Hewlett Packard Enterprise

FireEye SECURITY REIMAGINED

Produced by MIT Technology Review Custom in Partnership with Hewlett Packard Enterprise Security Services and FireEye

Cybersecurity Challenges, Risks, Trends, and Impacts: Survey Findings

Executive Summary

IN THIS REPORT

Inside this report are the survey's key findings, accompanied by expert insights, followed by additional results. Insights were provided by:

- Vitor De Souza, Vice President for Global Communications, FireEye Inc.
- Marshall Heilman, Vice President and Executive Director of Red-Team Operations, Mandiant
- Andrzej Kawalec, Chief Technology Officer (CTO), HPE Security Services
- Chris Leach, Chief Technologist, HPE Security Services

No question about it: information security – or, more precisely, the lack of it – is firmly on the radar of business and information-technology (IT) leaders in organizations of all sizes and in every sector. Many executives and managers fear that their companies are ill prepared to prevent, detect, and effectively respond to various types of cyberattacks, while the shortage of in-house security expertise is also a widespread concern.

Those are among the key findings of the February 2016 Cybersecurity Challenges, Risks, Trends, and Impacts Survey. Two hundred and twenty-five business and IT executives, directors, managers, and other leaders participated in the online survey, which was conducted by MIT Technology Review in partnership with Hewlett Packard Enterprise (HPE) Security Services and FireEye Inc.

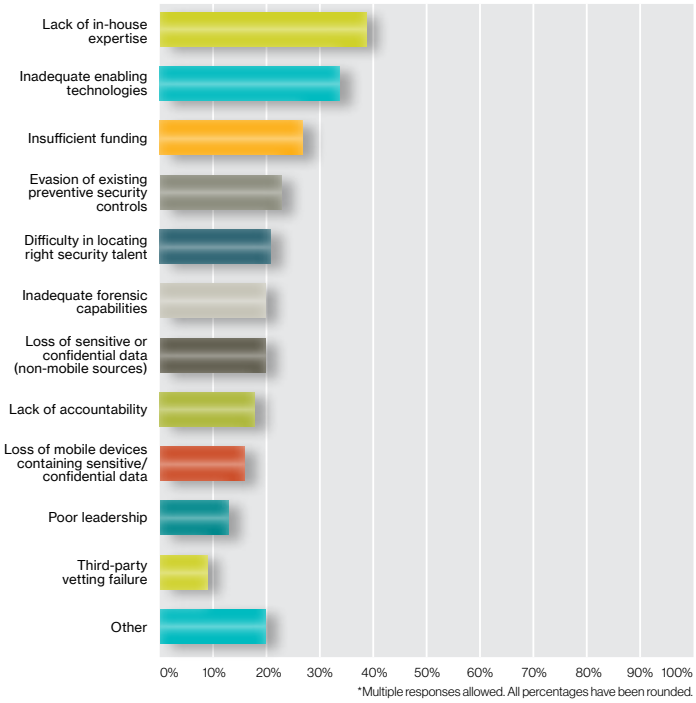
Several key themes have emerged from analysis of the survey results:

- **Few survey participants are fully confident about their ability to respond to security threats.** For instance, fewer than 6 percent of those surveyed believe their organizations are "extremely well prepared" to respond to a security breach involving a major loss of information.
- **Many struggle to hire and retain highly qualified security specialists.** "Lack of in-house expertise" ranks as the single greatest information-security challenge, cited by more than one-third of participants.
- **Most lack information risk-management strategies.** Although many expect to develop them, roughly 25 percent either have no plans to do so or simply don't know whether their organizations have – or eventually will have – such strategies.
- **Most see multiple security threats on the rise.** Areas of greatest concern include threats related to mobile computing, e-mail- or Web-based attacks, and the vulnerabilities created by the bring-your-own-device (BYOD) and bring-your-own-app (BYOA) workplace trends.
- **The majority report experiencing either more or as many data attacks today as in 2014.** Only 7 percent report fewer attacks now than two years ago.
- **Participants cite "lost time and productivity" as the most negative effect from recent breaches.** Other impacts include remediation time and necessary expenditures on consultants and additional technologies.

Information-Security Challenges

Q1: What are your organization's top information-security challenges?*

Finding: For more than a third of the survey respondents, the lack of in-house expertise ranks as the main information-security headache.



*Multiple responses allowed. All percentages have been rounded.

