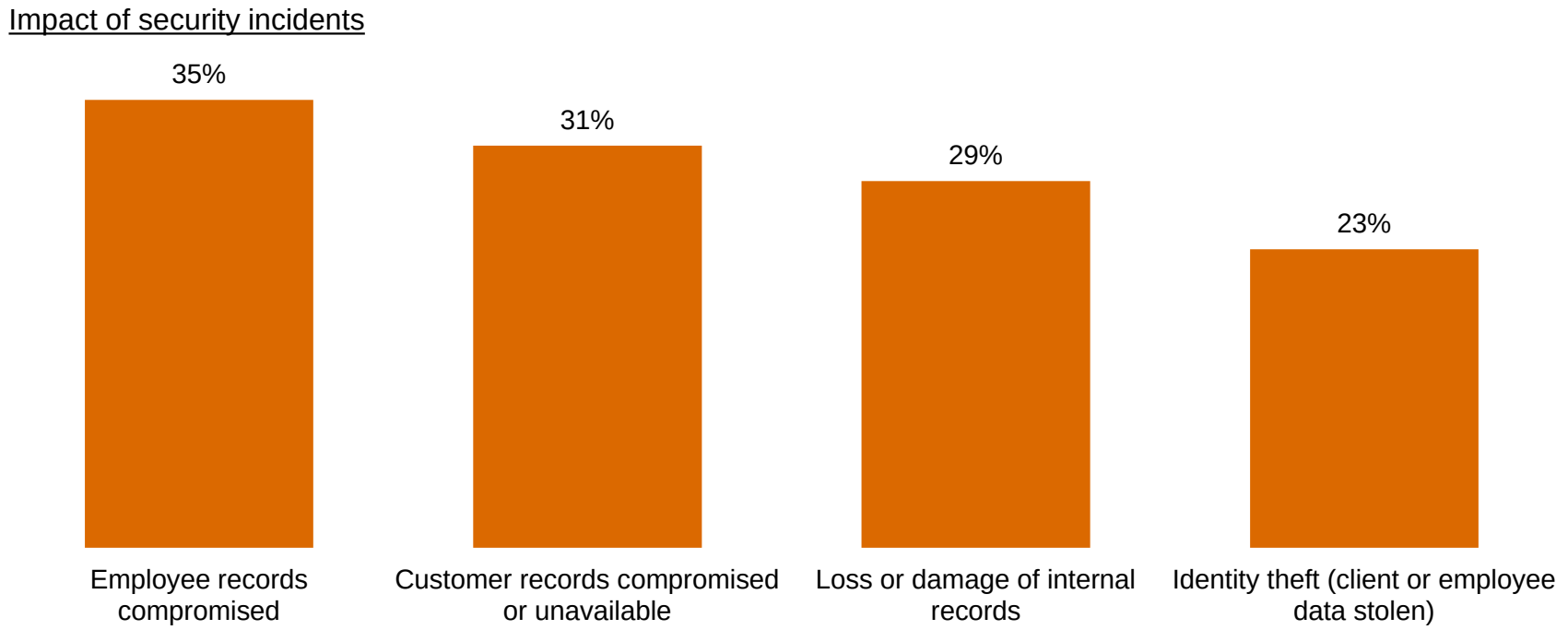
Respondents to the 2013 US State of Cybercrime Survey,[1] co-sponsored by PwC, say security incidents increased 33%, despite implementation of security practices. For many, existing security technologies and policies are simply not keeping pace with fast-evolving threats.

Security technologies and policies in place (US only)	
Use policy-based network connections to detect and/or counter security incidents	68%
Inspect inbound and outbound network traffic	61%
Use account/password management in an attempt to reduce security incidents	60%
Have an acceptable-use policy	55%
Use malware analysis as a tool to counter advanced persistent threats (APTs)	51%
Use data loss prevention technology to prevent and/or counter security incidents	51%
Use security event management to detect and/or counter security incidents	50%
Use cyber-threat research in an attempt to reduce security incidents	25%
Do not allow non-corporate-supplied devices in the workplace/network access	17%

[1] *2013 US State of Cybercrime Survey*, co-sponsored by *CSO* magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

Employee and customer data continue to be easy targets.

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 jumped more than 100% over last year.

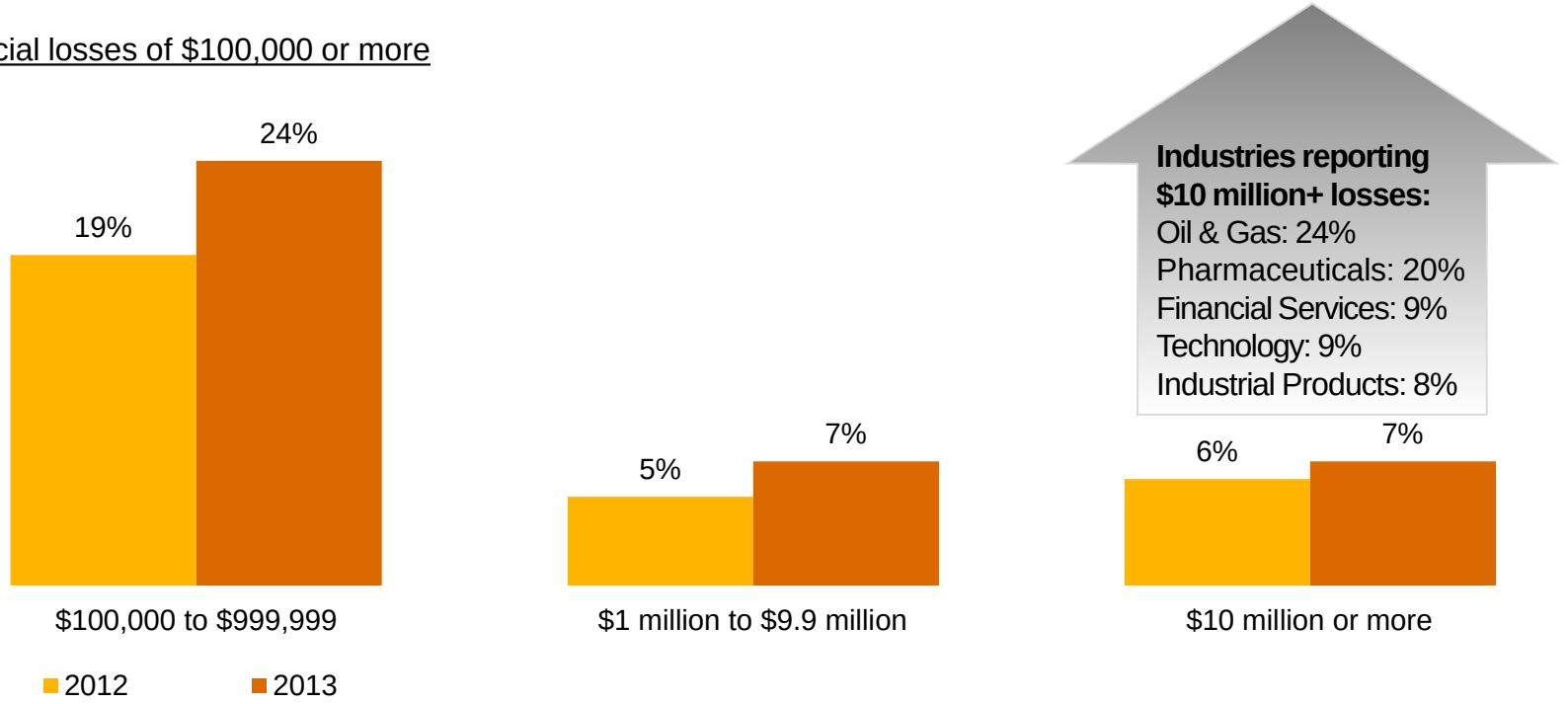


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

The financial costs of incidents are rising, particularly among organizations reporting high dollar-value impact.

