UNDER ATTACK:

An Examination of Cyber-Security Breaches on Industry

August 2018

BY

Taylor Brocato &

Robert Meadows

Techno Advantage
11805 N Union Church Rd Mooresville, IN 46158

ID AGENT

Techno Advantage

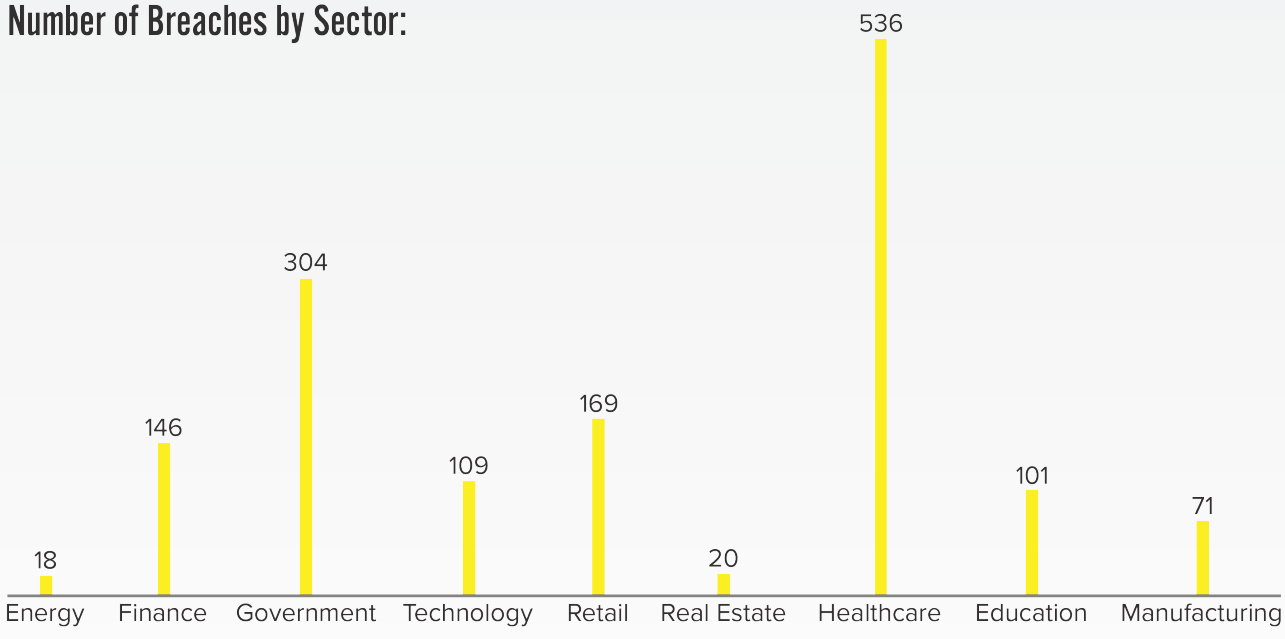
TABLE OF CONTENTS

www.technoadvantage.com
317-857-0150

SUMMARY

Over the past few years cyberattacks have left no industry unscathed. Of the 78,617 business and email account compromise scams, 41,058 occurred in the United States. The costs resulted in companies suffering $2.9 billion in losses from October 2013 to May 2018. Globally, cyber-crime is expected to cost the world $6 trillion per year by 2021. Damaging attacks such as NotPetya in Ukraine, which is estimated to have cost companies $1.2 billion, underscores the fact that cybercrime is a serious concern for every industry world-wide.

