Managing the Risk of Post-breach or “Resident” Attacks

Sponsored by Illusive Networks

Independently conducted by Ponemon Institute LLC

Publication Date: November 2018

Managing the Risk of Post-breach or "Resident" Attacks
Prepared by Ponemon Institute, November 2018

Executive Overview

Ponemon Institute surveyed 627 IT and IT security practitioners in the United States to understand how well organizations are addressing cyber risks associated with attackers who may already be residing within the perimeter, including insiders that might act maliciously. In this study, these are referred to as "post-breach" or "resident" attackers.

The findings consistently show that organizations do not fully understand the risks associated with this type of threat, are unprepared for resident attackers, and have little ability to discover and remove them.

Capabilities to preempt, detect, and respond to post-breach, resident threats need to be strengthened across the board:

- Organizations have low confidence in their ability to prevent serious damage from these attacks
- Senior leaders lack understanding of the threats and do not clearly communicate business risk
- Most organizations lack the ability to detect resident attackers, particularly insider threats
- Capabilities are low to prevent attackers from finding connections and credentials that enable lateral movement
- Incident response appears to be the weakest link in the threat-handling chain
- Investments in most areas will increase, but the budgets are shifting significantly toward threat detection

A comprehensive program for mitigating risks associated with resident attackers has many facets. This survey provides broad visibility into areas of relative strength and weakness common to many organizations.

Part 1. Introduction

Sponsored by Illusive Networks, Ponemon Institute surveyed 627 IT and IT security practitioners in the United States to understand how well organizations are addressing the cyber risks associated with attackers who may already be residing within the perimeter, including insiders that might act maliciously.

All participants in this research are involved in the evaluation, selection and/or implementation of IT security solutions and governance practices within their organizations.

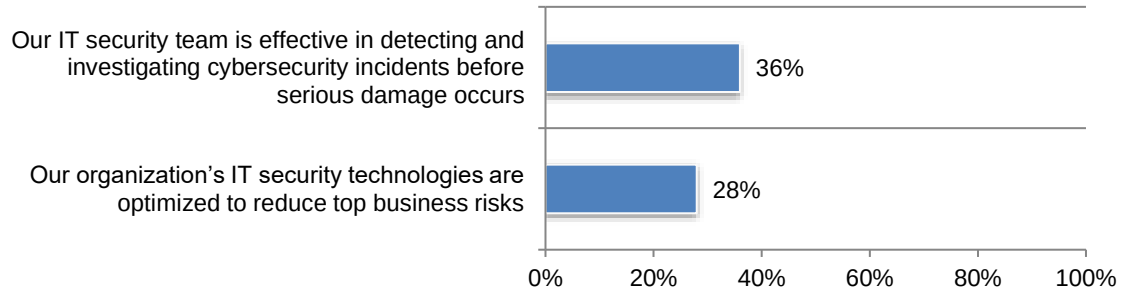
This study starts with the premise that mitigating business impact once attackers are within the environment requires the ability to:

1. Understand which cyberthreats pose the greatest risk and align the cybersecurity program accordingly;
2. Proactively shape security controls and improve cyber hygiene based on an understanding of how attackers operate;
3. Quickly detect attackers who are operating internally;
4. Efficiently prioritize and act on incidents based on real-time awareness of how the organization could be impacted.

The data indicates that organizations have low confidence in their ability to prevent serious damage from post-breach attacks. As shown in Figure 1, when presented with a set of statements, only 36 percent of respondents express agreement or strong agreement that their security team is effective in detecting and investigating cybersecurity incidents before serious damage occurs.

Figure 1. Effectiveness in managing business risks

Strongly agree and agree responses combined



It is welcome news, then, that security budgets are shifting in favor of allocating greater resources to threat detection and response.

For organizations to get to where they need to be is an uphill challenge. While more than half (56 percent) of respondents to this survey believe they have reduced attacker dwell time over the past year, over 44 percent say they have not (32 percent) or don't know (12 percent). And not all attacks and incidents are equal. Figure 1 also shows that only 28 percent of respondents agree or strongly agree that their security technologies are optimized to reduce top business risks. A recurring theme in this study is that the inability to see and act on what matters most to the organization hampers the effectiveness of multiple functions.

Part 2. Key Findings

In this section of the report we analyze the key findings of the research. The complete audited findings are presented in the Appendix of the report. We have organized the report according to the following topics:

A. The risk alignment problem between IT security and the business

B. Current capabilities to preempt, detect, and respond to post-breach attackers

C. Takeaways: Toward better risk mitigation for post-breach or resident attacks

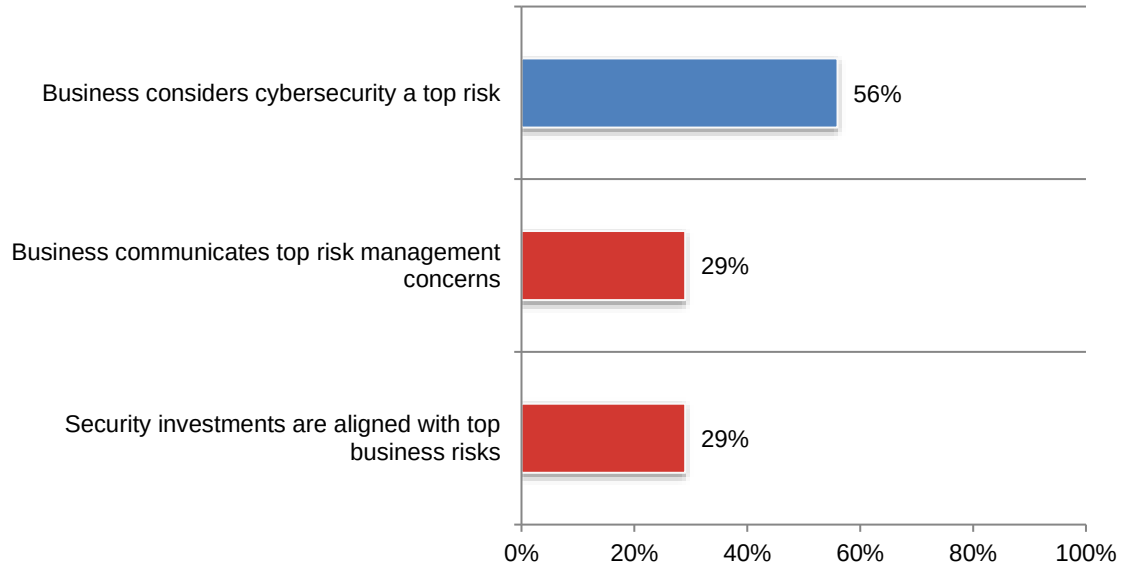
A. The risk alignment problem between IT security and the business

Comparing a few key data points makes it clear that the day-to-day functioning of IT security is not well-aligned to business needs.

As shown in Figure 2, although 56 percent of respondents say business leaders consider cybersecurity a top business risk, only 29 percent of respondents say business leaders communicate their business risk management priorities to IT security leaders, and only 29 percent of respondents say their security leaders effectively align security with top business risks.

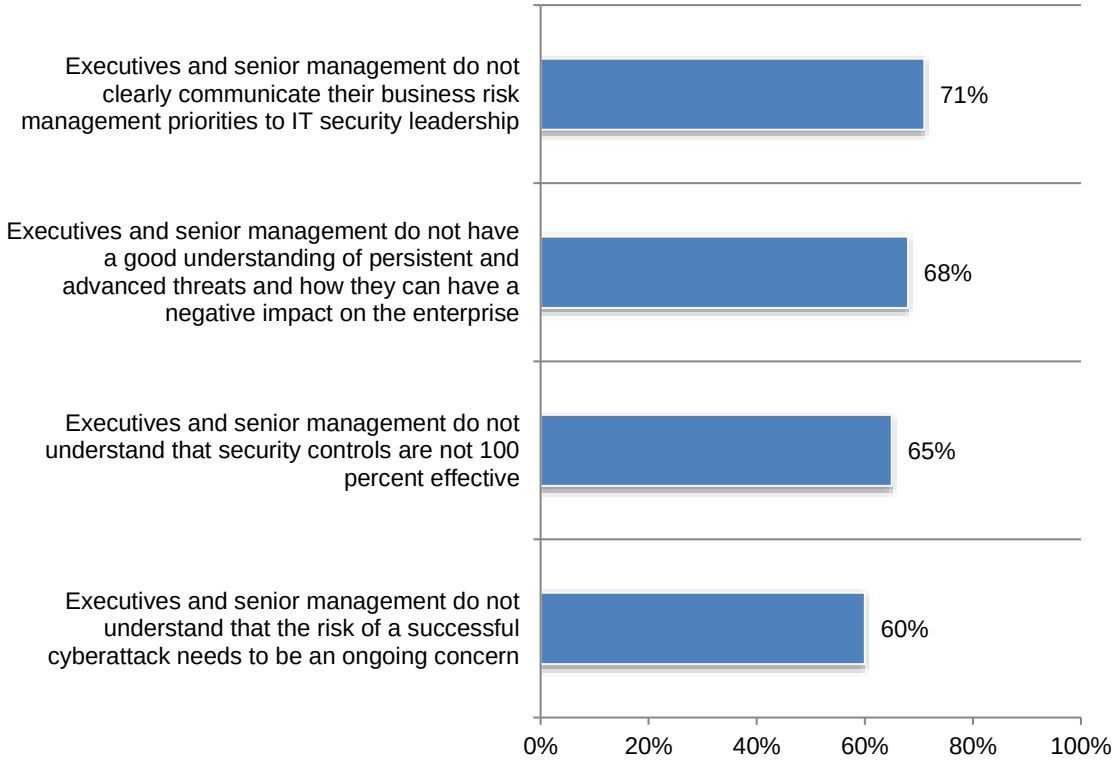
Figure 2. The risk alignment problem

Strongly agree and agree responses combined



Over 70 percent of respondents say senior leaders do not clearly communicate business risk. According to Figure 3, 71 percent of respondents say they are not informed about what senior managers consider their organizations' business risk management priorities—important guidance if IT security is to prioritize what's most important to the business.

Figure 3. Perceptions of senior management's views on security risks



Respondents also are not positive that their leadership understands how persistent and advanced threats can affect the enterprise and that IT security controls are not 100 percent effective (68 percent and 65 percent, respectively).

