REPORT

McAfee
Together is power.

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

Findings from a new McAfee® report

Table of Contents

REPORT

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

Findings from a new McAfee report

Confidential information continues to be extracted from organizations around the world, despite increases in security technology and security education spending. Essential tools, such as data loss prevention (DLP) and endpoint detection and response (EDR) that could stop a majority of these breaches remain stubbornly under-deployed or are running in monitor mode. The good news is that the increase in security education appears to have reduced the incidence of accidental and intentional insider data theft. Overall, IT professionals are now discovering the majority of these breaches and hold themselves responsible for data loss. Many also think that senior executives should lose their jobs if a breach occurs on their watch, possibly because those executives demand more open policies for themselves.

The IT security professionals we interviewed in December 2018 experienced an average of six significant data breaches over the course of their careers. In almost three quarters of these incidents, the data breach was serious enough to require public disclosure or have a negative financial impact on the company, an increase of five percentage points from our 2015 data exfiltration study.

This new study looks at the data breach realities and responses of commercial organizations (1,000 to 5,000 employees) and enterprise organizations (more than 5,000 employees) in Australia, Canada, France, Germany, India, Singapore, the United Kingdom, and the United States.

We surveyed 700 information technology and security professionals with decision-making authority in a wide range of industries who experienced at least one serious data breach in their careers. They were asked about breach and exfiltration details, insider versus external threats, and the people, processes, and technologies that helped prevent these breaches, or could have helped prevent them. Consistent with previous studies, theft of personally identifiable information (PII) is the number one concern. However, increases in intellectual property theft have raised it to a tie for first place, well ahead of appropriation of payment card information.

Key Findings

- A majority of IT professionals have experienced at least one data breach during their careers—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.
- Data breaches are getting more serious and are under greater scrutiny. 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 are finance (12%) and legal (6%).
- While cloud applications and infrastructure do not generate a disproportionate amount of breaches, IT professionals are most concerned about Microsoft OneDrive, Cisco WebEx, and Salesforce.com.
- Security technology continues to operate in isolation, with 81% reporting separate policies or management consoles for cloud access security brokers (CASBs) and 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.

Breaches Are Occurring

Data theft continues to affect most organizations, with 61% of IT professionals reporting at least one data theft incident over their careers. The frequency of these incidents appears to be increasing, as 61% reported a breach at their current company, but only 48% at their former company.

Figure 1. Data breach experiences.

Severity of breaches is also growing. Over the past three years, the percentage of organizations experiencing a breach serious enough to require public disclosure or having a negative financial impact on the company has risen from 68% to 73%. On average, respondents have experienced almost six serious breaches each during their professional lives to date, 5.4 each at commercial organizations and 6.1 at larger enterprises.

Who is taking the data?

External actors and threats are responsible for an increasing percentage of data theft, rising from 57% of breaches in 2015 to 61% in 2018. External actors include hackers, malware authors, organized crime, nation states, and activists. The most significant change over the past three years in this group was an increase in malware-driven theft, rising from 23% in 2015 to 29% in 2018.

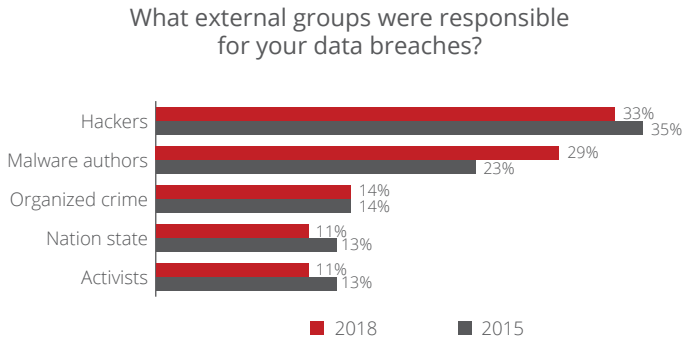

Figure 2. Sources of external data breaches.

Internal actors are a mix of employees, contractors, and other parties with inside access. This category includes both intentional and accidental exfiltrations. Employee-driven breaches account for almost 60% of internal incidents. The most significant changes in this group are a four-point increase in accidental breaches (27% to 31%) and a six-point drop in intentional breaches (30% to 24%). The shift towards more accidental breaches points to the continued importance of repeated security awareness training.

