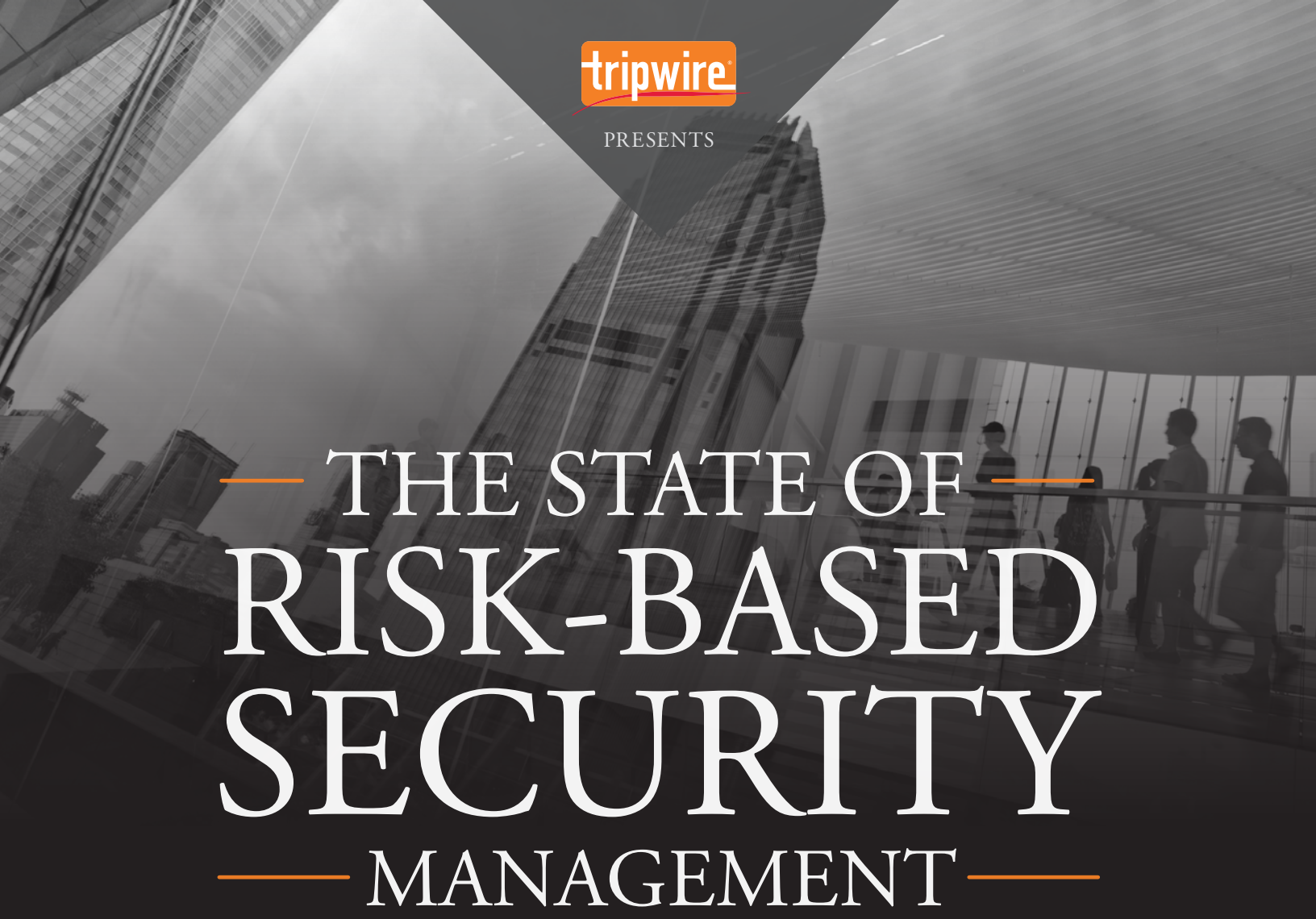


tripwire

PRESENTS

THE STATE OF RISK-BASED SECURITY MANAGEMENT

US & UK
2013

Ponemon Institute LLC

RESEARCH REPORT

CHAPTER 1: METHODOLOGY

A sampling frame of 24,550 US and 18,012 UK individuals who work in IT operations, IT security, business operations, compliance/internal audit and enterprise risk management were selected for this survey. As shown in Figure 1-1, 918 respondents completed the survey in the US and 706 in the UK. Screening and reliability checks removed 169 surveys in the US and 135 in the UK. The final sample in the US was 749 surveys (a 3.1% response rate) and in the UK was 571 surveys (a 3.2% response rate).

FIGURE 1-1. Sample Response–US & UK

	US–2013	UK–2013
Total sampling frame	24,550	18,012
Total returns	918	706
Rejected and screened surveys	169	135
Final sample	749	571
Response rate	3.1%	3.2%

Figures 1-2 and 1-3 report the respondents' current position level within the organization. Sixty percent of respondents in the US and 57% in the UK are at or above the supervisory level.

FIGURE 1-2. Organization level–US

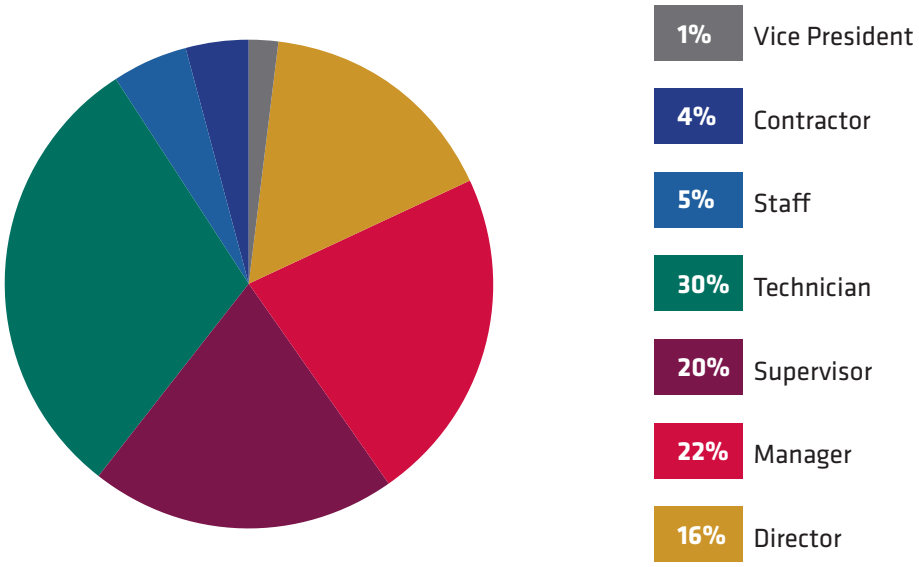
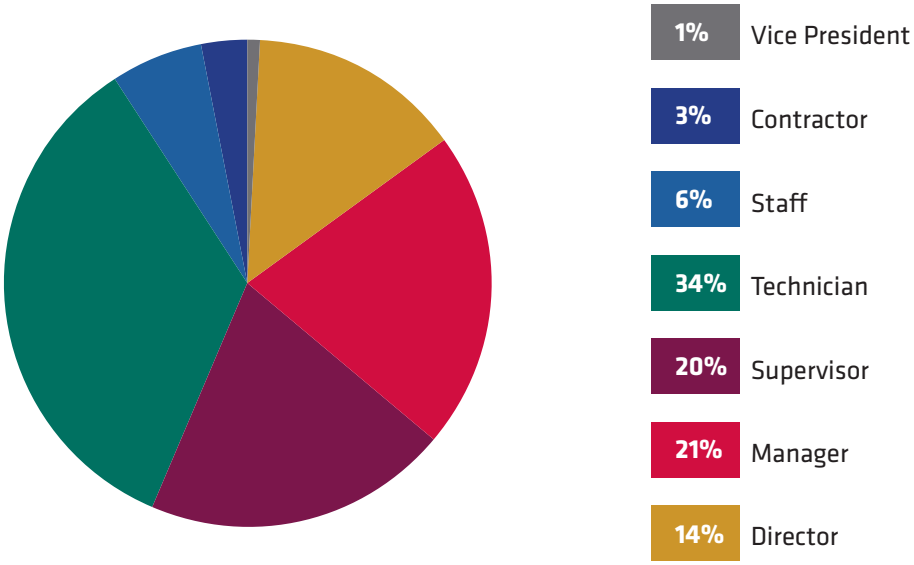


FIGURE 1-3. Organization level—UK



As shown in Figures 1-4 and 1-5, 53% of respondents in the US and 54% in the UK indicate they report to the Chief Information Officer. Twenty-two percent in US and 21% in the UK report to the Chief Information Security Officer.

FIGURE 1-4. Primary person reported to in the organization—US

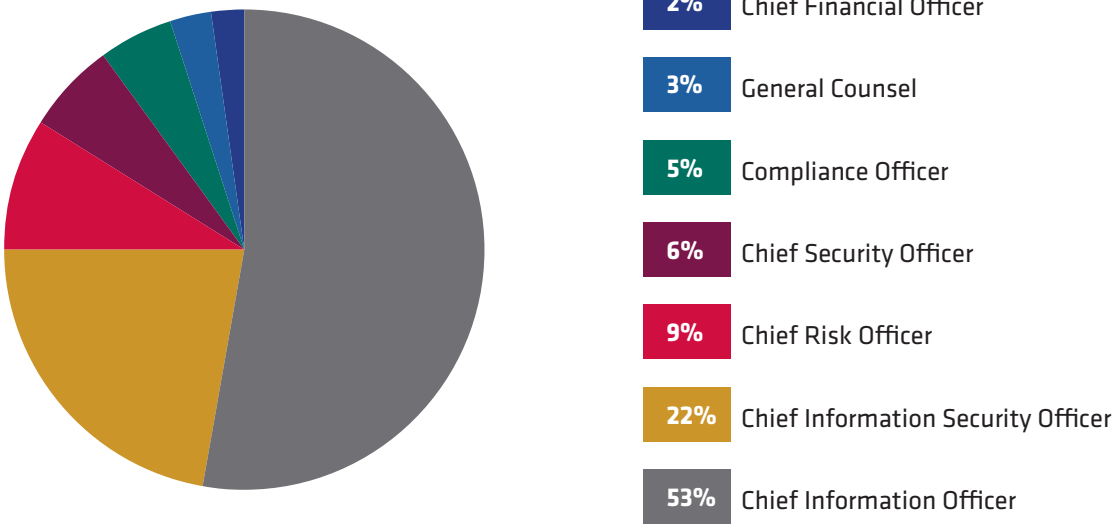
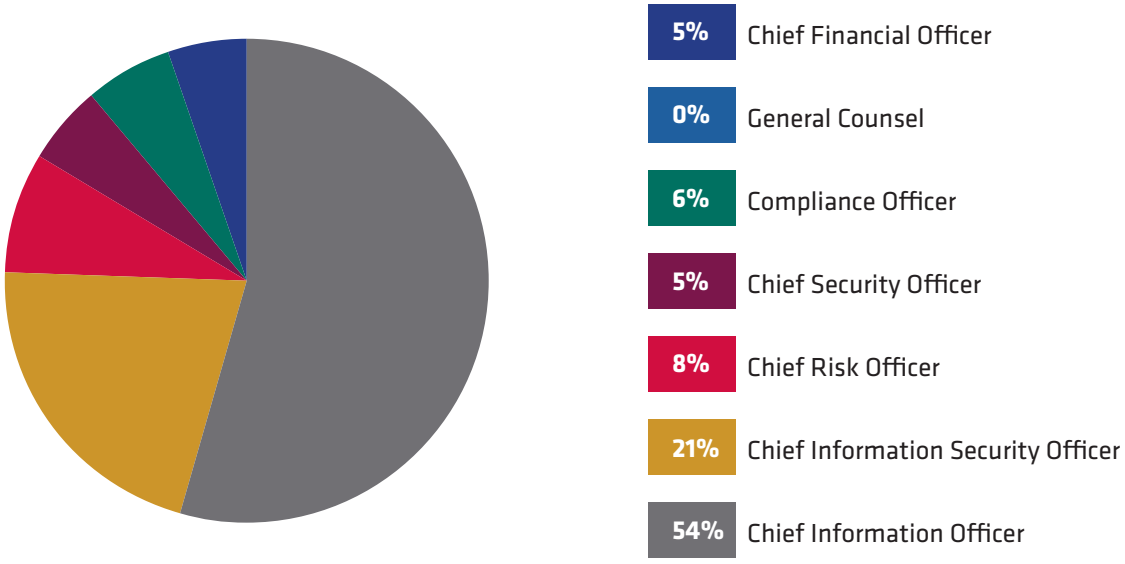


FIGURE 1-5. Primary person reported to in the organization–UK



Figures 1-6 and 1-7 report the industry segments of respondents' organizations. This chart identifies financial services (19% in US and 17% in the UK) as the largest segment, followed by public sector (13% in the US and 16% in the UK) and health and pharmaceutical (11% in the US and 14% in the UK).

FIGURE 1-6. Industry distribution of respondents' organizations–US

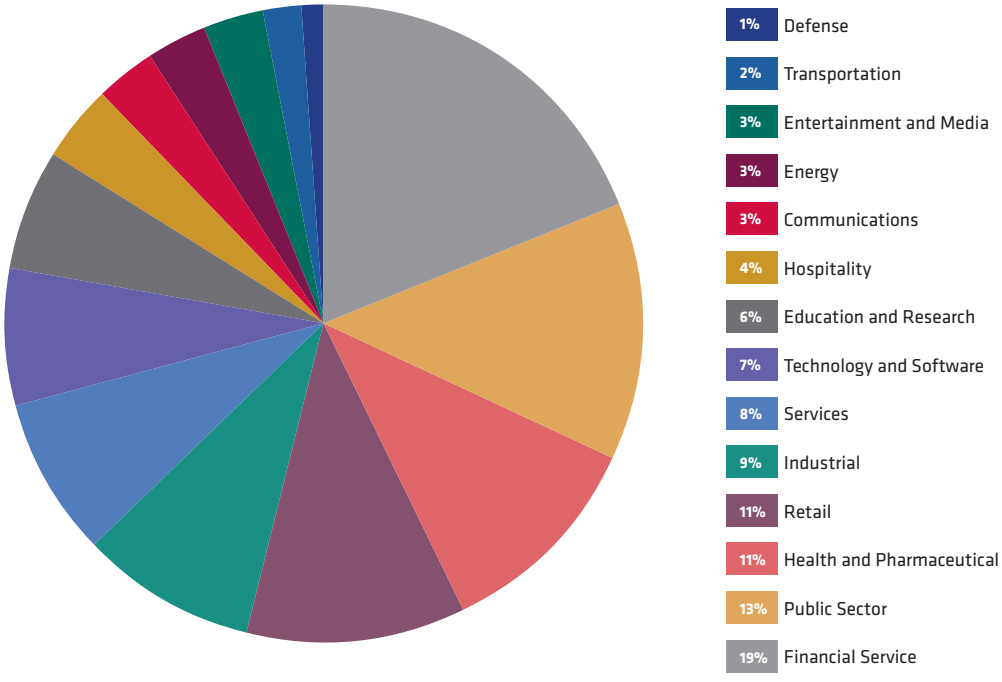
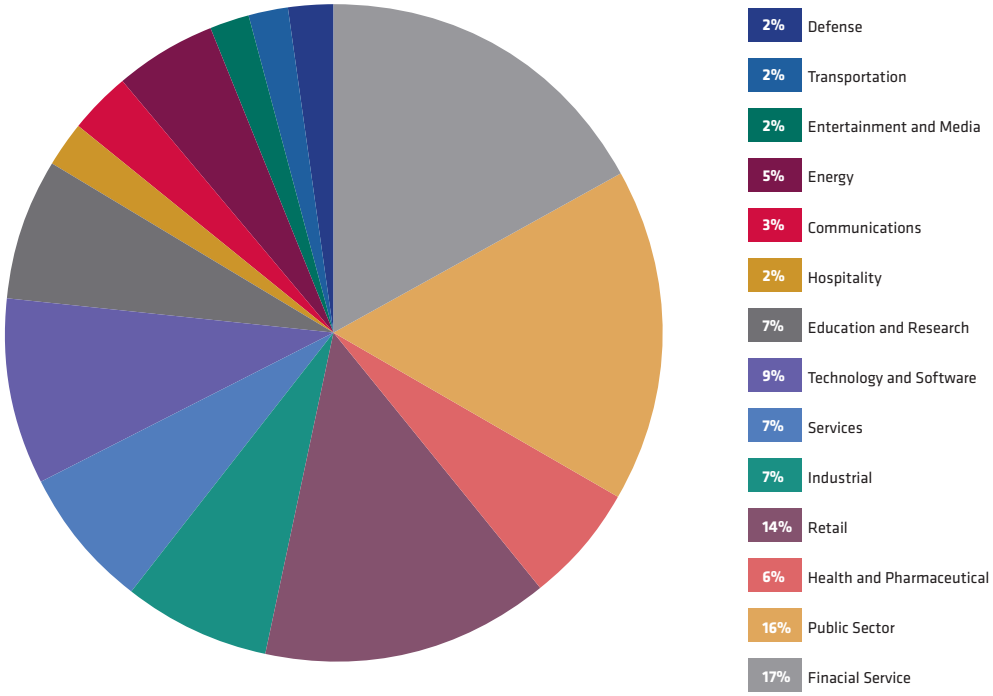


FIGURE 1-7. Industry distribution of respondents' organizations–UK



More than half of the respondents (68% US and 64% UK) are from organizations with a global headcount of over 500 employees, as shown in Figures 1-8 and 1-9.

FIGURE 1-8. Global headcount–US

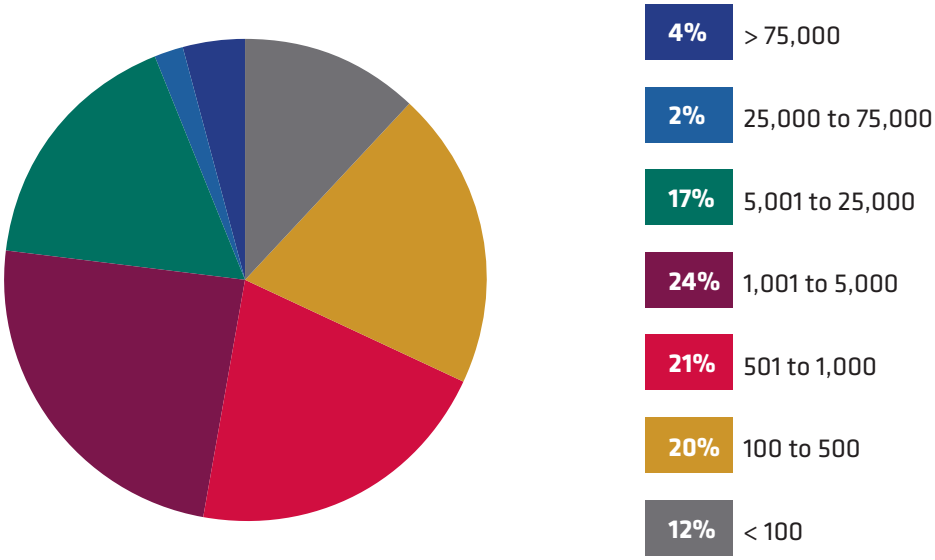
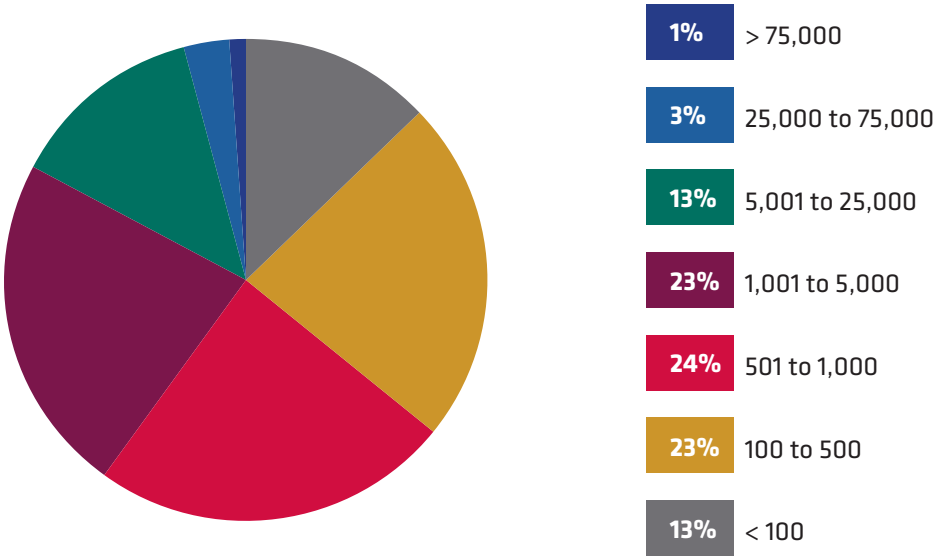


FIGURE 1-9. Global headcount–UK



CAVEATS

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings.

The following items are specific limitations that are germane to most web-based surveys.

» **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

» **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

» **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

CHAPTER 2: RISK-BASED SECURITY MANAGEMENT MATURITY & GOVERNANCE

In this section of the study, we evaluate the maturity of risk-based security management programs in organizations. To do that, we surveyed 749 US and 571 UK security and risk professionals, and collected quantitative and qualitative information about their strategy and governance programs.

Specifically, we examine respondents' views on risk-based security (including organizational commitments), and the program's impact on the business. We also review specific actions related to risk-based security programs, as well as key barriers to program success or growth.

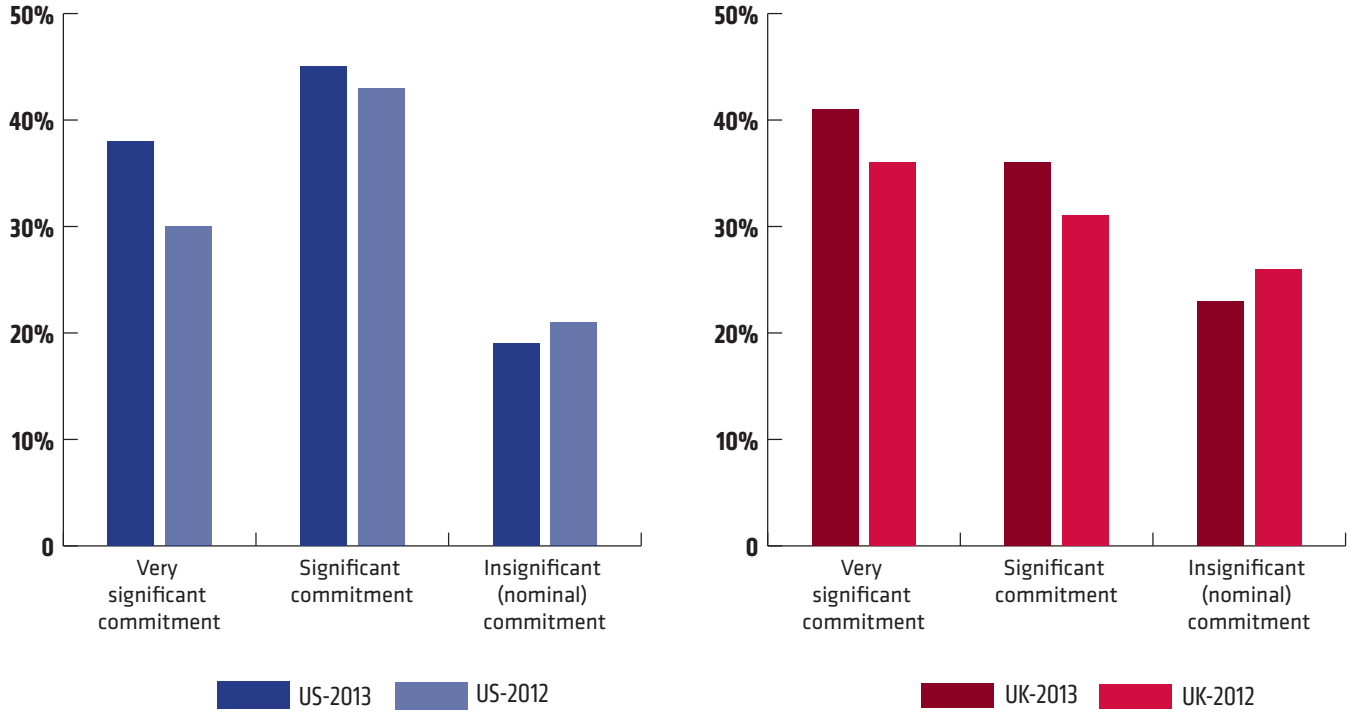
Together, these findings provide significant insight into the relatively slow growth of risk-based security management programs as compared with last year (www.tripwire.com/ponemon/2012)

In general, US and UK findings are presented separately, but the results for both sets of respondents are quite similar. When implications for the findings differ between the two countries, those differences are highlighted.

