Report

Grand Theft Data

Data exfiltration study: Actors, tactics, and detection

Grand Theft Data

Data exfiltration study: Actors, tactics, and detection

Table of Contents

Introduction

Security professionals have seen a lot of activity over the past few years. The ones we interviewed who had suffered a data breach experienced an average of six significant security breaches each. In 68% of these incidents, the data exfiltrated from the network was serious enough to require public disclosure or have a negative financial impact on the company, 70% of incidents in smaller commercial organizations and 61% in enterprises. The average number of breaches was highest in Asia-Pacific organizations and lowest in UK and US enterprises. More than 10% of Asia-Pacific companies reported over 20 breaches, compared to just above 1% of North American and 4% of UK enterprises reporting more than 20 breaches.

Most security studies and statistics focus on infiltration: how attackers are getting past security defenses and into the network. That part of the attack is more visible, compromising machines and triggering events and alarms in the security operations center. Until now, there has been very little information available on the less visible act of *data exfiltration*: how attackers are removing data. Whether you see it or not, data exfiltration is a real risk for most organizations. This report looks at the concerns and challenges facing commercial (1,000 to 5,000 employees) and enterprise (more than 5,000 employees) organizations in Australia, Canada, India, New Zealand, Singapore, the United States, and the United Kingdom.

Building on previous Intel Security research on the top five attack methods, improving attack detection and incident response, and critical infrastructure security, we embarked on new research to better understand data exfiltration. We spoke with information technology and security professionals with decision-making authority representing 1,155 organizations around the world, and interviewed 522 who had experienced at least one serious data breach in either their current or previous job. They were asked about their top concerns, breach and exfiltration details, outsider and insider threats, exfiltration differences between traditional networks and cloud applications, and the tools and practices they use to identify and prevent data exfiltration. Consistent with previous studies, privacy and confidentiality of customer and employee data were the biggest concern, and poor security practices the biggest challenge in the face of increasingly sophisticated attacks. Interestingly, insider threats, such as those perpetrated by disgruntled employees were the number two concern with the Asia-Pacific respondents, compared to sixth place overall.

Findings

- Internal actors were responsible for 43% of data loss, half of which is intentional, half accidental.
- Theft of physical media is still quite common, implicated in 40% of exfiltrations.
- 64% of security professionals felt data loss prevention (DLP) technology could have prevented their data exfiltration events.
- 25% of data exfiltrations used file transfer or tunneling protocols, such as FTP or SCP.
- 32% of data exfiltrations were encrypted.
- Microsoft Office documents were the most common format of stolen data (25%).
- Personal information from customers and employees was the number one target (62%), as the value of private personal data surpasses credit cards.
- Cloud deployments brought with them increased anxiety of more security breaches, although there was no indication of increased risk with cloud applications.
- Security professionals with five years or more experience at their current employer contributed to a stronger security posture and lower risk of serious data exfiltration.
- Respondents using data loss prevention (DLP) had a strong correlation with internal teams detecting and preventing data thefts.

The Perpetrators: External versus Internal Actors

Our research indicates that internal actors were responsible for more than 40% of the serious data breach incidents experienced by the respondents, and external actors were responsible for just under 60% of data breaches.

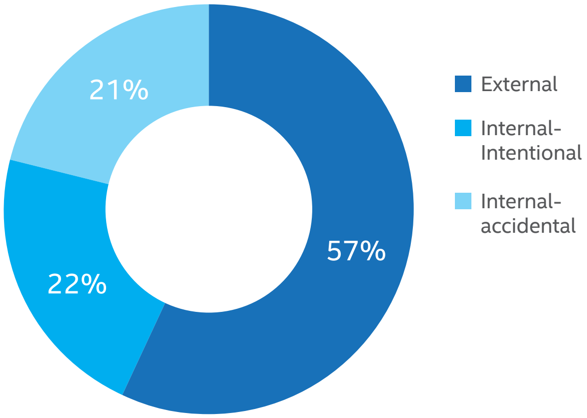

Figure 1. Actors involved in data breaches.

Internal actors include employees, contractors, and third-party suppliers, with a 60/40 split between employee/contractors and suppliers. When they were involved in data exfiltration, whether it was intentional (just over half) or accidental, internal actors were more likely to use physical media instead of electronic methods, especially USB drives and laptops. Employee information, both identity and health data, was a larger target for internal actors than customer data, perhaps because it is more accessible. Office documents were the most common format of data stolen by internal actors, probably because these documents are stored on employee devices and many organizations place few controls on the data once it is no longer in a database. Insider thefts accounted for almost 50% of data loss in Asia-Pacific, compared to less than 40% in the UK and 41% in North America.

