WELLS FARGO INSURANCE

White paper

2016 Network Security and Data Privacy Study: Are you prepared for a breach?

By Dena Cusick — Technology, Privacy, and Network Security Practice

August 2016

Together we'll go far

This study is a follow-up to the 2015 Wells Fargo Insurance Network Security and Data Privacy Study.

In this study, we surveyed 100 decision makers at companies with $100 million or more in annual revenue to understand:

- Trends between our 2015 and 2016 findings
- Perceptions of network security and data privacy vulnerabilities
- The challenges companies face when reviewing their exposures
- The prevalence of impostor fraud and paper breaches
- Plans for dealing with business interruption due to virus or denial of service attack

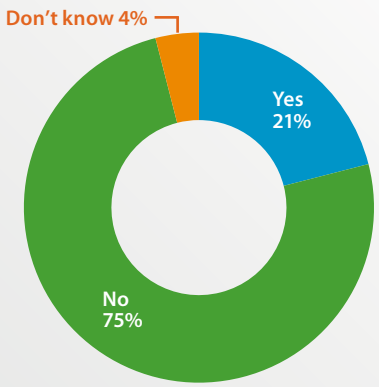
Key findings

Impostor fraud and paper breaches

While data breaches continue to make the headlines, there's another imminent threat for many companies — impostor fraud. One in five large companies surveyed has been a target of impostor fraud, and the incidence is even higher for companies with 2,000+ employees or $500 million in revenue or more.

Impostor fraud is also called fraudulent inducement, social engineering fraud, or business email compromise scams. But whatever you call it, these statistics show that it's a threat you should not underestimate.

Company has been a target of impostor fraud



2016 ONLY | Base: Total 2016 n=100

Impostor fraud specifics

Of the 21 companies that suffered from impostor fraud, respondents indicated:

Imposter was more likely to pose as an internal contact

Most of these respondents suffered a financial loss, and often it was significant ($500K or more)

The loss could often be attributed to a single instance

Data from an April 2016 FBI news release supports the case that impostor fraud is a rapidly growing threat. The release states that complaints to global law enforcement have come from victims in every U.S. state, and in at least 79 countries. From October 2013 through February 2016, law enforcement received reports from 17,642 victims, amounting to more than $2.3 billion in losses. Since January 2015, the FBI has seen a 270% increase in identified victims and exposed loss.[1]

Impostor fraud is particularly common among the larger companies surveyed and can cause significant financial losses.

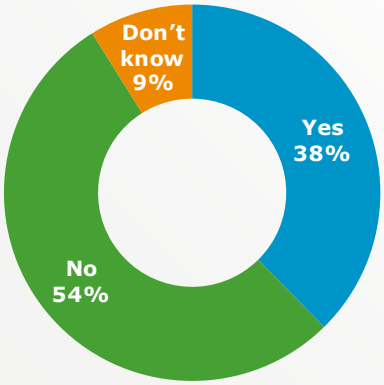
In our survey, many of the companies that were victims of impostor fraud suffered a financial loss, which was often significant (more than $500K). The numbers can go much higher. In April 2016, details of a lawsuit filed by the U.S. government revealed that an unidentified American company was defrauded in 2015 out of nearly $100 million by individuals who created a fake email address, posing as one of its legitimate vendors.

To help mitigate loss from this financial risk, some companies have impostor coverage under a network security and privacy liability policy and others have coverage under a crime policy. To date, there is no stand-alone coverage available for impostor fraud. Coverage for this 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. In order 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.

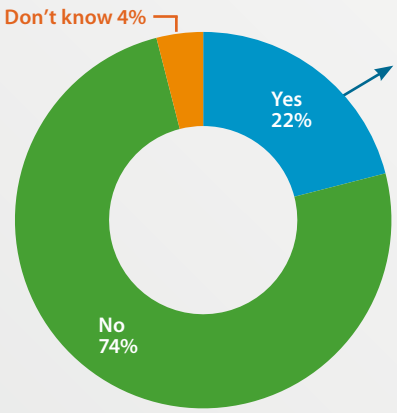
Paper breaches don't make the headlines, but 22% of our survey respondents report experiencing information loss from a paper breach — most often due to improper