Expert Insight:

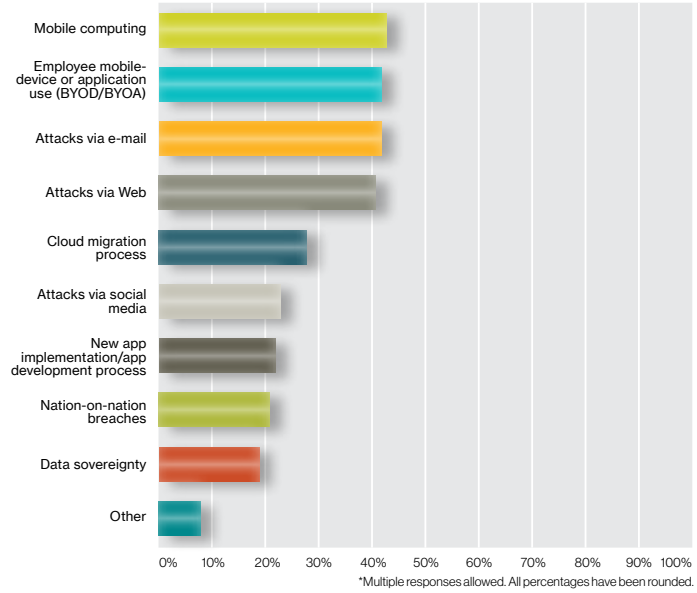
"The combination of new technology adoption, sophisticated adversaries, and disruptive regulation has placed cyber-risk high on every organization's agenda. The top concern of cyber-defense team leadership is attracting and retaining skilled resources. To address the ongoing skills and capability shortages, many organizations look to partners for everything from incident response to managed security services. Trusting a partner with any portion of your security operations is one of the most important decisions an organization can make, as it deals directly with the protection of your critical assets."

— Andrzej Kawalec, HPE Security Services

Information-Security Threats

Q2: Where do you see the most growth in security threats?*

Finding: Respondents perceive mobile computing as the fastest-growing threat to information security, but several other factors rank closely behind.



*Multiple responses allowed. All percentages have been rounded.

Expert Insight:

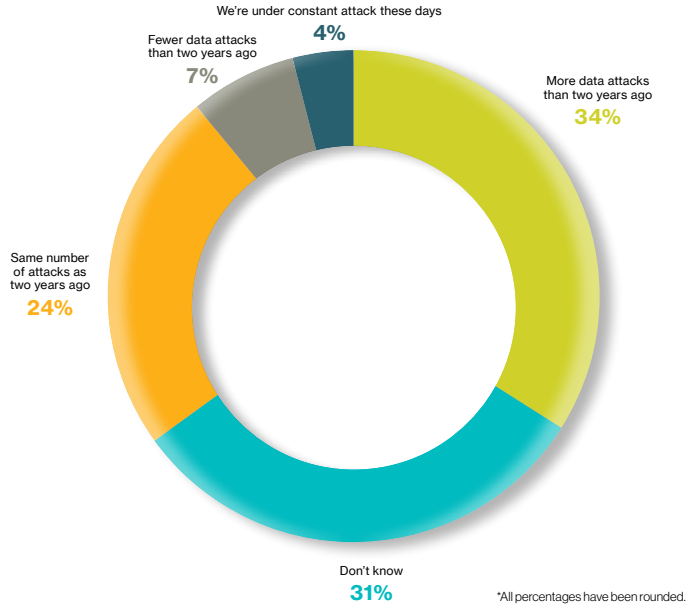
"These survey results accurately portray an issue within the cybersecurity community: namely, that we are more worried about what we don't understand or cannot control than what attackers are actually exploiting. In my experience, mobile computing and devices have the biggest growth potential, but we just haven't seen attacks go that way yet. For instance, when was the last time a major breach that hit the news was caused by the hacking of an employee's personal phone? Companies should spend more time protecting authentication and visibility than worrying about mobile devices. However, I appreciated that respondents ranked attacks via e-mail and the Web close to the top, because attackers are targeting those two areas."

— Marshall Heilman, Mandiant

Attack Frequency

Q3: Across your organization, do you feel that you are experiencing more, fewer, or the same number of data attacks today compared with two years ago?*

Finding: For more than a third of respondents, data attacks are clearly on the rise today, but nearly as many don't know for sure whether they're experiencing more or fewer attacks than they did two years ago. About a quarter of respondents see no change, while a few report being "under constant attack." Only a handful say data attacks have decreased.



*All percentages have been rounded.

Expert Insight:

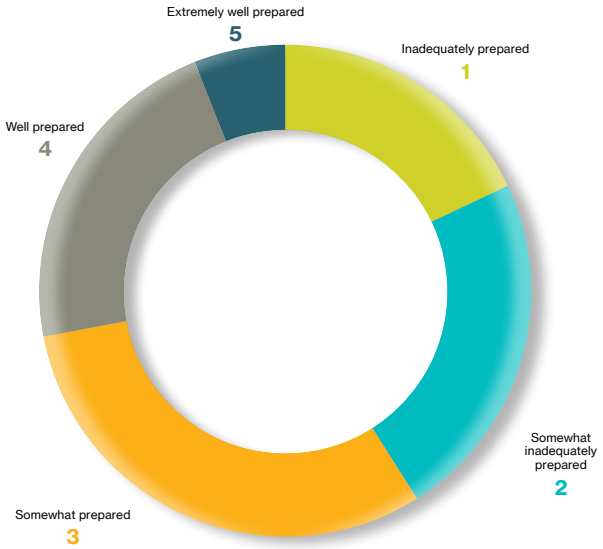
"Attack vectors and methodologies are constantly changing. Unlike the attacks of the past, where the objective was to deface a website or deny service to a site to prohibit business transactions, today's attacks are more nefarious: the objective of many is to go unnoticed. So while it may appear to some that cyberattacks are not as frequent today, they are in fact on the increase. A small shift in the enterprise strategy from a 'defend to perimeter' tradition to one of detecting hidden attacks will provide better protection and enhanced security of critical data."