What Data Are They Taking?

Data types	Internal Actors	External Actors
Customer Information	27%	32%
Employee Information	33%	28%
Intellectual Property	15%	14%
Payment Card Information	11%	15%
Other Financial Information	14%	11%

Data types	North America	United Kingdom	Asia-Pacific
Customer Information	31%	32%	34%
Employee Information	32%	25%	27%
Intellectual Property	13%	19%	12%
Payment Card Information	13%	14%	14%
Other Financial Information	11%	10%	13%

What Format Are They Taking?

Formats	Internal actors	External actors
Microsoft Office (Excel, PowerPoint, Word)	39%	21%
Plain Text/CSV	20%	21%
PDF	11%	20%
Images and Video	11%	18%
XML	12%	19%
Others	7%	1%

Formats	North America	United Kingdom	Asia-Pacific
Microsoft Office (Excel, PowerPoint, Word)	22%	30%	27%
Plain Text/CSV	24%	18%	16%
PDF	20%	13%	17%
Images and Video	16%	19%	19%
XML	17%	17%	18%
Others	1%	3%	3%

Respondents who had mostly experienced insider breaches indicated they were not as knowledgeable about email security, web security, and data loss protection (DLP). Likewise, they were less likely to have these technologies deployed than those who have experienced mostly external attacks. This is especially notable since DLP was identified as one of the two top security tools for catching insider data thefts.

"Organized crime, activists, and nation-states were identified 30% more often as external actors in Asia-Pacific than in other countries."

External actors included, in ranked order: hackers, malware authors, organized crime, activists, and nation-state intelligence services. Organized crime, activists, and nation-states were identified 30% more often as external actors in Asia-Pacific than in other countries. When external actors were doing the stealing, Microsoft Office documents remained the top exfiltration format, but only a couple of percentage points higher than plain text, CSV files, or PDFs. Image and video thefts were more likely perpetrated by external actors than internal actors, probably due to the attraction and value of finding images of celebrities and other public figures in compromising or embarrassing situations, which violated their privacy. When physical media were involved, external actors were more likely to target laptops, mobile phones, and webcams. External attackers were also more likely to steal customer data than employee data and were more interested in payment card information than internals.

With the significant contribution of exfiltration stemming from internal actors (43%), organizations should look at this as a cautionary tale. Reviewing operational practices and refreshing employee awareness training programs will help address the 50% accidental data loss. To adequately address the intentional internal threat, organizations should review their security technologies with the goal of understanding what controls are in place to protect the data from physical extraction, such as laptop theft or transmission to USB drive, and from digital extraction, such as email transmission or upload to cloud services.

What Data Is Being Taken and How?

Organizations are experiencing data loss across a wide range of content, formats, and methods—from documents to databases, stolen electronically or physically, and orchestrated by insiders or externals. More than 90% of security breaches in Asia-Pacific resulted in actual exfiltration of data, compared to 84% in North America and 80% in the UK.

Sixty percent of the reported data exfiltrations were achieved by direct electronic means, while the other 40% involved some type of physical media, such as stealing a laptop or downloading to a USB drive.

Customer and employee information were the top two content categories, including personally identifiable information (PII) and personal health information (PHI). Intellectual property was the next most popular content category, followed by payment card information and other financial information.

The most common data format for exfiltration was Microsoft Office documents, followed by plain text or CSV files, PDFs, images and video, and XML. Office documents topped the list in the UK and the Asian-Pacific countries, while plain text and CSV files moved into the top spot in North America. This could be due to a greater concentration of thefts targeting data centers and database storage in North America, rather than personal computers and other endpoints.

How Are They Taking Data?

Data exfiltration methods	Internal Actors	External Actors
Physical Media		
Laptops/Tablets	11%	13%
USB Drives	15%	8%
Mobile Phones	3%	6%
Printed Hardcopies	3%	4%
CDs/DVDs	4%	4%
Microphones/Webcams	2%	4%
Faxes	2%	3%
Electronic Methods		
Web Protocols	15%	16%
File Transfer Protocols	11%	15%
Email	10%	10%
Peer-to-Peer	6%	4%
SSH/VPN	3%	6%
Windows Management (WMI)	7%	5%
Images or Video	6%	5%
Routing Control Packets	3%	4%
Voice-over-IP (VoIP)	3%	4%
Instant Messaging	3%	3%
Remote Desktop	2%	3%
Other	5%	0%

Perhaps the most interesting part of the survey is how data was taken. The 40% of data stolen using physical media was mostly on laptops, tablets, or USB drives. Mobile phones, possibly due to the increased acceptance of bring-your-own-device programs, were involved in 15% of physical thefts. However, older types of physical media, such as printed copies, CDs, DVDs, and faxes are still being used to extract data from companies, so security teams must continue to include them in their planning. Even microphones and webcams were indicted, catching the blame in almost 10% of physical thefts.