Average losses are up 18% over last year, which is not surprising given the costs and complexity of responding to security incidents. Big liabilities are increasing faster than smaller losses: Respondents reporting losses of $10 million-plus is up 51% from 2011.

Financial losses of $100,000 or more

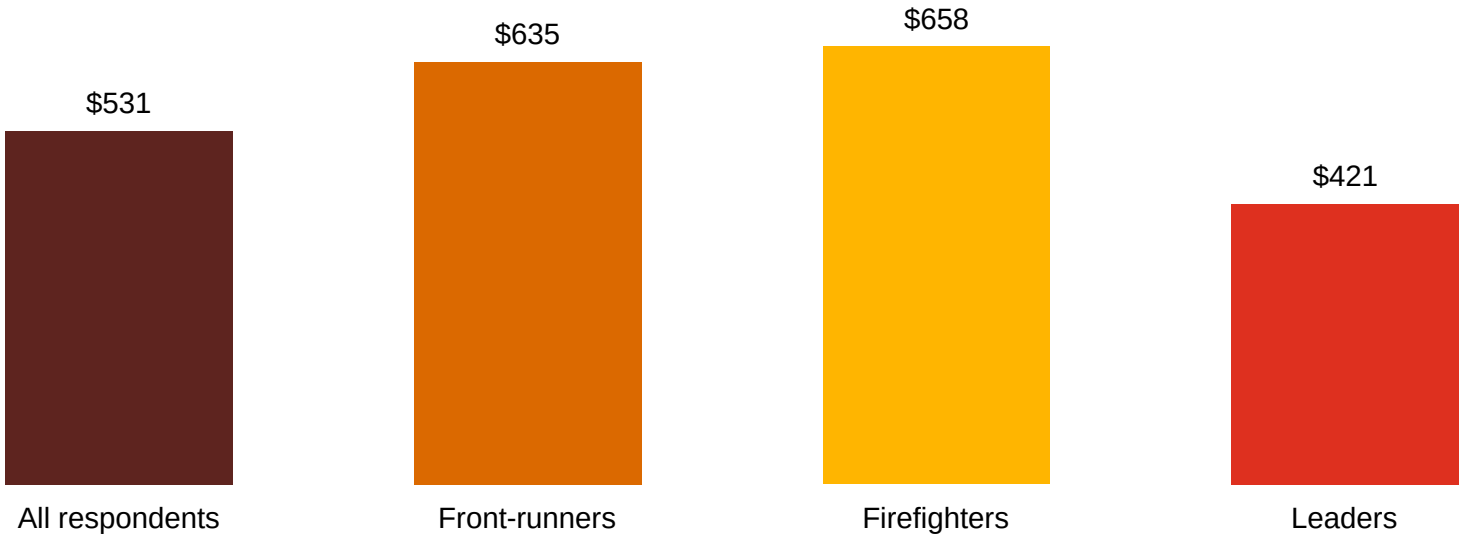


Question 22A: “Estimated total financial losses as a result of all security incidents”

Organizations that identify as front-runners report a high cost per security incident; leaders claim the lowest cost.

Front-runners spend almost as much per incident as firefighters—those least prepared to run an effective security program.

The average cost per security incident

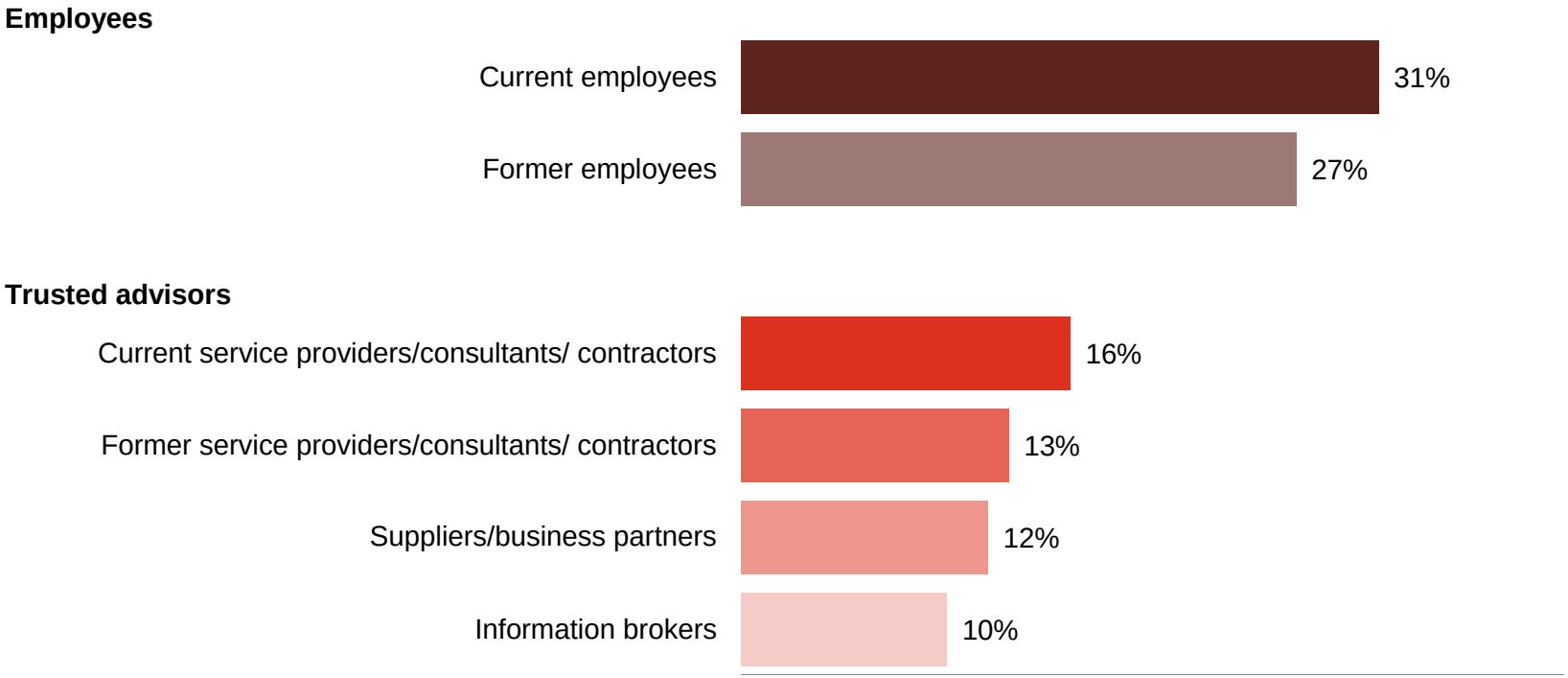


Question 18: “What is the number of security incidents detected in the past 12 months?” Question 22A: “Estimated total financial losses as a result of all security incidents”

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

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

Estimated likely source of incidents

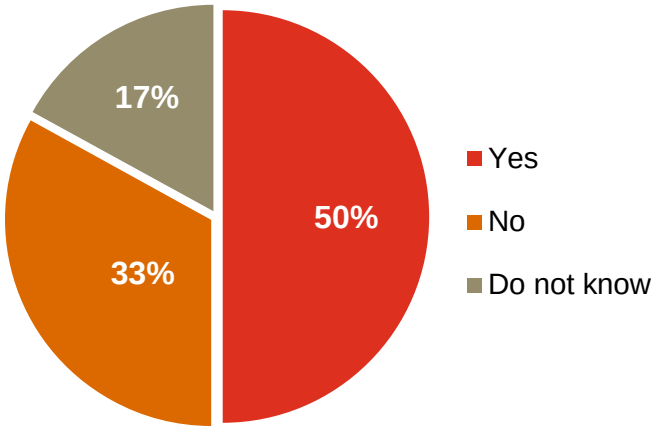


Question 21: "Estimated likely source of incidents" (Not all factors shown.)

