Hewlett Packard Enterprise

FireEye SECURITY REIMAGINED

Survey and Executive Summary Produced by MIT Technology Review Custom in Partnership with Hewlett Packard Enterprise Security Services and FireEye Inc.

Cybersecurity Challenges, Risks, Trends, and Impacts: Survey Executive Summary

IN THIS REPORT

No question about it: Information security—or, more precisely, the lack of it—is firmly on the radar for business and information-technology 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, and a shortage of in-house security expertise remains of widespread concern.

Those are among the initial findings of the Cybersecurity Challenges, Risks, Trends, and Impacts Survey, conducted by MIT Technology Review Custom in February 2016. About 225 business and IT executives, directors, managers, and other leaders participated in the online survey, which was commissioned by Hewlett Packard Enterprise Security Services and FireEye Inc.

While the research team continues to analyze survey results, themes about several key issues have already emerged. Among them:

- **Few survey respondents are fully confident in their ability to respond to security threats.** For instance, only about 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.** While 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, email- or Web-based attacks, and the vulnerabilities created by the bring-your-own-device (BYOD)/bring-your-own apps (BYOA) workplace trends.
- **A 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 call "lost time and productivity" the most negative effect of recent breaches.** Other impacts include remediation time and necessary expenditures on consultants and additional technologies.

Additional findings will be released later in 2016. Meanwhile, please read on for a few preliminary survey highlights.

