RESEARCH REPORT

**DECEMBER 2017**

# 2017 Cyber Security and Data Privacy Study

## How does your company compare?

THE USI ONE ADVANTAGE®

# TABLE OF CONTENTS

By Dena Cusick, National Practice Leader,
Technology, Privacy and Network Risk

# 2017 Cyber Security and Data Privacy Study

## How does your company compare?

## Ransomware. Denial of service. Malware. Business email compromise scams.

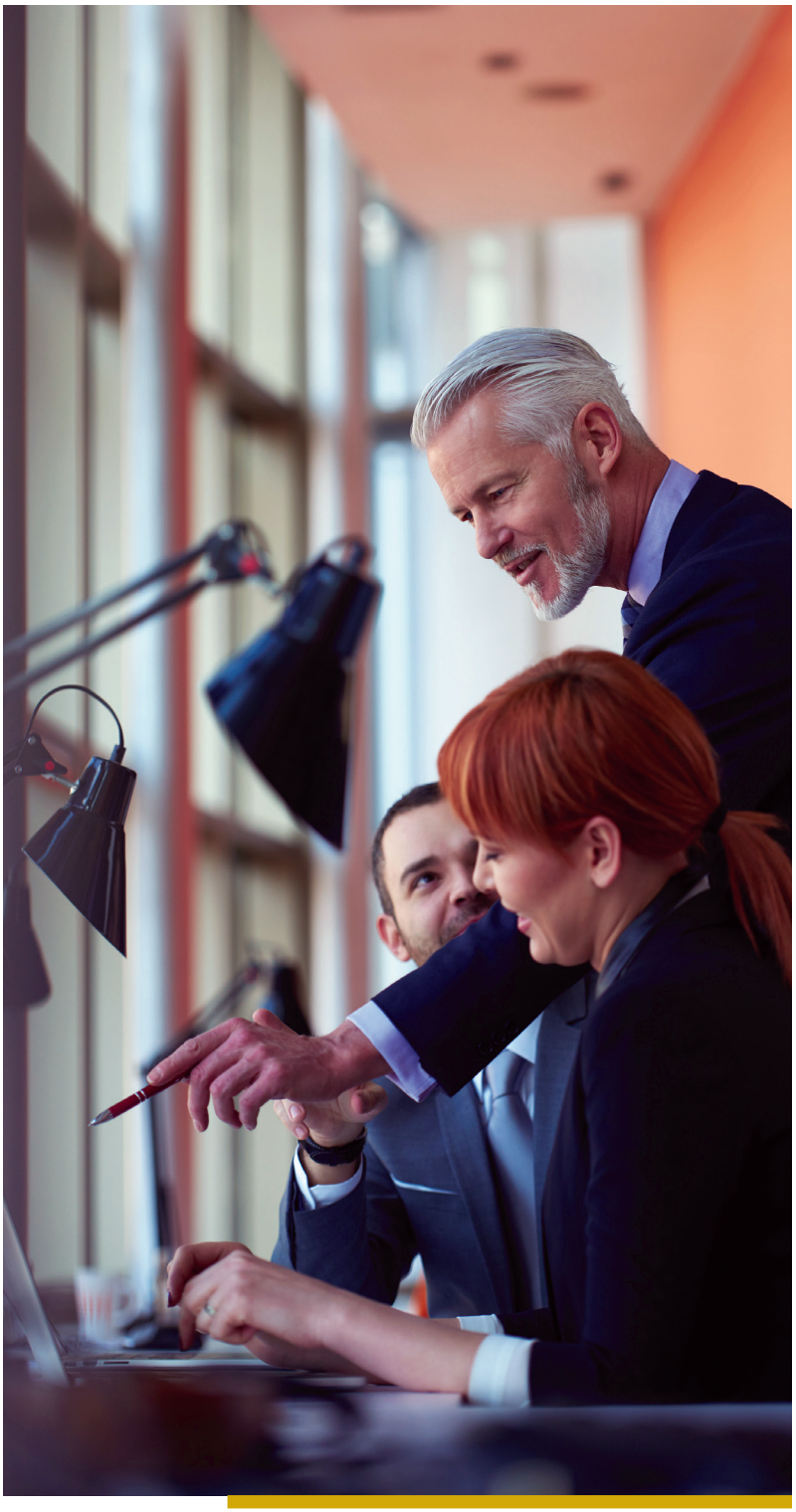
Increasing levels and types of cyber threats are making headlines and creating concerns for large and smaller businesses alike. Four in 10 large businesses have experienced ransomware, 70% of which suffered a monetary loss. Smaller businesses are not immune to threats either. Nearly one in three has experienced some sort of data privacy incident.

Companies, large and smaller, are aligning their information technology (IT) budgets to address cyber security. Nearly nine in 10 large businesses have increased their budgets for IT and data security in the past year. More than seven in 10 smaller businesses have also done so. In addition, companies are also taking other preparatory steps such as developing incident response plans and purchasing insurance to address the financial impact of a cyber event.

These findings are among the many insights from the USI 2017 Cyber Security and Data Privacy Study. This year's study is a follow-up to research conducted in 2015 and 2016. As in previous years, we surveyed 100 decision-makers at companies with $100 million or more in annual revenue. This year, we expanded the study to include another 100 businesses with annual revenues ranging from $5 million to $100 million.

### Our goal was to understand:

- Trends in whether companies' security vulnerabilities and perceptions are changing over time
- Current levels of preparedness and perceptions of security and network vulnerabilities
- Challenges that companies face when reviewing their coverage options
- Exposures related to business interruption costs
- Incident experiences



# KEY FINDINGS

## Most businesses, large and smaller, cite cyber security and data privacy risk as a high priority.

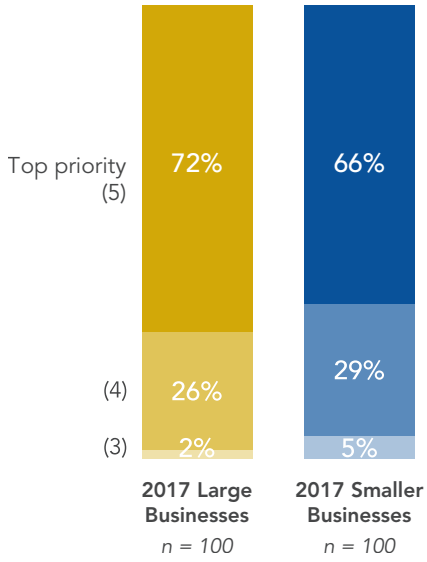
In 2017, cyber security and data privacy remain at the forefront as a critical issue affecting US businesses. With the complexity of cyber threats and their increasing frequency, it's no surprise that our study showed that more than seven in 10 large businesses and six in 10 smaller businesses cited cyber security and data privacy as a top priority. To address this concern, businesses in our study (both large and smaller) said they have increased their budgets for information technology and security over the past year.

The perceptions that cyber risk is increasing are accurate. According to the 2017 IBM X-Force Threat Intelligence Index, the number of records compromised grew 566% in 2016 from 600 million to more than 4 billion.[1] The index states that the leaked records included data traditionally targeted by cybercriminals, such as credit cards, passwords, and personal health information. There also were a significant number of breaches related to unstructured data, such as email archives, business documents, intellectual property, and source code.

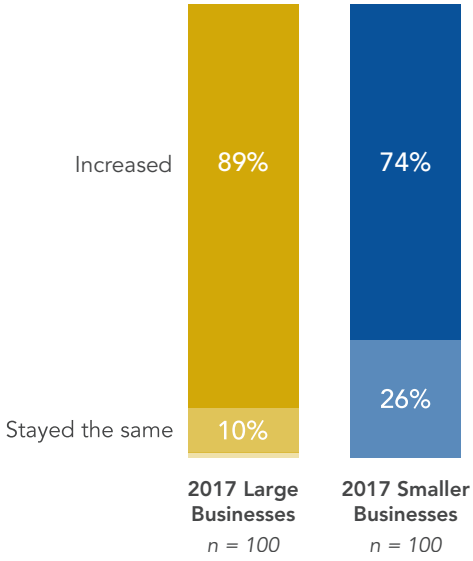
Meanwhile, Verizon's 2017 Data Breach Investigations Report cited a 50% increase in ransomware attacks, compared to figures from its 2016 report.[2] Ransomware is a type of malicious software that uses encryption to prevent an organization from accessing its own data, devices, files, folders, and computer systems. It's accompanied by a demand for payment — commonly in bitcoin or other form of cryptocurrency — to release the decryption key.

No matter what type of cyber incident may occur, the consequences to an organization of any size can be catastrophic. It can lead to loss of sensitive or proprietary information, disruption to regular operations and potential downtime, financial losses due to the cost to restore systems and files, and reputational harm.