— Chris Leach, HPE Security Services

Breach Preparedness

Q4: On a scale of 1 ("inadequately prepared") to 5 ("extremely well prepared"), how prepared is your organization to respond to an incident involving a material loss of information?

Finding: Only a handful of survey respondents — fewer than 6 percent — feel their organizations are "extremely well prepared" to respond to a security breach involving serious information loss.



Expert Insight:

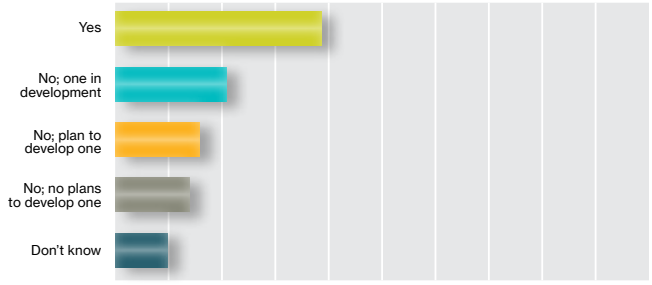
"Since it is no longer a matter of *if*, but *when*, a company will experience a security incident, it is no longer acceptable for a company's management to be unprepared to respond to and communicate the issues around a breach. The faster an organization can identify the root cause and respond to the weakness, the more rapidly the organization will be able to address the weakness and close the gap. This will not only allow for quicker business resumption, but will also instill confidence in customers and key stakeholders that the situation is being handled professionally and with precision."

— Chris Leach, HPE Security Services

Risk-Management Strategies

Q5: Does your organization have an information risk-management strategy?*

Finding: Nearly 40 percent of respondents have information risk-management strategies, and nearly as many are either developing such strategies or plan to do so. However, others either don't know whether their organizations have such strategies or don't expect to develop them.



*All percentages have been rounded.

Expert Insight:

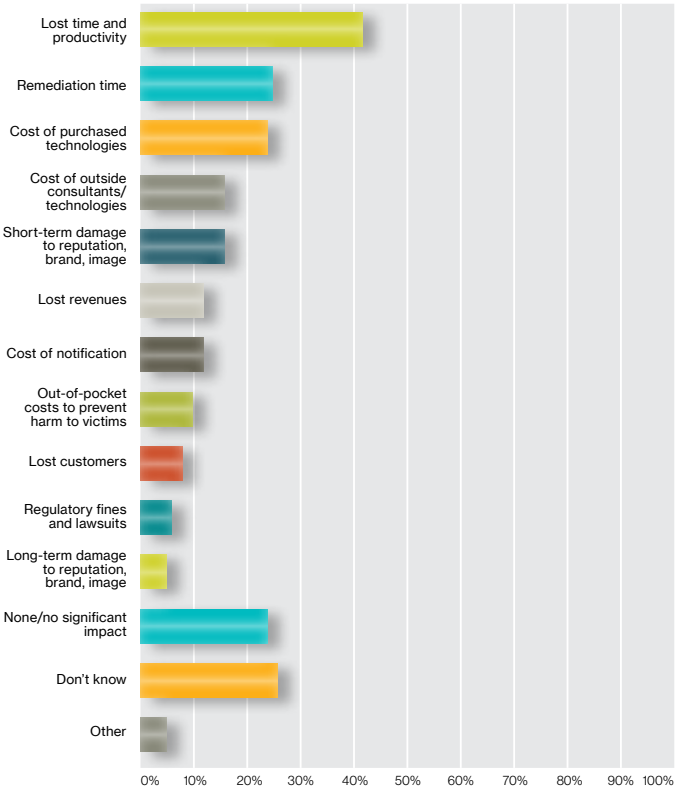
"Managing uncertainties is not an easy task. Limited resources and an ever-changing landscape of threats and vulnerabilities make completely mitigating all risks impossible. Therefore, IT security professionals must have a plan to assist them in sharing a commonly understood view with IT and business managers about the potential impact of security-related threats to the mission."

— Vitor De Souza, FireEye

Breach Impact

Q6: How have security breaches impacted your organization in the past two years?*

Finding: Security incidents affect organizations in a variety of ways, from remediation expenses to lost customers to brand-value damage. While about a quarter of survey respondents report "no significant impact" and about as many say they don't know how they've been impacted, the rest indicate that they've experienced one or more breach-related impacts in the past two years.



*Multiple responses allowed. All percentages have been rounded.

