WHITE PAPER

Market Pulse

Outrunning the Bear

5 CRITICAL WAYS TO TAKE A MORE COLLABORATIVE APPROACH TO IT SECURITY

Companies still rely heavily on fairly traditional methods of data security, such as password management and acceptable use policies, to protect their information from unauthorized access. Unfortunately, in the age of increasing cyber threats, these traditional approaches to security are no longer enough.

A new survey from IDG Research indicates that IT security professionals remain more reactive than proactive when implementing data security — a mindset that could leave them dangerously underprepared to respond effectively in the event of a breach, possibly letting small incidents become much more damaging. At the same time, however, even the best data security operations centers only have the resources to focus on the highest priority threats. This white paper will offer insights from the IDG Research survey and explore how organizations can be more proactive and efficient in understanding the threats they face and updating their data security to counter modern cyber threats.

» Threats Are Outpacing Security

IDG Research respondents' most common lines of defense against data breaches are the tried and true: account and password management policies, enforcement of acceptable use policies, and programs promoting security education and awareness *(figure 1, page 2)*. To be sure, these traditional approaches remain a critical baseline of IT security. However, as the nature and breadth of cyber threats grow – the Ponemon Institute found that cybercrime grew 10.4 percent in 2014[1] – IT security practices are not evolving quickly enough to keep pace.

Fewer than half of the respondents in the IDG study say their organization is highly successful in its ability to identify security threats, develop and enact plans for threat response, or effectively mitigate threats. Only half have deployed advanced methods of breach protection and prevention such as security event analysis, and just 38 percent are proactively researching cyber threats.

Digging further into organizations' security success reveals other perplexing discrepancies. While just 18 percent of respondents admit that they don't respond as well as they should to threats, 45 percent acknowledge that they often need several days or more to mitigate a known vulnerability, and one in three need several days or more to address an actual breach *(figures 2 and 3, page 3)*. And that's only after discovering the threat, which the Ponemon report found on average takes companies 170 days to detect.

"The expectation, fairly or otherwise, is that we need to be perfect all the time," says Dan Lamorena, senior director of product marketing for HP Enterprise Security. "But even the best security operations centers can only focus on the highest priority items because they don't have the personnel to handle the others."

» Challenges Inhibit Faster Response

A lack of trained and experienced IT security personnel, in fact, was cited as the top inhibitor of timely responses to security threats. Rounding out the top three challenges are a lack of definition around security processes and procedures and a lack

CIO Strategic Marketing Services

hp

of integration between different security layers and solutions. These barriers can cause IT to lose ground quickly. HP's Cyber Risk Report found that most of the top malware reports in 2014 were two to four years old and had available software patches that IT simply had not applied yet[2].

"Most security processes are currently very manual," says Lamorena. "You have to identify the vulnerability and figure out if it applies to you, where it applies, who owns those servers, and how to update them. Those are complex issues that are best addressed through better training, better processes, and better technology that automates a lot of the prioritization and mitigation."

Respondents to the IDG survey also cite automation, process improvement, and better integration between security policies as the best options for improving response time. However, many are apparently in no hurry to pick up the pace. A full 40 percent said they are not actively looking for ways to respond more quickly to a security event *(figure 4, page 4)*, and one in five said they have no plans to create a breach response plan.

It's evident that while every organization knows it's at risk, and security teams aspire to be more proactive, they clearly need a more evolved approach to protecting assets and mitigating known security incidents.

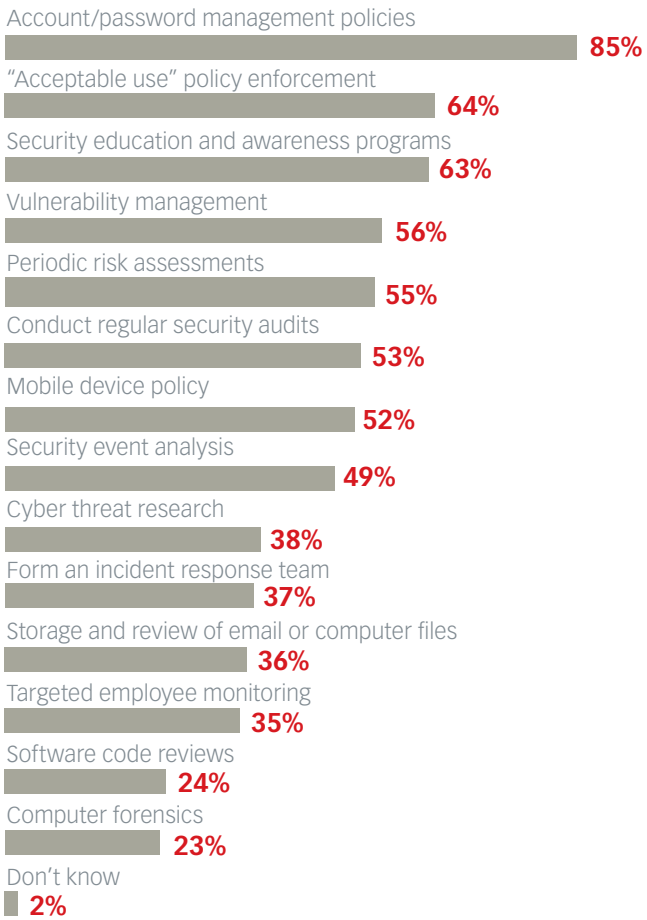
"Every company needs to know what steps to take in a breach," Lamorena says. "How do I respond? How do I react? Who do I contact, from both a law enforcement and PR standpoint? Eventually, you will experience a breach of some kind, so it's crazy not to do any planning."

