Security-Level Trends

The number and cost of cyberattacks continues to rise, and more of them are stealthy, highly targeted, and carried out by organized cybercrime gangs.

Hewlett Packard Enterprise

An October 2015 global study of 252 companies in seven countries conducted by the Ponemon Institute in conjunction with HPE Security shows that the number of cyberattacks against organizations continues to increase in frequency and sophistication.[1]

Organizations on average spent more per breach in 2015 than they did in 2014. The annualized cost to detect, respond to, and mitigate a breach globally was around $7.7 million—1.9% higher than in 2014. For U.S. companies, the average annualized costs were much higher, at around $15 million on an annualized basis.

The study also found that the average cost of a data breach was around $21,155 per day. So the longer an attack remained undetected, the higher the cost was to the breached organization. On average, organizations took around 46 days to resolve a cyberattack, which meant they spent around $973,000 just during the attack remediation phase.

Contrary to popular perception about external attackers causing the most damage, the costliest crimes were caused by insiders. Denial-of-service attacks and web application attacks were close behind in terms of costliest attacks.

The data revealed that unlike the mass attacks of a few years ago, a growing number of current attacks against organizations are stealthy, highly targeted, and carried out by organized cybercrime gangs.

With many advanced persistent threat (APT) campaigns, attackers have shown a tendency to use spear-phishing emails and other social engineering tricks to acquire login credentials belonging to legitimate users, which they then use to gain an initial foothold on an enterprise network.[2] Threat actors have been known to conduct extensive surveillance to gather information about victims in order to target them more effectively.

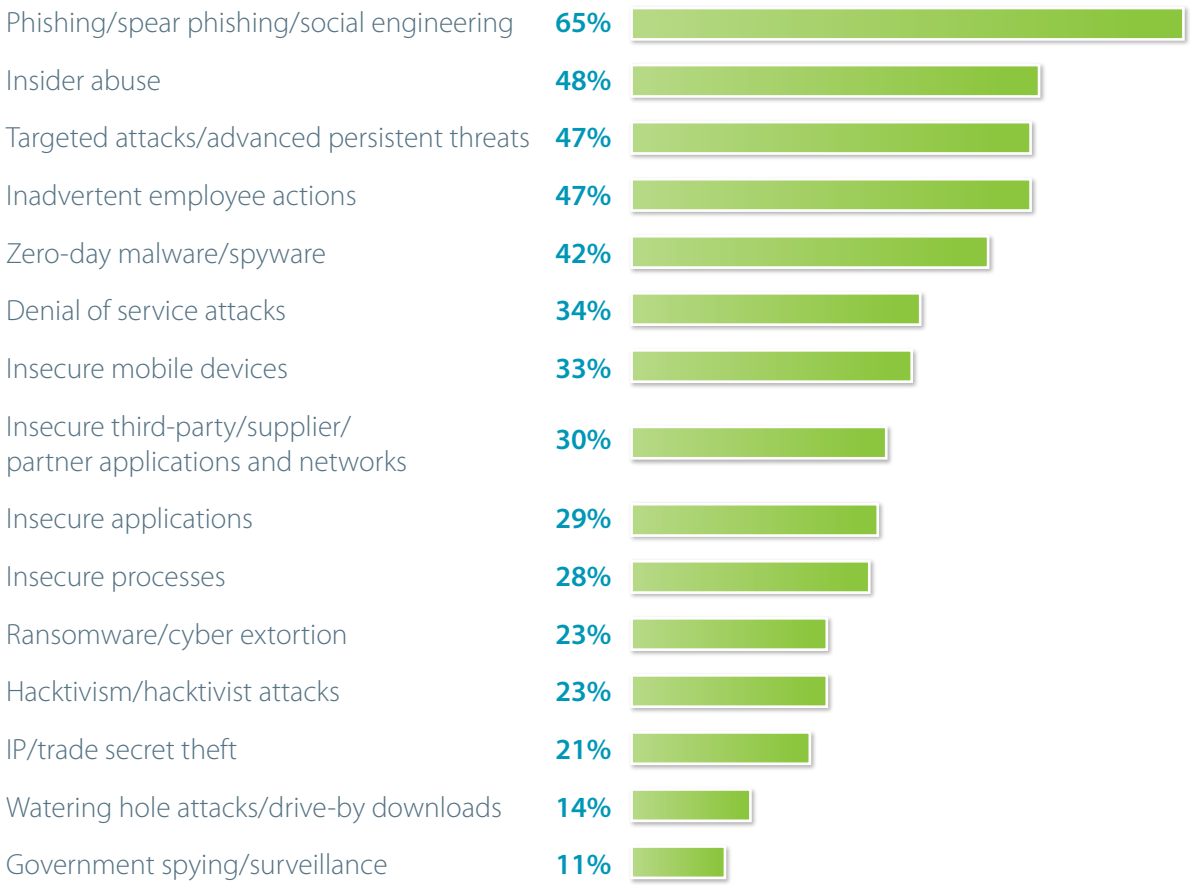
Previous APT attacks have shown that once attackers gain access to a system, they use sophisticated malware to move laterally across

