
Iris
Powered by Generali
The Impact of Cybersecurity Incidents on Financial Institutions
ITRC
IDENTITY THEFT
RESOURCE CENTER

Powered by Generali

CEO, Global Identity & Cyber Protection Services
Iris® Powered by Generali (Iris)
Paige L. Schaffer

President & CEO
Identity Theft Resource Center (ITRC)
Eva Velasquez

Contributors
Nikki Fiorentino, ITRC
Kelly Dwyer, ITRC
Alex Hamilton, ITRC
Karen Barney, ITRC
Megan Dwoskin, Iris
Eugenia Blackstone, Iris
Laurel Laluk, Iris

Contact
Eugenia Blackstone
Chief Marketing Officer
Iris Powered by Generali
1250 24th Street, Suite 600
Washington, DC 20037
240-330-1091
eblackstone@irisidentityprotection.com

Introduction

Data breaches are an ever-increasing threat to every industry, with the number of U.S. data breach incidents tracked in 2017 hitting a new record high of 1,579 breaches. Last year posted a 44.7 percent increase over 2016's record-breaking numbers[1]. Of the data breaches reported last year, 8.5 percent involved the financial sector, including entities such as banks, credit unions, credit card companies, mortgage and loan brokers, financial services, investment firms and trust companies, payday lenders and pension funds[2].

For years, the financial services sector globally has been a primary target for attacks by cybercriminals largely because of the tremendous value of the information available. In fact, financial services firms are reportedly hit by security incidents a staggering 300 times more frequently than businesses in other industries[3]. This startling statistic underscores the importance of financial services professionals being aware of the breadth and causes of successful cyberattacks and also their need to keep their knowledge of risk mitigation strategies current.

We aim to help financial institutions address this need in this white paper, by introducing the types of attacks behind data breaches in the financial industry and how they manifest. We also look at the impact that these events can have on a company, such as financial loss, damage to their reputation and reduced levels of trust in their brand. We will analyze current procedures companies are using to mitigate the risk and introduce best practices that companies in the financial industry, no matter their size, can utilize to protect themselves from data breaches.

U.S. data breach incidents tracked in 2017 hit a new record high of 1,579 breaches.

The Scope of the Problem

Given the nature of data held by financial institutions, including banks, credit unions, credit card companies and brokerage firms, it's no surprise they are the most at risk of cyberattacks[4]. Furthermore, not only are they at an increased risk, but they are also finding that certain attacks impacting their sector, like Distributed Denial of Service (DDoS) attacks, have grown in size and frequency[5]. DDoS attacks are defined as "those in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems[6]." A recent study discovered that 56 percent of financial institutions saw an uptick in the number of DDoS attacks waged against them in the previous year, and 60 percent said that attacks are larger than they were a year ago. DDoS attacks are increasingly being used to wage cyber-extortion attacks, which aim to blackmail financial institutions into paying out high ransoms to avoid having their sites taken down and intellectual property published in the underground[7].

Financial institutions saw a 56 percent increase in DDoS attacks in 2016 alone.

In addition to DDoS attacks, social engineering is being increasingly used in cyberattacks leading to data breaches. Social engineering relies on the trusting behavior of the initial victim, in many cases employees, and makes attacks better designed to trick the victim into allowing access to data. Social engineering is used in spearphishing, in which an employee responds to a request that appears to originate from someone higher up in the company. In 2016, Australian banks were among those targeted by a spearphishing campaign named "Carbanak."

Via the compromised Australian banks, cybercriminals targeted 100 banks in 30 countries and stole about 1.3 billion dollars over an 18-month period. This campaign used spearfishing techniques to encourage high-level employees to download the malware which then moved into the bank systems to issue transfers. In some instances, the malware ordered some ATMs to start dispensing cash[8].