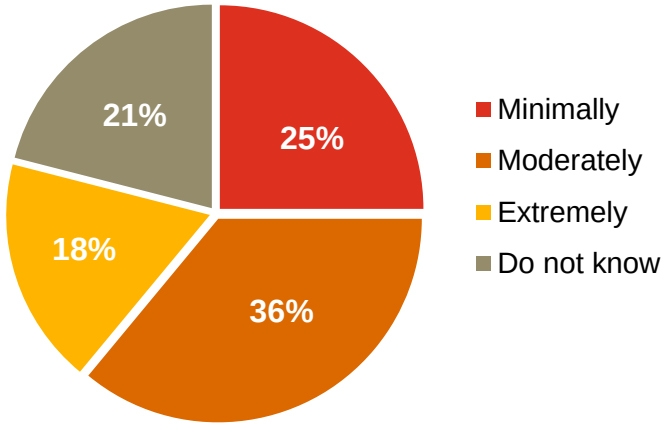
Yet many organizations do not have plans for responding to insider threats, and those that do are not highly effective.

The 2013 US State of Cybercrime Survey[2] shows that many organizations have not implemented effective strategies for responding to in-house adversaries.

Organization has a formal plan for responding to insider security incidents



Organization is effective in reporting, managing, and intervening cyber threats with internal employees

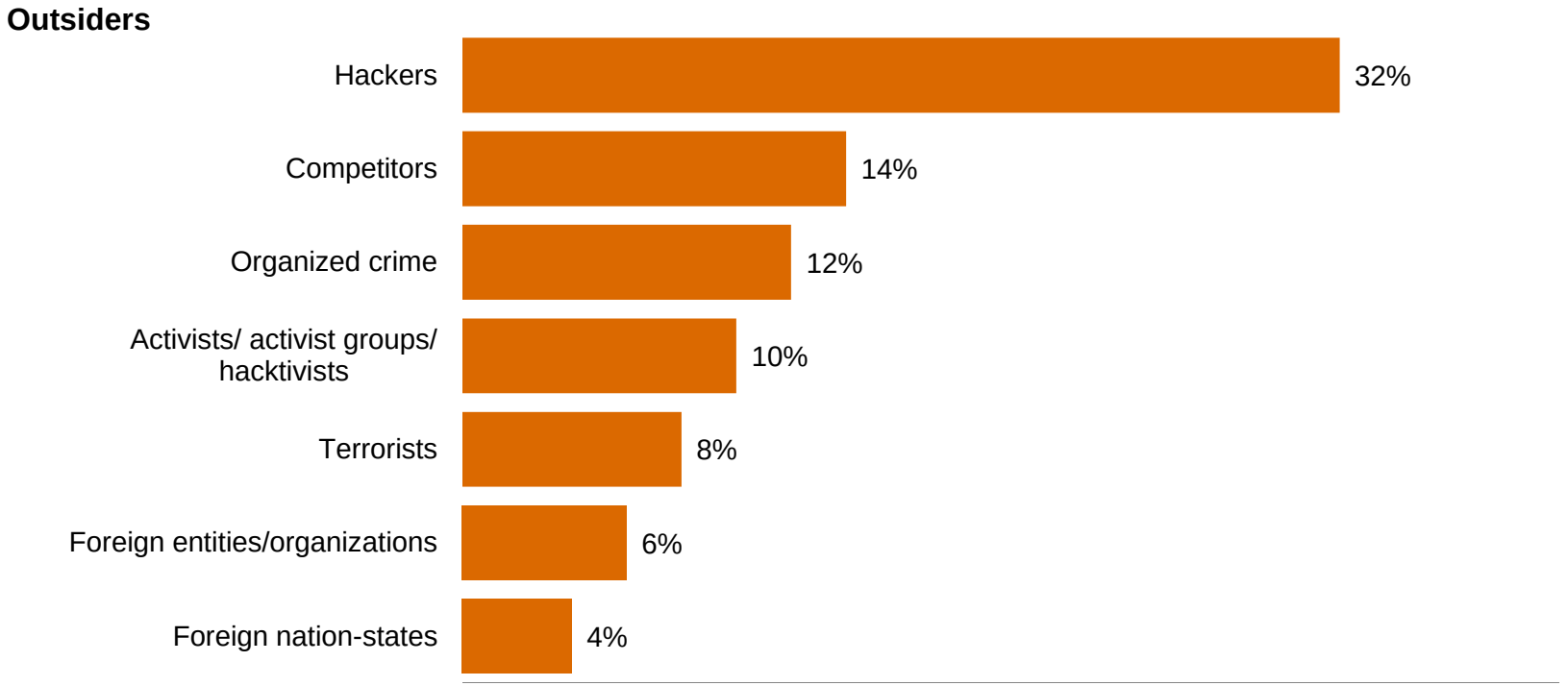


[2] *2013 US State of Cybercrime Survey*, co-sponsored by *CSO* magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

While attacks backed by nation-states make headlines, your organization is more likely to be hit by other outsiders.

Only 4% of respondents report security incidents perpetrated by foreign nation-states. Hackers represent a much more likely danger.

