EXCLUSIVE RESEARCH FROM

IDG

EXECUTIVE SUMMARY

2017

U.S. State of Cybercrime

CSO

IDG Communications, Inc.

2017 U.S. State of Cybercrime

TODAY'S CYBERCRIMES ARE BECOMING MORE TARGETED AND BUILT FOR MAXIMUM IMPACT, leading to higher loss for organizations. Yet companies report fewer cybersecurity events in 2017 than in previous years.

Influx of Security Threats

It seems that massive cybersecurity attacks have become alarmingly common in 2017. In May, the WannaCry ransomware infected 57,000 computers in more than 100 countries across the globe. A month later, a similar but more complex malware called Petya/NotPetya crippled businesses, airports, banks and government departments across Europe and then spread to U.S. hospitals and businesses. The cybercrime spree continued with Equifax, Nyetya, Goldeneye, CloudBleed, and the WikiLeaks CIA Vault 7 hack; followed by 198 million voter records exposed and a presidential campaign hacked in France.

It's true that the growing sophistication of cyber attacks and the organizations that hatch them continue to confound governments, enterprises (+1,000 employees) and small- to mid-size businesses (<1,000 employees) alike, but the average number of security events experienced by U.S. companies actually dropped from 2016 to 2017. However, those events imposed more damage to organizations than a year earlier because hackers chose more targeted, higher-impact attacks that yield more lucrative results.

39%

report that the frequency of cybersecurity events has increased over the past year

U.S. companies reported an average of 147.8 cybersecurity incidents in 2017, down from 161.1 incidents a year earlier. This year, the average loss for one cybersecurity event cost

organizations $381,000, up from $255,000 in 2015. For enterprises, the average financial hit climbs for a single cybersecurity event to $884,000, up from $471,000 in 2015.

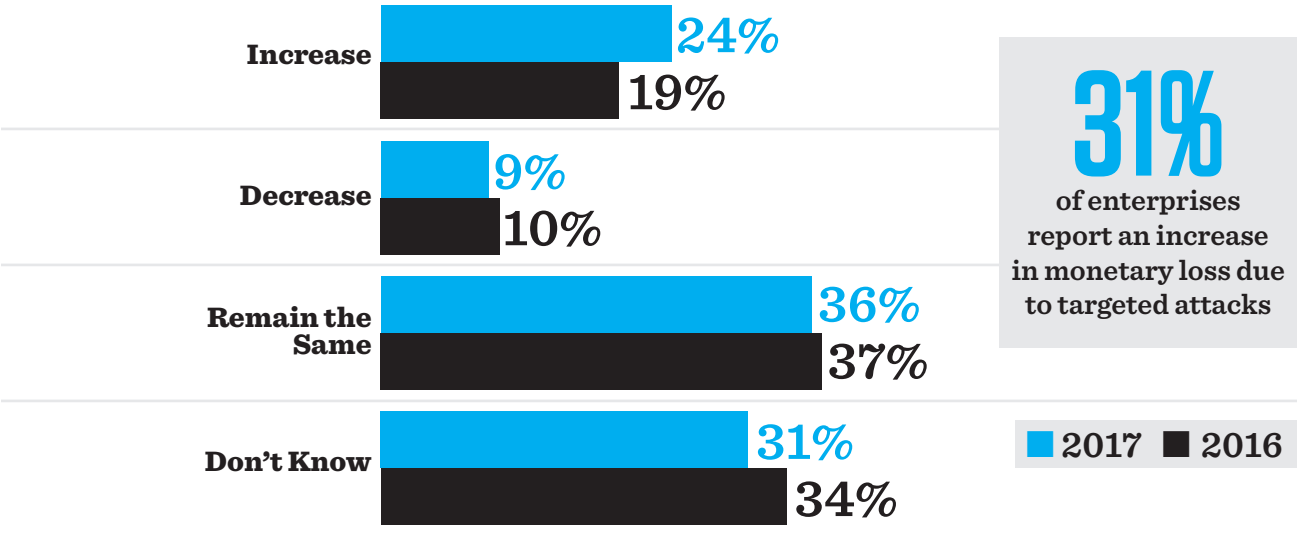
Those are just some of the findings of the 2017 U.S. State of Cybercrime Report, which surveyed 510 executives at U.S. businesses, law enforcement services and government agencies. The U.S. State of Cybercrime Survey, a partnership between CSO, U.S. Secret Service, CERT Division of Software Engineering Institute at Carnegie Mellon University and Forcepoint, is conducted annually to gain insight and evaluate trends in the frequency and impact of cybercrime incidents, cybersecurity threats and information security spending. The study also examines the risks of third-party business partners in private and public organizations. Respondents ran the gamut, from IT management (27%) and security management (21%) to business management (20%). The majority of those surveyed were manager level employees working in security, information technology or networking.