Security Challenges

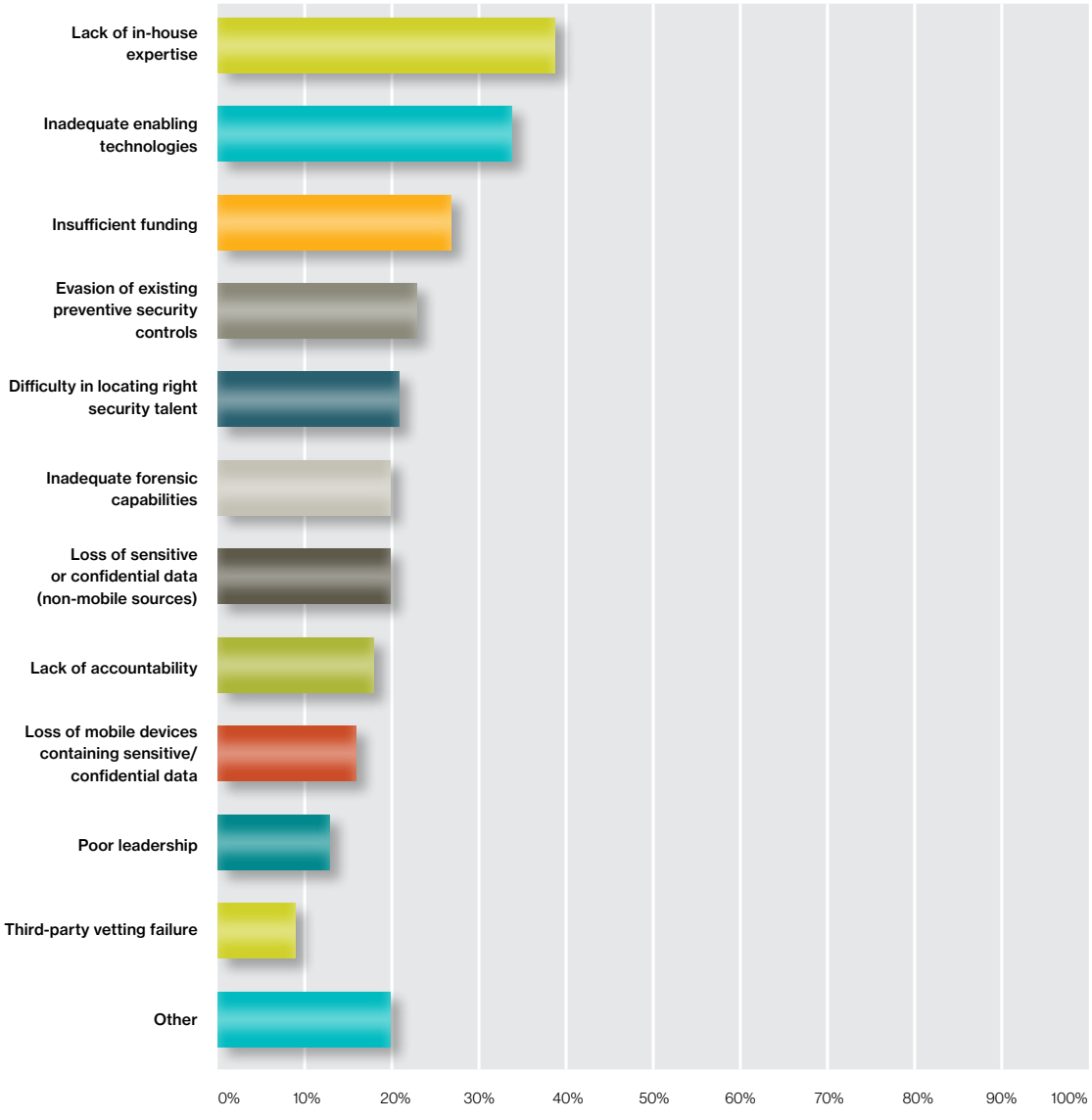
Survey Highlights

Following are initial survey results for several key issues: security challenges and threats, attack frequency, preparedness levels, information risk management strategies, and breach impact.

Issue 1: Security Challenges