Company purchases impostor fraud insurance



2016 ONLY | Base: Total 2016 n=100

Companies suffered information loss from paper breach

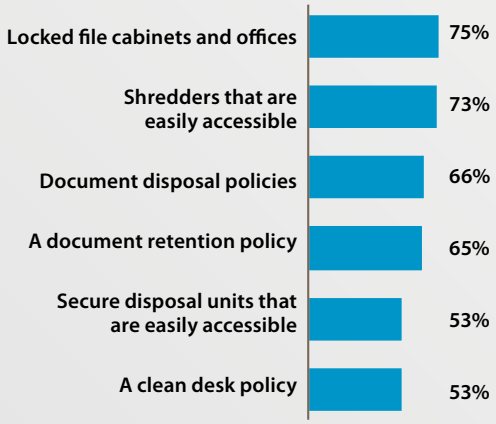


For the 22 companies who suffered a paper breach, causes included:

- Improper disposal
- Loss by employee
- Donation of office equipment
- Mismanagement by independent contractor

2016 ONLY | Base: Total 2016 n=100

Paper breach prevention practices in place



2016 ONLY | Base: Total 2016 n=100

disposal or loss by an employee. Most companies report having paper breach prevention practices in place, so they may want to look at enhancing employee training to help ensure a higher level of compliance.

Despite having paper breach prevention practices in place, paper breaches are still a problem.

Purchasing network security and data privacy insurance

In 2015, our study showed that 22% of companies buying network security and data privacy insurance took more than 12 months to make the purchase decision. However, our 2016 survey results show that just 8% of companies are currently taking that long; 59% are taking six months or less.

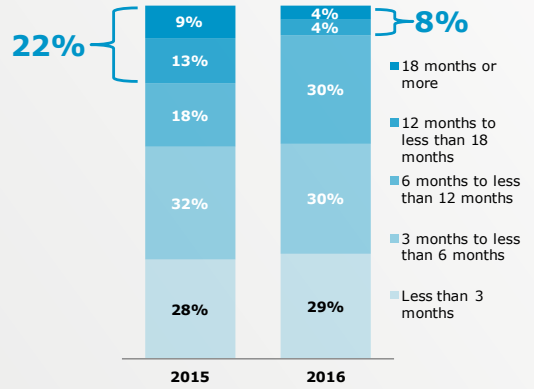
A majority of companies continue to have network security and data privacy insurance, but are now making their purchase decisions faster, and experiencing fewer purchasing challenges than in 2015.

The results are not surprising, given that network security and data privacy coverage has now been around for more than 10 years. Over time, senior leaders have become more familiar with this type of coverage. While our 2016 results show that, as in 2015, decisions about purchasing network security and data privacy insurance are most often made by the CEO (or equivalent), it appears that risk managers may be increasingly involved in the decision making. In 2016, risk managers were the second most common decision makers at 29%, compared with 35% of CEOs.

The top two challenges of 2016, similar to 2015, are cost at 47%, and finding a policy that fits the company's needs at 43%.

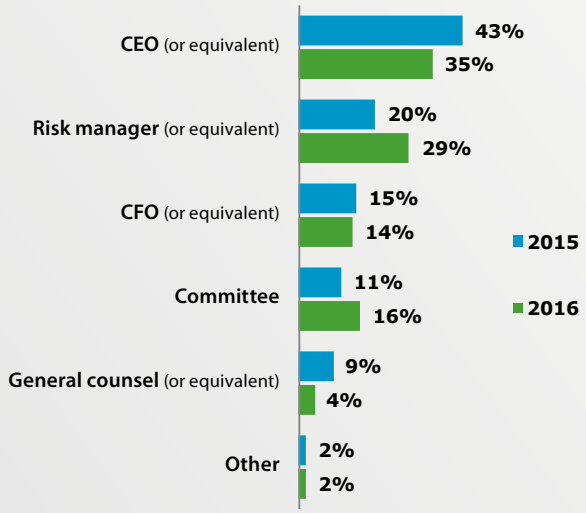
However, according to the 2016 study, 19% of the respondents did not experience any challenges while purchasing their coverage, which represents a significant

Decision time needed for network security and data privacy insurance purchase



Base: Purchases cyber and data privacy insurance
2015 n=84 | 2016 n=74

Decision maker for insurance purchase



Base: Purchases cyber and data privacy insurance
2015 n=84 | 2016 n=74

improvement over our 2015 survey results, when only 6% said they did not experience any challenges.