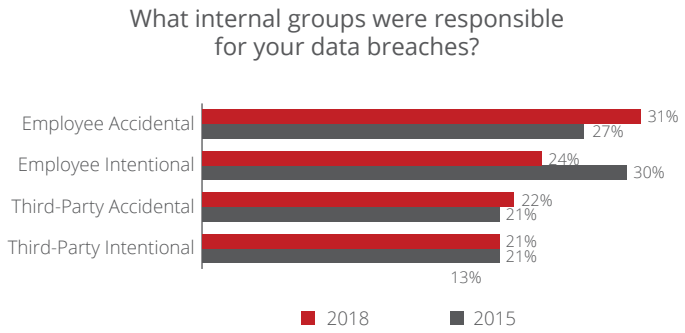

Figure 3. Sources of internal data breaches.

Which internal groups are the biggest risk?

New to this year's report was a question about which internal groups generate the most data leaks. Interestingly, IT or security departments are involved in just over half of all leakage events, and more than 60% of those occur in Asia-Pacific organizations.

Business operations and production are second at 29%, possibly due to their extensive interactions with a wide range of external entities. Sales employees are in third place, at 26%. A common case in sales is individuals downloading their contacts prior to leaving the company. Least likely groups to cause leaks are legal (6%), finance (12%), and human resources (15%), demonstrating that these groups are recognizing the sensitivity of the information they work with. Sixty percent of respondents use information like this to target their high-risk groups for additional information security training.

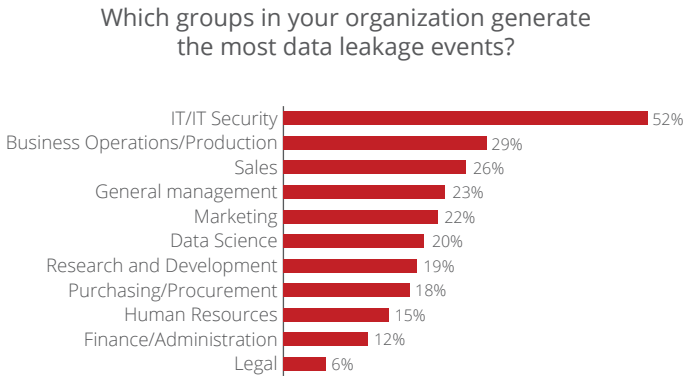

Figure 4. Data leakage events from different internal groups.

What data are you worried about insiders taking?

Personally identifiable information (PII) and intellectual property (IP) are now tied as the data categories with the highest potential impact to 43% of respondents. Notably, PII is of greater concern in Europe (49%), most likely due to the recent enforcement date of the General Data Protection Regulation (GDPR). In Asia-Pacific countries, intellectual property theft is of greater concern (51%) than PII. Continuing improvements in fraud detection and prevention methods for credit cards are likely responsible for the declining concern over theft of payment card information (PCI), which now ranks third at 30%.

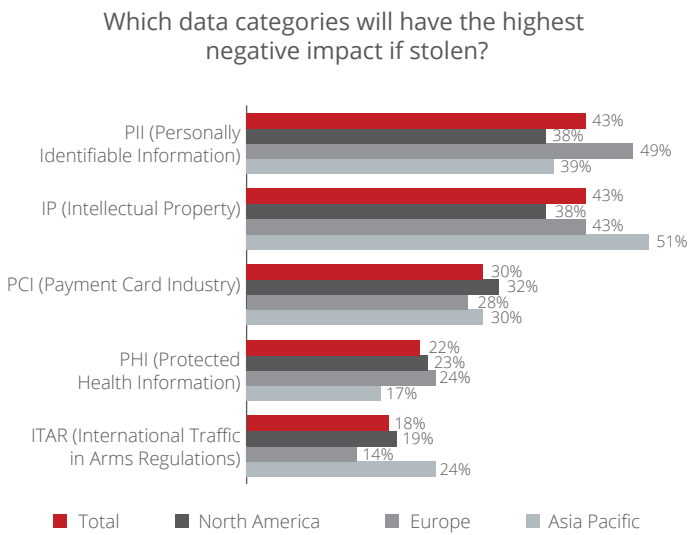

Figure 5. Data with biggest impact in a breach.

When it comes to intellectual property theft, direct competitors are seen as the primary source of concern (23%), followed by internal employees (19%). This may be a combined threat due to job changes and movement of people between companies within the industry.