Number of Breaches by Sector:



Source: 2018 Verizon DBIR

ACCOUNTING

Accounting firms are one of the more lucrative targets for hackers. Cyber incidents affecting firms have increased almost 10 times in the last 10 years. Small firms are at more risk than larger firms, with the smaller organizations composing 57% of the cases. In comparison, large firms only compose 21%. Since smaller firms have fewer resources to recover from a breach, the median loss of $800,000 can be extremely damaging to a company's ability to withstand an attack. Given the sensitive data that accounting firms store, it should come as no surprise that personal privacy & personal financial identity compose 80% of data losses for accounting firms. This can be extremely damaging not only monetarily, but in terms of an organization's reputation as well. The trust of clients is an invaluable asset to any business, but in the accounting sector this trust is vital for operations.

Personal privacy & personal financial identity compose 80% of data losses for accounting firms.

CASE STUDY

In 2017, one of the Big Four firms, Deloitte, had a breach that was kept under wrap for an extended period. The attackers had access to their major corporate and government clients because a Deloitte employee failed to use two-factor authentication. This incident demonstrates that even a firm which prides itself on its cybersecurity, an organization that was recognized in 2012 as the best cybersecurity consultant in the world, can easily be breached if cybersecurity protocols aren't followed.

Median loss amount of an accounting hack is $800,000

Description	Ref	Income	Expenses	Bank Balance
Balance before				$100,000
Hacked	1		$800,000	
Totals				-$700,000

www.technoadvantage.com
317-857-0150

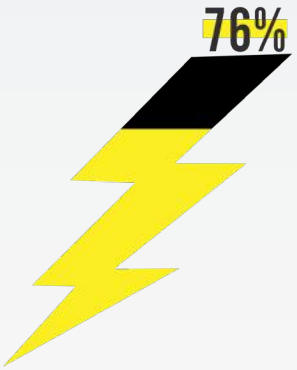
ENERGY

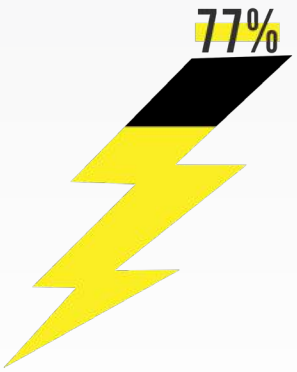
The energy sector plays a critical role in the United States economy. A successful cyberattack has the potential to create significant losses in the economy. In a recent survey published by the global insurance and risk management group Marsh, 76% of energy firms were worried about cyberattacks interrupting their business operations. Despite this worry, over 50% of energy executives surveyed had not quantified or were unsure of the worst potential exposure. Improving cyber security awareness is critical as energy firms face a multitude of cyberattacks.

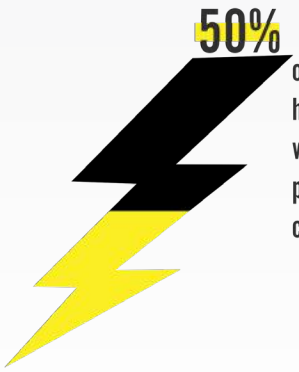
76% of energy firms [are] worried about cyberattacks interrupting their business operations.

CASE STUDY

Of significant concern is the vulnerability of the power grid. Although the United States has so far avoided a devastating attack, Ukraine experienced an attack on their power grid that cut service to 80,000 citizens. After cutting the power, attackers then bombarded customer service phone lines with fake calls to prevent the news of the power disruption being reported. If a similar attack was to occur in the United States, the effect on the country would be devastating. The attack in Ukraine is an important lesson for other energy firms to improve their defense against hackers.







FINANCE

The financial sector has seen the number of breaches it has experienced triple in the past five years. The average number of breaches per financial services firms increased from 40 in 2012 to 125 in 2017. This rapid increase can be partially attributed to malware. Between March and August 2017, 45% of financial firms experienced at least one malware attack. In 2016, financial services firms were attacked 65 times more than any other sector. Insider threat and employee error were the two main culprits, with 58% of the attacks attributed to insiders and 53% to employee error. Only 5% of those attacks were done maliciously. This highlights the importance of being aware of potential insider threats and educating employees to practice healthy cyber security standards.

