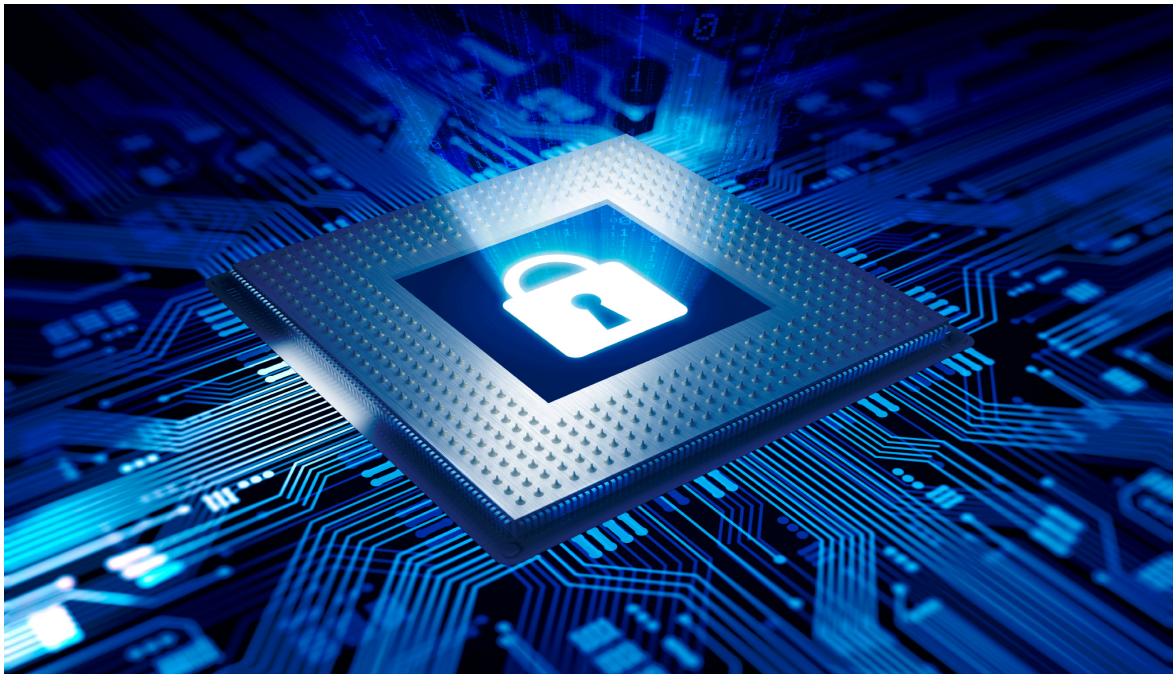
Ponemon INSTITUTE



# Security Metrics to Manage Change: Which Matter, Which Can Be Measured?

## Sponsored by FireMon

Independently conducted by Ponemon Institute LLC

Publication Date: April 2014

**Security Metrics to Manage Change:**
**Which Matter, Which Can Be Measured?**
Presented by Ponemon Institute, April 2014

## Part 1. Introduction

Ponemon Institute is pleased to present the findings of *Security Metrics to Manage Change: Which Matter, Which Can Be Measured?* sponsored by FireMon. The purpose of this research is to understand how organizations respond to changes in the security risk landscape and how metrics can help drive more effective and informed decisions. The benefits of more effective metrics can be greater reliability, resiliency and efficiencies of security defenses.

According to the findings, there is overwhelming agreement that metrics are critical to achieving an effective security change management process. Further, real-time analysis is essential or important to understanding new and emerging security risks. However, such metrics and analysis seem to be lacking in most organizations.

**What is security change management?**

In this study, we define security change management as a formal approach to assessing, prioritizing and managing transitions in personnel, technologies, policies and organizational structures to achieve a desired state of IT security.

The security risk landscape is defined as rapidly mutating threats at every point of entry from the perimeter to the desktop; from mobile to the cloud. The fast evolution of the threat landscape and changes in network and security architectures creates a challenging and complex security ecosystem.

What may affect the availability of resources necessary to build a strong security posture is the lack of communication between the C-suite and those in IT security. According to the findings, rarely does the IT security practitioner regularly meet with leadership about security issues. As a result, many senior executives do not have an accurate or complete picture of how successful (or unsuccessful) the IT security function is in protecting the organization and its data. In fact, security practitioners say the CEO and board have far more confidence in the security posture of the organization than they have.

The study surveyed 597 individuals who work in IT, IT security, compliance, risk management and other related fields. All respondents are involved in IT security management activities in their organizations. They also are involved in assessing or managing the impact of change on their organization's IT security operations. The following are the themes of this study:

- A tale of two security departments
- The importance of metrics to driving more informed decisions
- Practices to achieve effective security change management
- The right metrics for managing change

Some of the most salient findings include the following:

**The security posture perception gap puts organizations at risk.** Only 13 percent of respondents would rate the security posture as very strong whereas 33 percent of respondents say their CEO and Board believes the organization has a very strong security posture. Such a gap reveals the problems the security function acknowledges in accurately communicating the organization's true state of security.

**Why can't communication be better?** Seventy-one percent of respondents say communication occurs at too low a level or only when a security incident has already occurred (63 percent of respondents). The majority of respondents (51 percent) admit to filtering negative facts before talking to senior executives.

**Agility is key to managing change.** When asked to rate their organization's agility in managing the impact of change on IT security operations, only 16 percent of respondents say their organizations have a very high level of agility and 25 percent say it is very low.

**Metrics that reveal the impact of change are most valuable**. According to 74 percent of respondents, security metrics that measure the impact of disruptive technologies on security posture are important. However, 62 percent of respondents say metrics fail to provide this important information.

**Real time analysis for managing change is essential**. When asked about the importance of real time analysis for managing changes to the organization's security landscape, 72 percent of respondents say it is essential or very important. Only 12 percent say it is not important.

**Organizations are not using more advanced procedures to understand the impact of change on their organization's security posture.** Twenty-six percent of respondents say they are using manual processes or no proactive processes to identify the impact of changes on the organization's security posture. Only 15 percent are using automated risk impact assessments, 13 percent say they are using continuous compliance monitoring and 11 percent rely on internal or external audits.

## Part 2. Key Findings

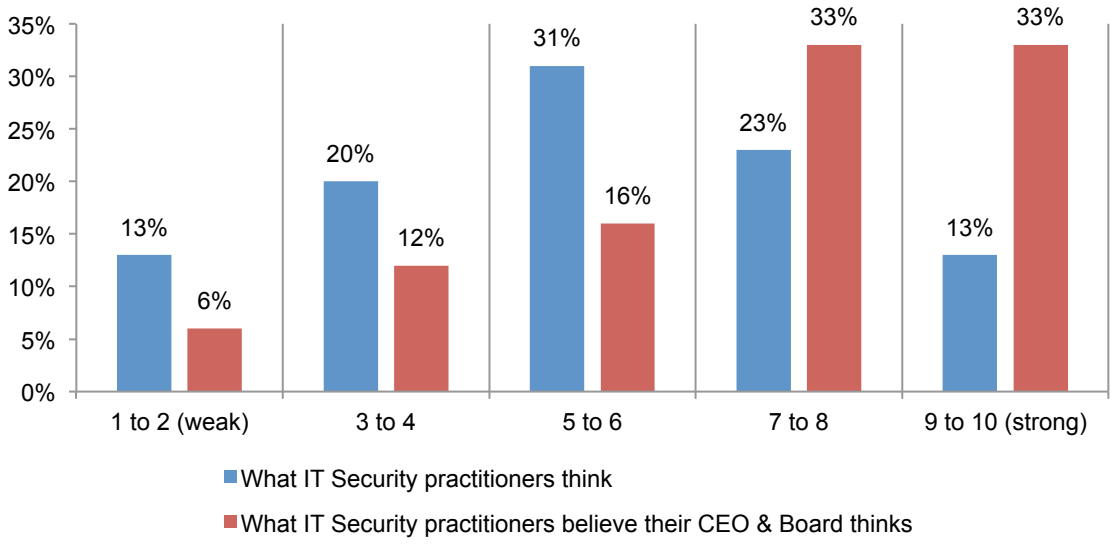
### A tale of two security departments

**Senior executives are believed to have a more positive outlook on the effectiveness of their IT security function.** While respondents rate their organization's security posture as just about average, they believe their CEOs and board members have a much more positive perception, and would rate their organization's security posture as above average.

In fact, only 13 percent of respondents would rate the security posture as strong whereas 33 percent of respondents say their CEO and Board believe their organization has a very strong security posture, as shown in Figure 1. This perception gap signals that security practitioners are not given an opportunity and/or cannot communicate effectively the true state of security in the organization. As a result it is difficult to convince senior management of the need to invest in the right people, processes and technologies to manage security threats.

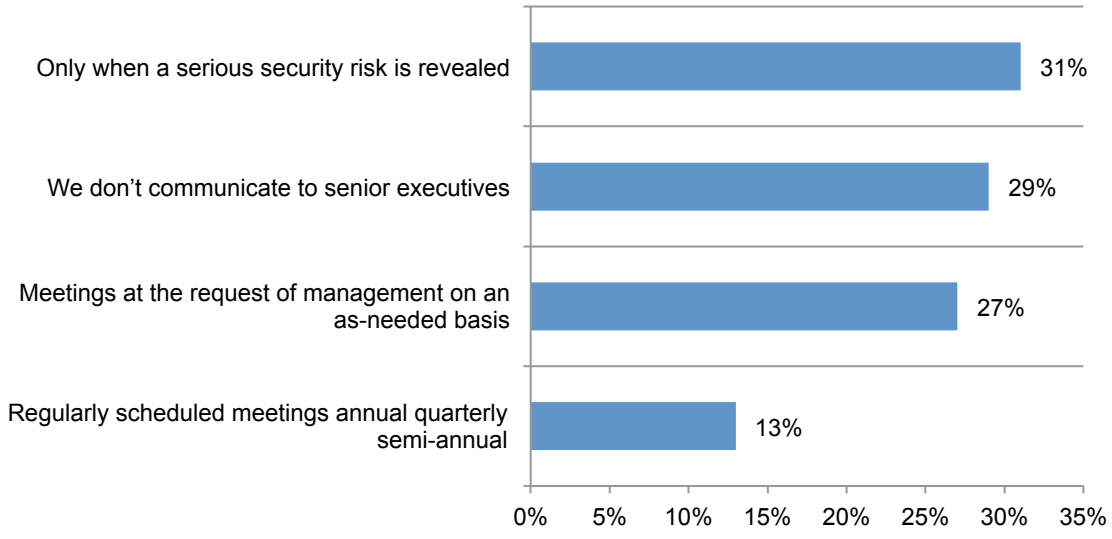
Likewise, respondents believe key stakeholders also consider the organization's security posture as being above average. Twenty-six percent of respondents say this group rates their organization's security posture as very strong. These include business partners, vendors, regulators and competitors.

