A Forrester Consulting Thought Leadership Paper Commissioned By IBM

Surviving The Technical Security Skills Crisis

An Assessment Of The Current Security Skills Landscape And How To Overcome It

May 2013

Headquarters | Forrester Research, Inc.
60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 | www.forrester.com

Table Of Contents

About Forrester Consulting
Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit www.forrester.com/consulting.

Executive Summary

Technical information security skills are in higher demand today than ever before. As IT environments become more complex and the threat landscape grows more malicious, organizations need skilled technical staff to meet increasing security and compliance demands. However, this has been a losing battle. IBM counted more than 137 million attempted attacks against its 3,700-plus customers in 2012, and although only a tiny percentage turn into incidents, failure can be devastating.[1] A 2012 study, for example, revealed that the average enterprise data breach costs $5.5 million.[2]

Technical security skills are in high demand but short supply. This means that security organizations are less efficient, and there is greater risk to business.

Without the properly skilled technical staff, chief information security officers (CISOs) and other security leaders are less able to manage risk and protect their organizations. Instead, they are forced to ignore innovation projects and business priorities and allocate scarce resource just to keep up with basic operational tasks. Ultimately, shortages in technical security skills across the industry raise the cost of recruiting proper talent and reduce the performance of the security programs.

All is not lost. Organizations today have suitable alternatives to deal with security skill shortages; security automation, managed security services (MSS), and outsourcing are all effective methods for compensating for deficiencies in key security areas. These options help organizations optimize operational efficiency and rapidly improve their security posture, enabling CISOs to focus on strategic priorities more critical to their organizations' success.

To help organizations better understand how to handle staff deficiency challenges, IBM commissioned Forrester Consulting to field an in-depth survey of security leaders at large enterprises (having 3,000-plus employees) located in North America, Europe, and Latin America.[3] The results of the survey confirmed the difficulties that CISOs have in recruiting and retaining technical security roles, particularly security architects, specialists, and network security staff. The survey also illustrates the increasing partnership that organizations have with managed security services providers (MSSPs) to address these challenges.

It's clear that organizations need to slingshot their current capabilities forward to meet increasing security demands, and high customer satisfaction levels demonstrate that MSSP partnerships can help. Quite simply, MSSPs can leverage economies of scale by recruiting skilled professionals that other organizations may not have the ability to source or retain, and they can then apply this expertise to help a large number of customers improve controls, mitigate risk, and meet strategic objectives.

Key Findings

Forrester's study yielded four key findings:

- **Even mature organizations feel that staffing shortages expose them to high levels of risk.**[4] Forrester's study found that organizations of all levels of maturity, size, and location recognize that they face increased risk exposure due to challenges with filling technical security roles with competent staff. The vast majority (86%) of security leaders believe that concerns relating to managing information risk were directly related to staffing difficulties.

- **Difficulties with sourcing and retaining technical security staff are not short-term issues.** Across the globe, CISOs and governments agree: Security staffing challenges aren't going away.[5] Security organizations will have to deal with technical skill shortages for the foreseeable future. Most (81%) of security leaders believe that staffing challenges will either stay the same or get worse over the next five to 10 years.

- **MSS can minimize issues with the technical skills dilemma.** Security organizations must press on and create suitable options to compensate for an understaffed team. In particular, security leaders have been increasing their levels of technical automation and engaging with MSSPs to source the specialized skills, analytics, and intelligence capabilities they need. Those who currently outsource in this way find it to be an effective approach, with more than two-thirds of security leaders satisfied or very satisfied with their security services — and as high as 83% in some MSS categories.

- **Security organizations should partner with third parties to slingshot ahead of the risk.** Too frequently today, security leaders engage with an MSSP after they have developed and refined internal operational processes. This is no longer the correct approach. Security leaders should engage early with third parties, establish trusted partnerships to enable rapid technical advances, and then optimize processes once the initial implementation is deployed.

Staffing Challenges Expose Firms Of All Sizes To Heightened Levels Of Risk

Chief information officers (CIOs) know that in order to launch new IT initiatives, they have to invest in the necessary technology and expertise to be successful. Unfortunately, it's all too easy to rein in expenses by neglecting similar investments in security, and as a result, security budgets fail to keep up with growing needs. In 2012, for example, security teams around the world saw budget allocation inch up from 7.6% to 8% of the entire IT budget.[6] To tackle the trends of increased internal responsibility and more advanced and malicious external threats, CISOs must rely on the deep technical expertise of their team to understand and secure their diverse IT environment and identify and remediate incidents as quickly as possible. Here's the problem: There aren't enough sound technical staff to fill industry demand.

For this study, Forrester defined three levels of information security maturity:

- **Reactive (14% of respondents).** Security controls and processes tend to be reactive to pressing needs. Although processes may be largely consistent, they are rarely documented and tend to be operator-dependent.
- **Managed (30% of respondents).** Security controls and processes are clearly defined and well documented but tend to be manually operated.
- **Optimized (56% of respondents).** Security controls and processes tend to have broad coverage and are automated and tracked with defined metrics. Key controls are regularly refined to ensure that they align with business requirements.

Forrester's survey highlighted how these shortages leave organizations of all sizes, operating regions, and maturity levels with heightened levels of information risk. Several troubling trends emerged:

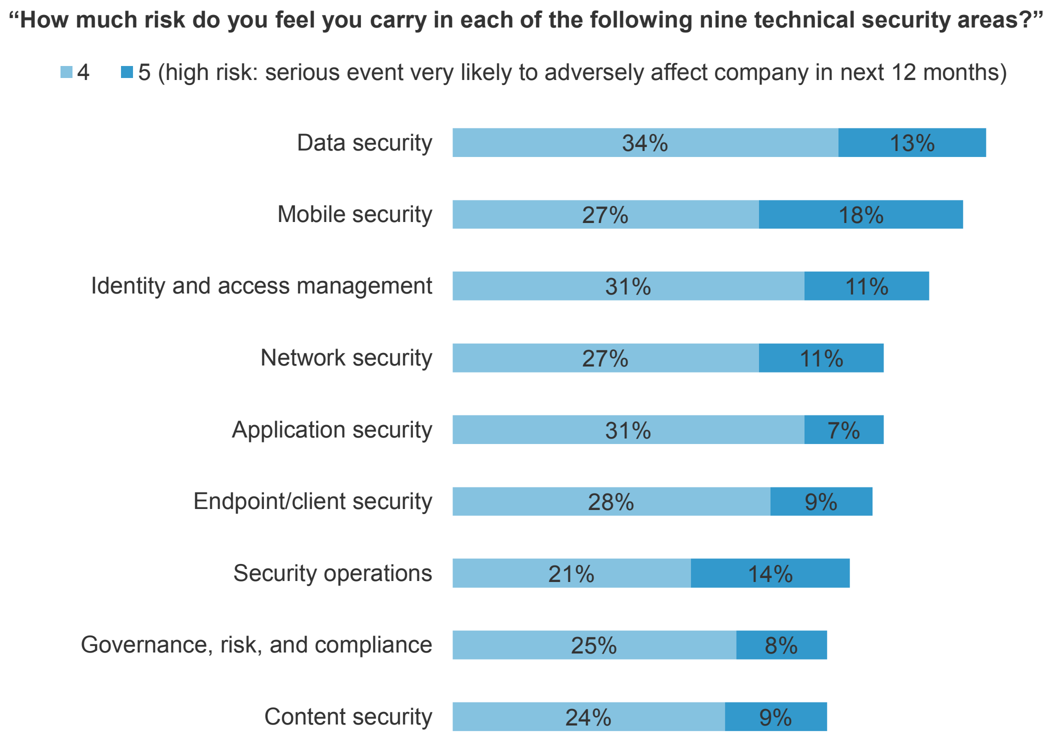
- **Even large mature enterprises carry too much risk.** Regardless of the size or relative maturity of the processes and techniques of the security organization, security leaders remain concerned about the current risk exposure of their companies (see Figure 1). In fact, in some cases, the mature, or optimized, security organizations are even more concerned about their risk exposure than their less mature peers. For example, leaders of optimized security organizations are more likely to believe that they carry higher levels of identity and access management (IAM) risk than those in less mature companies, with 45% indicating IAM as a high or very high risk, compared with 39% of the latter group.

- **Staffing challenges are a main cause of CISO concern.** The vast majority of security leaders (86%) feel that their waning confidence in their organization's ability to manage risk is due to staffing-related issues. Of highest concern are challenges with staff lacking thought leadership (37%) or sufficient experience to manage information security risks effectively (see Figure 2).[7] Optimized organizations are also more than twice as likely to be troubled by an inability to source specialized skills (28%), compared with less mature firms (13%) that may be relying on generalists with a broader set of skills.

- **Security teams fail to discover external threats and meet operational deadlines.** Without the right technical security staff in place, many security teams are unable to keep up with required tasks. Many find themselves unable to identify external threats (27%) and can't meet expected deadlines (27%), and this results in a growing gap between the threats and the implemented controls (24%) (see Figure 3). Make no mistake; the threats are real: In 2012, IBM noted in excess of 45 million malicious attacks across a monitored customer base of more than 3,700 clients, while Forrester noted that one in four organizations (24%) experienced at least one security breach.[8] At this rate, it's an issue of when you will be breached, not if it will happen.
- **US and EMEA staffing challenges are substantial but overshadowed by Latin America.** Organizations globally struggle with a lack of resources and understaffed teams. Around 32% of US organizations and 29% in Europe, the Middle East, and Africa (EMEA) report that more than 10% of their allotted technical security headcount is vacant. Unfortunately, the problem is much worse in Latin America, where a concerning 69% of firms have more than 10% of roles unfilled. To make matters worse, they also have to deal with rapid staff turnover; 52% of security leaders from Latin America noted that rapid staff turnover was a major reason for their lack of confidence in their ability to manage risk, with 79% of firms stating that the average length of service for technical security staff is fewer than 18 months.