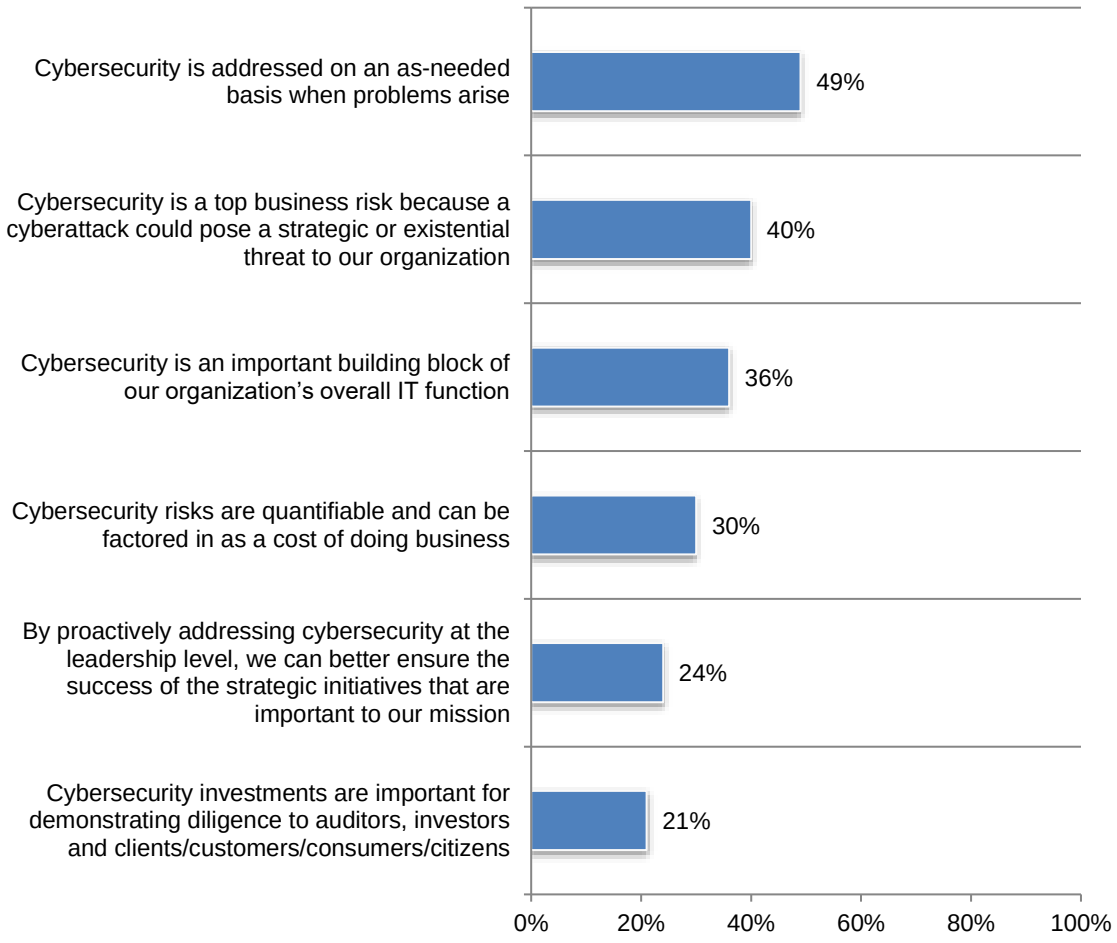
It makes sense, then, that 60 percent also indicate that leaders don't understand that the risk of a successful cyberattack should be an ongoing concern.

Business leaders appear to be conflicted about the importance of a strong cybersecurity posture—or perhaps leaders don't understand the importance of a business-aligned, proactive approach or their role in it. When respondents were asked to describe their executives' views of the importance of the cybersecurity program (Figure 4), the top two responses seem contradictory.

On the one hand, respondents indicate that executives think a cyberattack could pose a strategic or existential threat to their organization (40 percent of respondents), yet given how important cyber risk seems to be, a reactive approach seems fairly prevalent; almost half (49 percent of respondents) say their organizations' executives think cybersecurity should be addressed on an as-needed basis when problems arise.

Figure 4. What best describes how your organization's executives view the importance of the cybersecurity program?

Two responses permitted



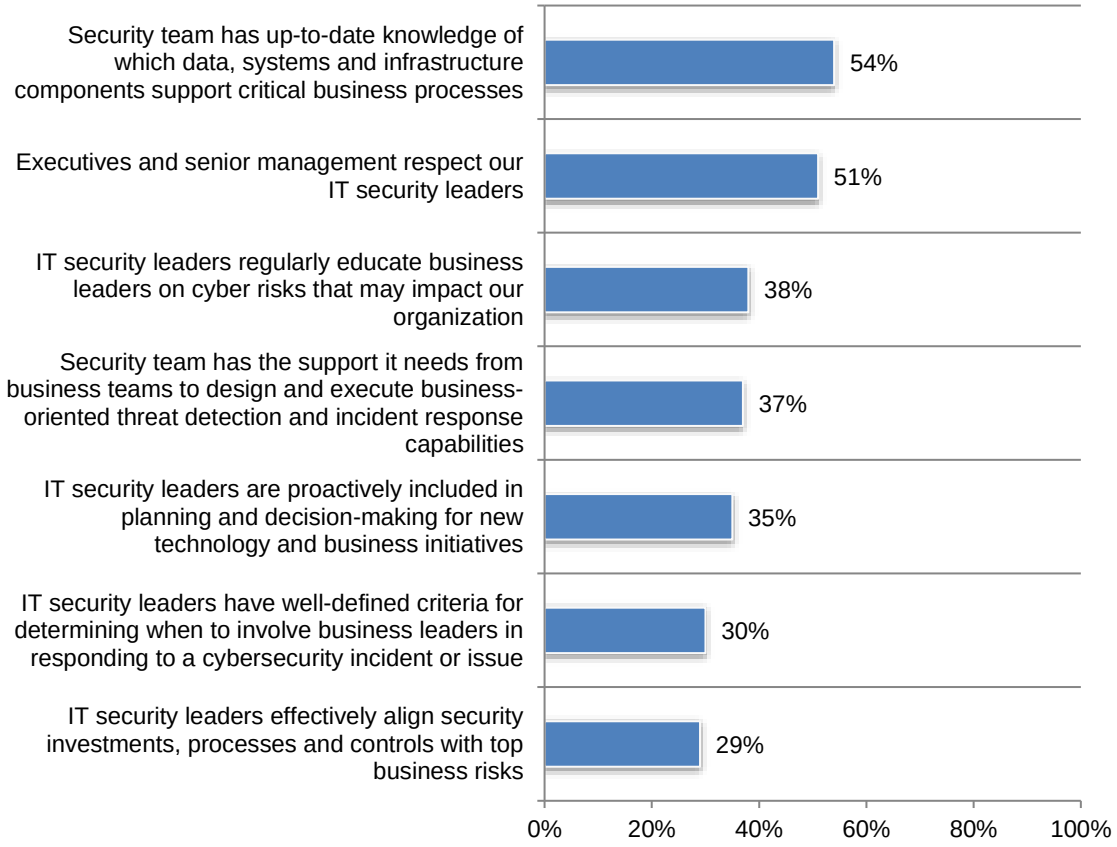
The business/security collaboration gap is reflected in many ways. Whether fault for the disconnect lies on the side of IT security leaders, senior executives, or both, Figure 5 shows a range of indicators that reveal a lack of engagement between them.

Only 35 percent of respondents say their IT security leaders are proactively included in planning and decision-making for new technology and business initiatives, and only 29 percent of respondents say IT security leaders effectively align security investments, processes, and controls with top business risks. Other steps not taken are having well-defined criteria for determining when to involve business leaders in responding to a cybersecurity incident or issue (only 30 percent of respondents agree), as well as educating business leaders on cyber risks that may impact their organization (only 38 percent of respondents agree).

Only about half (51 percent of respondents) say their organizations' executives and senior management respect IT security leaders. As a possible consequence, only 37 percent of respondents say the security team has the support it needs from business teams to design and execute business-oriented threat detection and incident response capabilities.

Figure 5. The lack of collaboration between senior management and IT security

Strongly agree and agree responses combined



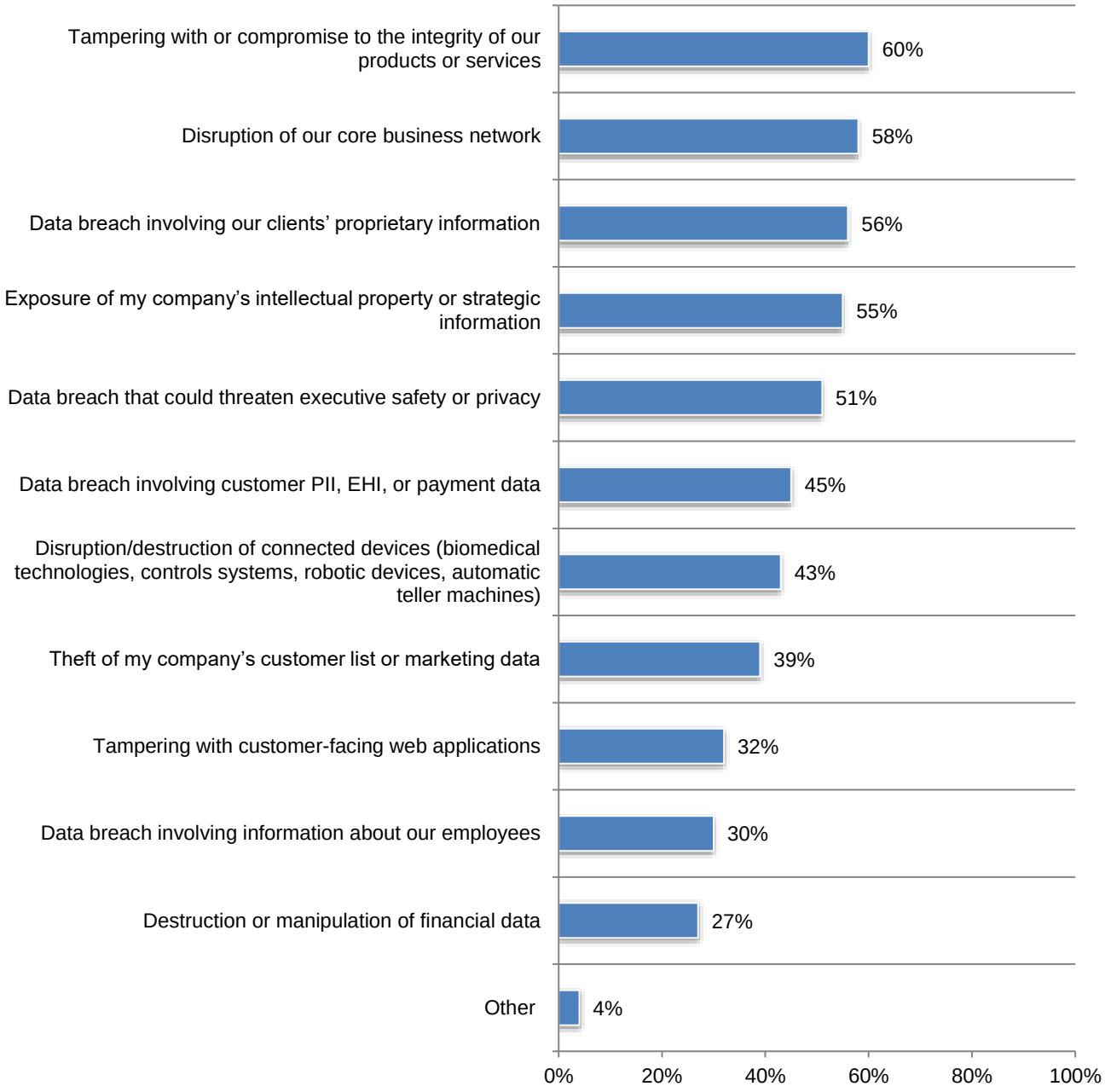
Respondents say that protecting high-volume private data is not the top concern. Respondents were asked to identify the cyberattacks that pose the greatest risk to their business. Given the lack of communication about business risk, these views may not reflect the views of business leaders, but it is notable that although large breaches of PII, EHI, payment and

employee data tend to hog the headlines, these are not respondents' top concerns. The data indicate that the threat of intellectual property or other strategic information theft—theirs or their clients—and various forms of disruption are significantly higher on the risk scale.