The decrease in purchase challenges may be related to a decrease in internal resistance; likewise, in 2016, fewer companies (24%) believed the risk was not big enough to warrant the purchase of network security and data privacy insurance.

Decision makers are anxious about the potential for data leaks, hackers, outside threats, and security breaches. They need ways to alleviate their concerns, and network security and data privacy insurance is one key way to do that. Of the companies in the study that had purchased insurance,

20% reported filing a network security and data privacy insurance claim in the last 12 months, and most were satisfied with their coverage.

Purchasing insurance is an important step, but it should be used in tandem with developing and testing a comprehensive incident response plan and performing a thorough cyber risk assessment.

Preventing financial loss remains the top reason for purchasing insurance, but protecting the company's reputation is an increasing concern.

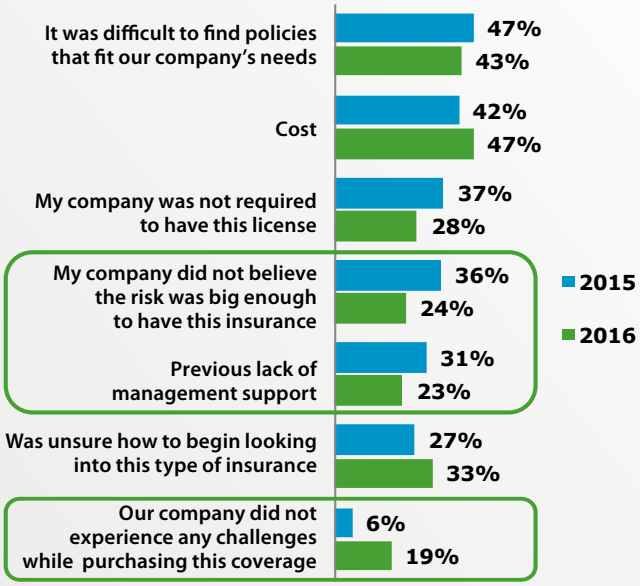
Decision makers realize that network security attacks and data breaches have the potential to cause financial loss and can also result in significant damage to a company's brand. As in 2015, our 2016 survey showed that protecting the business against financial loss was the primary reason for purchasing coverage (81%). However, companies are now increasingly looking to protect their reputations, with 70% citing this as a reason in 2016, compared with just 58% in 2015.

This finding is supported by the Ponemon Institute's 2014 Mega Breaches study, which found that loss of reputation, brand value, and marketplace image were the main consequences of the data breaches experienced by the companies involved.[2]

Damage to the reputation of the breached entity can be catastrophic or minimal, depending 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.

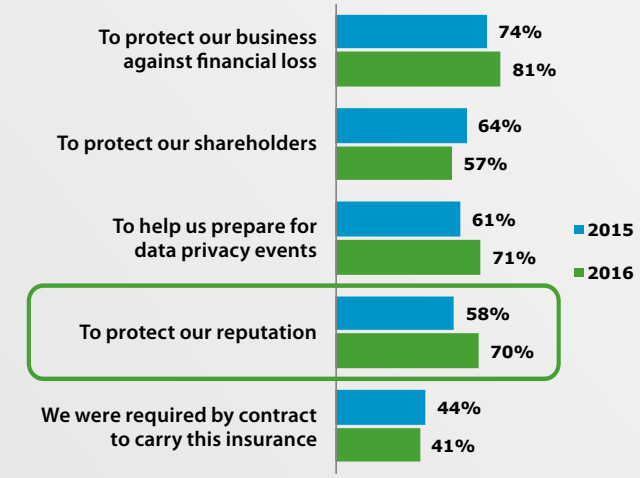
At the same time, the legal arena for data privacy breaches is changing, and an increased number of high-profile lawsuits have the potential to be costly to organizations, in terms of both money and brand reputation. However, a current trend is that courts are refusing to grant certification to class-action lawsuits for data privacy breaches.