For more than a third of survey participants, lack of in-house expertise ranks as the top information-security headache.

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



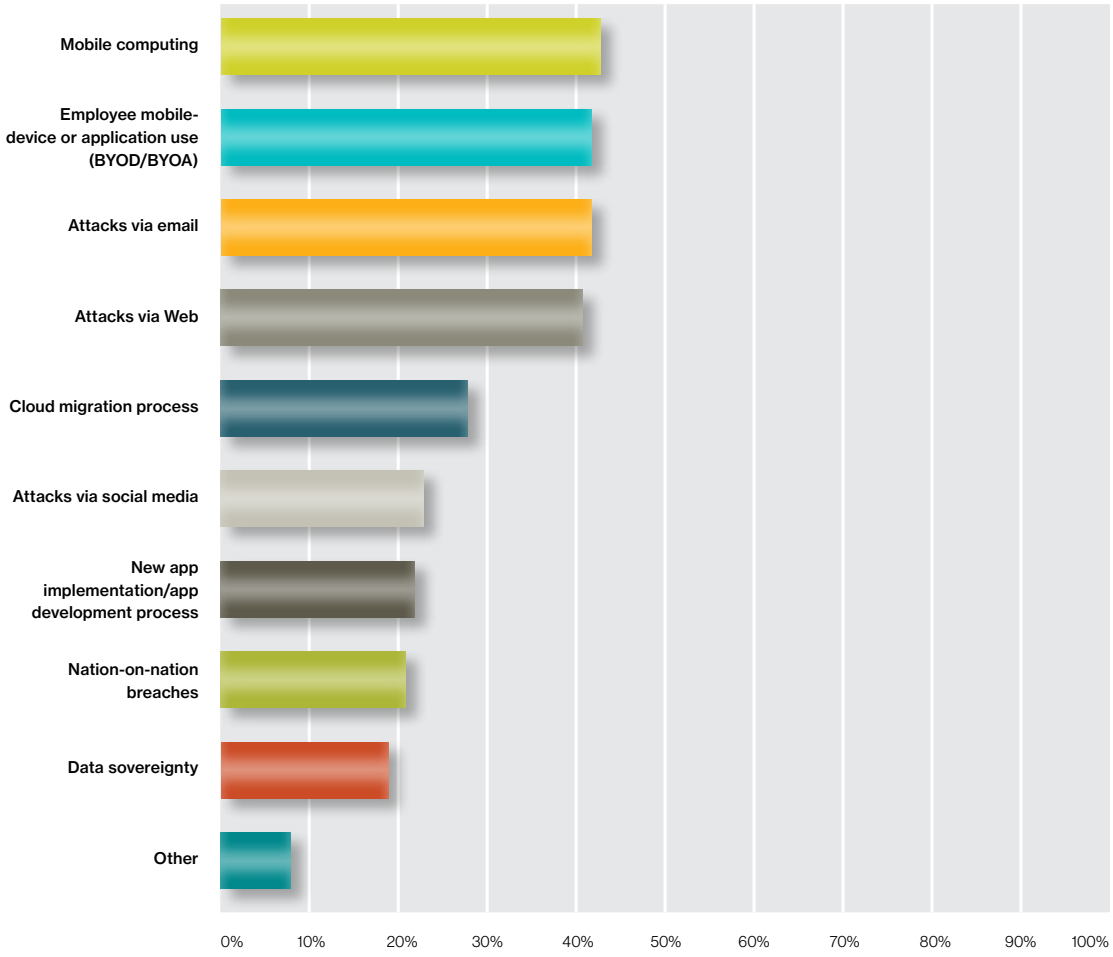
*Multiple responses allowed. All percentages have been rounded.