Level of priority of protecting company from cyber security and data privacy risk from board/senior management




Change in budget allocation for information technology and security over the past year

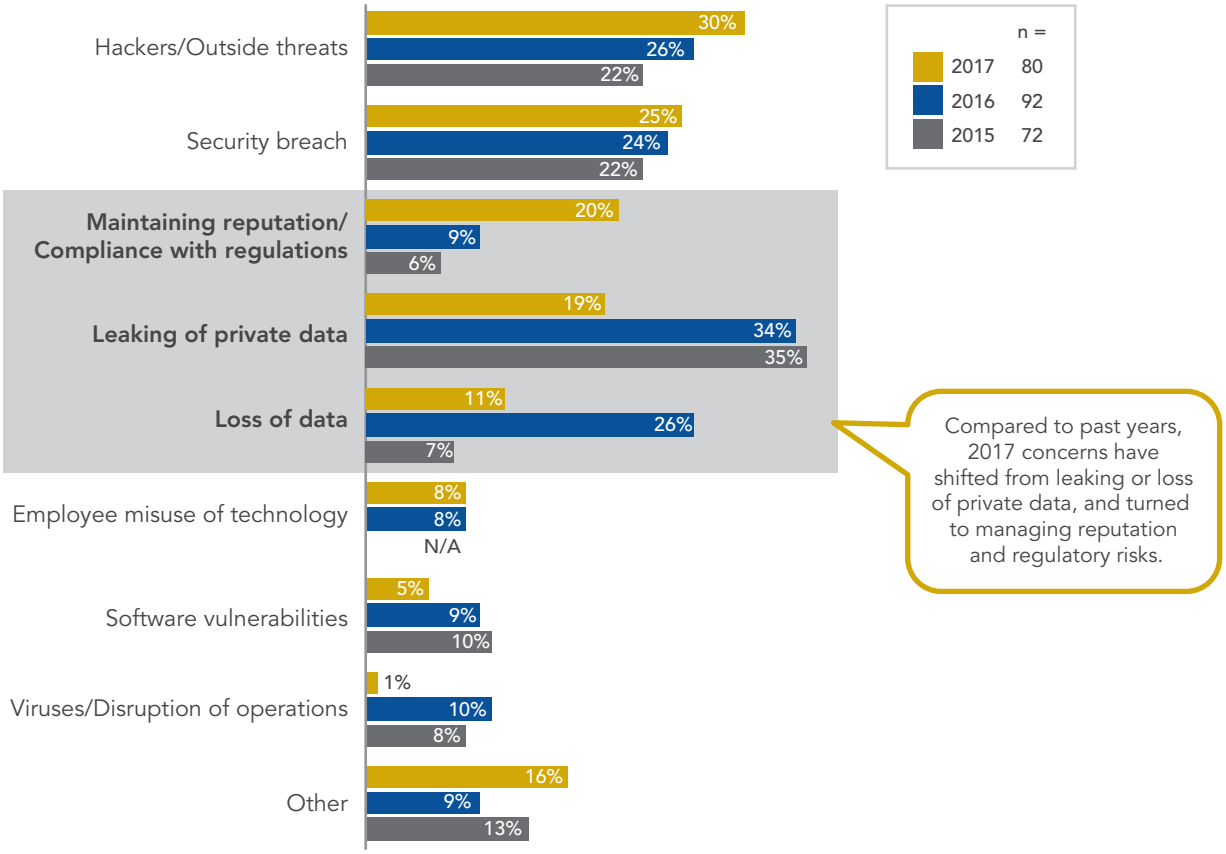


# CYBER SECURITY AND DATA PRIVACY RISK

## Cyber security and data privacy concerns have been relatively consistent during the past three years. However, maintaining reputation is now significantly more important.

### Primary cyber security and data privacy risk concerns for company

*2017 Comparison — Large Businesses*



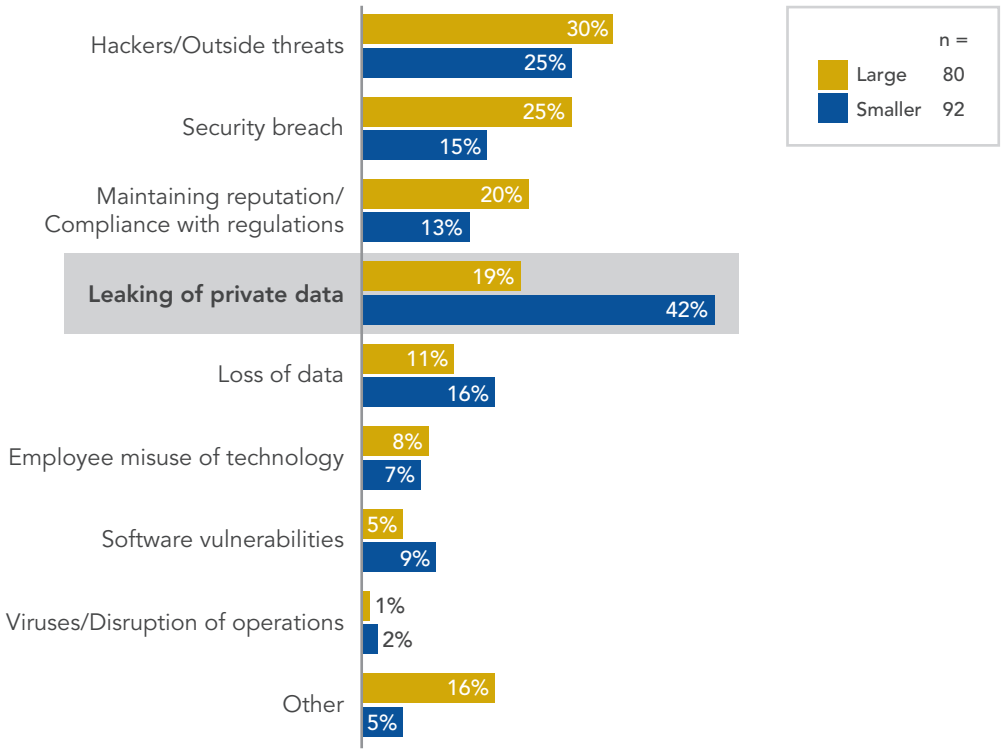

While the cost of dealing with cyber incidents continues to grow, so does the concern over less tangible losses. Among large companies, our study showed a notable increase in concerns about maintaining reputation and compliance with regulations. This concern jumped to the #3 spot, with 20% indicating they were worried about it compared to just 9% in 2016 and 6% in 2015. This finding is supported by a recent Forbes Insights report, which said that 46% of organizations suffered damage to their reputation and brand value as a result of a security breach.[3]

Damage to the reputation of an organization that experiences a breach can be catastrophic or minimal — it depends on the public's perception and understanding of the event. Engaging the right people at the right time to communicate a well-thought-out message is the first step to managing an organization's reputation in the wake of an incident and is a critical part of an incident response plan.

## Smaller businesses are significantly more likely than large companies to mention leaking of private data as a primary concern.

### Primary cyber security and data privacy risk concerns for company

*2017 Comparison — Large vs. Smaller Businesses*




For large businesses, concerns about hackers and outside threats in 2017 surpassed the leaking of private data, which was the top concern in both 2015 and 2016. Smaller businesses, however, ranked leaking of private data high on the list of concerns, with more than four in 10 citing it as their top concern. The difference in concern levels may be because smaller businesses don't have the resources to respond to a leak of private data.

In addition to the FBI recommendations presented here, other best practices include instituting a "clean desk" policy, ensuring security for physical locations, restricting access to sensitive information and databases, instituting record retention and destruction policies, evaluating mobile device management, and encrypting portable devices.

**According to the FBI, best practices to protect private data include:**

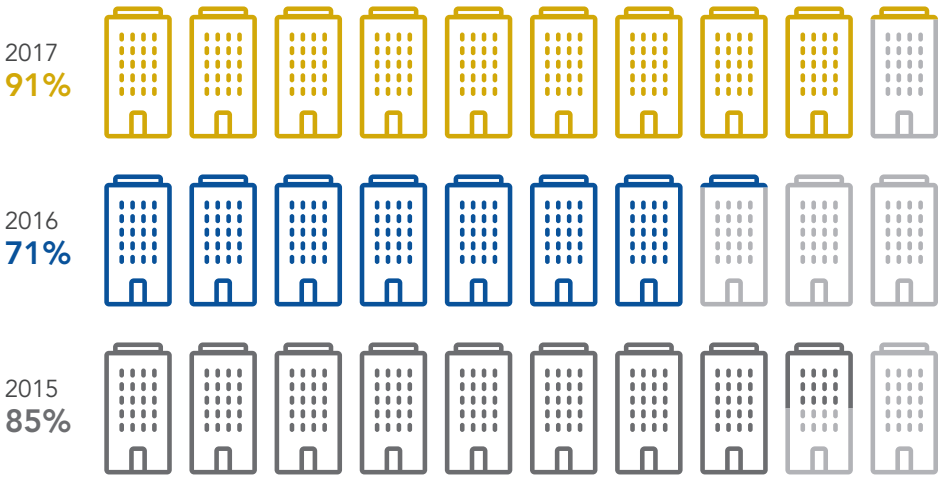
- Educating and regularly training employees on security or other protocols
- Ensuring that proprietary information is adequately protected
- Using appropriate screening processes to select new employees
- Providing nonthreatening, convenient ways for employees to report suspicions
- Routinely monitoring computer networks for suspicious activity
- Ensuring security and computer data security personnel have the tools they need[4]

# CYBER SECURITY AND DATA PRIVACY INSURANCE OWNERSHIP

**A majority of large and smaller businesses purchase cyber security and data privacy insurance. The top reasons for doing so are preparation for data breaches and protection against financial loss.**

## Large businesses currently purchasing cyber security and data privacy insurance

n = 100 for all years

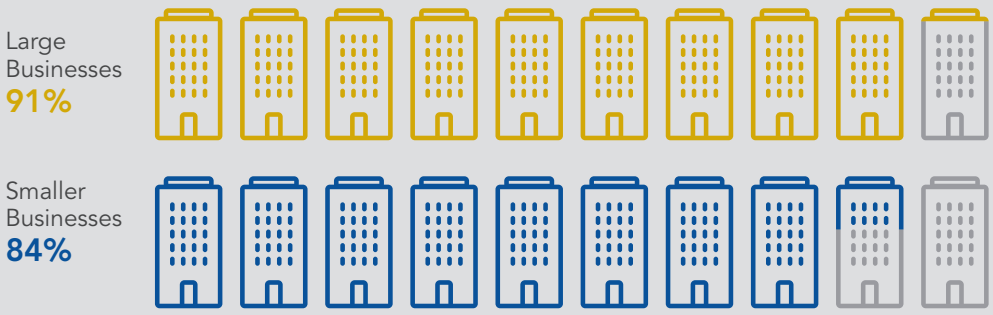



In our 2017 study, 91% of large businesses reported that they purchase cyber security and data privacy insurance, which is a higher percentage than in both the 2015 and 2016 studies.