Between March and August 2017, 45% of financial firms experienced at least one malware attack.

CASE STUDY

The cost of a financial record is also typically higher compared to other industries. The average United States business' compromised record brought in around $225; whereas the financial industry's average was $336. This makes the breach of Equifax all the more damaging. One of the more serious attacks in the financial service industry occurred when Equifax was breached and reported that as many as 147.9 million consumers had their data compromised. This was a serious compromise that put almost half of American citizen's social security and other private credentials at risk.

In 2016, the financial sector was attacked 65 times more than any other sector

53% Due to employee error

5% Done maliciously

58% Due to insiders

www.technoadvantage.com
317-857-0150

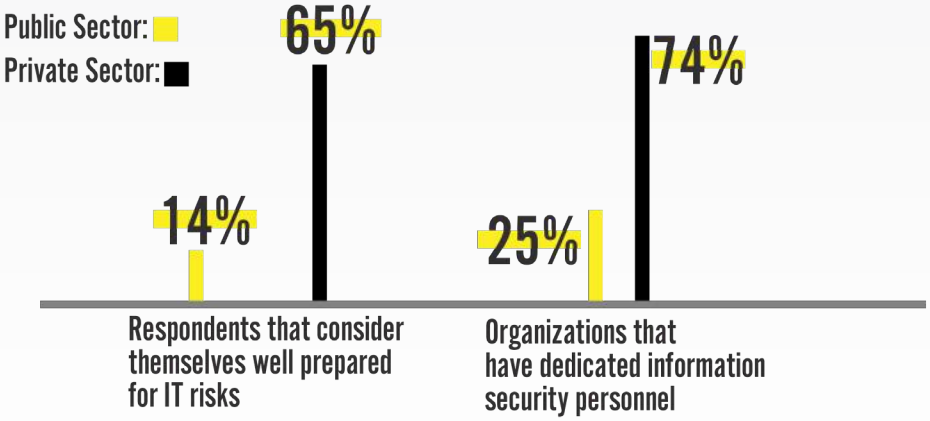
GOVERNMENT

The past year has demonstrated that government institutions are extremely vulnerable to cyberattacks. Despite this, government agencies are significantly less prepared than private sector organizations. A survey comparing the government to the private sector found only 14% of government respondents consider themselves "well prepared" for IT risks compared to 26% of private sector respondents. In addition, 75% of government respondents said their organizations lacked dedicated information security personnel versus 65% in the private sector. Government institutions are constantly in danger of a breach and if they lack sufficient cyber defense plans their operations are at risk of paralysis following a breach.

14% of government respondents consider themselves "well prepared" for IT risks.

CASE STUDY

On March 22nd, Atlanta was hit with a severe ransomware attack. The message locked files across the city, with culprits demanding around $50,000 in bitcoin. It took five days until city employees were able to re-access their computers. Even then, many systems could not be recovered. This past June, a new report claimed that at least one third of the 424 software programs the city runs remain offline or partially inoperable. Around 30% of these programs are deemed as mission critical. Mission critical programs constitute services such as the court system and law enforcement. Having such key institutions unable to function as needed is a huge threat to operating the city effectively.