Figure 1

Security Organizations Are Exposed To High Levels Of Risk

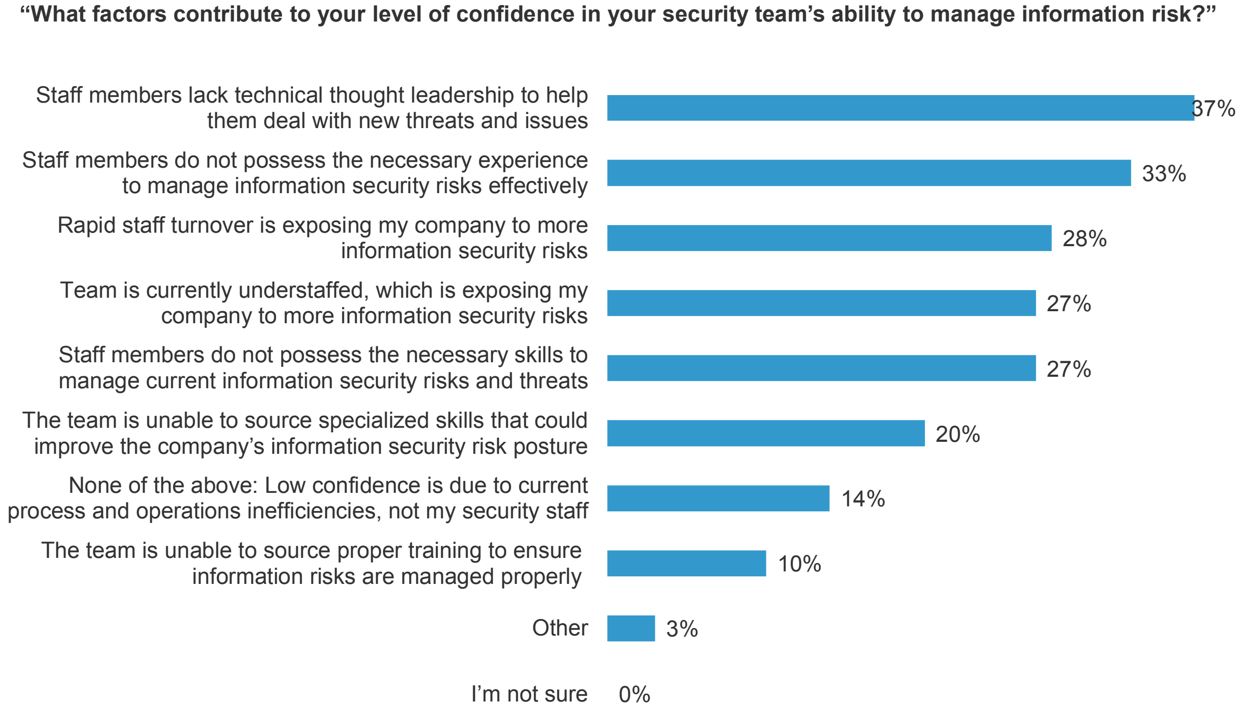


Base: 158 IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

Figure 2

Staffing Issues Raise Significant Concerns

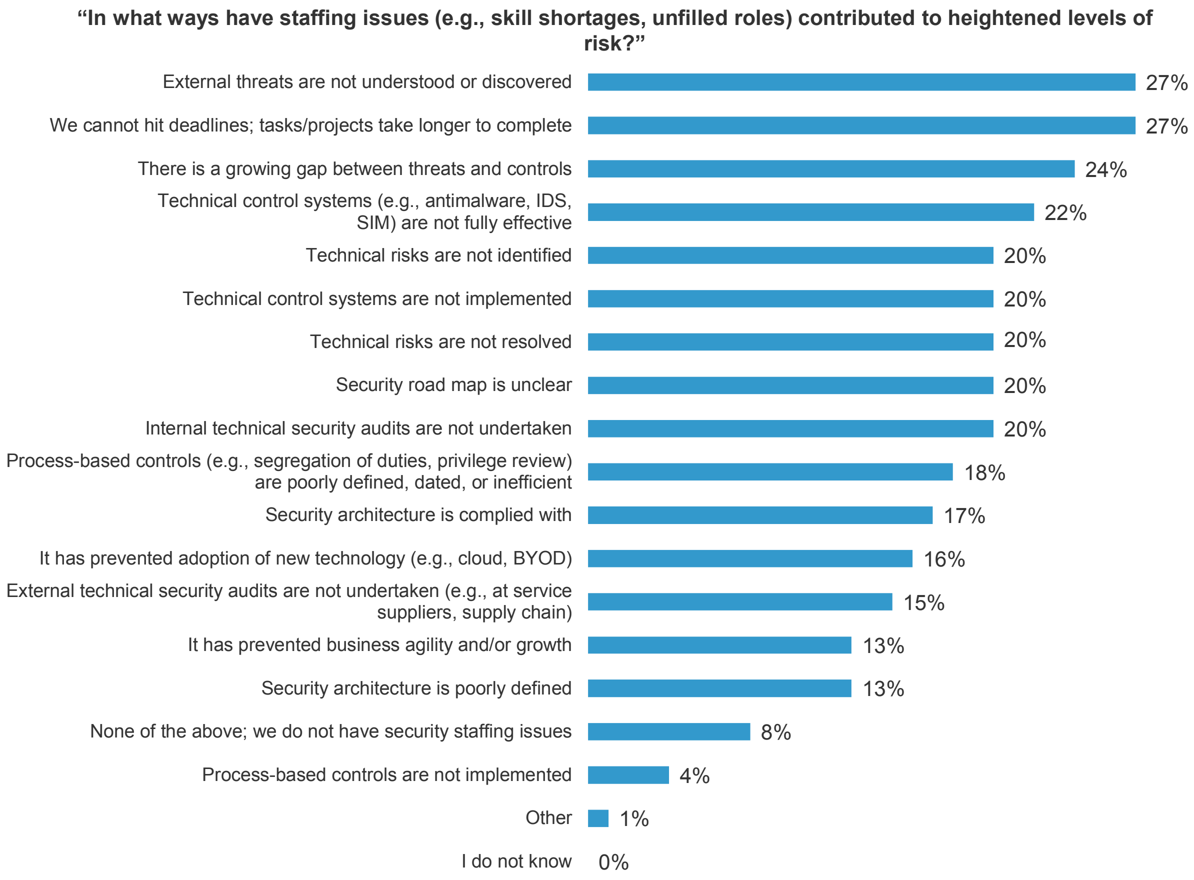


Base: 132 IT security decision-makers with low level of confidence in their security team's ability to manage information risk (multiple responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

Figure 3

Security Organizations Remain Vulnerable Without The Right Security Talent



Base: 158 IT security decision-makers
(multiple responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

Technical Staff Demand Outstrips Supply, And The Situation Won't Improve

An alarming 80% of security leaders believe that it is difficult or very difficult to find and hire technical security staff that fit all of their requirements (see Figure 4). This challenge is even more pervasive in Latin America, where a stunning 96% of regional security leaders noted this difficulty. It's clear that technical staffers are in extremely high demand, and security leaders have to invest substantial time and effort to locate, engage, and retain essential technical security skills just to keep their security organization running efficiently and effectively.

Security leaders are especially concerned with staffing challenges because:

- **The technical skills shortage is an issue of both supply and demand.** It's not only that technical security skills are in high demand but also that the talent pool is decidedly small. Security leaders cited competition with other firms (44%) and poor staff quality (39%) as top issues in recruiting technical staff (see Figure 5). Competition is much less of a concern in Latin America (23%). Instead, the major challenge there is an insufficient number of applicants (38%) and poor quality of staff (40%), which is a problem shared by EMEA (51%).[9] In addition, this technical skills shortage has become more pronounced among staff members with low levels of experience (one year to five years) because CISOs often try to address any shortage by recruiting further down the ladder of experience.