## Businesses currently purchasing cyber security and data privacy insurance

*2017 Comparison — Large vs. Smaller Businesses*

n = 100 for Large and Smaller



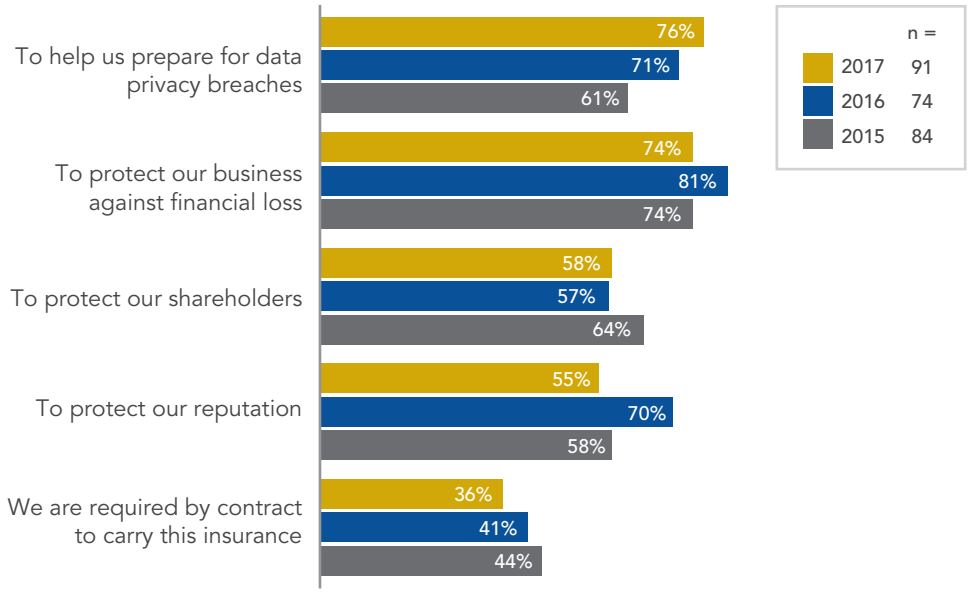
Many companies now likely accept that it's not a question of if they will have a breach, but when. In discussing the results of the June 2016 IBM & Ponemon Institute Study, Dr. Larry Ponemon said,

> *Over the many years of studying the data breach experience of more than 2,000 organizations in every industry, we see that data breaches are now a consistent 'cost of doing business' in the cybercrime era. The evidence shows that this is a permanent cost organizations need to be prepared to deal with and incorporate into their data protection strategies.*[5]

For large companies, preparation for data privacy breaches (at 76%) in our 2017 study outranked to protect against financial loss, which was the top reason cited in our 2015 and 2016 reports.

**Reasons for purchasing cyber security and data privacy risk insurance**

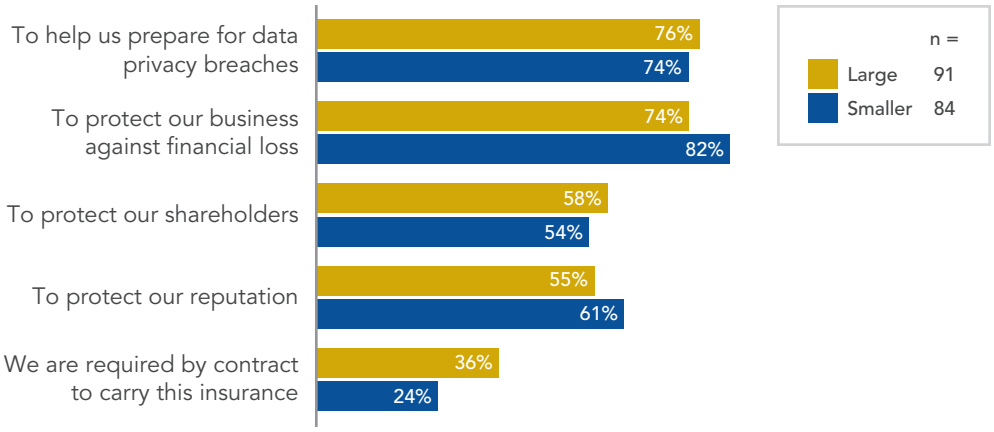
*Large Businesses*



Of the 84% of smaller businesses that reported purchasing cyber security and data privacy risk insurance, 82% said protecting their business against financial loss was their top reason for purchasing it. Preparing for a data privacy breach was the second top reason cited (74%). Financial losses for any size business can be significant, especially because the costs associated with a breach continue to rise.

### Reasons for purchasing cyber security and data privacy risk insurance

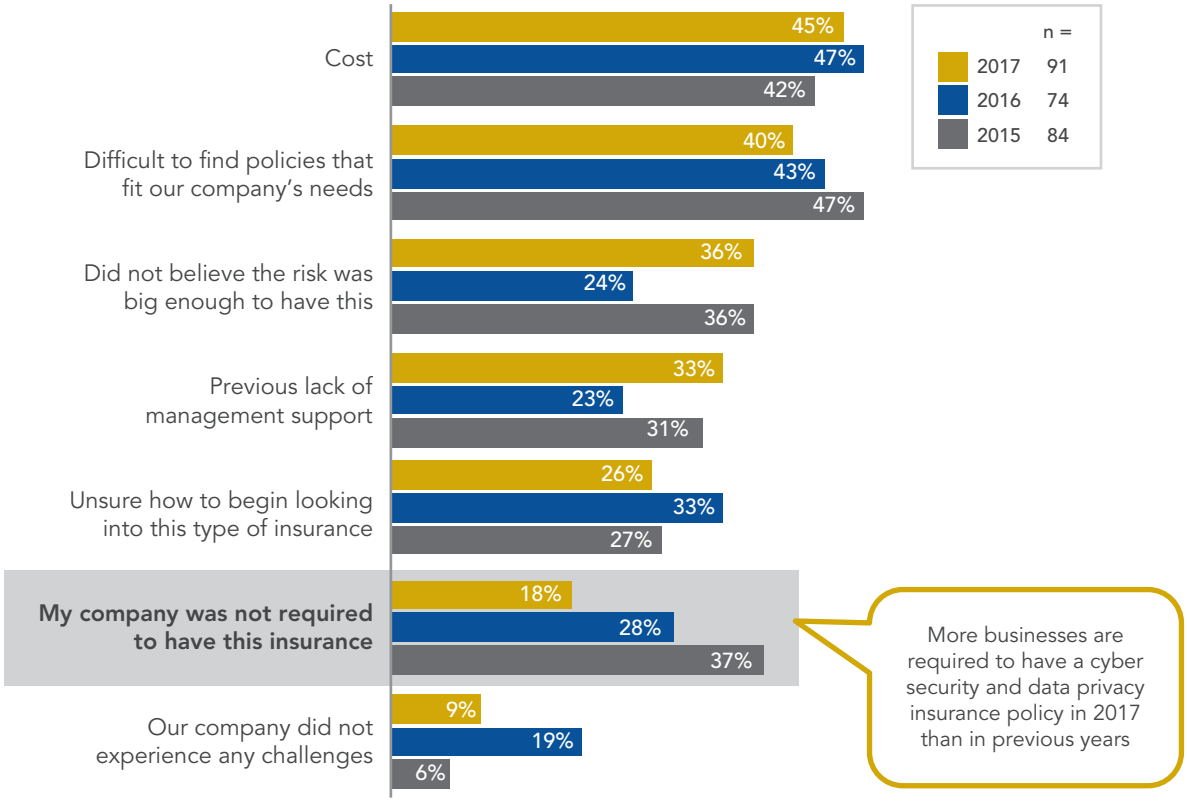
*2017 Comparison — Large vs. Smaller Businesses*




## While cost is a consistent challenge for large businesses when acquiring insurance, it is now easier to find policies.