As shown in Figure 6, 60 percent of respondents say the worst consequence of a cyberattack would be the tampering with or compromise to the integrity of their products or services followed by the disruption of their core business network (58 percent of respondents). Threats to executive safety and privacy are also high on the list.

Figure 6. The greatest cybersecurity risks to business

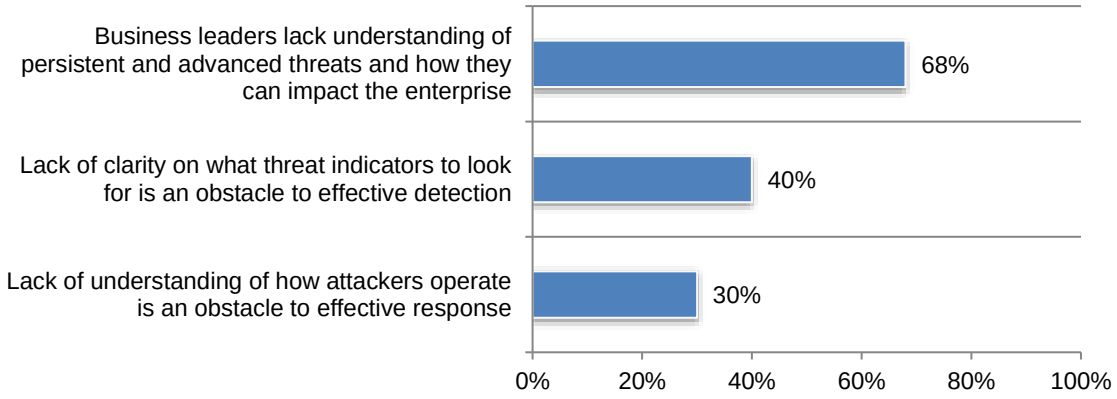
Five responses permitted



Business leaders lack understanding of the threats. Leaders cannot communicate effectively with IT security leaders or set cyber risk management priorities without a foundational understanding of the threat actors an organization needs to contend with, yet 68 percent of respondents say their executives and senior management do not have a good understanding of how threat actors work and the harm they can cause. Among technical functions, where granular threat understanding is necessary for strong detection and response, organizations fare better, but could be stronger.

Figure 7. Threat understanding impedes multiple functions

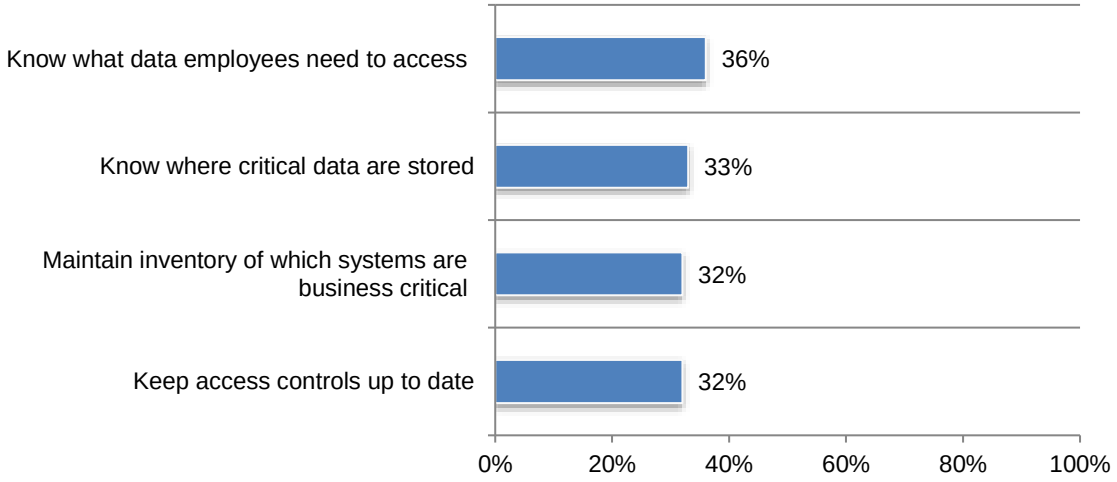
More than one response permitted



Basic asset and access governance are only half-way there. A risk-focused approach also requires a strong picture of where the important IT assets are and who has access to them. Figure 5 shows that 54 percent of respondents agree or strongly agree that their security team has up-to-date knowledge of which data, systems and infrastructure components support critical business processes, yet Figure 8 shows that when asked a series of more detailed questions pertaining to asset awareness and change management, respondents rate themselves considerably lower. The ability to keep pace with rapidly changing users, user functions, and IT infrastructure continues to be a challenge. (Data below includes 7+ on a scale of 1 to 10.)

Figure 8. The ability to achieve basic asset and access

1 = no ability to 10 = high ability, 7+ responses presented

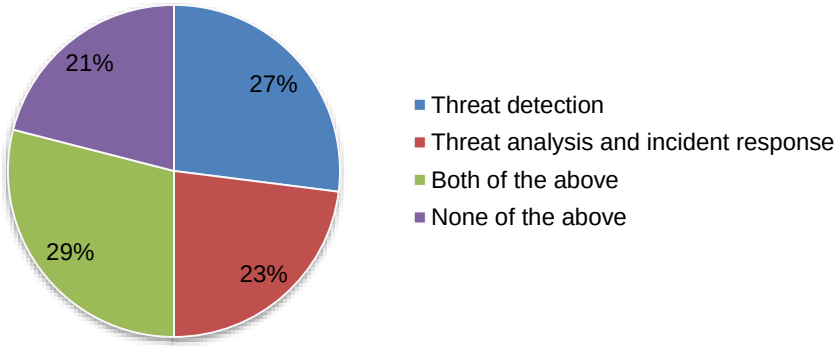


B. Current capabilities to preempt, detect, and respond to resident attackers

A second set of questions in the survey look at operational strengths and weaknesses across the incident lifecycle, from detection to incident escalation and response, and also at capabilities to inhibit the ability of attackers to move laterally and harden the environment against future attacks.

Most organizations rely on outside expertise. How much are organizations trying to be self-reliant, versus engaging MSSPs, MDR services, or other third parties for threat detection and incident response? It is notable that only 21% of organizations are "going it alone." Also notable is that more than half (a total of 52 percent) are already using service providers for analysis and incident response.

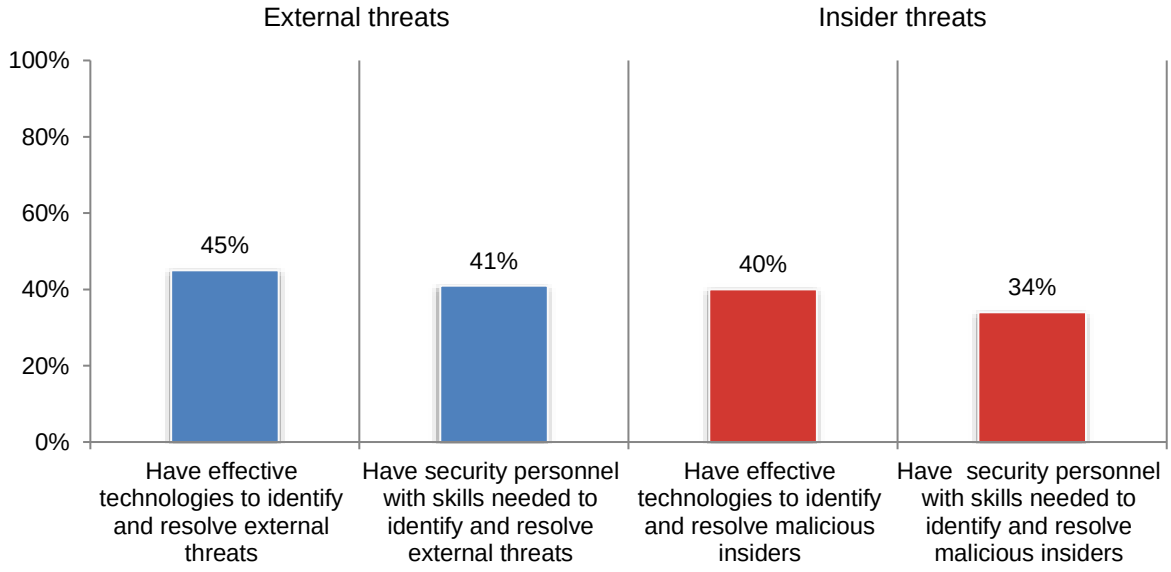
Figure 9. Use of MSSPs, MDRs and other third parties



Organizations are more confident in their ability to handle attacks by external actors compared to insiders. As shown in Figure 10, 45 percent of respondents agree or strongly agree that their technologies are effective in identifying and resolving external threats that have penetrated their defenses, whereas only 40 percent of respondents feel confidence in their technologies used to detect malicious insiders. Similarly, on the skills front, organizations feel better equipped to address outsiders over insiders.

Figure 10. Capabilities to identify and resolve threats and risks

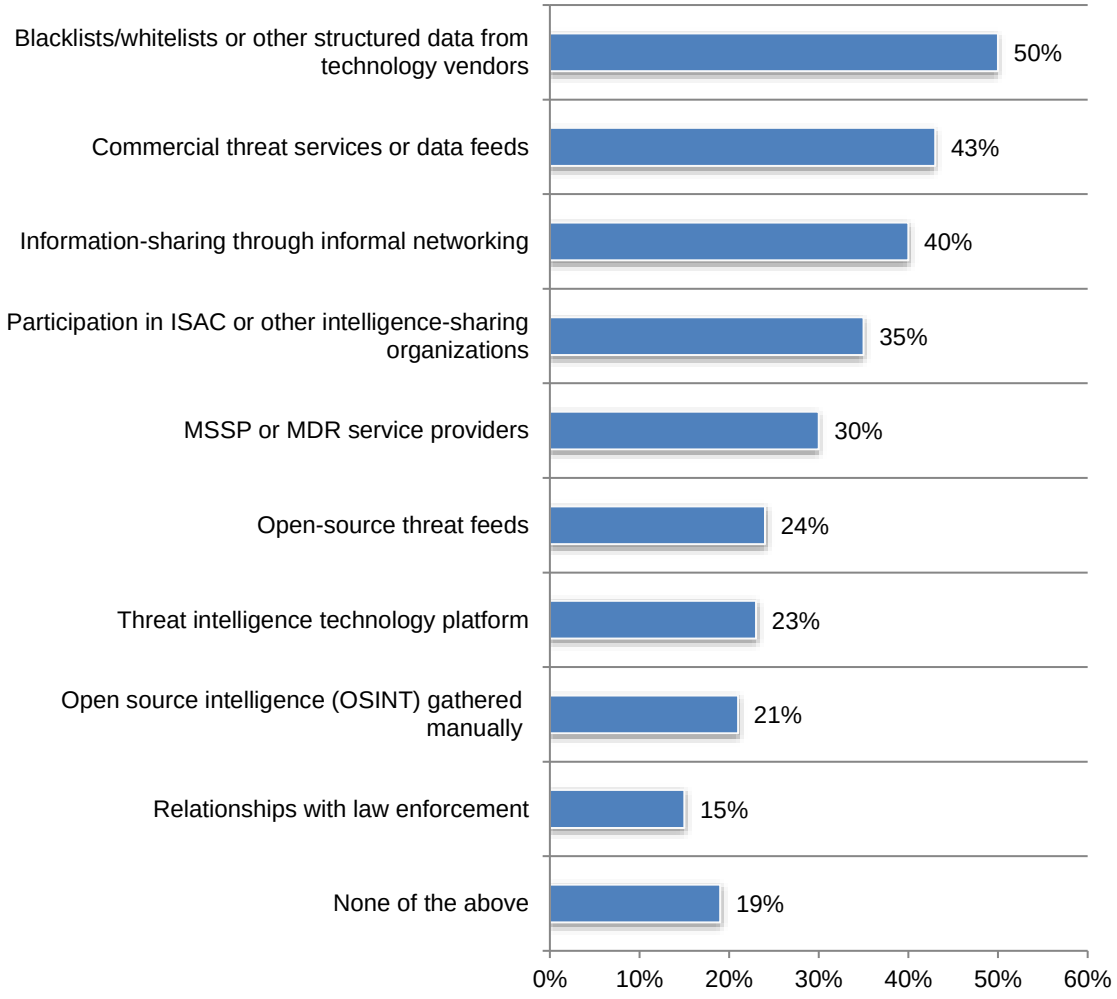
Strongly agree and agree responses combined



Blacklists/whitelists or other structured data from technology vendors are considered the most important threat intelligence. As shown in Figure 11, 50 percent of respondents say their organizations use blacklists/whitelists or other structured data from technology vendors and 43 percent of respondents say they use commercial threat services or data feeds to plan preventive measures, detect threats and resolve security incidents.