The survey also found that companies, in response, are becoming more sophisticated when it comes to cybersecurity prevention and countermeasures. They're making more technology investments, bolstering communication between security leaders and the board of directors, and scrutinizing business partners' security practices, to name a few.

Targeted Attacks on the Rise

While cybersecurity incidents are down, the damage they cause, measured in both data and financial losses, has risen, which indicates a growing number of premeditated attacks against a particular organization.

MONETARY LOSSES FROM TARGETED ATTACKS



31%
of enterprises report an increase in monetary loss due to targeted attacks

Targeted attacks aimed at a specific company, its employees, resources or customers accounted for 39% of cybersecurity incidents in 2017, up from 32% in 2016. Those targeted attacks attributed to 44% of financial losses in 2016, up from 34% in 2016. Incidental attacks, such as malware or phishing scams that happen to affect a company, accounted for 61% of cybersecurity events in 2017, down from 68% a year earlier.

Bad actors launched a breadth of attacks against organizations in 2017. Half of enterprises and 29% of SMBs report being most impacted by phishing attacks, the most widespread attacks with known losses. Viruses, worms and other malicious code impacted 34% of enterprises and 18% of SMBs, followed by spyware implanted into systems (27%/19%), network slowdowns (25% reported by both groups), email or app unavailability (23%/16%), ransomware infections (23%/14%) and denial of service attacks (23%/14%).

Average IT security budget

$11M

Not surprisingly, large companies are increasing their security budgets to address these targeted threats. More than half (59%) of enterprises increased their security budgets in 2017, with an average increase of 7.5%, while one-third of large companies held security budgets steady. Some 44% of SMBs increased their security budgets, while 52% saw no increase. Companies in the survey budgeted an average of $11 million for IT security.

Security Investments Paying Off

The boost in IT security investments may be responsible for the decrease in security incidents, according to survey figures. Cybersecurity events that organizations experienced over the past 12 months has decreased 9.5% since 2015. Companies have invested in new technologies (40%), conducted audits and assessments (34%), added new skills and capabilities (33%), redesigned process (17%) and participated in knowledge sharing (15%) to fortify their IT security posture.

When it comes to technology investments, survey respondents are mixed when it comes to their confidence in security solutions. The majority of security leaders say that the most effective security solutions continue to be firewalls, spam filtering, network-based antivirus, access controls and encryption. They view the least-effective solutions as manual patch management, complex passwords, change control/configuration management systems, one-time passwords, video surveillance and wireless monitoring.

Enterprises are also learning that cyber threats don't always come from the outside. Remote workers, countless contractors scattered globally, combined with a growing dependency on cloud services as well as BYOD devices, are ushering in a new era of insider threat-related security risks. One-third of enterprises surveyed say they are investing in initiatives that combat insider threats, such as upgrading security controls.

Our Own Worst Enemy

User behavior continues to be the weakest link in any organization's security chain, yet 19% of enterprises and 38% of SMBs don't monitor user behavior in their systems. Tools such as user behavior analytics can build a data analytics model where all log files, endpoint and network forensics, authentication requests and data access actions are aligned with individual users. While a third (34%) of enterprises say yes to having visibility into data protection vulnerabilities, compared to only 23% of SMBs, critics say this type of monitoring should be reserved for specific investigations, not security.

66%
of enterprise organizations have a formalized plan to respond to insider security events

When inside actors strike, the majority of enterprises (66%) have a formalized plan in place to respond to insider security events, compared to 40% of SMBs. Three quarters of respondents say they will handle the matter internally and without legal action.

Security Garners Slightly More Attention from the Board

Security is getting more mindshare at the corporate level and more resources, even if in some cases the gains are incremental. Twenty percent of CSOs/CISOs now advise the board of directors on a monthly basis, up from 17% last year. Yet 61% of the boards still believe security is an IT issue rather than a corporate governance issue. That number has barely changed from last year's 63%. With cybersecurity dominating much of the business conversation today, security executives are also taking a more prominent role. Today 35% of top security executives report to the CEO.

35%
of top security executives report to the CEO

More Firms Scrutinize Business Partners' Security Practices

High-profile breaches at Target, Home Depot and Wendy's that have been traced to vulnerabilities in third-party systems have prompted enterprises to take extra precautions when evaluating their supply chain and business partners. They're not afraid to take a hard line on those vendors that don't live up to their security standards.