Security experts are aware of the risks of social engineering. In a survey of more than 200 U.S.-based security leaders, 60 percent of respondents stated they were certain they were victimized or have reason to believe they might have been victims of social engineering attacks[9]. Additionally, of those attacks, 65 percent of the malicious activity pertained in some way to employees' login credentials, and 17 percent involved accounts belonging to customers[10]. Overall, 94 percent of those surveyed recognize the power of social engineering attempts, like spearphishing, to cause serious damage to a company[11]. Given the aforementioned statistics, it's important for financial institutions to have a heightened awareness of the dangers they face and learn how to protect their services, customers, employees and brands from harm[12].

Financial Impact of Cybersecurity Incidents

Data breaches can have lasting harmful effects for any business, regardless of its industry. A 2017 report by the Ponemon Institute and IBM revealed the average total cost of a data breach in the U.S. reached a record-breaking $7.35 million, a 5 percent increase from the previous year[13]. However, when it comes to the financial sector, those costs can be exponentially larger. While the average cost to U.S. businesses per record lost or stolen in a breach was $225 across all industries, the cost for businesses in the financial industry was $336[14].

One contributing factor to the higher cost may be the specific types of attacks that hackers can use to target financial institutions. For

example, a malware attack cost a financial business around $825,000 on average to resolve[15]. However, when a financial company faces a DDoS attack, which specifically targets their online banking services, the business costs skyrocket to an average of around $1.8 million[16].

Why is there such a discrepancy? DDoS attacks that target financial institutions are specifically designed to cripple their websites by overwhelming it with traffic and taking it offline to halt transactions. In many cases, this method serves as a smokescreen to commit other attacks[17]. It's worth noting that when a DDoS attack takes place, customer-facing resources actually suffer more in banking than in any other sector[18]. Forty-nine percent of financial institutions that experience a DDoS attack were targeted via their public website, compared to only 41 percent of businesses outside the financial sector[19]. Additionally, 48 percent of financial institutions had their online banking services impacted by this form of attack[20].

The cost to a financial institution facing a cyberattack specifically targeting their online banking services costs an average of $1.8 million.

Brand Reputation & Trust Impact of a Cybersecurity Incident

The financial impact of a loss of brand reputation and trust after a cybersecurity incident can be significant across all industries. A report by the Ponemon Institute and IBM reported customer churn caused by this loss was a leading contributor to the growth in the increased indirect cost of a data breach. In fact, companies that experienced less than 1 percent churn or the loss of existing customers, had an average total cost of data breach of $5.3 million, and those that experienced churn greater than 4 percent had an average total cost of data breach of $10.1 million[21].

The increased cost should be particularly concerning to companies in the financial sector because they experienced the highest rate of customer churn after a breach compared to all other industries[22]. One major reason financial institutions experience a more significant impact than a company in another industry is because consumers have to deal with fear regarding the safety of their finances. Financial institutions are aware of the impact of a damaged relationship to their bottom line. In fact, one out of every five financial institutions cited loss of brand trust or damage to their reputations as the number one concern related to a data breach incident because it may result in the loss of customers[23].

The loss of customers should rightly be of real concern to financial institutions. In a 2016 survey of identity theft and fraud victims, 12.3 percent of respondents left their credit unions, 28 percent left their banks, and 22.4 percent left their credit card companies as result of unauthorized activity on their accounts[24]. Therefore, the protection against a cybersecurity incident by financial institutions should be a top priority, as well as the need for preventative steps taken to mitigate fall-out of any potential breaches.

Targeting of Financial Institutions in Cybersecurity Attacks

Financial institutions have long been a lucrative target for cybercriminals because of the massive volumes of data and money that can be stolen[25]. As our society continues to operate more and more online (mobile banking, online banking, online shopping, the cloud, etc.) cybercriminals have increased potential routes to breach companies' defenses.

