State of Cybercrime 2017

Security events decline, but not the impact

Even as the average number of security events dropped year-over-year, events that resulted in a loss or damage rose, and fewer companies reported no losses.

The past year has been tough for enterprise security teams. Attacks like **Petya** and **NotPetya** suggest that the impact scale is increasing dramatically. The recent leak of government-developed malware and hoarded vulnerabilities has given cybercriminals greater capabilities.

IT is struggling to keep pace with the flow of important security software patches and updates, and the continued adoption of recent technologies like the internet of things (IoT) creates new vulnerabilities to contend with.

Getting more serious about security

Security is getting more mindshare at the corporate level and more resources. Twenty percent of CSOs/CISOs now report to the board of directors monthly, *yet 61% of the boards still see security as an IT issue rather than a corporate governance issue.*

Companies are spending more on IT security. The bulk of that money is being spent on new technologies (40%), but companies are paying for knowledge, too, like audits and assessments, adding new skills, and knowledge sharing. They are also investing in redesigning their cybersecurity strategy and processes as well.

Security events declining, but not the impact

Estimated show that the number of security events have dropped 8.2 percent in the past 12 months, from an average of about 161 to 148 incidents. Despite the drop in the number of events, *68 percent of companies reported that their losses were the same or higher than the previous year.*

Although the overall number of events declined, events that resulted in a loss or damage rose. In the past 12 months, and the number of incidents involving phishing and ransomware attacks are also on the rise, as is the number of companies that experienced losses from a cyberattack.

The State of Cybercrime survey results show that most companies are raising the bar in their efforts to prevent or minimize damage from attacks. It also reveals that too many companies are not keeping pace with the threat environment or their peers' cybersecurity standards.