Challenges to obtaining network security and data privacy insurance



Base: Purchases cyber and data privacy insurance
2015 n=84 | 2016 n=74

Reasons for purchasing network security and data privacy insurance



Base: Purchases cyber and data privacy insurance
2015 n=84 | 2016 n=74

Incident response planning

Among survey respondents, the most frequently mentioned network security and data privacy concern in 2016 is a leak or loss of private data, with 47% citing this as a threat. One in four mentions hackers, outside threats, or security breaches as primary concerns.

Loss of private data continues to be a top concern in 2016, but employee misuse of data is also a growing threat.

Interestingly, however, 7% of respondents say they are concerned about employee misuse of technology, and the increase in concern appears to be validated by results of other surveys. According to the Ponemon Institute's 2014 Mega Breaches study, a trusted insider was the root cause of 30% of all breaches, second only to malware.[2]

In SailPoint's 2016 Market Pulse Survey, the results showed that a surprising disconnect exists between employees' growing concern over the security of their personal information and their attitudes toward data security practices in the workplace. The survey found that 85% of people would react negatively if their personal information was breached by a company, yet one in five individuals surveyed would sell their company work passwords to hackers. Of the 20% who would sell the password, 44% would do it for less than $1,000, and some were willing to sell company credentials for less than $100.[4]

Our 2016 survey results show that there is still room for companies to improve in the area of employee awareness training. Two in 10 do not have an employee awareness training program, and 15% do not require training for all employees.

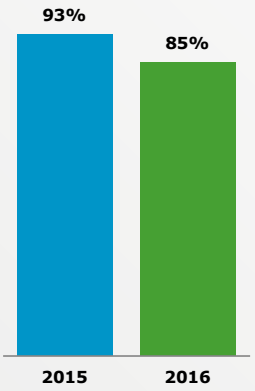
Top network security and data privacy concerns

Category	2015	2016
Leaking private data/loss of data	45%	47%
Hackers/outside threats	25%	26%
Security breach	20%	26%
Viruses/disruption of operations	10%	7%
Software vulnerabilities	7%	7%
Maintaining reputation / keeping compliant with regulations	4%	9%
Employee misuse of technology	0%	7%
Other	13%	7%

Has employee awareness training program

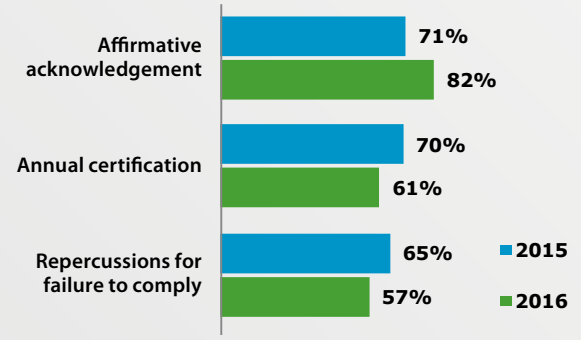
Base: 2015 n=100 | 2016 n=100

Training is required for all employees



Base: 2015 n=79 | 2016 n=83

Elements of employee awareness training



Respondents elaborated on their primary network security and data privacy concerns for their companies, including employee misuse:

"I am always concerned by the attitudes of people we hire, and whether they are going places on our system that we don't want them to go."

"Training; everyday changes in hacking; hackers; the cloud. Is it safe? Is anything safe on the internet?"

"We have concerns on security of devices being lost, or employees taking a work device out of the building and using it for personal uses."

FBI best practice recommendations to prevent accidental or malicious employee misuse of data:

- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is adequately, if not robustly, protected.
- Use appropriate screening processes to select new employees.
- Provide nonthreatening, convenient ways for employees to report suspicions.
- Routinely monitor computer networks for suspicious activity.
- Ensure security (to include computer network security) personnel have the tools they need.[5]

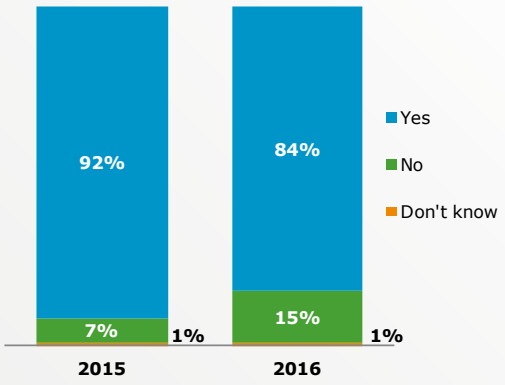
Our survey showed that 84% of companies have an incident response plan and, of those, 84% have tested the plan. Companies with higher revenues ($500 million or more) are more likely to have tested and used their response plans than companies with lower revenues (between $100 to $500 million).