Their attractiveness to cybercriminals isn't surprising news to financial institutions. One of the top concerns for them, largely based on their own experience in fending off or fielding cybersecurity attacks, is how they will fare in the face of a cybersecurity threat. Areas of

major concern for financial service providers included threats against their digital/online banking services (45 percent), point-of-sale (POS) payment systems (40 percent), and phishing/social engineering of the institution's customers (35 percent). Companies are also concerned about attacks on their office administrative networks (35 percent) and their ATMs (26 percent)[26].

One of the largest hacks in history involved a financial institution which had its servers hijacked. The stolen data, in this case, was used to commit ongoing fraud schemes yielding some $100 million[27]. More recently, the Security and Exchange Commission (S.E.C) announced its computer system had been hacked in 2016. The hack provided the thieves with private information that may have been exploited to commit insider trading. Not only is this hack an issue in the crime itself, but is also notable in its undermining of the public's trust in the financial system itself. Although the repercussions are somewhat unknown at this time, the S.E.C recognizes that there will continue to be attacks and that a key factor of cyber risk management is resilience and recovery[28].

The methods of attack hackers employ are quite varied. They can include techniques such as spearphishing, DDoS attacks that "mask" the real activity of hackers, direct hacking of networks by taking advantage of security flaws, attacks on third-party connections that spread malware or even the company's employees themselves can lead to a data breach.

High-Profile Sustained DDos Attack

Dyn, one of several companies responsible for hosting the web directory known as the Domain Name System (DNS), suffered a sustained so-called "Distributed Denial of Service" (DDoS) attack, leading many people to intermittently lose access to specific sites (Twitter, Netflix, Spotify, Reddit, PayPal and eBay) or to the internet entirely. Dyn was hit three times and was able to successfully mitigate all attacks.

DDoS Attacks

There has been a rise in high-profile DDoS attacks in recent months, such as the attack on the Dyn web domain that crippled sites like Facebook and Twitter briefly[32]. Other DDoS attacks have affected major universities, medical centers, and of course, financial institutions. Unfortunately, the abundance of non-password protected Internet of Things devices has given hackers the tools they need to flood a website with pointless repetitive traffic, blocking access to the site for legitimate customers. Hacking groups have also found a unique way to monetize on a very simple DDoS attack, essentially using the tactic to extort ransom from the affected business.

Phishing

The total number of phishing attacks, also referred to as social engineering, in 2016 was 1,220,523[29]. This was a 65 percent increase over 2015[30]. In many instances, social engineering requires very little technical know-how and instead relies mostly on finesse. It's also rather effective, as an estimated two-thirds of data breaches and hacking events now rely on social engineering[31].

Malware

It's become a catch-all term for any form of malicious software that infects a business' network, and there are a wide variety of methods by which it can be installed. The vast majority of malware is categorized as Trojan Horse and comprises typical malicious activities like downloading and dropping files, spyware, keyloggers and password stealers, integration into botnets and conducting distributed denial of service attacks (DDoS)[33]. The number of cyberattacks targeting financial institutions and their customers soared to new heights in 2016, according to Kaspersky Lab, which observed nearly 1.09 million banking trojan attacks on users in 2016 – a roughly 30.6 percent jump over the previous year[34].

Employee Negligence or Insider Threat

No company wants to think its own employees may be the weakest link in exposing the business to a data breach, but employees can

contribute to cybersecurity incidents in a variety of both intentional and accidental ways. In terms of both data loss and dollar amounts, bank tellers are believed to pose a bigger threat to financial institutions than hackers, either through targeted theft, unauthorized access to data and funds or other circumstances such as falling for social engineering tactics[35].

Current Practices in Cybersecurity Incident Mitigation

Fortunately, raising awareness and recognition of potential cybersecurity risks among financial institutions has proven largely successful. Statistics and data cited throughout this paper have already shown that cybersecurity and data breaches are among the chief concerns for financial institutions, meaning the industry has moved forward from the days when organizations were completely blindsided by hacking events.