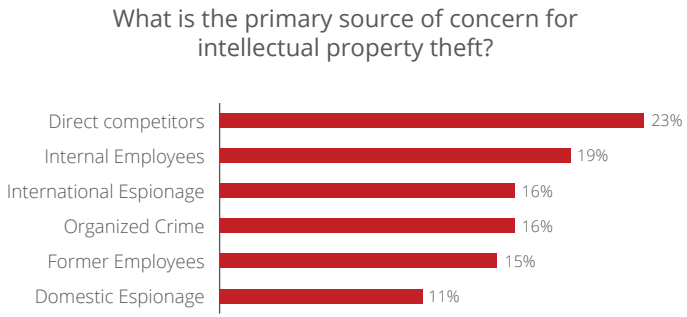

Figure 6. Worries about IP theft.

In general, companies consider structured data to be a higher priority for protection (45%) than unstructured data (39%), but North American firms are most likely to consider both equally important (48%). In the survey, structured data is defined as databases typically associated with information such as payment card data and health records. Unstructured data is defined as documents typically associated with intellectual property like formulas, designs, and proprietary knowledge.

Who are you afraid of?

Intellectual property and international espionage

Overall, nation-state actors are the number three source of concern for international property theft. The top countries of concern are China, Russia, and North Korea.

For some industries, however, international espionage is the number one concern for IP theft. These include automotive, biotechnology, electronics, financial services, and manufacturing.

Overall, 55% of organizations buy insurance to protect themselves from IP theft, and a further 36% plan to add this protection within the next few years.

How are they taking data?

Confidential data is being stolen by a wide range of vectors, both electronic and physical. Overall, database leaks and network traffic are the most common vectors. However, corporate email is number one in North America, while USB drives are the number one exfiltration vector in European and Asia-Pacific countries.

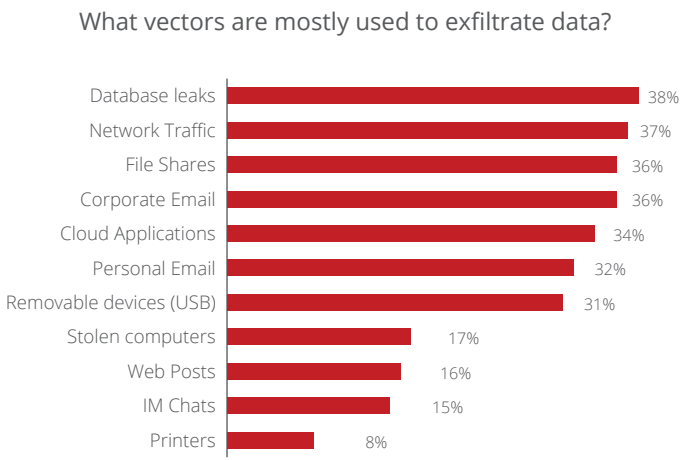

Figure 7. Data exfiltration vectors.

When it comes to insider threats, email leakage is the biggest security hole, followed by risky users and USB drives. All of these could be significantly reduced with additional education on corporate policies and appropriate online behavior. This helps explain why education is one of the top two tactics targeted to help reduce exfiltration.

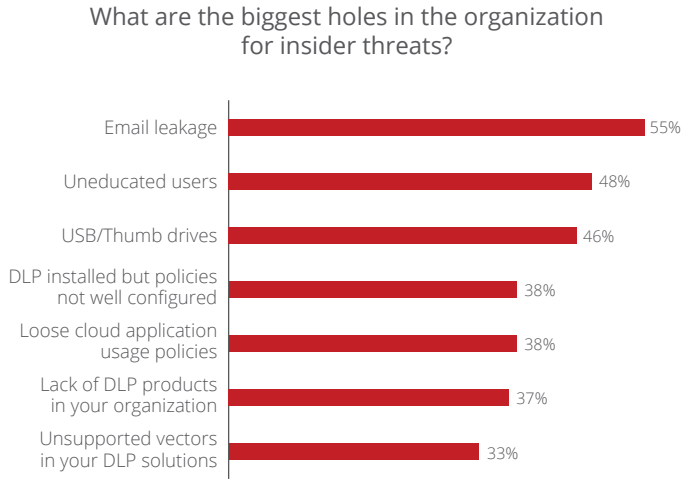

Figure 8. Biggest holes for insider theft.

How are the clouds doing?

Cloud applications and infrastructure are widely deployed, yet do not appear to result in any more data theft than traditional networks and data centers. Almost half of the organizations surveyed (46%) use a hybrid cloud/on-premises data storage approach, 29% are cloud only, and 25% keep their data on premises. Around two-thirds (63%) of the breaches experienced by the respondents occurred on traditional networks, and one-third were on cloud infrastructure. Even with the substantial increase in cloud usage over the past three years, this ratio has remained the same, pointing to the potentially effective security available for or from cloud providers.