Estimated likely source of incidents



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

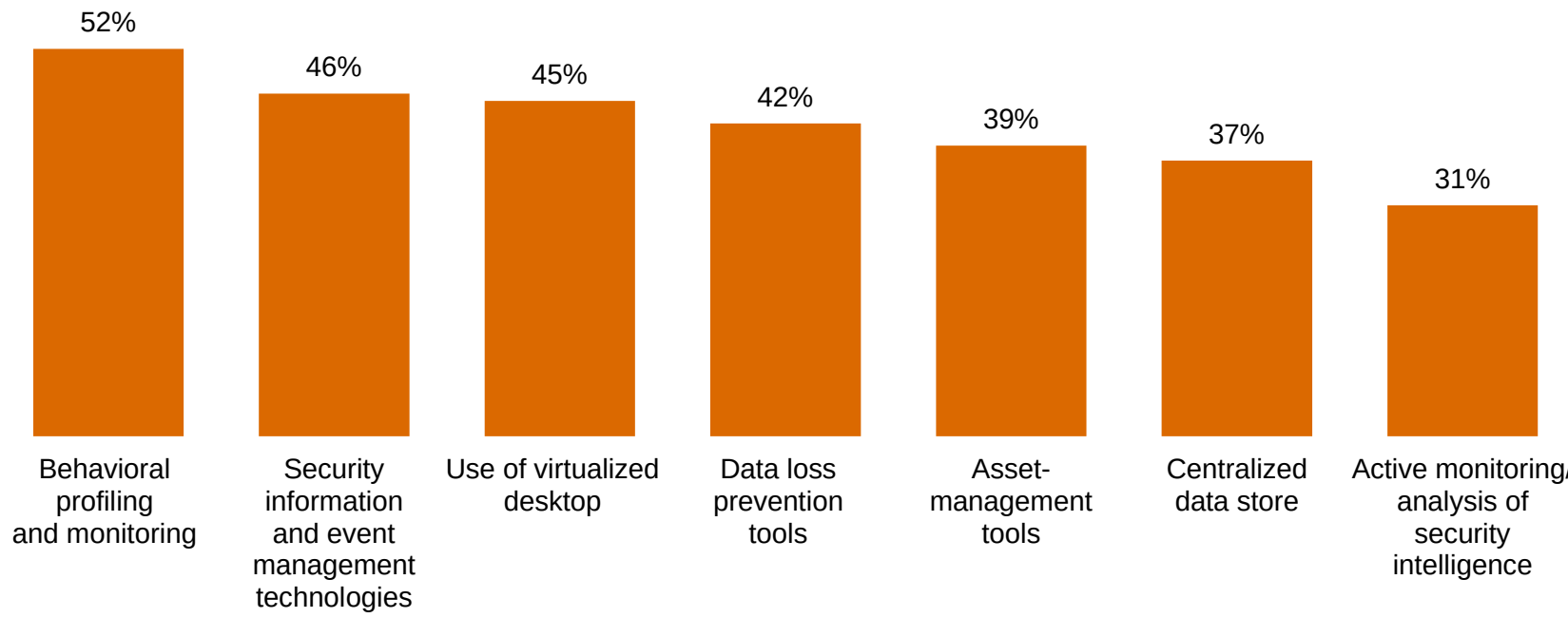
Section 4

A weak defense against adversaries

Many organizations have not 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. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place



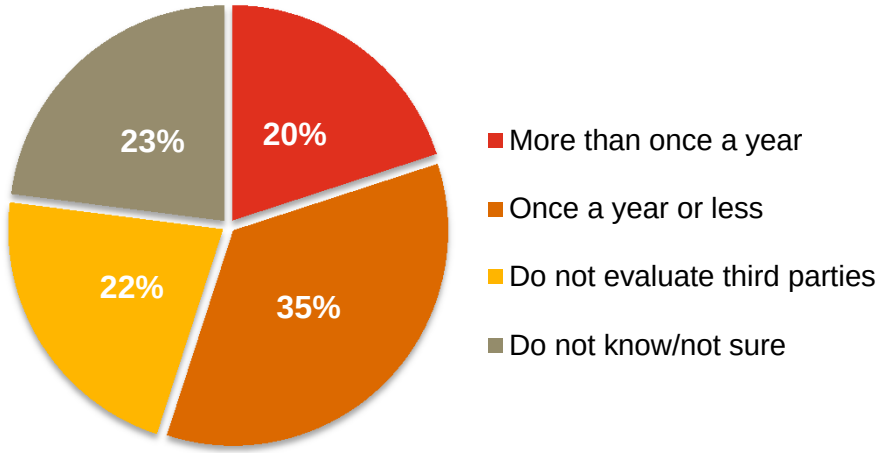
Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "Which technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

In the US, many organizations lack an understanding of risks associated with third parties.

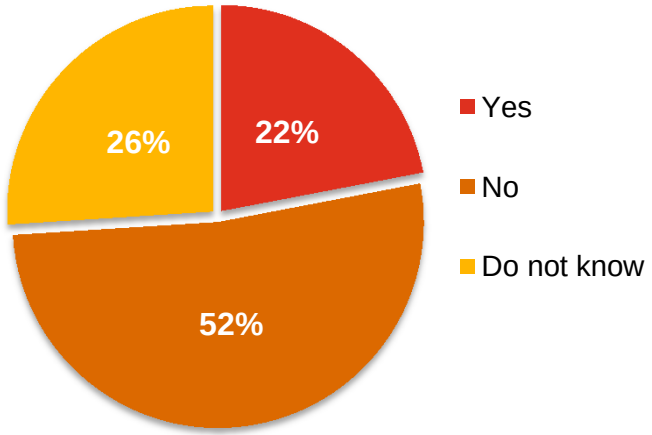
The 2013 US State of Cybercrime Survey[3] found that many respondents do not have policies and tools to assess security risks of third parties. More than ever, company leaders should not view cybersecurity as simply a technology problem; it is now a risk-management issue.

Does your organization:

Evaluate the security of third parties with which the organization shares data or network access?



Conduct incident response planning with third-party supply chain?

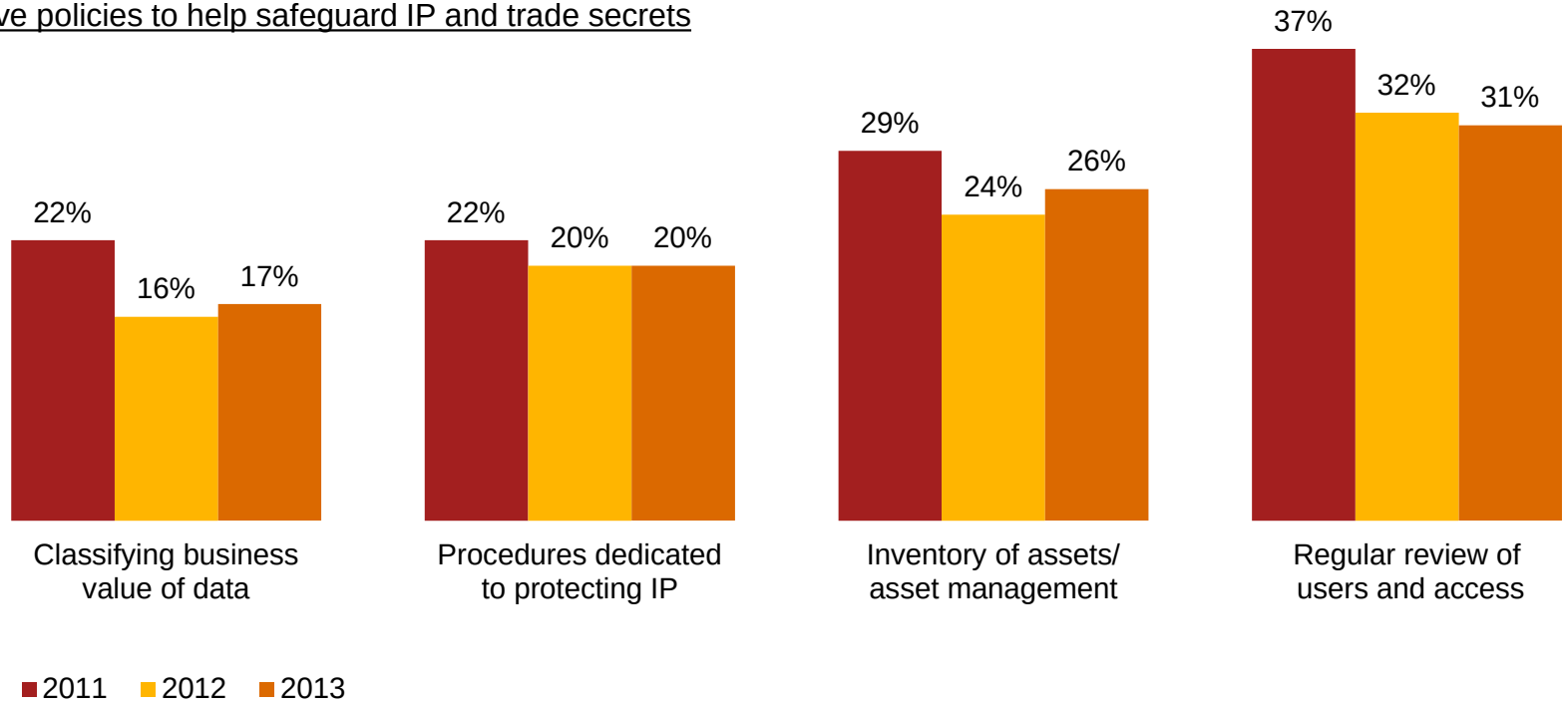


[3] *2013 US State of Cybercrime Survey*, co-sponsored by *CSO* magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

Despite the potential consequences, many respondents do not adequately safeguard their high-value information.