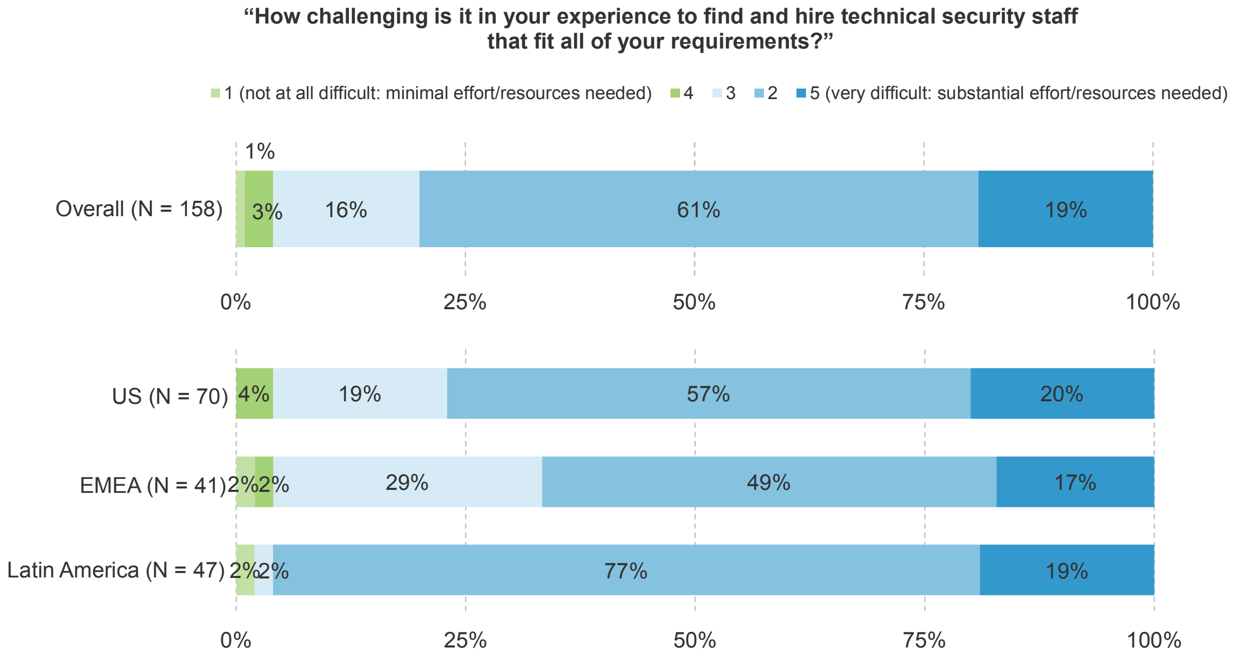
- **Regular turnover and long vacancies force security organizations to run at suboptimal levels.** More than 60% of organizations state that it takes at least four to six months to fill vacancies on technical security teams, and for a minority (12%), it can take closer to a year. Of course, this is just the time it takes to hire the staff; security leaders then need to account for the time to onboard and train the new employees to get them fully ramped up. Considering that only 25% of security leaders say that technical security staff members remain on the team for three or more years, it's easy to see the constant resource strain these teams are under, trapped in a loop of eternally trying to reach full and effective headcount.

- **Deep technical specialists and architects are hardest to find.** Security leaders across all sizes of firms and all regions indicated that the security architect (41%) is the most difficult role to fill, followed by security specialists with deep technical skills in areas such as malware and forensics (35%) (see Figure 6). Security specialists are especially challenging to find in the US (40%) and EMEA (49%), but this seems to be less of a problem for security leaders in Latin America (17%). Network security positions (34%) were tough to source in the US (40%) and EMEA (39%), but again they are not in terribly short supply in Latin America (21%). Not surprisingly, security leaders in each region felt that their region was the most challenging for recruitment and staffing, although everyone recognized the challenges associated with Latin America.

- **Staffing challenges will only get worse, not better.** Unfortunately, there's little good news to report with regard to the skills shortage dilemma. Recruitment specialists in each region spoke of growing demand and insufficient entrants to the market. Statistics in the UK support the assertion that the supply of suitable candidates is deteriorating. As an example, in 2012, only 3% of applications to universities were for computing-related courses, and this is on a downward trend that showed a 6.4% fall in that year alone.[10] Similarly, in mid-2012, the US Office of Personnel Management identified cybersecurity as the No. 1 high-risk skill gap for the federal government.[11] Our survey confirmed these challenges, and unfortunately, the large majority of security leaders (81%) believe that security skill shortages will stay the same or likely get worse.

Figure 4

CISOs Struggle Mightily To Recruit Technical Skills

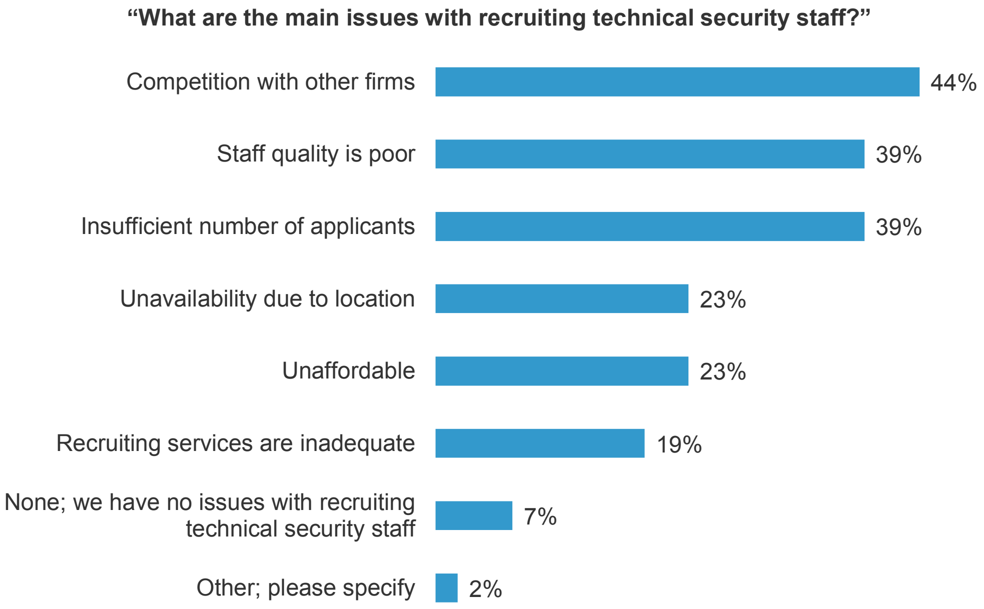


Base: 158 IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

Figure 5

Recruiting Efforts Intensify In A Competitive Market With A Shortage Of Skilled Applicants