Figure 11. What sources of threat intelligence are most important to planning preventive measures, detecting threats and resolving security incidents?

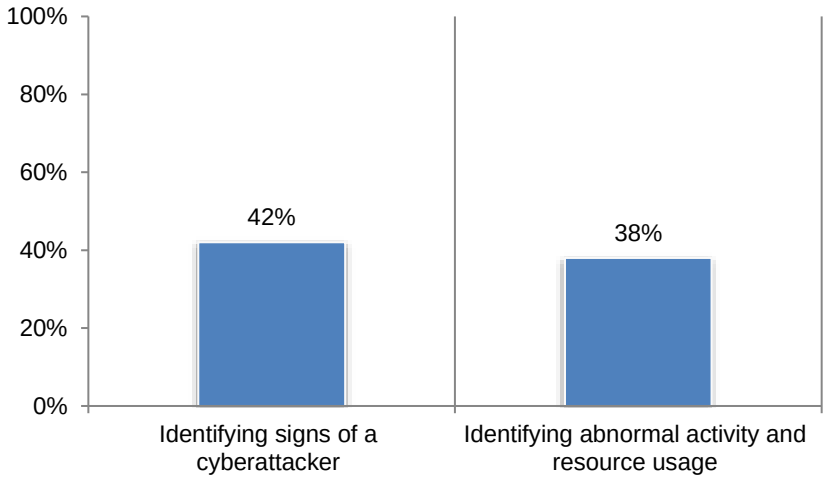
Three responses permitted



The ability to detect "stealth" attackers is lower than it needs to be. As shown in Figure 12, only 42 percent of respondents say their IT security team is doing a good job knowing if there is a cyberattacker within their environment, and effectiveness in identifying abnormal activity and resource usage scores even lower (38 percent of respondents).

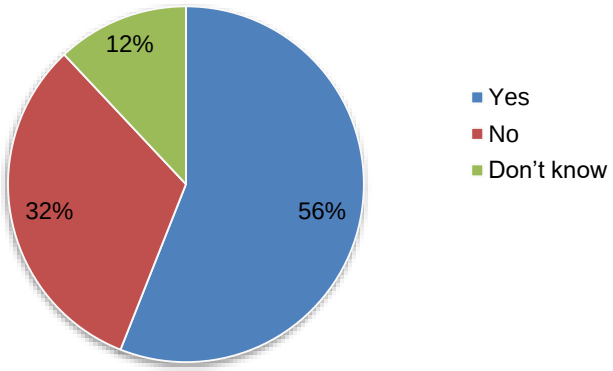
Figure 12. Effectiveness in identifying cyberattackers and abnormal activity

1 = not effective to 10 = very effective, 7+ responses presented



Detection is also slower than it needs to be. Being able to detect is one thing, but because damage can increase with every system the attacker touches, detection needs to happen as early as possible. Figure 13 indicates that while more than half of respondents believe they have reduced dwell time in the past year, 44% either have not or don't know.

Figure 13. Have you reduced attacker "dwell time" over the past year?

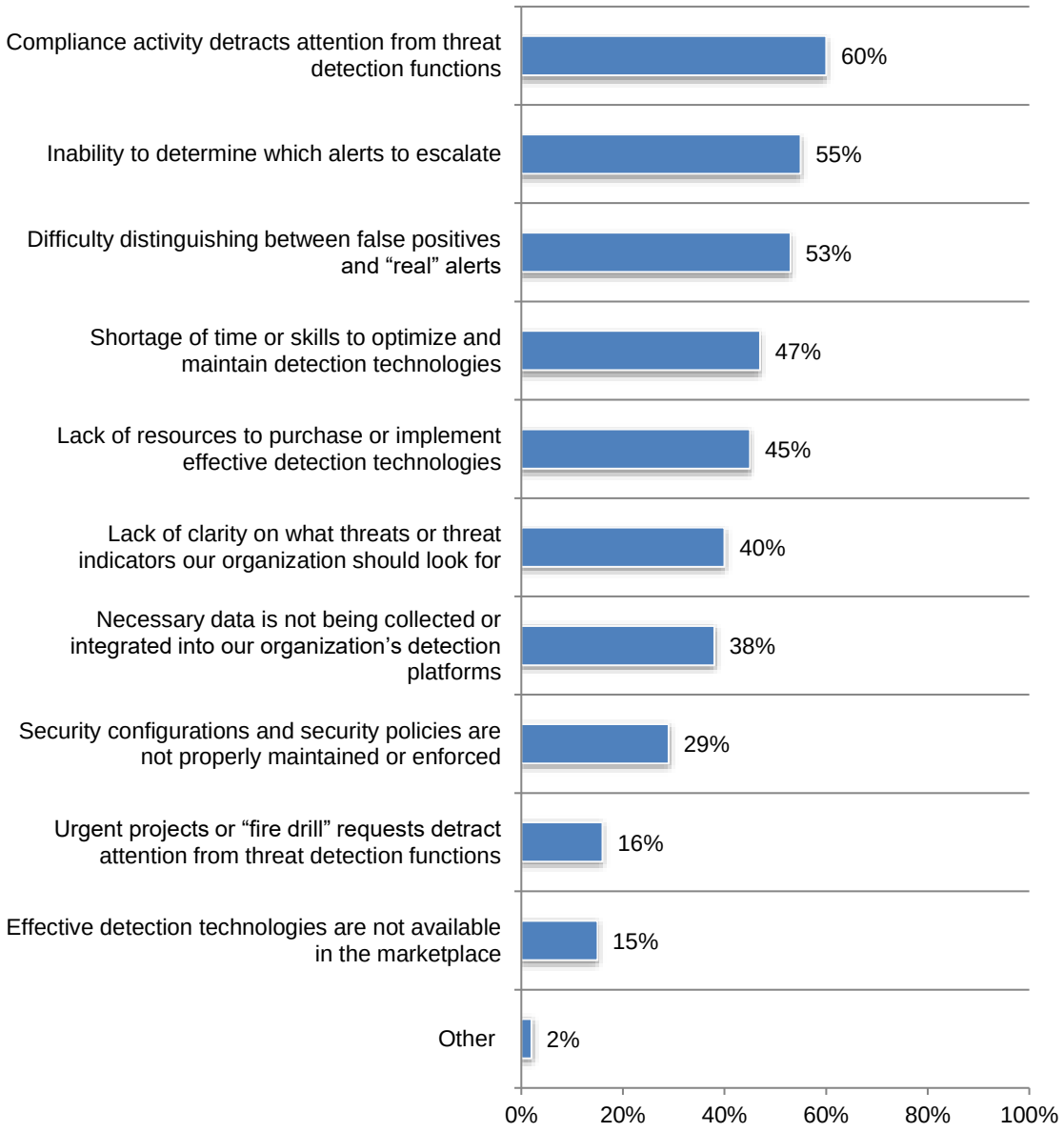


Compliance activity takes attention away from effective threat detection. Figure 14 presents a list of barriers to effectively detecting cyber attackers operating within the network. While frequently-cited issues relating to "noise" in the SOC rank high, the most-cited barrier to more effective detection (by 60 percent of respondents) is that compliance activity prevents the IT security team from fulfilling threat detection functions.

Perhaps reflecting the previously noted weakness in optimizing security technologies to reduce top business risks, the second most commonly cited barrier to effective detection is the inability to determine which alerts to escalate (55 percent of respondents).

Figure 14. Obstacles to an organization's ability to detect cyberattackers within its network

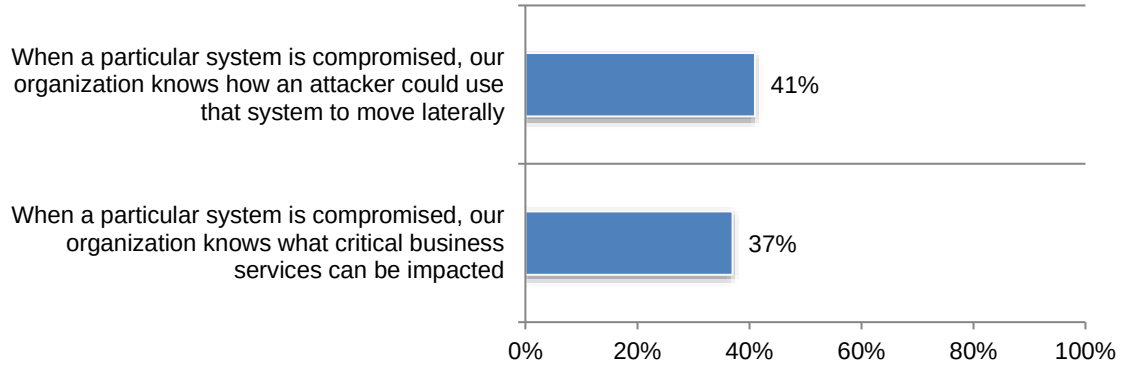
Four responses permitted



Inability to choose which alerts to escalate may be more than a "needle in the haystack" issue. While there may be too much "noise" in the SOC, seeing what's important may be as much about lack of contextual insights needed to prioritize response. When a particular system is compromised, only 41 percent of respondents agreed or strongly agreed that their organization would know how an attacker could use that system to move laterally in the environment. Fewer felt strong in their ability to know what critical business services could be impacted.