Security Threats

Issue 2: Security Threats

Participants perceive mobile computing as the biggest current threat to information security, but several other factors rank close behind.

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

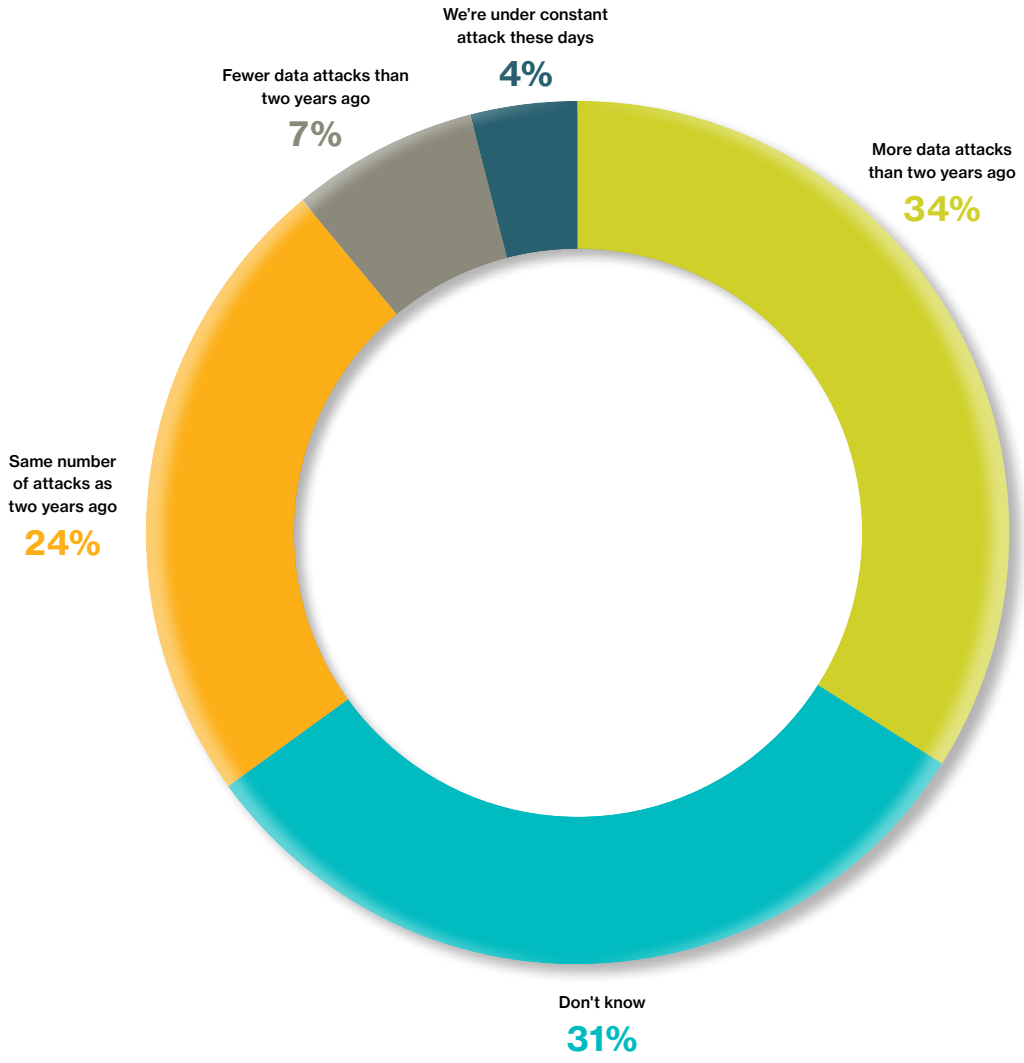


*Multiple responses allowed. All percentages have been rounded.

Issue 3: Attack Frequency

For more than a third of survey participants, 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 survey participants see no change, while a few report being "under constant attack." Only a handful say data attacks have decreased.

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?*



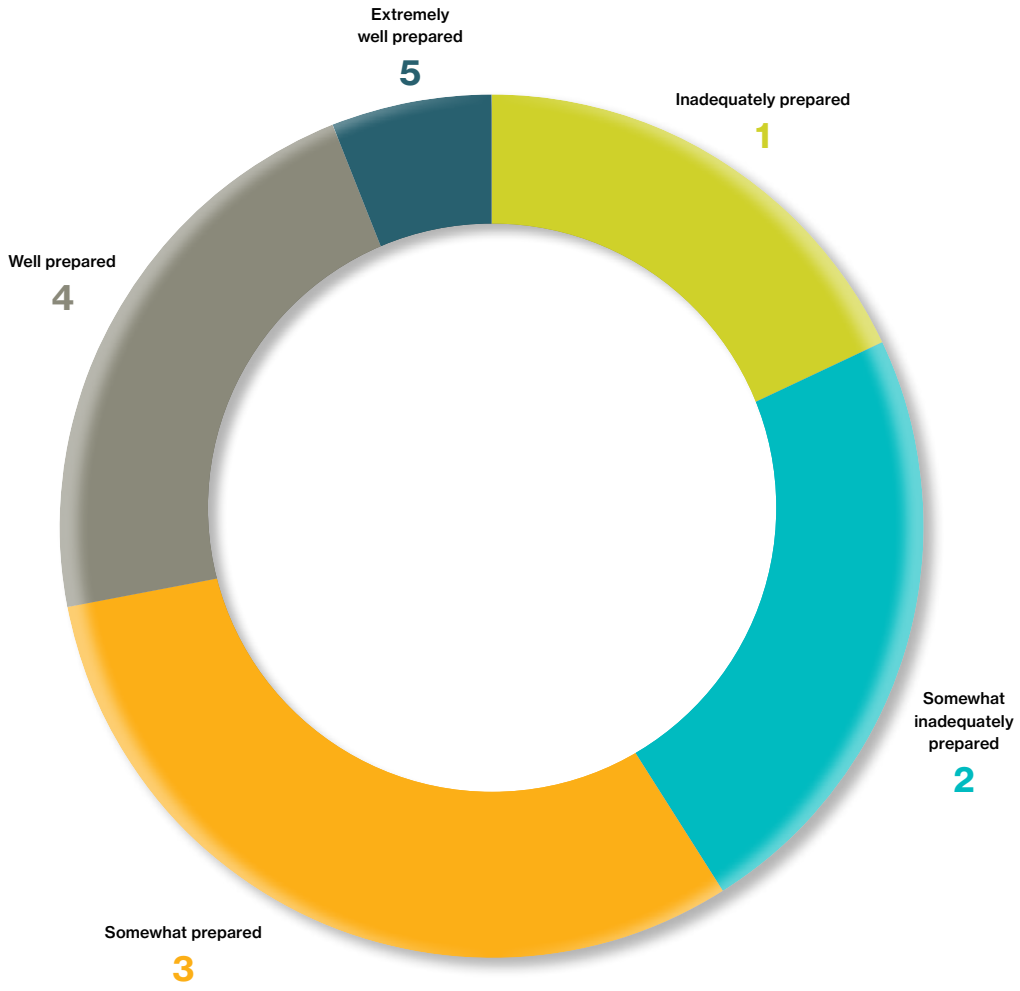
*All percentages have been rounded.