COMMITMENT TO RISK-BASED SECURITY MANAGEMENT CONTINUES TO GROW

The majority of respondents—a whopping 81% in the US and 77% in the UK—state that their organization has a significant or very significant commitment to risk-based security management (see Figure 2-1). In comparison, last year only 73% of respondents in the US and 67% in the UK had the same level of commitment. We view this increase as a positive sign of broader acceptance of the benefits of risk-based security management.

FIGURE 2-1. Commitment to risk-based security management

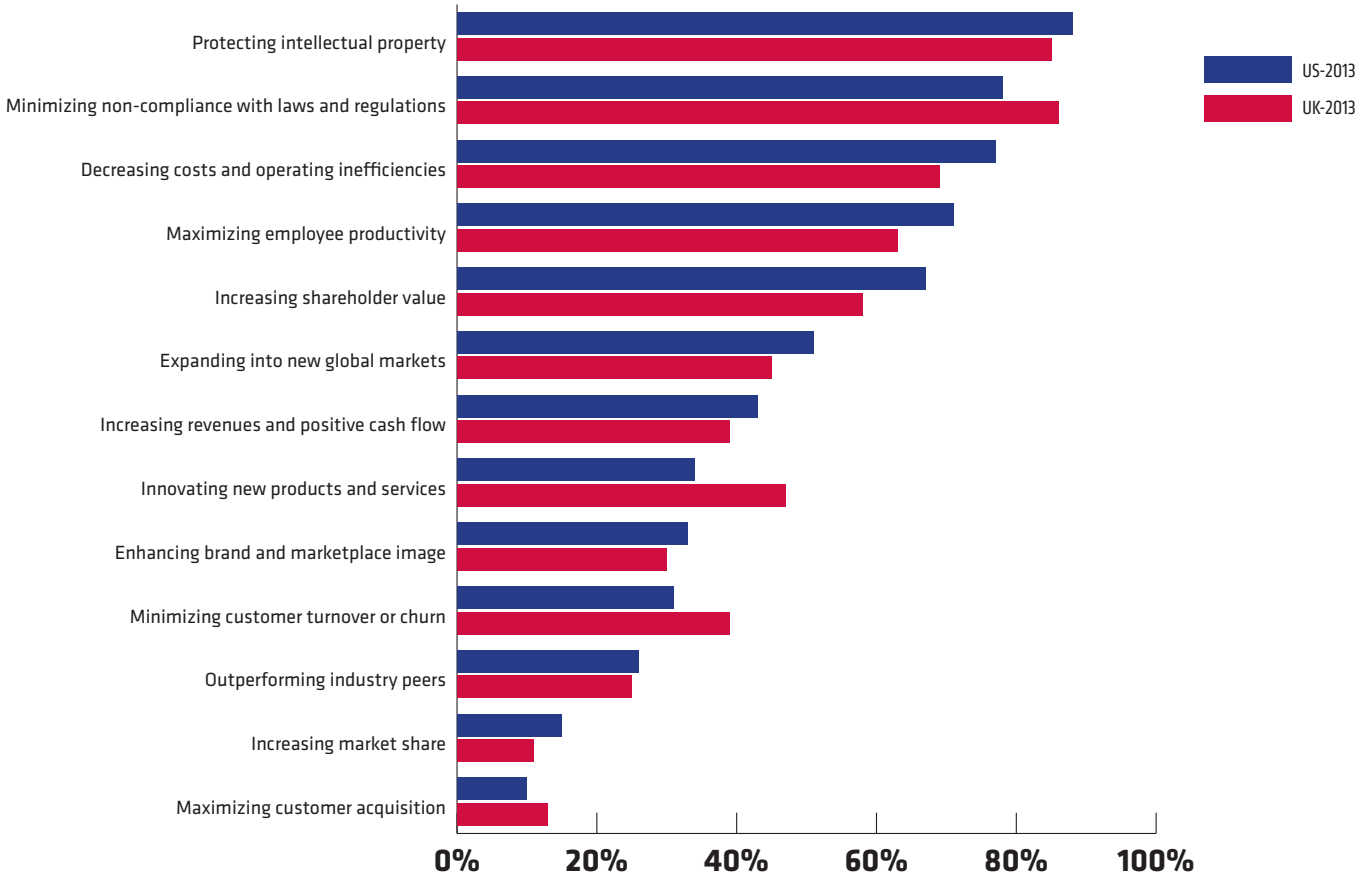


RISK-BASED SECURITY MANAGEMENT PROTECTS INTELLECTUAL PROPERTY AND MINIMIZES NON-COMPLIANCE

As Figure 2-2 demonstrates, the biggest business drivers for risk-based security management programs in the US are the protection of intellectual property (88%) and the minimization of non-compliance (78%). Decreasing costs and operational efficiencies (77%) and maximizing employee productivity (71%) are also important program objectives.

In the UK, minimizing non-compliance (86%) is the top driver—perhaps due to the highly regulated environment in the country—but the protection of intellectual property is nearly as important (85%). Decreasing costs and operational efficiencies (69%) and maximizing employee productivity (63%) are also strong drivers for UK risk-based security management programs.

FIGURE 2-2. Critical business objectives met by risk-based security management



SNAIL-PACED GROWTH IN RISK-BASED SECURITY MANAGEMENT DEPLOYMENT

Despite a significant increase in the organizational commitment to risk-based security management and a belief it can help meet key business objectives, actual risk-based security management deployment just inched forward since last year's study—deployment has only increased 5% and 3% in the US and UK, respectively (as shown in Figure 2-3).

Improvements in commitment to risk-based security management haven't translated to a wider acceptance for a strategic approach to risk management among organizations. Nearly half of the respondents describe their risk-based security management approach or strategy as 'non-existent' or 'ad hoc' (46% US and 48% UK) In contrast, only 29% (US) and 27% (UK) have a risk-based security management strategy applied consistently across the enterprise.

FIGURE 2-3. Approach or strategy taken to risk-based security management

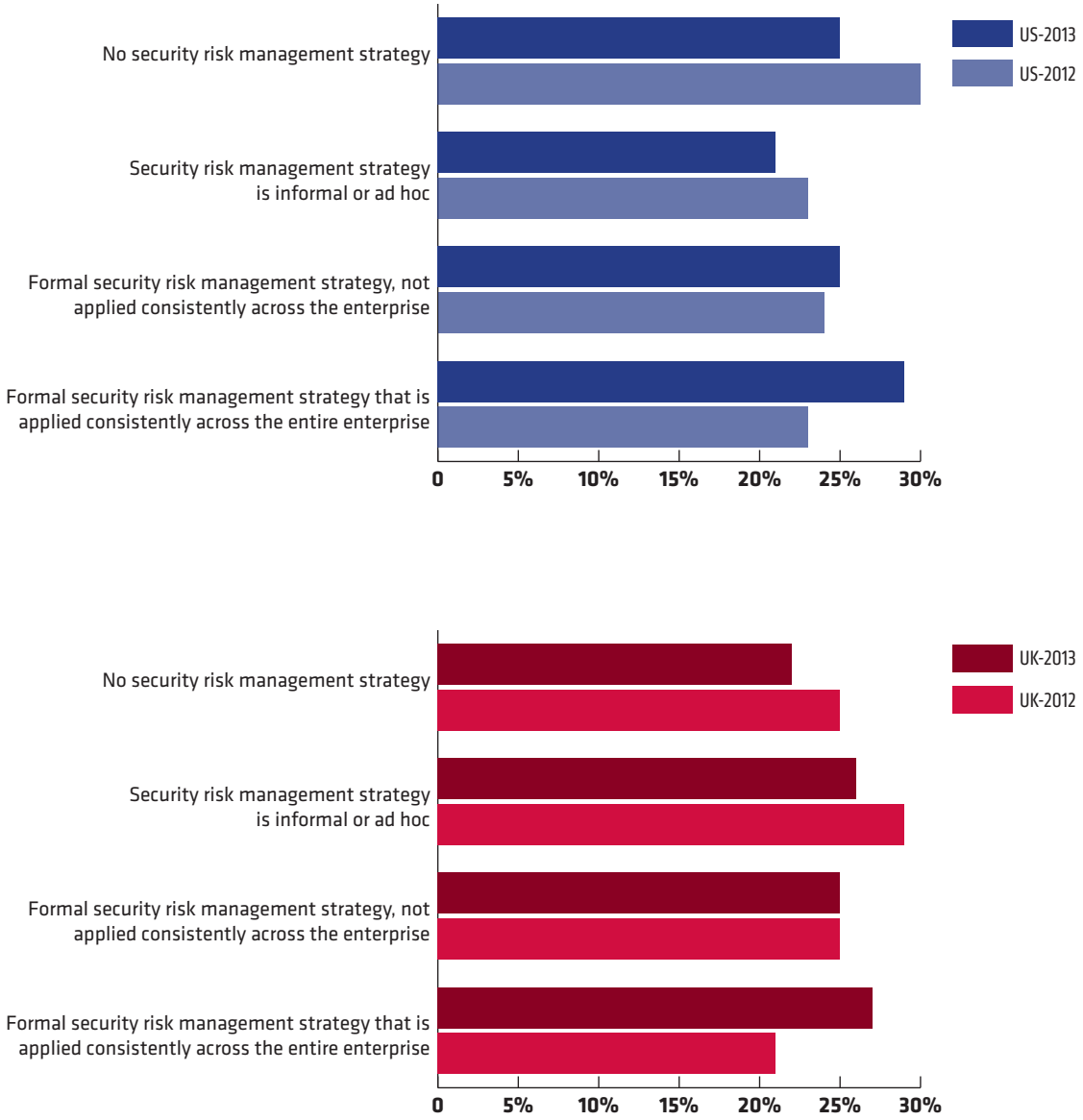
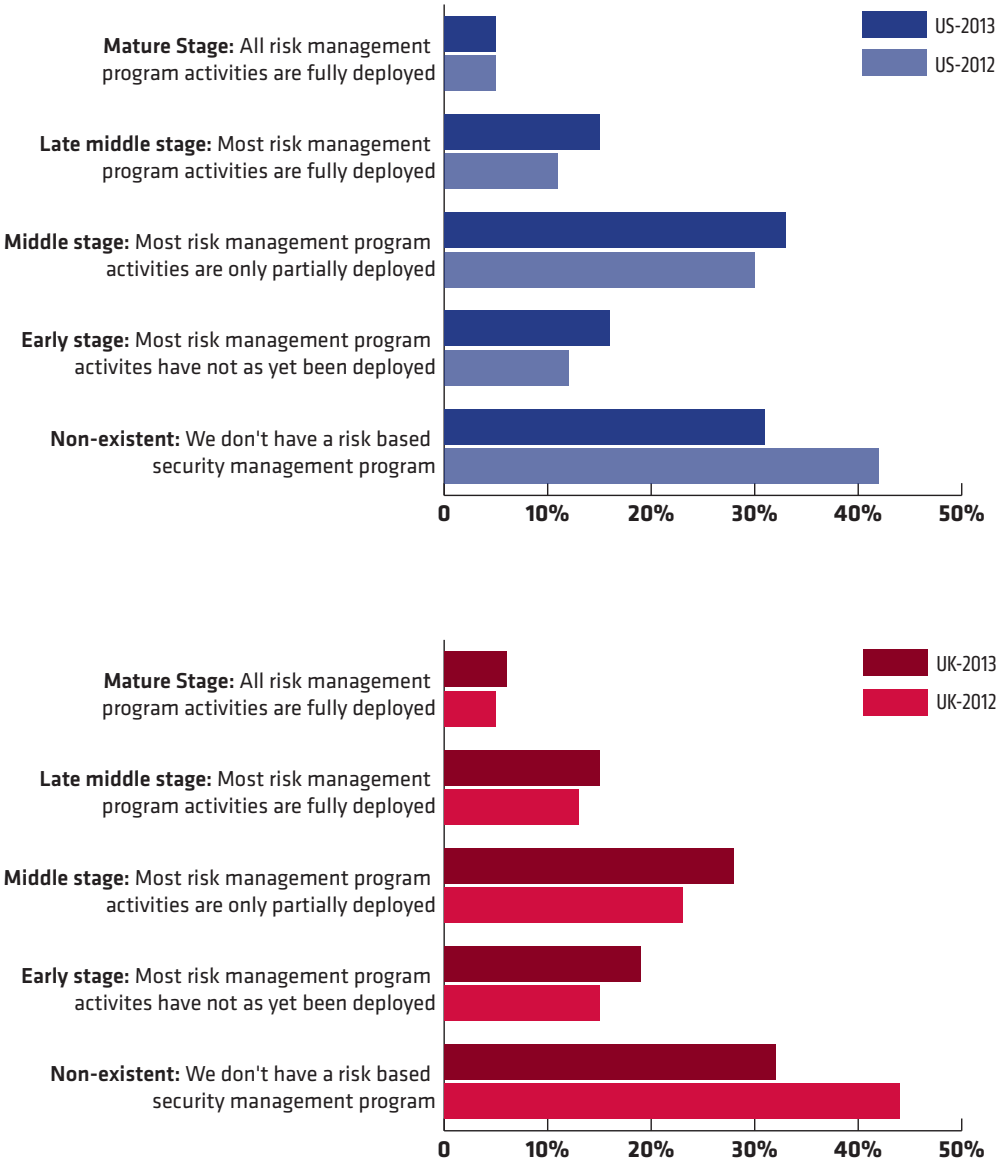


Figure 2-4 illustrates risk-based security based on the organization's level of program activity deployment. About half of the respondents (47% in the US and 51% in the UK) have no risk-based security management program, or if they have a program, have not deployed most of the program's activities.

So, why haven't organizations deployed the risk-based security management more widely? Factors affecting risk-based security management deployment are discussed in the next section.

FIGURE 2-4A/B. The maturity of the organization's risk-based security management program today



ARE THE RIGHT PEOPLE LEADING RISK-BASED SECURITY PROGRAMS?

Risk-based security management programs need champions with the ability to create and promote an organizational culture that supports enterprise-wide deployment of risk-based security programs and activities. Ideally, these champions should also have at least some responsibility for risk-based security management strategy as well as the authority and ability to affect change across the organization.

The reality varies significantly from this ideal. Figure 2-5 illustrates the organizational roles that have overall responsibility for risk-based security management today, while Figure 2-6 shows the top two roles respondents believe should champion risk-based security management.

FIGURE 2-5. Who has overall responsibility for the organization's risk-based security management approach or strategy

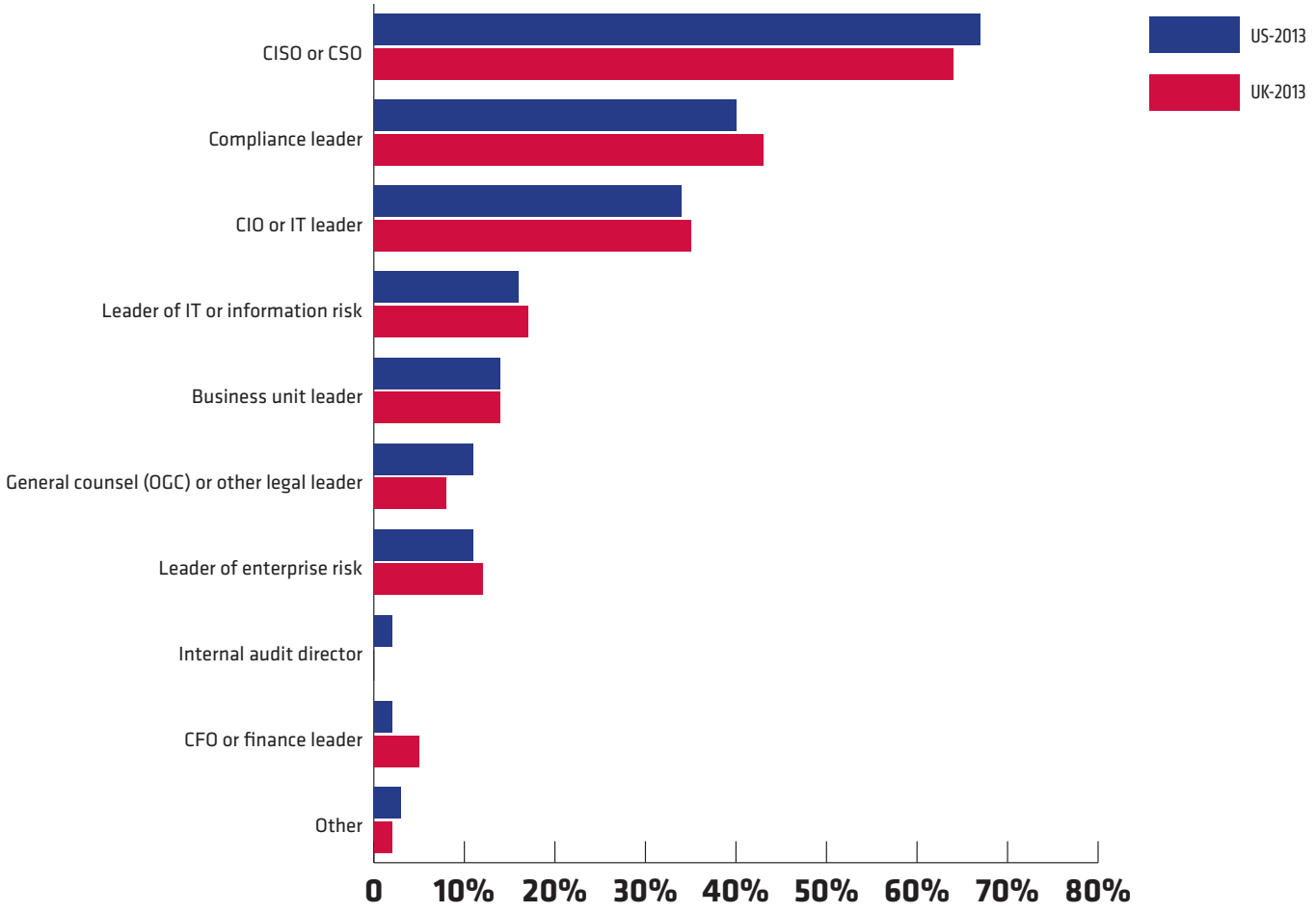
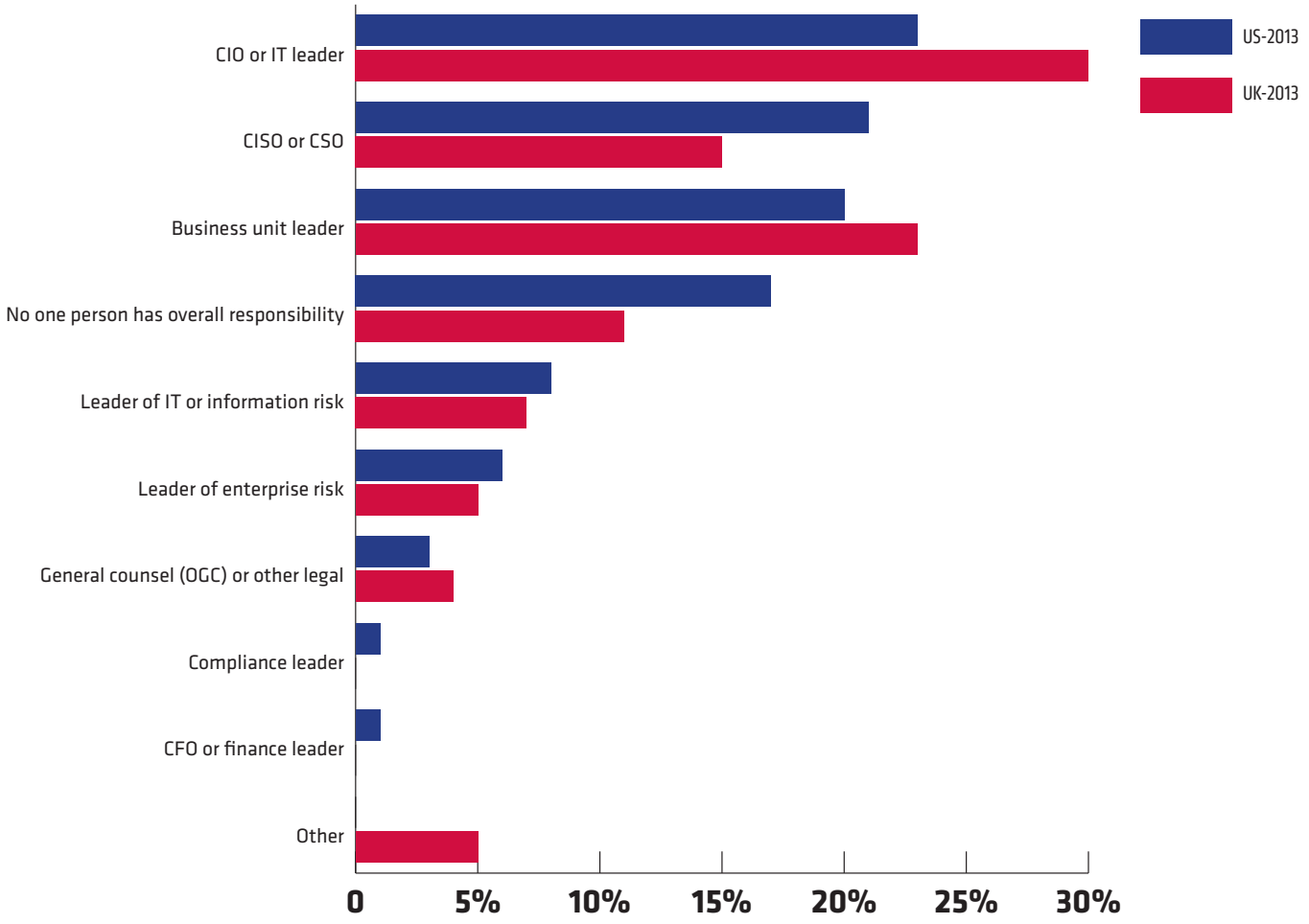


FIGURE 2-6. Who should be championing risk-based security management



These findings highlight an organizational disconnect: 67% (US) and 64% (UK) of respondents selected the CISO or CSO as their top two choices for risk-based security champions, but only 44% (US) and 45% (UK) indicate that a C-level business leader has responsibility for risk-based security management in their organization.

Surprisingly, despite the lack of cooperation that can exist between security and compliance, 40% of US and 43% of UK respondents believe compliance leaders should champion risk-based security management (second only to the CISO/CSO) and the percent of respondents who indicate this is the case in their organizations is miniscule (1% in the US and 0% in the UK).

Only 20% (US) and 23% (UK) of organizations note that business unit leaders have responsibility for risk-based security management today, yet the full benefits of a risk-based approach isn't possible without the influence and perspective of senior business leadership.

A small percentage of organizations (17% in the US and 15% in the UK) indicate that no one in their organization is responsible for risk-based security management. However, someone within the organization is always legally responsible, whether they know it or not (especially in the UK).

IT SECURITY COMPLEXITY MAY HINDER RISK-BASED SECURITY MANAGEMENT PROGRESS

Not surprisingly, over half of respondents (56% US and 55% UK) indicate that IT complexity has a significant impact on the organization's ability to perform risk-based security management (Figure 2-7). When this finding is combined with those indicating that it has 'some' impact, that number jumps to around three-quarters (77% US and 74% UK).

CHALLENGES IN ALIGNING RISK-BASED SECURITY MANAGEMENT WITH BUSINESS OBJECTIVES

While 60% (US) and 59% (UK) of respondents think that risk-based security management helps security align with business objectives, Figure 2-8 shows that most respondents don't believe their organizations are actually involved (62% in the US and UK) in the process of aligning risk with business objectives.