The majority of companies have an incident response plan in place and have also tested it, but these companies still revise at least half of their plans after use.

Of all the companies that actually used their incident response plan, 86% believe they were effective, but they revised an average of 54% of their plans after their most recent use. Given that one third of companies actually use their plan each year, and there is often the need for revisions, the need for annual (or more frequent) testing of a plan before an incident occurs is critical.

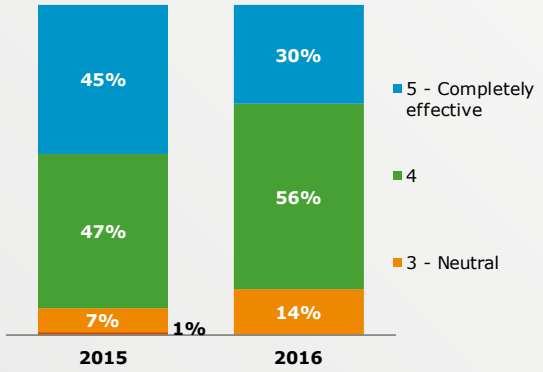
Companies may also wish to consider working with a third party to develop, review, or revise their incident response plans. Our survey showed a significant drop in the percentage of companies consulting a third party to develop their plans, from 85% in 2015 to 65% in 2016. Working with a third party can be advantageous because it provides an outside, objective perspective.

Has an incident response plan



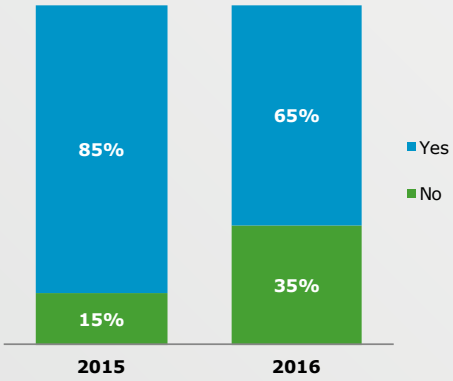
Base: Total 2015 n=100 | 2016 n=100

Effectiveness of incident response plan



Base: Has incident response plan 2015 n=69 | 2016 n=36*
*Small base size

Consulted third-parties to develop incident response plan



Base: Has incident response plan 2015 n=92 | 2016 n=87

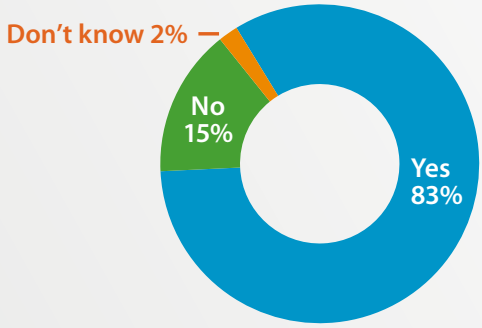
Business continuity planning

Business continuity planning is the process of identifying critical business functions, prioritizing resources to support those functions, and developing strategies to maintain operations before a business interruption or crisis event. Many people associate business continuity planning with large scale, catastrophic incidents; however, business continuity plans are often used in response to smaller, company-specific events, such as a disruption to technology.

A majority of companies have a business continuity plan in place for virus or denial of service attacks and have tested it, but still revise at least half of the plan after using it.

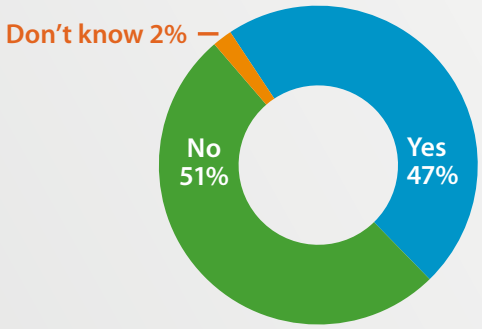
While having a documented plan is important, nothing can match the benefit of practical experience. Our survey shows most companies have good practices in the area of business continuity planning. Most companies (86%) have a business continuity plan for a virus or denial of service attack, and 83% have tested those plans. The companies (47% of respondents) that have used the plans to respond to an actual incident revised an average of 53% of their plans after using them.