The 60% of data stolen electronically was mostly via various web protocols, file transfer and tunneling protocols, or email. However, a wide array of other protocols and techniques were used between 5% and 10% of the time, such as peer-to-peer, secure shell, routing control packets, Windows Management Instrumentation, instant messaging, VoIP, and hiding the data within images or video. In addition, attackers are disguising the data being stolen to shield it from security defenses, using encryption, compression, obfuscation, chunking, and steganography. This range of protocols and concealment techniques illustrates the growing sophistication of cyberattacks and why it is challenging to catch data exfiltration with just perimeter and endpoint security—from threats both inside and outside the organization.

Exfiltration: Traditional versus Cloud Networks

Many technologies and applications are moving into the cloud. About 60% of respondents have officially deployed cloud-based applications, with a slightly greater percentage of cloud application usage in enterprise companies than in commercial organizations. In North America, cloud deployments were skewed even more towards enterprises, with 75% reporting cloud applications compared to 56% commercial, while in the UK it was almost the exact opposite. The UK also had higher overall cloud deployments, at nearly 70%. Fewer than half of Asia-Pacific respondents, commercial or enterprise, have cloud applications deployed, possibly due to bandwidth and latency constraints or their greater concern about a cloud service breach. Notably, professional services and manufacturing companies report a higher usage of cloud applications than the other industries represented.

Companies with cloud applications deployed were more likely to be very familiar with a wide range of security technologies and were probably already using the full range of tools within the organization. They were also deploying cloud applications with greater awareness of threats; on average, they thought that serious breaches were more likely to increase over the next two years. Given that virtually all of the respondents have already deployed cloud applications or plan to deploy them in the next 12 months, the benefits of clouds appear to outweigh the risks to most organizations.

When it comes to stealing corporate data, almost two-thirds of the breaches involved traditional corporate networks, and cloud break-ins accounted for the other third. While Asia-Pacific had fewer cloud deployments, they had a higher percentage of cloud-based thefts. North America and the UK had more traditional network thefts but more cloud deployments, so there was no statistical correlation in this research between volume of cloud deployments and risk of a security breach. It is probably more a case of thieves going where the valuables are.

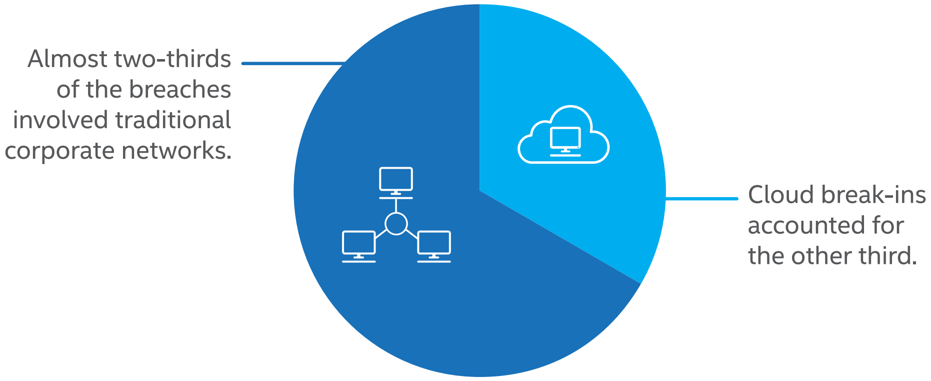

Figure 2. Cloud versus traditional network break-ins.

Organizations that experienced breaches on a traditional network tended to have a lower number of breaches overall, presumably indicating their ability to take direct action and address vulnerabilities, while cloud breaches were more likely to result in actual data exfiltration. Comparing traditional and cloud network breaches by type of content, the numbers are similar. Customer personally identifiable information accounted for 22% traditional and 20% cloud network theft. Employee personal information was taken in 19% of traditional network and 18% of cloud incidents. Payment card information was stolen in 14% of both cloud and traditional breaches. These results indicate that organizations invested in or looking to expand to cloud networks should conduct an assessment of the security controls in place by the data center or service, as is typically done for the corporate network.