FIGURE 2-7. The impact of IT security complexity on risk-based security management

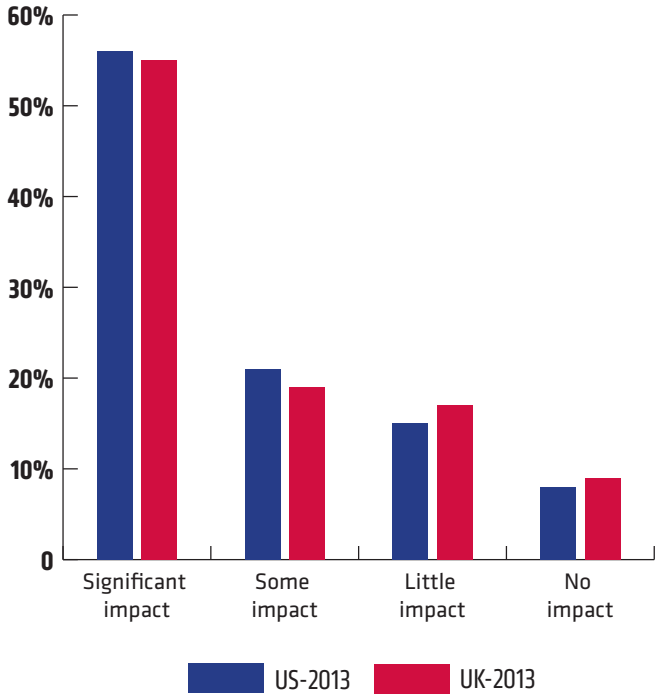
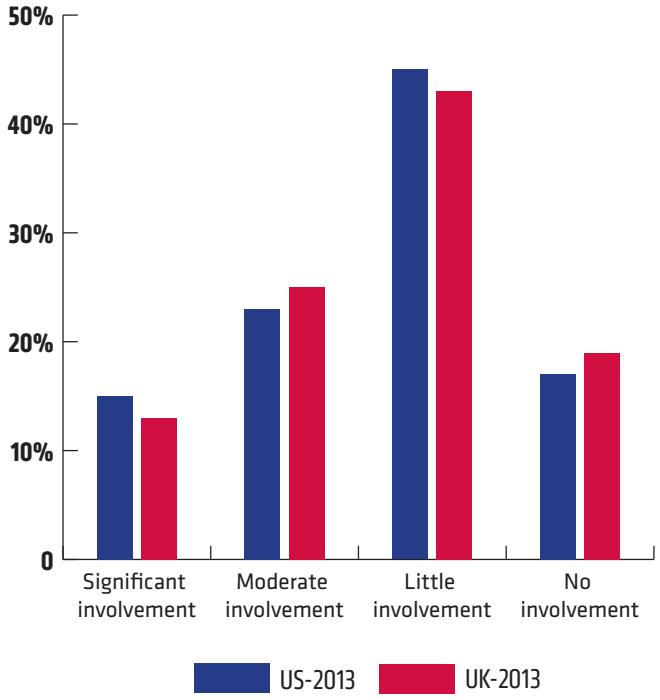


FIGURE 2-8. Organizational involvement in aligning risk-based security management with business objectives



PERCEPTIONS ABOUT RISK-BASED SECURITY MANAGEMENT PORTEND SUCCESS

It's likely that organizations still in early stages of risk-based security management deployment haven't yet experienced its benefits. That said, around two-thirds of respondents are informed about risk-based security management benefits, believing it reduces conjecture and uncertainty and lets them challenge existing assumptions about the organization's security posture. Respondents are realistic about what it takes to have a mature risk-based security management program, understanding that an effective program can only be accomplished by using a broad set of relevant data. Just under half of the respondents (48% US and 49% UK) believe risk-based security management has the ability to create an environment and culture of informed choice.

SUMMARY

On the whole, organizations are making slow progress with deployment of risk-based security management strategies and programs. Given the increase in organizational commitment and the understanding that risk-based security management can align security with key business, organizations appear poised to make more significant strides over the next 12 to 18 months. However, in order to achieve benefits like protection of intellectual property and the minimization of compliance issues, it's clear senior business leaders need to become more deeply involved in risk-based security programs.

CHAPTER 3: SECURITY METRICS—IMPORTANT BUT STILL NOT EFFECTIVE FOR COMMUNICATING RISK

Security metrics are the primary tools IT professionals use to communicate security risk and posture to business leaders and executive teams, but are these metrics effective?

This Ponemon Institute study was designed to build a deeper understanding of the benefits and efficacy of security metrics in the communication of risk-based security status and posture.

The study reveals key insights and challenges that IT professionals face in selecting appropriate metrics that accurately convey the status of their security initiatives to senior business leaders. It also reveals challenges in connecting risk-based security programs to key business objectives.

The study also reflects the importance security metrics play in risk-based security programs and adds new insight and focus to the full study.

Although the results for both sets of respondents are generally quite similar, the US and UK findings are usually presented separately. When implications for the findings differ between the two countries, those differences are highlighted.

SECURITY METRICS REVEAL BIGGER, MORE COMPLEX ISSUES

The vast majority of security professionals responding to this study do not dispute the worth of metrics as a key performance indicator. After all, without metrics, it's difficult to demonstrate improvement or measure success. Asked about the importance of metrics in achieving a mature risk-based security management process, 75% of respondents in the US and 72% in the UK said either "very important" or "important" (Figure 3-1).

When asked if their organization's existing metrics are properly aligned with business objectives, more than half (53% in the US and 51% in the UK) said either "no" or "unsure" (Figure 3-2).

FIGURE 3-1. How important are metrics in achieving a mature risk-based security management process?

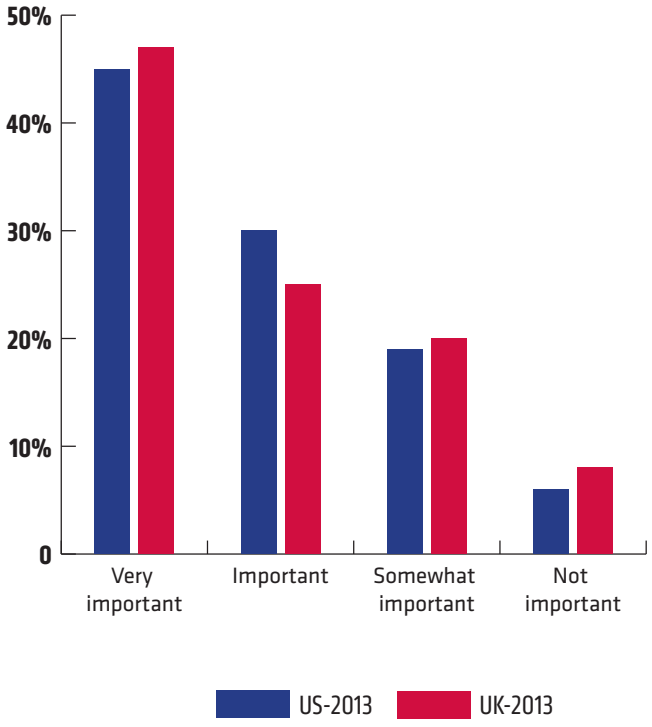
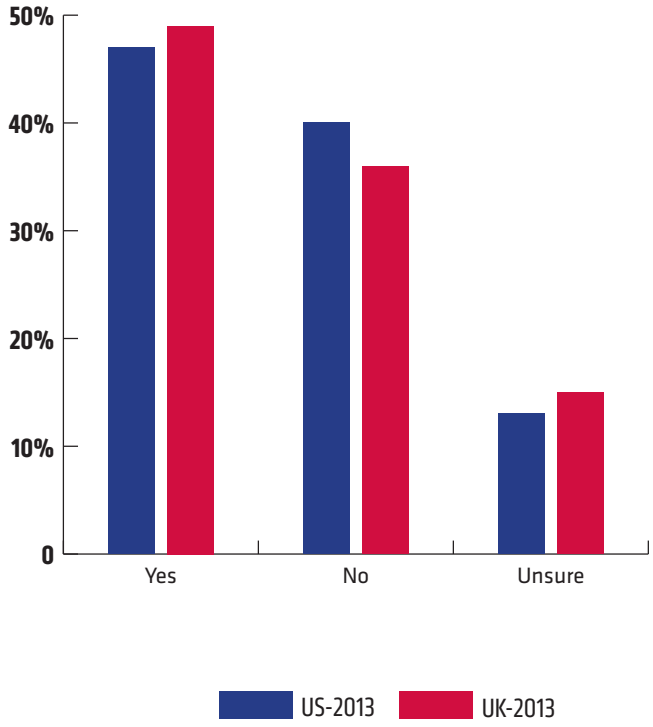


FIGURE 3-2. Do you believe that your company's existing metrics are properly aligned with business objectives?



These findings highlight a security communication gap that still exists in many organizations. While there is broad agreement on the value of a risk-based security approach, there is significant disparity when it comes to implementing security metrics that are aligned with business initiatives.

The study also revealed significant challenges in the use of metrics to adequately convey the effectiveness of security risk management efforts to the C-suite (Figure 3-3). Only half of the respondents believe that the metrics they use are aligned with business objectives, and just under half believe that their communications with business executives about risk-based security are effective.

One potential contributing factor in this disconnect is that security professionals have traditionally viewed metrics as valuable operational performance measurements, while executives tend to evaluate security based on cost. Neither of these approaches is well adapted to communicating the effectiveness of risk-based security programs.

This disconnect demonstrates the escalating value of communication skills in senior security roles. As business leaders are required to disclose more about their organization's security risks, those business-oriented security executives with good communication skills will be in even greater demand.

IT SPEAKS A DIFFERENT LANGUAGE

Additional study questions help shed some light on the issues surrounding the apparent communication disconnect between security objectives and business goals. In rating their own effectiveness in communicating all relevant facts about the state of security risk to senior executives, about half of IT professionals (51% in the US and 47% in the UK) say they are "not effective" (Figure 3-4).

FIGURE 3-3. Do you believe these metrics adequately convey the effectiveness of security risk management efforts to senior executives?

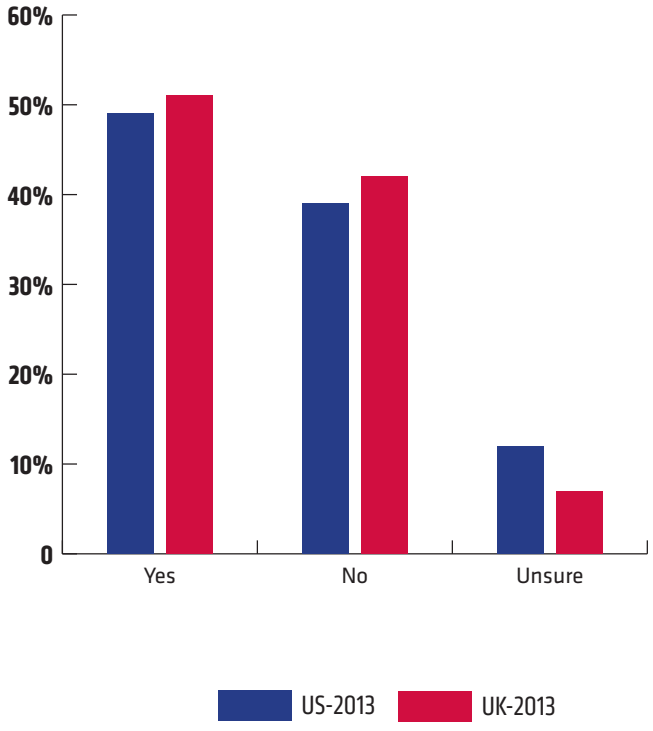
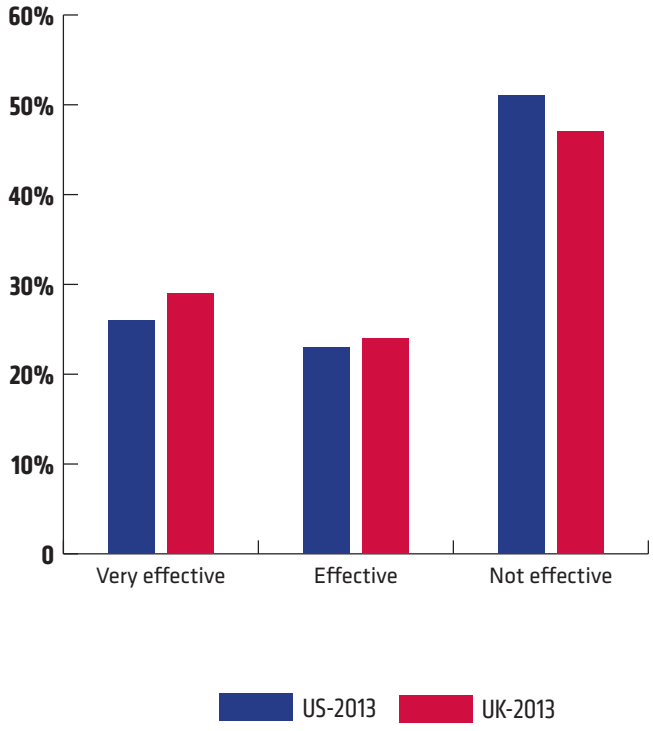


FIGURE 3-4. Please rate your effectiveness in communicating all relevant facts about the state of security risk to senior executives.



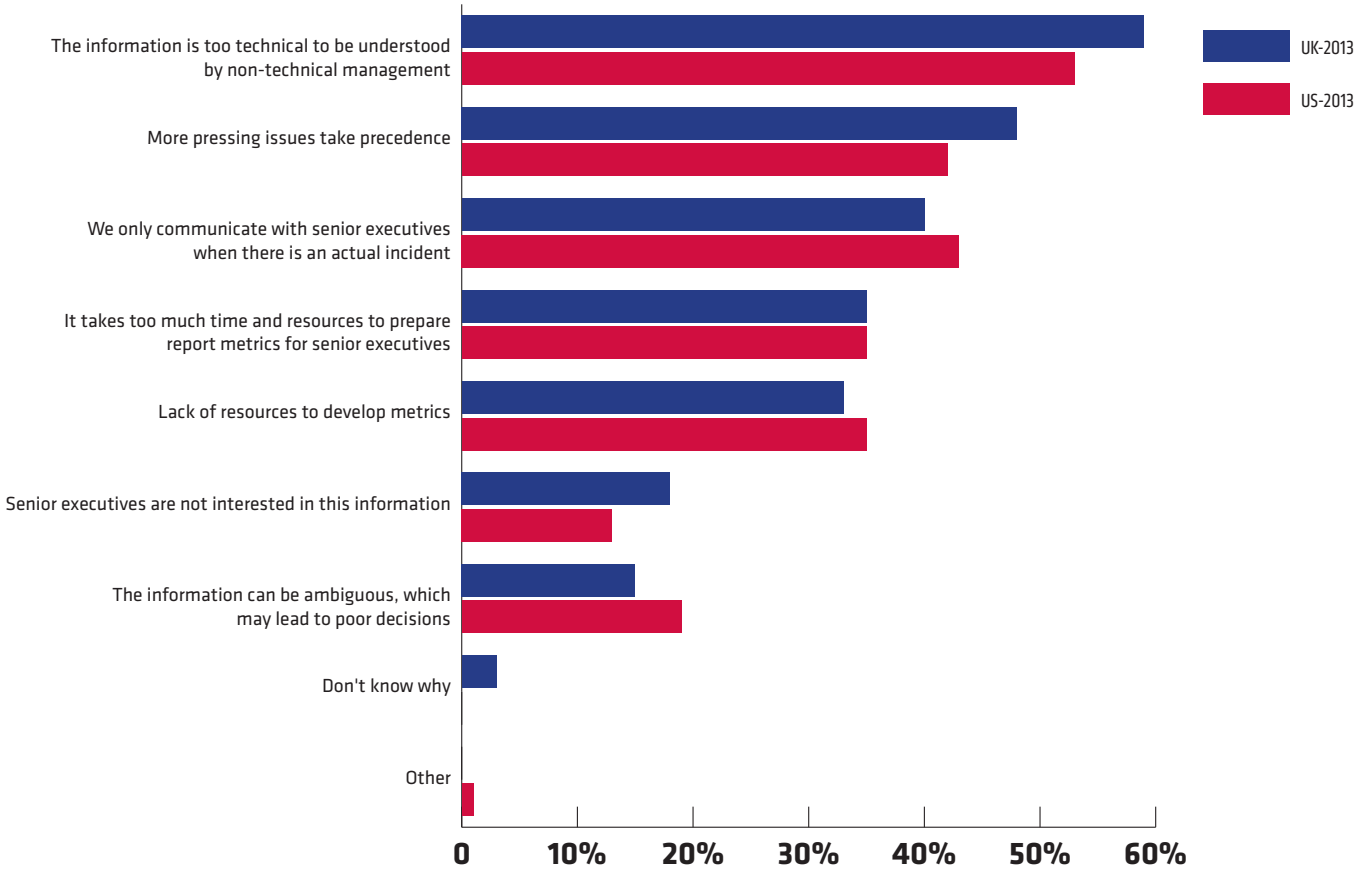
When asked why they don't create metrics that are well understood when communicating to senior executives, more than half of respondents in the US and UK indicate that the security metrics collected in their organizations are too technical to be understood by senior leadership (Figure 3-5).

There appears to be another underlying reason that has almost as much impact on effective communication as the technology divide: A significant number of respondents (48% in the US and 42% in the UK) say pressing issues take precedence over regular, proactive communication with their executive team.

In fact, 40% of the respondents in the US and 43% in the UK say they only communicate with executives when there is a security incident—the least conducive time for constructive communication.

In the same way it's not acceptable for a CFO to say that he's too busy to prepare financial reports for the board or senior executive team, in the near future it will not be acceptable for senior IT leaders to be too busy to prepare understandable security reports. Security professionals must find or create metrics that are more broadly understood by business leaders.

FIGURE 3-5. If no or unsure, why? In other words, why don't you create metrics that are well understood by senior executives?



So, why isn't communication between security professionals and executives more effective? Respondents were asked to select all the factors that apply from a list of nine possible reasons, and their answers present a wide range of serious challenges (Figure 3-6). The top three responses include organizations hampered by siloed information, presenting information not easily understood by non-technical managers, and the practice of filtering "bad news" from the C-suite.

- 68% of US and 57% of UK respondents say communications are confined to one department or line of business
- 61% say the information is too technical and occurs at too low a level
- 59% state that negative facts are filtered before they are communicated to executives

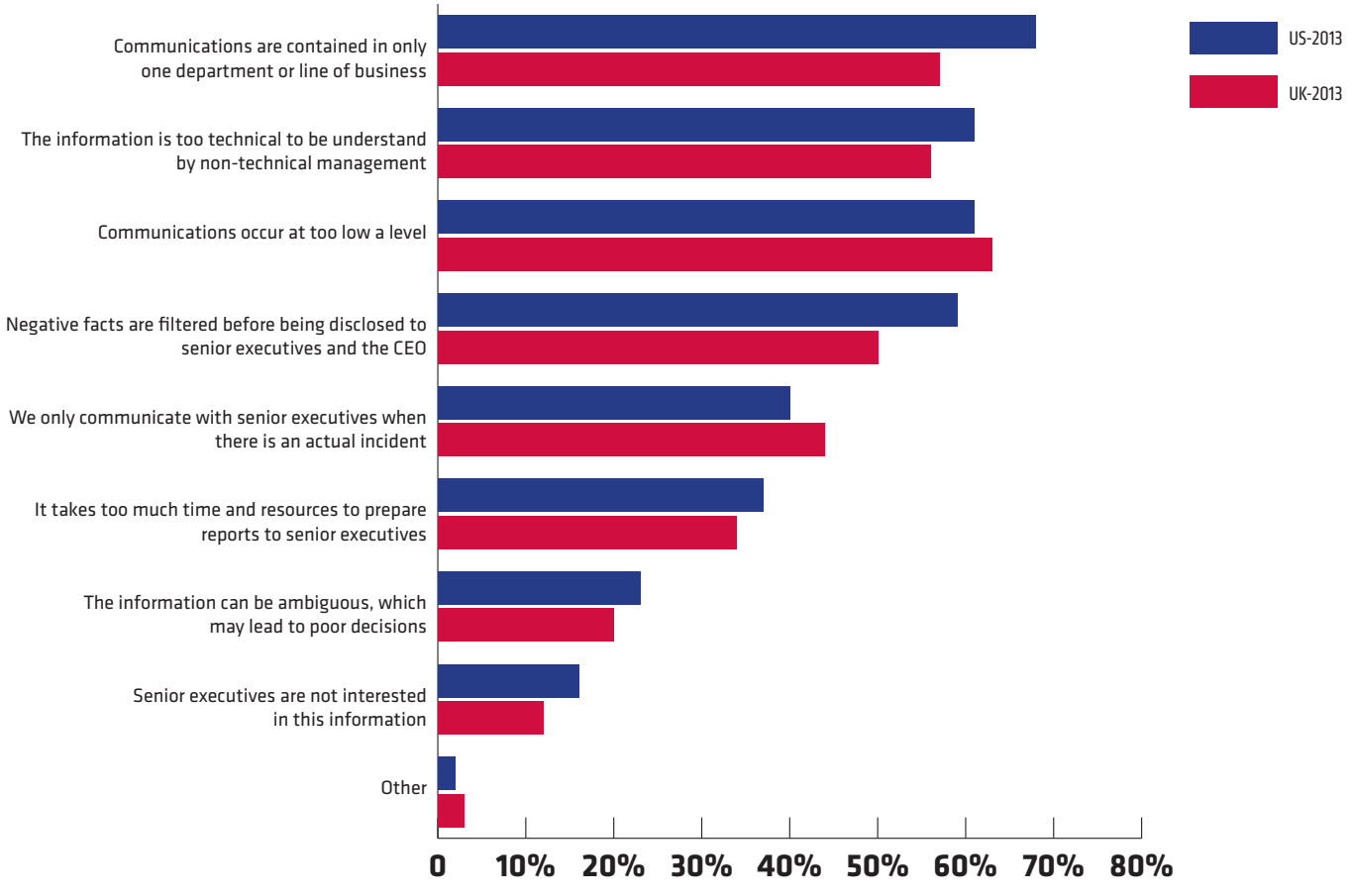
It's also interesting to note that 23% of US respondents and 20% of those in the UK (Figure 3-6) think security metrics can be ambiguous, which may lead to poor decisions. Additionally, another 16% of US and 12% of UK respondents believe senior executives are not interested in this information.

SUMMARY

While the majority of security professionals agree they need significant amounts of data in order to build a culture of accountability, they aren't sure how to distill this information into metrics that are understandable, relevant and actionable to senior business leadership. Business metrics tend to reflect the value of strategic goals rather than technical goals, and may prioritize cost over less tangible security benefits. Security metrics tend to reflect operational goals and may prioritize technical improvement over business context.

Finding meaningful ways to successfully bridge this communication gap is critical to broader adoption of risk-based security programs. The onus for this effort clearly lies with IT security and risk professionals.

FIGURE 3-6. If no or unsure, why? In other words, why don't you create metrics that are well understood by senior executives?

