McAfee
Together is power.

Grand Theft Data II: The Drivers and Shifting State of Data Breaches

Findings from a new McAfee® report

With the growth of cloud adoption and the rise in data breach visibility, is data exfiltration the same high-stakes game it was a few years ago? A new report from McAfee reveals the current state of data exfiltration, including employment repercussions and reputation damage if a breach occurs.

McAfee surveyed 700 IT security professionals from commercial organizations (1,000 to 5,000 employees) and enterprise organizations (more than 5,000 employees) around the world to learn about their data breach experiences. We asked about their success in finding breaches, how thieves are stealing data, the adversaries they are most concerned about, and what they plan to do to reduce the risk of a breach in the future.

Key Findings

- A majority of IT professionals have experienced at least one data breach during their career—61% at their current company and 48% at a previous company. On average, they have dealt with six breaches over the course of their professional lives.
- Nearly three-quarters of all breaches have required public disclosure or have affected financial results, up five points from 2015.
- Internal security is discovering the majority of breaches, with 61% of incidents discovered by the security team—up 14 points from 2015.
- The top three vectors for exfiltrating data are database leaks, cloud applications, and removable USB drives.
- Intentional insider theft is down 6% from 2015, and now accounts for 45% of incidents.
- IT is implicated in 52% of breaches. Business operations is the next most likely to be involved (29% of breaches). The most secure internal groups were finance (12%) and legal (6%).
- While cloud applications and infrastructure did not generate a disproportionate amount of breaches, IT professionals are most worried about leaks from Microsoft OneDrive, Cisco WebEx, and Salesforce.com. Since these popular cloud applications are widely used, it makes sense that they would be top of mind for respondents.

Connect With Us

- Security technology continues to operate in isolation, with 81% reporting separate policies or management consoles for cloud access security brokers (CASBs) and data loss prevention (DLP).
- More than half of IT professionals think that senior and C-level executives should lose their jobs if a data breach is serious enough, while a quarter think that they should absolutely lose their jobs after any breach.
- "Do as I say, not as I do." A full 61% say their executives expect more lenient security policies for themselves, and 65% of those respondents believe this leniency results in more incidents.
- The top two actions cited for reducing the risk of breaches in the future are integrating the various security technologies into a more cohesive defense and additional education and training for employees on security risks.

Who Is Responsible, How Data Is Exfiltrated, and What to Do About It

While data theft continues to affect most organizations, the nature of those thefts has evolved over the past three years. External adversaries are responsible for a growing percentage of thefts, possibly explaining the increase in breaches that require public disclosure. Hackers remain the leading criminal group, while malware authors increased their hold on the number two slot. For insider thefts, intentional employee thefts declined, while accidental ones increased, supporting the importance of continued security training.

Intellectual property is now tied with personally identifiable information as the data categories IT professionals are most worried about being stolen. Thanks to improvements in fraud detection and smart cards, payment card information has dropped to the number three concern. Direct competitors are the biggest concern when it comes to intellectual property theft, followed closely by internal employees. When international espionage is brought up, IT professionals are most concerned about China, Russia, and North Korea.

Data is stolen by a wide range of methods, with no single technique dominating the industry. Database leaks, network traffic, file sharing, corporate email, cloud applications, personal email, and removable USB drives all generated similar levels of response, possibly because multiple methods are used in a breach. Overall, cloud infrastructure and applications do not appear to be any more or less secure than traditional data centers.

Adding security technology to keep up with evolving threats is the first priority of about half of the IT professionals, and almost two-thirds have purchased additional products over the past 12 months. Data loss prevention, CASB, and endpoint detection and response (EDR) are the typical technologies in use, but more than half of organizations have yet to install (or properly configure) at least one of these. Between 65% and 80% of breaches experienced would have likely been prevented if one or more of these systems had been installed.

More than half of IT professionals think that senior and C-level executives should lose their jobs if a data breach is serious enough.

Investing in people, whether training existing employees or hiring new ones, is the second priority. Likely due to the shortage of staff, fewer than half of organizations surveyed said they managed to hire additional staff but almost two-thirds are investing in more education. Process changes are the third priority. Over the past year, more than half of the organizations surveyed have further developed their security operations center. One-third opted to work with an external managed security service provider.

Conclusions

Data thefts continue to increase and are a painful reality for most IT professionals. However, there is good news in this study. On the technology front, some fundamental tools remain under-deployed and, in most organizations, they operate in relative isolation and leave unnecessary gaps in coverage. Deploying, configuring, and integrating these security tools could go a long way toward reducing data thefts.

All employees are part of an organization's security posture, not just the IT team. Accidental disclosures represent more than half of the internal breaches. Education on identifying security risks, protecting sensitive information, and adhering to corporate policies is an important and continual task that can help reduce these incidents. So too, is providing learning opportunities for the security staff, as the shortage of experienced personnel makes it difficult to replace them.

Finally, lack of security best practices are still at the center of many data breaches. Default accounts, weak passwords, missing patches, and other features of good security hygiene may explain why IT is the group named by a majority as most likely to be responsible for a breach. At the same time, IT is now detecting a majority of the breaches, so process changes like active threat hunting and developing security operations centers is paying off.

Read the full report.

Learn More

For more information, visit us at **www.mcafee.com**.

For information on McAfee solutions to curb data exfiltration, visit:

McAfee® Data Protection
McAfee® MVISION Cloud
McAfee® MVISION EDR
McAfee® Database Security
McAfee® Web Protection

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com