www.technoadvantage.com
317-857-0150

MOBILE

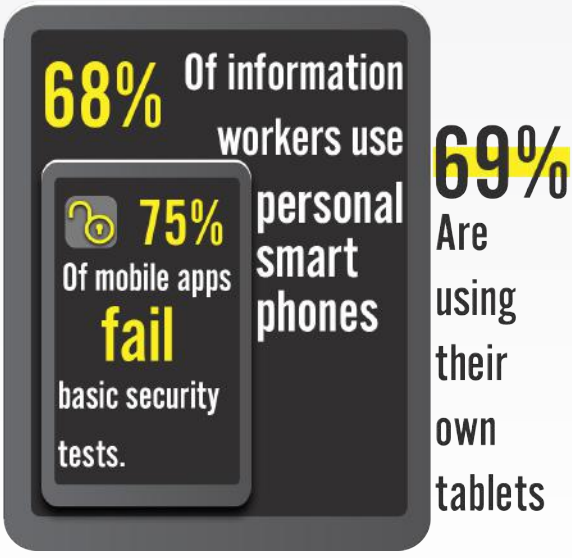
In an alarming study by Gartner, it was discovered that 75% of mobile applications would fail basic security tests. With mobile applications being extremely popular, the amount of personal data that would be exposed in a breach is significant. One reason for this lackadaisical security can be seen in the industry's own security practices. One study found that 50% of information workers use personal laptops for work, 68% use personal smartphones, and 69% are using their own tablets. This is troubling, because 21% of organizations that allow their workers to use personal laptops on their network have experienced a data breach, and 24% of organizations found these devices have at some point been connected to a malicious hotspot. Hackers can easily exploit these vulnerabilities and gain access to a company's network.

75% of mobile applications would fail basic security tests.

CASE STUDY

One of the recent breaches in the mobile industry occurred with Facebook using a third-party app called NameTest that revealed data for 120 million Facebook users over multiple years. The breach occurred due to NameTest storing users' data on a JavaScript file that could be requested by any website. Potential information exposed includes: Facebook ID, first name, last name, language, gender, date of birth, profile picture, cover photo, currency, devices used, last information update, posts, and photos of users and their friends. The popularity of mobile applications combined with poor security practices puts millions of users' data at risk.

35% of professionals work devices had no mandated measures to secure corporate data



24% of organizations found that these devices have at one point been connected to a malicious hotspot

www.technoadvantage.com
317-857-0150

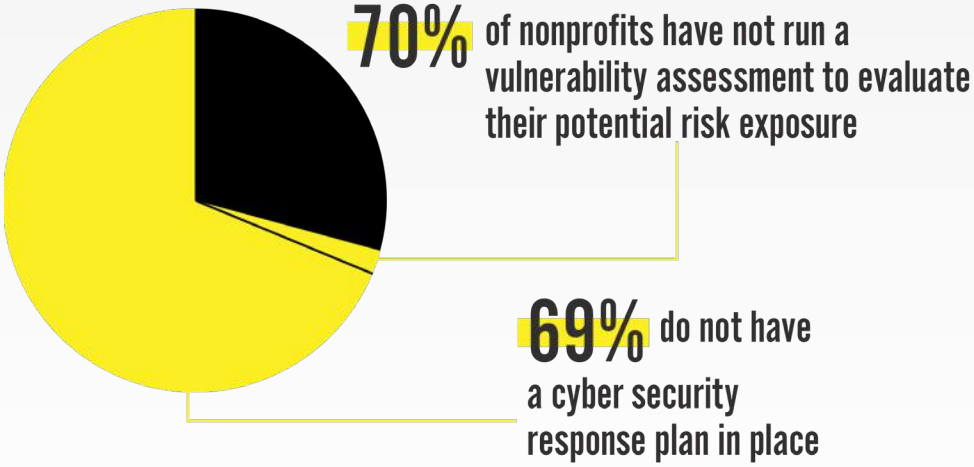
NON-PROFIT

Non-profits are a high-risk sector for breaches. A survey conducted by Cohn Reznick found more than 70% have not run one vulnerability assessment to evaluate their potential risk exposure. Even more alarming is the fact that 69% of non-profits have no cybersecurity response plan. This can endanger sensitive information and communications that non-profits engage in. Protecting the personal information of members, donors and volunteers is critical to engaging successfully with stakeholders and maintaining trust. It is vital that non-profits begin to usher in better cybersecurity practices to protect the information they store.

69% [of non-profits] have no cybersecurity response plan.