**Figure 1. How strong is your organization's security posture?**
1 = weak and 10 = strong



**Lack of communication seems to be at the root of the C-suite and IT security disconnect.** Too little and too late characterizes communication to senior executives about the state of security risk. As shown in Figure 2, 29 percent of respondents say they do not communicate to senior executives about risks and 31 percent say such communication only occurs when a serious security risk is revealed. As a result, they admit the state of communication about security risks is not effective. Only 6 percent of respondents say they are highly effective in communicating all relevant facts to management.

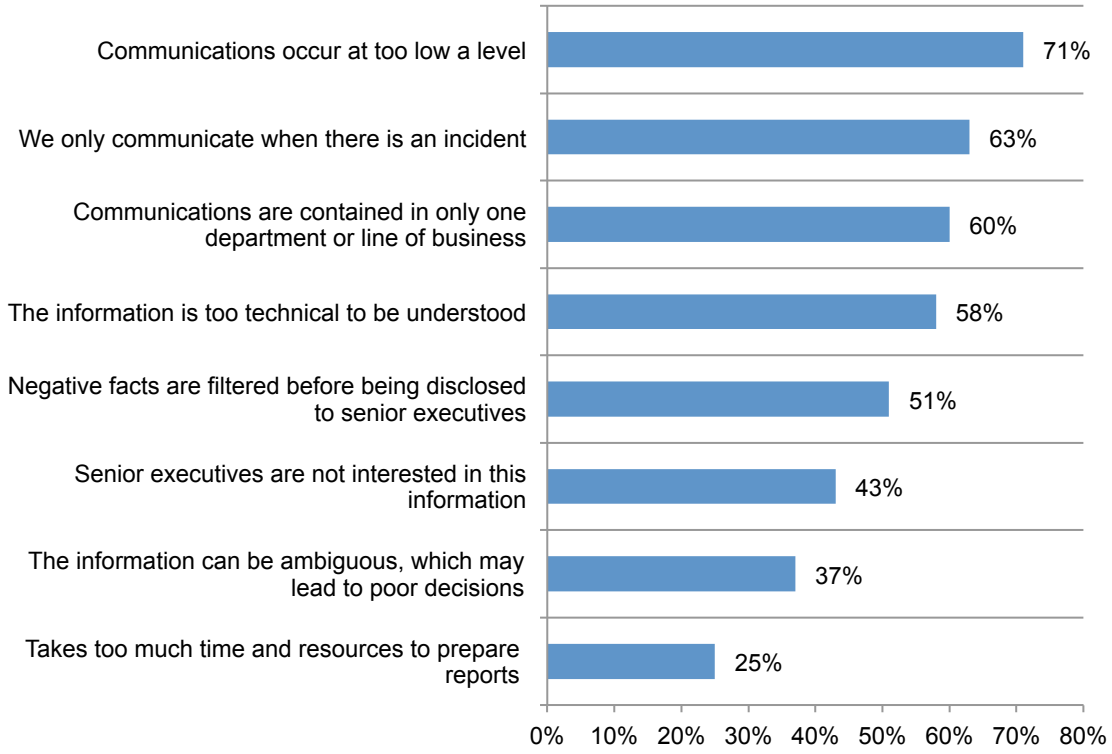
**Figure 2. When do IT security practitioners meet with senior executives?**



**Why can't communication be better?** As revealed in Figure 3, the main complaints are that communication occurs at too low a level or when a security incident has already occurred. Other problems stem from the existence of silos that keep information from being communicated throughout the organization.

Respondents also recognize that the technical nature of the information could be frustrating for senior executives. Very often, the whole story is not revealed because negative facts are filtered before being disclosed to senior executives and the CEO.

**Figure 3. What's wrong with communication?**
More than one response permitted

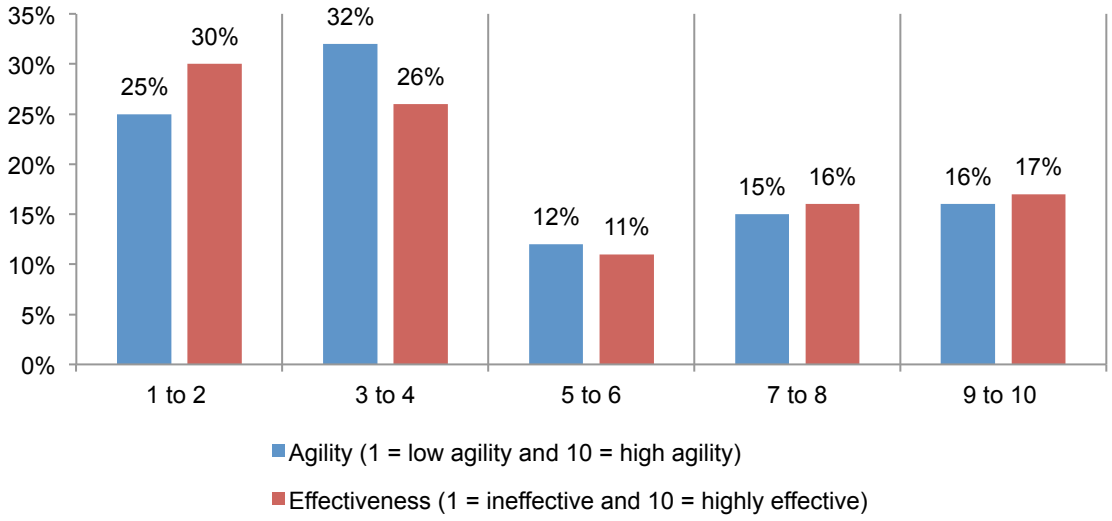


**What are the implications of senior executives and IT security not having the same understanding of the organization's security effectiveness?** According to the findings, an important capability such as having the agility to manage the impact of change on IT security operations could be affected by not being able to convince management of the need for enough resources, budget and technologies.

When asked to rate their organization's overall agility in managing the impact of change on IT security operations, respondents say they are overall fairly low. As revealed in Figure 4, only 16 percent of respondents say their organizations have a very high level of agility and 25 percent say it is very low.

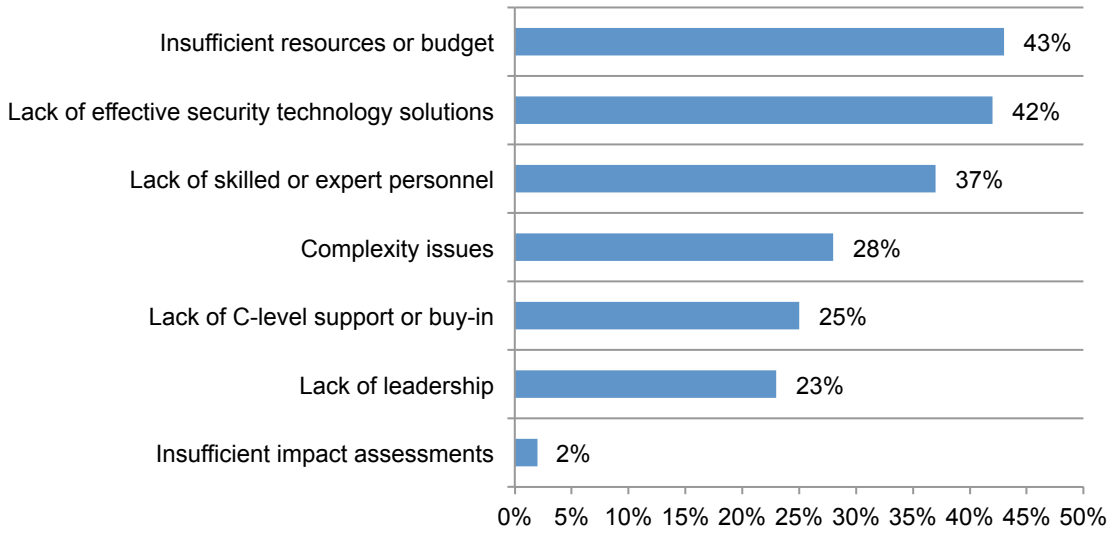
This is also the case when asked to rate their organization's effectiveness in managing the impact of change on IT security operations. Only 17 percent say their organizations are very effective and 30 percent say their organizations are very ineffective (Figure 4).

**Figure 4. Agility and effectiveness in managing the impact of change on IT security operations**



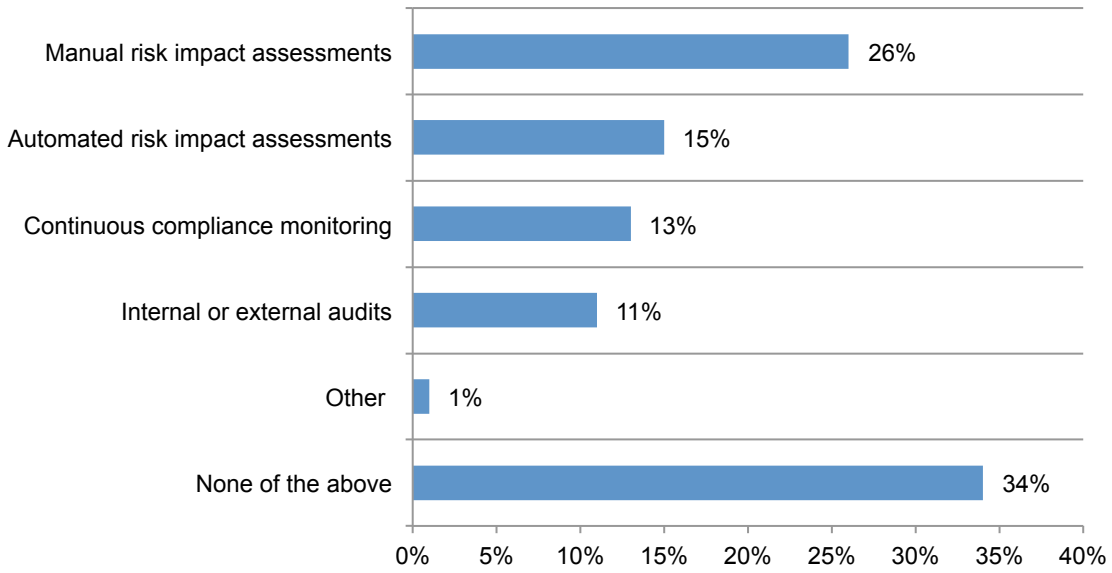
The top three barriers to achieving effective security change management activities are insufficient resources or budget, lack of effective security technology solutions and lack of skilled or expert personnel (43 percent, 42 percent and 37 percent, respectively), as shown in Figure 5. When asked about the importance of real time analysis for managing changes to the organization's security landscape, 72 percent of respondents say it is essential or very important. Only 12 percent say it is not important.