What financial institutions are seeing happen around them is moving this industry to better protect themselves. Financial institutions have reported that just hearing about cybersecurity incidents affecting other organizations has encouraged them to invest more in their own cybersecurity practices[36]. Other reasons financial institutions give for making an investment in better cybersecurity protection include: upper management wanting to improve the company's defenses, experiencing an attack on their own organization and demands from their customers[37]. That being said, with the threat landscape constantly evolving in this industry, financial institutions can never be too prepared to address new emerging cyber risks.

Best Cybersecurity Practices for Financial Companies

As with any overarching concern affecting an entire industry, there are some best practices financial institutions can implement in order to remain proactive about cybersecurity threats and data breaches. While there is no one-size-fits-all approach, many of the proposed measures

can be tailored to specific organizations and segments of the industry. The below recommendations will help a financial company lessen the destruction caused by cybersecurity incidents.

Be Prepared for an Attack

In 2016, 75 percent of businesses surveyed said they did not have a formal cybersecurity incident response plan across their organization, leaving them even more vulnerable in the aftermath of a hacking event or data breach[38]. In addition, 66 percent stated they were not confident in their organization's ability to recover from an attack[39]. With numbers demonstrating that a cyberattack can be a matter of when, not if, there is no reason for a functioning organization to not have a data breach response plan in place, one that clearly outlines the step-by-step procedures to follow from the moment a cyberattack is suspected. Given the potential devastation a breach can cause, some institutions have explored cyber insurance policies to help them with the repercussions of being a victim of a breach. A cyber insurance policy, which is also referred to as cyber risk insurance or cyber liability insurance coverage, is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event[40].

Over 50 percent of respondents said they would look to their financial institution to purchase identity protection.

Mitigate Fall-Out of Potential Breaches

With the increase in DDoS attacks, ransomware, global-reach malware and social engineering, financial institutions should consider not just how they can mitigate their risk of a cyberattack, but also how they will mitigate fall-out with their customer base if they do fall victim to one[41]. One way to do this is to offer their customers resources to help resolve any issues that could arise from compromised data, such as the free resolution assistance offered by the Identity Theft Resource Center (ITRC) or an identity protection service with resolution included from a trusted provider.

The return on investment for offering such a service or resources, which can preserve customer trust and help reduce the number of lost customers, in advance of the breach can be significant. Research has shown that organizations that have initiatives that aim to improve customers' trust in how the organization safeguards their personal information will reduce churn and the cost of the breach. Organizations that offer data breach victims breach identity protection in the aftermath of the breach are also more successful in reducing churn[42]. Moreover, customers appear to be looking to their financial institutions for identity protection services and/or resources, regardless of whether their information is compromised in a breach of that organization. In a recent consumer survey, over 50 percent of respondents said they would look to their financial institution to purchase identity protection[43].

Employee Education

Oftentimes, companies invest a lot of time and money into strengthening their cybersecurity technology but fail to invest equally in their biggest potential vulnerability – their employees. This disparity is concerning considering the three leading causes of breaches are often or always caused by employees. Hacking/skimming/phishing attacks were the leading cause of data breach incidents, accounting for more than half of the overall number of breaches. Of these, many were a result of CEO spearphishing efforts, in which highly sensitive data, typically information required for state and federal tax filings, was exposed. In fact, in 2016 the IRS saw a 400 percent increase in this type of fraud. The second and third most common cause of data breaches reported were accidental email/internet exposure of information and employee error[44].

Businesses should address this by ensuring employees are sufficiently educated about procedures for identifying a threat, responding to any perceived threat and maintaining regulatory and company-wide compliance[45]. Investing in employee education has a significant return on investment. The Ponemon Institute calculated the effectiveness of anti-phishing training programs and found that the average-performing program resulted in a 37-fold return on investment, even taking into account the loss of productivity during the time the employees spent being trained[46].