Even worse is failing to change your approach in the wake of a threat or incident. Just over one-third of respondents whose organization was affected by a major security event in the last year changed threat mitigation policies or end user security policies in response. Fewer than half said they changed their approach to threat monitoring to better identify potential future problems.

This is likely a case of IT teams doing the best they can with the resources they have. "IT security budgets remain a tiny percentage of the total IT budget, and even with high-profile breaches driving small increases in funding, business may be reluctant to invest more in security because you can't always put an ROI on it," says Lamorena. "There's also a huge shortage of qualified security professionals. Companies need to be able to look at threats more holistically than they currently do."

FIGURE 1. **Policies and Procedures to Mitigate Security Threats**

85% of organizations are ***using account/password policies*** to mitigate threats.



» Share and Share Alike

Looking at threats holistically means sharing intelligence across tools and vendors as well as between products and teams. The IDG Research survey indicates some reasons why this is currently difficult.

First, it seems that most organizations' approach to security is inward-focused. Call it the "outrunning the bear" response: the IT team at your organization doesn't have to be faster than the cybercriminals, only faster than the other organizations trying to outrun them. While about 75 percent of IT security staffers say they have

FIGURE 2. **Initiating a Response to Security Breaches**

32% of respondents say it may take ***several days or longer*** once a response is initiated.

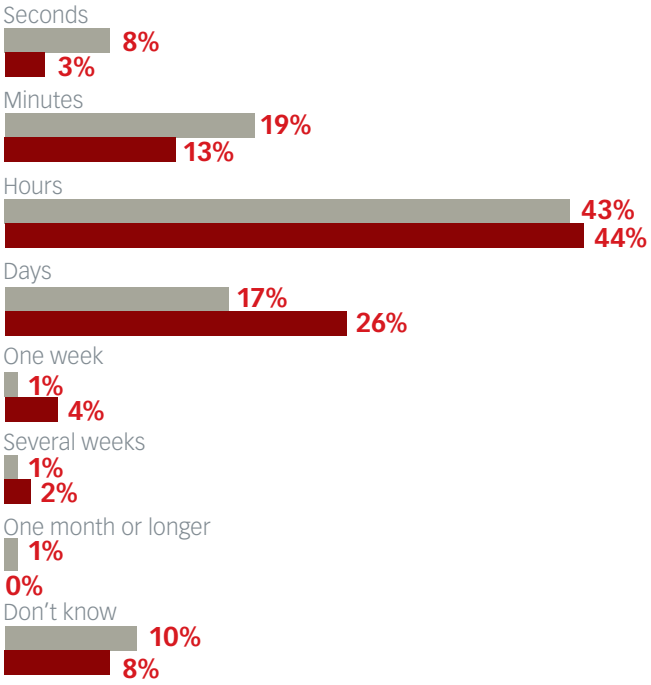
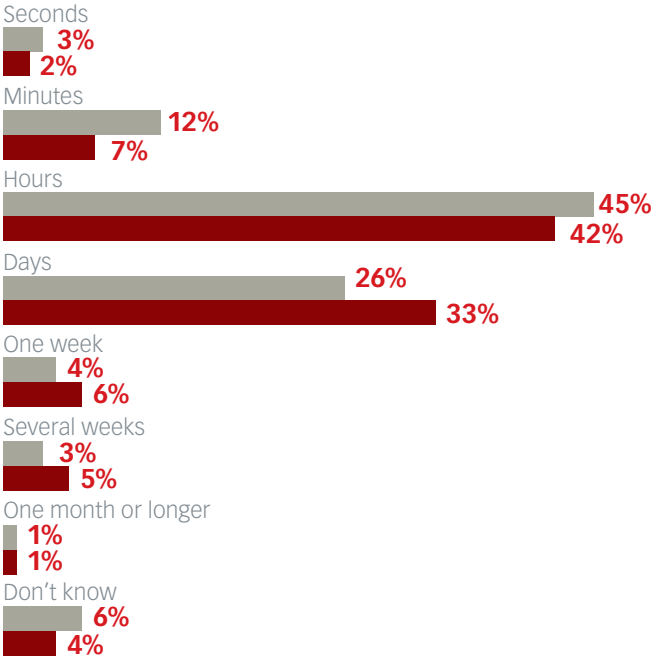