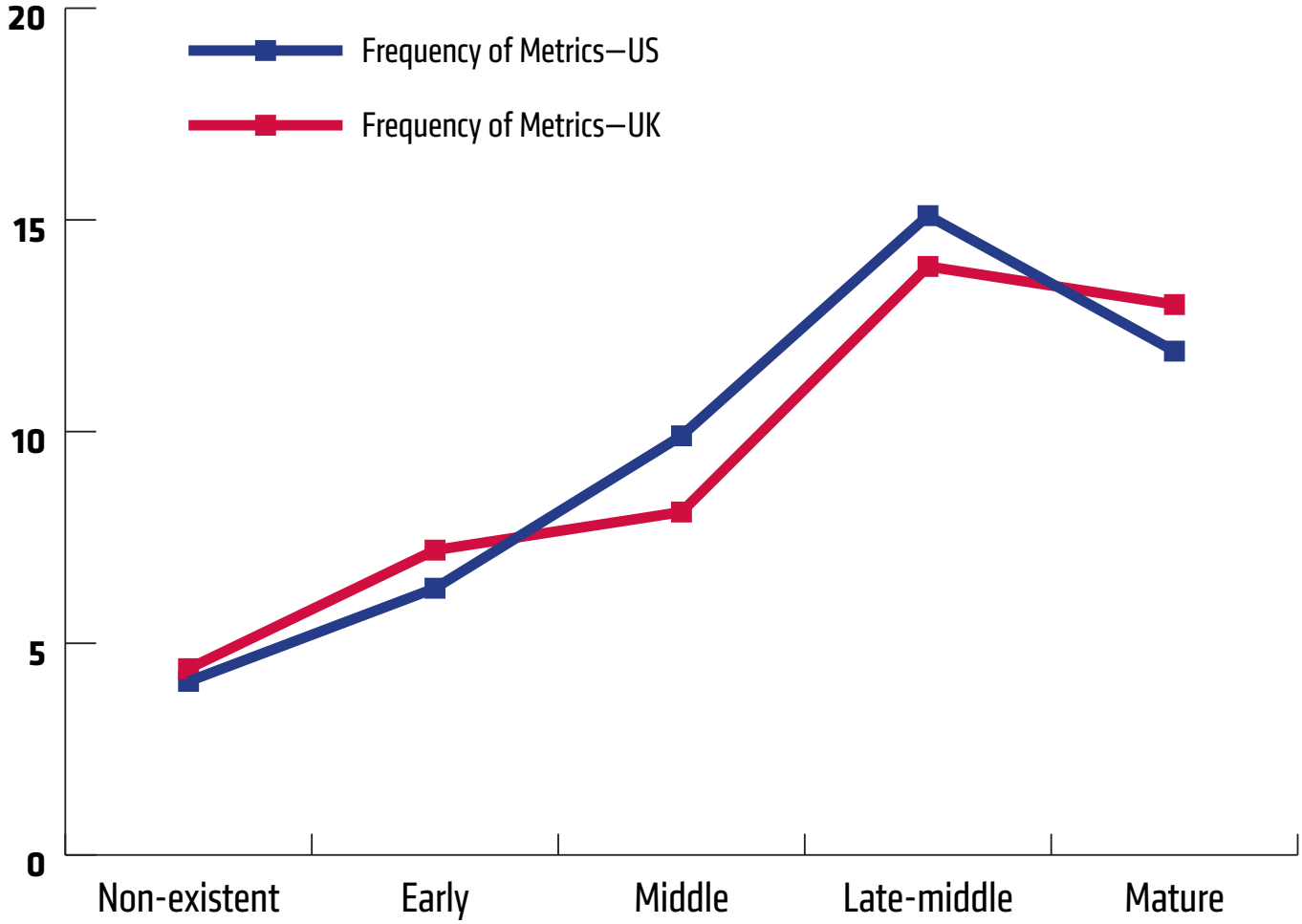


CHAPTER 4: MEASURING THE EFFECTIVENESS OF RISK-BASED SECURITY MANAGEMENT

While there is no one set of standards for measuring the effectiveness of security metrics, there are basic indicators frequently used in organizations no matter where they are in the maturity of their risk-based security program. This chapter of the 2013 Ponemon Institute study on risk-based security management asks respondents about the relative efficacy of the metrics they use to measure risk-based security in their organizations.

For this study, early maturity organizations are defined as those where the use of risk-based security management metrics is non-existent or in early stages. Higher maturity is defined as organizations where the use of risk-based security management metrics are in middle, late-middle and mature stages. Figure 4-1 shows metrics frequency by maturity level.

FIGURE 4-1. Analysis of metrics frequency by Risk-based Security Management maturity stages.



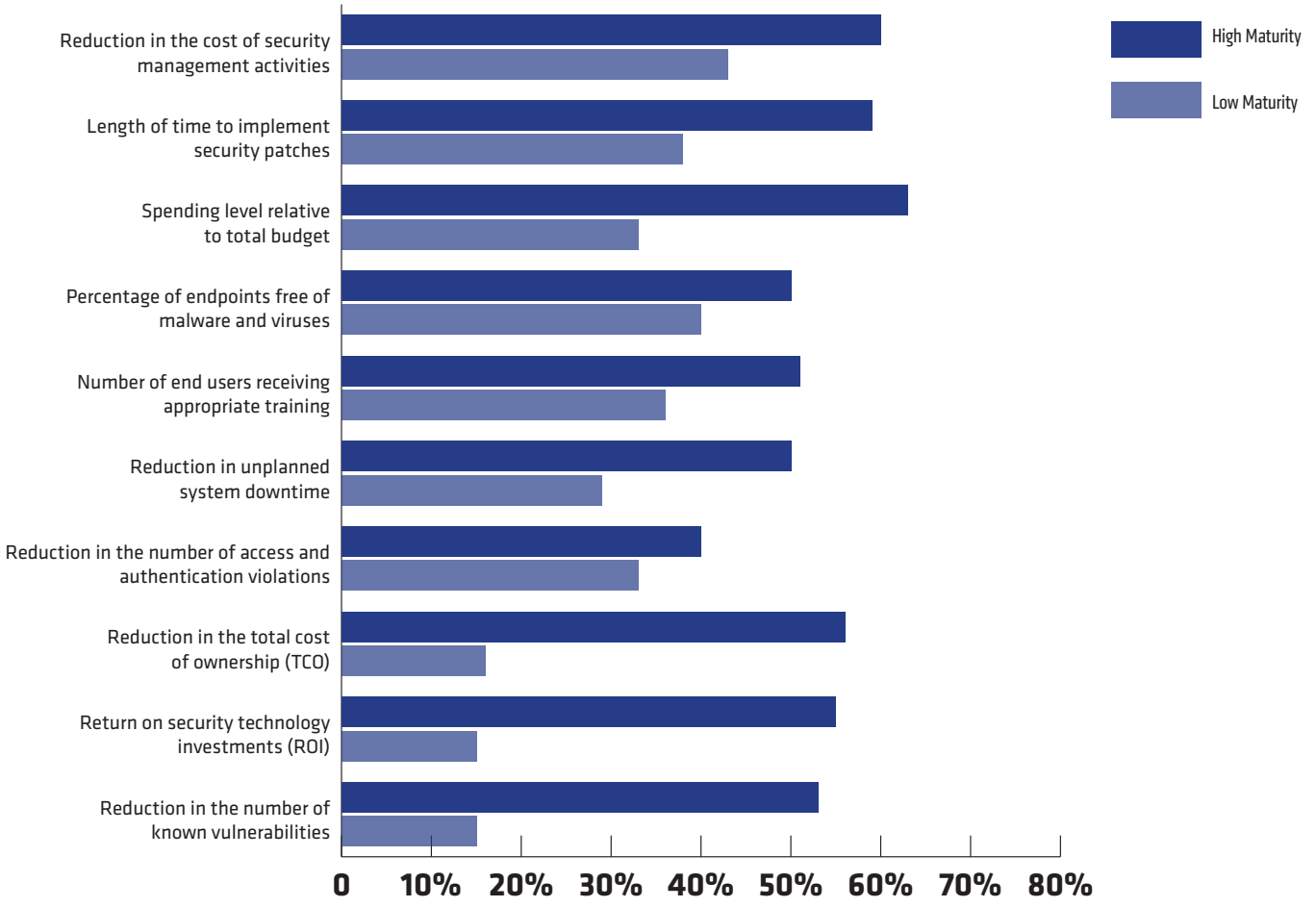
FREQUENCY OF USE OF METRICS

Security professionals from the US and UK were asked to rank the following 29 risk-based security management metrics by frequency of use:

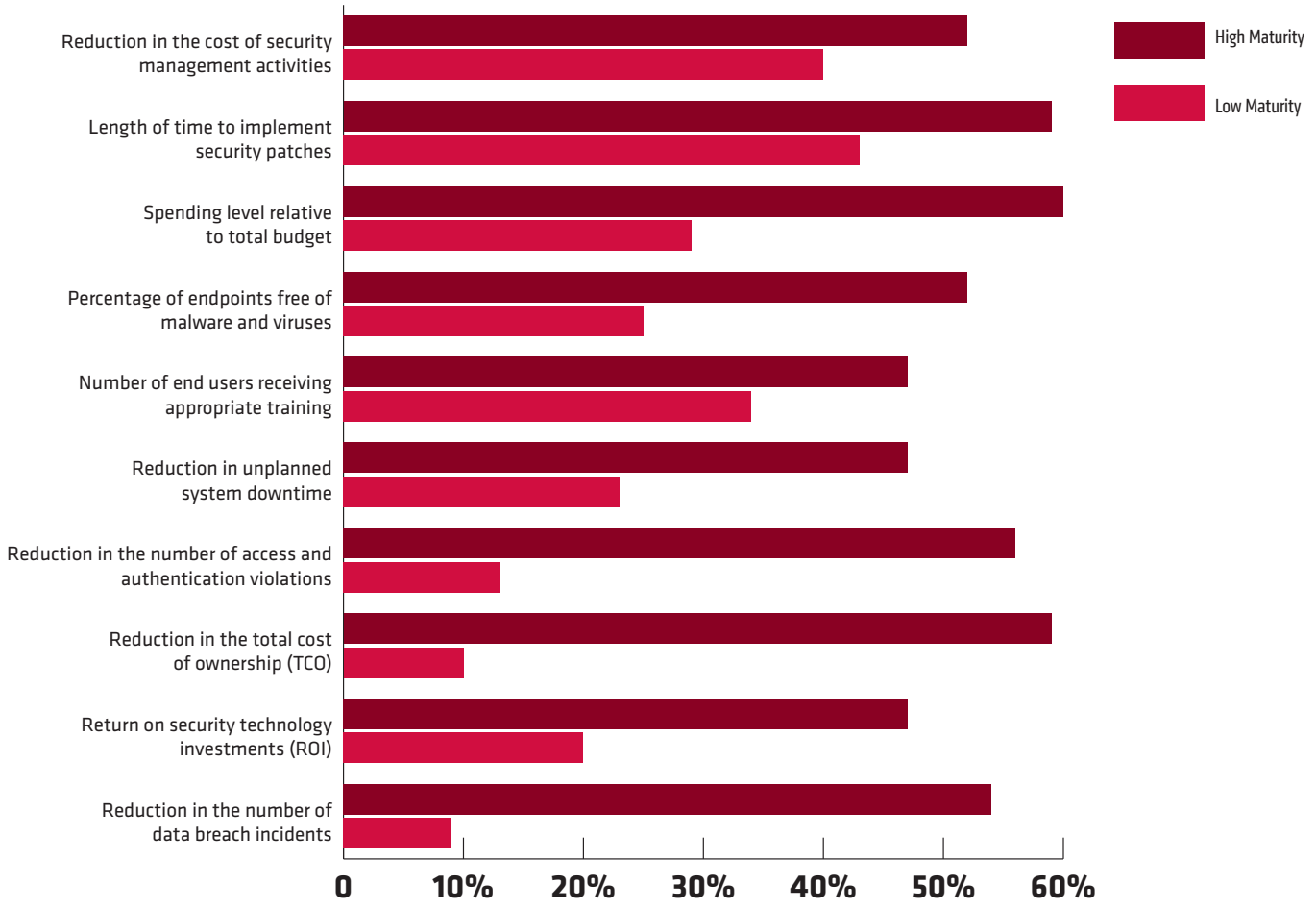
- Reduction in the cost of security management activities
- Length of time to implement security patches
- Spending level relative to total budget
- Percentage of endpoints free of malware and viruses
- Number of end users receiving appropriate training
- Reduction in unplanned system downtime
- Reduction in number of access and authentication violations
- Reduction in the total cost of ownership (TCO)
- Return on security technology investments (ROI)
- Reduction in number of known vulnerabilities
- Reduction in number of data breach incidents
- Reduction in number of percentage of policy violations
- Reduction in audit findings and repeat findings
- Number of security personnel achieving certification
- Number of records or files detected as compliance infractions
- Percentage of software applications tested
- Reduction in the frequency of denial of service attacks
- Reduction in regulatory actions and lawsuits
- Reduction in expired certificates (including SSL and SSH keys)
- Mean time to detect security incidents
- Reduction in the number of threats
- Reduction in the cost of cyber crime remediation
- Percentage of recurring incidents
- Percentage of incidents detected by automated control
- Performance of users on security training retention tests
- Time to contain data breaches and security exploits
- Reduction in the number or percentage of end user enforcement actions
- Reduction in loss of data-bearing devices (laptops, tablets, smartphones)

Of the 29 basic indicators most frequently used to assess security efforts, 10 metrics emerge for organizations of both low and high maturity, with nine of the 10 consistent across the US and UK. Reduction in the cost of security was rated No. 1 and No. 2, and in both countries, two of the top three metrics focus on budget concerns (Figures 4-2a and 4-2b).

FIGURES 4-2A. What metrics are used by your organization to assess the effectiveness of security risk management efforts? (US)



FIGURES 4-2B. What metrics are used by your organization to assess the effectiveness of security risk management efforts? (UK)



Based on these responses, operational metrics such as anti-virus and malware status, percentage of policy violations and security incidents detected continue to be the standard for evaluating the success of security efforts; however, they may not be good indicators to demonstrate the effectiveness of risk-based security management efforts. Operational metrics continue to be widely used, perhaps because they are easier to automate and therefore easier to measure.

Of those metrics not in the top 10, patterns also emerge. Metrics that indicate responsiveness to security issues were not widely used. For instance, 'mean time to detect security incidents' was only used by 13% of US and 17% of UK respondents and 'mean time to resolve security incidents' has use rates of just 8% in the US and 13% in the UK. Performance metrics are harder to measure and their adoption may depend on the maturity level of the organization, budget, skilled resources and availability of the technology necessary to implement measurement processes.

GAUGING THE EFFECTIVENESS OF COMPLIANCE EFFORTS

Compliance to internal standards, industry frameworks or government regulations, is a major driver of risk-based security management operations. In order to dig deeper into risk-based security management practices for compliance, respondents were asked about specific measures they use to determine effectiveness of compliance (Figures 4-3a and 4-3b).

FIGURE 4-3A. Measures for compliance, US respondents

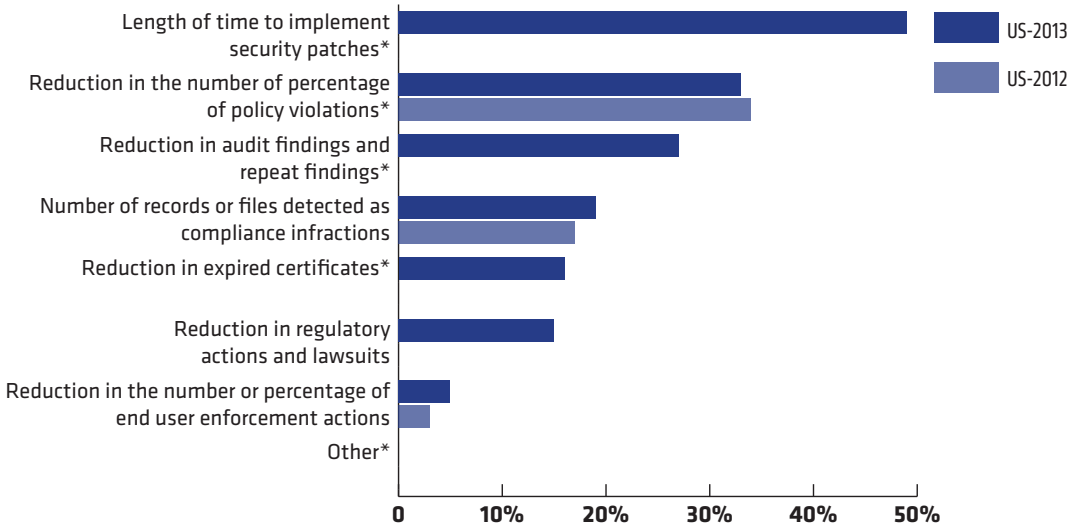
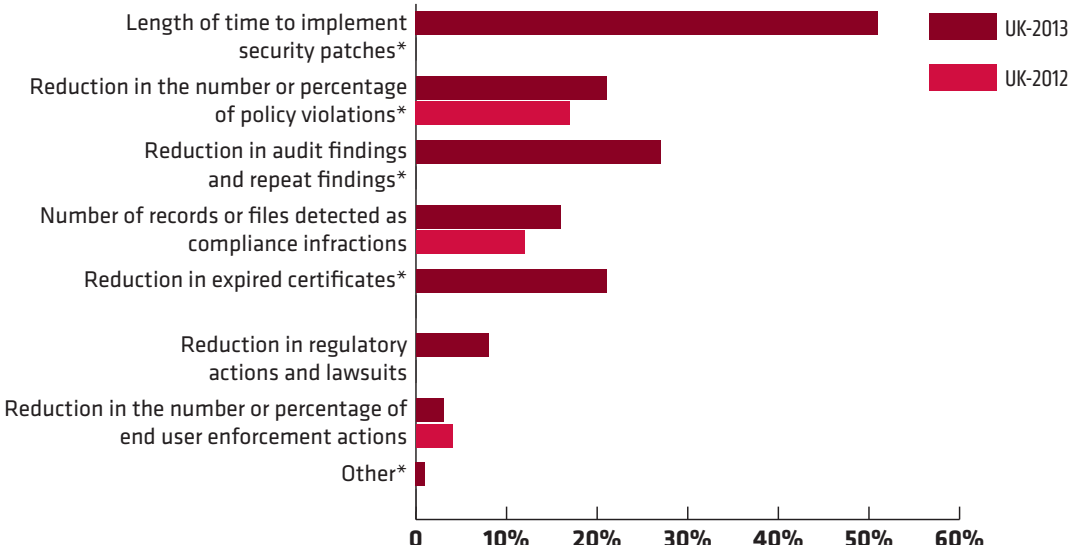


FIGURE 4-3B. Measures for compliance, UK respondents



*This choice was not available in 2012

Organizations in both the US and UK rank 'length of time to implement security patches' as the number one indicator of compliance effectiveness. Given that security patches help prevent many threats and that the less time required to patch a system means the less risk an organization faces due to vulnerabilities, it makes sense that this metric is the top choice for measuring compliance effectiveness.

Respondents in both countries rank audit findings as their next highest metric (No. 3 in the US and No. 2 in the UK). However, this is a metric that is usually tracked at board level, so it's interesting to see the visibility it garners.

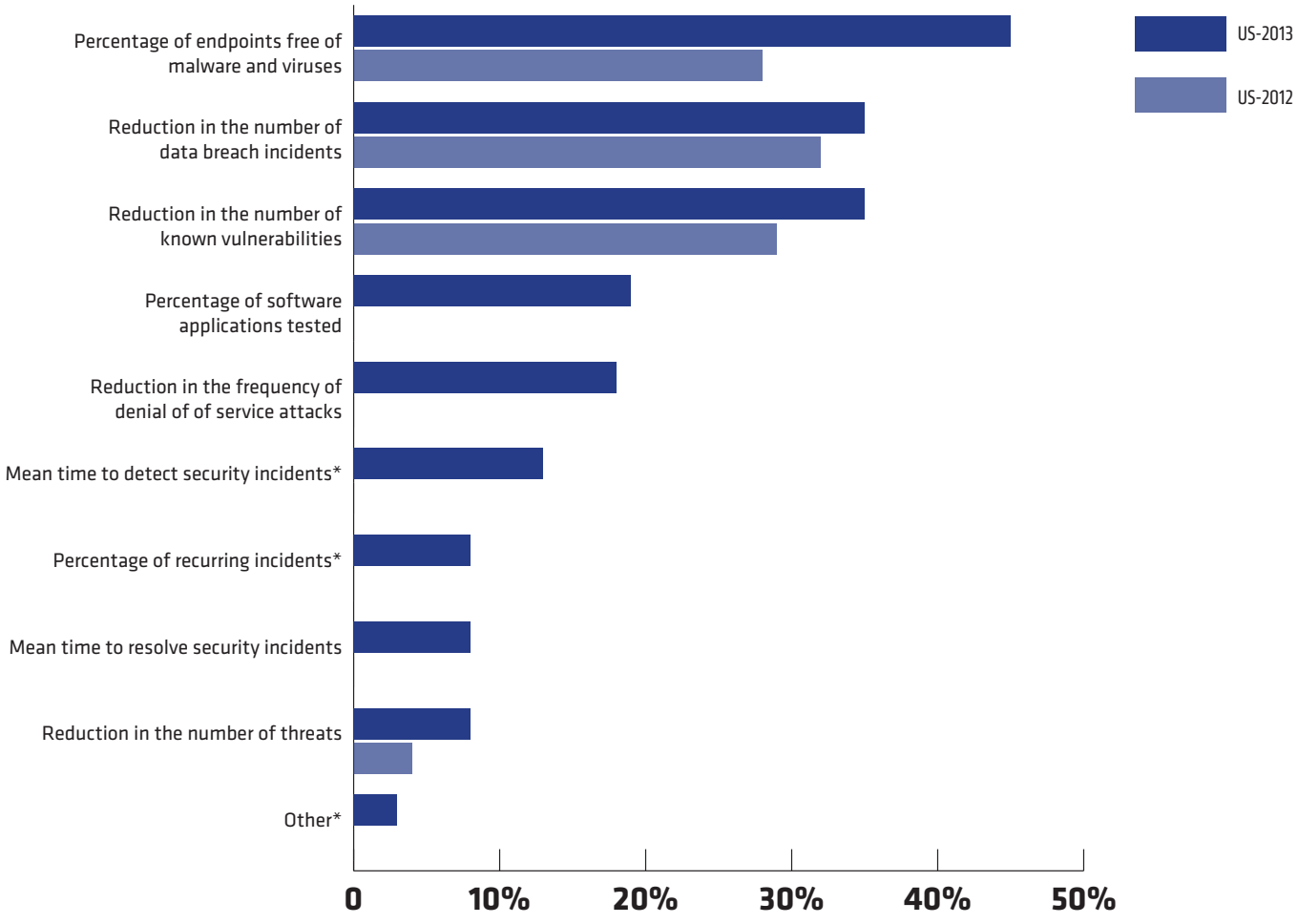
Metrics for 'reduction in the number or percentage of policy violations' (33% US, 21% UK) and 'reduction in audit findings and repeat findings' (27% US, 25% UK) may indicate that organizations are getting more skilled at managing, automating and complying with standards, and employee awareness is certainly a component of this metric as well.

Surprisingly, reduction in expired certificates was identified as a useful metric by just 16% (US) and 21% (UK). According to the Verizon 2013 *Data Breach Investigations Report* (DBIR), 76% of network intrusions exploit weak or stolen credentials (such as passwords, administrator privileges, misuse or expired or stolen certificates). This is an easily preventable risk when strict policies are in place and enforced.

MEASURES FOR THREAT MANAGEMENT

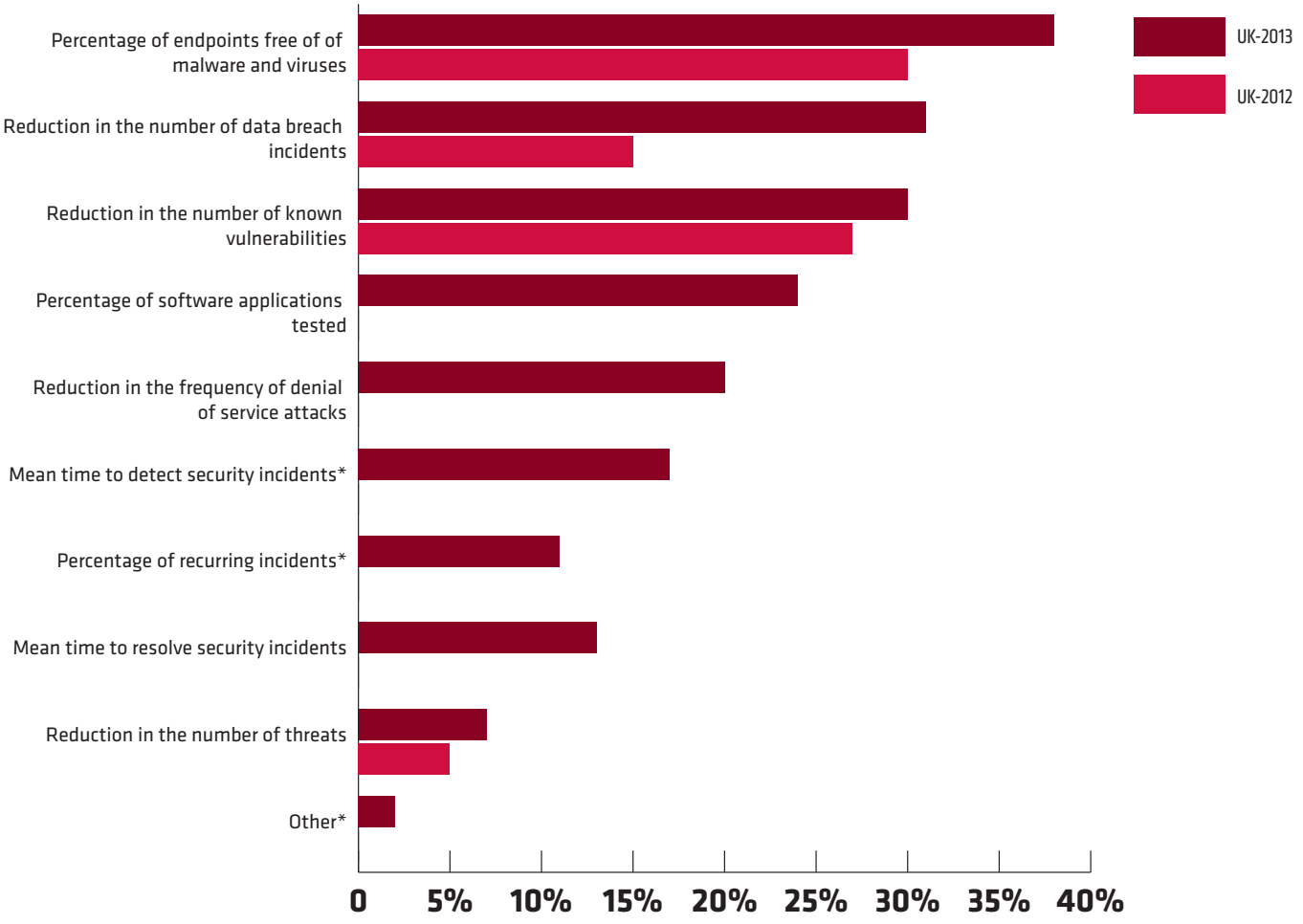
In light of the maturity curve in the deployment of risk-based security management practices, it's not surprising that many organizations are not yet using threat metrics oriented toward higher order outcomes. The majority of respondents are still focused on operational metrics (Figures 4-4a and 4-4b).