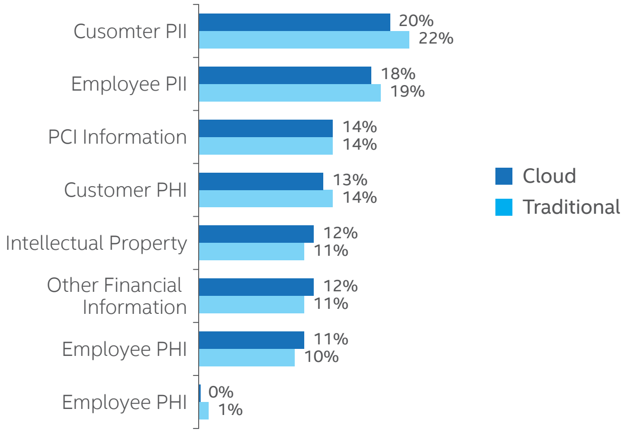

Figure 3. Comparison of the types of data targeted in the cloud versus traditional networks.

Education and Experience Matter

Education and experience play a big role in detecting and preventing data exfiltration. The survey respondents were split almost equally between professionals who have been with their current employer more than five years and those who have been there less than five years.

Professionals with more than five years of experience with their current employer were more likely to be very familiar with a full range of security technologies and were more likely to have them all deployed for a defense-in-depth security posture. Across the board, deployment of security technologies was higher in the UK than in any other country.

Experienced professionals were gathering information and educating themselves from a wider range of sources than those with less time at their current employer, especially from external advisors such as forensics firms, cyber infrastructure providers, and identity theft and credit monitoring companies. They were also more likely to be prepared—with risk and impact assessments of vulnerable areas, privacy and data protection awareness programs, and data breach response plans. Whether this is due to greater confidence, comfort level, or tenure, it makes a compelling argument for retaining security professionals and investing in their career growth. Experience also builds greater familiarity with the business, architectures, storage, processing, and applications and helps improve the efficacy of security solutions. Frequent turnover in the security team could likely increase the risk of experiencing another breach.

Data Breach Prevention Resources

Which of the following sources do you use to learn about how to prevent and/or manage through a data breach incident?	Five years or more at current employer	Less than five years at current employer
Privacy and security publications and websites	72%	66%
Privacy and security associations and conferences	67%	62%
Security technology/software vendors	66%	60%
Information from forensics firms, cyber insurance providers, identity theft/credit monitoring companies	53%	40%
Business publications and television programs	20%	10%

Security teams can improve their organization's security posture by learning from colleagues with more experience and taking these steps:

- Investing in employee security training and developing a security operations center.
- Increasing the frequency of network monitoring for unusual or anomalous traffic from weekly or monthly to at least daily or continuously. Almost 70% of those with five years or more experience monitored the organization's network at least daily, compared to 57% of those with less than five years of experience.
- Increasing their knowledge by reading more privacy and security publications, attending association meetings and conferences, soliciting input from external experts, and paying attention to the business publications relevant to their industry sector to understand what is valuable.
- Developing risk assessments and incident response plans.
- Focusing on basic security practices, such as employee training and awareness. Those with more experience realize that poor user security practices are still the biggest single threat to enterprises.

"... almost 70% of respondents felt that data loss prevention (DLP) technology could have prevented their past data exfiltration incidents."

Detection and Prevention Technologies Used

No single tool or technology will solve all data security problems, but almost 70% of respondents felt that data loss prevention (DLP) technology could have prevented their past data exfiltration incidents, especially the commercial organizations that were less likely to have it installed. Along with DLP, intrusion detection and prevention systems and next-generation firewalls accounted for the largest proportion of data breach discovery and prevention. Organizations that were continuously monitoring their network for unusual or anomalous behavior were more likely to detect data breaches with internal resources and more likely to have zero exfiltrations.

Continuous network monitoring and DLP technology displayed a strong correlation with improved security posture and breach detection. Those with DLP deployed reported a higher level of familiarity with and higher deployment rate of security technologies, a higher level of education and consumption of security information, and were 15% more likely to have their internal security team catch data breaches. For too many organizations, DLP was deployed or is still pending deployment only after the company experienced a serious data breach that required public disclosure. Many times, DLP was in monitor mode and not taking any action. The smallest commercial organizations were the least likely to have DLP currently in use, while almost 80% of North American enterprises had DLP currently installed.