It is imperative that organizations identify, prioritize, and protect their "crown jewels." Many, however, have not yet implemented basic policies necessary to safeguard intellectual property (IP).

Have policies to help safeguard IP and trade secrets

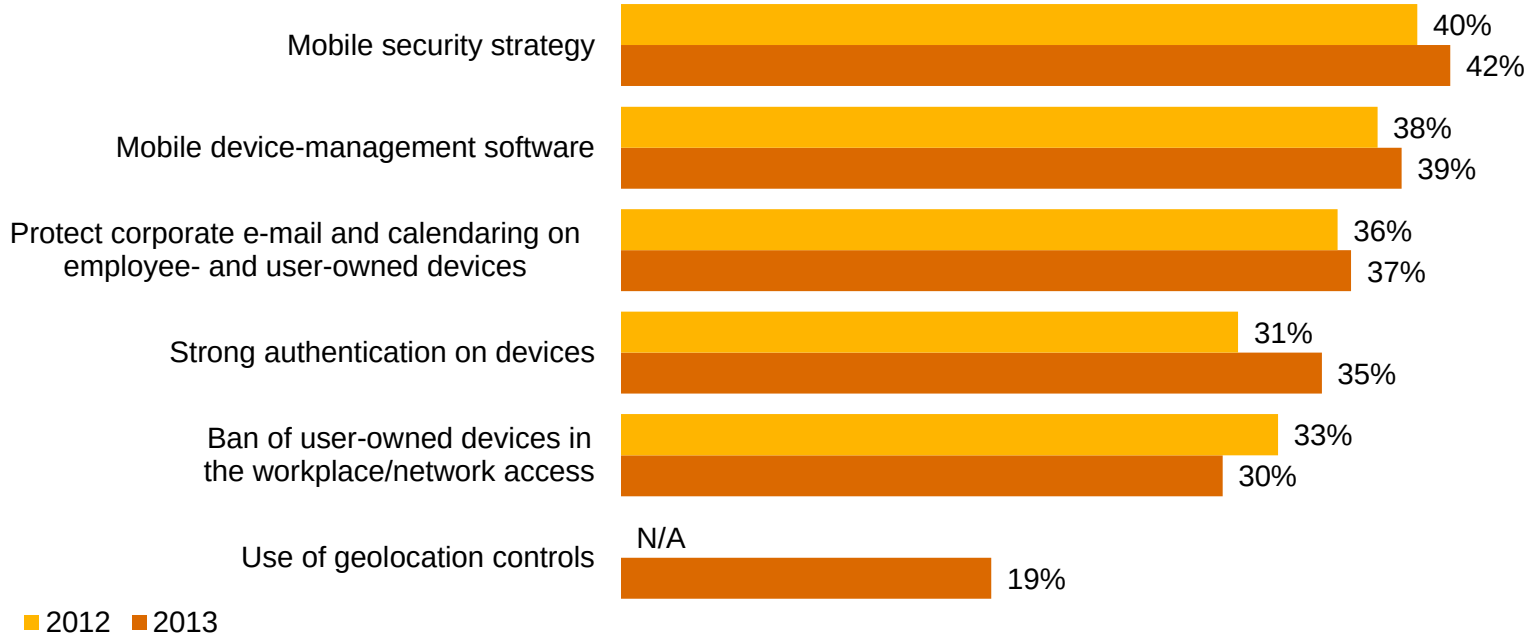


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

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

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

Initiatives launched to address mobile security risks

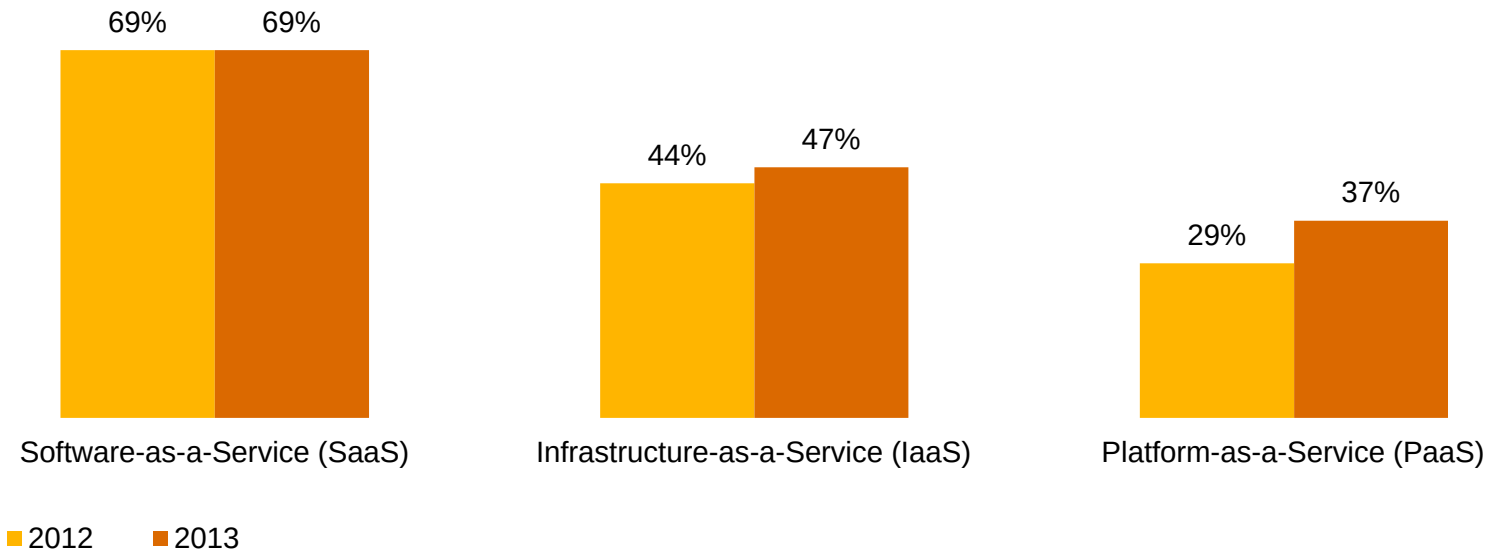


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

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

While 47% of respondents use cloud computing—and among those who do, 59% say security has improved—only 18% include provisions for cloud in their security policy. SaaS is the most widely adopted cloud service, but PaaS shows strong 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.)

28% of respondents do not collaborate with others to improve security, forgoing a powerful offensive tool.