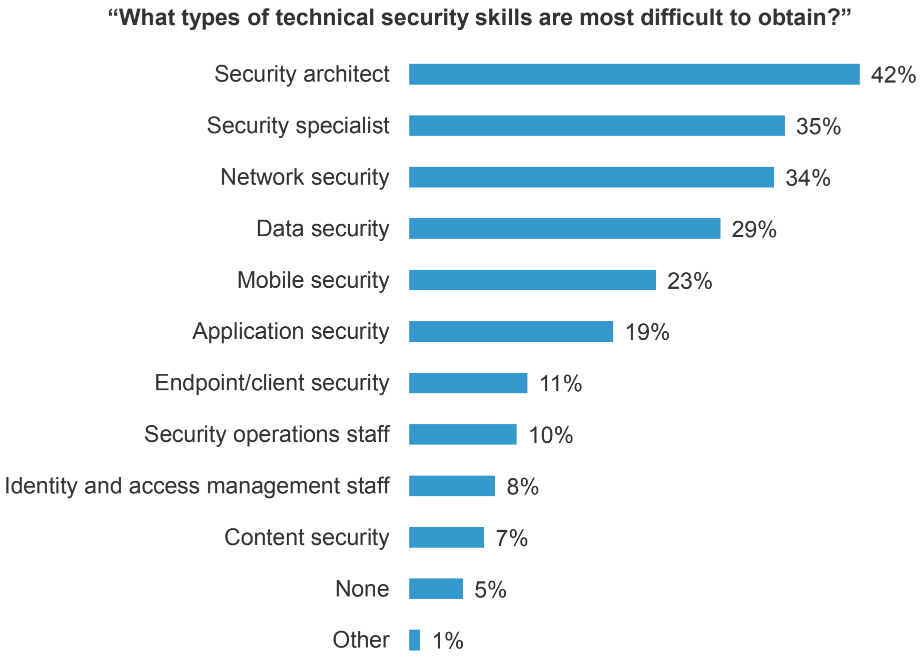


Base: 158 IT security decision-makers
(top three responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

Figure 6

Security Architects, Specialists, And Network Security Skills Are The Hardest To Obtain



Base: 158 IT security decision-makers
(top three responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

Consider MSSPs To Address Staffing Concerns And Enable Rapid Capability Leaps

In spite of the fact that staffing issues will continue to be an issue for security organizations in the immediate and medium term, most organizations are not standing idly by. They are finding new ways to obtain the required skills and abilities by engaging MSS for a host of strategic and operational security tasks as well as for more advanced technical capabilities such as threat intelligence and advanced malware protection. In fact, organizations that are higher on the maturity curve are more likely to have plans in place to implement or expand their existing implementation of MSS (see Figure 7). A number of factors are driving this trend:

Forrester identified three habits of organizations that have reached the highest level of maturity, known as "optimized":

1. Optimized security organizations are much more likely to be planning to expand utilization of MSS than firms of lesser maturity.
2. Optimized security organizations utilize strategic plans, such as security architecture and road maps, to drive performance and ensure business alignment.
3. Optimized security organizations utilize metrics to measure performance and refine controls.

- **MSS reduces in-house staffing requirements while maintaining operational effectiveness.** With constant staffing strains on security organizations today, MSSPs are able to offer levels of competency that are comparable to, or surpass, internal resources, while leveraging economies of scale. MSS can bring many benefits, allowing CISOs to circumvent difficult staffing challenges. Specifically, across all security services, nearly one in three (31%) security leaders cited the ability to reduce the number of technical security staff members as a result of MSS adoption. Alternatively, they were able to employ staff with lower skill levels (27%) and reduce budget spent on security operations (32%) (see Figure 8). Many organizations, especially the immature ("reactive") ones that continue to fire-fight issues, found that utilizing an MSSP freed up vital internal resources, enabling them to spend time focusing on meeting business demands for new technology and innovation.

- **Organizations build solutions in-house first — but this approach is unsustainable.** Security organizations have an understandable tendency to build systems or processes in-house before transferring that operation to an MSSP. Intrusion detection and prevention capabilities (IDS/IPS) were most prone to be internally created and refined before being outsourced (83%). At the other end of the spectrum, security information management (SIM) and log management were least likely to be built internally, although more than two-thirds still were (68%).

- **The traditional method of "build, document, refine, then outsource" is inefficient, consuming valuable resources.** Few CISOs today ever get to a breakeven point where they have full staffing, and this leaves them without the skilled resources to build and perfect an internal solution. Indeed, developing a security solution in-house first can take time and money, draining already stretched budgets and enabling the attackers to move further in front. It's time for a new model: Consider skipping the difficult, time-consuming steps and engaging with MSSPs for strategic security assessments and key services from the outset. By outsourcing the heavy lifting, organizations can benefit from the experience, technology, and staffing of the MSSP, freeing up internal resources to work on higher-profile tasks that add to your firm's agility and fulfill the staff you hope to retain.

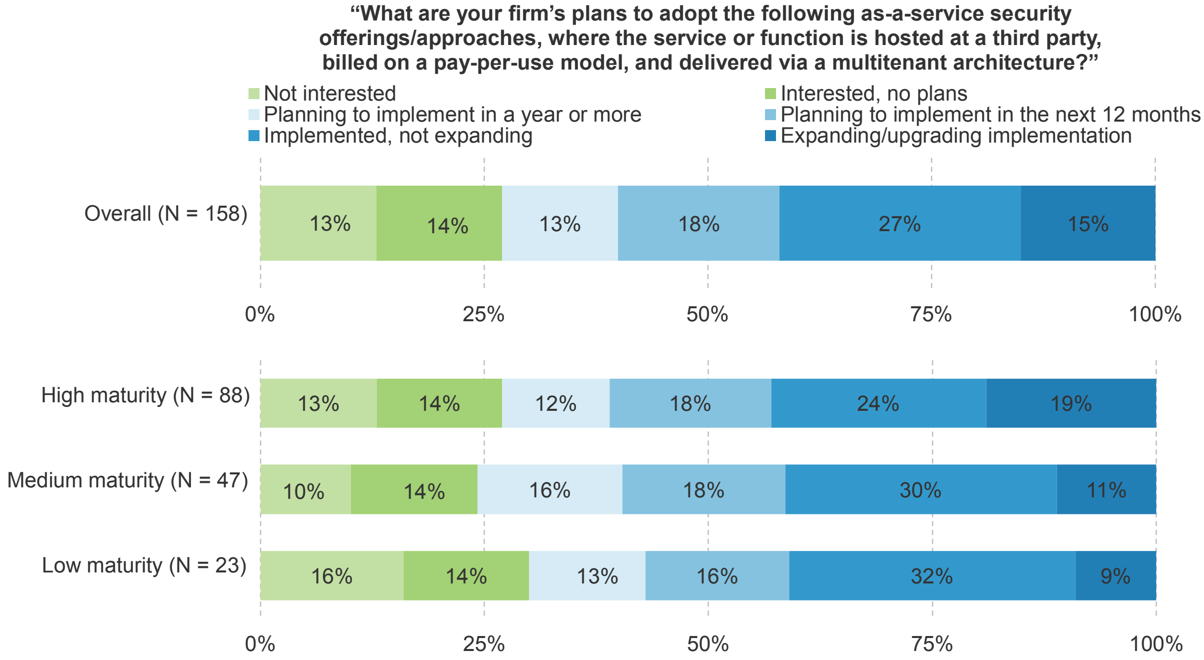
> "It's time for a new model: consider skipping the difficult, time-consuming steps and engaging with MSSPs for strategic security assessments and key services from the outset."