Attack Frequency

Issue 4: Breach Preparedness

Only a handful of survey participants feel their organizations are "extremely well prepared" to respond to a security breach involving serious information loss.

On a scale of 1 to 5, how prepared is your organization to respond to an incident involving a material loss of information?

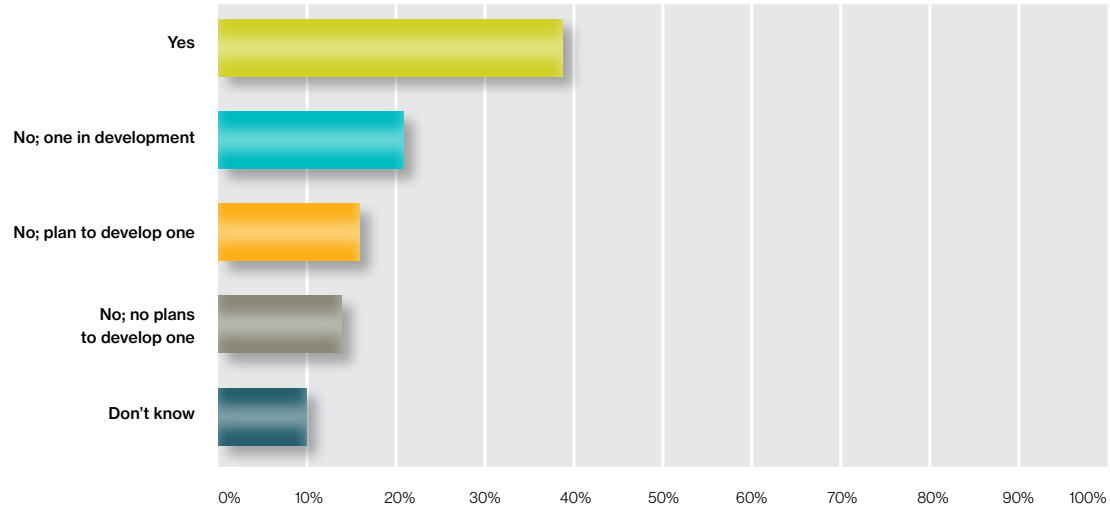


Breach Preparedness

Issue 5: Risk Management Strategies

Roughly 40 percent of participants 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.