Expert Insight:

"The most disruptive event that can befall your organization is a destructive data breach; it will have a long-term impact upon your business, your risk posture, and your customers' perceptions. Counting the discrete financial cost of a significant data breach is difficult and only tells part of the story. The brand damage, executive distraction, and direct business-disruption impacts are more telling. What the results show is that many organizations still don't understand the damage that a breach causes to their operations."

— Vitor De Souza, FireEye

Attack Detection

Q7: How prepared is your organization to *detect* each of the following kinds of security threats?*

(Respondents rated preparedness for each kind of threat on a scale of 1 to 5, with 1 being "inadequately prepared" and 5 being "extremely well prepared.")

Finding: *When* an attack is detected can determine an organization's success in responding to it, but most respondents say their organizations are either "inadequately prepared" or "somewhat inadequately prepared" to detect all threats. But while the overall level of confidence is relatively low, survey participants rate detection as most effective against hacktivists and cybercriminals.

	Inadequately prepared	Somewhat inadequately prepared	Somewhat prepared	Well prepared	Extremely well prepared	N/A
Migration to cloud-based applications	20%	23%	24%	12%	12%	9%
Insider attack	20%	20%	26%	17%	13%	3%
APT (nation/state) attack	23%	25%	25%	14%	7%	6%
Internet of Things–related threats	22%	27%	19%	11%	8%	12%
Process control logic (PCL) and supervisory control and data acquisition (SCADA) threats	18%	21%	23%	15%	10%	13%
Hacktivist threats	19%	24%	25%	18%	8%	5%
Cybercriminal threats	22%	27%	21%	16%	10%	4%

*All percentages have been rounded.

Expert Insight:

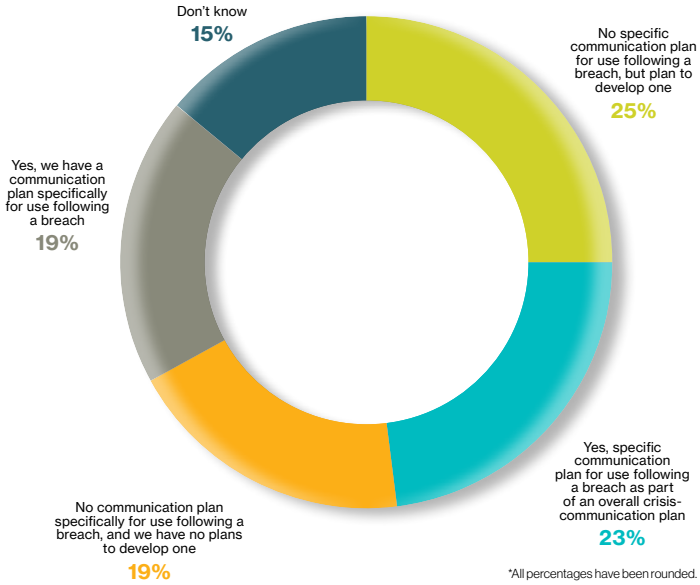
"Detection is the most effective means of thwarting hacktivists and cybercriminals. It just isn't possible to prevent all attacks, so detecting attacks in progress becomes your only recourse. Companies are likely reticent to claim they are good at detecting malicious activity because so many big-name companies—along with the military and federal government—are getting hacked."

— Marshall Heilman, Mandiant

Crisis Communication

Q8: Does your organization currently have a plan for communicating with internal and external stakeholders following a security breach?*

Finding: Within hours, or even minutes, after breach detection, various audiences, both inside and outside the organization, must be notified. Stakeholders include C-suite executives, the board of directors, customers, suppliers, partners, the public, and the media. However, in this survey, 44 percent of respondents say they do not have a post-detection communication plan. Of those, 19 percent do not plan to create one.



*All percentages have been rounded.

Expert Insight:

"I am a little surprised by these findings because our field experiences have shown us that the vast majority of companies have not developed a crisis-communications plan for a breach event. On the other side, I am encouraged by the numbers of respondents planning to create a plan of their own. But just as important is the tabletop exercise to make these plans operational."

— Vitor De Souza, FireEye

Additional Results

Information-Security Threats

Q9: How do you rate your level of security in each of the following areas?*

(Respondents rated each area on a scale of 1 to 5, with 1 being "inadequately secure" and 5 being "extremely secure.")

	Inadequately secure	Somewhat inadequately secure	Somewhat secure	Secure	Extremely secure
Mobile computing	22%	26%	28%	19%	4%
Employee mobile-device or application use (BYOD/BYOA))	26%	24%	27%	17%	7%
New application implementation/ application development process	15%	19%	35%	24%	6%
E-mail security	11%	18%	33%	30%	7%
Cloud-migration process	9%	26%	36%	22%	7%
Data sovereignty/Data security	11%	23%	34%	24%	8%

*All percentages have been rounded.