Figure 15. Key capabilities for incident escalation

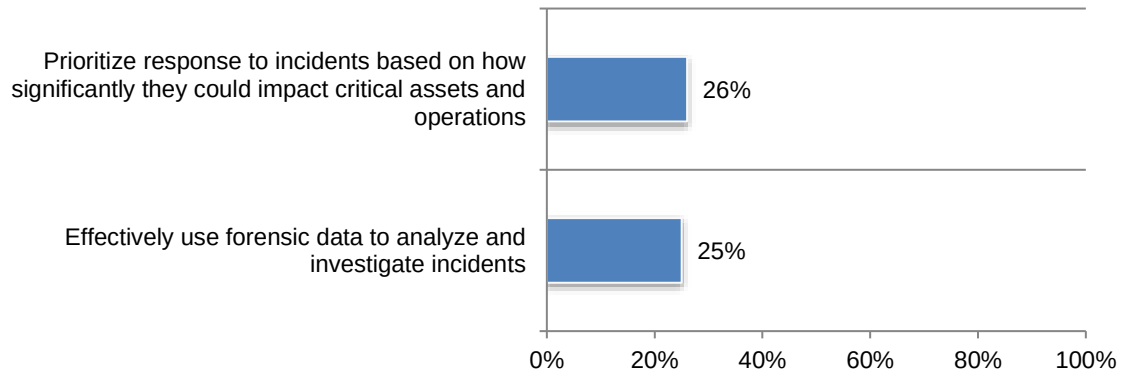
Strongly agree and agree responses combined



Incident response may be the weakest link in the risk mitigation chain. Gaps on the incident response side may explain why more than half (52 percent) of respondents' companies use service providers for analysis and incident response (see Figure 9). Figure 16 shows that when asked to rate their ability to use forensic data to analyze and investigate incidents, only 25 percent rated their organizations at 7 or more on a scale of 1 to 10. An almost equal number rated themselves at that level on their ability to prioritize response based on business criticality.

Figure 16. Ability to use forensic data and prioritize response to incidents

1 = no ability to 10 = high ability, 7+ responses presented



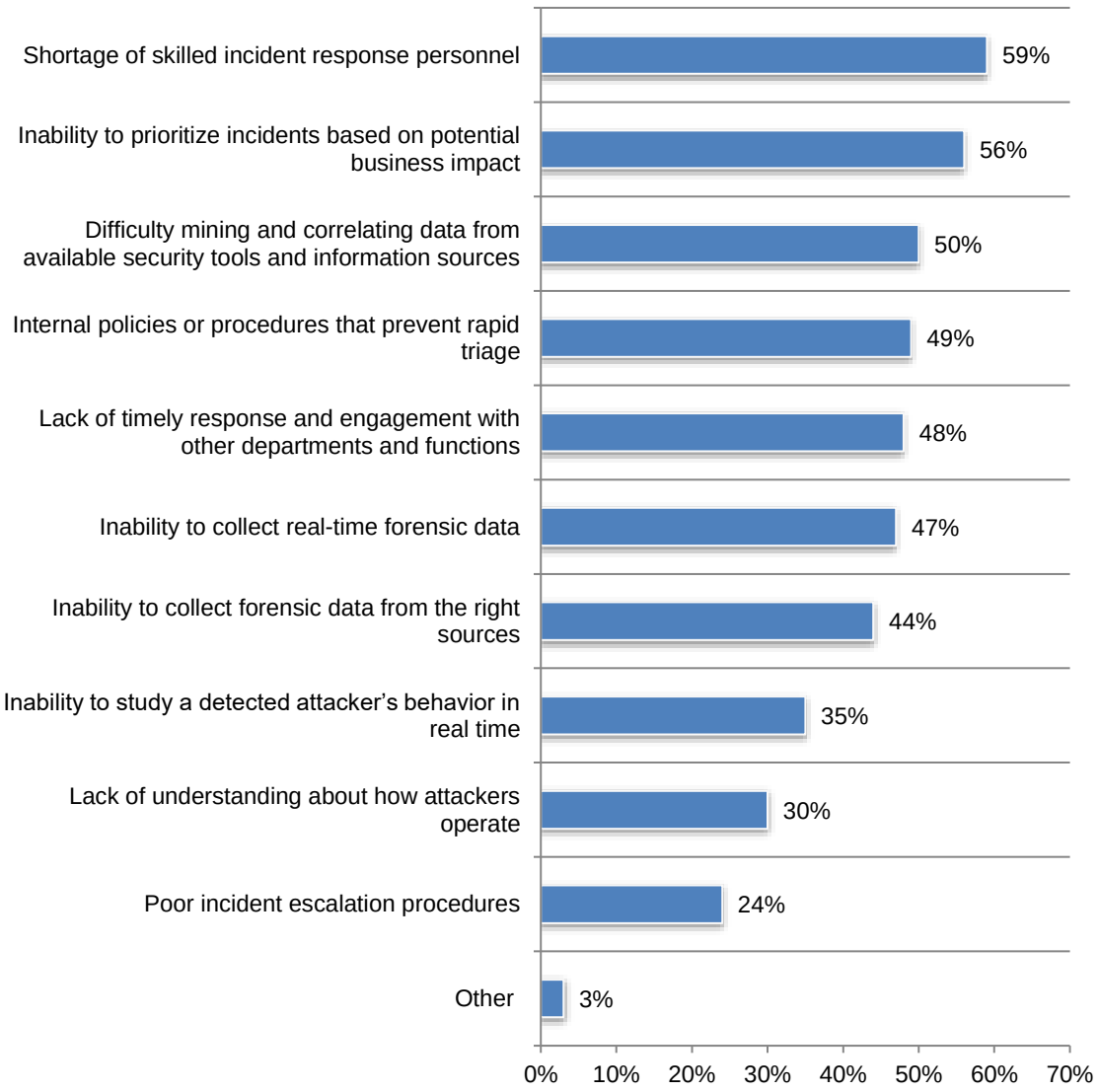
Incident response is another area where communication and alignment between security and business functions may be a problem—especially when a crisis calls for executive action. As previously shown in Figure 5, less than one-third of respondents agree or strongly agree that they have well-defined criteria for when to involve business leaders in a security incident.

Incident response suffers from people, process and technology gaps. While in Figure 14, 47 percent of respondents cite shortage of time or skills as an inhibitor to better threat detection, Figure 17 shows that the "people" gap is even higher on the incident response side, with 59 percent of respondents indicating shortage of skilled personnel as an inhibitor to better cyberattack response.

The second most cited obstacle to better incident response reflects the familiar risk alignment refrain: 56 percent of respondents cite the inability to prioritize incidents based on potential business impact. Fifty percent of respondents cite difficulty mining and correlating data. Close behind, in fourth and fifth place, are two process-oriented obstacles: policies and procedures stand in the way of rapid triage (49 percent of respondents) and engagement with other departments and functions (48 percent of respondents) causes delays.

Figure 17. Which of the following are obstacles to your organization's ability to effectively respond to cyberattacks?

More than one response permitted

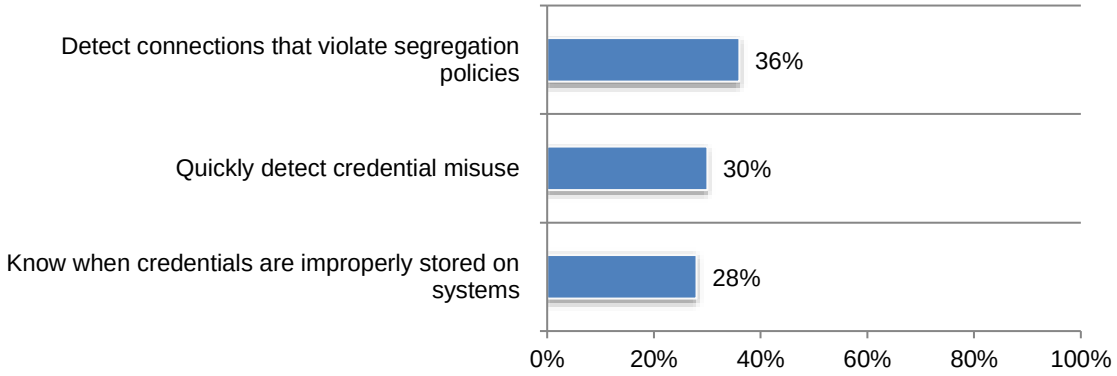


It is too easy for attackers to find connections and credentials that enable lateral movement. Although establishing preventive controls to keep attackers out of corporate networks has always been a top priority, preventive action to reduce attacker mobility inside the network should perhaps be the next frontier for investment. Once inside, an attacker looks for credentials and connections to other systems that can be leveraged to progress the attack.

When asked whether their organizations could quickly identify misuse of credentials, only 30 percent of respondents rated their capabilities at 7 or more. Only 28 percent of respondents rated at that level their organizations' ability to determine when credentials are being improperly stored on systems. Slightly more—36 percent of respondents—rated themselves at 7 or higher in their ability to detect rogue system connections.

Figure 18. Ability to identify misuse of credentials and detect rogue system connections

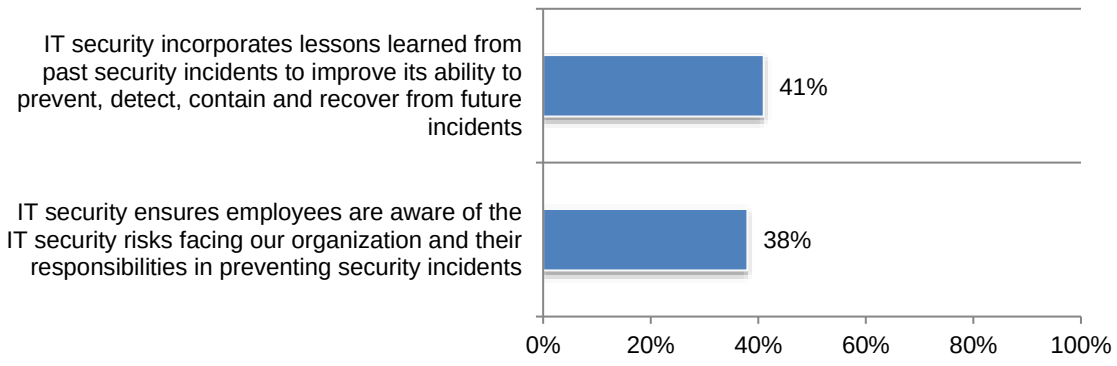
1 = no ability to 10 = high ability, 7+ responses presented



Prevention gaps need attention at both ends of the incident lifecycle. Persistent or advanced attacks typically begin with some form of human manipulation to establish a beachhead. As shown in Figure 19, only 38 percent of respondents agree or strongly agree that their organization's security function ensures that employees do their part to prevent security incidents. The "lessons learned" loop at the tail end of an incident is probably being missed within many organizations. Only 41 percent of respondents agree or strongly agree that their security team effectively incorporates lessons from security incidents to improve the organization's ability to prevent, detect and respond to future ones.