### Challenges to obtaining cyber security and data risk privacy insurance

*Large Businesses*



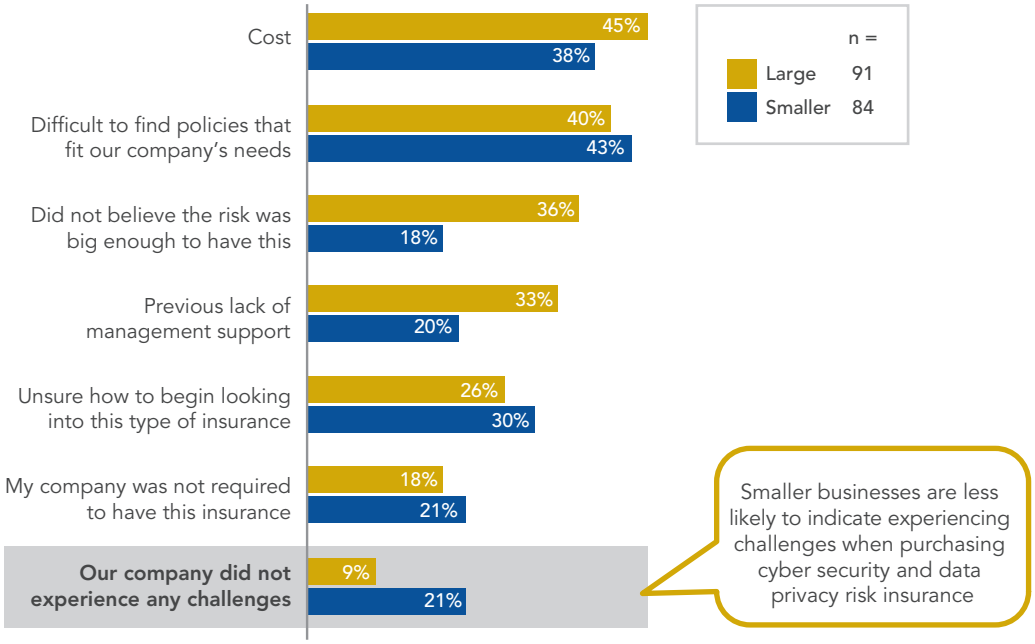
The cost of cyber security and data privacy insurance was cited by 45% of large companies as their #1 challenge, and 38% of smaller companies felt cost was their main challenge. While 40% of large companies cited difficulty in finding policies that fit their needs, this number has steadily decreased since 2015, when our study showed that 47% of large companies felt it was difficult to find insurance and considered this to be their #1 challenge.

Often contracts with customers or lenders require businesses to have cyber security and data privacy insurance. In 2017, more large businesses are also being required to have this insurance than in 2015. In 2017, only 18% of large businesses reported that they are not required to have cyber security and data privacy insurance, compared to 37% not being required to have it in 2015.

While a higher percentage of smaller businesses (21%) are not required to have insurance, they appear to see the need — only 18% said they did not believe the risk was big enough to warrant the purchase of insurance. This is an interesting contrast with the 36% of large businesses that did not believe the risk was big enough to purchase insurance, perhaps due to concerns about cost.

## Challenges to obtaining cyber security and data privacy risk insurance

*2017 Comparison — Large vs. Smaller Businesses*

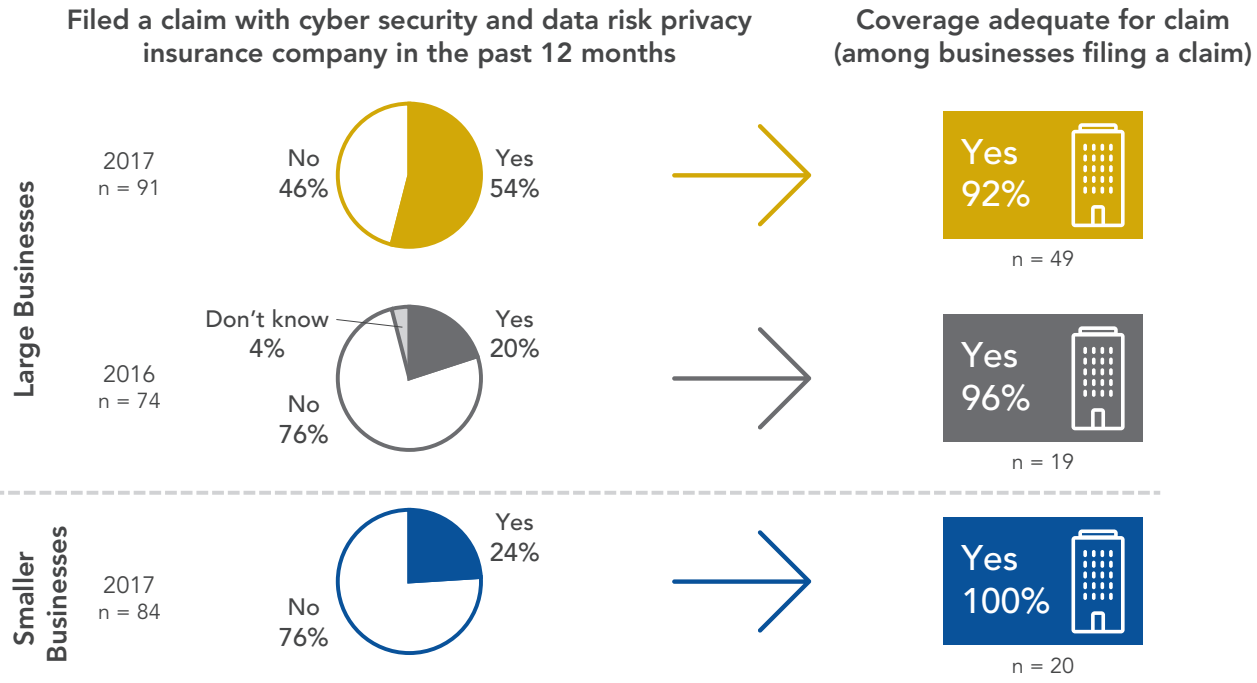



In its 2017 Insurance Market Outlook, USI noted that organizations outside of traditional buyers (manufacturing, for example) are adding cyber security and data privacy to their insurance portfolio as they realize the risk inherent in their collection of employee records, as well as an increased reliance on computer networks, which makes companies more susceptible to ransomware attacks. Many companies may not be familiar with the cost of cyber security and data privacy insurance before inquiring about it. The cyber security and data privacy insurance market is becoming more competitive and prices are beginning to drop.

To help keep the cost of coverage down, a broker can use the results of a third-party cyber risk assessment to negotiate the best insurance premium, coverage enhancements, and deductibles on an organization's behalf. A cyber risk assessment can help an organization identify strengths and weaknesses in its data security plan and make suggestions for improvement. An assessment also helps provide tangible information to senior management to help them better understand specific cyber security strengths and weaknesses. An organization that has an in-depth understanding of the overall risk will be better positioned to determine its optimal level of risk transfer.

Cyber security and data privacy insurance remains a specialized product, and an experienced broker can negotiate tailored coverage with insurance carriers to meet an organization's specific needs, both current and future. In general, insurance brokers are becoming better educated about policy coverage needs so they can recommend the best solution to their clients.

## More than half of large businesses surveyed in 2017 filed a claim with their insurance company in the past year, and found their coverage adequate for the claim.




Our study showed that 54% of large businesses filed a claim with their insurance carrier in the past year, compared with just 20% that filed a claim in 2016. Of these large businesses that filed a claim, 92% felt their coverage was adequate. A much smaller percentage of smaller companies, 24%, filed a claim, and 100% reported that they felt their coverage was adequate.

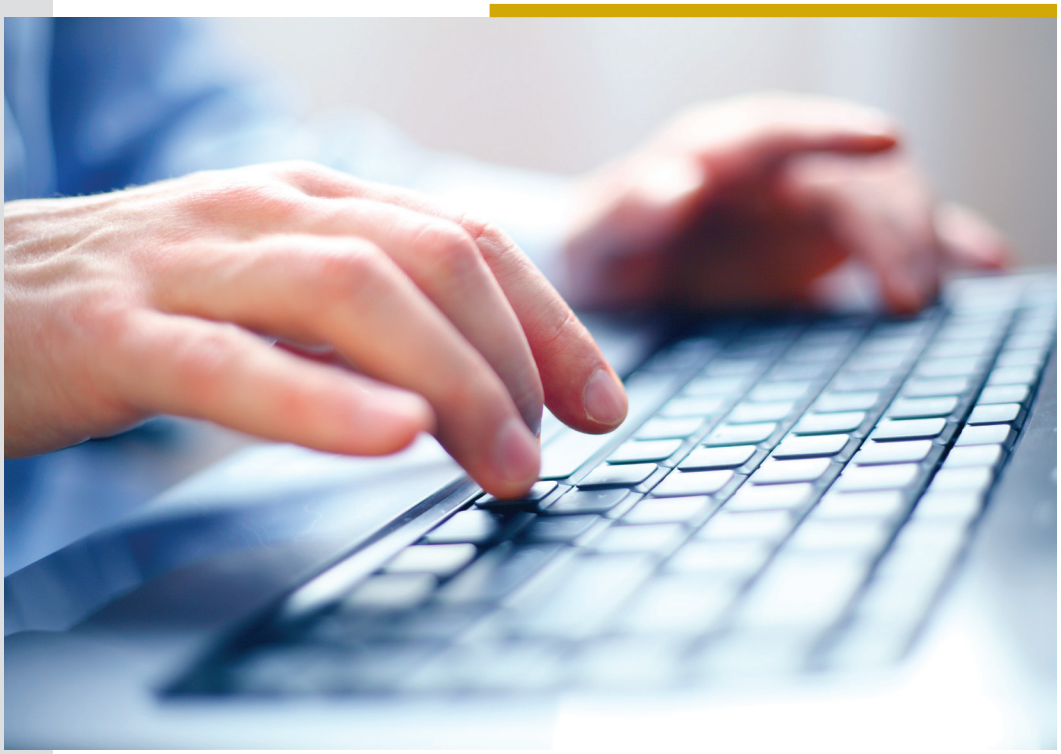
As cyber security and data privacy insurance has evolved, the breadth of coverage has increased, according to USI Insurance brokers. This has likely enabled more large businesses to recover losses under their policies. Carriers have created hotlines and email channels for claims reporting, making it easier to file a claim. Additionally, carriers are becoming involved sooner in the process, which helps the insured manage the event.