Successful Employee Education Program

Safety product manufacturer MSA Safety, implemented a training program and, within the first year, their rate of employees failing the simulated phishing attacks reduced from 25 percent to between 5 and 8 percent.

Transforming cybersecurity from an infrequently-occurring webinar into a key part of company culture can result in even bigger dividends for businesses. According to Siobhan MacDermott, principal in the cybersecurity practice at Ernst & Young, "If good security hygiene permeates a company, then it's something that can be successful[47]."

One way to promote cybersecurity awareness continually and create a culture of cybersecurity among employees is by offering access to either free identity theft and cybersecurity resources through organizations like the ITRC, or even access to identity protection services that have educational resource libraries, as an employee benefit. In the event a business is breached as a result of a phishing scam, offering such resources with identity theft resolution assistance may help reduce the reported $1.8 million average lost productivity costs business incur[48].

Commit to Cybersecurity

One key way financial institutions can demonstrate their full support of preventing cybercrimes is to partner with, and/or support organizations, like National Cyber Security Alliance (NCSA) which can be instrumental in not only advocating about the issues in the financial industry but they can also educate Congress about cybersecurity best practices that will better protect both consumers and businesses[49]. Investing in cybersecurity is another approach a financial institution can take to further combat this crime. One well-known financial institution in particular, Bank of America, is leading by example by taking a "blank check approach." There are no budget restrictions on this institution's cybersecurity efforts because protecting their entity from cyber threats is of utmost importance[50].

Implement New Tools and Strategies

With news of major data breaches being reported on a seemingly daily basis, consumer confidence in service providers' ability to protect their data is reaching new lows. In fact, over 50 percent of consumers indicated a lack of confidence that credit card companies' would keep the data they shared with them private and secure[51]. To address the cyberattacks causing this lack of trust, security technology is evolving rapidly to keep pace with development of technology used in cybersecurity threats. Financial institutions need to be nimble and quick in updating their existing technology and adding new solutions in order to stay one step ahead of hackers. Institutions should consider adopting new options like multi-factor authentication, artificial intelligence and machine learning, and biometric credentials for account access, to help restore and increase consumer trust in their business practices[52].

Conclusion

When it comes to the cybersecurity threats financial institutions face every day, there is only one guarantee: hackers will continue to find new ways to infiltrate your organization's network. The goal might be ruining a company's good name, causing a political stir or simply extorting money, but the methods cybercriminals employ are constantly evolving into newer, unforeseen dangers. In order to fight back, financial institutions must be prepared to adapt and redirect at every turn, facing both new threats and the old proven methods. It is also critical that these companies take steps to preventatively prepare for the seemingly inevitable successful cyberattack by having a data breach response plan in place and offering identity theft protection resources to demonstrate their commitment to protecting customers' data.

References

(1) Identity Theft Resource Center (ITRC). (2017, July 18). At Mid-Year, U.S. Data Breaches Increase at Record Pace. Retrieved from http://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release

(2) Ibid

(3) Muncaster, P. (2015, June 24). Finance Hit by 300 Times More Attacks Than Other Industries. Retrieved from https://www.infosecurity-magazine.com/news/banks-hit-300-times-more-attacks/

(4) Cawley, J. (2017, May 19). The Impact of Cyber Attacks on the Banking Industry. Retrieved from https://wall-street.com/impact-cyber-attacks-banking-industry/

(5) Kitten, T. (2015, August 24). DDoS Attacks Against Banks Increasing. Retrieved from http://www.bankinfosecurity.com/ddos-a-8497

(6) Tech Target. (2017, January). "Distributed denial of service (DDoS) attack." Retrieved from http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

(7) Kitten, T. (2015, August 24). DDoS Attacks Against Banks Increasing. Retrieved from http://www.bankinfosecurity.com/ddos-a-8497

(8) Dunn, J. (2017, June 20). Anyone can be a target of hacking. Retrieved from http://www.afr.com/news/special-reports/technology-outlook-series/anyone-can-be-a-target-of-hacking-20170618-gwthfe