**Figure 5. Significant barriers to managing IT security changes effectively**
Two choices permitted




As shown in Figure 6, 26 percent of respondents say they are using manual processes or no proactive processes to identify the impact of changes on the organization's security posture. Only 15 percent are using automated risk impact assessments, 13 percent say they are using continuous compliance monitoring and 11 percent rely on internal or external audits.

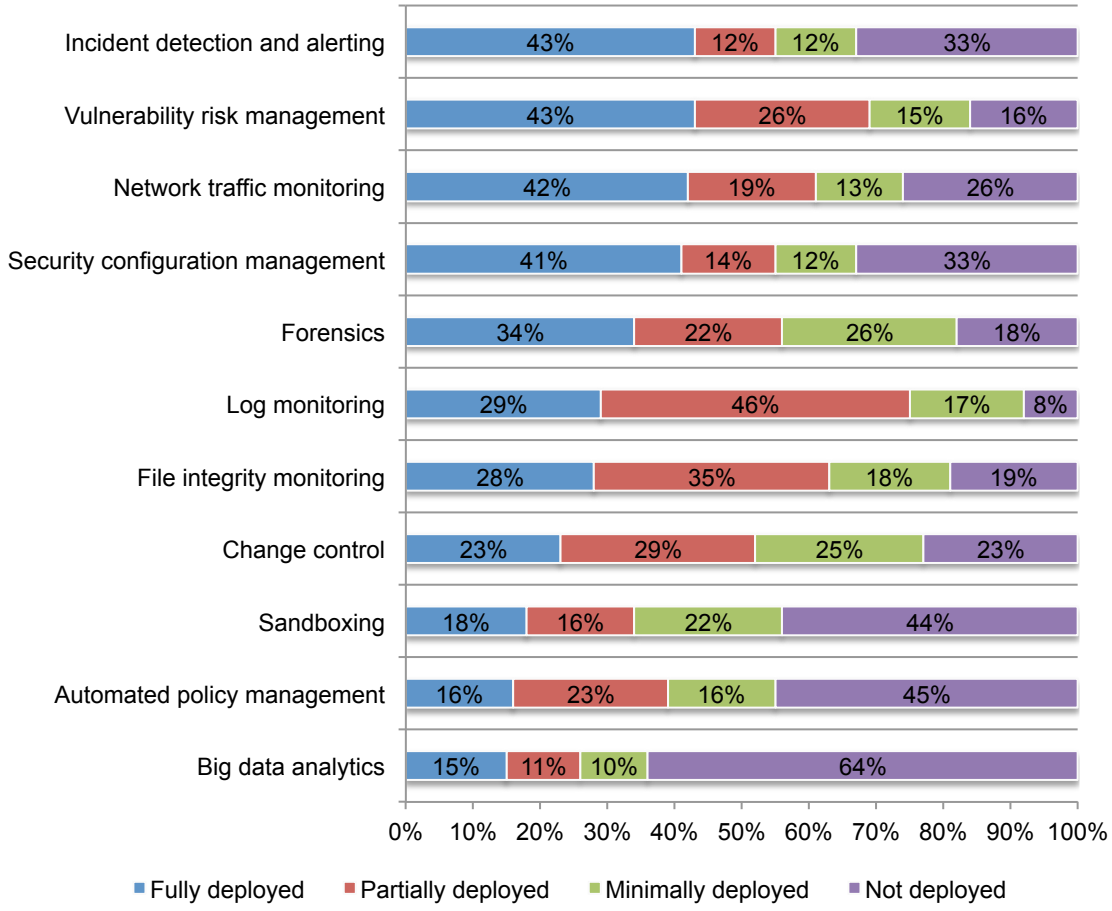
**Figure 6. How organizations identify the impact of changes on IT security posture**
More than one response permitted



Those technologies most often fully deployed to facilitate the management of changes that impact an organization's security risk profile are: incident detection and alerting (including SIEM) and vulnerability risk management, both 43 percent of respondents. Network traffic monitoring and security configuration management follow at (42 percent of respondents and 41 percent of respondents), as shown in Figure 7.

Technologies that are often partially deployed are log monitoring (46 percent of respondents) and file integrity monitoring (35 percent of respondents). Minimally or not deployed at all are: big data analytics (64 percent of respondents), automated policy management (45 percent of respondents) and sandboxing (44 percent of respondents).

**Figure 7. Technologies that facilitate the management of changes**



**The importance of metrics to driving more informed decisions**

**Current metrics in use do not communicate the true state of security efforts.** When asked if the metrics used adequately convey the true state of security efforts deployed by their organization**,** 43 percent of respondents say they do not and 11 percent are unsure.

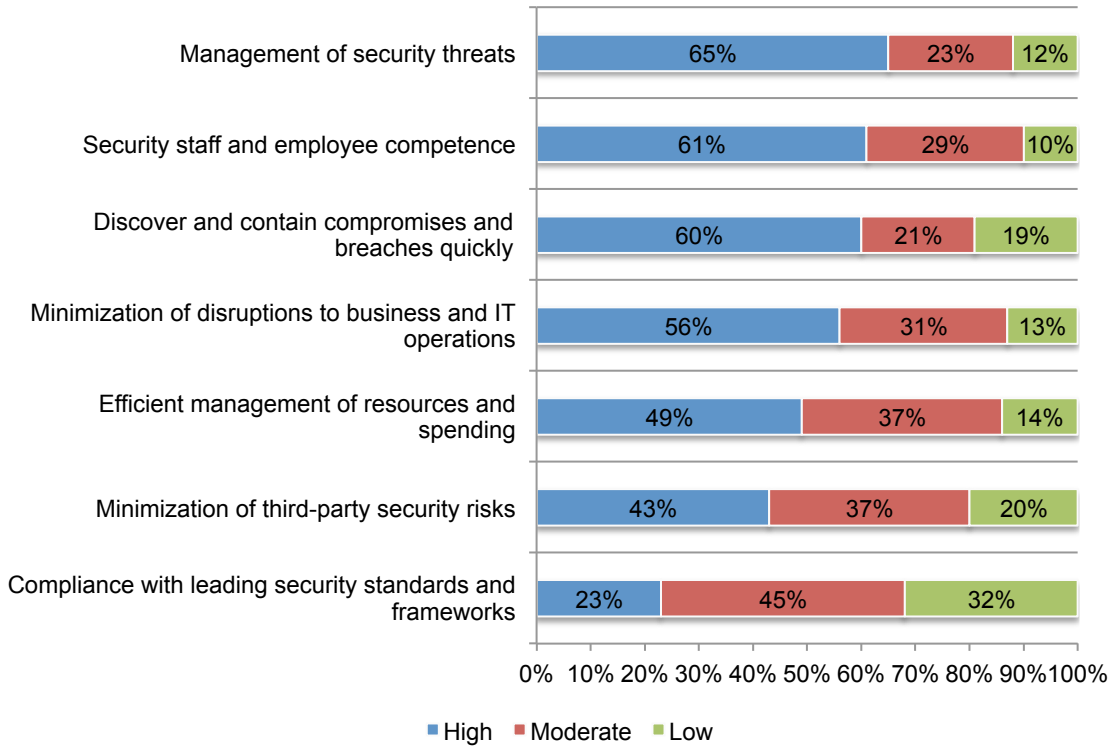
According to Figure 8, the biggest reasons for the failure to accurately measure the state of security are more pressing issues take precedence, communication with management only occurs when there is an actual incident, the information is too technical to be understood by non-technical management and a lack of resources to develop or refine metrics.

**Figure 8. Reasons for not using metrics that convey the true state of security**
More than one response permitted

**Do organizations really understand the strengths and weaknesses of the security function?** Based on the findings that most respondents do not believe current metrics convey the true state of their organization's security efforts, how can they accurately assess its strengths and weaknesses?

However, when asked about their strengths and weaknesses, Figure 9 reveals that most respondents say their organizations are best at managing security threats, hiring and retaining competent security staff and employees and discovering and containing compromises and breaches quickly. They are not as effective at achieving compliance with leading security standards and frameworks and minimizing third-party security risks.

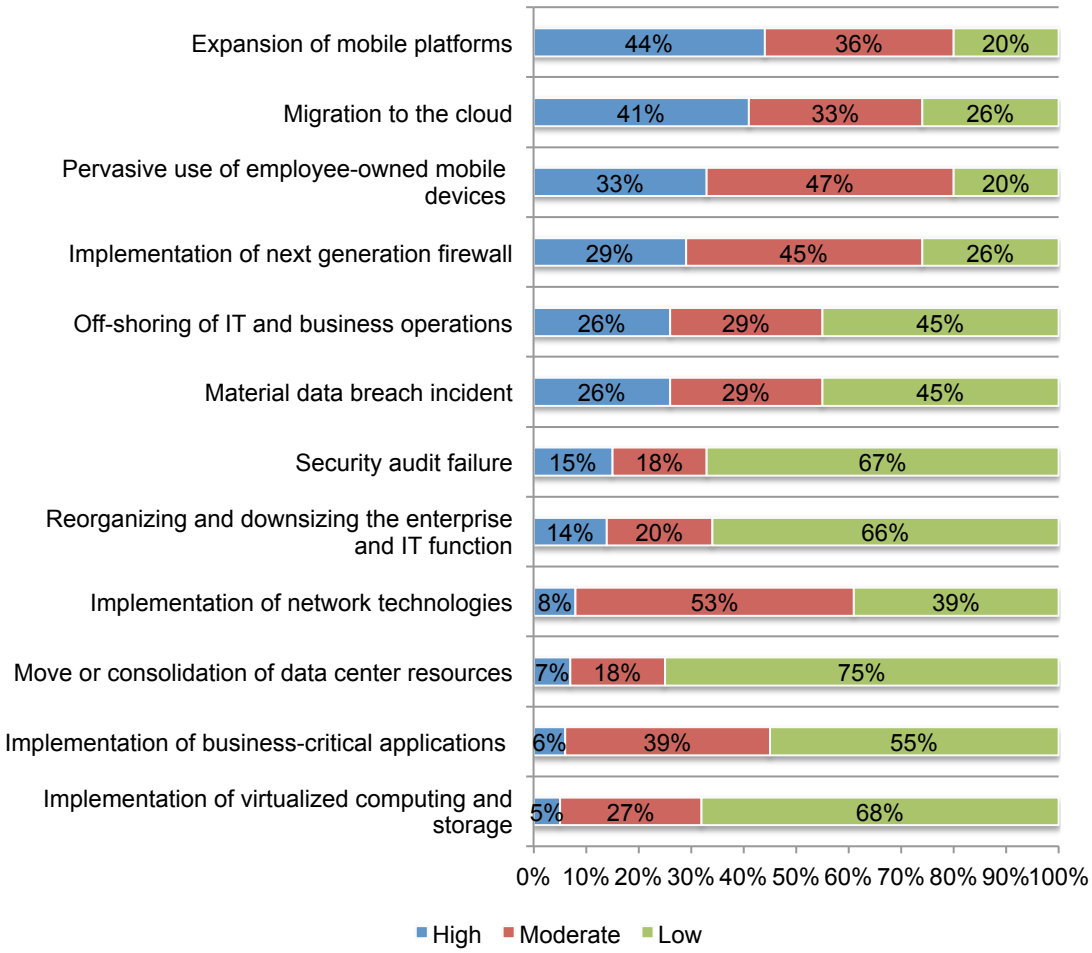
**Figure 9. The strengths and weaknesses of IT security**