Q10: How prepared is your organization to *prevent* each of the following kinds of security threats?*

(Respondents rated preparedness for each kind of threat on a scale of 1 to 5, with 1 being "inadequately prepared" and 5 being "extremely well prepared.")

	Inadequately prepared	Somewhat inadequately prepared	Somewhat prepared	Well prepared	Extremely well prepared	N/A
Migration to cloud-based applications	15%	23%	24%	17%	12%	10%
Insider attack	22%	24%	21%	17%	12%	5%
APT (nation/state) attack	28%	22%	23%	12%	6%	9%
Executive breach response	17%	25%	25%	16%	12%	5%
Internet of Things–related threats	23%	23%	19%	12%	9%	14%
Process control logic (PCL) and supervisory control and data acquisition (SCADA) threats	15%	21%	25%	12%	10%	16%
Hacktivist threats	20%	27%	25%	16%	8%	4%
Cybercriminal threats	21%	28%	24%	16%	1%	3%

*All percentages have been rounded.

Q11: How prepared is your organization to *respond to* each of the following kinds of security threats?*

(Respondents rated preparedness for each kind of threat on a scale of 1 to 5, with 1 being "inadequately prepared" and 5 being "extremely well prepared.")

	Inadequately prepared	Somewhat inadequately prepared	Somewhat prepared	Well prepared	Extremely well prepared	N/A
Migration to cloud-based applications	19%	19%	24%	16%	11%	11%
Insider attack	18%	20%	27%	18%	14%	3%
APT (nation/state) attack	25%	21%	26%	14%	7%	7%
Executive breach response	18%	21%	27%	18%	11%	5%
Internet of Things-related threats	23%	23%	22%	15%	7%	11%
Process control logic (PCL) and supervisory control and data acquisition (SCADA) threats	19%	23%	22%	12%	12%	13%
Hacktivist threats	22%	20%	26%	18%	9%	5%
Cybercriminal threats	22%	22%	25%	14%	12%	5%

*All percentages have been rounded.

Information-Security Threats

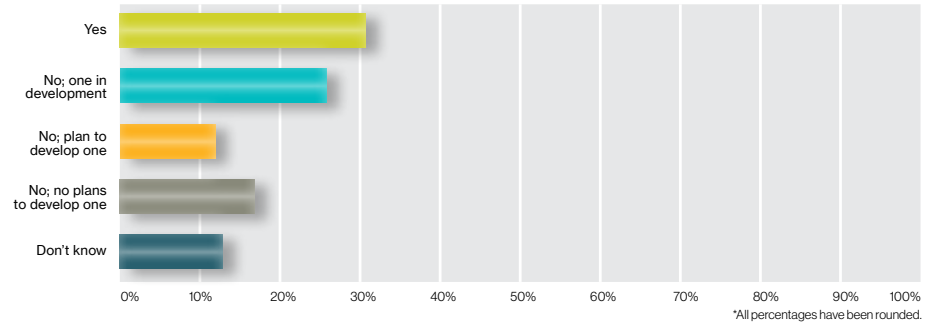
Q12: Compared to a few years ago, do you feel that it's easier or more difficult to do the following?*

	More difficult	Easier	No significant change	Don't know
Protect against security breaches?	57%	18%	17%	9%
Detect security breaches?	52%	22%	19%	8%
Respond to security breaches?	44%	28%	17%	10%

*All percentages have been rounded.

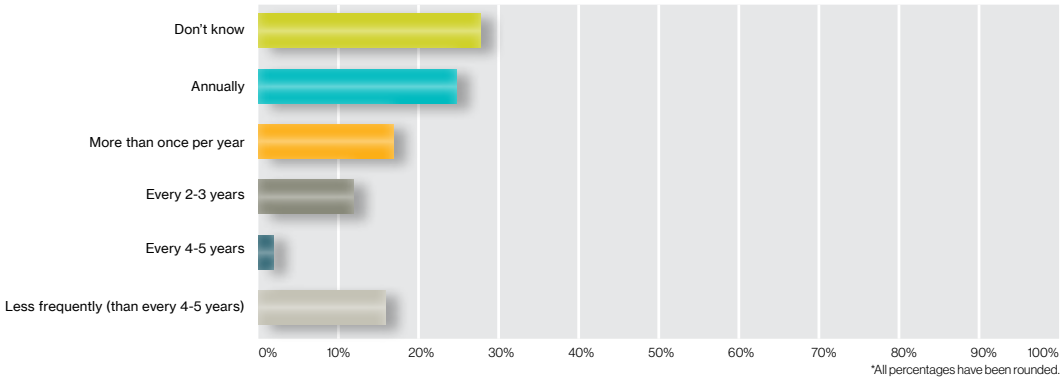
Risk Management

Q13: Does your organization have an information risk-management roadmap or tactical plan?*