(9) Urrico, R. (2017, January 31). Social Engineering Scams Evolve and Threaten Financial Institutions. Retrieved from http://www.cutimes.com/2017/01/31/social-engineering-scams-evolve-threaten-financia?&slreturn=1504036405

(10) Ibid

(11) Ibid

(12) Kaspersky Lab. (2017, June 14). Cyberthreats to Online Banking Services Cost Banks Nearly $1.8 Million. Retrieved from https://usa.kaspersky.com/about/press-releases/2017_cyberthreats-to-online-banking-services-cost-banks-nearly-18-million

(13) IBM. (2017). 2017 Ponemon Cost of Data Breach Study. Retrieved from https://www.ibm.com/security/data-breach

(14) Ibid

(15) Kaspersky Lab. (2017, June 14). Cyberthreats to Online Banking Services Cost Banks Nearly $1.8 Million. Retrieved from https://usa.kaspersky.com/about/press-releases/2017_cyberthreats-to-online-banking-services-cost-banks-nearly-18-million

(16) Ibid

(17) The Guardian. (2016, January 29). HSBC suffers online banking cyber-attack. Retrieved from https://www.theguardian.com/money/2016/jan/29/hsbc-online-banking-cyber-attack

(18) Kaspersky Lab. (2017, June 14). Cyberthreats to Online Banking Services Cost Banks Nearly $1.8 Million. Retrieved from https://usa.kaspersky.com/about/press-releases/2017_cyberthreats-to-online-banking-services-cost-banks-nearly-18-million

(19) Ibid

(20) Ibid

(21) IBM. (2017). 2017 Ponemon Cost of Data Breach Study. Retrieved from https://www.ibm.com/security/data-breach

(22) Ibid

(23) Kaspersky Lab. (2017, June 14). Cyberthreats to Online Banking Services Cost Banks Nearly $1.8 Million. Retrieved from https://usa.kaspersky.com/about/press-releases/2017_cyberthreats-to-online-banking-services-cost-banks-nearly-18-million

(24) Identity Theft Resource Center (ITRC). (2016, October 17). Identity Theft: The Aftermath (Rep.). Retrieved from http://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf

(25) Help Net Security. (2016, November 9) Increasing number of financial institutions falling prey to cyber attacks. Retrieved from https://www.helpnetsecurity.com/2016/11/09/financial-institutions-cyber-attacks/

(26) Kaspersky Lab. (2017, March 27). Cybersecurity in financial institutions 2016 — and what 2017 holds. Retrieved from https://www.kaspersky.com/blog/from-the-perils-to-strategies/6682/

(27) Roberts, Jeff John. (2017, June 21). Here Are 10 of the Biggest Corporate Hacks in History. Retrieved from

http://fortune.com/2017/06/22/cybersecurity-hacks-history/

(28) Stevenson, A. and Tejadasept, C. (2017, September 20). S.E.C. Says It Was a Victim of Computer Hacking Last Year. Retrieved from https://www.nytimes.com/2017/09/20/business/sec-hacking-attack.html

(29) Anti-Phishing Working Group. (2016). Phishing Activity Trends Report (Rep.). Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

(30) Ibid

(31) Shin, L. (2017, January 14). Be Prepared: The Top 'Social Engineering' Scams Of 2017. Retrieved from https://www.forbes.com/sites/laurashin/2017/01/04/be-prepared-the-top-social-engineering-scams-of-2017/#247030887fec

(32) Morris, D. (2016, October 22). How Hackers Make Money from DDoS Attacks. Retrieved from http://fortune.com/2016/10/22/ddos-attack-hacker-profit/

(33) Benzmuller, R. (2017, April 10). Malware trends 2017. Retrieved from https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017