Subdivision 3
Subdivision 2
Others
Main company
Product placement in different regions
Detailed information of changing business activity of subdivisions of main company
700
may
june
july
aug
sept

# INCIDENT RESPONSE PLANNING

While purchasing cyber security and data privacy insurance is a solid step, it should be used in tandem with developing and testing a comprehensive incident response plan. Among large businesses, 96% reported having a written, detailed incident response plan, and 90% of those have tested their plan. The need for annual (or more frequent) plan testing before an incident occurs is critical, as it allows companies to make necessary revisions.

In 2017, 56% of large companies reported using their incident response plan in the past 12 months, up from 34% who reported using their plan in 2016. While large companies that used their plan in 2017 reported they found it to be 98% effective, the study showed that, on average, more than half (57%) of the plan was revised after its most recent use. This amount of revision is encouraging, as an incident response plan should be a fluid document that can be adjusted based on new threats that emerge and as lessons are learned.



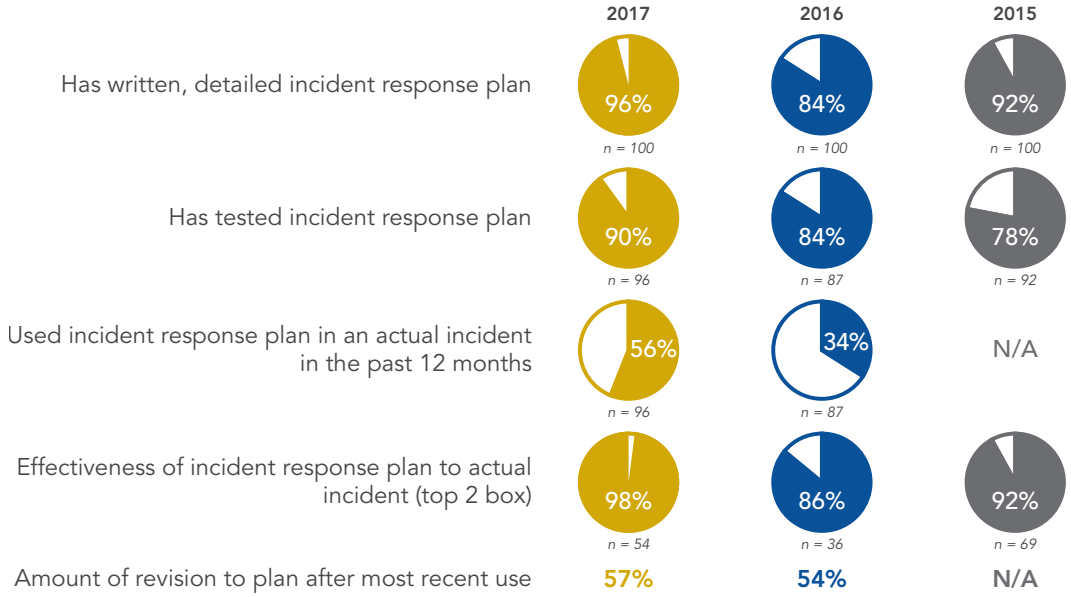
### Incident response plan

A documented process to recover your IT infrastructure in the event of a network intrusion, receipt of malicious code (virus), a ransomware attack, or a denial of service attack.

## Most large and smaller businesses report having an incident response plan and just over half of large companies have had to use it.

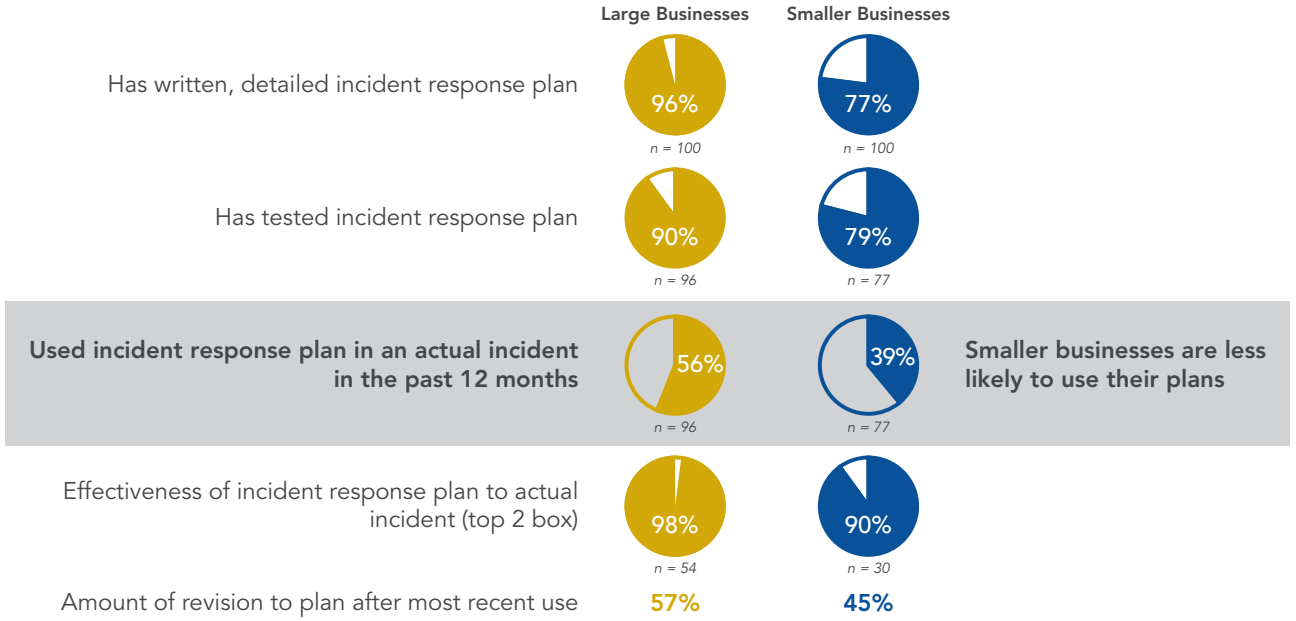
### Incident response plan

*Large Businesses*




### Incident response plan

*2017 Comparison — Large vs. Smaller Businesses*



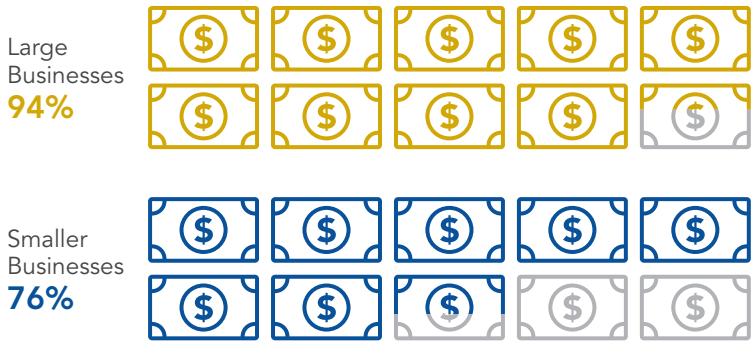
# BUSINESS CONTINUITY PLANNING

## While nearly all large businesses evaluate the potential financial impact of a disruption, only three in four smaller businesses do. And, fewer smaller companies have network business interruption insurance.

### Business has evaluated potential financial impact of a disruption to IT infrastructure from a virus or denial of service attack

*2017 Comparison — Large vs. Smaller Businesses*

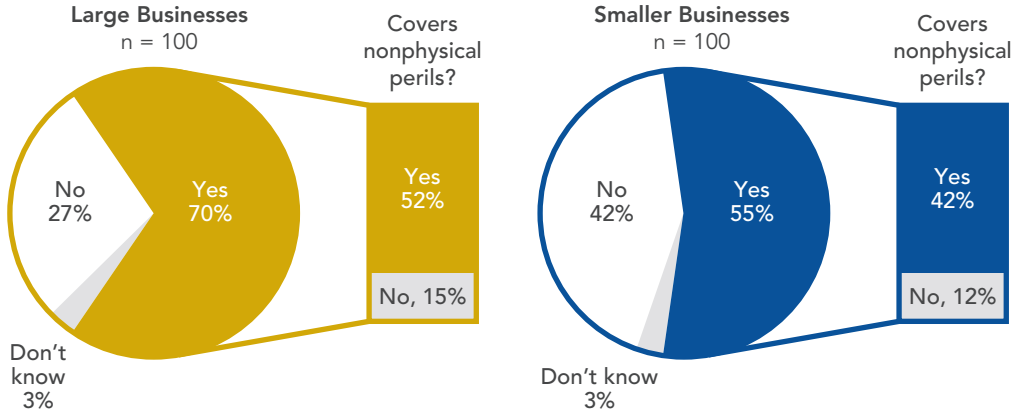
n = 100 for Large and Smaller




For smaller businesses, 76% of companies reported that they have evaluated the financial effects of a disruption from a virus or denial of service (DNS) attack, yet only 55% have network business interruption insurance. Large businesses report that cyber security is increasingly becoming a board-level concern. The study showed 94% of large businesses have evaluated this risk, 70% have network business interruption insurance, and 52% of those policies cover nonphysical perils, such as lost revenue and extra expense arising from a network event that results in a material interruption.