However, this does not stop people from worrying about the cloud. When asked if they had big concerns about Infrastructure-as-a-Service (IaaS) cloud providers, respondents named Amazon Web Services (AWS) (22%), Google Cloud (21%), Oracle Cloud (18%), and Microsoft Azure (16%). When presented with a list of cloud applications and services and asked which ones they are most concerned about, respondents listed Microsoft OneDrive as number one, followed by Cisco WebEx and Salesforce. Since these popular cloud applications are widely used, it makes sense that they would be top of mind for respondents.

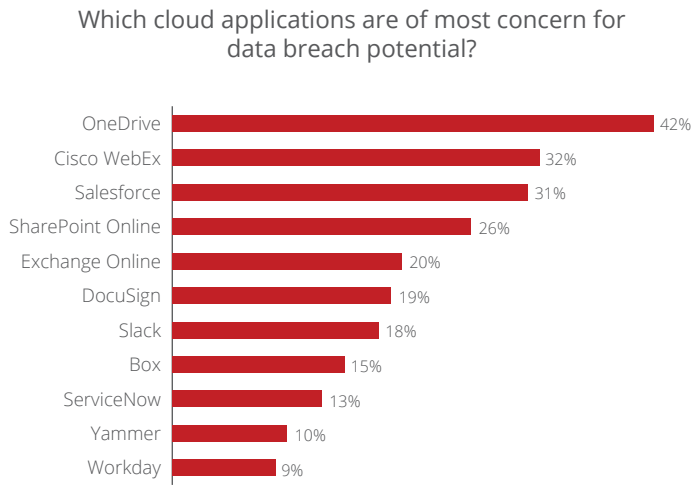

Figure 9. Worry about cloud applications.

What to Do About It

Security technology continues to be the first priority in terms of keeping up with evolving threats for about half of organizations worldwide (49%), followed by enhancing the skills of their people (29%), and changes to business processes (22%). One reason that people are not the top priority is the scarcity of security expertise. Identifying and hiring additional security people may not be a viable option, due to lack of availability or the salary expense.

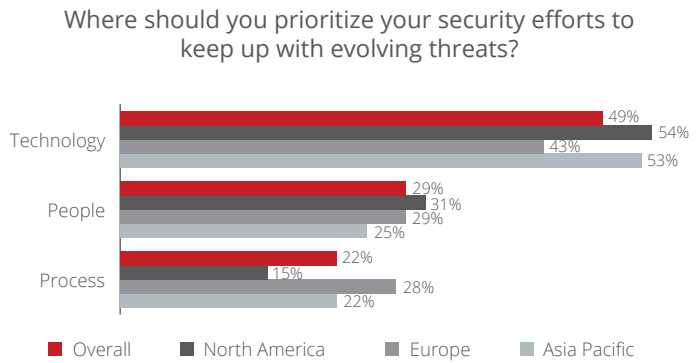

Figure 10. Priorities: technology, people, process.

Over the last 12 months, more than half of all organizations have purchased additional security products, invested in employee security training, and enhanced the capabilities of their security operations center (SOC). Just under half have hired more security staff, while a third have chosen to work with a managed security service provider.

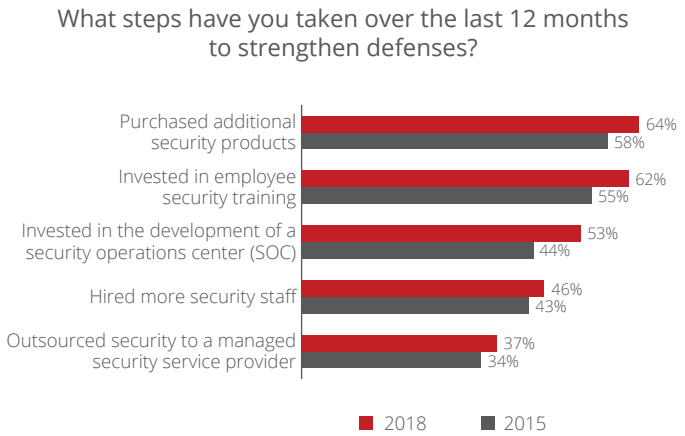

Figure 11. Steps taken to strengthen defenses.

What technologies are used (or should be)?