CASE STUDY

In February of 2017, a small non-profit in Indiana called Little Red Door experienced a catastrophic breach that resulted in the theft of all their data. Their information was then held for ransom at $43,000. Little Red Door eventually decided to forgo the hackers demands. As a result, hackers took to Twitter and published the letters the organization had in their files. This was very damaging to the non-profit, causing a loss of trust among partners and donors.



TECHNOLOGY

IT was the most intensely targeted industry for web application cyberattacks in 2017; an average of 1,014 attacks occurred each day. These frequent attacks emphasize the need to take an active approach to preventing a damaging data breach. A Deloitte report on the technology sector noted that high tech companies usually have a higher risk appetite than their counterparts in other sectors. This can be concerning without proper cybersecurity measures in place, especially since some tech companies provide products that are key infrastructure components for other organizations. With many high-tech companies exhibiting riskier practices with regards to cybersecurity, it is important that more technology firms implement security protocols to protect their business and clients.

In 2017 an average of 1,014 attacks occurred each day.

CASE STUDY

One of the recent IT companies that suffered a breach was Avast Software. The resulting compromise affected over two million computers. The attackers used advanced reconnaissance systems that aimed to penetrate tech companies' domains and extract valuable intellectual property.

Hackers launched an average of **1,014** attacks on firms each day

www.technoadvantage.com
317-857-0150

RETAIL

The 2017 Trustwave Security Report discovered that the retail sector suffered the most breach incidents at 22%. In total, retailers suffered more than 4,000 security incidents from 2016-2017. These successful attacks could result in a store going out of business; particularly due to loss of customers. 19% of customers wouldn't shop at a store that has been hacked recently, and 33% of customers stay away for at least three months. This represents a large chunk of business that retail stores will lose if they fail to successfully prevent a breach.

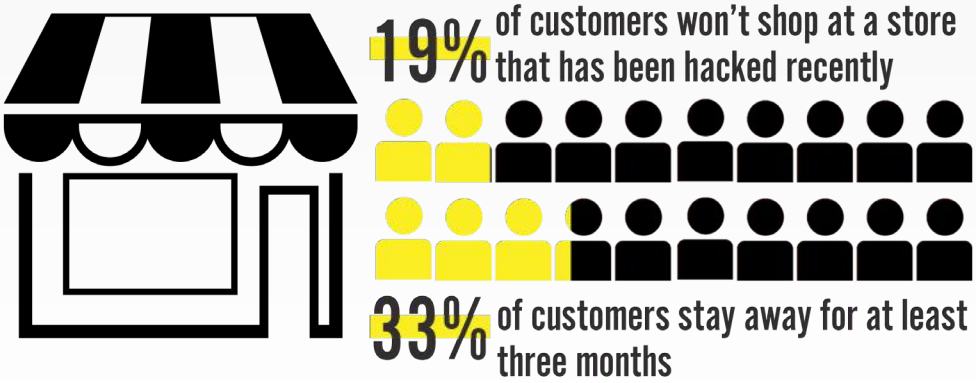
The 2018 Thales Data Threat Report discovered 75% of retailers have experienced a breach. 50% have been breached in the last year and 26% have been breached multiple times. United States retail stores are also more likely to save sensitive data in the cloud, despite only 26% of retailers implementing encryption. This leaves customer data extremely vulnerable to hackers.

75% of retailers have experienced a breach.

CASE STUDY

The Hudson Bay Company, which owns the stores Saks 5th Avenue, Saks off 5th, and Lord & Taylor experienced a breach this year. Discovered by the cybersecurity firm Gemini Advisory, they wrote this "attack is amongst the biggest and most damaging to ever hit retail companies." The firm found that credit card data dating back to May 2017 was stolen by hackers. With customers valuing retail stores they feel securely store their information, this is a very damaging hack for the organization.