### Company purchases network business interruption insurance

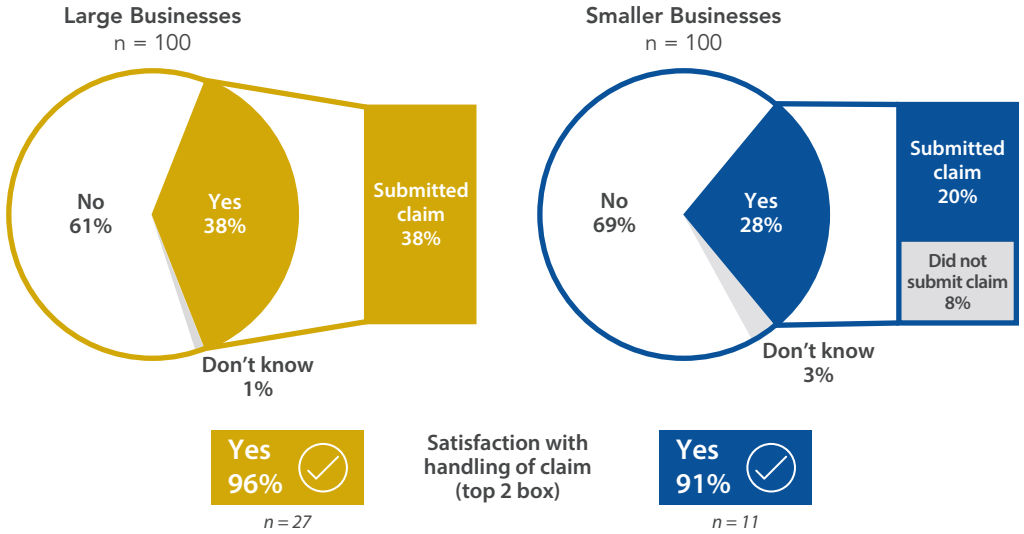
*2017 Comparison — Large vs. Smaller Businesses*



## Experienced an interruption in operations

*2017 Comparison — Large vs. Smaller Businesses*

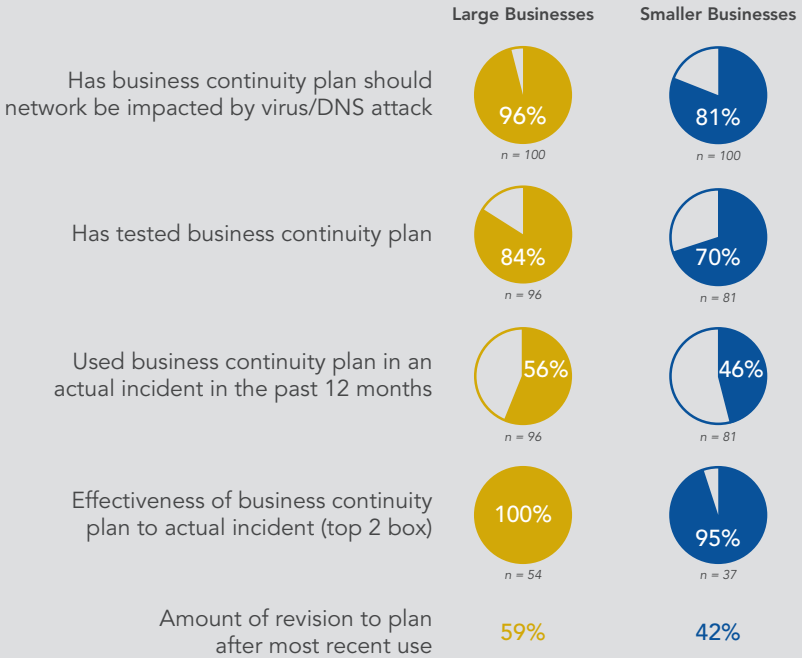
The study showed 38% of large businesses experienced an interruption in operations due to a nonphysical peril, compared to 28% of smaller businesses.




## Similar to incident response planning, a significantly higher number of large companies have business continuity plans and have tested them.

### Business continuity plan

*2017 Comparison — Large vs. Smaller Businesses*



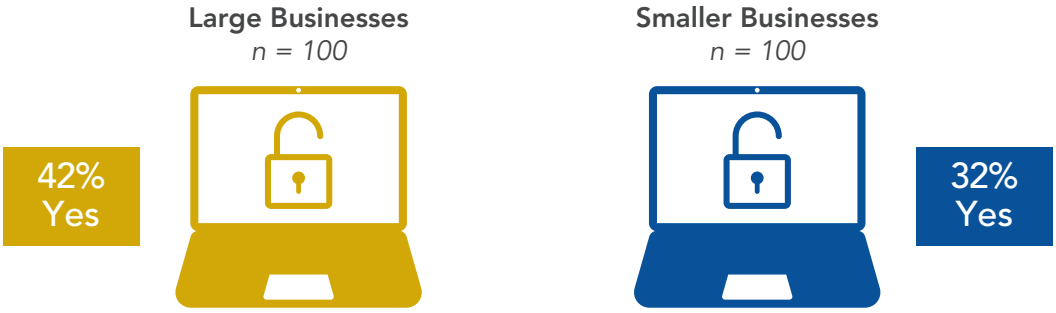

Prior to a network interruption or crisis, it is essential to develop a business continuity plan to identify critical business functions, prioritize resources to support those functions, and develop strategies to maintain operations in the wake of a cyber event.

# TYPES OF INCIDENTS

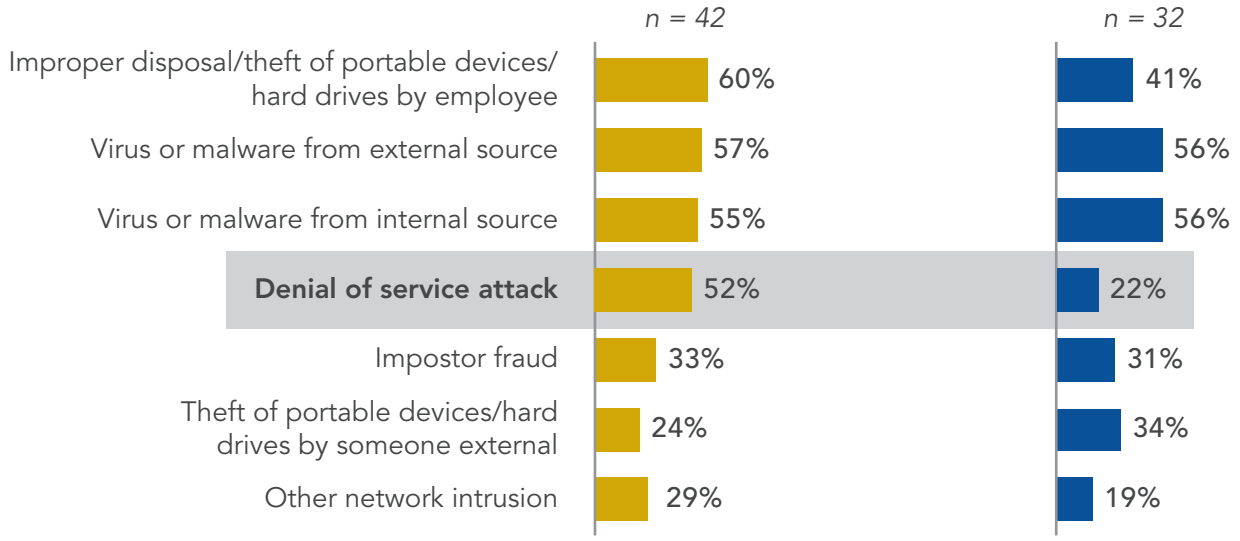
## Large businesses are more likely than smaller businesses to experience a data privacy incident and ransomware.