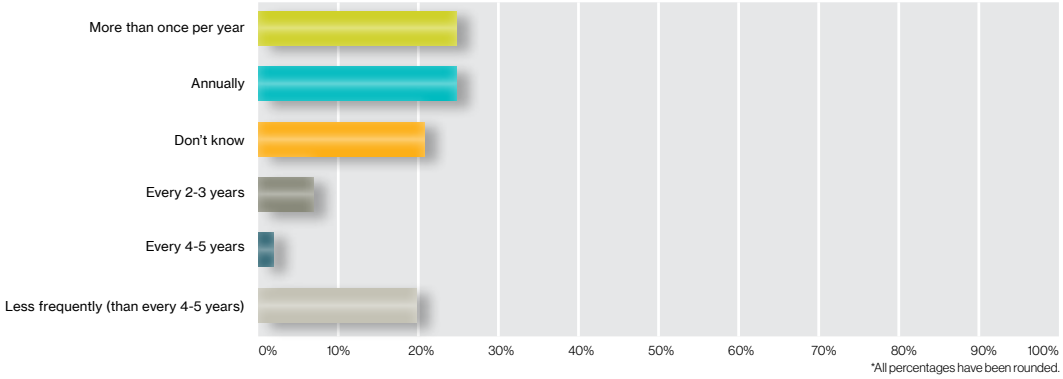
*All percentages have been rounded.

Q14: How frequently is your organization's information risk-management roadmap or plan updated?*



*All percentages have been rounded.

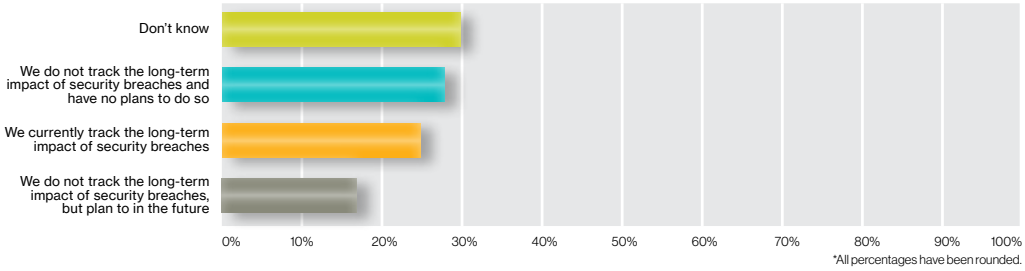
Q15: How often does your organization perform information risk assessments (that is, measure the inherent risk for the business or company)?*



*All percentages have been rounded.

Long-Term Impacts

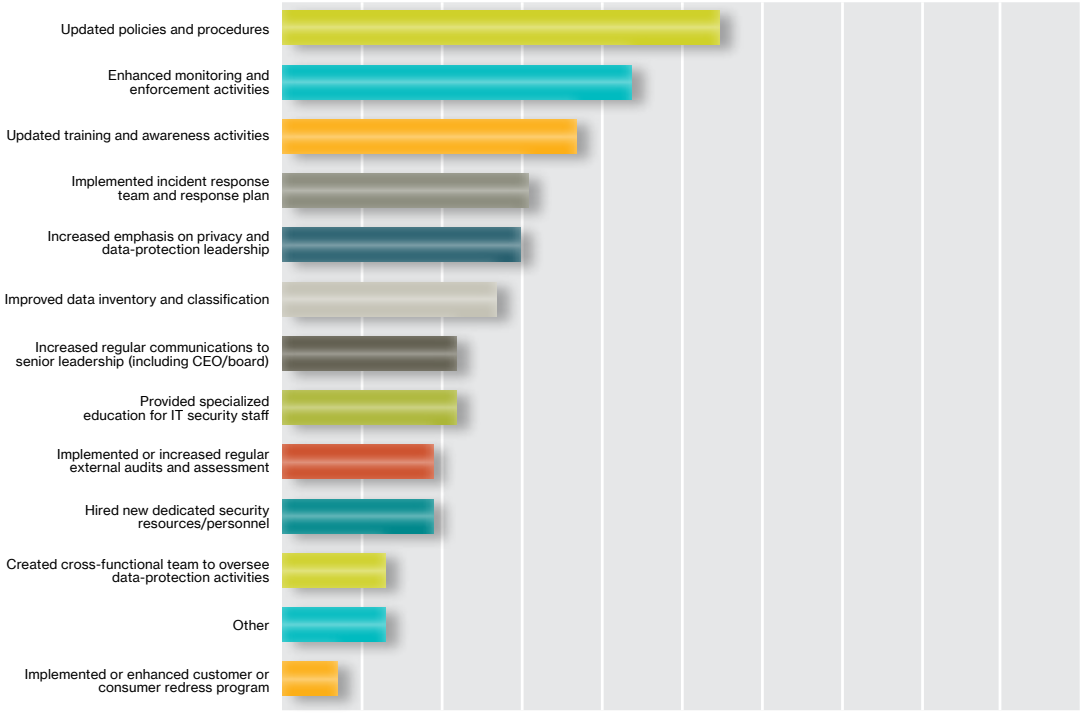
Q16: Do you track the long-term impact of security breaches in your organization?*



*All percentages have been rounded.