**What events are most likely to disrupt the organization's infrastructure and ability to manage security threats?** As shown in Figure 10, expansion of mobile platforms and migration to the cloud are the most likely to affect the security posture. Use of employee-owned devices (BYOD) and the implementation of a next generation firewall have moderate impact. Events that are considered to have a low impact are the move or consolidation of data center resources, implementation of virtualized computing and storage, a security audit failure and reorganizing and downsizing the enterprise and IT function.

Who is accountable for managing the risk created by the introduction of such changes as mobile platforms and the clouds? According to respondents, most responsible for managing the impact of these changes is the CIO or CTO followed by no one has overall responsibility.

**Figure 10. What is the impact of certain events on the ability to manage security threats?**

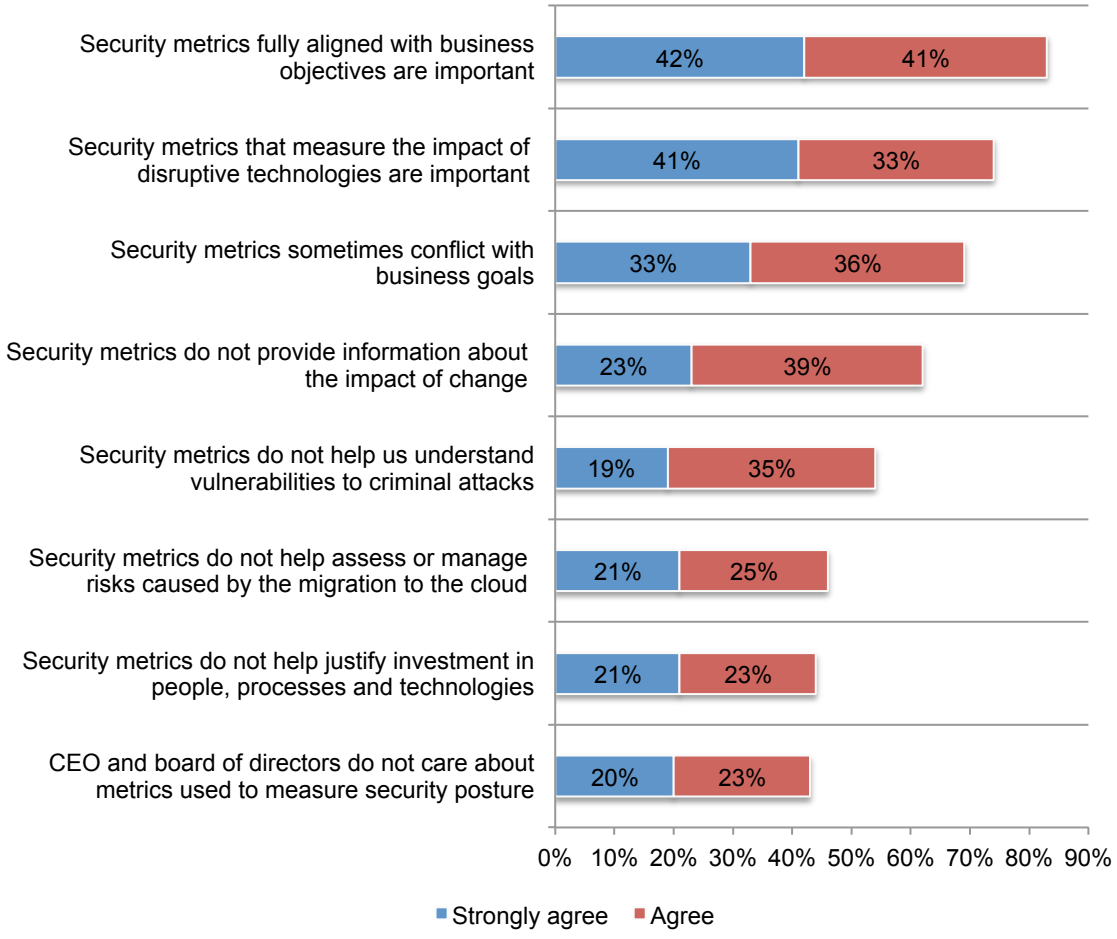


**Metrics must be aligned with business goals**. Eighty-three percent of respondents say it is important to have security metrics fully aligned with business objectives. However, most organizations represented in this study do not seem to be achieving this goal. In fact, 69 percent say security metrics sometimes conflict with the organization's business goals, as shown in Figure 11.

Seventy-four percent agree that security metrics that show the impact of disruptive technologies on security posture are important. However, 62 percent of respondents say metrics fail to provide information about the impact of change. Respondents also agree that metrics do not help understand the vulnerabilities to criminal attacks (54 percent of respondents) and 46 percent of respondents say they do not help assess or manage risks caused by the migration to the cloud.

On a positive note, 56 respondents agree that metrics can help justify investment in people, processes and technologies (100 percent – 44 percent) and 57 percent of respondents agree the CEO and board do care about the metrics used to measure security posture (100 percent – 43).

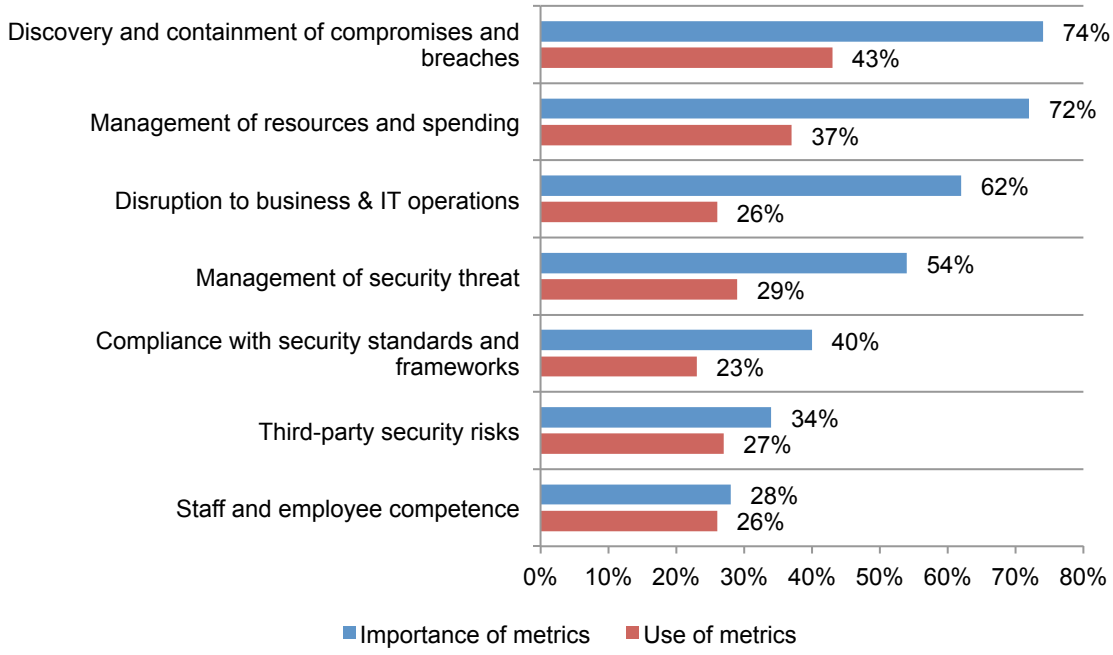
**Figure 11. Perceptions about security metrics**
Strongly agree and agree response



**The metrics that matter gap.** Respondents were asked to rate the metrics most important in communicating relevant facts about the state of security risks to senior executives and IT management. As shown in Figure 12, the top metrics in terms of their importance are discovery and containment of compromises and breaches and management of resources and spending. However, the actual average use of metrics in these categories average only 43 percent and 37 percent of organizations represented in this research.

The biggest gaps in importance vs. use are with metrics that track disruption to business & IT operations (36 percent gap), management of resources and spending (35 percent gap) and discovery and containment of compromises and breaches (31 percent gap). The smallest gaps between importance and use are with third-party risks (7 percent) and staff and employee competence (2 percent).

**Figure 12. Importance of metrics and use of metrics**



**Tracking how fast a security incident is discovered and contained is the most important metric but not often used, as shown in Figure 12 above.** Respondents were asked to rate the importance of specific metrics in communicating the state of security risk to senior executives and IT management. The following metrics are considered to be most important in achieving more effective communications.

- Metrics on compliance with security standards and frameworks. Most often used are length of time to implement security patches and reduction in audit findings (especially repeat findings).
- Metrics on the management of security threat. Most often used are reduction in the number of known vulnerabilities and percentage of endpoints free of malware and viruses.
- Metrics on the minimization of disruption to business & IT operations. Most often used is reduction in unplanned system downtime.
- Metrics on staff and employee competence. Most often used is number of end users receiving appropriate training.
- Metrics on efficient management of resources and spending. Most often used is reduction in the cost of security management activities.
- Time-dependent metrics on the discovery and containment of compromises and breaches. The most often used are mean time to fix, to identify and know root causes.
- Metrics on the minimization of third-party security risks. The most often used is the number of third parties that attest to meeting compliance and security standards.