DLP, EDR, and CASB are the typical security technologies deployed to combat data theft.

Security technology	Deployed percentage	Likely would have prevented breach if it had been installed
EDR	67%	80%
CASB	65%	68%
DLP	42%	68%

All too often, even if these tools are deployed in an organization, they are left in a default configuration or in monitor-only mode. There can be several reasons for this, but the two most common are lack of experienced resources to properly configure the tools or a belief that automatically blocking suspicious activities causes too much disruption to business activities or production processes.

After getting the above tools deployed and configured effectively, the top technology-related step towards reducing the risk of data exfiltration is integrating the multitude of security technologies. For example, while 62% of organizations interviewed have both CASB and DLP in place, 81% of those have separate policies and/or management consoles for these tools, resulting in delayed detection and remediation actions.

Figure 12. Steps planned to reduce risk.

Which people are helping?

There have been interesting changes in who is discovering data breaches. In 2015, only 47% were discovered by internal actors, and that has risen to 61% in 2018. Internal security teams were responsible for finding 42%, and other non-security employees caught 19%.

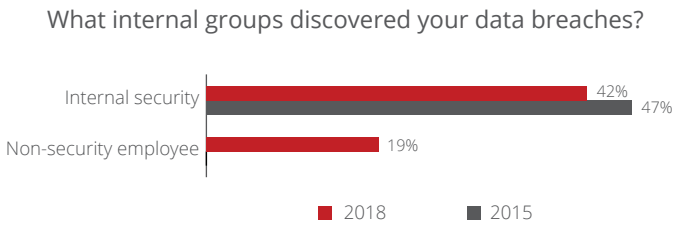

Figure 13. Internal breach discoveries.

External discoveries dropped from 53% to 39% over the past three years. "White hat" hackers lead the group of external allies (16%), followed by law enforcement agencies and credit card companies (tied at 11%).

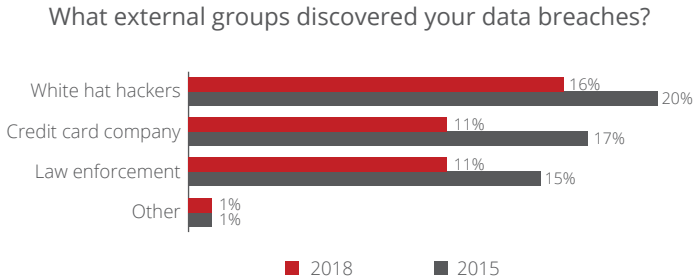

Figure 14. External breach discoveries.

Active threat hunting has been shown to have a significant impact on the speed of threat discoveries. More than half (52%) of organizations have people and resources allocated to threat hunting, while 30% are planning to implement this strategy.

Going forward, 17% of organizations plan to invest in more security professionals, while just 12% plan to prioritize better human-machine teaming. This last point has been shown to have a significant impact, improving time to discovery and remediation, reducing data overload, and decreasing false positives, according to MIT researchers.

When asked about personal responsibility, more than 70% of IT professionals believe that the IT department holds primary responsibility for a breach. Further, about 25% think that C-level executives should absolutely lose their jobs after a breach occurs, and 55% think that job loss depends on the severity of the breach. This could be related to the fact that 61% of respondents believe executives at their organization expect more open and lenient policies. Of those respondents 65% believe this leniency results in more incidents.

How are processes changing?

The most important process change, according to 18% of respondents, is additional security education or training. In six out of 10 organizations, this additional training is focused on the groups that are more likely to generate incidents. (See Figure 4. Data leakage events from different internal groups.) A small group (14%) are working to establish more formalized information-sharing policies related to sensitive and confidential data.

Many of the process changes are aimed at containing insider threats. Half of the organizations surveyed are using some type of digital forensic tools to counter these activities. However, there was little consensus on the most effective insider threat detection technologies. Respondents listed a broad range of tools and processes in use for this purpose, including email filtering, web filtering, DLP, EDR, user and entity behavior analytics (UEBA), and CASB. No single process or tool was used by more than 60% of organizations. This could be partially due to the broad range of insider exfiltration mechanisms, including email leakage, uneducated users, and USB drives.

Figure 15. Insider threat detection processes.

Most respondents (74%) feel that the enactment of GDPR has resulted in data security improvements for their organizations, and that they are prepared to make breach notifications within the three-day period specified in the regulation.