And that can impede security in today's interconnected world. In PwC's 5th Annual Digital IQ Survey,[4] we found that firms with collaborative C-suites intertwine business strategy and IT—and that often improves performance and enables quick adaption to market changes.

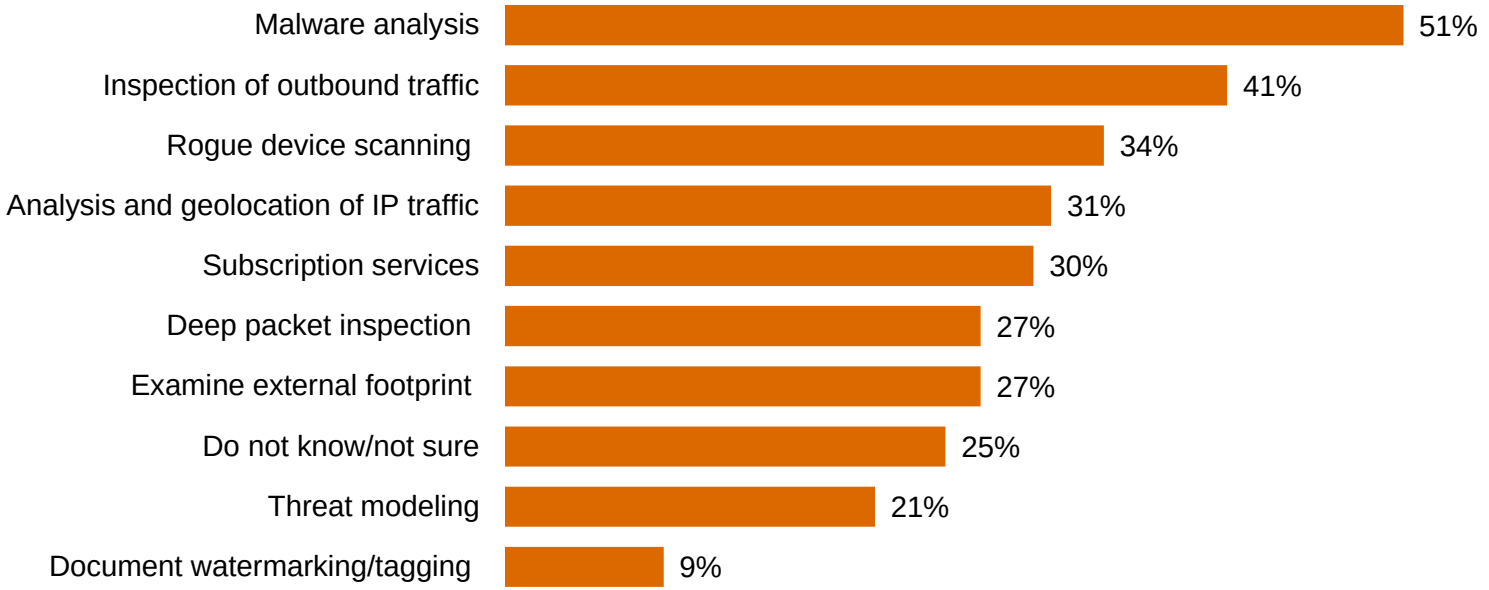
Reasons for not collaborating on information security

[4] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
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.)

In the US, sophisticated threat-intelligence tools necessary to combat advanced persistent threats are largely absent.

Advanced persistent threats require a new information-protection model that focuses on continuous monitoring of network activity and high-value information. The 2013 US State of Cybercrime Survey[5] found that the majority of US organizations lack these capabilities.

Activities and techniques used to counter advanced persistent threats



[5] *2013 US State of Cybercrime Survey*, co-sponsored by *CSO* magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

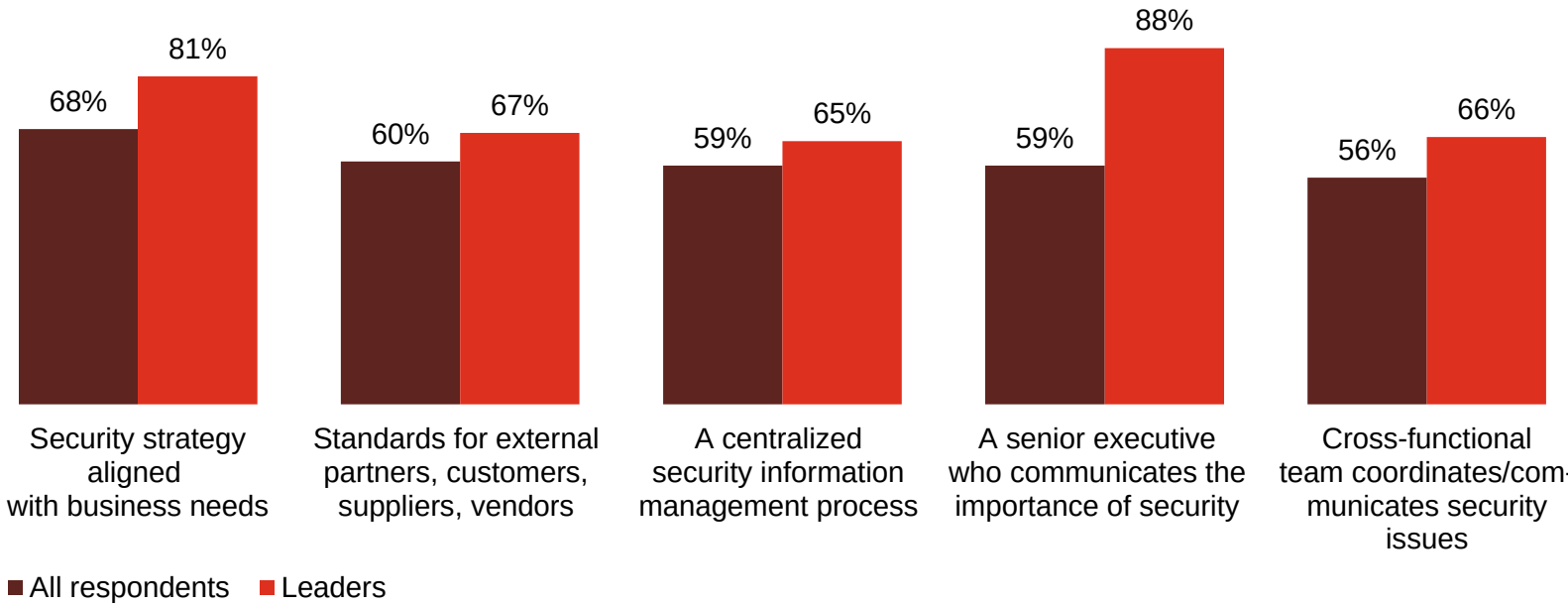
Section 5

Preparing for the threats of tomorrow

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

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

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



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?"

Many organizations have invested in technology safeguards to secure their ecosystems against today's evolving threats.

Leaders are more likely to have implemented these technologies. But given today's elevated threat landscape, *all* organizations should strongly consider implementation of these safeguards.