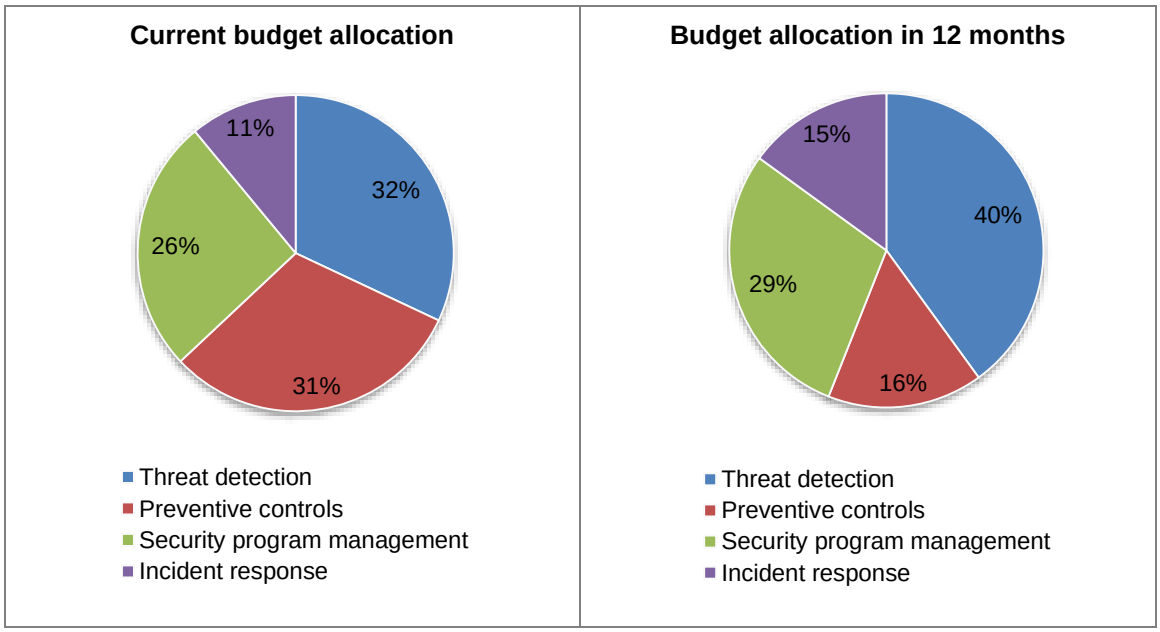
Figure 19. Reducing post-breach attack risk across the incident lifecycle

Strongly agree and agree responses combined



Budget balance shifts toward threat detection. Fifty-six percent of respondents expect their IT security budget to increase an average of 20 percent. Whereas current-year budgets have been relatively balanced between preventive controls and threat detection, that is expected to shift significantly over the coming year. As shown in Figure 20, threat detection will receive the greatest increase in allocation, while the share of budget dedicated to preventive controls is expected to decrease—by almost half on a proportional basis. Incident response and program management (including assessment, design, planning, project management and reporting) will increase more modestly.

Figure 20. IT security budget allocation



C. Takeaways: Toward better risk mitigation for resident or post-breach attacks

A comprehensive program for mitigating risks associated with resident attacks has many facets. This survey provides broad visibility into some areas of relative strength and weakness common to many organizations. The indicator (in Figure 20) that respondents plan to tilt spend toward threat detection is a welcome and necessary shift when, today, only slightly more than one-third of respondents appear confident in their organizations' ability to prevent serious damage from cyber incidents once attackers have established a presence in the network.

Capabilities to preempt, detect and respond need to be strengthened across the board
Because preventive controls can't keep all attackers out, cyber programs need to anticipate the presence of attackers within—both insider threats and external actors—and drive improvements in their abilities to:

- **Preempt** – Undertake proactive measures to improve hygiene to make the environment more difficult for the attacker to operate in.
- **Detect** – Identify signs of attacker presence as close to their initial beachhead ("patient zero") as possible.
- **Respond** – Act efficiently to stop attacks in progress while reducing disruption to the business.

Respondents were asked to rate themselves on a number of capabilities associated with these categories. While each would be worth a dedicated survey, comparing the skeletal data in Figures 12 (detect), 16 (respond) and 18 (preempt) provides some useful high-level insights:

- Organizations seem to feel most confident in their detection capabilities, with roughly 40% rating themselves at 7 or above.
- On the response side, 7+ responses fall off to about the 25% mark.
- In the preempt category, which includes the ability to minimize conditions that enable an attacker to move laterally, the 7+ responses fall in between; organizations seem better at detecting improper system connections than they are at managing credential-related issues.

Given the potentially dire consequences and costs that cyberattacks can have, it appears that all areas need significant improvement in most organizations.

Weak business risk alignment is a primary problem

Realignment of cybersecurity priorities and improvements at the operational levels, alone, will not improve the ability to stop resident attackers from causing serious business impact. It is not enough that technical experts understand the cyberthreat landscape, know what threat indicators to look for, deploy the right detection tools, and so on.

Data in this survey echo the familiar refrain that the SOC is too noisy and that there is a general shortage of resources to keep up with threats. “Inability to determine which alerts to escalate” and “difficulty distinguishing between false positives and real alerts” (Figure 14) are among the top three obstacles to better threat detection. Talent shortages continue to be a top problem for many; “shortage of skilled incident response personnel” (Figure 17), “shortage of time or skills to optimize and maintain detection technologies” and “lack of resources to purchase or implement effective detection technologies” (Figure 14) are significant inhibitors. And while compliance imperatives may help ensure a baseline of standard security practices, the burden they place on limited resources is named as the number one obstacle to better threat detection.

The security team’s job is never close to being done. Given the resource squeeze, the challenge to make sense of mountains of security data, the matrix of technologies to be maintained, and the ease with which a single machine can become infected with malware, important alerts get missed; proactive improvement efforts get postponed. To stop resident attackers before serious damage occurs—to know how to focus routine maintenance, monitoring functions, alert escalation, or incident response—requires the ability to prioritize based on level of importance to the business.

This survey indicates serious alignment gaps:

- Nearly three quarters of respondents say business leaders do not clearly communicate business risk priorities and more than two-thirds don’t have a good understanding of how threats can impact the enterprise
- Security leaders are not included often enough in the planning of new technology and business initiatives
- Security technologies in most organizations are not optimized to reduce top business risk
- Only one-third have strong capabilities to maintain an inventory of business-critical systems

All too often the assertion is made that IT security needs to “align to the business.” The decree is one thing; getting there is very challenging. This survey suggests that the disconnect has very direct operational impact. For example:

- An inability to prioritize incidents based on potential impact is cited as the second most significant obstacle to better incident response.
- Only 37 percent feel agree that when a system is compromised, they know what critical services may be impacted
- Only one-third of respondents rate highly their knowledge of where critical data are stored.
- Most companies apparently lack clear criteria for when to escalate a security incident to business leaders.

There is no universal formula for improving risk alignment, but one near-universal statement can probably be made: for organizations that are struggling in this area, unless operational capabilities can be better prioritized by likely business impact, many other problems in the ability to protect against resident attackers will likely persist because there are simply not enough resources to handle everything equally.

Sharpen focus on the lateral movement process

In most cases, attackers operating within the environment are so difficult to detect specifically because they leverage the connectivity that the business itself enables, and thereby remain relatively invisible. Presumably, ongoing or accelerating interest in SIEM technology, security analytics, user and entity behavior and analytics (UEBA), network traffic analysis (NTA) and various "next gen" security technologies is driven by the search for practical solutions to this problem, though they were not necessarily built for this purpose.

There is no such thing as zero risk in today's fast-changing environment. It is therefore important to weigh the benefits of an "ultimate" solution that—while well-conceived—may be time-consuming to build, and one that delivers rapid value in mitigating the majority of higher-impact threats. Threats evolve so rapidly that in many cases a "perfectly" designed detection solution is obsolete by the time it is actually implemented.

Organizations may derive the greatest risk reduction by focusing hygiene and detection mechanisms on the lateral movement process itself, and by leveraging mechanisms that help prioritize protection of critical business services and assets. Some efforts to consider:

- **Attend to "hidden" credentials in the environment.** During normal business activity, credentials remain persistent in many ways, some intentionally, but mostly by accident. While maintaining strong access controls is essential, traditional identity and access management (IAM) and privileged access management (PAM) products provide very limited visibility on this problem and should be augmented by other approaches. If it is not possible to prevent the presence of all attackers, it *is* possible to reduce their mobility within the environment by keeping it as clean as possible of excess connectivity by removing, where possible, credentials that are cached on systems, with special attention to domain admins and other high-privilege credentials.

- **Strengthen visibility on how endpoints are connected to critical business systems.** When an attack occurs, responders would ideally see where, from a connectivity standpoint, the compromised systems sit in relation to high-value assets. Organizations that don't have this contextual risk visibility today could work to begin to establish it for at least some of the most essential operations within the business. When alert fire that are associated with systems in these pathways, they can be prioritized, helping to cut through "noise" in the SOC.

- **Consider endpoint-based deception.** Different than the function of honeypots, these solutions are designed to detect the behavior that attackers must engage in while trying to move laterally. Setting thresholds for failed login attempts—a staple detection use case—is one technique in this direction, but it covers only one small aspect of what attackers might do

in trying to traverse the network and generates an overwhelming number of alerts. Distributed deception technologies place fake information that would be interesting to an attacker conducting reconnaissance or “beachhead introspection”, or making trial-and-error attempts to move from one system to another. Alerts generated in this process are sure-fire signals of activity that is likely to be malicious.

- **Look for endpoint-based products that integrate collection of forensics and empower non-expert responders.** Instant capture of forensics at the moment of detection both preserves important data and accelerates response times. Vendors should be expected to provide greater forensic intelligence, formatted and enriched in ways that enable analysts at all levels, including more junior ones.

- **Rehearse incident response.** Although it is not possible to perfectly predict the impact a cyberattack will have, practicing response to a potential crisis—from the executive level to the analyst level—will help organizations be better equipped to handle the decisions that need to be made under pressure, and will also help improve risk alignment and garner the business-level engagement necessary for proactive program improvements.

About Illusive Networks

Illusive Networks is a pioneer of deception-based cybersecurity, empowering security teams to take informed action against high-impact cyberattacks by detecting and disrupting lateral movement toward critical business assets early in the attack life cycle. Agentless and driven by intelligent automation, Illusive technology enables organizations to significantly increase proactive defense ability while adding almost no operational overhead. Illusive’s Deceptions Everywhere® approach was conceived by cybersecurity experts with decades of combined experience in cyber warfare and cyber intelligence. With the ability to proactively intervene in the attack process, technology-dependent organizations can preempt significant operational disruption and business losses, and function with greater confidence in today’s complex, hyper-connected world. For more information, visit us at **www.illusivenetworks.com** or contact info@illusivenetworks.com.

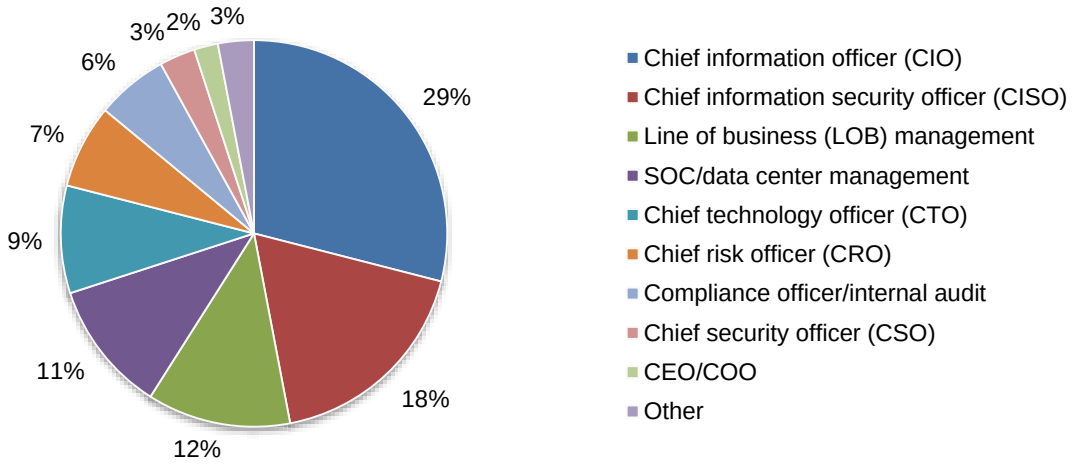
Part 3. Methods

A sampling frame of 17,100 IT and IT security practitioners located in the United States was selected as participants in this survey. To ensure knowledgeable responses, all respondents are involved in the evaluation, selection and/or implementation of IT security solutions and governance practices. Table 2 shows 686 total returns. Screening and reliability checks required the removal of 59 surveys. Our final sample consisted of 627 surveys or a 3.7 percent response.