Q17: If your organization has been breached, what changes to operations, compliance processes, and other activities did it make to help prevent and/or detect future breaches?*

(Respondents selected all that apply.)



*All percentages have been rounded.

Human Resources and Skills

Q18: For each of these security- and risk-related functions, does your organization have the human resources and skills needed to adequately address them?*

	Yes	No	Don't know
Consulting	50%	32%	19%
Risk management	57%	29%	13%
Auditing	53%	36%	11%
Monitoring	61%	27%	12%
Incident response	52%	33%	14%
Forensics	23%	56%	21%
Legal advice	56%	29%	14%
Implementation	55%	28%	17%

*All percentages have been rounded.

Q19: To what extent is your organization able to recruit, develop, and retain security talent?*

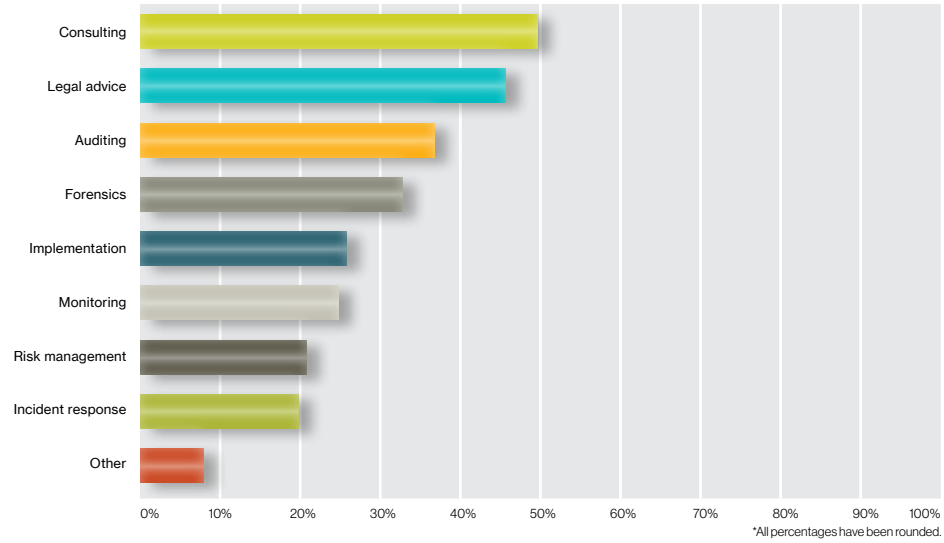
(Respondents rated their organizations' capability for each factor on a scale of 1 to 5, with 1 being "inadequately prepared" and 5 being "extremely well prepared.")

	Inadequately prepared	Somewhat inadequately prepared	Somewhat prepared	Well prepared	Extremely well prepared
Recruit talent	27%	21%	31%	16%	5%
Develop talent	26%	25%	27%	16%	7%
Retain talent	22%	25%	30%	17%	7%
Not applicable/we outsource all or most security functions	29%	13%	37%	12%	9%
Don't know	34%	13%	41%	4%	8%

*All percentages have been rounded.

Q20: For which of the following security- and risk-related functions does your organization *currently use* third-party service providers?*

(Respondents selected all that apply.)

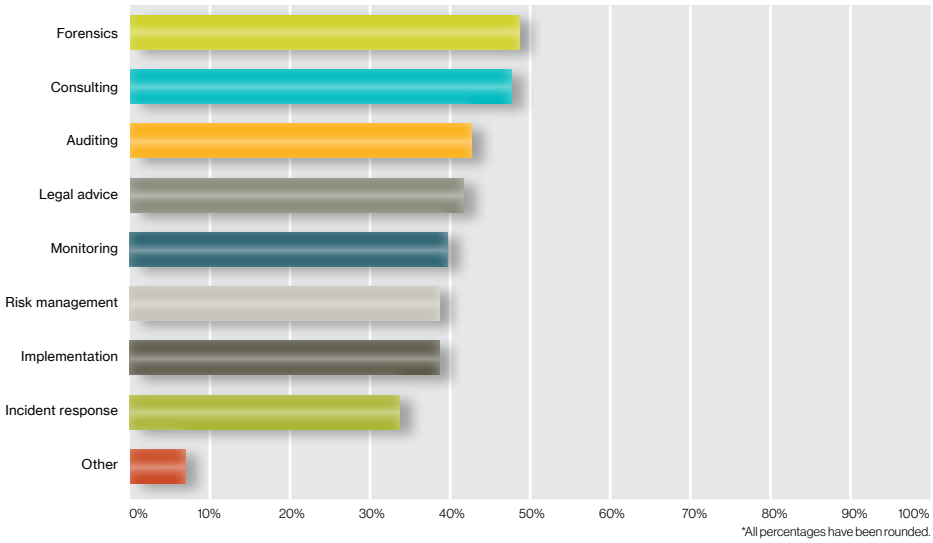


*All percentages have been rounded.