**Experienced a data privacy incident in the past year (other than paper breach)**

*2017 Comparison — Large vs. Smaller Businesses*




Type of cyber-attacks and data privacy incidents experienced



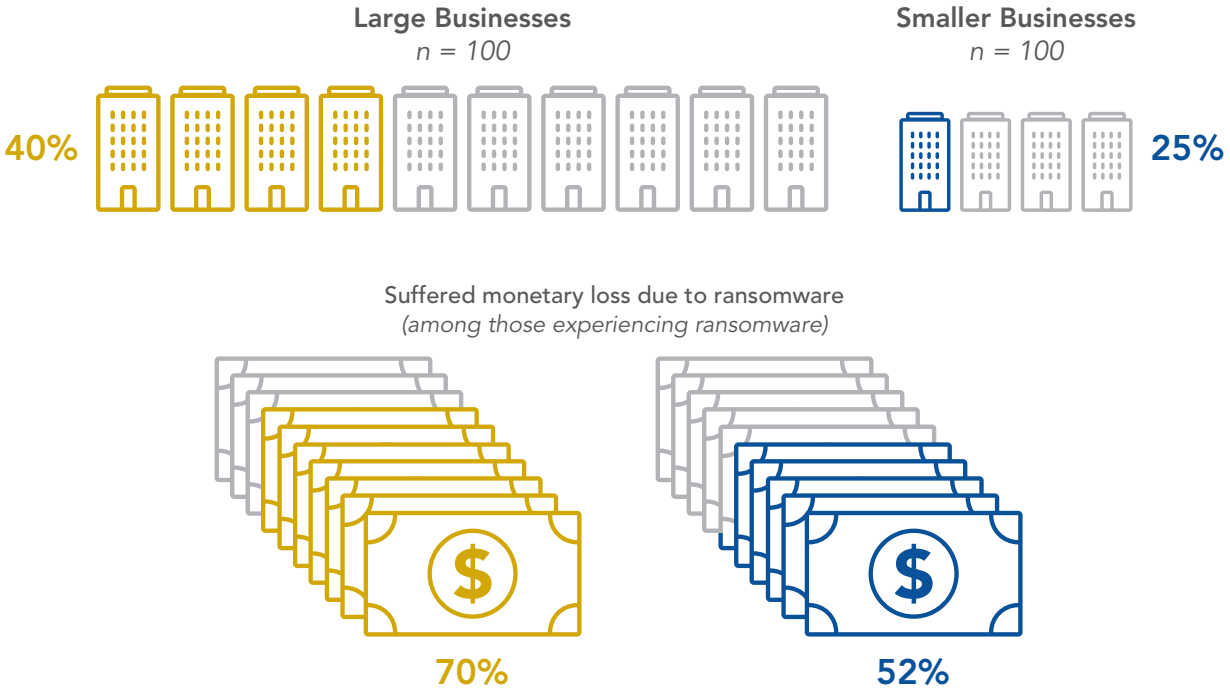

Our study looked at the various types of cyber security and data privacy incidents that large and smaller companies have faced in the past year.

Among large companies, 52% reported experiencing a denial of service attack compared with only 22% of smaller companies. But 34% of smaller companies reported experiencing theft of portable devices or hard drives by someone external to the organization, compared with only 24% at large companies.

Among large businesses, 40% reported being a target of ransomware, while 25% of smaller businesses said they were targeted. A significant percentage of both large and small firms targeted by ransomware attacks suffered a financial loss (70% and 52% respectively).

## Target of ransomware

*2017 Comparison — Large vs. Smaller Businesses*




The majority of large and smaller businesses experiencing a financial loss indicate a loss less than $250,000. However, 14% of large businesses experiencing a loss indicate costs of $1 million and higher.

According to the 2017 Verizon Report, ransomware is now the fifth most common variety of malware, up from the 22nd most common in 2014.[2]

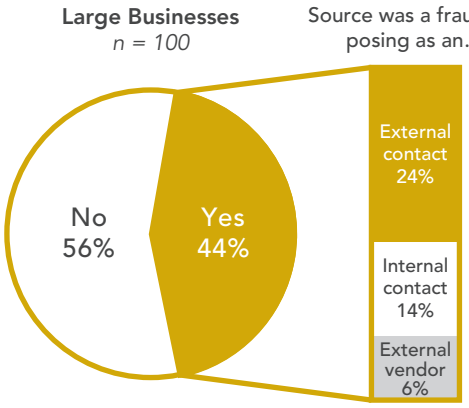
USI expects the frequency of ransomware and cyber extortion threats to increase and become more varied. The FBI has prepared a list of steps you can take to avoid ransomware. These can be found at: fbi.gov/investigate/cyber.

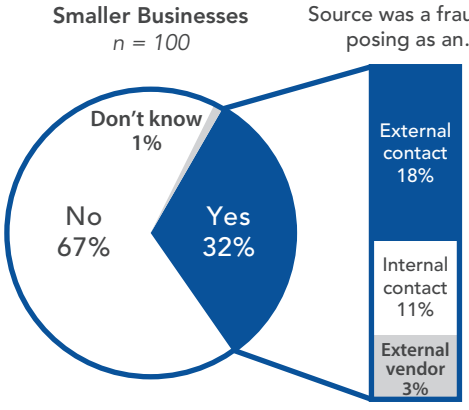
## While most businesses have not been a target of impostor fraud, it is likely to become a growing issue and frequently results in monetary loss.

Impostor fraud is also called fraudulent inducement, social engineering fraud, business email compromise scam (BEC), or email account compromise scam (EAC). Our study showed that 44% of large businesses had been the target of impostor fraud and 64% of those targeted had suffered monetary loss as a result. While smaller businesses were less likely to have been targeted (32%), half of the targeted businesses reported suffering monetary loss. Anecdotally, a significantly higher number of our large insurance customers tell us that they've been a target of an impostor fraud attack than what is reported in this study.

### Business was the target of impostor fraud: Source of fraud attempt

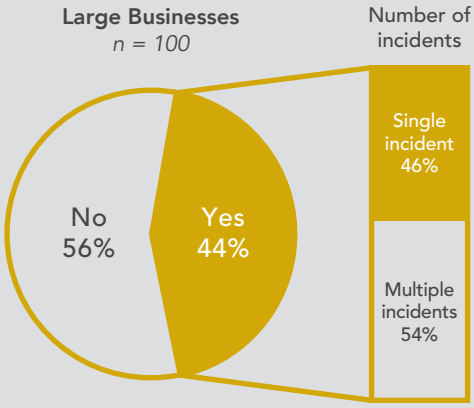
*2017 Comparison — Large vs. Smaller Businesses*

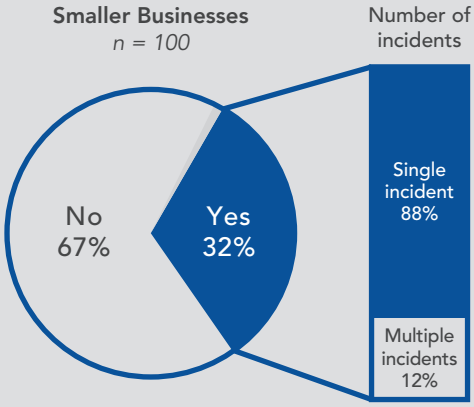


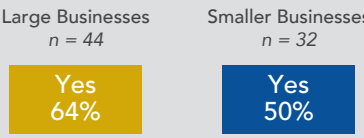

### Business was the target of impostor fraud: Number of incidents

*2017 Comparison — Large vs. Smaller Businesses*




**Suffered monetary loss due to impostor fraud**
*(among those experiencing impostor fraud)*

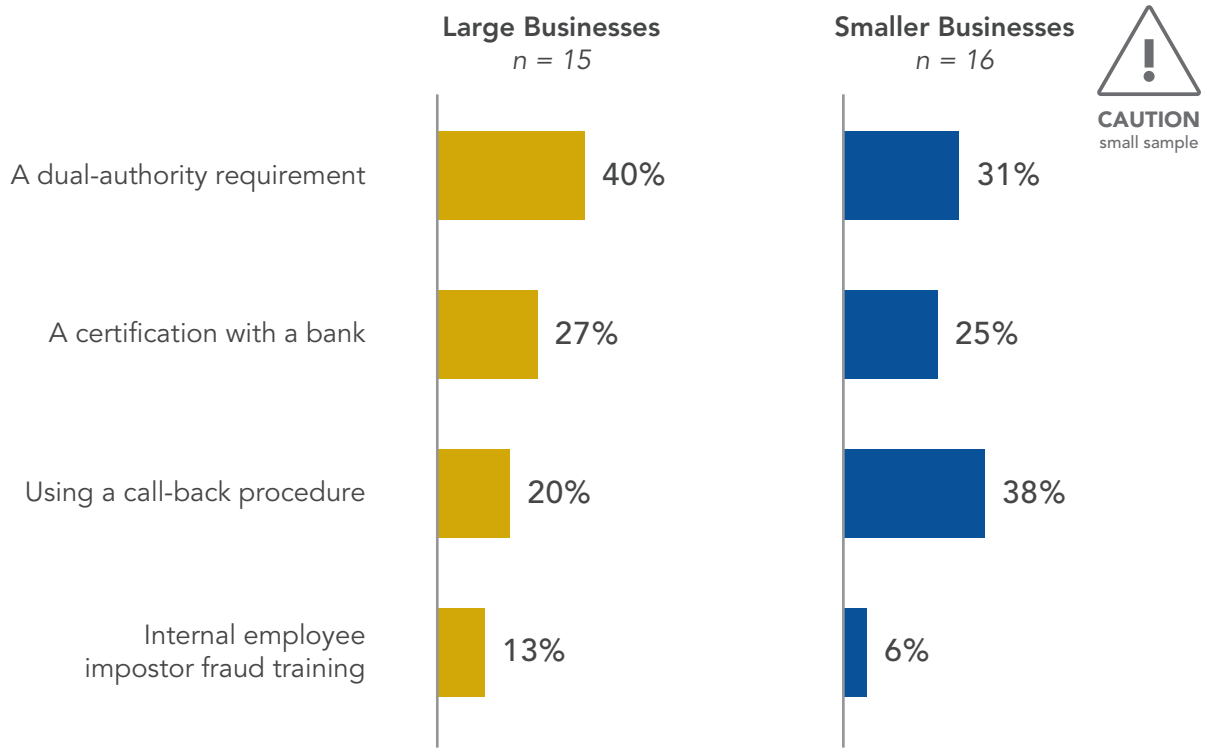



The majority of large businesses experiencing a financial loss indicate losses between $100,000 and $500,000. Expectedly, smaller business losses range from $25,000 to less than $250,000.