- **Current satisfaction levels with MSSPs are extremely high.** Across the various MSS solutions, 90% of CISOs stated that the skill set was as good as, or better than, internal resources (see Figure 9). Security leaders who continue to remain tentative about the prospect of handing over any part of their security operations should take note; organizations that capitalize on the potential value of MSSPs can refocus their attention on greater, more strategic initiatives within their own organization.

- **Reliance on MSSPs and other third parties will grow, and that's OK.** Security leaders understand that technical security skills shortages are here to stay and believe that, in order to cope with this reality, their reliance on third parties will grow substantially over the next five to 10 years. Less than one in three security leaders (30%) believe that the future of technical security programs will consist of entirely in-house teams with no reliance on third parties. For many years, security leaders have had to do more with less, and now 50% of them believe that this means that they'll become more reliant on third parties for skills and consulting services in the future.

Figure 7

Enterprises At All Maturity Levels Are Turning To MSSPs

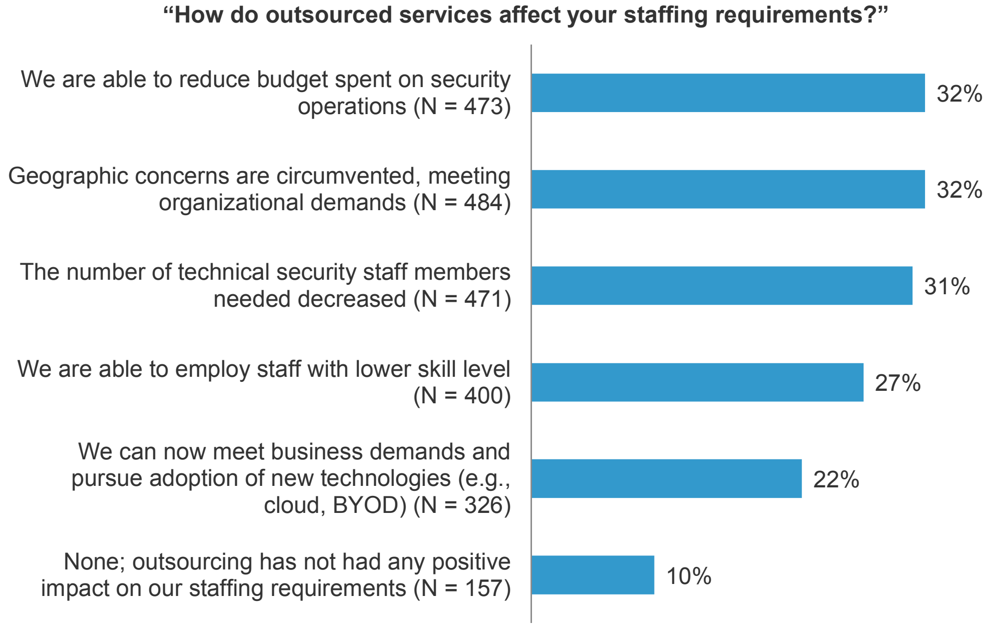


Base: 158 IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

Figure 8

MSSPs Address Security Challenges And Free Resources For Innovation

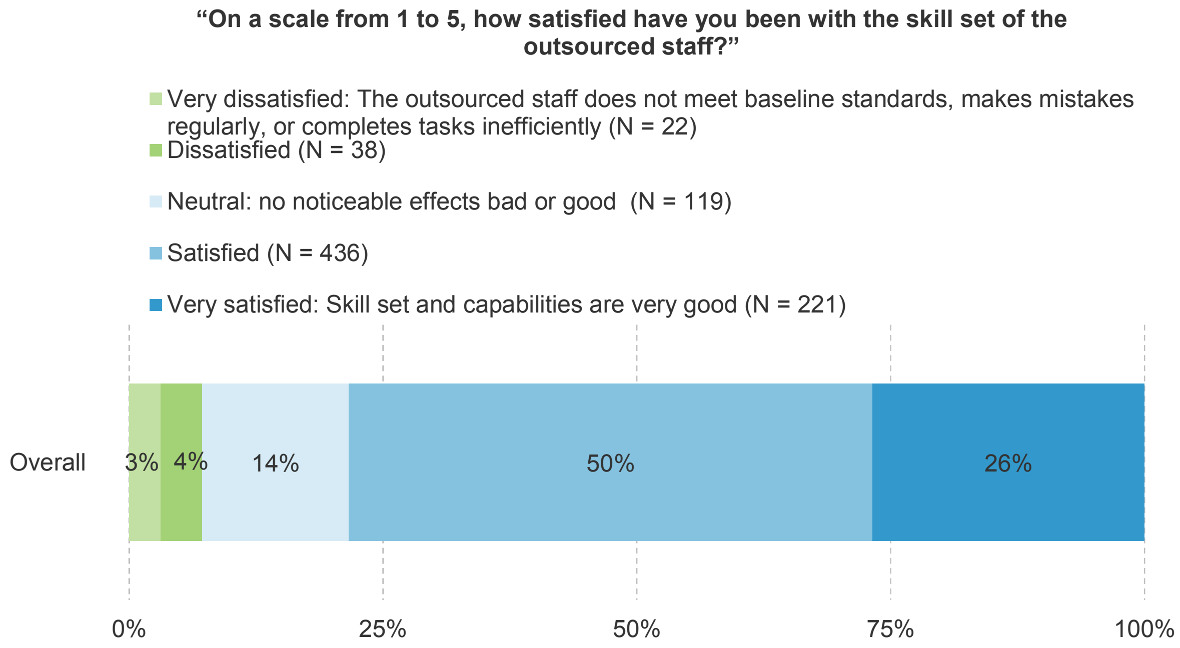


Base: 158 IT security decision-makers
(multiple responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

Figure 9

Security Leaders Are Extremely Satisfied With The Skills Of Their Outsourcers



Base: 158 IT security decision-makers

(percentages do not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

KEY RECOMMENDATIONS

For too long, security leaders have been sacrificing their top talent to backfill on operational tasks caused by staff vacancies or skill shortages. While this practice may patch the day-to-day holes in the system, it's preventing information security from supporting new business initiatives, and it's allowing threats to move further beyond our capability to protect. Security leaders must look for new approaches to leverage all available skills and resources. Forrester's in-depth study uncovered several ways to address these challenges:

- **Prepare for a future where technical skills are in even higher demand than today.** Technical security skill shortages aren't going away, regardless of the location, maturity, or size of your organization. Security leaders need to prepare their organization for this new reality and identify ways to improve their current IT services. This means maximizing existing resources in an environment where the pressure continues to ramp up on every side — new threats, new regulations, cost restrictions, quality-of-service issues, and rapidly changing business demands.