FIGURE 4-4A. Measures for threat management. US respondents



*This choice was not available in 2012

FIGURE 4-4B. Measures for threat management, UK respondents



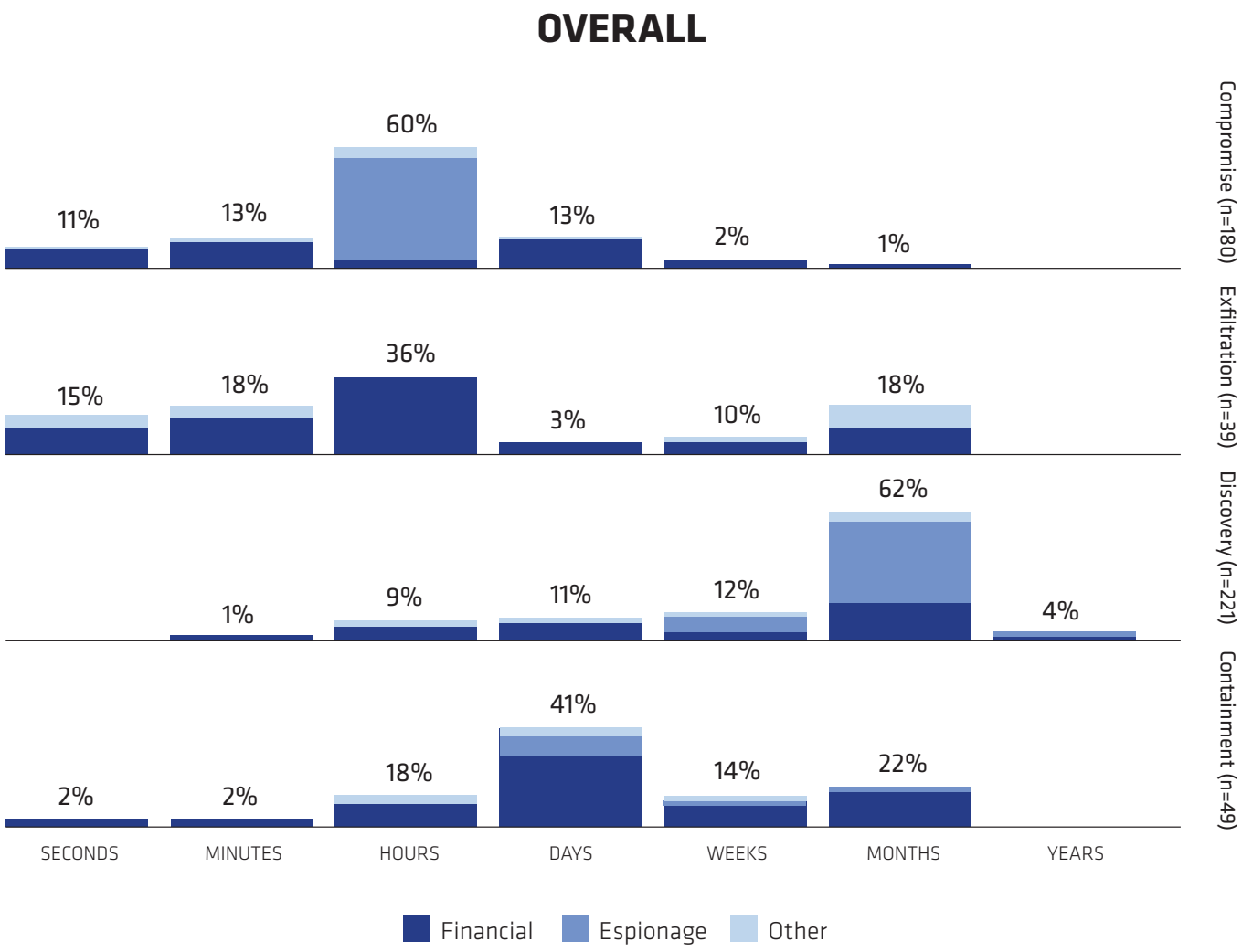
*This choice was not available in 2012

Not surprisingly, anti-virus and endpoint protection are among the most widely adopted security methods (45% US, 38% UK). This metric is driven by compliance and by continuing phishing and malware attacks, which was the highest and most likely breach method following weak, stolen or misused credentials, per the 2013 DBIR. These technologies have been available longer and are likely to be completely deployed across the enterprise.

While many companies are still focusing on reducing the number of data breaches (35% US, 31% UK) and the number of known vulnerabilities (35% US, 30% UK), very few companies are tracking 'mean time to detect security incidents' and 'mean time to resolve security incidents.' Although these metrics are more difficult to collect and require a more mature risk-based security program, early discovery provides the best chance to limit the impact of breaches.

As reported in the 2012 DBIR, most organizations can be breached within minutes to hours, and the event can go undiscovered for weeks and months—or even years in the worst cases. IT security organizations focused on risk-based security might consider placing more focus on early detection and response in order to improve incident outcomes. Figure 4-5 is a sobering reflection of how long an attacker may go undetected.

FIGURE 4-5. Breach timeline, Verizon 2013 *Data Breach Investigations Report*.



The Conclusions and Recommendations section of the 2013 DBIR suggests that implementing and adhering to the 20 Critical Security Controls framework would correct a majority of the weaknesses exploited in the data breaches investigated in 2012. The report states: "If you haven't already, the first recommendation of this section is to familiarize yourself with the content and structure of the 20 Critical Security Controls (CSC)."

KEY METRICS FOR COST CONTAINMENT

Although there's no simple equation that correlates security spending with program efficiency, cost metrics continue to be important, particularly to executives and boards. Respondents indicate that 'reduction in the cost of security management activities' (52% US, 46% UK) and 'reduction in unplanned system downtime' (40% US, 35% UK) are the top two metrics for measuring effectiveness of cost containment (Figures 4-6a and 4-6b).

Unfortunately, the 'length of time to contain data breaches and security exploits' (one of the most important variables affecting the cost of a data breach) is infrequently used as a metric of cost containment—only 5% in the US and 12% in the UK use this metric. The cost of a breach tends to increase the longer the attacker remains undetected, but this metric is more difficult to measure. Despite the difficulties in collecting this data, there does seem to be an obvious disconnect for organizations that haven't yet recognized the cost savings inherent in early incident detection.

FIGURE 4-6A. Metrics for cost containment, US respondents

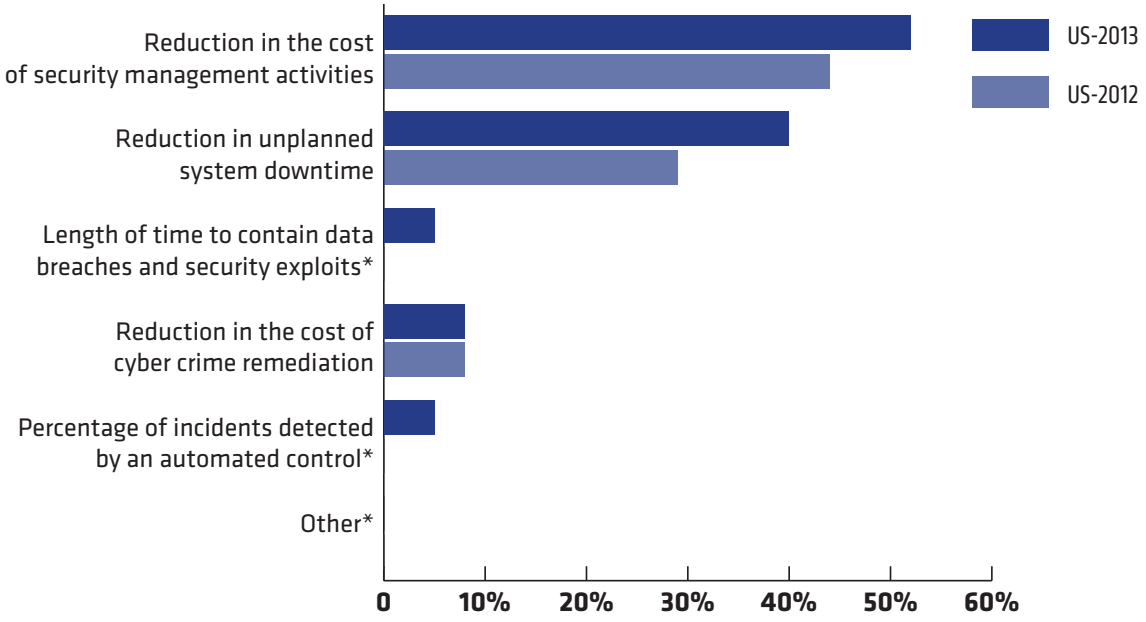
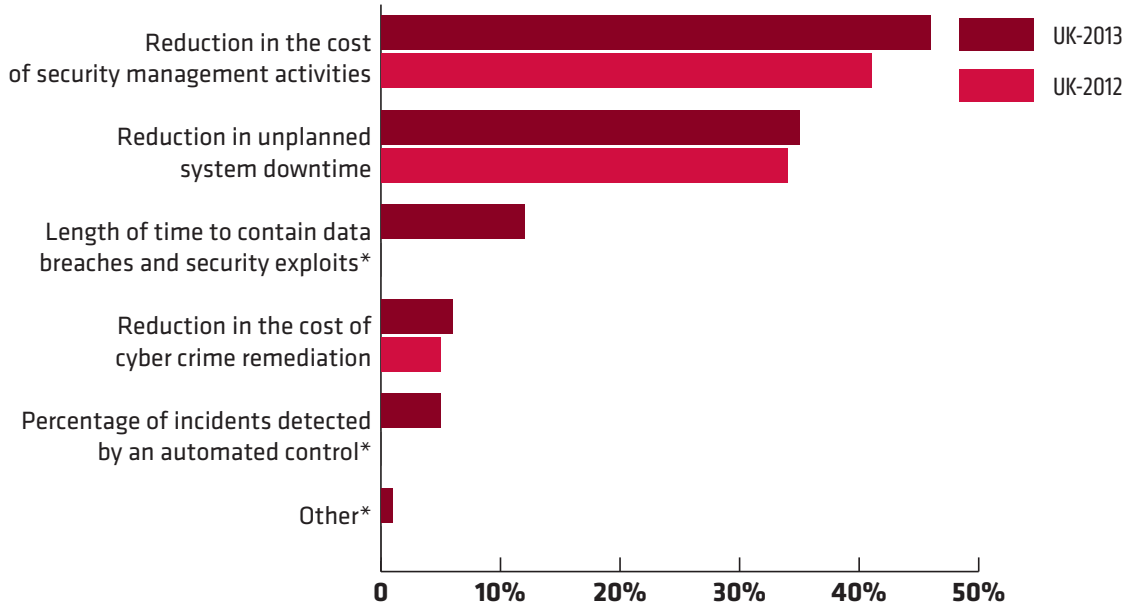


FIGURE 4-6B. Metrics for cost containment, UK respondents



*This choice was not available in 2012

Automation as a tool for detection isn't frequently measured either (6% US, 5% UK), but automation is a key driver in reducing security costs. It's also interesting that unplanned system downtime is a key security metric in the US This may be an indicator that security is starting to be held to the same performance requirements as IT.

MEASURES FOR STAFF AND EMPLOYEE COMPETENCE

Despite increases in other measures for security effectiveness from 2012, staff and employee competence isn't often used as a key metric. This may reflect industry ambivalence toward the effectiveness of security training or the lack of budget earmarked for training. Given that only 8% in the US and 6% in the UK even track retention of security awareness training, it's not surprising that the industry hasn't yet solved the problem of developing security expertise for personnel (Figures 4-7a and 4-7b).

FIGURE 4-7A. Metrics for staff and employee competence, US respondents

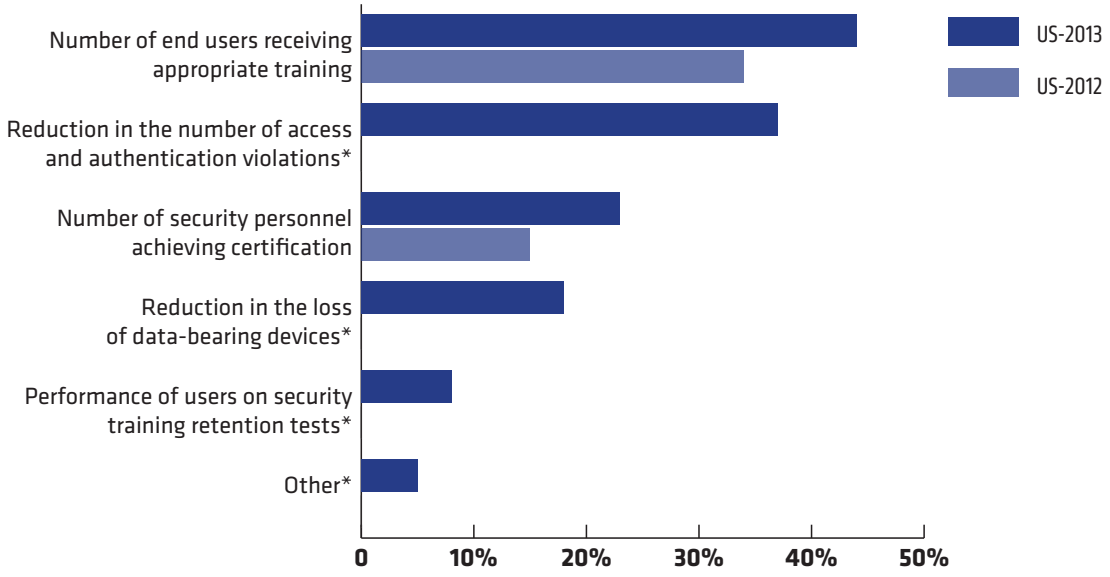
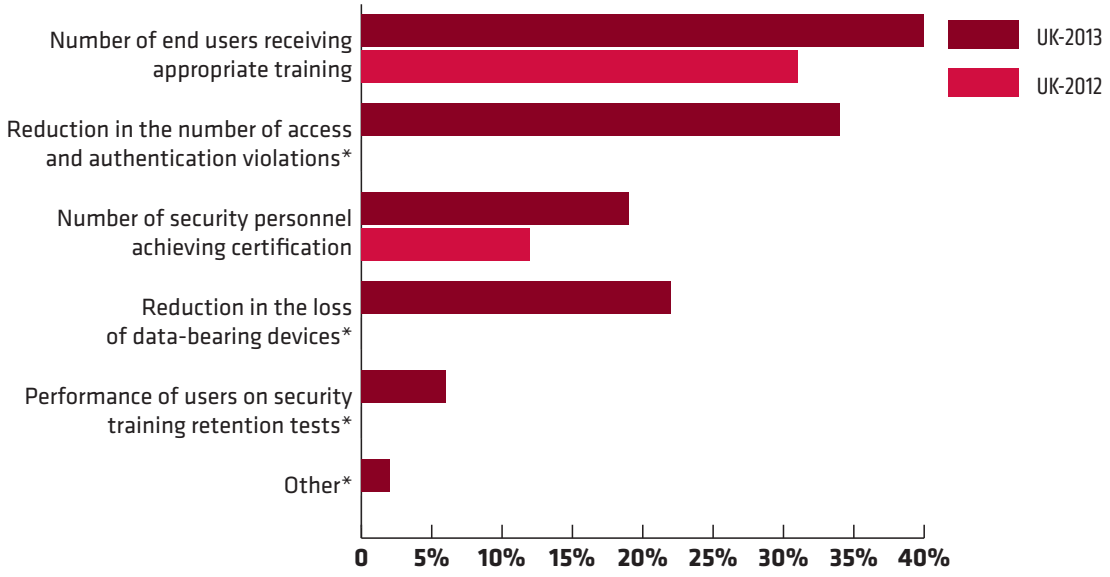


FIGURE 4-7B. Metrics for staff and employee competence, UK respondents



*This choice was not available in 2012

MEASURES FOR SECURITY EFFICIENCY

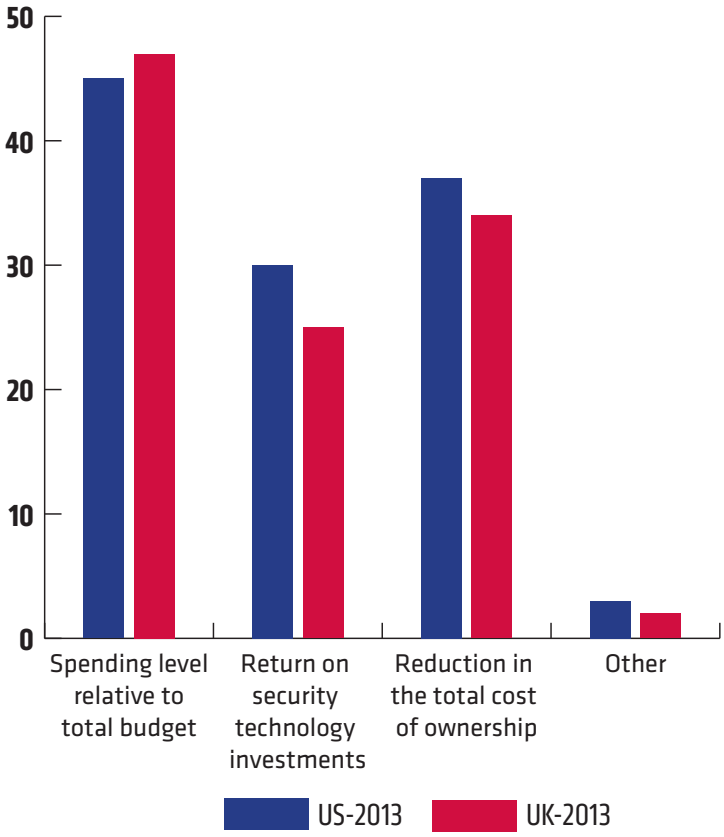
Responses to the question about which metrics are used to indicate security efficiency focus on budget, cost and return on investment. This is understandable, as monetary measures tend to be most valued by executives, corporate boards and investors. However, there is a notable lack of metrics that might track the efficiency with which security teams identify, prevent or remediate threats (Figure 4-8).

The most frequently used metric for security efficiency in both the US and UK is 'spending relative to total budget.' This is followed by 'reduction in the total cost of ownership' and 'return on technology investments.'

Why the emphasis on containing and reducing costs rather than containing and reducing threats? Budgeting and spending are not accurate measurements of risk-based security management; doubling risk-based security spending doesn't double security.

Metrics that focus on internal performance and process, such as how many people trained or how much money is spent, are easily measured—organizations tend to have business processes in place that can be easily adapted to these tasks. On the other hand, metrics that deliver more nuanced information about risk-based security programs, such as early detection of breaches and breach recovery time, are not as easy to quantify, particularly for organizations that are early in the risk-based security management deployment cycle.

FIGURE 4-8. Measures for security efficiency. US and UK respondents



SUMMARY

From this study, we can glean several useful indicators of how and where security managers are improving their use of security metrics—and where room for improvement remains.

Particularly encouraging is the finding that length of time to implement patches is a top metric. Speedier patching drives continuous improvement in security and highlights assets in an organization where issues exist that increase security risks.

On the other hand, recent breach analysis shows that expired certificates within an organization are a leading opportunity for exploitation, but this metric is not currently tracked by most organizations. A reduction in expired certificates is a proven best practice and should be tracked.

Cost continues to be an issue for security managers. Driving costs down is always a valid business concern, and security organizations are not exempt from contributing toward that goal. That said, it is important to balance the emphasis on containing and reducing costs with the need to contain and reduce threats.

Security metrics as measurements of risk-based security effectiveness are both an art and a science. Metrics can be also selective: just because it's possible create or track a metric doesn't mean the organization really needs or wants this information—or knows how to properly apply it. For instance, cost containment (reducing or cutting costs) is a metric. However, the benefit or detriment of cost cutting may not be realized until a security event threatens the company's data or reputation.

To be valuable, metrics for security effectiveness must be meaningful to organizational goals or key performance indicators. Security managers should review metrics currently in place and ensure they are aligned not only with overall industry standards for security management, but also with the organizational and business goals of their particular employer.

CHAPTER 5: SECURITY CONTROLS AND SPENDING

Considering costs that can result from a single data breach—a whopping $5.4 million per data breach in the US, according to the Ponemon Institute in *The 2013 Cost of a Data Breach: Global Analysis*—it's easy to assume IT organizations are granted generous budgets in order to undertake a comprehensive risk-based security program. For most organizations this is not the case. However, organizations are making tangible progress when it comes to connecting security risks with security spending.

This chapter of the 2013 Ponemon Institute study on risk-based security management addresses security controls and spending in the US and UK. The nearly 2,000 respondents were first asked to identify how well their organization accomplished the key steps necessary to assess and prioritize security risks. It's particularly interesting to note that 51 percent of study respondents in the US and 49 percent in the UK said they have identified specific controls at various network layers to ensure the risks were acceptable to the business, but only 43 percent in the US and 39 percent in the UK said they had implemented those controls.

FIGURE 5-1A. Rate how well your organizations accomplishes each step used to assess and prioritize risks. Fully and partially accomplished responses combined.