**Practices to achieve effective security change management**

In this section, we look at the different practices of organizations that were self-reported to have a high security posture and those that have a low security posture. The findings reveal that there is a difference in the technologies deployed, perceptions about barriers to managing the impact of change to the security infrastructure, effectiveness in communication with senior management and frequency of communications.

Figure 13 compares the security posture of the organizations in this study to the technologies fully or partially deployed to facilitate the management of changes that impact an organization's security risk profile. As shown, there are significant differences in the use of log monitoring, vulnerability risk management, forensics, incident detection and alerting and big data analytics between those with a high security posture and those with a low posture.

**Figure 13. High and low security posture for deployed technologies**

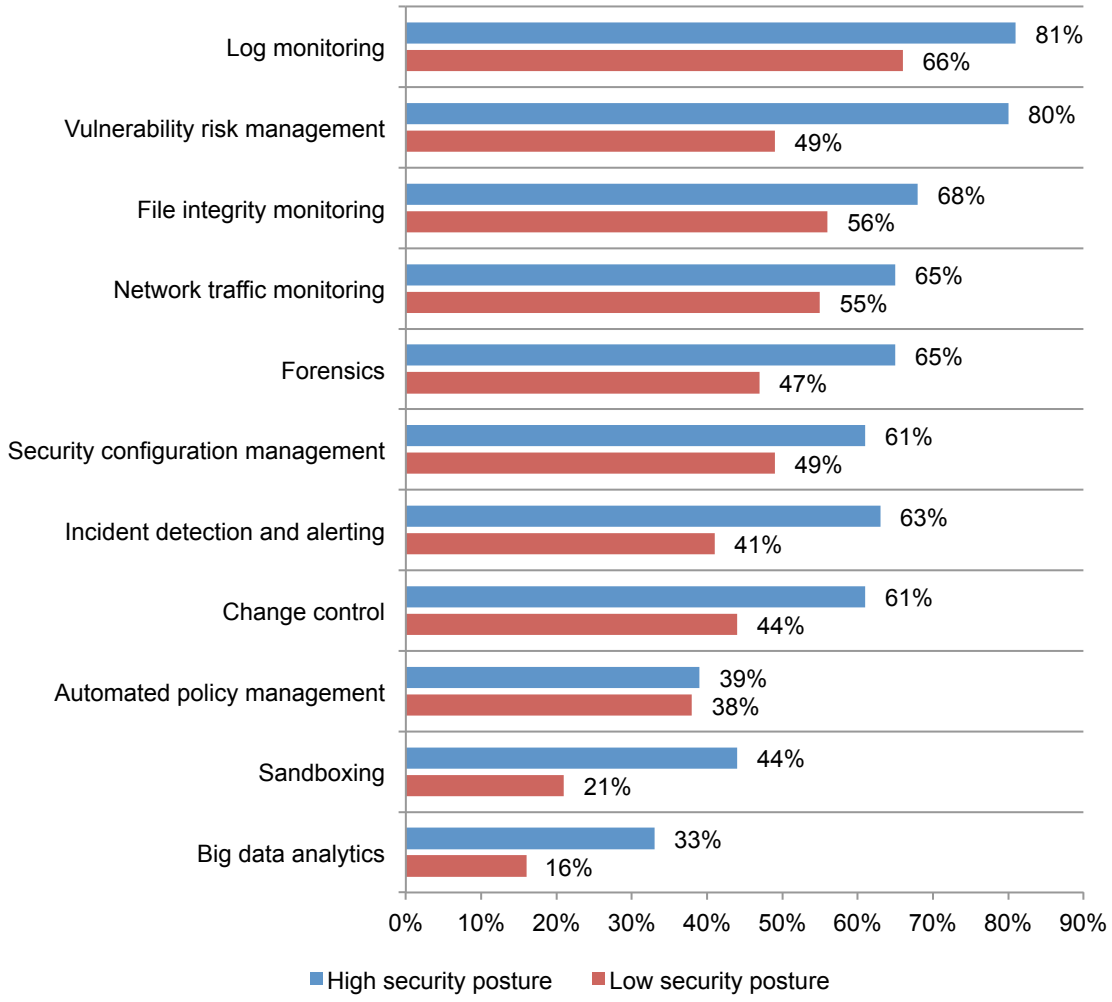


Figure 14 highlights the difference in barriers faced in achieving effective security change management activities between those organizations with a high and low security posture. Specifically, budget and available technology solutions are a much bigger barrier for those with a low security budget. Complexity is more of a barrier for those organizations with a higher security posture. Lack of leadership and C-level support are minor for both groups.

**Figure 14. High and low security posture for list of barriers**

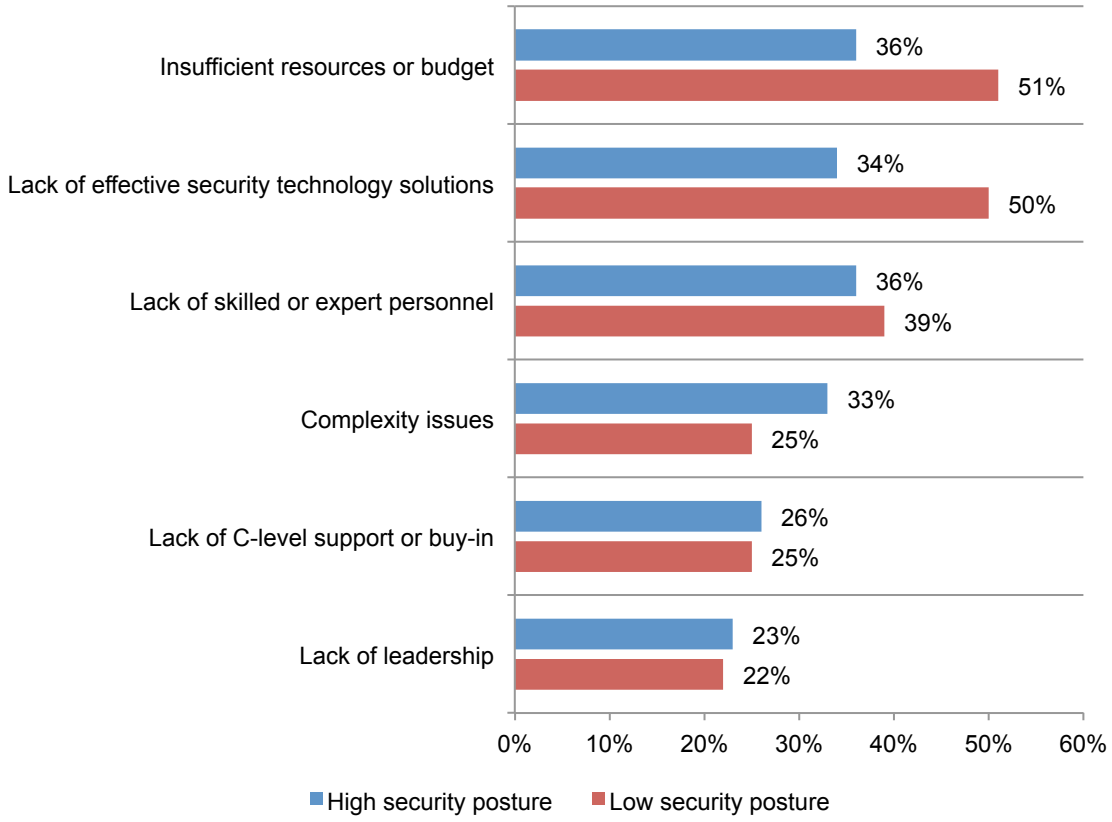
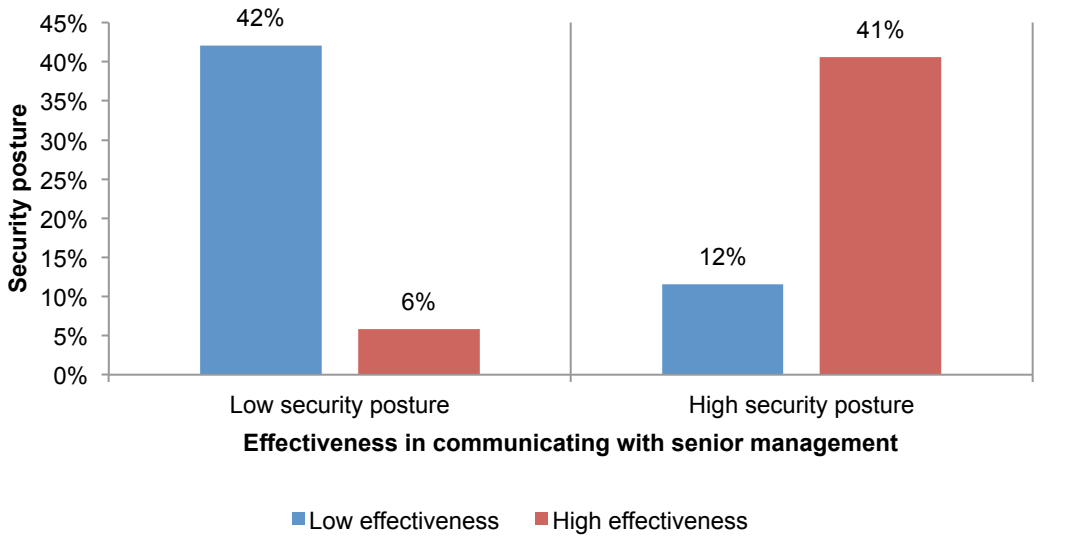