Business continuity plan tested



2016 ONLY | Base: Has business continuity plan | 2016 n=86

Business continuity plan used to respond to incident



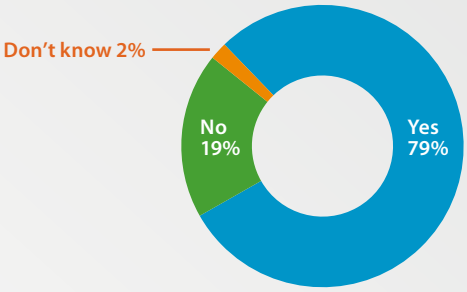
2016 ONLY | Base: Has business continuity plan | 2016 n=86

To further our understanding, in our 2016 study we asked new questions about whether companies have evaluated the financial impact of a disruption from a virus or denial of service attack, and whether they have network business interruption insurance to replace lost business income as a result of an event. When servers experience downtime, a loss of productivity and business interruption may result in significant financial costs.

Nearly eight in 10 companies have evaluated their financial impact of disruption from a virus or denial of service attack, yet only 47% purchase network interruption insurance, with 43% of these policies being a part of the company's network security and privacy liability policies.

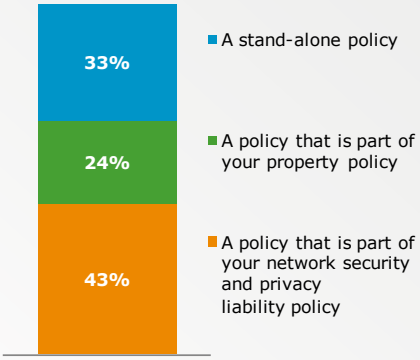
As indicated by this study, year-over-year awareness of network security and data privacy risk is increasing, coverage is more accessible, and data protection is becoming part of everyday conversation.

Company evaluated financial impact of disruption from a virus or denial of service attack



2016 ONLY | Base: Total 2016 n=100

Type of network business interruption insurance purchased



2016 ONLY | Base: Purchases network business interruption insurance
Total 2016 n=51

How can we help?

No matter your industry, there are key steps that you can take to protect your organization, including:

- Conduct a cyber risk assessment to determine how vulnerable you are to attacks.
- Develop and test an incident response plan.
- Develop a privacy policy and ensure that it's followed.
- Require all employees to take training on protecting data.

Wells Fargo Insurance Technology, Privacy and Network Security Practice group's knowledgeable and experienced brokers focus on network security and privacy liability every day. They can help you understand your specific exposures and recommend the customized solutions that meet the needs of your business. Wells Fargo Insurance clients also enjoy access to other training and guidance resources available from insurance carriers, as well as the *eRiskHub*®, a private, web-based portal that provides information and technical resources to assist in preparing for a network security or data privacy incident, and mitigating both the monetary and reputational impact associated with a breach.

For more information, please contact your Wells Fargo Insurance sales executive or visit wfis.wellsfargo.com.

Sources:

1. FBI new release: "FBI Warns of Dramatic Increase in Business Email Scams." https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams
2. Ponemon Institute: "2014: A Year of Mega Breaches." http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL_3.pdf
3. Wells Fargo Insurance Client advisory: "Privacy liability litigation update." https://wfis.wellsfargo.com/insights/clientadvisories/Pages/Privacy-Liability-Litigation-Updates.aspx
4. SailPoint 2016 Market Pulse Survey. https://www.sailpoint.com/news/market-pulse-survey-2016/
5. 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

About this research: The Wells Fargo 2016 Network Security and Data privacy Study was conducted from June 3-9, 2016 among influential cyber and data privacy risk decision makers, who work at companies with $100 million or more in annual revenue. In the study, 100 decision makers responded to help us understand trends between our 2015 and 2016 findings, perceptions of network security and data privacy vulnerabilities, challenges companies face when reviewing their exposures, the prevalence of impostor fraud and paper breaches, and plans for dealing with business interruption due to virus or denial of service attack.