Retailers suffered more than 4,000 security incidents from 2016-2017



www.technoadvantage.com
317-857-0150

REAL ESTATE

A report by the professional service firm, KPMG, discovered that one-third of real estate firms have experienced a cybersecurity attack themselves or at one or more of their properties in the last two years. In addition, half of their respondents reported they were not adequately prepared to prevent an attack. The real estate sector is one of the more vulnerable industries due to lack of preparedness in addition to the wealth of sensitive personal and financial information kept on their clients. Taking steps to improve cybersecurity practices can help prevent breaches, such as one recently announced by the FBI.

one-third of real estate firms have experienced a cybersecurity attack

CASE STUDY

A recent report by the FBI alerted real estate companies in California that almost all transactions are being targeted by hackers. In 2017, there was nearly $1 billion stolen of home purchase funds.

www.technoadvantage.com
317-857-0150

HEALTHCARE

Healthcare is a very profitable target for cyber criminals. However, the biggest threat to the healthcare industry are internal actors. The Verizon 2018 Data Breach Report found 58% of cyber incidents in healthcare organizations involved insiders. In addition to purposeful insider attacks, 81% of these cybersecurity incidents are caused from employee negligence. With such a high percentage of breaches coming from their own employees, it is imperative that healthcare organizations have a proactive approach to combat the leak of stolen credentials.

These breaches have cost the United States healthcare industry an estimated $6.2 billion. Medical information is valuable to hackers and likely to be resold on the Dark Web. A pilfered medical record can be sold for $50 on the Dark Web, compared to $1 for a social security number or credit card. This high price of medical records provides cyber criminals with a priority target, and their pursuit could be successful if healthcare organizations are not implementing strong cyber-security defenses.

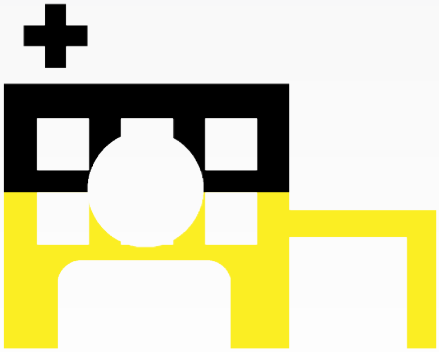
Breaches have cost the United States healthcare industry an estimated $6.2 billion.

CASE STUDY

UnityPoint Health suffered its second breach of the year. A phishing attack was used to compromise 1.4 million patient records. Because this is the second time UnityPoint Health has fallen victim to a phishing attack in the span of 5 months, the determination of cybercriminals and their attraction to the medical sector is glaringly obvious.

Cost on the Dark Web:

58% of cyber incidents in healthcare organizations involved insiders



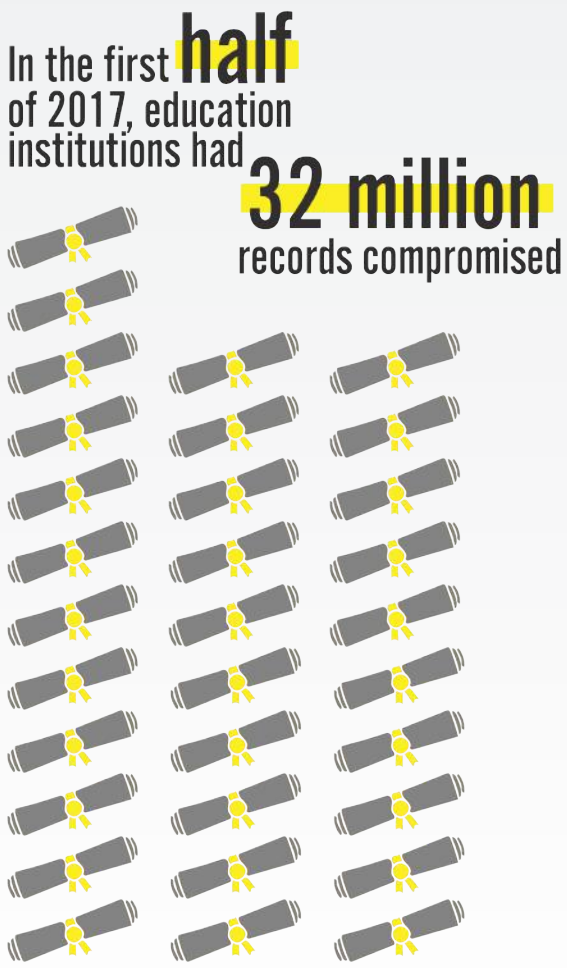
81% of these cybersecurity incidents are caused from employee negligence