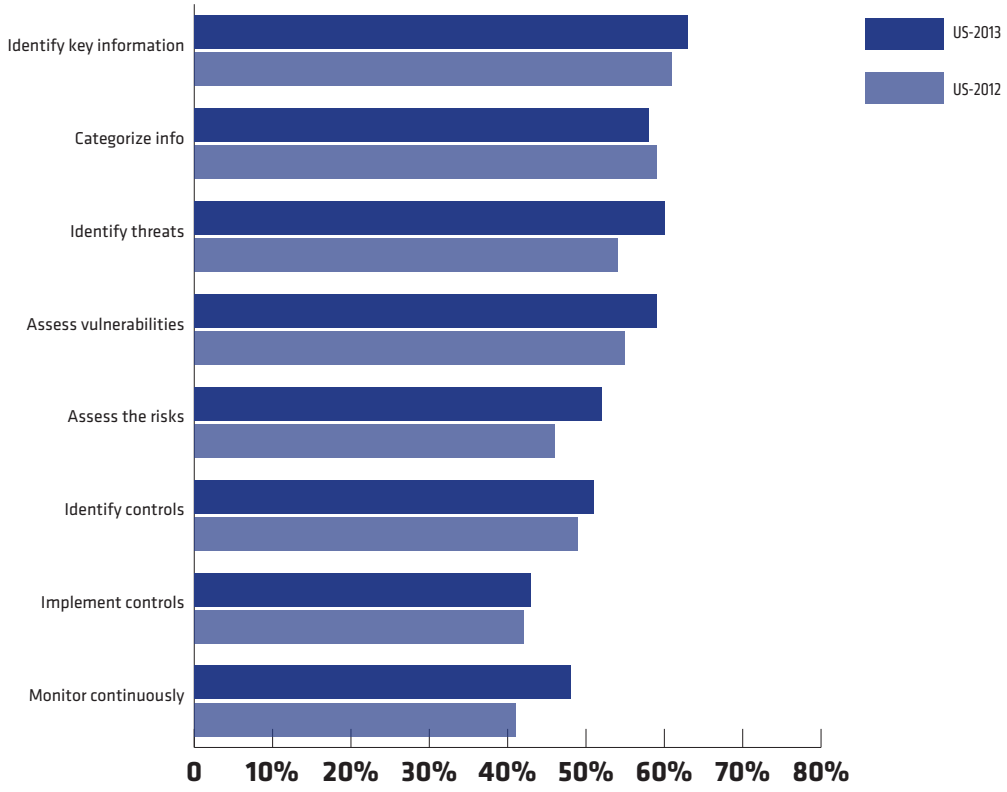
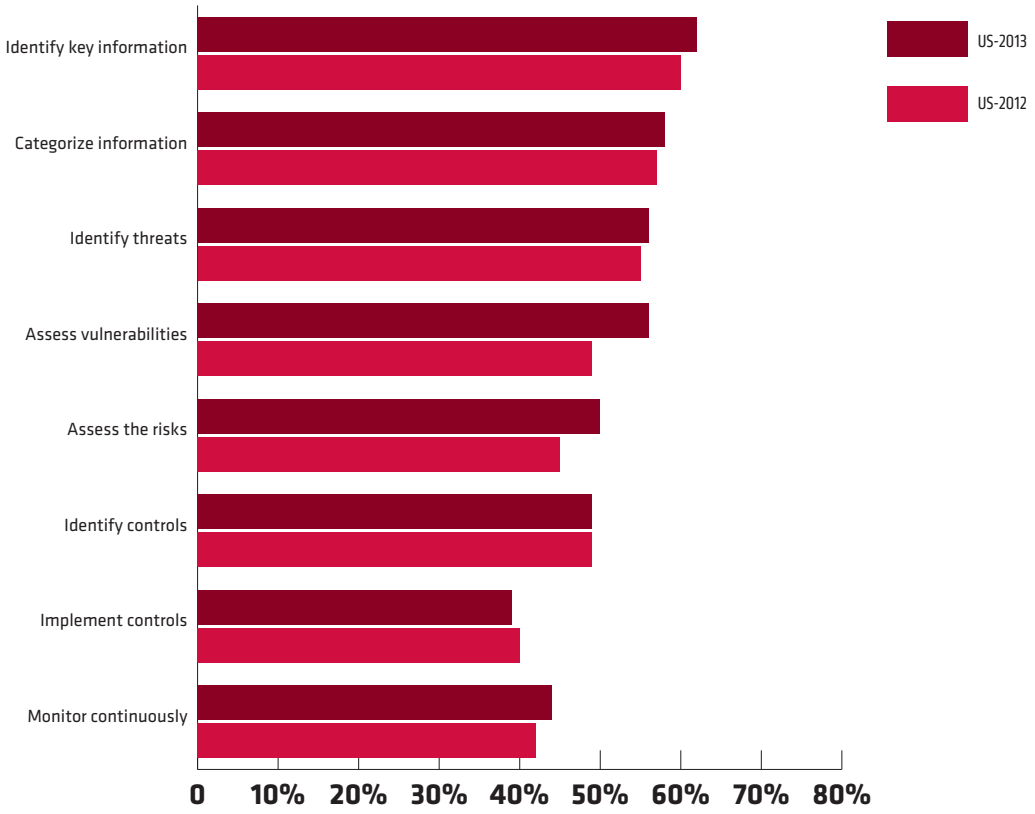


FIGURE 5-1B. Rate how well your organizations accomplishes each step used to assess and prioritize risks. Fully and partially accomplished responses combined.



IT organizations generally follow a progression of eight basic steps when implementing a security-based risk management program. Those steps, in order of implementation, include:

1. Identify information that is key to the business

2. Categorize information according to its importance to the business

3. Identify threats to the information

4. Assess vulnerabilities to the systems that process the information

5. Assess the security risks associated with loss of the information

6. Identify security controls necessary to mitigate the risks

7. Implement the controls

8. Monitor controls continuously

Responses shown in Figures 5-1a and 5-1b might seem to cast the practice of continuous monitoring into a yes or no category; however, the reality of continuous monitoring is that its implementation is more of a spectrum. The good news—evident in the results—is that even though less than half of the organizations have adopted continuous monitoring in 2013, many organizations are making progress, particularly in the US, with 7 percent improvement over 2012 results. Nevertheless, there's still a lot of room for improvement in the maturity of risk-based security programs and continuous monitoring of controls.

PREVENTIVE CONTROLS MORE EASILY UNDERSTOOD

Many IT professionals also view preventive controls in terms of two black and white variables: deployed or not deployed. This question asked respondents about controls that are fully and partially deployed, which provides a broader view of preventive practices.

FIGURE 5-2A. Indicate which of the following preventive controls are deployed in your organization's current security infrastructure. Fully and partially deployed responses combined.

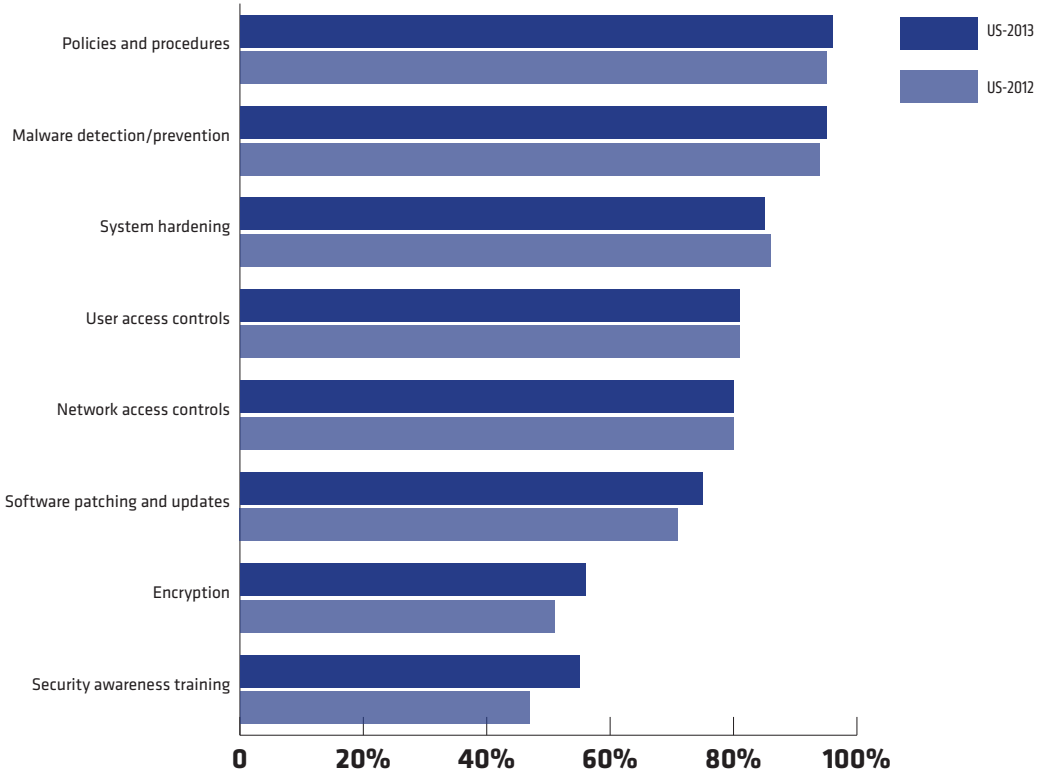
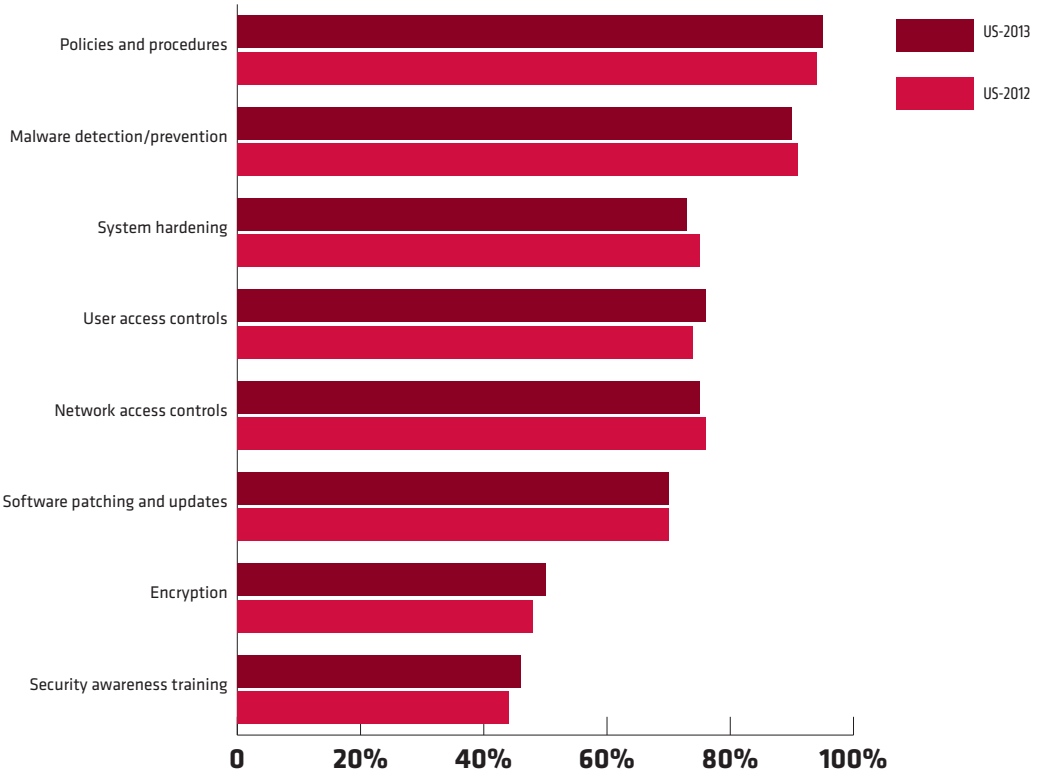


FIGURE 5-2B. Indicate which of the following preventive controls are deployed in your organization's current security infrastructure. Fully and partially deployed responses combined.



It is not surprising that policies and procedures, and malware prevention are widely deployed. Many industry studies have indicated a sharp rise in the success of malware as an exploit vector in 2012 and 2013, especially when combined with phishing. In addition, malware detection and prevention controls have been widely available for more than ten years and are well understood by executives. These controls are easier to implement than many other security controls and are included in many compliance standards and regulations.

Encryption was rated near the bottom (No. 7 among the eight controls for both US (56 percent) and the 50 percent in the UK), despite being one of the controls with the most potential to reduce risk. However, encryption adoption can be expensive and difficult, particularly for legacy systems. Encryption can also add significant overhead on network infrastructure, and complete deployment may require heavy investment in new network and storage systems as well as a revision of organization procedures and workflows.

Security awareness training is the lowest ranked preventive control in both the US and UK. Since human error is widely acknowledged as a significant factor in many security breaches, these results could be seen as an indictment of the efficacy of existing security training programs. Limited budgets dedicated to security awareness programs may just reflect the relative expense of these programs compared with other more technology centric controls. In addition, in some IT organizations, security tools and technology are given far more emphasis than security awareness training.

DETECTION CONTROLS: GREATER POTENTIAL FOR SECURITY

While preventive controls are established and relatively well understood, detective controls are relatively new. Although adoption has increased modestly over 2012 numbers, survey results indicate that adoption and deployment of detective controls still lag significantly behind preventive controls.

While the 2013 DBIR 'access to compromise gap' is measured in seconds to hours, the 'breach to detection gap' is typically measured in months to years. Breaches often go undetected for a long periods of time, a trend that is alarming given the number of well established and widely available preventive controls. The DBIR advises organizations to continue preventive measures but also urges organizations to place increasing resources and renewed effort on breach detection and containment. The report points out that reducing the time it takes to detect and contain a breach results in a significant reduction of breach costs.

Log management, incident detection/alerting and file integrity monitoring are listed as critical security controls in almost every standardized security controls framework and are also required by nearly every major compliance regulation. Yet, just over half of organizations report that they are fully utilizing these security controls (Figures 5-3a and 5-3b).

FIGURE 5-3A. In your organization's current security infrastructure, place a check by each of the following detective controls currently deployed. Fully and partially deployed responses combined.

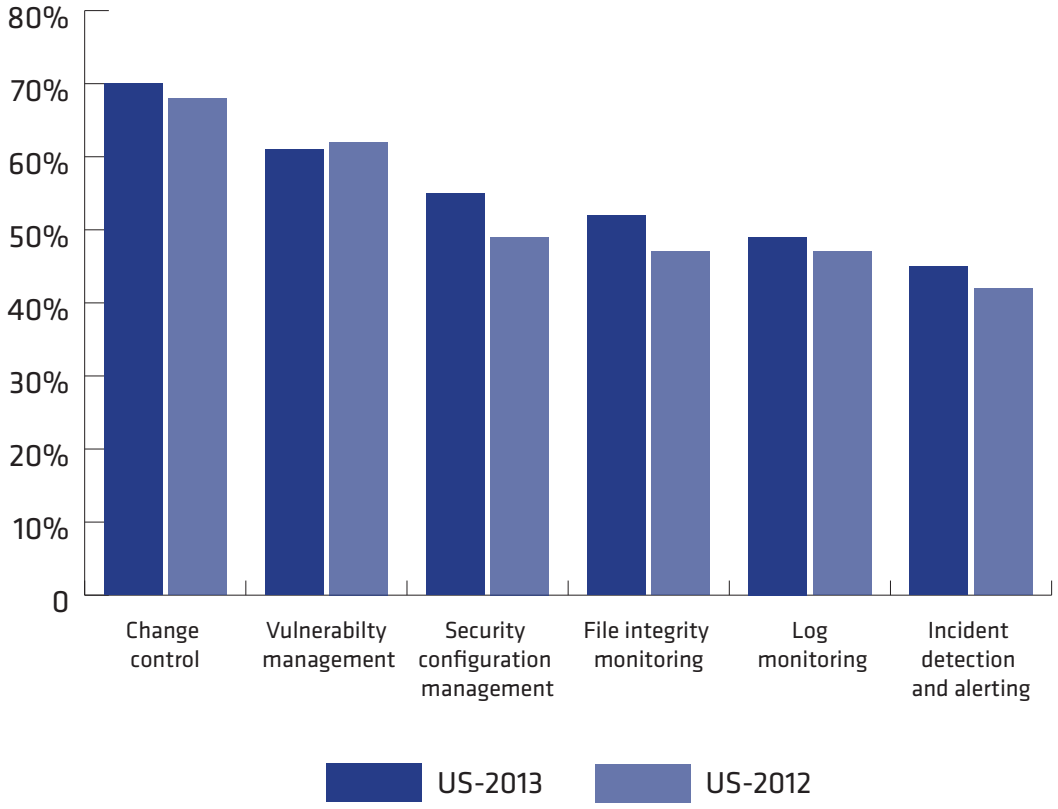
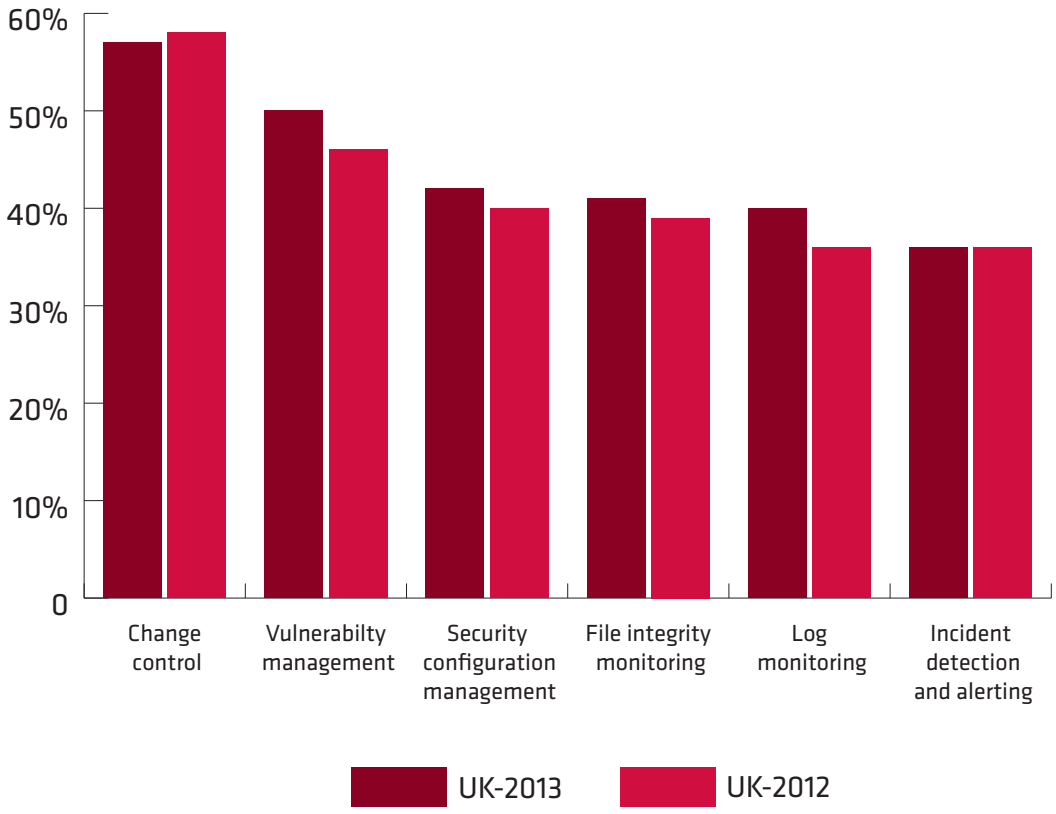


FIGURE 5-3B. In your organization's current security infrastructure, place a check by each of the following detective controls currently deployed. Fully and partially deployed responses combined.



Organizations that invest in detective controls often choose a multi-functional solution, even when the purchase is driven by a single need, such as compliance or change control. Due to limitations in staffing and training, it may be difficult to deploy and utilize the complete capabilities of these multi-function tools. This may explain why 70 percent of respondents in the US and 68 percent in the UK have implemented change control, but only 45 percent US and 40 percent UK are using incident detection and alerting.

PERCEIVED RISK AND SPENDING

Among the seven layers of the Open Systems Interconnection (OSI) model, the application layer is associated with the highest security risk. Respondents both in the US (36 percent) and UK (38 percent) agree with this assessment, rating the application layer much higher than the other layers in the typical multi-layered security infrastructure, which includes the data, network, human, host and physical layers. Application layer risks include many third party solutions where accurate risk assessment and control is challenging (Figures 5-4a and 5-4b).

FIGURE 5-4A. Allocate security risks in each of the six layers in a typical multi-layered security infrastructure.

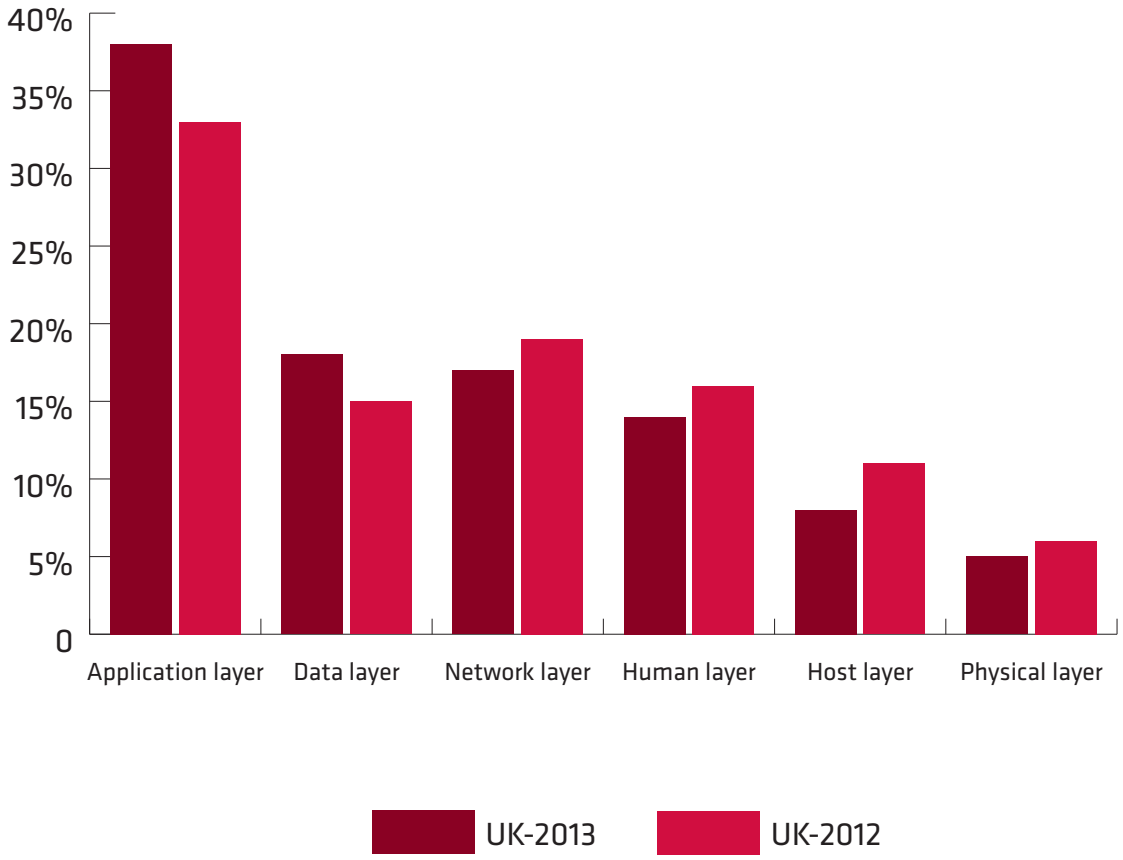
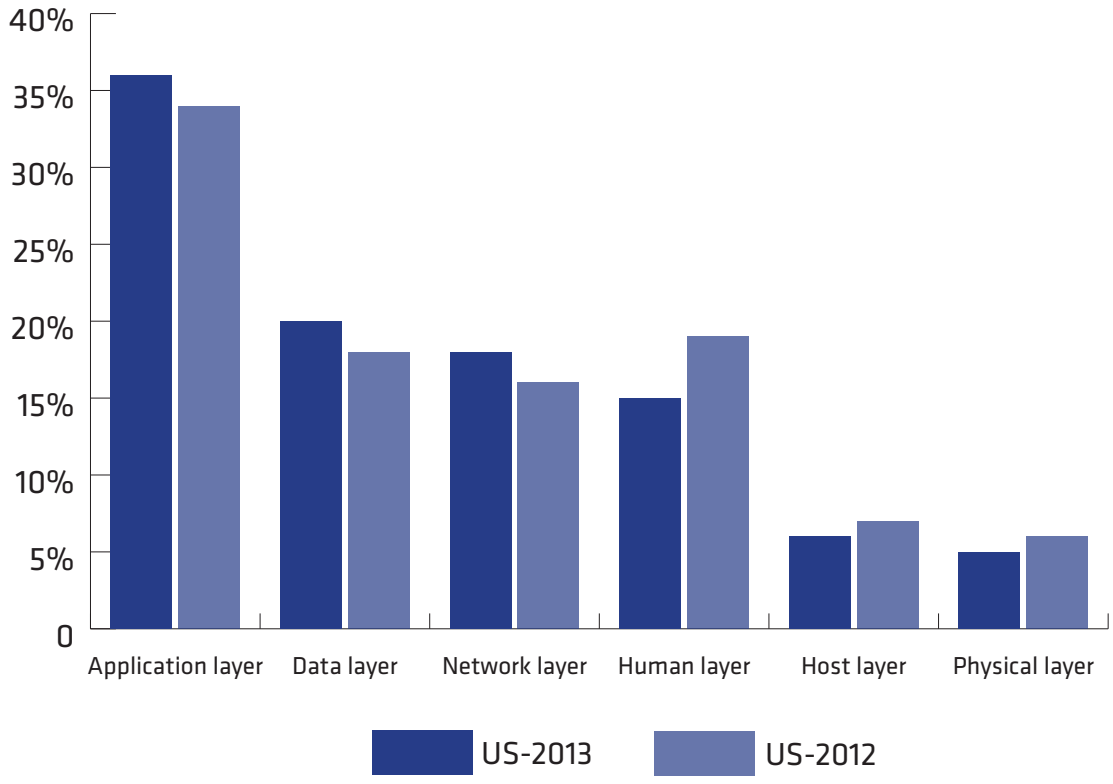


FIGURE 5-4B. Allocate security risks in each of the six layers in a typical multi-layered security infrastructure.



Yet, while the application layer is understood to have the most significant security risks, the majority of security spending is focused on the network layer, as shown in Figures 5-5a and 5-5b.