Table 2. Sample response	Freq	Pct%
Total sample frame	17,100	100%
Total returns	686	4.0%
Rejected surveys	59	0.3%
Final sample	627	3.7%

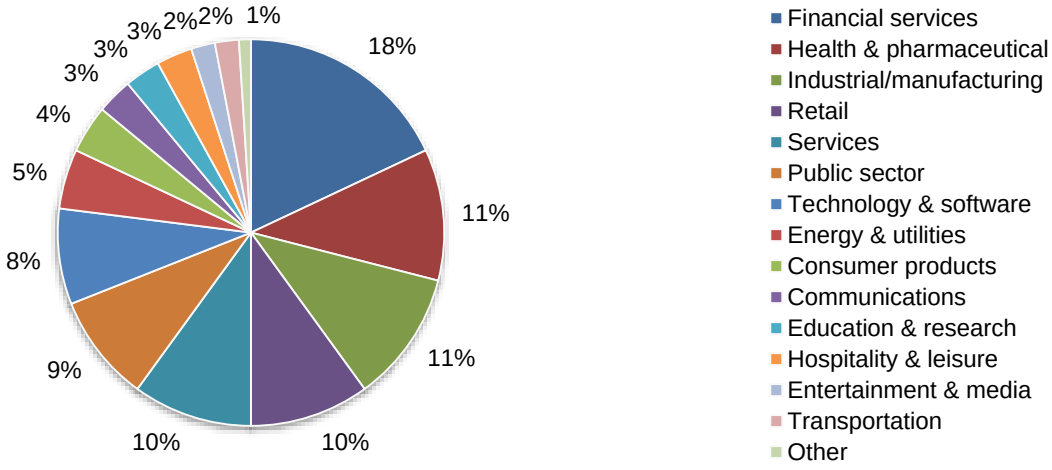
As shown in Pie Chart 1, 29 percent of respondents report to the chief information officer, 18 percent of respondents report to the chief information security officer, 12 percent of respondents report to line of business management and 11 percent of respondents report to the SOC/data center management.

Pie Chart 1. Primary person you or your leader reports to



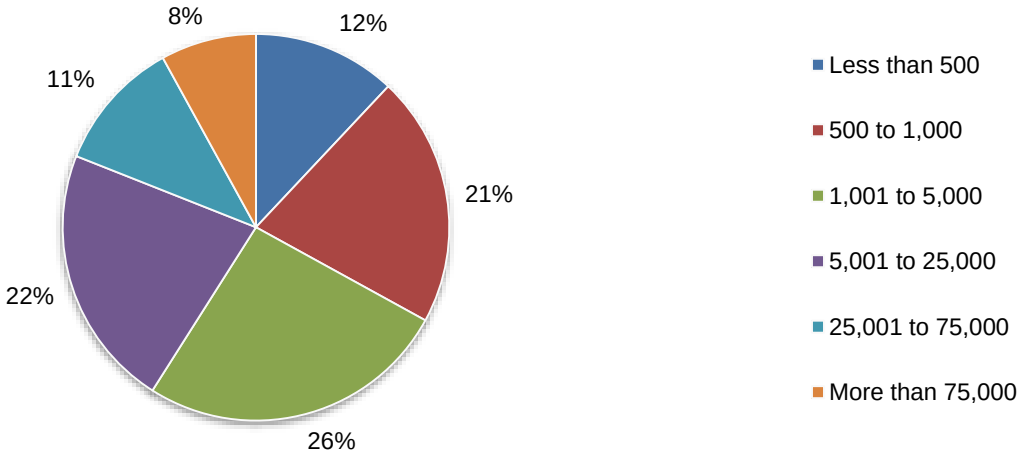
Pie Chart 2 reports the industry sectors of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest sector, followed by health and pharmaceuticals (11 percent of respondents), industrial/manufacturing (11 percent of respondents), retail (10 percent of respondents) and service sector (10 percent of respondents).

Pie Chart 2. Industry distribution of respondents' organizations



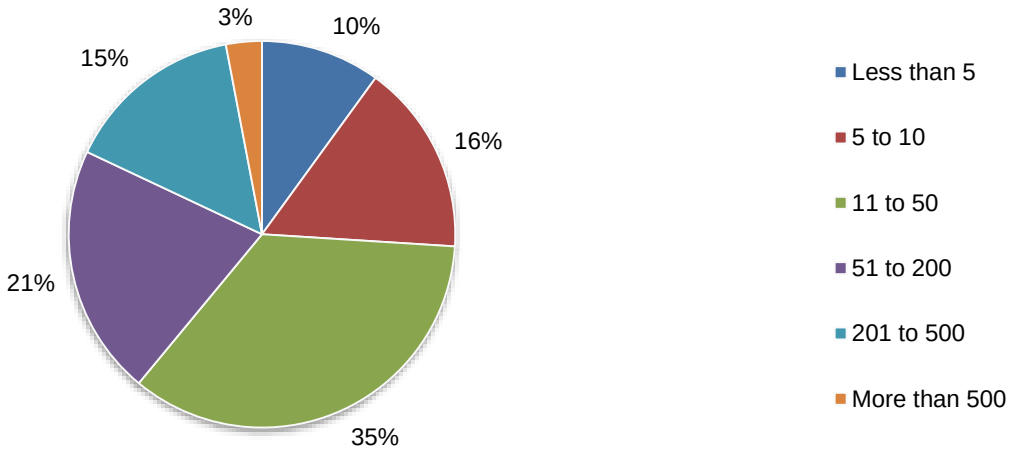
As shown in Pie Chart 3, 67 percent of respondents are from organizations with a global headcount of more than1,000 employees.

Pie Chart 3. Worldwide headcount of the organization



Pie Chart 4 reports the number of individuals the respondents' organization has dedicated to cybersecurity. Fifty-six percent of respondents indicated their organization has between 11 and 200 dedicated cybersecurity staff.

Pie Chart 4. The number of individuals dedicated to cybersecurity



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 IT and IT security practitioners who are involved in the evaluation, selection and/or implementation of IT security solutions and governance practices. 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 from July 19, 2018 to August 3, 2018.

Survey response	Freq	Pct%
Total sample frame	17,100	100.0%
Total returns	686	4.0%
Rejected surveys	59	0.3%
Final sample	627	3.7%

Part 1. Screening

S1. How familiar are you with threat detection technologies deployed by your company?	Pct%
Very familiar	31%
Familiar	39%
Somewhat familiar	30%
Not familiar (stop)	0%
Total	100%

S2. What best describes your role in managing the IT security function or activities within your organization? Check all that apply.	Pct%
Setting IT security priorities	53%
Managing IT security budgets	47%
Selecting vendors and contractors	56%
Determining IT security strategy	32%
Evaluating program performance	60%
None of the above (stop)	0%
Total	248%

S3. How do you rate your level of involvement in the evaluation, selection, and/or implementation of IT security solutions and governance practices within your organization?	Pct%
Very high level of involvement	27%
High level of involvement	40%
Moderate level of involvement	33%
Low level of involvement (stop)	0%
Not involved (stop)	0%
Total	100%

S4. What organizational level best describes your current position?	Pct%
Senior executive	5%
Vice president	7%
Director	27%
Manager	31%
Supervisor	30%
Technician (stop)	0%
Staff/analyst (stop)	0%
Contractor (stop)	0%
Total	100%

Part 2. Executive cyber risk involvement

Please rate the following statements using the 5-point scale provided below each item. **Strongly Agree and Agree response combined**.	Pct%
Q1a. Our organization's executives and senior management consider IT security risk a top business risk.	56%
Q1b. Our organization's executives and senior management understand that security controls are not 100 percent effective.	35%
Q1c. Our organization's executives and senior management understand that the risk of a successful cyberattack needs to be an ongoing concern.	40%
Q1d. Our organization's executives and senior management have a good understanding of persistent and advanced threats and how they can have a negative impact on the enterprise.	32%
Q1e. Our organization's executives and senior management clearly communicate their business risk management priorities to IT security leadership.	29%

Q2. What types of cyberattacks pose the greatest risk to your business? Please select the top 5.	Pct%
Data breach involving customer PII, EHI, or payment data	45%
Data breach involving information about our employees	30%
Data breach involving our clients' proprietary information	56%
Exposure of my company's intellectual property or strategic information	55%
Theft of my company's customer list or marketing data	39%
Data breach that could threaten executive safety or privacy	51%
Tampering with or compromising to the integrity of our products or services	60%
Destruction or manipulation of financial data	27%
Disruption of our core business network	58%
Disruption/destruction of connected devices (such as biomedical technologies, controls systems, robotic devices, automatic teller machines)	43%
Tampering with customer-facing web applications	32%
Other (please specify)	4%
Total	500%

Q3. What best describes how your organization's executives view cybersecurity? Please select only two top responses.	Pct%
Cybersecurity is a top business risk because a cyberattack could pose a strategic or existential threat to our organization.	40%
By proactively addressing cybersecurity at the leadership level, we can better ensure the success of the strategic initiatives that are important to our mission.	24%
Cybersecurity risks are quantifiable and can be factored in as a cost of doing business.	30%
Cybersecurity investments are important for demonstrating diligence to auditors, investors and clients/customers/consumers/citizens.	21%
Cybersecurity is an important building block of our organization's overall IT function.	36%
Cybersecurity is addressed on an as-needed basis when problems arise.	49%
Total	200%

Q4. Who is most involved from IT security in the organization's business risk management? Plesase provide your one top response.	Pct%
Chief Information Officer	32%
Chief Information Security Officer	29%
Chief Security Officer	3%
Chief Risk Officer	12%
Chief Technology Officer	11%
Other Senior Technology Leader	10%
Other (please specify	3%
Total	100%

Q5. Has your organization purchased, or does it plan to purchase, cyber insurance?	Pct%
Yes, we currently have a cyber insurance policy	31%
We are planning to purchase cyber insurance in the next six months	16%
Yes, we are planning to purchase cyber insurance within the next year	24%
No, we do not plan to purchase cyber insurance	29%
Total	100%

Part 3. Business and IT security collaboration. Strongly Agree and Agree response combined.	Pct%
Q6a. Our organization's executives and senior management respect our IT security leaders.	51%
Q6b. Our IT security leaders are proactively included in planning and decision-making for new technology and business initiatives.	35%
Q6c. Our IT security leaders regularly educate business leaders on cyber risks that may impact our organization.	38%
Q6d. Our organization's IT security leaders effectively align security investments, processes and controls with top business risks.	29%
Q6e. Our organization's security team has up-to-date knowledge of which data, systems and infrastructure components support critical business processes.	54%
Q6f. Our organization's security team has the support it needs from business teams to design and execute business-oriented threat detection and incident response capabilities.	37%
Q6g. Our organization's IT security leaders have well-defined criteria for determining when to involve business leaders in responding to a cybersecurity incident or issue.	30%