www.technoadvantage.com
317-857-0150

EDUCATION

Universities have faced an increasing onslaught of cyberattacks due to the personal information they store on thousands of students. In the first half of 2017, education institutions had 32 million records compromised. Obtaining these records enable hackers to perpetrate identity theft schemes. Hackers don't just limit themselves to universities but also target lower education institutions as well.

In the first half of 2017, education institutions had 32 million records compromised.



CASE STUDY

Late in 2017, the Department of Education sent a warning about the threat of hacking for educational organizations. One successful breach occurred in Columbia Falls, Montana. Messages demanding $150,000 in bitcoin in exchange for not releasing stolen school records, were sent out to students and administrators. In addition, threatening messages had been sent to students referencing Sandy Hook. These attacks resulted in over 30 schools closing for three days for law enforcement to identify the hackers. These cases are extremely disturbing with hackers using violence against children to intimidate their victims.

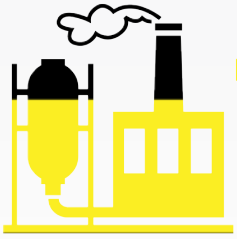
MANUFACTURING

A very striking quote by Rebecca Taylor, Senior Vice President for NCMS (National Council for Manufacturing Sciences), indicates the vulnerability of manufacturing companies to cyberattacks; “Most manufacturing systems today were made to be productive – they were not made to be secure. Every manufacturer is at risk – it isn’t a matter of if they will be targeted, it’s a matter of when.” Considering that customers are beginning to value strong cybersecurity in which companies they choose, manufacturers would be wise to heed her words. A survey conducted by the Government’s Cyber Streetwise campaign and KPMG noted that 96% of small manufacturing businesses think about creating a strong reputation frequently or all the time. However, only 30% of those surveyed who have not been compromised are seriously considering the impact a successful breach could have on their business. This should be a major concern since 83% of consumers surveyed are worried about their data being safe, and another 58% say a data breach would discourage them from using a business in the future. Losing such a large amount of their customers could decimate a small manufacturing company. With customers becoming more concerned about which companies best protect their information, it is critical that businesses take steps to ensure their clients trust.

Every manufacturer is at risk – it isn’t a matter of if they will be targeted, it’s a matter of when.

CASE STUDY

In April of 2018 a manufacturer of portable oxygen devices named Inogen experienced a breach that affected 30,000 individuals. The personal information of the individuals was compromised using a phishing scheme. The hacker was able to access an employee’s email, compromising Medicare identification numbers, insurance policy information and the medical equipment the company sold to individuals.



58% of consumers say a data breach would discourage them from using a business in the future

96% of small manufacturing businesses think about creating a strong reputation frequently or all the time

www.technoadvantage.com
317-857-0150

CONCLUSION

Cyberattacks do not discriminate against any sector. Every sector endures challenges when working to prevent, stop, or overcome a cyberattack. Working to educate employees on practicing the best cybersecurity defense can significantly reduce the potential for a successful breach. It is important to be vigilant in combating potential compromises. This is especially true in the sectors that rely on client trust. When customers feel their personal information is at risk, companies will have a more difficult time re-gaining the trust of once loyal customers. The Internet Age has brought an amazing ability to conduct business at a new level of profitability. With this increased reward brings more danger of threat actors inflicting harmful attacks on business. Being proactive in developing a cybersecurity plan can be the difference in successfully defending a breach or losing millions to a harmful attack.