- **Give experienced employees more important projects to increase their value and sense of contribution.** Skilled and experienced technical staff are hard to find and harder to retain. Make sure that your top talent is focused on projects that benefit your organization and engage their interests and ambition, rather than reinforce operational mundanity. If you don't ensure that your staff members are both stretched and fulfilled, you can be sure that your competition will.

- **Slingshot forward with an MSSP, and then refine and optimize processes as a partnership.** Although the CIO may be uncomfortable with the concept, security leaders currently face the dilemma of only being able to address two of three essential tasks: 1) manage costs; 2) keep up with threats; and 3) build and refine solutions internally. Early MSSP adopters provide very positive feedback about the multiple benefits of outsourcing operational tasks, and an established MSSP partnership will mean that processes can be refined and optimized as the relationship continues.

- **Embrace third parties, but set clear expectations and defined service-level agreements (SLAs).** The future is clear; third parties and MSSPs will likely be an integral part of many enterprises' security solution. Security leaders need to embrace this new model and seek out trustworthy long-term partners. Work to formalize acceptable parameters for the service, such as service levels and response times, and insist that the provider engages internal talent to enable bidirectional skill and knowledge transfer.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 158 security organizations in Brazil, France, Germany, Mexico, the UK, and the US to evaluate the difficulties CISOs currently face and to better understand how to handle staff deficiency challenges. Survey participants included security decision-makers at firms with 3,000-plus employees. Questions provided to the participants asked about challenges in recruiting and staffing, the maturity and risk of the organization, and current and future approaches to resolve challenges. Respondents were offered an electronic gift card as a thank you for time spent on the survey. The study began in January 2013 and was completed in February 2013.

Appendix B: Supplemental Material

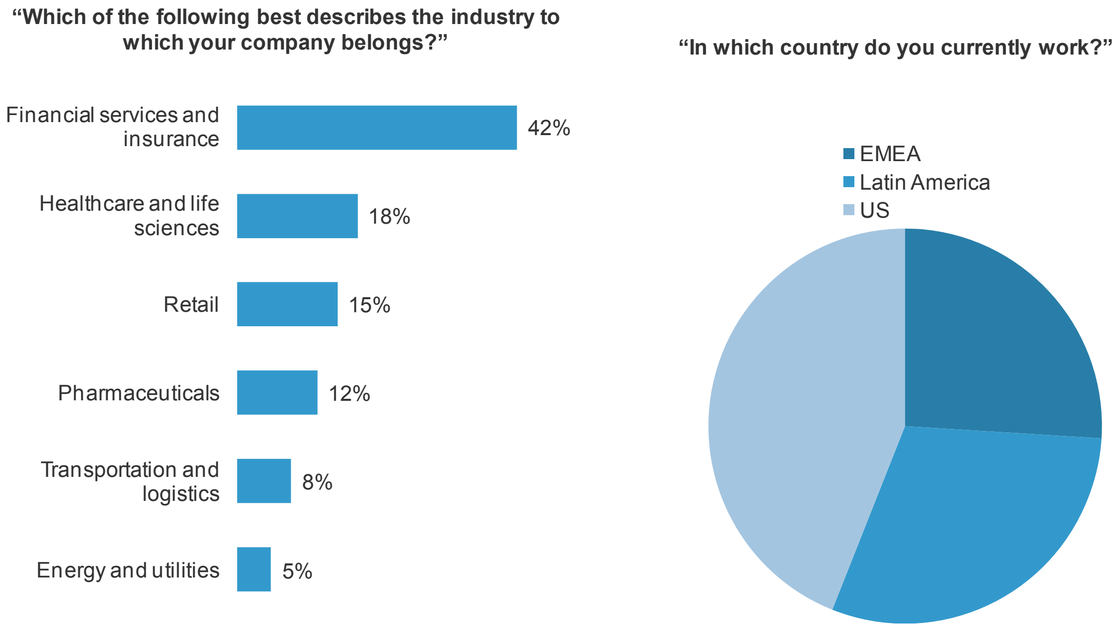
Related Forrester Research

"Defining The Online Marketing Suite," Forrester Research, Inc., October 17, 2007