FIGURE 5-5A. Allocate the level of spending incurred by your organization for each of these six layers to lessen or mitigate security risk.

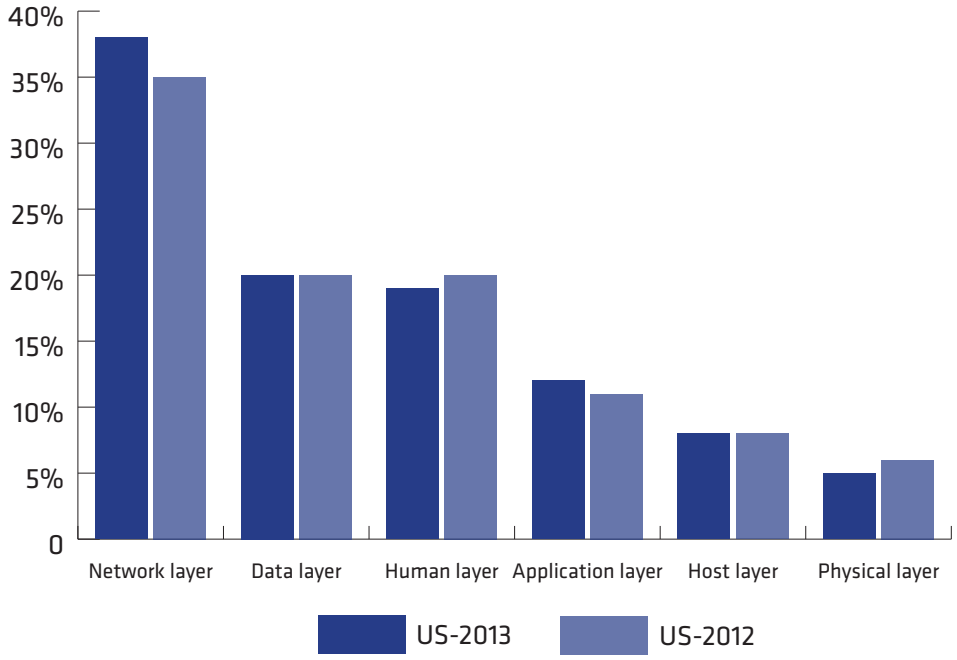
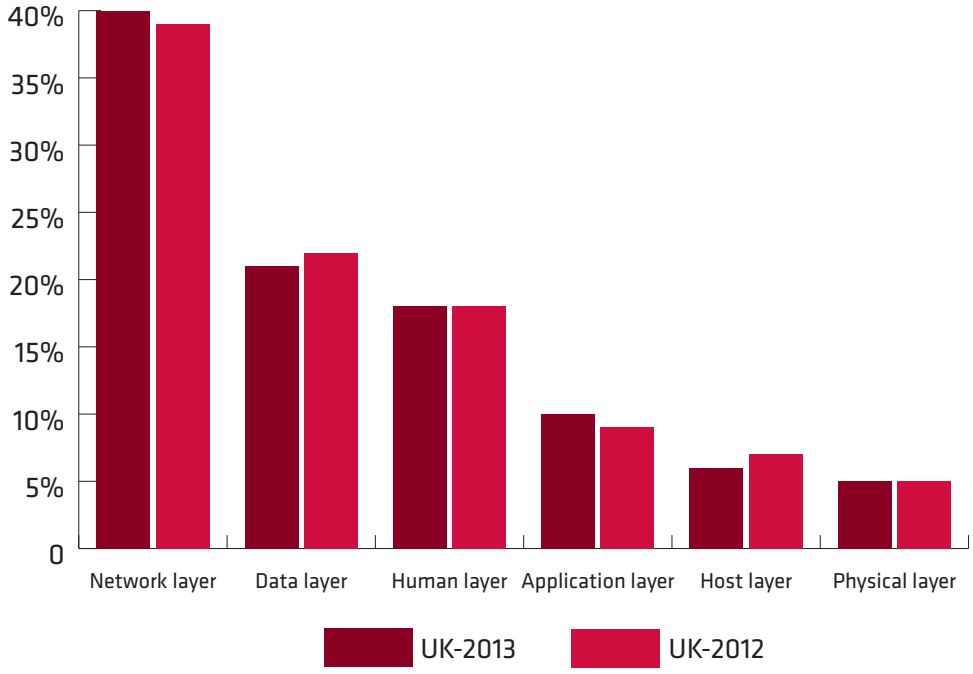


FIGURE 5-5B. Allocate the level of spending incurred by your organization for each of these six layers to lessen or mitigate security risk.



Figures 5-6a and 5-6b compare the difference between perceived risk and spending for each network layer. In the US, spending on the network layer is two times greater than its perceived risk, and in the UK, it's almost 2.5 times greater. In comparison, spending on the application layer is three times less than its perceived risk in the US and almost four times less in the UK. Perceived risk and spending on the host and physical layers are basically in balance.

In summary, these survey results indicate that security spending is higher on layers with lower perceived risk, such as the network layer, for all respondents. This could be because many organizations are still in the early stages of managing and implementing their risk programs, and spending on the network layer may reflect the relative level of program maturity for this layer. Capital spending for network layer equipment is depreciated, so it may be easier to attain budget for network layer equipment. Organizations with less mature security programs may have difficulty reducing the risk at the application layer because this typically involves third party and partner organizations. Finally, during difficult economic times, many organizations deferred or cut back on security spending. Perhaps it has now become essential.

FIGURE 5-6A. Difference between perceived risk and spending for each network layer (US respondents).

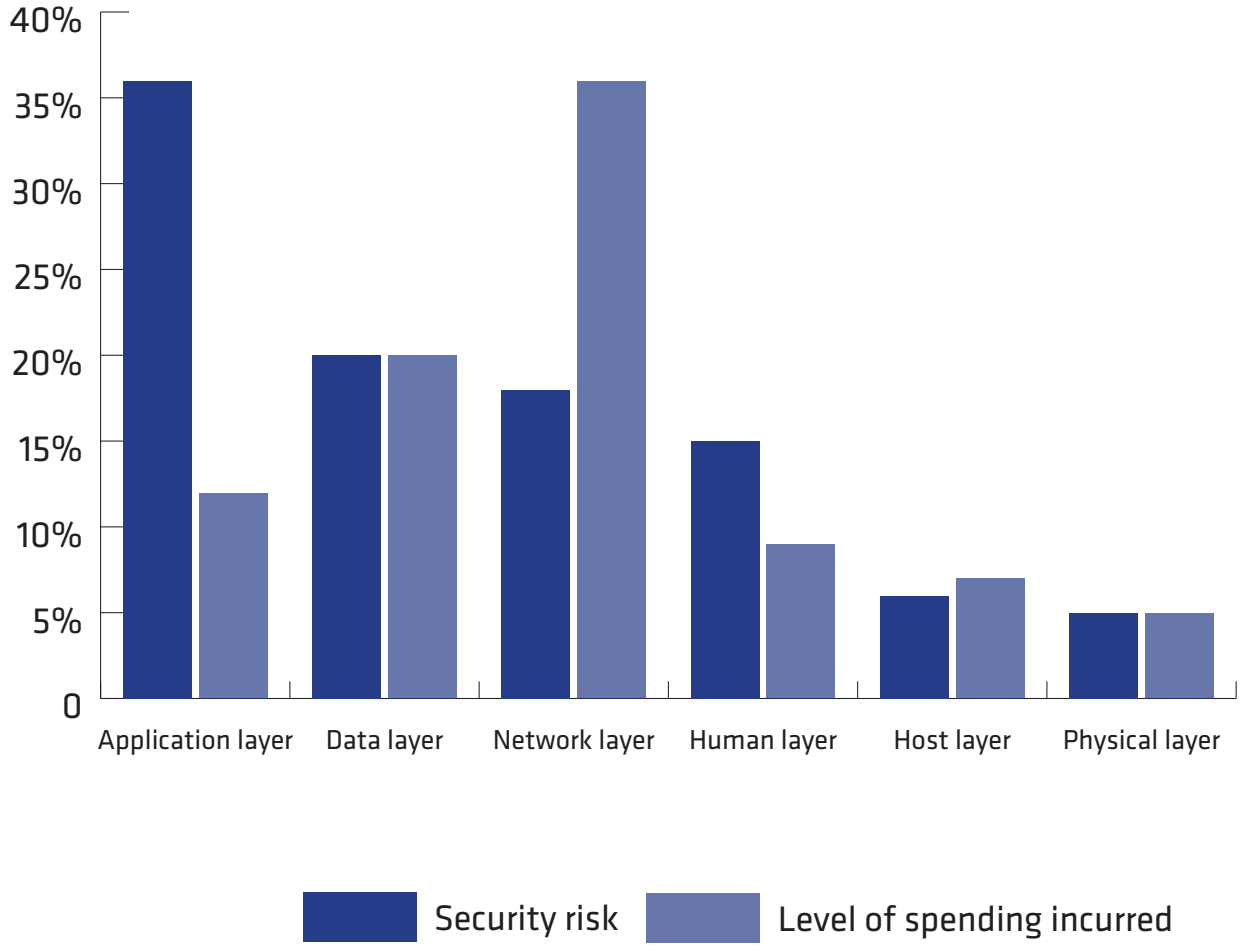
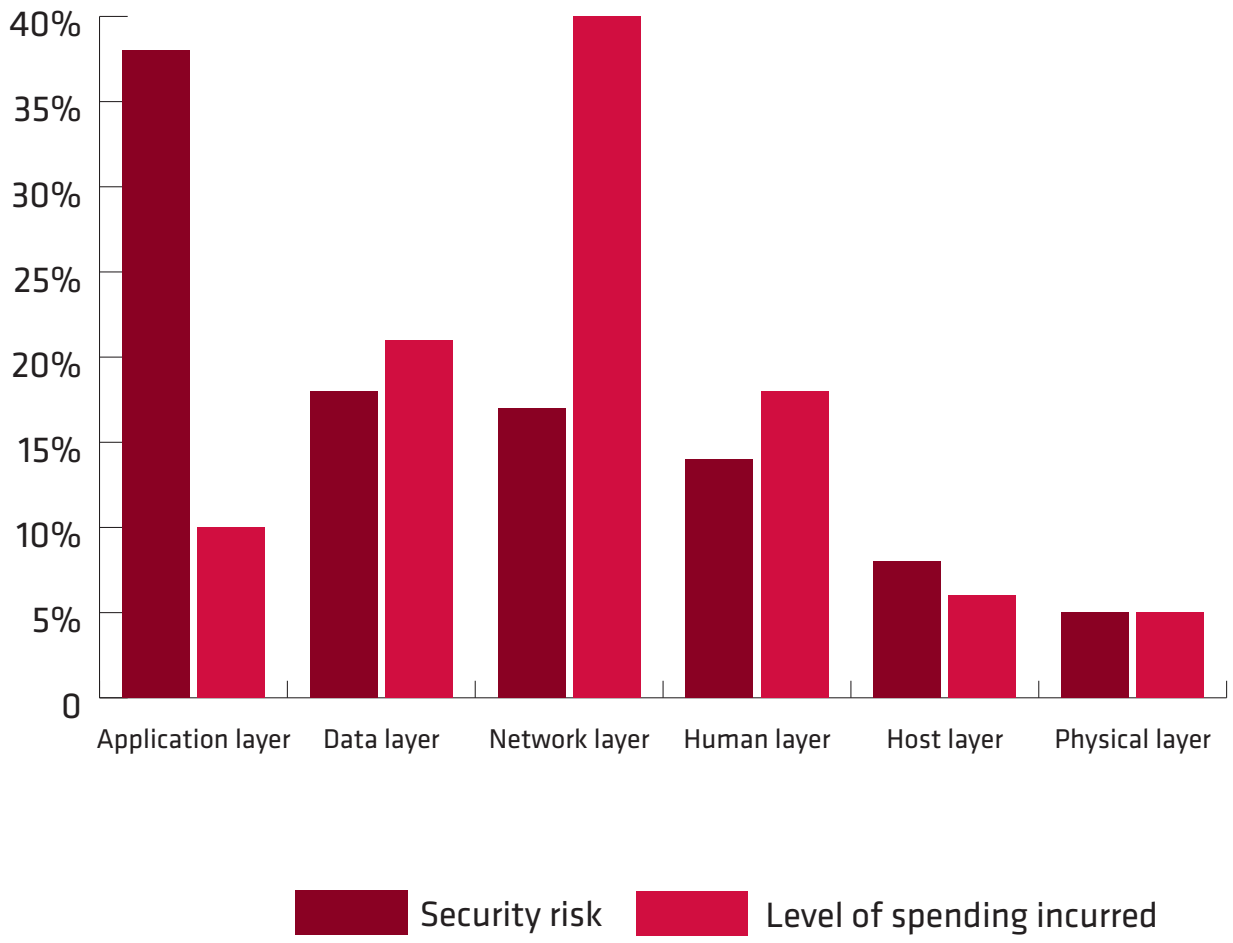


FIGURE 5-6B Difference between perceived risk and spending for each network layer (UK respondents).



METHODS FOR IDENTIFYING SECURITY RISKS

Insights into security and spending in this section of the study are among the most surprising survey results. Figures 5-7a and 5-8b detail responses to questions about the methods organizations use to identify security risks.

FIGURE 5-7A What steps does your organization take to identify security risks? Check all that apply.

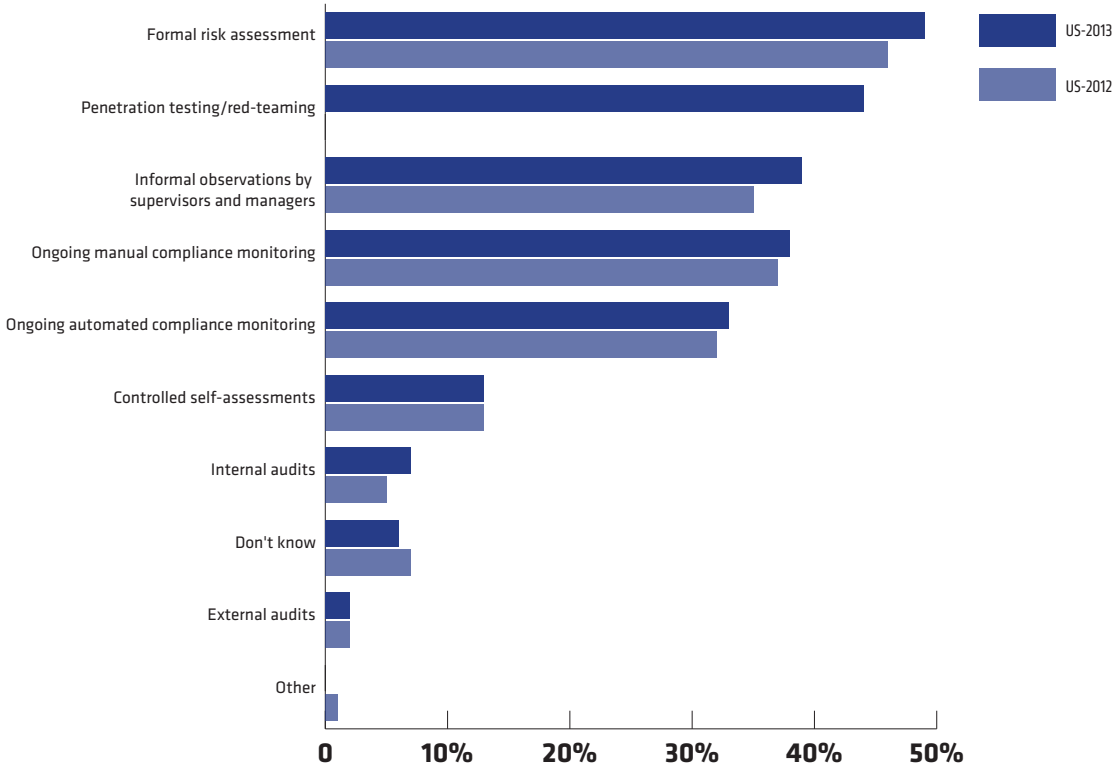
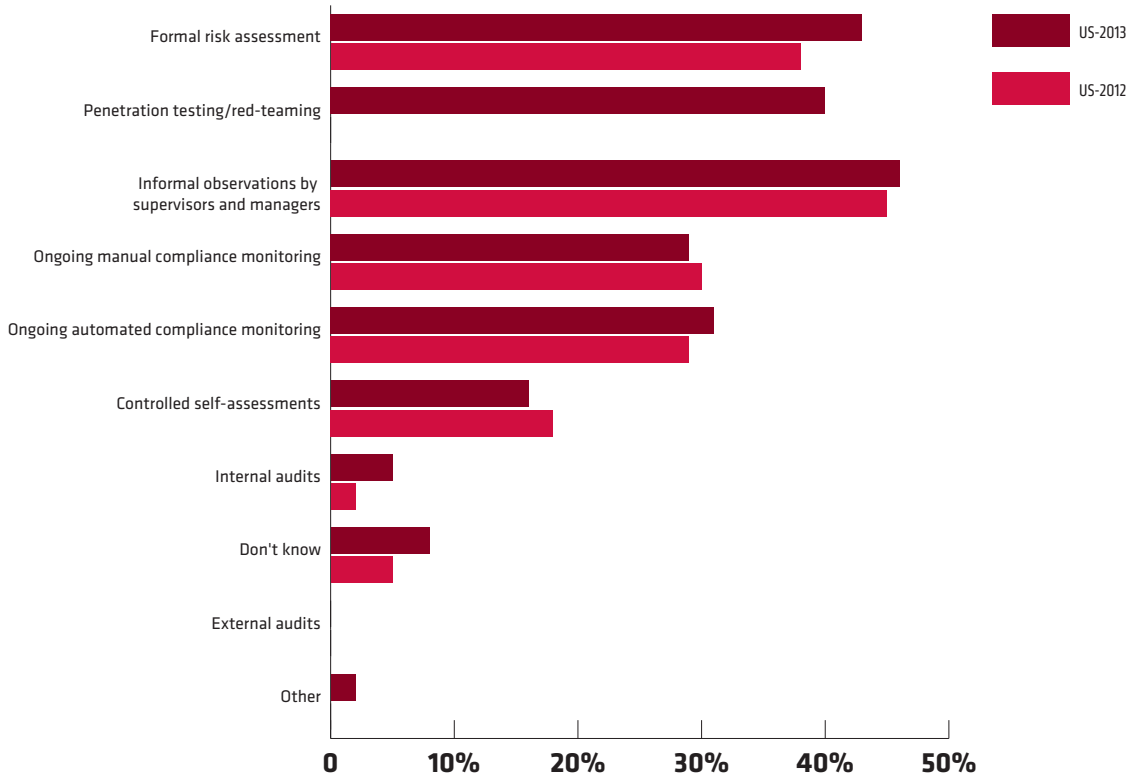


FIGURE 5-7B What steps does your organization take to identify security risks? Check all that apply.



"Informal observations by supervisors" ranked third in the US (39 percent) and first in the UK (46 percent). In addition, just 49 percent in US and 43 percent in UK use formal risk assessments to identify security risks, and only 38 percent US and 31 percent UK use automated compliance monitoring for this purpose, even though automated security tools significantly reduce both risks and costs.

Informal or "drive-by" management assessments are surprising because these assessments aren't quantifiable, formal or reproducible. Despite these obvious drawbacks, informal feedback and observation by management are widely used in the UK This type of informal assessment makes it difficult to quantify improvements and identify trends in security, and these less formal methods may contribute to the difficulty many organizations face while trying to effectively communicate security risks to senior executives. While low-tech, observational-based methods may have worked in the past, automation and new technologies now make it possible to provide better, more consistent insight into the rapid changes taking place in security risk intelligence.

SUMMARY

Risk-based security management is moving in the right direction, albeit slowly. At best, the results indicate that more organizations are beginning to address their security risks with some type of security control framework, and about 10 percent of those organizations that were in the process of deploying security controls in the 2012 survey have advanced to a more mature approach. However, it's clear that many organizations have identified controls and conducted the necessary assessments but haven't yet implemented many of the controls that can be most effective at reducing security risks.

Security practitioners and risk managers need to move away from a binary model of security controls and begin to evaluate them in the context of their businesses. This approach can effectively deliver a more nuanced and accurate assessment of the organization's security risk and provide clearer insights into the efficacy of specific security controls and technologies.

CHAPTER 6: COMMUNICATION, COLLABORATION AND CULTURE IN A RISK-BASED SECURITY MANAGEMENT ORGANIZATION

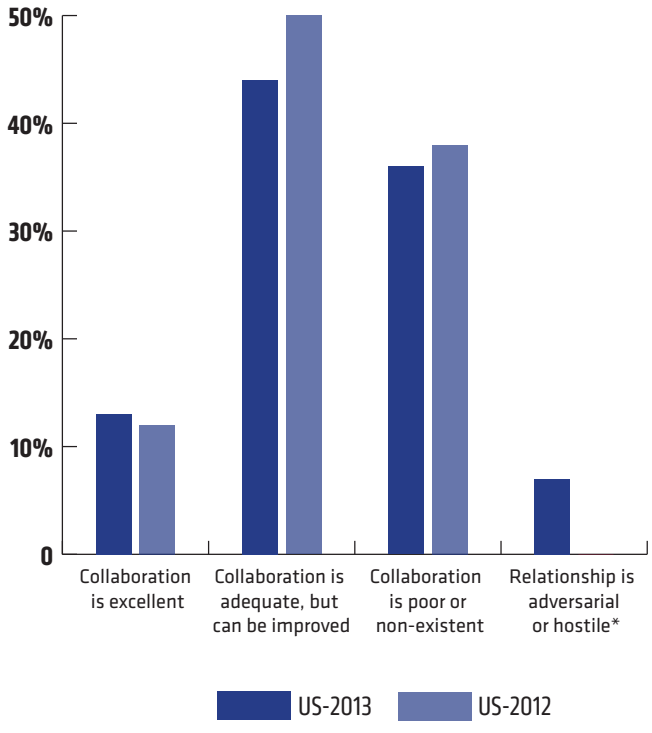
In Chapter 3 of this study conducted by Ponemon Institute, 81 percent of respondents said that their organization's commitment to risk-based security management was significant or very significant. In this chapter, we dig deeper into the disconnect between an organization's commitments to risk-based security management and its ability to develop the collaboration, communication styles and culture necessary to make risk-based security programs effective across the organization.

COLLABORATION EFFECTIVENESS

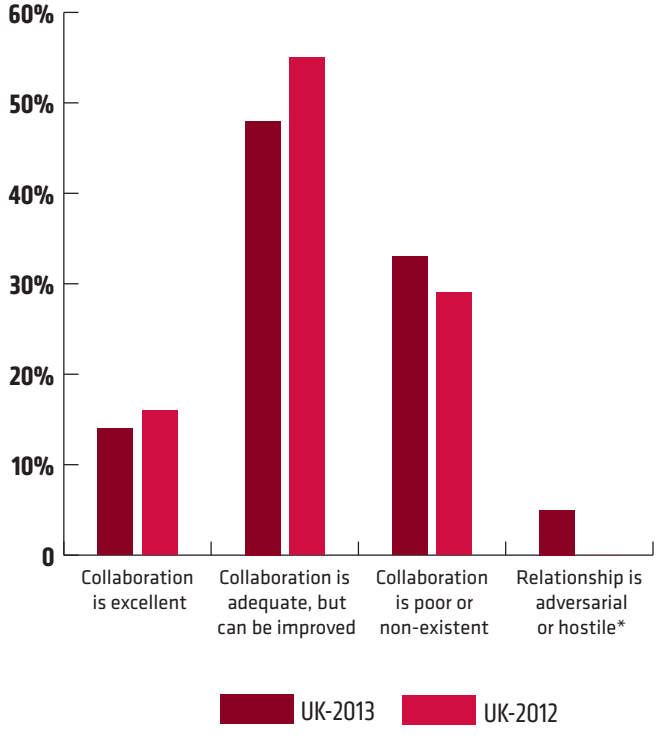
The key ingredient in the creation of an organizational culture that is security-aware is collaboration. Higher levels of collaboration ensure that security is not isolated from other areas of company operations and helps avoid information silos.

When asked to rate the level of security and risk management collaboration in their organizations, just 13 percent in the US and 14 percent in the UK said it was 'excellent.' The majority of respondents (50 percent in the US and 44 percent in the UK) said collaboration was adequate but can be improved, and a significant number (41 percent in the US and 38 percent in the UK) rated collaboration as poor or nonexistent (Figures 6-1a and 6-1b).

