Over half of companies are upping spending on IT security: eSecurity Planet Survey

Data breaches and new privacy regulations prompting increased spending on products and staff

---

Driven by fear of data breaches and new privacy regulations, such as Europe's General Data Protection Regulation (GDPR), large enterprises are spending aggressively on IT security measures, according to *eSecurity Planet*'s newly released 2019 State of IT Security survey.

The survey found that 54 percent of companies will increase their IT security spending this year, and 30 percent will increase their spending by 10 to 20 percent or more.

The survey also found strong hiring demand for IT security staff, despite a global shortage of about 3 million cybersecurity pros. About 57 percent said their organizations are hiring security staff in the next 12 months.
"Writing about data breaches and vulnerabilities that occur on an all-too frequent basis, I'm often disillusioned about the state of cybersecurity," said Sean Michael Kerner, senior security editor for *eSecurity Planet* and its sibling publication *eWeek*. "The 2019 State of IT Security survey gives me hope, as organizations are responding to the challenges and are not idly sitting by waiting for the next breach."

The survey was conducted in January 2019 and included eSecurity Planet subscribers from security engineers up to CIOs and CEOs.

Analyst firm Gartner has predicted an 8.7 percent increase in IT security spending for 2019. Based on the *eSecurity Planet* survey, large companies will drive that spending increase–and possibly exceed expectations.

The vast majority of big spenders in the survey (69 percent) were mid-sized through very large organizations, and their spending lists are long.

By contrast, of the 46 percent of respondents who said their cybersecurity spending will remain flat or down slightly, 62 percent were from companies with fewer than 100 employees, and only a few were from very large companies.
The results point to robust demand for security products, as companies try to counter increasingly sophisticated attacks and protect data from breaches that could lead to steep fines under the EU's GDPR, with California soon to enact its own strict data privacy requirements, the California Consumer Privacy Act. As the regulations cover any company doing business in these regions, they affect companies around the globe.

For more on the survey's compliance results, see Most Companies are Confident in Their Compliance Controls: eSecurity Planet Survey.

IT security spending priorities: NAC, DLP, gateways

The survey also had much to say about IT security spending priorities.

Network access control (NAC), web gateways and data loss prevention (DLP) are the top IT security spending priorities, revealing a need for security teams to balance external and internal threats.

While NAC and web gateways can help keep out the bad guys, data loss prevention can prevent unauthorized parties from making off with sensitive data, both employees and hackers who have successfully penetrated network defenses. It's a particularly key technology for data privacy regulations like GDPR.

Among survey respondents, a very large city government plans web gateway and network access control purchases. A large federal agency had a wish list of a half-dozen security technologies. A leading business services firm plans DLP,

SIEM and DDoS protection purchases. A large financial services firm is trying out new breach and attack simulation technology.

An IT services company had the longest shopping list: web gateways, network access control, DLP, deception technology, UEBA, phishing simulation and patch management.

Network access control and web gateways are already some of the most widely deployed security technologies among survey respondents, with about 54 percent of respondents already using NAC and 41 percent using web gateways. With around 20 percent of respondents planning to purchase those technologies in the next 12 months, those adoption rates are set to rise significantly.

Data loss prevention is also on track for significant growth. About 35 percent of those surveyed have already adopted DLP tools, and 21 percent plan to acquire them within the next year.

Which security tools inspire confidence?

Network access controls also topped the list of security technologies that users have the most confidence in, with 25.8 percent of respondents saying they trust NAC most of all. DNS filtering came in second at 24.2 percent, anti-virus technology at 20.8 percent and web gateways at 20 percent.

Which technologies do IT security pros have the least amount of confidence in? Phishing simulation products topped that list, with 24.2 percent of respondents expressing dissatisfaction, followed by breach and attack simulation (BAS) technology at 20 percent, perhaps because of some overlap between the two. The success of phishing simulation training depends entirely on end user compliance, making it one of the biggest security nightmares for organizations, and also one of the hardest to fix.

Not surprisingly, phishing topped the list of areas where employees need training, at 31.7 percent, followed by data loss prevention at 27.5 percent–two areas characterized by employee error or malicious intent.
For more on the product confidence results, see Cybersecurity Simulation Tools Don't Inspire Confidence: eSecurity Planet Survey.

Emerging technologies face mixed demand

The survey looked at demand for newer security technologies and found mixed results.
Deception technology fared best among newer technologies, with 13 percent planning to adopt it in the next 12 months, followed by 11 percent planning to purchase breach and attack simulation technologies. Security orchestration, automation and response (SOAR) didn't fare as well, with planned adoption at 4 percent on top of 21 percent already using the technology.

Roughly a third of organizations unprepared

Drawing broad conclusions from the survey, roughly two-thirds of organizations appear well prepared to address security risks, while a third should reassess their controls.

About 64 percent of respondents said they conduct penetration testing at least annually, and 60 percent conduct threat hunting exercises at the same rate.

Respondents said they have the most the confidence in their regulatory compliance preparedness, with 75 percent expressing some level of comfort with their compliance controls.

Database security, advanced persistent threats (APTs), DDoS attacks, insider threats and ransomware are the biggest areas of concern, with a range of 27 to 38 percent of respondents expressing doubts about their preparedness for those threats.

One interesting note about enterprise security buying habits: A third of survey respondents said they conduct competitive "bakeoffs" between security products at least annually, but just under 7 percent have switched products as a result of those comparative evaluations.

For more on the cyber preparedness results, see A Third of Companies Are Largely Unprepared for Cyber Attacks: eSecurity Planet Survey.

Paul Shread is editor of eSecurity Planet