WHITE PAPER

Causes and Effects of Data Breaches

Introduction

Anyone who regularly reads newspapers or watches television news does not need to be told that data breaches are serious and prevalent issues. They are reported on frequently, often in ominous tones.

The concern is warranted. According to IBM-sponsored research by Ponemon Institute, in 2016 the average cost of a data breach was $216 for each lost or stolen record that included sensitive and confidential information. The average total cost for the organization as a whole was $7.01 million per incident. And, these aren't merely a few isolated occurrences. There were 1,093 reported data breaches in 2016 in the United States alone.[1]

Clearly, the total cost for an organization varies depending on its size and the magnitude of the breach, but it can represent a material portion of annual revenue.

And, keep in mind that many of the victim companies already had some level of data security in place—and, in many cases, a high level. The consequences could have been even direr without it.

As familiar as you may be with these news stories and statistics, it is still important to take a step back and ensure you are familiar with exactly what data breaches are, what causes them, the costs your organization might incur as a result of them, and how you can prevent them. This white paper presents a high-level overview of these topics.

[1] Here's What the Average Data Breach Cost in 2016, Information Security Solutions Review, January 20, 2017 (https://solutionsreview.com/security-information-event-management/heres-what-the-average-data-breach-cost-in-2016/)

Definition: Data Breach

The simplest definition of a data breach is:

> Any incident that exposes data to an unauthorized environment. The affected data may or may not still be accessible to the victim organization after the breach. This definition holds whether the breach was caused by intentional or unintentional actions.

The breached data can include anything from relatively inconsequential personal files up to details of highly confidential health records and financial information.

Data Breach Causes

Thanks primarily to blaring headlines, when people hear the phrase "data breach," they often think of hackers with malevolent intent. That's definitely a serious threat, but it's not the only one. Other causes of data breaches, such as human error and system glitches, are inadvertent and, therefore, have benign or no intent. Nevertheless, a non-malicious breach can sometimes be almost as costly as a malevolent one.

3 type of data breaches

- Human Error
- System Glitch
- Criminal Attack

Human Error

Headlines about outsider hacking thefts of massive volumes of personal and financial data notwithstanding, although there are some outliers, most studies show that more data breaches result from human error than from criminal attacks. In fact, 62% of the data breaches reported to the U.K. Information Commissioners Office resulted from human error.[2]

A CompTIA survey pegged the number somewhat lower, 52%, but still found that the majority of data breaches were caused by human error.[3]

[2] Human error causes more data loss than malicious attacks, ComputerWeekly.com, June 2, 2016. (http://www.computerweekly.com/news/450297535/Human-error-causes-more-data-loss-than-malicious-attacks)

[3] Surveys: Employees at fault in majority of breaches, CSO, April 10, 2015. (http://www.csoonline.com/article/2908475/security-awareness/surveys-employees-at-fault-in-majority-of-breaches.html)

That having been said, those numbers can be subject to some interpretation. For instance, if a laptop, tablet or smartphone—or even something as old-fashioned as a sheet of paper—it is inadvertently lost and the data on it is subsequently accessed by someone who serendipitously found it, that's a data breach, but is it human error? The loss was human error, but the access of the data may have been an intentional act.

Likewise, should a breach initiated by a phishing attack be considered human error or a criminal attack? There are elements of both. The sending of the phishing email and the intrusion the attacker executed through it may have been criminal, but the click on the link in the email, without which the attack would have failed, was human error.

However, there is little point in spending too much time on what is primarily a pedantic data-breach taxonomy exercise. Whether you classify it as human error or something else, the point is that data has been put at possibly serious risk.

Under its broadest definition, human error is a notoriously difficult to defend against because there are almost unlimited variations on the theme, it occurs randomly, and there are few warning signs.

System Glitch

Even with today's exceptionally dependable hardware and almost as reliable software, sometimes things go bump in the night.

It goes without saying that these problems follow no patter of logic. If they did, the bugs would have been patched and the glitch avoided. Often, the resulting data breach is not spotted until some time after the damage is done. And sometimes, even after it is discovered, the source of the problem, and an explanation for it, is never determined.

Because these are internal, chaotic faults, cyber-attack countermeasures do little or nothing to prevent them. An organization with the most stringent of security controls may experience many of them, while an organization with minimal security may experience none. Or vice versa.

Nevertheless, security software can still provide value in these situations. While the software likely won't stop a system fault from causing a data breach, it might recognize that an infringement occurred and initiate automated investigation and monitoring to find out exactly what happened. The organization can use the resulting information in its remediation efforts and to implement practices and technologies that might prevent it happening again.

Criminal Attack

For the purposes of this white paper, a criminal attack is considered to be any unauthorized, intentional access to protected data, regardless of whether that data was secured as stringently as it should have been, and regardless of whether the attacker hopes to profit from the attack.

Of the three breach types, a criminal attack is almost always the most costly. Industry surveys report a wide range in the prevalence of malicious attacks as a cause of data breaches—from 37% to 50% in the studies we've found in the public domain. The reported costs also vary, from about $150 to $300 per compromised record.

There are typically higher costs associated with data compromised via a criminal attack because it is exactly that, a criminal attack. A user error, or particularly a system failure, may have not involve any malicious intent at any stage of the breach and its repair, but a criminal attack is almost always undertaken to extract value from or do damage with the purloined data.

Without adequet safe guards your company runs the risk of financial penalties and even jail time

Some Industries Require Higher Than Normal Data Security

All organizations must take the threat of data breaches seriously. They owe it to their customers, suppliers and shareholders. What's more, in many countries they face legal penalties if they do not employ adequate safeguards. This is particularly true for publicly traded companies that operate under securities regulations.

However, while all companies must protect their data, some industries require an even higher level of security due to the nature of the data they manage and the regulatory environment in which they operate. Two such industries are healthcare and finance.

Healthcare

Few records are considered more private than health records. Protecting them from exposure isn't just a moral obligation on the part of healthcare providers. It's also a legal requirement in most jurisdictions.

For example, in the United States, the Privacy Rule of the Health Insurance Portability And Accountability Act (HIPAA) "requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.[4]

In addition, the HIPAA Security Rule "requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[5]

It's important to note that, despite the inclusion of the word "insurance" in the HIPAA title, these rules apply beyond health insurance providers. They bind all organizations that process health information. Thus, for example, in addition to health insurers, healthcare providers, third-party claims processors and "healthcare clearinghouses" are covered by the regulations.

Depending on which of five categories it falls into, each violation can result in minimum fines of from $100 to $50,000 per violation, with a maximum of $1.5-million per violation category per year. In addition, if those violations result in a data breach or security incident, the organization may incur an additional fine of up to $50,000 per violation.

Furthermore, depending on the nature of the violation, criminal penalties of as long 10 years in prison may be applied if the violation was committed for personal gain or with malicious intent.[6]

[4] Health Information Privacy, The HIPAA Privacy Rule, U.S. Department of Health & Human Services (https://www.hhs.gov/hipaa/for-professionals/privacy/index.html)

[5] Health Information Privacy, The HIPAA Security Rule, U.S. Department of Health & Human Services (https://www.hhs.gov/hipaa/for-professionals/security/index.html)

[6] What are the Penalties for HIPAA Violations?, HIPAA Journal, June 24, 2015 (http://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/)

Finance

Clearly, the importance of privacy and data security is also high in the financial services industry. Few people want the details of their financial assets spread across the Internet. And it goes without saying that no one wants the electronic accounting of his or her financial assets tampered with to their detriment.

Not surprisingly, laws require that financial institutions secure the data they manage. For example, in the United States, the Safeguards Rule of the Gramm-Leach-Bliley Act requires that financial institutions protect themselves against any anticipated threats or hazards to the integrity of customer records and information.

In addition, the Payment Card Industry (PCI) Security Standards stipulates that all organizations that accept or process credit card payments must, among other requirements, protect stored cardholder data, develop and maintain secure systems and applications, restrict access to cardholder data by business need-to-know, restrict physical access to cardholder data, and maintain a policy that addresses information security for employees and contractors.[7]

Consequences of Data Breaches

The numbers are staggering. Juniper Research estimates that cost of data breaches will increase to $2.1 trillion globally by 2019. Furthermore, it estimates that the average cost of a data breach will exceed $150 million by 2020.[8]

Yet while direct financial impacts are normally the largest component of the costs of data breaches, they alone do not tell the whole story. A company's reputation is also at stake. In addition, the cost of recovering from a breach may also be high.

[7] Maintaining Payment Security, PCI Security Standards Council, LLC (https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security)

[8] Cybercrime Will Cost Businesses Over $2 Trillion By 2019, Juniper Research Ltd., May 2015. (https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion)

Direct Financial Costs

The most obvious costs of data breaches and the easiest to measure are the direct financial costs. The largest of those costs are frequently legal liabilities. As illustrated by the examples in the accompanying sidebar titled Data Breach Lawsuit Examples, some notable settlements in data breach cases have ranged up to more than $100 million.

As the variety and volume of digitized data increases, and as people become more aware of and sensitive to the vulnerabilities they face when their data is exposed, these costs are likely to rise, possibly substantially.

In addition to the costs of settling lawsuits or of judgments from trials, regulators may impose penalties after a breach. The discussion above touched on some of the regulations in the healthcare and financial industries, but most, if not all, organizations that manage customer data operate under some data security regulations. For example, under the Sarbanes-Oxley Act (SOX), all publicly traded companies in the United States must put adequate security controls in place to protect against data corruption and loss.

These regulations each impose different penalties. An enumeration of them all is beyond the scope of this white paper. Suffice it to say that contravening the regulations can result in substantial direct costs to the offending company.

Brand and Trust Costs

Many companies expend considerable resources—including, but not exclusively hard-dollar expenditures—to position their companies in the minds of the market and to build brand equity. If those positions and brands are built, at least in part, on a message of trust, much of that equity may be lost if a significant data breach results in a serious loss of customers' privacy and/or the jeopardizing of their financial data.

Customers whose credit cards were compromised because of a data breach may be reluctant to provide their new card numbers to the same company. And prospective customers may share that reluctance after reading or hearing news reports about a large-scale credit card theft.

Likewise, customers who shared private information—email addresses, street addresses, phone numbers, birthdays, etc.—in return for taking advantage of a company's goods and/or services might think twice before entering into that bargain again if their information was compromised. Likewise, prospective customers may decide to never share their information under those conditions.

There is also a question of the damage to the company's overall reputation. Customers and prospective customers may wonder if they can, in general, trust a company that is, rightly or wrongly, perceived to be careless with data.

These costs are impossible to predict accurately a priori. What's more, they are even difficult to estimate with precision after the fact because they are typically opportunity costs. It's not a question of dollars paid out, but rather revenues and profits that the company would have received if the event hadn't happened.

Recovery Costs

Problems must be solved. Depending on the nature of the data breach, affected customers may have to be notified. They may need to be assigned new accounts and passwords. They may need assistance with avoiding, or at least mitigating, he consequences of identity theft. And lost data may need to be recovered.

Some of these activities can be automated. But most, if not all, will require some level of human intervention, if only helpdesk support to walk people through the remediation steps when they run into problems.

Consequently, employees may need to work overtime. Temporary staff may need to be brought in. And some of the work may need to be outsourced.

Data Breach Lawsuit Examples

- **2017 — Anthem Inc. agreed to pay $115 million to settle after a cyber-attack exposed the personal information of 78 million people.** (http://www.foxbusiness.com/features/2017/06/23/anthem-agrees-to-115-million-settlement-data-breach-lawsuit.html)
- **2017 — Target Corp. agreed to pay a $18.5 million to settle a lawsuit related to a cyber-attack data breach** http://fortune.com/2017/05/23/target-settlement-data-breach-lawsuits/
- **2017- Home Depot agreed to pay a $25 million settlement as a result of a data breach.** (http://fortune.com/2017/03/09/home-depot-data-breach-banks/)
- **2014 — LinkedIn agreed to pay a settlement of $1.25 million after 6.5 million passwords were compromised.** http://www.bankinfosecurity.com/linkedin-a-7229)

How Data Security Software Can Help

Modern systems are complex. That statement is trite, but it's also an understatement. Systems today tend to be many-layered things, possibly including layers that reside in nebulous clouds. Furthermore, they are typically at least partially open to the world through direct or, possibly, indirect Internet connections. Consequently, they often expose many points of vulnerability.

In some cases, those vulnerabilities are unknown and unintentional. However, in most cases they're merely a necessary evil in systems that must serve audiences both inside and outside the organization.

Fortunately, security software can help to monitor the points of exposure, detect breaches, and, possibly, plug the holes before damage is done or lessen the damage.

However, it's necessary to recognize the multifaceted nature of the threats. Standing guard over all but one threat vector does no good if all of your data pours out through that one opening. Comprehensive security software and practices is, therefore, critical to reducing the threat to an acceptable level.

The meaning of data-security comprehensiveness varies somewhat among different platforms. And it's much too broad and deep a topic for this white paper. Nevertheless, when evaluating data security software it's important to first learn what holes need to be at least monitored, if not plugged. Then find solutions that address all of the vulnerabilities.

Security Software is critical to reducing the threat of exposer to modern systems

Conclusion

Data breaches should alarm every organization. Their costs are increasing, dramatically in some cases. And their negative impacts may extend well beyond the event. Customers are more likely to sever relationships with a company—and prospective customers are less likely to form new relationships—after a serious data breach. When this happens, the company loses the potential lifetime value of those customers and prospects.

In addition to increasing costs, the frequency of data breaches is also rising. Regardless of the type or size of a business, these two factors can produce disastrous effects. However, by tightening security appropriately, organizations can greatly reduce the odds of becoming victims. Furthermore, they gain greater peace of mind, knowing that their most sensitive data is adequately protected.

Effective protection against security threats includes multi-layered defenses. No safeguard can be guaranteed to be 100 percent foolproof. With a multi-layered approach, on those rare occasions when one layer fails, the layers above and/or below it provide a granular, backup defense that reduces the threat.

Enforcive provides several layers of security for IBM i (iSeries/AS/400) to help keep your systems and data safe. For more information, contact Syncsort.

About Syncsort

Syncsort is the global leader in Big Iron to Big Data software. We organize data everywhere to keep the world working – the same data that powers machine learning, AI and predictive analytics. We use our decades of experience so that more than 7,000 customers, including 84 of the Fortune 100, can quickly extract value from their critical data anytime, anywhere. Our products provide a simple way to optimize, integrate, assure and advance data, helping to solve for the present and prepare for the future. Learn more at syncsort.com.

syncsort