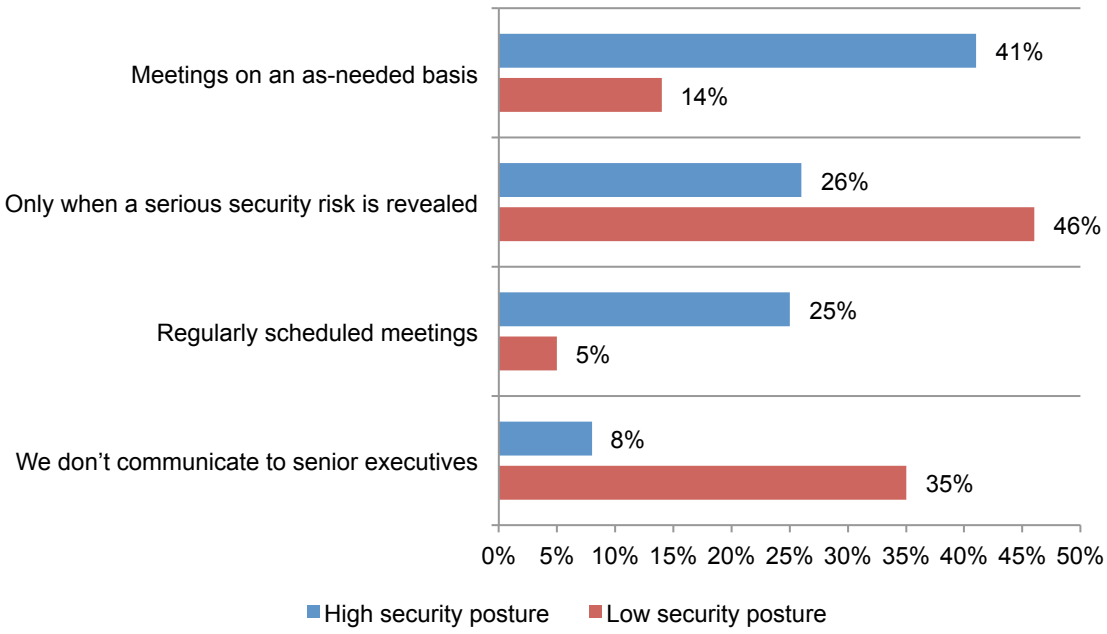
Figure 15 compares security posture to the effectiveness of communication. These findings make the point that a high security posture is linked to effective communication with senior management. Specifically, only 6 percent of respondents in organizations with a low security posture say their communication is highly effective. Whereas, in the high security posture organizations 41 percent of respondents say their communication is highly effective.

**Figure 15. High and low security posture by high and low communication effectiveness**




According to Figure 16, a high security posture is also linked to the frequency of communications with the CEO and board. The biggest differences are having access to management on an as-needed basis (41 percent of respondents vs. 14 percent of respondents) and only when a serious security risk is revealed (26 percent of respondents vs. 46 percent of respondents).

**Figure 16. High and low security posture for list of communication options**



## Conclusion: The right metrics to manage change

The tale of two security departments is evidence that the IT security function needs to improve its communication with senior executives. Respondents in this survey believe that senior executives have a far more optimistic view of the state of security in their organizations.

Based on the findings in this research, metrics should be designed to: clearly convey the organization's security posture, provide guidance on how to manage change to the security function due to the introduction of disruptive technologies and be supportive of the organization's goals and mission.

Some metrics that matter and can be measured include:

- Assessment of an organization's vulnerability to attacks
- Assessment of the impact of disruptive technologies on the organization's security posture
- Assessment of technologies used to manage change to the security function
- Assessment of risks caused by the migration to the cloud and changes in the mobile platform

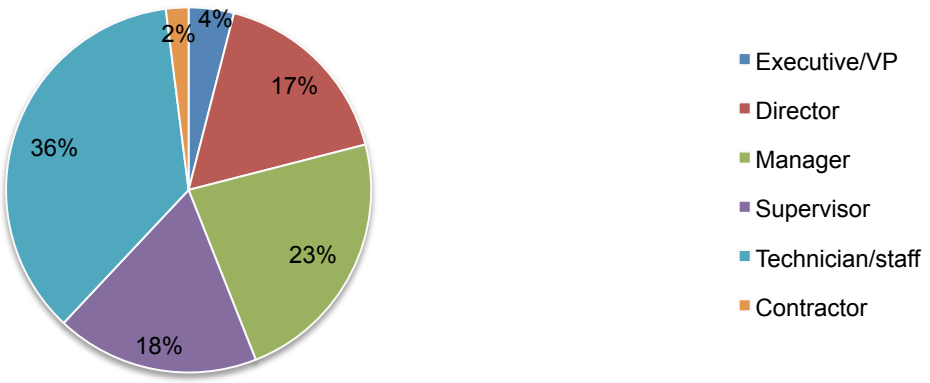
## Methods

A sampling frame of 17,443 experienced IT, IT security, compliance, risk management and other related fields, located in all regions of the United States were selected as survey participants. To ensure knowledgeable responses, all respondents are involved in IT security management activities, assessing or managing the impact of change on their organization's IT security operations. Respondents averaged 12 years of IT experience and approximately 6 years in their current position. Table 1 shows 690 total returns. Screening and reliability checks required the removal of 93 surveys. Our final sample consisted of 597 surveys (3.4 percent response rate).

| **Table 1. Sample response** | Freq | Pct% |
|---|---|---|
| Total sampling frame | 17,443 | 100.0% |
| Total returns | 690 | 4.0% |
| Rejected or screened surveys | 93 | 0.5% |
| Final sample | 597 | 3.4% |

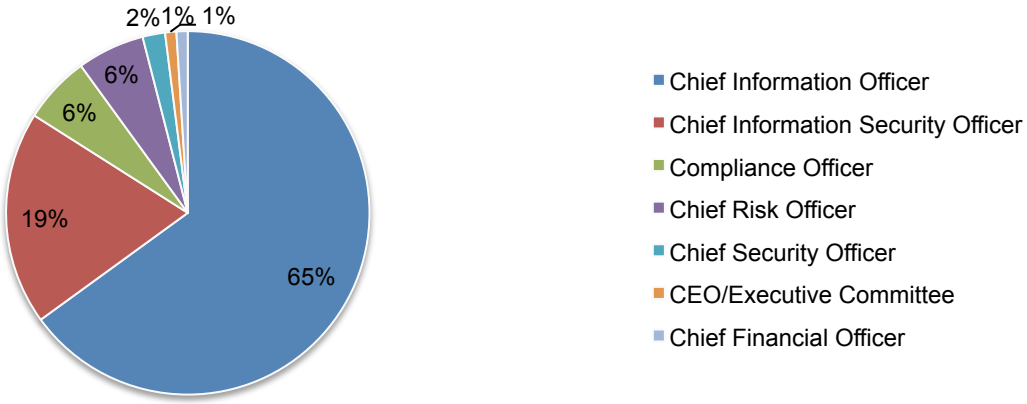
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 62 percent of respondents are at or above the supervisory levels.

**Pie Chart 1. Current position within the organization**



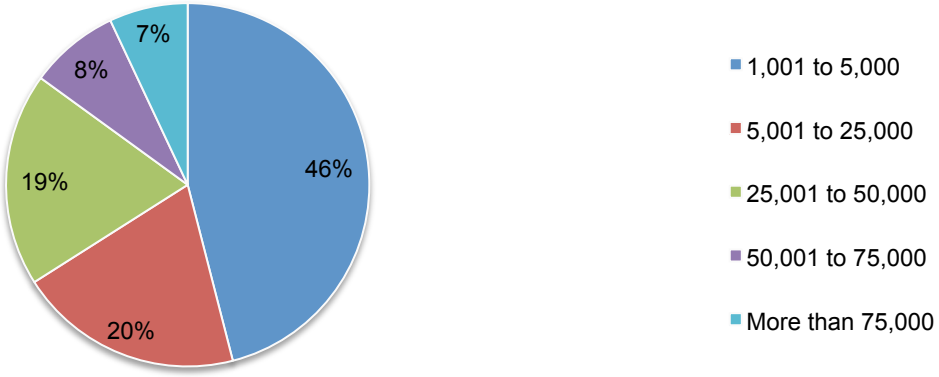

As shown in Pie Chart 2, 65 percent of respondents report to the CIO and 19 percent indicated they report to the CISO.

**Pie Chart 2. Primary Person you or your IT security leader reports to**



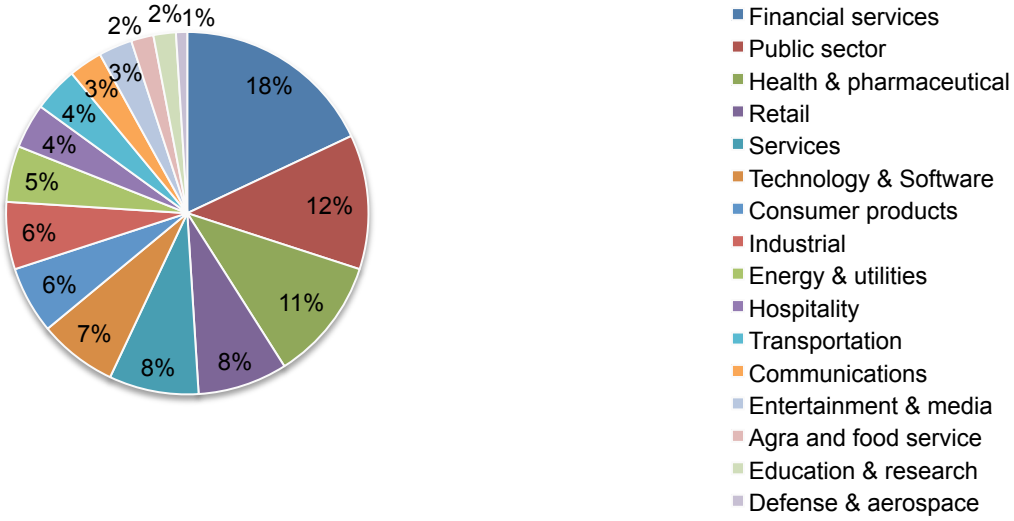
As shown in Pie Chart 3, 66 percent of respondents are from organizations with a global headcount of 1,000 10 25,000 employees. Thirty-four percent are from organizations with a global headcount of more than 25,000.

**Pie Chart 3. Worldwide headcount of the organization**




Pie Chart 4 reports the industry segments of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by public sector (12 percent), health & pharmaceutical (11 percent), and retail (8 percent).

**Pie Chart 4. Industry distribution of respondents' organizations**



**Part 4. Caveats to this study**

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, IT security, compliance, risk management and other related fields. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- 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 accurate responses.

## Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in February 2014.

| **Survey response** | Freq | Pct% |
|---|---|---|
| Total sampling frame | 17,443 | 100.0% |
| Total returns | 690 | 4.0% |
| Rejected or screened surveys | 93 | 0.5% |
| Final sample | 597 | 3.4% |

**Part 1. Screening**

| S1. What best describes your level of involvement in IT security management activities within your organization? | Pct% |
|---|---|
| Low or none (stop) | 0% |
| Moderate | 27% |
| Significant | 43% |
| Very significant | 30% |
| Total | 100% |

| S2. What best describes the function or department where you work? | Pct% |
|---|---|
| Corporate IT | 43% |
| IT network security | 26% |
| IT network operations | 22% |
| Data center operations | 21% |
| Business operations | 16% |
| IT compliance/audit | 11% |
| IT risk management | 8% |
| Other (please specify) | 3% |
| None of the above (stop) | 0% |
| Total | 150% |

| S3. What is your level of involvement in accessing or managing the impact of change on your organization's IT security operations. | Pct% |
|---|---|
| Significant involvement | 39% |
| Moderate involvement | 45% |
| Little involvement | 16% |
| No involvement (stop) | 0% |
| Total | 100% |

**Part 2. Capabilities & Change**

| Q1. Using the following 10-point scale, please rate your organization's overall security posture. 1 = weak and 10 = strong. | Pct% |
|---|---|
| 1 to 2 (weak) | 13% |
| 3 to 4 | 20% |
| 5 to 6 | 31% |
| 7 to 8 | 23% |
| 9 to 10 (strong) | 13% |
| Total | 100% |
| Extrapolated value | 5.56 |

| Q2. Following are seven capabilities or factors that may impact your organization's security posture. Please rate your organization's ability to accomplish each factor as either high, moderate or low. | High | Moderate | Low |
|---|---|---|---|
| Compliance with leading security standards and frameworks | 23% | 45% | 32% |
| Management of security threats | 65% | 23% | 12% |
| Minimization of disruptions to business and IT operations | 56% | 31% | 13% |
| Security staff and employee competence | 61% | 29% | 10% |
| Efficient management of resources and spending | 49% | 37% | 14% |
| Discover and contain compromises and breaches quickly | 60% | 21% | 19% |
| Minimization of third-party security risks | 43% | 37% | 20% |

| Q3. Using the following 10-point scale, please estimate how your organization's **CEO and Board** would rate your organization's security posture. 1 = weak and 10 = strong. | Pct% |
|---|---|
| 1 to 2 (weak) | 6% |
| 3 to 4 | 12% |
| 5 to 6 | 16% |
| 7 to 8 | 33% |
| 9 to 10 (strong) | 33% |
| Total | 100% |
| Extrapolated value | 7.00 |

| Q4. Using the following 10-point scale, please estimate how **relevant outside parties** such as business partners, vendors, regulators, competitors and others would rate your organization's security posture. 1 = weak and 10 = strong. | Pct% |
|---|---|
| 1 to 2 (weak) | 5% |
| 3 to 4 | 12% |
| 5 to 6 | 20% |
| 7 to 8 | 37% |
| 9 to 10 (strong) | 26% |
| Total | 100% |
| Extrapolated value | 6.84 |

| Q5. Following are 12 change events that may disrupt your organization's infrastructure and its ability to manage security threats. Please rate the impact of each change event as either high, moderate or low on your organization's security posture. | High | Moderate | Low |
|---|---|---|---|
| Migration to the cloud | 41% | 33% | 26% |
| Expansion of mobile platforms | 44% | 36% | 20% |
| Pervasive use of employee-owned mobile devices (BYOD) | 33% | 47% | 20% |
| Material data breach incident | 26% | 29% | 45% |
| Security audit failure | 15% | 18% | 67% |
| Implementation of network technologies | 8% | 53% | 39% |
| Implementation next generation firewall | 29% | 45% | 26% |
| Implementation of business-critical applications such as ERP | 6% | 39% | 55% |
| Implementation of virtualized computing and storage | 5% | 27% | 68% |
| Move or consolidation of data center resources | 7% | 18% | 75% |
| Off-shoring of IT and business operations | 26% | 29% | 45% |
| Reorganizing and downsizing the enterprise and IT function | 14% | 20% | 66% |

| Q6. Using the following 10-point scale, please rate your organization's agility in managing the impact of change on IT security operations. 1 = low agility and 10 = high agility. | Pct% |
|---|---|
| 1 to 2 (low agility) | 25% |
| 3 to 4 | 32% |
| 5 to 6 | 12% |
| 7 to 8 | 15% |
| 9 to 10 (high agility) | 16% |
| Total | 100% |
| Extrapolated value | 4.80 |

| Q7. Using the following 10-point scale, please rate your organization's effectiveness in managing the impact of change on IT security operations. 1 = ineffective and 10 = highly effective. | Pct% |
|---|---|
| 1 to 2 (ineffective) | 30% |
| 3 to 4 | 26% |
| 5 to 6 | 11% |
| 7 to 8 | 16% |
| 9 to 10 (highly effective) | 17% |
| Total | 100% |
| Extrapolated value | 4.78 |

| Q8. Who within your organization has overall responsibility for managing the impact of the above-mentioned change events on IT security operations? Please check **one** best choice. | Pct% |
|---|---|
| CEO, COO, CFO | 2% |
| CIO or CTO | 35% |
| CISO or CSO | 21% |
| Compliance/audit | 6% |
| General counsel (OGC) | 2% |
| Leader of enterprise or IT risk management | 5% |
| No one person has overall responsibility | 28% |
| Other (please specify) | 1% |
| Total | 100% |

| Q9. The following statements pertain to security metrics that help organizations to manage changes that impact its ability to meet IT security objectives. Please rate your level of agreement with each statement using the five-point scale provided below the item. | Strongly agree | Agree |
|---|---|---|
| Q9a. Security metrics do not provide information about the impact of change on our organization. | 23% | 39% |
| Q9b. Security metrics do not help the IT function assess or manage risks caused by the migration to cloud environments. | 21% | 25% |
| Q9c. Our organization's CEO and board of directors do not care about metrics used to measure our security posture. | 20% | 23% |
| Q9d. Security metrics do not help us understand our organization's vulnerabilities to criminal attacks. | 19% | 35% |
| Q9e. Security metrics sometimes conflict with of the organization's business goals. | 33% | 36% |
| Q9f. Security metrics that measure the impact of disruptive technologies on security posture are important. | 41% | 33% |
| Q9g. Security metrics do not help us justify investment in people, processes and technologies. | 21% | 23% |
| Q9h. It is important to have security metrics that are fully aligned with business objectives. | 42% | 41% |

| Q10. What do you see as the most significant barriers to achieving effective security change management activities within your organization today? Please select your **top two** choices. | Pct% |
|---|---|
| Insufficient resources or budget | 43% |
| Lack of effective security technology solutions | 42% |
| Lack of skilled or expert personnel | 37% |
| Lack of leadership | 23% |
| Lack of C-level support or buy-in | 25% |
| Insufficient impact assessments | 2% |
| Complexity issues | 28% |
| Other (please specify) | 0% |
| Total | 200% |

| Q11. Following are technologies that may facilitate the management of changes that impact an organization's security risk profile. Please check each technology category used by your organization (under the heading: fully deployed, partially deployed, minimally deployed or not deployed). | Fully deployed | Partially deployed | Minimally deployed | Not deployed |
|---|---|---|---|---|
| Automated policy management | 16% | 23% | 16% | 45% |
| Big data analytics | 15% | 11% | 10% | 64% |
| Change control | 23% | 29% | 25% | 23% |
| File integrity monitoring | 28% | 35% | 18% | 19% |
| Forensics | 34% | 22% | 26% | 18% |
| Incident detection and alerting (including SIEM) | 43% | 12% | 12% | 33% |
| Log monitoring | 29% | 46% | 17% | 8% |
| Network traffic monitoring | 42% | 19% | 13% | 26% |
| Sandboxing | 18% | 16% | 22% | 44% |
| Security configuration management | 41% | 14% | 12% | 33% |
| Vulnerability risk management | 43% | 26% | 15% | 16% |

| Q12. How does your organization identify the impact of changes on its IT security posture? Please select all that apply. | Pct% |
|---|---|
| Automated risk impact assessments | 15% |
| Manual risk impact assessments | 26% |
| Continuous compliance monitoring | 13% |
| Internal or external audits | 11% |
| None of the above | 34% |
| Other (please specify) | 1% |
| Total | 100% |

| Q13. How important is real time analysis for managing changes to the organization's security risk landscape? | Pct% |
|---|---|
| Essential | 33% |
| Very important | 39% |
| Important | 12% |
| Not important | 12% |
| Irrelevant | 4% |
| Total | 100% |

**Part 3. Communications & Metrics**

| Q14. When do you communicate the state of security risk to senior executives in your organization? | Pct% |
|---|---|
| Regularly scheduled meetings annual quarterly semi-annual | 13% |
| Meetings at the request of management on an as-needed basis | 27% |
| Only when a serious security risk is revealed | 31% |
| We don't communicate to senior executives | 29% |
| Other (please specify) | 0% |
| Total | 100% |

| Q15a. Using the following 10-point scale, please rate your organization's effectiveness in communicating all relevant facts about the state of security risk to **senior executives**. 1 = ineffective and 10 = highly effective. | Pct% |
|---|---|
| 1 to 2 (ineffective) | 35% |
| 3 to 4 | 33% |
| 5 to 6 | 11% |
| 7 to 8 | 15% |
| 9 to 10 (highly effective) | 6% |
| Total | 100% |
| Extrapolated value | 3.98 |

| Q15b. If not effective [rating below 5], why not? Please select all that apply. | Pct% |
|---|---|
| Communications occur at too low a level | 71% |
| We only communicate with senior executives when there is an actual incident | 63% |
| Communications are contained in only one department or line of business (silos) | 60% |
| The information is too technical to be understood by non-technical management | 58% |
| Negative facts are filtered before being disclosed to senior executives and the CEO | 51% |
| Senior executives are not interested in this information | 43% |
| The information can be ambiguous, which may lead to poor decisions | 37% |
| It takes too much time and resources to prepare reports to senior executives | 25% |
| Other (please specify) | 0% |
| Total | 408% |

| Q16a. Using the following 10-point scale, please rate your organization's effectiveness in communicating all relevant facts about the state of security risk to **IT management**. 1 = ineffective and 10 = highly effective. | Pct% |
|---|---|
| 1 to 2 (ineffective) | 11% |
| 3 to 4 | 23% |
| 5 to 6 | 33% |
| 7 to 8 | 18% |
| 9 to 10 (highly effective) | 15% |
| Total | 100% |
| Extrapolated value | 5.56 |