Does your organization have an information risk management strategy?*



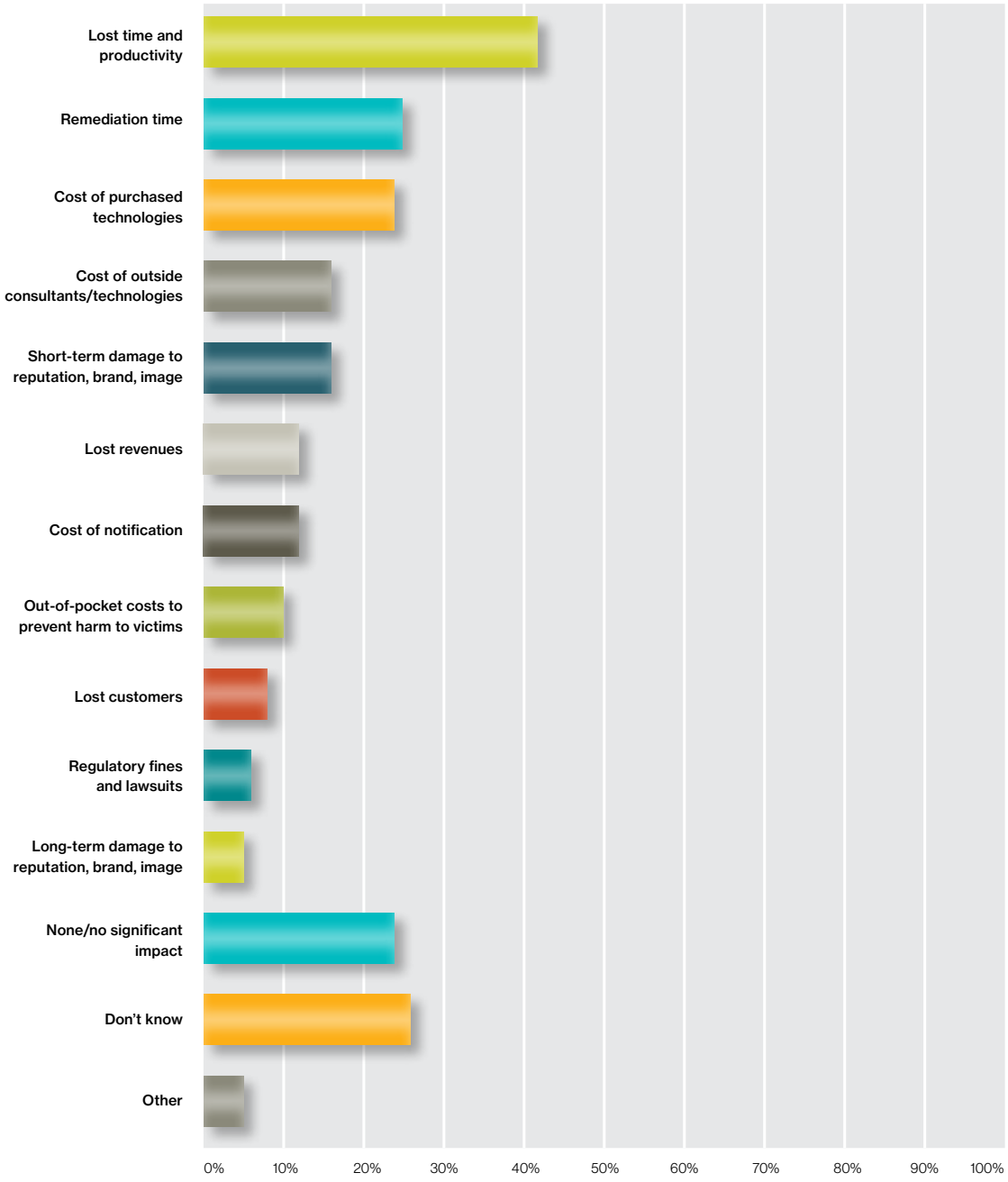
*All percentages have been rounded.

Breach Impact

Issue 6: Breach Impact

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

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



*Multiple responses allowed. All percentages have been rounded.

Methodology and Participant Profile

Methodology and Participant Profile:

MIT Technology Review Custom conducted an online survey of IT and business executives and managers across a broad range of industries in February 2016. About 225 qualified participants—primarily from North America, the United Kingdom, Western Europe, India, China, Latin America, and the Asia-Pacific region—completed the 31-question survey. Additional findings will be released in mid-March 2016.

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, or 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

Hewlett Packard Enterprise

FireEye SECURITY REIMAGINED