Human Resources and Skills

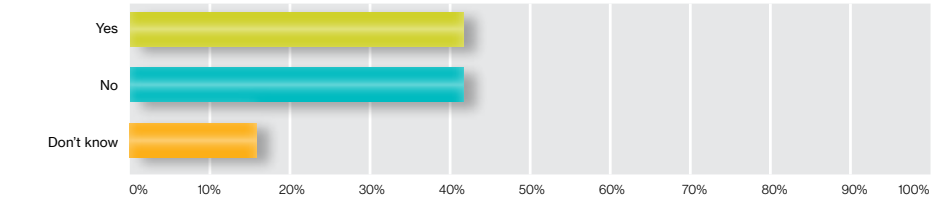
Q21: For which of the following security- and risk-related functions would your organization *consider using* third-party services?*

(Respondents selected all that apply.)



*All percentages have been rounded.

Q22: Do you believe the management team or executives at the highest level of your organization truly understand the time and resources needed to mitigate risk and minimize cyberthreat exposure?*

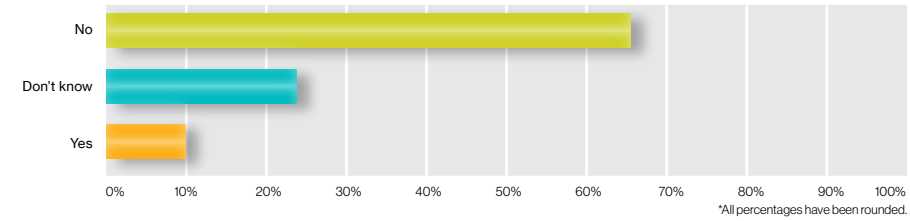


*All percentages have been rounded.

> **"What the results show is that many organizations still don't understand the damage that a breach causes to their operations."**
>
> *– Andrzej Kawalec, HPE Security Services*

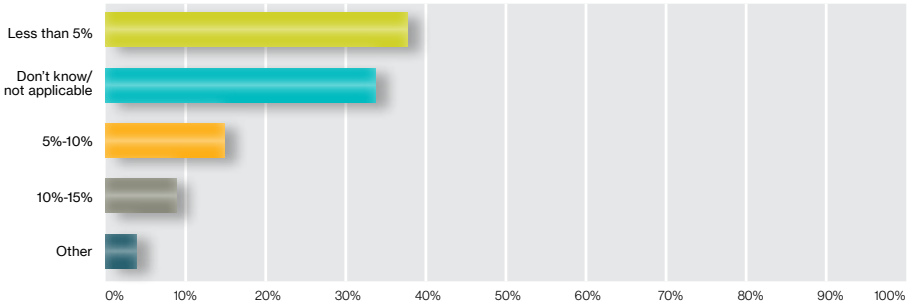
Cybersecurity Spending

Q23: Do you benchmark your security expenditures?*



*All percentages have been rounded.

Q24: What percentage of your IT budget is earmarked for cybersecurity?*



*All percentages have been rounded.

> "IT security professionals must have a plan to assist them in sharing a commonly understood view with IT and business managers about the potential impact of security-related threats to the mission."
>
> – *Vitor De Souza, FireEye*

Additional Information

More than ever, information security is – or should be – top of mind for business and IT leaders worldwide. "Taking on the Cybersecurity Challenge," an exclusive new content hub on TechnologyReview.com produced by MIT Technology Review Custom in partnership with Hewlett Packard Enterprise Security Services and FireEye, takes a multifaceted look at this critical concept through articles, infographics, videos, and original research on security trends.

Please visit www.technologyreview.com/cybersecurity

Methodology and Participant Profile

MIT Technology Review Custom conducted an online survey of 225 IT and business executives and managers in February 2016. Participants represented a broad range of industries and were primarily from North America, the United Kingdom, Western Europe, India, China, Latin America, and the Asia-Pacific region.

Sponsors

Hewlett Packard Enterprise

Hewlett Packard Enterprise is an industry-leading technology company that enables customers to go further, faster. With the industry's most comprehensive portfolio, spanning the cloud to the data center to workplace applications, our technology and services help customers around the world make IT more efficient, more productive, and more secure.

FireEye
SECURITY REIMAGINED

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyberattacks. These highly sophisticated cyberattacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyberattacks in real time. FireEye has more than 4,400 customers across 67 countries, including more than 680 of the Forbes Global 2000.

About MIT Technology Review Custom

Built on more than 115 years of excellence in technology journalism, MIT Technology Review Custom is the arm of global media company MIT Technology Review that creates and distributes custom content. Our turnkey solutions include everything from writing, editing, and design expertise to multiple options for promotional support. Working closely with clients, our expert custom-editorial staff develops a range of high-quality, relevant content, delivering it to users when and where they want it – in digital, print, online, and in-person experiences. Everything is customized to fit clients' content marketing goals and position them as thought leaders aligned with the authority on technology that matters.

www.technologyreview.com/media