Part 4. Security capabilities

Q7. Does your IT security team attempt to quantify and track the company's IT security posture?	Pct%
Yes, we have a fairly mature measurement and metrics program	27%
Yes, we have a partial program in place	39%
No, we do not quantify and track the company's IT security posture	30%
Unsure	4%
Totals	100%

Q8. Do you use a managed security services (MSSP/MDR) or other third party for any of the following purposes?	Pct%
Threat detection	27%
Threat analysis and incident response	23%
Both of the above	29%
None of the above	21%
Total	100%

Please rate the following statements using the 5-point scale provided below each item. **Strongly Agree and Agree response combined**.	Pct%
Q9a. Our organization's IT security technologies are optimized to reduce top business risks.	28%
Q9b. Our IT security team is effective in detecting and investigating cybersecurity incidents before serious damage occurs.	36%
Q9c. My organization has effective technologies to quickly identify and resolve external threats that have penetrated our defenses.	45%
Q9d. Our IT security personnel have the skills needed to identify and resolve external threats that have penetrated our defenses.	41%
Q9e. Our organization has effective technologies to quickly identify and resolve malicious insider activity.	40%
Q9f. Our IT security personnel have the skills needed to identify and resolve malicious insider activity.	34%

Q10. What sources of threat intelligence are most important in your ability to plan preventive measures, detect threats, and resolve security incidents? Please select the top three.	Pct%
Open source intelligence (OSINT) gathered manually	21%
Open-source threat feeds	24%
Information-sharing through informal networking	40%
Participation in ISAC or other intelligence-sharing organizations	35%
Relationships with law enforcement	15%
Blacklists/whitelists or other structured data from technology vendors	50%
Commercial threat services or data feeds	43%
MSSP or MDR service providers	30%
Threat intelligence technology platform	23%
None of the above	19%
Total	300%

Please rate the following statements using the 10-point scale from 1 = not effective to 10 = very effective.

Q11. How effective is your IT security team in identifying signs of a cyberattacker operating within your environment?	Pct%
1 or 2	12%
3 or 4	19%
5 or 6	27%
7 or 8	23%
9 or 10	19%
Total	100%
Extrapolated value	5.86

Q12. How effective is your IT security team in identifying abnormal activity and resource usage within your environment?	Pct%
1 or 2	14%
3 or 4	22%
5 or 6	26%
7 or 8	20%
9 or 10	18%
Total	100%
Extrapolated value	5.62

Please rate the following statements using the 5-point scale provided below each item. Strongly Agree and Agree response combined.	Pct%
Q13a. When a particular system is compromised, our organization knows how an attacker could use that system to move laterally.	41%
Q13b. When a particular system is compromised, our organization knows what critical business services can be impacted.	37%

Q14. Which of the following are obstacles to your organization's ability to effectively detect cyber attackers operating within its network? Please select the top four.	Pct%
Lack of clarity on what threats or threat indicators our organization should look for	40%
Security configurations and security policies are not properly maintained or enforced	29%
Effective detection technologies are not available in the marketplace	15%
Lack of resources to purchase or implement effective detection technologies	45%
Shortage of time or skills to optimize and maintain detection technologies	47%
Necessary data is not being collected or integrated into our organization's detection platforms	38%
Difficulty distinguishing between false positives and "real" alerts	53%
Inability to determine which alerts to escalate	55%
Compliance activity detracts attention from threat detection functions	60%
Urgent projects or "fire drill" requests detract attention from threat detection functions	16%
Other (please specify)	2%
Total	400%

Q15. Do you believe you have reduced attacker "dwell time" in your environment over the past year?	Pct%
Yes	56%
No	32%
Don't know	12%
Total	100%

Q16. Which of the following are obstacles to your organization's ability to effectively respond to cyberattacks? Please select all that apply.	Pct%
Poor incident escalation procedures	24%
Inability to prioritize incidents based on potential business impact	56%
Lack of understanding about how attackers operate	30%
Shortage of skilled incident response personnel	59%
Inability to collect forensic data from the right sources	44%
Inability to collect real-time forensic data	47%
Inability to study a detected attacker's behavior in real time	35%
Difficulty mining and correlating data from available security tools and information sources	50%
Lack of timely response and engagement with other departments and functions	48%
Internal policies or procedures that prevent rapid triage	49%
Other (please specify)	3%
Total	445%

On a scale of 1 = no ability to 10 = high ability, please rate your organization's ability to achieve the following:

Q17a. Effectively use forensic data to analyze and investigate incidents	Pct%
1 or 2	18%
3 or 4	27%
5 or 6	30%
7 or 8	19%
9 or 10	6%
Total	100%
Extrapolated value	4.86

Q17b. Prioritize response to incidents based on how significantly they could impact critical assets and operations	Pct%
1 or 2	16%
3 or 4	26%
5 or 6	32%
7 or 8	18%
9 or 10	8%
Total	100%
Extrapolated value	5.02

Q17c. Quickly identify the misuse of credentials	Pct%
1 or 2	19%
3 or 4	21%
5 or 6	30%
7 or 8	20%
9 or 10	10%
Total	100%
Extrapolated value	5.12

Q17d. Determine when credentials are being improperly stored on systems	Pct%
1 or 2	21%
3 or 4	18%
5 or 6	33%
7 or 8	19%
9 or 10	9%
Total	100%
Extrapolated value	5.04

Q17e. Detect rogue system connections that violate our organization's network segregation policies	Pct%
1 or 2	9%
3 or 4	17%
5 or 6	38%
7 or 8	18%
9 or 10	18%
Total	100%
Extrapolated value	5.88

Q17f. Maintain an accurate inventory of which IT systems and devices are most critical to the business	Pct%
1 or 2	11%
3 or 4	21%
5 or 6	36%
7 or 8	17%
9 or 10	15%
Total	100%
Extrapolated value	5.58

Q17g.Maintain awareness of where the company's most critical data are stored	Pct%
1 or 2	21%
3 or 4	17%
5 or 6	29%
7 or 8	18%
9 or 10	15%
Total	100%
Extrapolated value	5.28

Q17h. Know what data various users need to access in order to perform their work functions	Pct%
1 or 2	12%
3 or 4	23%
5 or 6	29%
7 or 8	23%
9 or 10	13%
Total	100%
Extrapolated value	5.54

Q17i. Keep employee access controls up to date	Pct%
1 or 2	13%
3 or 4	28%
5 or 6	27%
7 or 8	17%
9 or 10	15%
Total	100%
Extrapolated value	5.36

Please rate the following statements using the 5-point scale provided below each item. Strongly Agree and Agree response combined.	Pct%
Q18a. Our IT security function ensures employees are aware of the IT security risks facing our organization and their responsibilities in preventing security incidents.	38%
Q18b. Our IT security function incorporates lessons learned from past security incidents to improve its ability to prevent, detect, contain and recover from future incidents.	41%

Part 5. Priorities and improvements

Q19a. Will your organization's IT security budget increase in the next 12 months?	Pct%
Yes	56%
No	30%
Unsure	14%
Total	100%

Q19b. If yes, how much will your organization's IT security budget increase?	Pct%
Less than 10%	23%
10% to 15%	33%
16% to 20%	15%
21% to 30%	11%
31% to 40%	7%
41% to 50%	6%
55% to 75%	3%
76% to 100%	2%
Total	100%
Extrapolated value	19.7%

Q20a. Please allocate 100 percentage points to show how your IT security budget **is allocated today**.	Points
Security program management (e.g. assessment, design, planning, project management and reporting)	26
Improvement, management and maintenance of preventive controls	31
Improvement, management and maintenance of threat detection	32
Planning, rehearsal and execution of incident response and remediation activities	11
Total	100

Q20b. Please allocate 100 percentage points to show how your IT security budget **will be allocated** in the next 12 months. Your best guess is welcome.	Points
Security program management (e.g. assessment, design, planning, project management and reporting)	29
Improvement, management and maintenance of preventive controls	16
Improvement, management and maintenance of threat detection	40
Planning, rehearsal and execution of incident response and remediation activities	15
Total	100

Q21a. The following table lists 19 enabling security technologies that may be deployed by your organization. For each item, indicate the relative importance of this technology in stopping successful cyberattacks once an attacker is inside your network. **Very Important and Important response combined**.	Pct%
Access governance systems	56%
Advanced firewalls (e.g., NGFW and UTM)	32%
Big data analytics for cybersecurity	44%
Data loss prevention (DLP)	41%
Distributed deception technology	39%
Endpoint security solutions/EDR	45%
Forensic suite	27%
Honeypots	32%
Identity & access management (IAM)	50%
Incident response orchestration	27%
Intrusion detection systems (IDS)	45%
Intrusion prevention systems (IPS)	43%
Mobile threat prevention	29%
Netflow or network behavior analysis tools	36%
Security incident & event management (SIEM)	46%
Sinkholes	18%
User/employee behavior analytics (UEBA)	26%
VPN or secure gateways	29%
Web application firewalls (WAF)	35%
Total	700%

Q21b. The following table lists 19 enabling security technologies that may be deployed by your organization. Please check all the technologies that **will be purchased** by your organization within the next 12 to 24 months.	Pct%
Access governance systems	65%
Advanced firewalls (e.g., NGFW and UTM)	45%
Big data analytics for cybersecurity	53%
Data loss prevention (DLP)	39%
Distributed deception technology	45%
Endpoint security solutions/EDR	53%
Forensic suite	19%
Honeypots	36%
Identity & access management (IAM)	70%
Incident response orchestration	34%
Intrusion detection systems (IDS)	47%
Intrusion prevention systems (IPS)	45%
Mobile threat prevention	21%
Netflow or network behavior analysis tools	46%
Security incident & event management (SIEM)	60%
Sinkholes	39%
User/employee behavior analytics (UEBA)	48%
VPN or secure gateways	33%
Web application firewalls (WAF)	42%
Total	840%

Part 6. Role and organization characteristics

D1. Check the **Primary Person** you or your leader reports to within the organization.	Pct%
CEO/COO	2%
Chief financial officer (CFO)	0%
General counsel	1%
Chief information officer (CIO)	29%
Chief technology officer (CTO)	9%
Chief risk officer (CRO)	7%
Chief information security officer (CISO)	18%
Compliance officer/internal audit	6%
Human resources VP	0%
Chief security officer (CSO)	3%
Line of business (LOB) management	12%
SOC/data center management	11%
Other (please specify)	2%
Total	100%

D2. What best describes your organization's primary industry sector?	Pct%
Aerospace and defense	1%
Agriculture & food services	0%
Communications	3%
Consumer products	4%
Education & research	3%
Energy & utilities	5%
Entertainment & media	2%
Financial services	18%
Health & pharmaceutical	11%
Hospitality & leisure	3%
Industrial/manufacturing	11%
Public sector	9%
Retail	10%
Services	10%
Technology & software	8%
Transportation	2%
Other (please specify)	0%
Total	100%

D3. What is the worldwide headcount of your organization?	Pct%
Less than 500	12%
500 to 1,000	21%
1,001 to 5,000	26%
5,001 to 25,000	22%
25,001 to 75,000	11%
More than 75,000	8%
Total	100%

D4. How many individuals do you have dedicated to cybersecurity?	Pct%
Less than 5	10%
5 to 10	16%
11 to 50	35%
51 to 200	21%
201 to 500	15%
More than 500	3%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

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.

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.