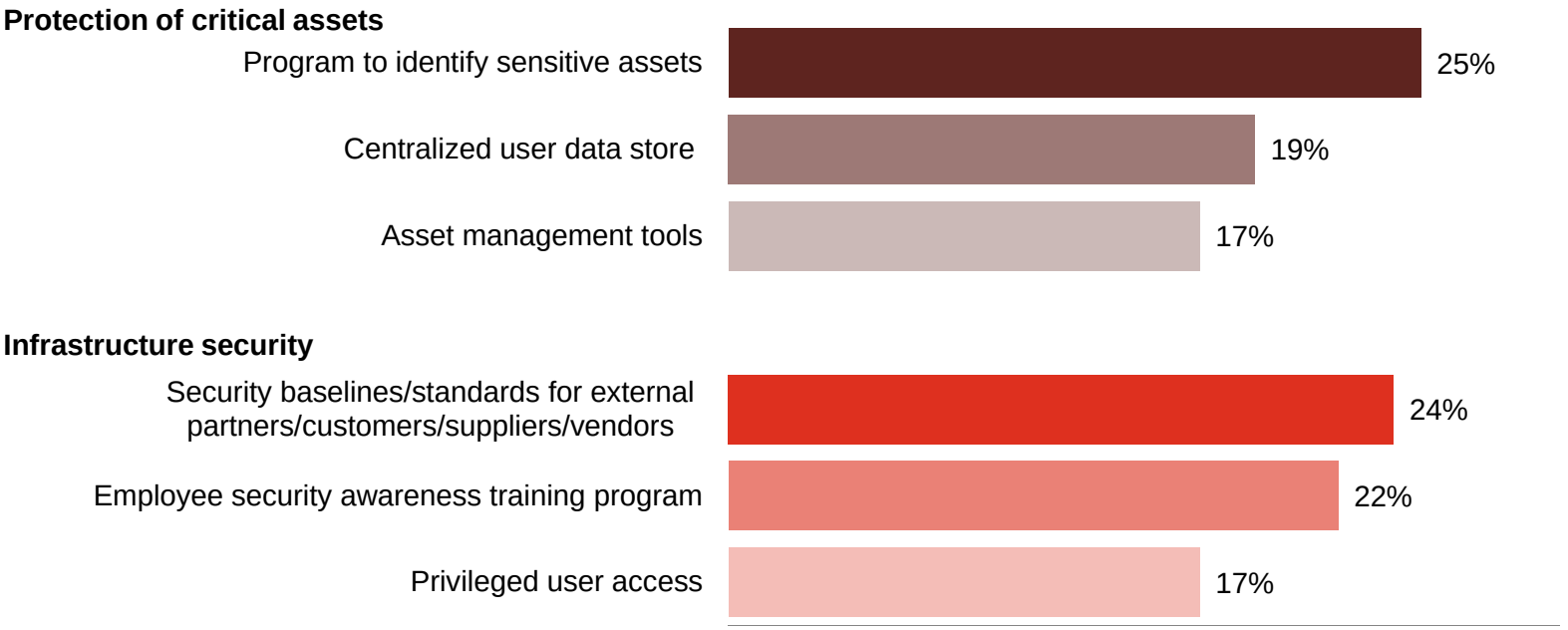
Technology safeguards currently in place	All Respondents	Leaders
Malicious code detection tools	74%	88%
Vulnerability scanning tools	62%	71%
Data loss prevention tools	58%	67%
Mobile device malware detection	57%	67%
Security event correlation tools	57%	66%
Virtualized desktop interface	55%	65%
Code analysis tools	54%	64%
Protection/detection management solution for APTs	54%	66%
Security information and event management technologies	54%	66%

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

What business imperatives and processes will respondents invest in?

Some of the highest priorities include technologies that can help the organization protect its most valuable assets and gain strategic advantages.

Safeguards not in place but a top priority over the next 12 months

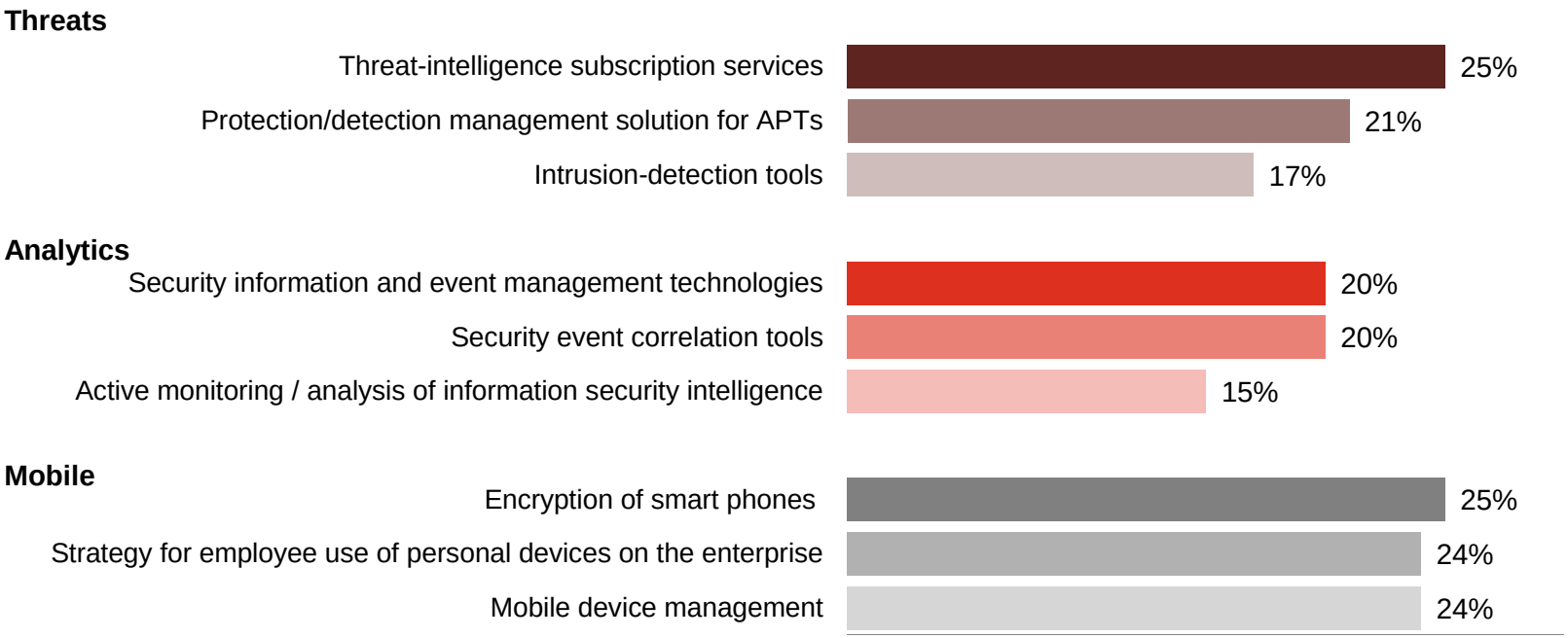


Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and organizations are prioritizing technologies that can help gain a better understanding of threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months



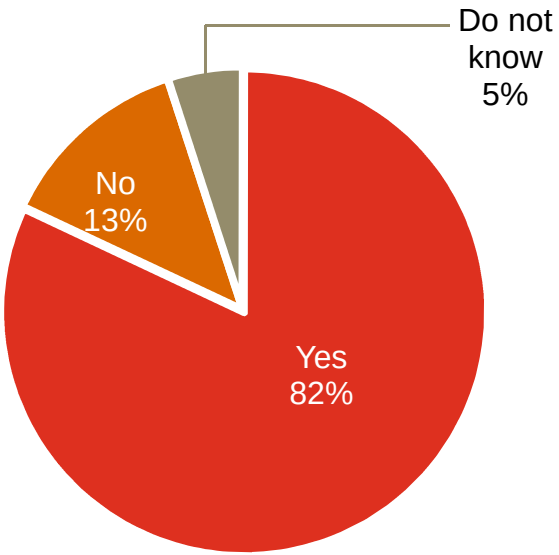
Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Global leaders are likely to see the potential benefits of collaboration and information sharing.