Just over half of serious data breaches were discovered by internal security teams in the UK (55%), just under half in North America (48%), and even less in Asia-Pacific (39%). The remainder were caught by external agents, such as white hat hackers, credit card companies, and law enforcement.

Discovery of breaches by external actors was split almost 50/50 between internal security and external agents, while over two-thirds of insider thefts were caught by internal security teams. Remarkably, medium-size commercial organizations (2,500 to 5,000 employees) were the most likely to have their breaches discovered by external agents, perhaps due to growing pains and budget stresses as the IT and security organizations mature.

If the internal security team was catching security incidents, the organization was less likely to suffer actual data loss or theft. This is not surprising, since external agents can really only identify an exfiltration after data has been published or leaked. Security professionals reported an average of two breaches at their current employer when discovered by internal security versus five incidents on average for companies whose breaches were discovered mostly by external entities. Internally caught incidents are also less likely to result in actual data exfiltration, with a 70% probability compared to 92% for those found externally. Internal teams were also catching different things. For example, they were more likely to catch hackers, employee leaks, and theft of laptops or USB drives. External groups were more likely to catch attacks by organized crime, activists, and national intelligence services, stolen images and videos, leaks by third-party suppliers, and thefts by other physical media, such as mobile phones, printouts, CDs/DVDs, and faxes.

Types of Breaches Caught Internally versus Externally

Internal Teams	External Groups
• Hackers • Employee Leaks • Theft of Laptops or USB Drives	• Organized Crime and Activists • Stolen Images • Stolen Videos • Leaks by Third-Party Suppliers • Thefts by Physical Media (Such as Mobile Phones)

Notably, security professionals at companies that have experienced either a greater percentage of breaches by external actors or a greater percentage of breach discoveries externally are more likely to attribute their data losses to a wide range of causes, such as insufficient security training, failure to keep security patches up to date, employee actions, and insufficient funding from senior management. Commercial organizations were the most likely to identify insufficient funding as the main cause. Those experiencing more insider exfiltrations or internal detections were focused more on targeted phishing attacks and insufficient security training and awareness as the primary culprits.

Conclusion

The security market in general focuses more on preventing threats from entering the network than on detecting and stopping data from being exfiltrated. While preventing infections remains important, resources must be balanced to also search for indicators of compromise (IoCs) and protect valuable data from exfiltration. The most common responses to a security breach were to purchase more security products and invest more in employee security training. Asia-Pacific companies, which have overall reported a higher number of breaches and corresponding higher levels of security concern, were even more likely to take these steps, and also to invest in their security operations center and hire more staff.

With inside actors responsible for such a significant percentage of data loss, and half of that accidental, simple dynamic feedback can have a significant impact. For example, pop-up messages that let employees know a copy of their message is going to their manager and the security operations center due to the content sensitivity can quickly and effectively reduce risky behavior.

Physical media remains a high-risk area, and increases in flash memory density and device capacity will continue to increase the potential exposure. Classic perimeter and endpoint security provide little protection here, so other technologies, like encryption, data loss prevention, and even cloud applications help reduce this risk.

The growth in volume and complexity of personal information that organizations collect and store is increasing the value of this information exponentially. Determining what is appropriate to collect and what is justifiable to keep, developing detailed data policies, and frequently reminding employees of the importance of data privacy and confidentiality are at least as important as any security technology in protecting this valuable data.

Cloud applications, processing, and storage are already deployed by a majority of organizations worldwide, and this trend is on the increase. Almost all respondents who had not yet deployed cloud applications plan to do so within the next year. While cloud usage brings with it greater anxiety about security breaches, security technology providers are recognizing this and solutions are available today to help control where sensitive data is stored, how it is stored, and who has access to it. However, greater familiarity with and deployment of security technologies was strongly associated with a better cloud experience.

What do you do to prevent data breaches? Make efforts to retain your security professionals. Whether it is greater comfort or learning from their mistakes, professionals with longer tenure at their current employer delivered a broader and deeper set of security defenses, with more complete plans and assessments, built on a wider range of education and information sources.

Finally, investigate the benefits of DLP and intrusion detection and prevention systems, if they are not already installed, as they had a strong correlation with detecting and preventing data exfiltration. If they are installed, make sure that they are appropriately configured and actively contributing to your security posture, not sitting in a default passive or monitoring-only mode. Together, this combination of security tools, response plans, awareness training, and education will make your organization more defensible and less likely to suffer from data loss.

For more information about data loss prevention, visit www.mcafee.com/DLP. For more information about intrusion detection and prevention, visit www.mcafee.com/IPS.

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com