Almost half (47%) of enterprises evaluate the cybersecurity of supply chain and business partners before conducting business with them, according to the survey, and nearly a third (31%) of respondents say they've terminated contracts or relationships with existing partners who don't live up to the company's security standards. More than half of large companies have service-level agreements with their business partners to specify minimum cybersecurity standards, compared to 36% of small and mid-size businesses. Almost half of all respondents

(48%) conduct incident response planning if and when third-party breaches arise.

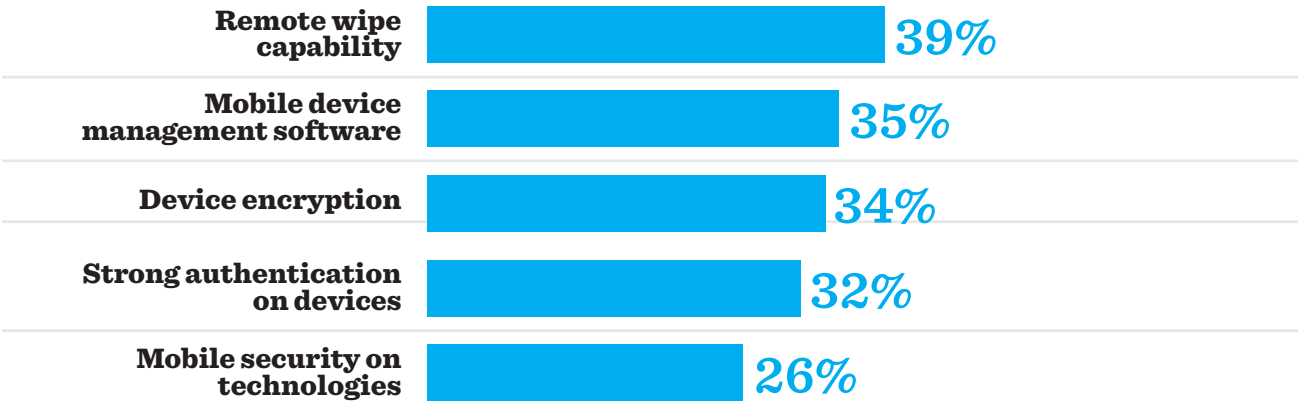
Fickle About Mobile Security Tools

Mobile devices, once considered immune from malware, are increasingly coming under attack. More than 1.5 million new incidents of mobile malware were detected by McAfee Labs in the first quarter of the year alone – for a total of more than 16 million mobile malware incidents reported to date. In response, organizations are taking steps to avoid mobile disruptions, and they're using a wide range of tools.

Some once popular tools have lost some luster. While remote wipe capabilities still lead the pack at 39%, its use is down from 50% from 2016. This could be because if the theft is intended to steal an employee's company data, by the time the user realized that his device has been lost or stolen and IT sends the commands necessary to perform a wipe, the data may already be compromised. More than 30% of organizations surveyed also use mobile device management software, device encryption and strong authentication on mobile devices. With it becoming easier and more common to mix personal and business devices, these technologies aim to bring a sense of comfort to the organization by adding an extra layer of defense.

MULTIPLE TOOLS USED TO SECURE MOBILE WORKFORCE

Which of the following does your company utilize to secure mobile devices?



Conclusion

The 2017 U.S. State of Cybercrime Survey shows that while the number of cybersecurity events is down, threat actors are targeting their prey for more lucrative breaches. Meanwhile, successful phishing and ransomware attacks are climbing and growing more difficult to detect. Concerns about security threats took a significant jump this year, but organizations are rising to the challenge with new tools, policies, board interaction and standards for third-party providers.

METHODOLOGY

The 2017 U.S. State of Cybercrime Survey was conducted among the CSO, U.S. Secret Service, CERT Division of Software Engineering Institute at Carnegie Mellon University, and Forcepoint audience/members. The survey fielded online between May 9, 2017 and June 27, 2017 with the objective to gain insight and evaluate trends in the frequency and impact of cybercrime incidents, cybersecurity threats and information security spending. The study also examines the risks of third-party business partners in private and public organizations.

Respondents job titles include IT management (27%), security management (21%), business management (20%), consultant (16%), staff (14%) and law enforcement (3%).

A broad range of industries are represented including information and telecommunications (17%), banking & finance (11%), electronics/technology (11%), education (10%), services (8%), healthcare (5%) and government (5%).

Results are based on 510 qualified responses. The margin of error on a sample size of 510 is +/- 4.3 percentage points.