Appendix C: Demographics/Data

Figure 10

Region And Industry

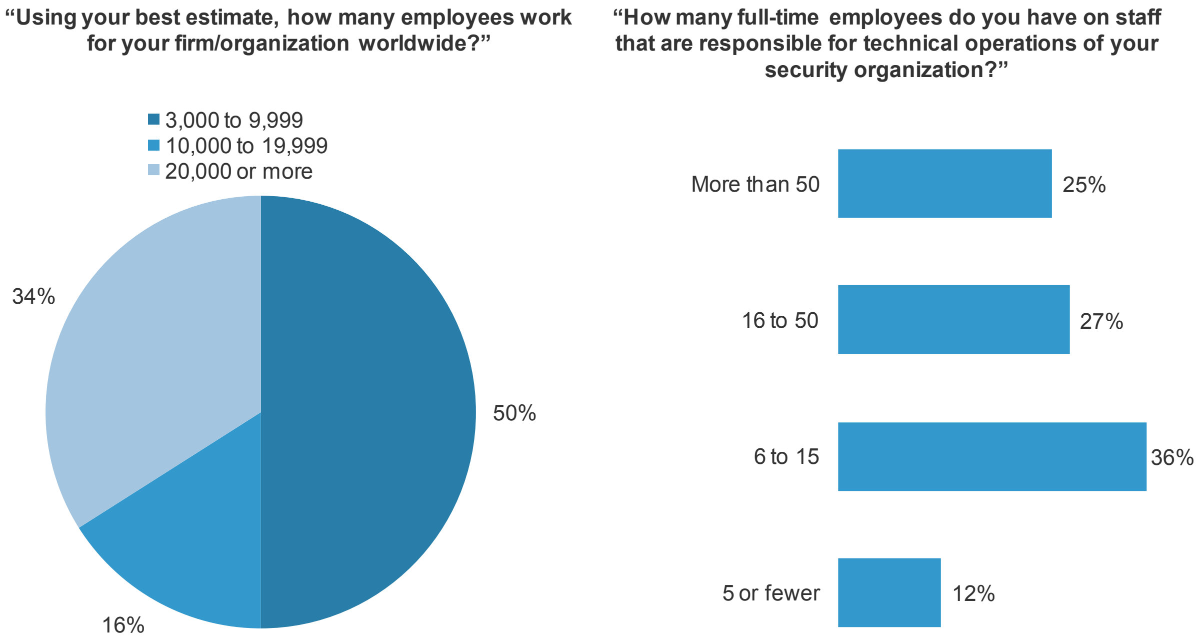


Base: 158 IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

Figure 11

Company Size



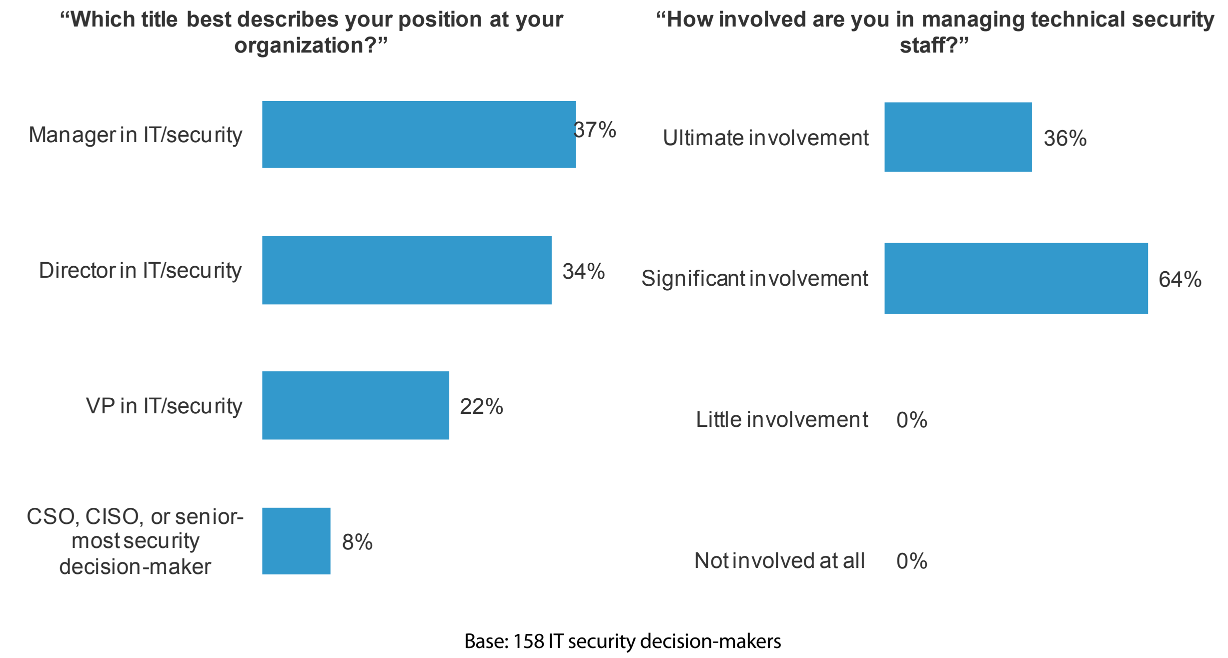
"Using your best estimate, how many employees work for your firm/organization worldwide?"

"How many full-time employees do you have on staff that are responsible for technical operations of your security organization?"

Base: 158 IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

Figure 12
Respondent Profile: CISOs And Other Security Leaders



Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, February 2013

Appendix D: Endnotes

[1] Source: IBM Security Services Cyber Security Intelligence Index, IBM, April 2013.

[2] Source: "2011 Cost Of Data Breach Study," Ponemon Institute, March 2012 (http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf).

[3] Please refer to Appendix C for further demographic data.

[4] For this study, Forrester defined three levels of maturity. The first is reactive. At this level, security controls and processes tend to be reactive to pressing needs. Although processes may be largely consistent, they are rarely documented and tend to be operator-dependent. The second is managed. At this level, security controls and processes are clearly defined and well documented but tend to be manually operated. The third is optimized. At this level, security controls and processes tend to have broad coverage and are automated and tracked with defined metrics. Key controls are regularly refined to ensure that they align with business requirements.

[5] The UK's National Audit Office estimated that it could take "up to 20 years to address the skills gap." Source: "National Audit Office Warns UK Needs More Skilled Cyber-Crime Fighters," BBC News, February 12, 2013 (http://www.bbc.co.uk/news/uk-politics-21414831).

[6] Forrester published a review of information security spending across 2012 and found that budget allocation had risen for the third year running, with 8% of the IT budget now being spent on security. Source: "Understand Security And Risk Budgeting For 2013," Forrester Research, Inc., January 10, 2013.

[7] When considering information security skills, technical thought leadership refers to the ability of the staff member to act independently, demonstrate innovation and influence, and bring fresh perspective and leadership with regard to technology challenges.

[8] Source: IBM Security Services Cyber Security Intelligence Index, IBM, April 2013; Forrsights Security Survey, Q2 2012.

[9] The definition of poor staff quality is a judgment call by the respondents based on factors such as lack of qualifications, poor references, inadequate experience, or existing skills not being aligned with the vacancy.

[10] Source: "Data Reported For Applications Considered On Time For 15 January Deadline," UCAS press release, January 30, 2012 (http://www.ucas.com/about_us/media_enquiries/media_releases/2012/20120130).

[11] Source: Tim Wilson, "Federal Officials Say Cybersecurity Is Greatest High-Risk Skill Gap," Dark Reading, June 2, 2012 (http://www.darkreading.com/security/news/240001380/federal-officials-say-cybersecurity-is-greatest-high-risk-skill-gap.html).