| Q16b. If not effective [rating below 5], why not? Please select all that apply. | Pct% |
|---|---|
| Negative facts are filtered before being disclosed to IT management | 25% |
| IT managers are not interested in this information | 26% |
| Communications occur at too low a level | 56% |
| Communications are contained in only one department or line of business (silos) | 58% |
| The information is too technical to be understood by non-technical management | 12% |
| The information can be ambiguous, which may lead to poor decisions | 36% |
| It takes too much time and resources to prepare reports to IT management | 31% |
| We only communicate with IT management when there is an actual incident | 34% |
| Other (please specify) | 0% |
| Total | 278% |

| Q17. How important are metrics in achieving an effective security change management process? | Pct% |
|---|---|
| Essential | 23% |
| Very important | 39% |
| Important | 20% |
| Not important | 13% |
| Irrelevant | 5% |
| Total | 100% |

| Q18a. Metrics on compliance with security standards and frameworks | Pct% |
|---|---|
| Length of time to implement security patches | 53% |
| Reduction in audit findings (especially repeat findings) | 39% |
| Reduction in the number or percentage of policy violations | 25% |
| Reduction in expired certificates and keys | 18% |
| Number of records or files detected as compliance infractions | 16% |
| Reduction in the number or percentage of end user enforcement actions | 6% |
| Reduction in regulatory actions and lawsuits | 2% |
| None (skip 18b) | 32% |
| Total | 191% |

| Q18b. Using the following 10-point scale, please rate the importance of these metrics in communicating relevant facts about the state of security risk to **senior executives and IT management**. 1 = not important and 10 = very important. | Pct% | | | |
|---|---|---|---|---|
| 1 to 2 (not important) | 13% | | | |
| 3 to 4 | 17% | | | |
| 5 to 6 | 30% | | | |
| 7 to 8 | 23% | | | |
| 9 to 10 (very important) | 17% | | | |
| Total | 100% | High | Moderate | Low |
| Extrapolated value | 5.78 | 40% | 30% | 30% |

| Q19a. Metrics on the management of security threat | Pct% |
|---|---|
| Reduction in the number of known vulnerabilities | 46% |
| Percentage of endpoints free of malware and viruses | 45% |
| Reduction in the number of data breach incidents | 31% |
| Percentage of software applications tested | 24% |
| Reduction in the number of threats | 15% |
| Percentage reduction in recurring incidents | 10% |
| None (skip 19b) | 30% |
| Total | 201% |

| Q19b. Using the following 10-point scale, please rate the importance of these metrics in communicating relevant facts about the state of security risk to **senior executives and IT management**. 1 = not important and 10 = very important. | Pct% | | | |
|---|---|---|---|---|
| 1 to 2 (not important) | 10% | | | |
| 3 to 4 | 12% | | | |
| 5 to 6 | 24% | | | |
| 7 to 8 | 24% | | | |
| 9 to 10 (very important) | 30% | | | |
| Total | 100% | High | Moderate | Low |
| Extrapolated value | 6.54 | 54% | 24% | 22% |

| Q20a. Metrics on the minimization of disruption to business & IT operations | Pct% |
|---|---|
| Reduction in unplanned system downtime | 45% |
| Length of time to contain data breaches and security exploits | 27% |
| Percentage of incidents detected by an automated controls | 18% |
| Reduction in the frequency of denial of service attacks | 15% |
| None (skip 20b) | 43% |
| Total | 148% |

| Q20b. Using the following 10-point scale, please rate the importance of these metrics in communicating relevant facts about the state of security risk to **senior executives and IT management**. 1 = not important and 10 = very important. | Pct% | | | |
|---|---|---|---|---|
| 1 to 2 (not important) | 10% | | | |
| 3 to 4 | 10% | | | |
| 5 to 6 | 18% | | | |
| 7 to 8 | 33% | | | |
| 9 to 10 (very important) | 29% | | | |
| Total | 100% | High | Moderate | Low |
| Extrapolated value | 6.72 | 62% | 18% | 20% |

| Q21a. Metrics on staff and employee competence | Pct% |
|---|---|
| Number of end users receiving appropriate training | 53% |
| Reduction in the number of access and authentication violations (tickets) | 30% |
| Number of security personnel achieving certification | 29% |
| Reduction in the loss of data-bearing devices (laptops, tablets, smart phones) | 25% |
| Job vacancies (open requisitions) for IT security personnel and other related fields | 14% |
| Performance of users on security training retention tests | 6% |
| None (skip 21b) | 33% |
| Total | 190% |

| Q21b. Using the following 10-point scale, please rate the importance of these metrics in communicating relevant facts about the state of security risk to **senior executives and IT management**. 1 = not important and 10 = very important. | Pct% | | | |
|---|---|---|---|---|
| 1 to 2 (not important) | 16% | | | |
| 3 to 4 | 29% | | | |
| 5 to 6 | 27% | | | |
| 7 to 8 | 19% | | | |
| 9 to 10 (very important) | 9% | | | |
| Total | 100% | High | Moderate | Low |
| Extrapolated value | 5.02 | 28% | 27% | 45% |

| Q22a. Metrics on efficient management of resources and spending | Pct% |
|---|---|
| Reduction in the cost of security management activities | 56% |
| Spending level relative to total budget | 42% |
| Reduction in the total cost of ownership (TCO) | 40% |
| Return on security technology investments (ROI) | 36% |
| Reduction in the cost of cyber crime remediation | 12% |
| None (skip 22b) | 35% |
| Total | 221% |

| Q22b. Using the following 10-point scale, please rate the importance of these metrics in communicating relevant facts about the state of security risk to **senior executives and IT management**. 1 = not important and 10 = very important. | Pct% | | | |
|---|---|---|---|---|
| 1 to 2 (not important) | 8% | | | |
| 3 to 4 | 9% | | | |
| 5 to 6 | 11% | | | |
| 7 to 8 | 34% | | | |
| 9 to 10 (very important) | 38% | | | |
| Total | 100% | High | Moderate | Low |
| Extrapolated value | 7.20 | 72% | 11% | 17% |

| Q23a. Time-dependent metrics on the discovery and containment of compromises and breaches | Pct% |
|---|---|
| Mean time to fix | 51% |
| Mean time to identify | 49% |
| Mean time to know root causes | 41% |
| Mean time to verify | 38% |
| Mean time to contain | 38% |
| None (skip 23b) | 45% |
| Total | 262% |

| Q23b. Using the following 10-point scale, please rate the importance of these metrics in communicating relevant facts about the state of security risk to **senior executives and IT management**. 1 = not important and 10 = very important. | Pct% | | | |
|---|---|---|---|---|
| 1 to 2 (not important) | 8% | | | |
| 3 to 4 | 9% | | | |
| 5 to 6 | 9% | | | |
| 7 to 8 | 34% | | | |
| 9 to 10 (very important) | 40% | | | |
| Total | 100% | High | Moderate | Low |
| Extrapolated value | 7.28 | 74% | 9% | 17% |

| Q24a. Metrics on the minimization of third-party security risks | Pct% |
|---|---|
| Number of third parties that attest to meeting compliance and security standards | 45% |
| Number of third parties that experience special vetting before granting access to networks | 27% |
| Length of time access is granted to third parties | 23% |
| Number of third parties with access to networks | 22% |
| Number of third parties that indemnify the company against security breaches | 20% |
| None (skip 24b) | 44% |
| Total | 181% |

| Q24b. Using the following 10-point scale, please rate the importance of these metrics in communicating relevant facts about the state of security risk to **senior executives and IT management**. 1 = not important and 10 = very important. | Pct% | | | |
|---|---|---|---|---|
| 1 to 2 (not important) | 13% | | | |
| 3 to 4 | 23% | | | |
| 5 to 6 | 30% | | | |
| 7 to 8 | 18% | | | |
| 9 to 10 (very important) | 16% | | | |
| Total | 100% | High | Moderate | Low |
| Extrapolated value | 5.52 | 34% | 30% | 36% |

| Q25a. Do you believe these metrics adequately convey the true state of security efforts deployed by your organization today? | Pct% |
|---|---|
| Yes | 46% |
| No | 43% |
| Unsure | 11% |
| Total | 100% |

| Q25b. If no or unsure, why? In other words, why don't you use metrics that convey the true state of security within your organization? | Pct% |
|---|---|
| More pressing issues take precedence | 72% |
| We only communicate with management when there is an actual incident | 63% |
| The information is too technical to be understood by non-technical management | 59% |
| Lack of resources to develop or refine metrics | 54% |
| Management is not interested in this information | 43% |
| The information can be ambiguous, which may lead to poor decisions | 36% |
| It takes too much time and resources to prepare report metrics | 25% |
| Don't know why | 23% |
| Other (please specify) | 0% |
| Total | 375% |

**Part 6. Demographics & Organizational Characteristics**

| D1. What organizational level best describes your current position? | Pct% |
|---|---|
| Executive/VP | 4% |
| Director | 17% |
| Manager | 23% |
| Supervisor | 18% |
| Technician/staff | 36% |
| Contractor | 2% |
| Total | 100% |

| D2. Check the **Primary Person** you or your IT security leader reports to within the organization. | Pct% |
|---|---|
| Chief Information Officer | 65% |
| Chief Information Security Officer | 19% |
| Compliance Officer | 6% |
| Chief Risk Officer | 6% |
| Chief Security Officer | 2% |
| CEO/Executive Committee | 1% |
| Chief Financial Officer | 1% |
| Total | 100% |

| D3. Experience: | Mean | Median |
|---|---|---|
| Total years in IT, security, compliance, risk management or other related fields | 11.7 | 11.0 |
| Total years in current position years | 6.0 | 6.0 |
| Number of professional certifications in IT security and other related fields | 2.7 | 2.0 |

| D4. What is the worldwide headcount of your company? | Pct% |
|---|---|
| 1,001 to 5,000 | 46% |
| 5,001 to 25,000 | 20% |
| 25,001 to 50,000 | 19% |
| 50,001 to 75,000 | 8% |
| More than 75,000 | 7% |
| Total | 100% |
| Extrapolated mean headcount | 22,105 |
| Median headcount | 9,000 |

| D5. What industry best describes your organization's industry focus? | Pct% |
|---|---|
| Financial services | 18% |
| Public sector | 12% |
| Health & pharmaceutical | 11% |
| Retail | 8% |
| Services | 8% |
| Technology & Software | 7% |
| Consumer products | 6% |
| Industrial | 6% |
| Energy & utilities | 5% |
| Hospitality | 4% |
| Transportation | 4% |
| Communications | 3% |
| Entertainment & media | 3% |
| Agra and food service | 2% |
| Education & research | 2% |
| Defense & aerospace | 1% |
| Total | 100% |

## Ponemon Institute

*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 organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.