FIGURE 3. **Initiating a Response to Vulnerability in IT Environment**

45% of respondents say it may take ***several days or longer*** once a response is initiated.



plenty of opportunity to collaborate with peers within their organization, 60 percent say they have little to no opportunity to collaborate with peers at other companies. The lower they are on the organizational chart, the less often this interaction occurs, even though the lower-level IT staffers are the ones on the front lines and therefore the ones best placed to alert each other to emerging threats.

Second, IT security staffers get most of their information about security trends, threats, vulnerabilities, warnings, and technologies not from their peers, but from online forums and cybersecurity news sites. In other words, the bear can get the latest security news in the same places and at the same time they do – often before patches are released to plug any vulnerabilities. These sources might make an IT team aware of a threat against their industry and the tools the attackers are using, but they might not be able to link the threat to actual suspicious activity on the company network that indicates a need to act.

Buying point products further exacerbates this lack of shared intelligence by creating silos of technology and people, both within a given company and across the broader security community.

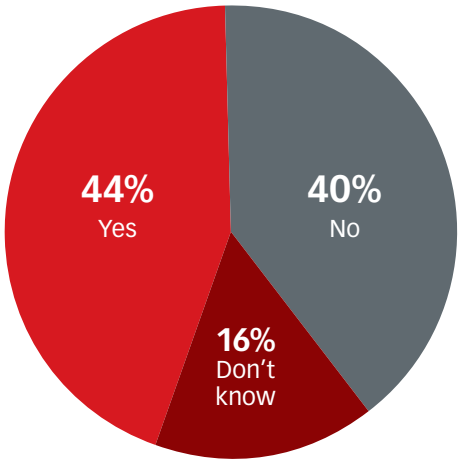
» Turning Intelligence into Action

The lack of proactive planning, combined with the tendency to rely on traditional solutions that are becoming increasingly less effective, leaves companies at a growing disadvantage against cybercriminals. To streamline their ability to detect, respond to, and mitigate threats, organizations need to gather more security intelligence and transform it into action. To do this, they need to shift their approach to information in five critical ways:

- Take a more holistic approach that supports sharing security intelligence both internally and externally. This ensures

FIGURE 4. **Seeking Ways to Reduce Response Time to Security Event**

55% of larger companies are seeking ways to ***reduce response time*** to security events.



a more comprehensive view of threats across organizations, technologies, and industries.

- Increase automation to make processes more efficient and less prone to human error. Every dollar spent on security intelligence systems delivers $26 in ROI, and every dollar spent on encryption returns $20, Lamorena notes. Increased automation also helps mitigate the problems caused by high vacancy rates for IT security positions, which Ponemon currently estimates at 40 percent for security analysts and 60 percent for operations team managers.
- Improve integration of tools and processes by incorporating open source solutions that work across vendors. All security solutions must be able to communicate with each other to minimize the risk of gaps in threat detection and response.
- Create and/or fortify a breach response plan to ensure that when the inevitable happens, organizations can limit and quickly mitigate the resulting damage to both data and reputation.
- Increase research and collaboration with IT security staffers at other organizations as well as external security experts who have a broad view of the latest threats and trends.

Conclusion

The "old" approach to IT security focused on protecting the infrastructure: the hardware, the server, the laptop. The new approach recognizes that information resides and travels beyond the devices an organization can control, and therefore requires protecting the applications that use the data and the interactions users have with it.

However, as data volumes increase and applications proliferate, relying on point products for security creates silos and makes it more likely that both data and security intelligence will fall into the gaps – making it more difficult to respond to a rising tide of threats in less time than ever before.

There are no silver bullet technologies. However, an integrated approach lets security professionals share information across tools and technologies. By strengthening breach protection and defense, the security community can apply its collective knowledge to address cybercrime — and make sure everyone stays one step ahead of the bear.

For more information, visit **www.hp.com/go/esp**

1. 2014 Cost of Cybercrime Study, Ponemon Institute, http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/

2. "HP Cyber Risk Report 2015," http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/