Impostor fraud is an increasingly dangerous threat. According to a May 2017 FBI public service announcement, the BEC/EAC scam continues to grow, evolve, and target smaller, medium, and large businesses. Between January 2015 and December 2016, there was a 2,370% increase in identified exposed losses. From October 2013 through December 2016, there were more than 22,000 US victims, with a total US exposed dollar loss of more than $1.5 billion.[6]

## Prevention of monetary loss due to impostor fraud

*2017 Comparison — Large vs. Smaller Businesses*




The good news about impostor fraud is that strong internal controls can be effective in thwarting a scam. According to our study, among businesses that avoided monetary loss from an impostor fraud threat, a requirement for dual authorization was a top reason, with 40% of large companies citing it as the top reason. Among smaller companies, 31% cited it as the second top reason, with a call-back procedure taking the spot as the top reason at 38%.

To avoid becoming a victim, requiring dual authorization for payments above a certain threshold is an excellent best practice. The initiator and the approver must:

- Pay close attention to payment details — not just give them a rubber stamp.
- Authenticate the request before they initiate or before they approve to ensure it's not fraudulent.
- Require a third-level review for any payments to a new beneficiary.

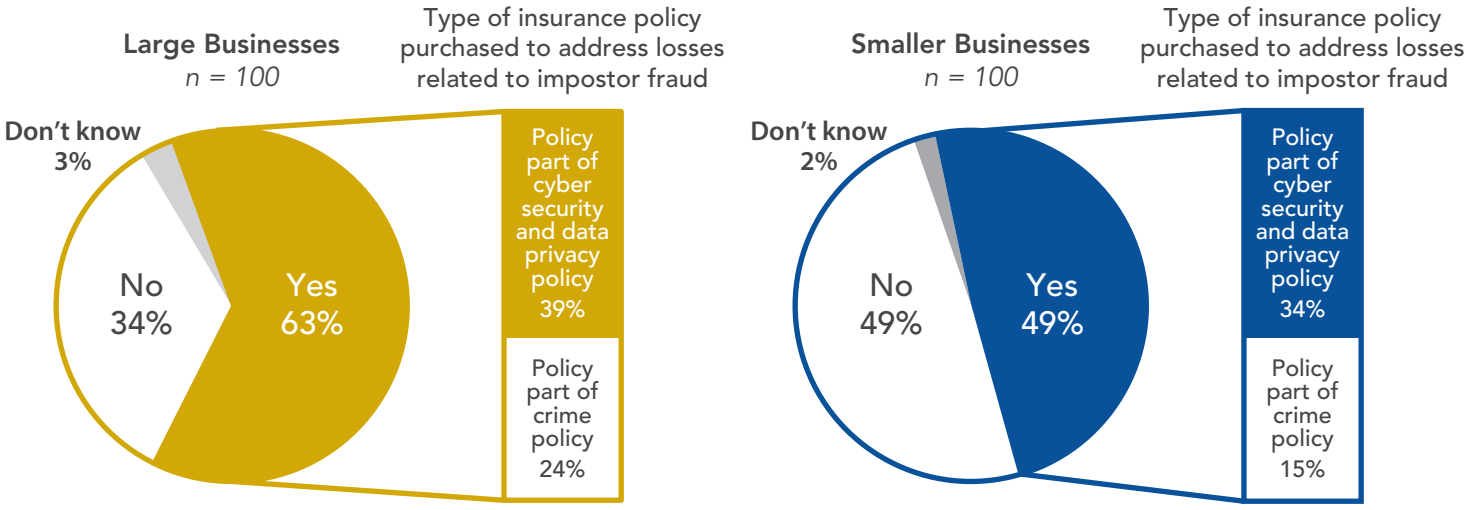
## Other best practices employers can follow to reduce exposure to impostor fraud:

1. Ensure company executives communicate with back-office staff and ensure them that it's okay, and even expected, to question any payment requests.
2. Ensure accounts payable staff is empowered to authenticate payment requests or changes to account information.
3. Educate all internal business partners that communicate with vendors. Alert lines of business that receive and approve invoices, and then send the invoices to accounts payable for processing.
4. Ask IT partners if they can block spoofed emails.
5. Tell vendors you'll no longer accept changes to bank account information by email. Warn them that they're targets, too.
6. Confirm new vendor accounts with the receiving bank before establishing these in your accounts payable system.
7. Always authenticate payment requests that are received by email, made outside your company's normal channels, made to accounts or countries you've never sent money to, or ask to change a vendor's payment remittance information.
    - If a request comes by email, fax, or mail, verify it with a phone call. If it comes by phone, verify it by email.
    - Use contact information on file to verify the requestor. Never use the information that comes with the request — it's fraudulent, too.
    - Prohibit executive payment requests made by email. Encourage staff to contact executives directly to verify requests.
    - If you don't authenticate vendor or executive requests, audit requests several months back. You could be a fraud victim and not know it.
8. Ensure wire payment authority is limited in scope and is consistent across all business units.
9. Monitor accounts daily. The sooner you spot a fraudulent transaction, the sooner you can start your recovery efforts and take steps to help ensure you don't become a victim again.

## A sizeable proportion of businesses have coverage for impostor fraud as part of their insurance portfolio.

### Business purchases insurance to address losses related to impostor fraud

*2017 Comparison — Large vs. Smaller Businesses*




To help mitigate potential financial loss from an impostor fraud attack, some companies have impostor coverage under a cyber security and data privacy liability policy, while others have coverage under a crime policy. There is no standalone coverage available for impostor fraud.

Our study showed that 63% of large businesses and 49% of smaller businesses reported purchasing impostor fraud coverage as part of their insurance portfolio. This is not as high as the percentage of those having business interruption insurance. However, as the threat of this type of fraud continues to grow, companies may want to talk with their broker about adding this coverage.

Coverage for an impostor fraud type of claim is complicated, as most crime policies require either direct theft by an employee or someone without authority initiating a fraudulent payment. In a case of impostor fraud, neither of these circumstances applies. The individuals sending payments are fully authorized to do so within the scope of their employment; they simply send it to an impostor. To obtain coverage for this exposure, the standard crime policy must have an affirmative coverage grant added by endorsement. The insurance market for impostor fraud coverage is evolving rapidly. Organizations should consult a broker regarding the options currently available.

# HOW CAN WE HELP?

No matter your industry or the size of your company, the data you have in your care, custody or control present a risk to your bottom line. Talk to us about customized risk transfer solutions and best practices to help protect your organization.

For more information, visit www.usi.com.

## Sources


1. 2017 IBM X-Force Threat Intelligence Index news release.
   http://www.prnewswire.com/news-releases/ibm-x-force-finds-historic-number-of-records-leaked-and-vulnerabilities-disclosed-in-2016-300430876.html
2. "Cyberespionage and ransomware attacks are on the increase warns the Verizon 2017 Data Breach Investigations Report," Verizon news release.
   https://www.prnewswire.com/news-releases/cyberespionage-and-ransomware-attacks-are-on-the-increase-warns-the-verizon-2017-data-breach-investigations-report-300446807.html
3. Fallout: The Reputational Impact of IT Risk, Forbes Insight Report.
   http://www-935.ibm.com/services/multimedia/RLL12363USEN_2014_Forbes_Insights.pdf
4. Federal Bureau of Investigation: "The Insider Threat: An introduction to detecting and deterring an insider spy."
   https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view
5. "IBM & Ponemon Institute Study: Data Breach Costs Rising, Now $4 million per Incident." IBM news release.
   http://www.prnewswire.com/news-releases/ibm--ponemon-institute-study-data-breach-costs-rising-now-4-million-per-incident-300284792.html
6. "Business E-mail Compromise, E-mail Account Compromise: The $5 Billion Scam." FBI Public Service Announcement, May 2017.
   https://www.ic3.gov/media/2017/170504.aspx


About this research: USI 2017 Cyber Security and Data Privacy Study was conducted in 2017, among cyber security and data privacy risk decision-makers. Half of the decision-makers work at companies with $100 million or more in annual revenue, while the other half work at companies with $5 million to just under $100 million in annual revenue. In the 2015 and 2016 studies, we exclusively surveyed decision-makers of large businesses. We conducted the study to help us understand trends as well as perceptions of cyber security and data privacy vulnerabilities, the challenges companies face when reviewing their exposures, the prevalence of impostor fraud and ransomware, and plans for dealing with business interruption due to virus or denial of service attack.