Taking It Personally: Personal Data Breaches Against IT Professionals

More than one quarter of the survey respondents have experienced a breach of their own personal data. Only 8% thought that the organization in question handled this personal breach poorly, although 38% thought that it could have been better. Interestingly, 53% thought their own employer would do a better job handling such a breach, and 20% thought they could do much better.

Conclusions

Data theft is a large and growing concern affecting almost every size and type of organization. A majority of IT professionals have experienced at least one breach, and, on average, they have experienced six breaches over the course of their careers. Breaches are also getting more serious, impacting financial results or requiring public disclosure. New and pending privacy legislation around the world, such as GDPR, will only increase the level of scrutiny.

External actors are responsible for an increasing percentage of thefts. Payment card information is now much less of a target, likely thanks to better protections, deployment of new payment technologies, and enhanced fraud detection systems. However, this has shifted criminals' focus to personal information and intellectual property. Database leaks, network traffic, and file shares are the most likely exfiltration vectors. Cloud usage continues to increase but is not responsible for a disproportionate amount of data breaches. That does not stop people from worrying about it.

The bad news is that IT and security organizations are considered the biggest sources of data exfiltration events, probably due to weak or default passwords, missing security patches, and other poor security hygiene. Business operations are second on this list, probably as a result of poorly secured data and file-sharing processes and shadow IT. Legal and finance departments are the least likely to cause a breach and should be studied further to identify their best practices.

The good news is that IT teams appear to be getting better at finding the breaches. A majority of breaches are now discovered by the internal security team, as they expand their security activities from primarily prevention to encompass rapid detection and remediation. There is a strong sense of personal responsibility within IT, which many respondents think should extend to the executive levels. A majority believe that C-level executives should lose their jobs after a serious breach.

Technology integration and employee education are thought to be the top two actions to reduce the risk of data exfiltration. However, full deployment and active configuration of fundamental security technologies—such as CASB, DLP, EDR—is an important step that would be likely to stop as much as 80% of breaches experienced by respondents.

Learn More

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

For information on McAfee solutions to these issues, visit:

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

About This Study

This study was conducted by MSI-ACI Europe, on behalf of McAfee. Survey respondents had to have experienced a serious data breach incident sometime in their careers as IT professionals. Data was collected via online interviews between December 12, 2018 and 31, 2018. To qualify for the survey, organizations had to have more than 1,000 employees, and were evenly split between commercial organizations (1,000 to 5,000 employees) and enterprise organizations (more than 5,000 employees). The resulting global group represented three major regions and a wide range of industries.

See the infographic and executive summary associated with this report.

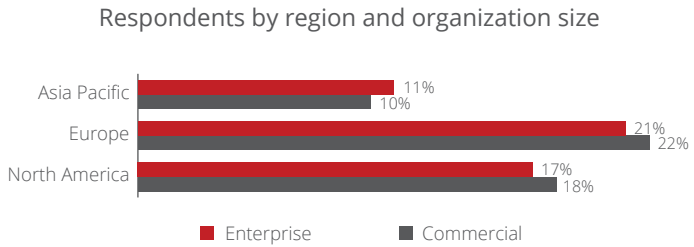

Figure 16. Survey demographics.

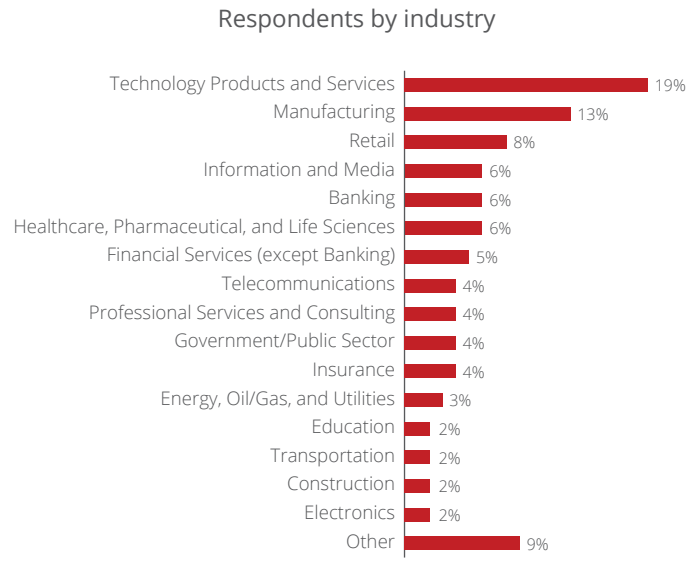

Figure 17. Survey industries.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com