ADDITIONAL RESOURCES

https://itsecuritycentral.teramind.co/2018/01/03/cyber-security-statistics-data-breaches-and-cyber-attacks/

https://www.bbc.co.uk/news/technology-35667989

https://www.hiscox.com/documents/brokers/Hiscox-Cyber-Loss-ACCT.pdf

https://gizmodo.com/one-of-the-worlds-biggest-accounting-firms-hacked-after-1818722565

https://www.forbes.com/sites/mikescott/2018/03/07/energy-industry-worried-about-cyber-attacks-but-doesnt-really-know-what-to-do/#131d5d9268bb

https://www.scmagazine.com/financial-services-sector-most-attacked-in-2016-ibm/article/653706/

https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?utm_term=.1af388a043ff

http://www.govtech.com/security/Survey-Highlights-Cybersecurity-Gaps-Between-Government-and-Private-Sector.html

https://techcrunch.com/2018/06/06/atlanta-cyberattack-atlanta-information-management/

https://www.bankinfosecurity.com/law-firms-under-fire-a-9026

https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html

https://www.iqvis.com/blog/guide-protect-mobile-app-cyber-attacks/

https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html

http://fortune.com/2018/06/29/facebook-nametest-data-breach/

https://blog.kennasecurity.com/2017/10/nonprofits-cannot-ignore-cybersecurity/

https://nonprofitquarterly.org/2017/06/08/nonprofit-cybersecurity-pay-attention/

https://www.mercurynews.com/2017/09/21/tech-companies-targeted-by-sophisticated-malware-attack/

https://www.techrepublic.com/article/it-companies-face-1000-cyberattacks-per-day-heres-how-to-protect-your-business/

https://www2.trustwave.com/rs/815-RFM-693/images/2017%20Trustwave%20Global%20Security%20Report-FINAL-6-20-2017.pdf?mkt_tok=eyJpIjoiWmpFeE16Z3dOamsxTTJVNSIsInQiOiJXMTFTblZTcUpaU3FqbUJPWFlaRzF4RWFXM2xicGtCUkxjTU1zcnZxTVVoVDZ4NlE2WFZPVHpcL2xJYmo4QTdhNHRmTXM1eVR3TlZYdnBqWmpIbVNMMWtwZDF5QjFTUVptQkxBVDVMbklJKzZWcXN1NGdWclZaempZUWJtQ0JuOXEifQ%3D%3D (Page 3)

https://www.brinknews.com/study-reveals-flaws-in-u-s-retail-cybersecurity/

https://www.helpnetsecurity.com/2018/07/19/retail-data-breaches/

https://money.cnn.com/2018/04/01/technology/saks-hack-credit-debit-card/index.html

https://commercialobserver.com/2017/08/real-estate-is-not-above-the-cyber-attack-risk/

https://www.nbcbayarea.com/news/local/Experts-Virtually-All-CA-Real-Estate-Transactions-Targeted-By-Hackers-487165181.html

http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

https://cyberpolicy.com/cybersecurity-education/4-healthcare-cybersecurity-stats-thatll-raise-your-blood-pressure

https://www.healthcareitnews.com/news/14-million-patient-records-breached-unitypoint-health-phishing-attack
https://www.csoonline.com/article/3250862/security/top-cybersecurity-exploits-active-in-the-education-sector-today-and-why-you-should-care.html

https://www.cnbc.com/2017/10/24/department-of-education-warns-that-hackers-are-now-targeting-schools.html

https://advancedmanufacturing.org/manufacturers-leading-target-infrastructure-cyber-attacks/

https://www.manufacturingglobal.com/technology/small-manufacturers-must-not-underestimate-impact-cyber-attacks

https://www.jdsupra.com/legalnews/manufacturing-sector-getting-hit-with-11366/