(34) Barth, B. (2017, February 23). Kaspersky: Banking malware attacks up 30.6% in 2016; finance sector phishing also more prevalent. Retrieved from https://www.scmagazine.com/kaspersky-banking-malware-attacks-up-306-in-2016-finance-sector-phishing-also-more-prevalent/article/639969/

(35) Neil, M (2016, February 3). Bank tellers may pose greater threat to customers than hackers, NY Times says. Retrieved from http://www.abajournal.com/news/article/bank_tellers_may_pose_greater_threat_to_customers_than_hackers_ny_times_say

(36) Kaspersky Lab. (2017, March 27). Cybersecurity in financial institutions 2016 — and what 2017 holds. Retrieved from https://www.kaspersky.com/blog/from-the-perils-to-strategies/6682/

(37) Ibid

(38) Roberts, J. (2017, June 21). Hacked: How Business Is Fighting Back Against the Explosion in Cybercrime. Retrieved from http://fortune.com/2017/06/22/cybersecurity-business-fights-back/

(39) Ibid

(40) Lindros, K. and Tittel, E. (2016, May 4). What is cyber insurance and why you need it. Retrieved from: https://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html

(41) Moore, M. (n.d.). Don't ignore DDoS protection when attack trends change. Retrieved from https://betanews.com/2017/06/26/ddos-protection-do-not-ignore-trends-change/

(42) IBM. (2017). 2017 Ponemon Cost of Data Breach Study. Retrieved from https://www.ibm.com/security/data-breach

(43) Iris Powered by Generali. (2017, October 30). Infographic: Help Your Customers Overcome Cybersecurity Fears by Promoting Cyber Awareness. Retrieved from https://www.irisidentityprotection.com/infographic-overcome-cybersecurity-fears

(44) Iris Powered by Generali. (2017, October 9). Are Your Employees Your Biggest Cybersecurity Risk? Retrieved from https://www.irisidentityprotection.com/blog/employees-cybersecurity-awareness-month/

(45) Iris Powered by Generali (2016, June 7). Safeguarding Customer Data and Building Loyalty – from the Inside Out. Retrieved from https://www.irisidentityprotection.com/blog/safeguarding-against-data-hacker/

(46) Iris Powered by Generali. (2017, October 9). Are Your Employees Your Biggest Cybersecurity Risk? Retrieved from https://www.irisidentityprotection.com/blog/employees-cybersecurity-awareness-month/

(47) Ibid

(48) Ponemon. (August 2015). The Cost of Phishing and The Value of Employee Training. Retrieved from https://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf

(49) Iris Powered by Generali (2017, August 4). Top Concerns for Financial and Insurance Institutions. Retrieved from https://www.irisidentityprotection.com/blog/banking-malware-financial-sector-concern/

(50) Morgan, S. (2016, January 27). Bank of America's Unlimited Cybersecurity Budget Sums Up Spending Plans In A War Against Hackers. Retrieved from https://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#925202a264cd

(51) Rainie, L. (2016, September 21). The state of privacy in post-Snowden America. Retrieved from http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

(52) Oren, S. (2017, June 29). Protecting Financial Institutions – Q&A with Deep Instinct's Shimon Noam Oren. Retrieved from http://www.itproportal.com/features/protecting-financial-institutions-qa-with-deep-instincts-shimon-noam-oren/

Powered by Generali

Iris® Powered by Generali is a B2B2C global identity and cyber protection company owned by the 190-year-old multinational insurance company, Generali, offering always-available identity resolution experts (yes, real people available 24/7/365) and tech-forward solutions that uncomplicate the protection process. We opened our first Washington, DC office in 1983 with a simple mission, bringing customers from distress to relief – anytime, anywhere – and went on to become one of the very first identity theft resolution providers in the U.S. in 2003. Today, understanding that victimization has no geographical boundaries, we've got a solution no matter what your customers' coordinates are.

To learn how you can help mitigate your employees, customers, or members risk of identity theft and fraud, visit

IrisIdentityProtection.com