Many leaders realize that public-private partnerships can be an effective way to gain intelligence about fast-changing security threats.

Formally collaborate on information security with others in the industry (leaders)

82% of **leaders** collaborate



Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?"

Effective security demands that organizations align information security with business strategy and objectives.

More respondents say security spending and policies are completely aligned with business objectives. In other words, they are starting to understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

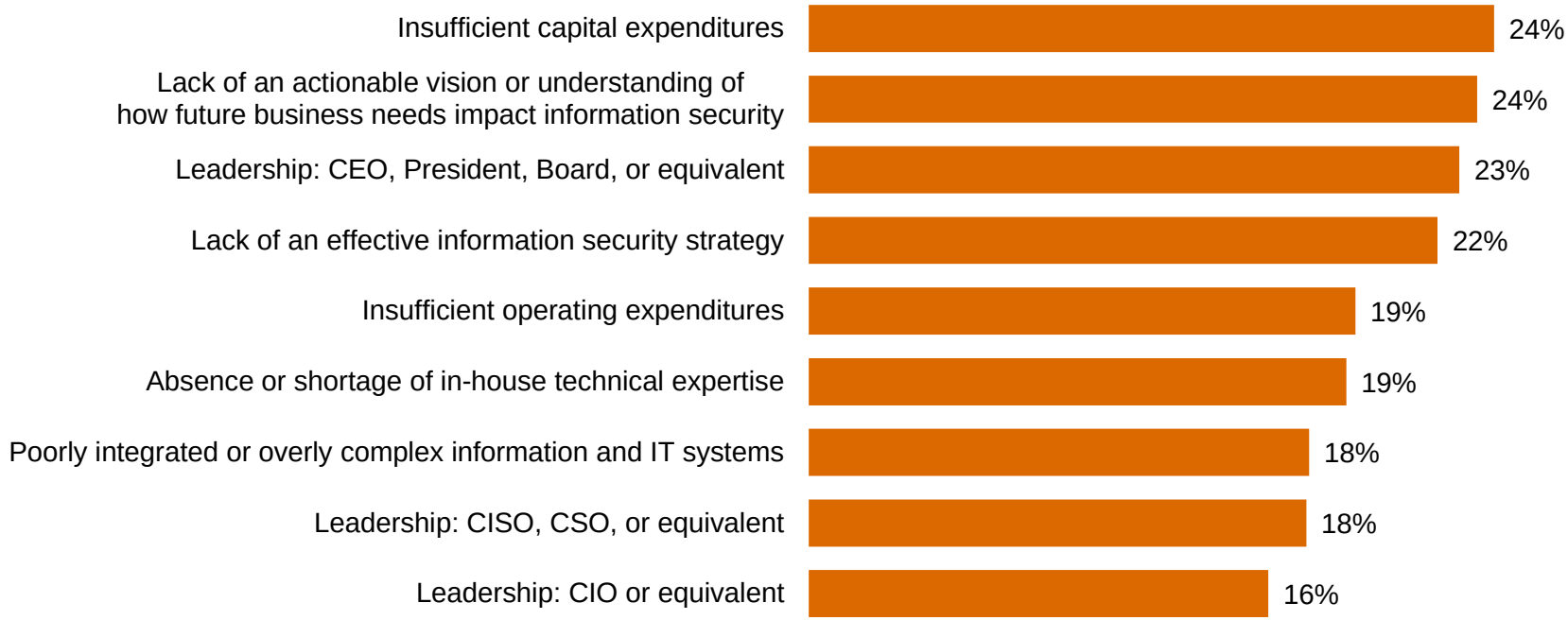
Level of alignment with organization's business objectives (somewhat or very aligned)

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?"

More money and committed leadership are needed to overcome obstacles to advancing security.

These are critical because an evolved approach to security requires the support of top executives and an adequate budget that is aligned with business needs.

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?"

Section 6

The global cyber-defense race

South America is poised to take the lead in information security investment, safeguards, and policies.

Asia Pacific remains very strong in security spending and leading practices, while Europe and North America lag in many aspects.

	South America	Asia Pacific	Europe	North America
Security spending will increase over the next 12 months	66%	60%	46%	38%
Have an overall security strategy	75%	79%	77%	81%
Employ a Chief Information Security Officer	75%	74%	68%	65%
Have a senior executive who communicates the importance of security	68%	69%	51%	55%
Measured/reviewed effectiveness of security policies and procedures in past year	70%	69%	53%	49%
Have policy for backup and recovery/business continuity	58%	55%	45%	47%
Require third parties to comply with privacy policies	55%	58%	55%	62%
Employee security awareness training program	54%	63%	55%	64%
Have procedures dedicated to protecting intellectual property (IP)	20%	24%	17%	21%
Have intrusion-detection technologies in place	64%	67%	63%	67%
Inventory of where personal data are collected, transmitted, and stored	53%	60%	52%	64%
Collaborate with others to improve security and reduce risks	66%	59%	45%	42%

(Not all factors shown.)

China has the advantage in implementation of technology safeguards to protect against today's dynamic threats.

Russia also shows solid progress in deployment of safeguards that monitor data and assets, while the US leads Brazil—and India plays catch-up.

	China	Russia	US	Brazil	India
Centralized user data store	73%	68%	65%	64%	61%
Behavioral profiling and monitoring	60%	48%	44%	57%	48%
Encryption of smartphones	61%	51%	57%	52%	53%
Intrusion detection tools	65%	76%	67%	64%	68%
Vulnerability scanning tools	72%	60%	63%	63%	58%
Asset management tools	71%	60%	64%	59%	62%
Use of virtual desktop interface	64%	61%	56%	55%	52%
Protection/detection management solution for APTs	62%	56%	56%	54%	48%
Security information and event management (SIEM) technologies	66%	59%	57%	54%	48%

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

The fusion of cloud computing, mobility, personal devices, and social media is a unified challenge for all countries.

No country has fully addressed the potential impact of these four interconnected issues, but China and the US are setting the pace for implementation of security strategy.

	China	US	Russia	Brazil	India
Cloud security strategy	51%	52%	45%	49%	47%
Mobile device security strategy	64%	57%	51%	49%	50%
Social media security strategy	59%	58%	47%	51%	50%
Security strategy for employee use of personal devices on the enterprise	71%	64%	56%	53%	54%

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

Section 7

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 ten 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

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying 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.

Gain advantage from 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.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

Gary Loveland
Products & Services Industries
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Products & Services Industries
646.471.5731
mark.a.lobel@us.pwc.com

Joe Nocera
Financial Services Industry
312.298.2745
joseph.nocera@us.pwc.com

Peter Harries
Health Industries
213.356.6760
peter.harries@us.pwc.com

John Hunt
Public Sector
703.918.3767
john.d.hunt@us.pwc.com

Dave Burg
Forensic Services
703.918.1067
david.b.burg@us.pwc.com

Dave Roath
Risk Assurance Services
646.471.5876
david.roath@us.pwc.com

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

PwC