FIGURES 6-1A/B. What one statement best describes how security and risk management functions within your organization work together to support business objectives?



*This choice was not available in 2012

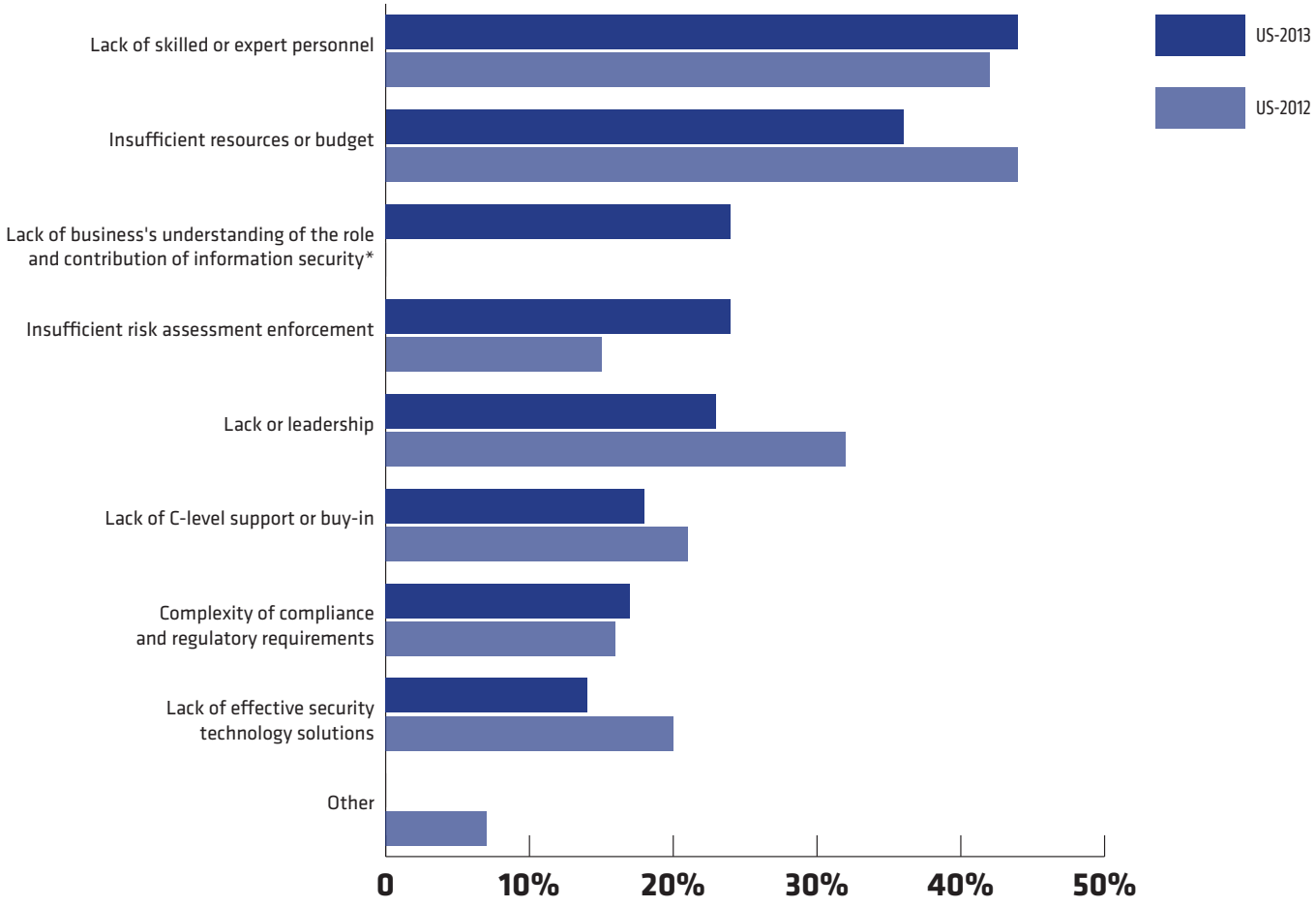


*This choice was not available in 2012

Although company cultures vary significantly, there are common barriers that impact collaboration. The most significant barrier in both the US and UK is the lack of skilled or experienced personnel, followed closely by insufficient resources or budget (Figure 6-2A and 6-2B). These findings are not surprising, since resource limitations often mean that security resources are stretched very thin.

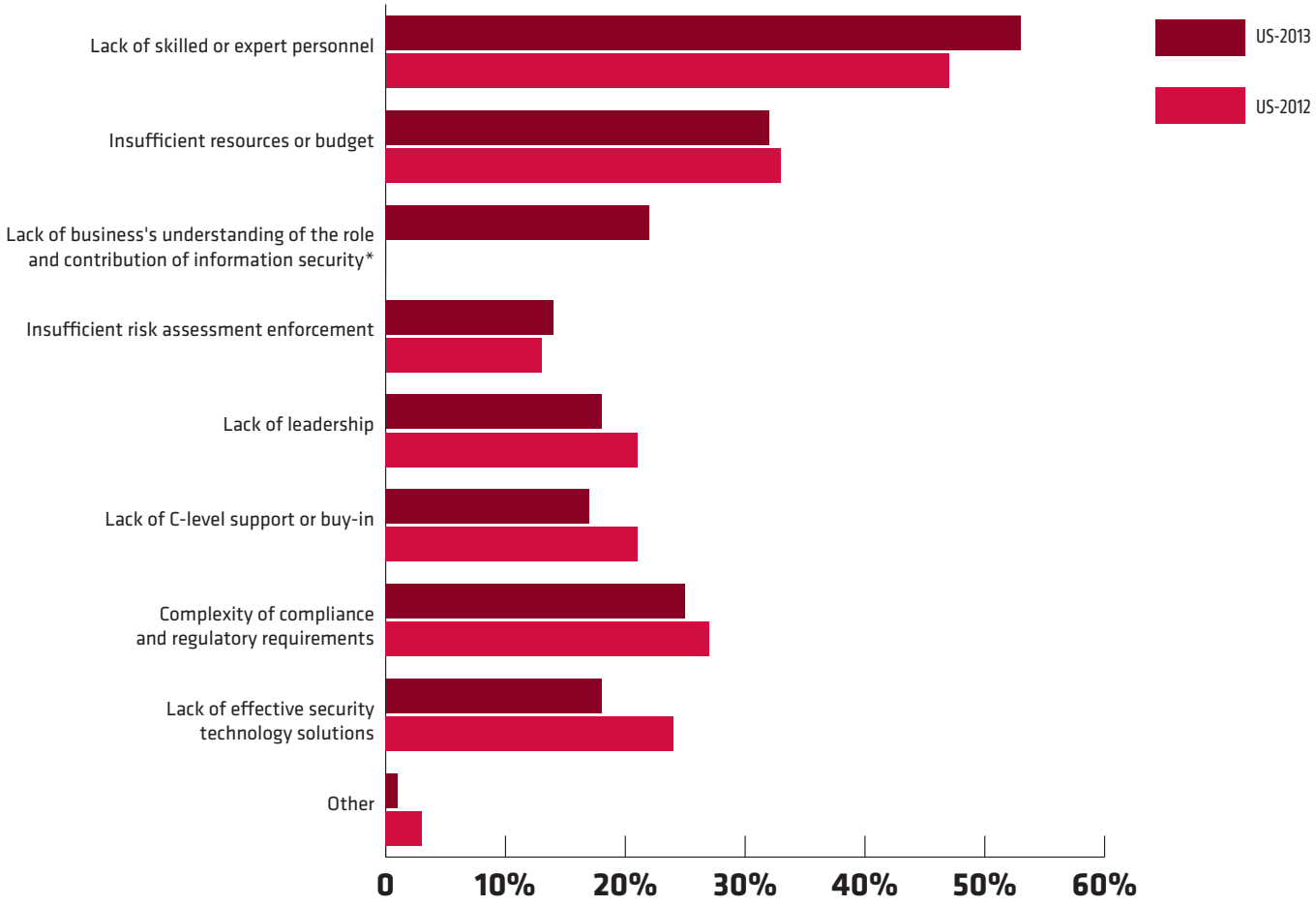
Based on these survey responses, it's not possible to assess whether the skill gap is on the technical side or on the 'soft skills' side. However, given the deep technical background of many IT security professionals, it's probably both.

FIGURE 6-2A. What do you see as the most significant barriers to achieving effective risk-based security management activities within your organization today? Please select your top two choices.



*This choice was not available in 2012

FIGURE 6-2B. What do you see as the most significant barriers to achieving effective risk-based security management activities within your organization today? Please select your top two choices.



*This choice was not available in 2012

Lack of skilled personnel is a very significant problem for almost every organization. Studies conducted by the Ponemon Institute show that demand for skilled security professionals is four times greater than supply. Contributing to this problem, security engineers are expected to be generalists across many evolving, complex security disciplines. Successful cyber attackers, though, frequently specialize in a specific area.

Security skills take significant time and effort to develop, and it takes time and budget to find and hire security experts. As a result, the scarcity of skilled security professionals has become a systemic problem for most organizations. Effective information security professionals also need to develop business and communication skills, further compounding this problem.

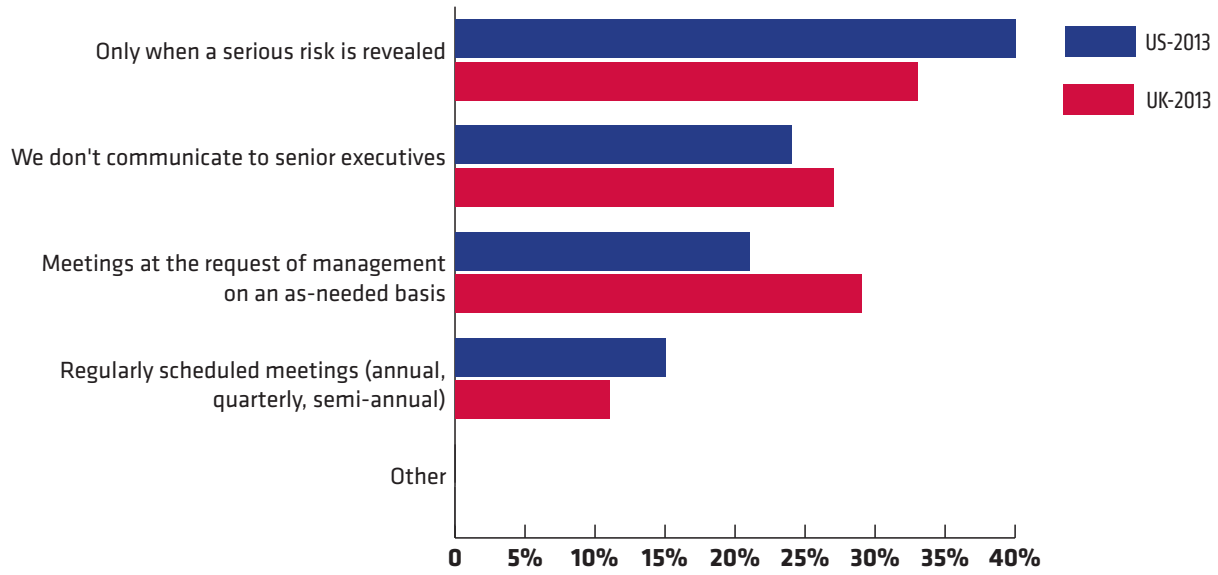
On the bright side, both US and UK figures indicate that lack of leadership is less of a barrier to effective risk-based security than it was in 2012. This was particularly true in the US—2013 figures showed a nearly 29 percent gain in this area.

PROACTIVE COMMUNICATION OF SECURITY RISKS

The lack of proactive security communication that can be understood by nontechnical executives is a significant challenge for a majority of security professionals. In the US, 64 percent of respondents (and 60 percent in the UK) admit they either do not communicate security risks to senior executives or do so only when a serious risk is revealed (Figure 6-3).

The chain of communication to the senior executive team is definitely broken. Eighty-five percent of US respondents and 89 percent of UK respondents don't meet with senior executives routinely about cybersecurity risks. The majority of security professionals are not able to effectively articulate the security risk or demonstrate clearly that security is aligned with the goals of the business.

FIGURE 6-3. When do you communicate the state of security risk to senior executives in your organization?



In light of these findings, it is not surprising that half of respondents rated their own communication skills as 'not effective' (Figure 6-4).

It is apparent from these responses that security professionals are aware of the importance of building a bridge, yet about half of the respondents (51 percent in the US and 47 percent in the UK) rate communication with senior executives as not effective. What is keeping them from being effective communicators? Figure 6-5 helps explain the issue.

FIGURE 6-4. Please rate your effectiveness in communicating all relevant facts about the state of security risk to senior executives?

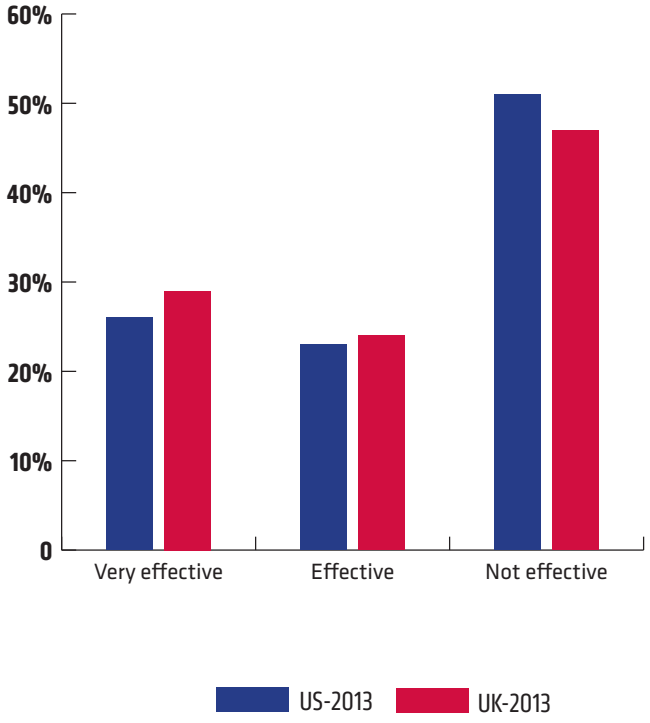
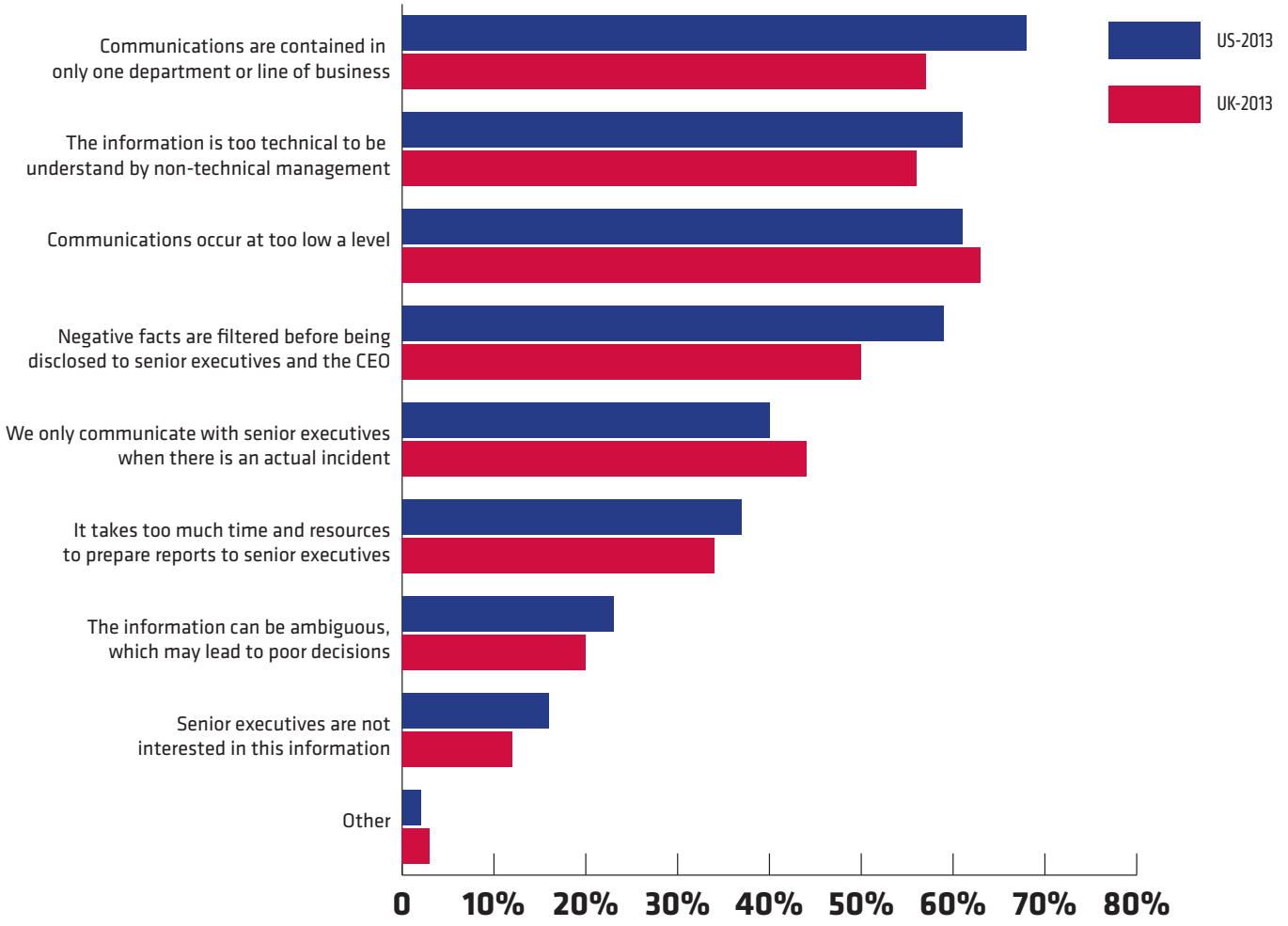


FIGURE 6-5. If not effective, why not? Please select all that apply.



When asked why communication with senior executives was not effective, 68 percent in the US and 57 percent in the UK said the information was too siloed, while 61 percent US and 56 percent UK said the information was too technical to be understood by nontechnical management. This is understandable as IT security has its own jargon—acronyms, technology and terminology—that can make it a difficult for nontechnical executives to understand.

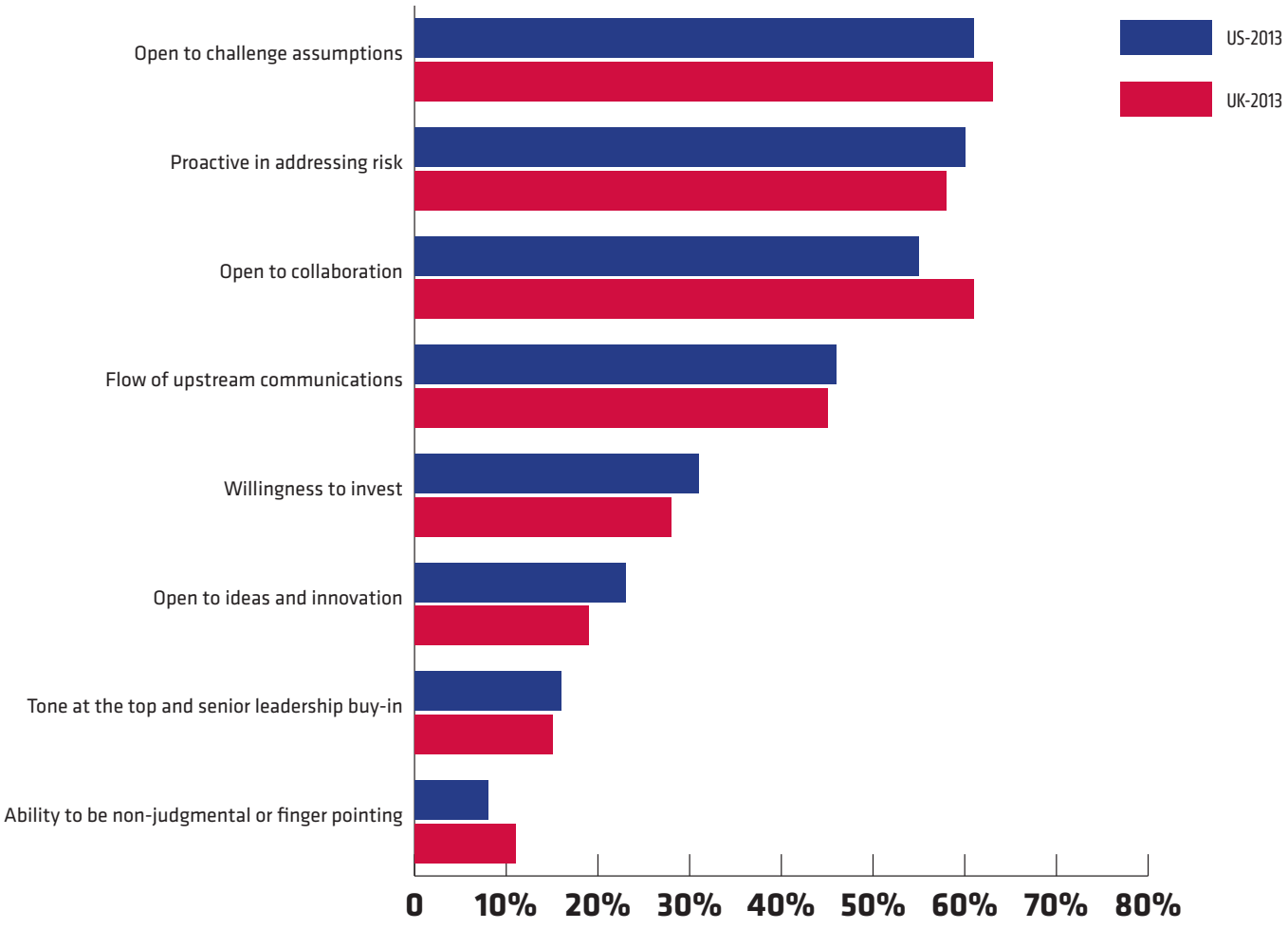
A more serious problem, particularly in light of the frequency and seriousness of cyberattacks, is that 59 percent of respondents say that negative facts are filtered before being disclosed to senior executives and the CEO, dramatically limiting the opportunity for effective communication and reducing the organization's visibility into the urgency of security issues.

A small but still troubling percentage of respondents (16 percent of US and 12 percent of those in the UK) say that senior executives are not interested in risk-based security management communications. Given the rising media profile of cybersecurity issues, these results are more likely an indictment of security professionals' ability to communicate effectively than an accurate barometer of executive disinterest.

COMPANY CULTURE CAN MAKE OR BREAK RISK-BASED SECURITY MANAGEMENT

The key factors that affect an organization's ability to support risk-based security management include openness to challenge assumptions and being proactive in addressing risk (Figure 6-6). However, given the other communication challenges listed in Figure 6-5, it's likely that most organizations are still struggling to establish a culture that supports the communication essential to risk-based security management.

FIGURE 6-6. The following is a list of eight factors that affect organizational culture. Which features are most critical to the success of a risk-based security management approach. Please select your top three choices.



CONCLUSION: LUCK FAVORS THE PREPARED

In business there exist degrees of randomness, ranging from perfectly predictable to dynamic chaos. Security lives in the middle—a stochastic zone of complexity, predictability and outcome, and where assumptions are constantly morphing. This means that even the most secure and sophisticated organizations are at risk because there are too many variables in play. Since this is unlikely to change any time soon, effective communication and collaboration are critical for mitigation when things awry.

As cyber attacks increase in sophistication and quantity, the need for security professionals and C-suite executives to effectively understand and exchange information is even more pressing. Good communication—both downstream and up—is an essential part of every good security program. In the same way that every company has a crisis communication plan, every organization also needs a security communication process in order to embed security in day-to-day operations.

Both sides have a responsibility to meet this challenge. Not only does IT security need to learn how to report actionable security information within a business context, executives must ask relevant questions and require adequate answers in order to progress from silent participants to informed leaders.

However, with buy-in and awareness from every level—from rank-and-file employees to the C-suite—organizations can mitigate security risks to critical assets such as high-valued data, customers, revenue and reputation.

It's been said that luck favors the prepared. If true, then those organizations with the culture and communication to establish a solid security posture on risk-based security management principles are on the strongest footing.

ADVANCING RESPONSIBLE INFORMATION MANAGEMENT

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

For more information about this study visit
www.tripwire.com/ponemon/2013
and follow on twitter @TripwireInc