the network until they gain access to systems containing customer, financial, and other valuable data. Unlike the smash-and-grab raids of the past, many of the attacks have emphasized persistence and stealth during the data exfiltration stage, which can last for months.

The results of an October 2015 UBM Tech survey of 185 business technology professionals at medium and large companies reflect a growing awareness of the problem, with 65% of respondents identifying phishing and social engineering as their biggest security concern. Nearly half (47%) identified APTs and targeted attacks as a major concern, while 42% cited zero-day threats as a problem. Other major concerns included insider abuse, inadvertent employee actions, and denial-of-service attacks.

Somewhat surprisingly, only 24% of those who responded to the UBM survey admitted their organizations have suffered a data breach in the past 12 months. Fifty-six percent said they have not experienced a data breach, while 20% said they didn't know whether they have been breached.

The relatively high proportion of respondents who said their organizations have not suffered a data breach is significant because it



What do you see as the biggest security threats to your organization?

Note: Multiple responses allowed

Data: UBM Tech survey of 185 business technology professionals at companies with 500 or more employees, October 2015

suggests one of two things: The organizations are either doing an exceptionally good job preventing cyberattacks, or they don't yet realize that they have been breached.

While enterprises clearly want to be able to respond as quickly as they can to a data breach, it's taking longer and longer for many to detect intrusions. For instance, it takes financial services companies up to 98 days on average to detect a breach. The dwell time—the period between intrusion and breach discovery—is even longer for retailers, at around 197 days.[3]

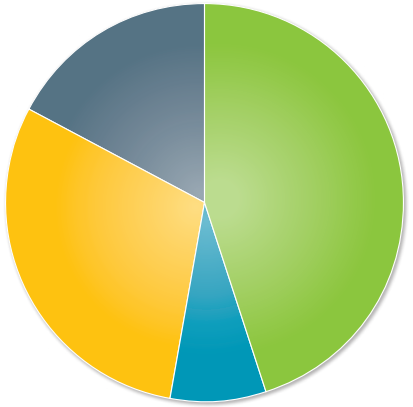
Results from the UBM survey reflected this trend, with 50% of the respondents saying their organizations would take several days to several weeks to detect an intrusion, 8% saying it could take months, and 4% saying they'd never know.

The numbers highlight the need for enterprises to have more robust capabilities for detecting and responding to intrusions. Most organizations see perimeter tools as being vital to their ability to defend against attacks. But there appears to be a growing trend among security administrators and managers about the need for tools that can help them mitigate the fallout of an intrusion, should one occur.

In the coming year, most organizations surveyed plan to increase spending on application security, data security, and information security. For instance, 45% of respondents said they expect to spend more on application security in the next 12 months, while another 30% expect spending to remain the same.

A similar proportion (43%) of respondents said their organizations would increase spending on data security tools for database activity monitoring, data loss prevention, encryption, and tokenization, while 33% planned to keep their spending at current levels.

The heightened awareness for incident detection and response was also reflected in the survey results pertaining to security information and event management tools. Some 42% of the organizations surveyed already use SIEM tools to correlate and analyze threat data from multiple sources, while another 14% plan to implement the capability in the next 12 months. Similarly, 45% use tools to monitor DNS and NetFlow, and 17% will do so in the coming year.



- More 45%
- Less 8%
- Spending will remain the same 30%
- Don't know 17%

↑ Over the next 12 months, do you expect your organization to spend more or less money on application security products and processes?

Data: UBM Tech survey of 185 business technology professionals at companies with 500 or more employees, October 2015

[1] *https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf*
[2] *http://www.infosecurity-magazine.com/news/91-of-apt-attacks-start-with-a-spear-phishing/*
[3] *http://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches*