The Methods and Costs of Data Breaches

"Data breach" has become a common term, so much so that it seems as though not a day goes by without mention of a data breach occurring. Everyone has seen the evolution of a data breach and how it evaporates into the index of digital data breach history. Time and time again, reminders arise about the vulnerability of all data and how easily data can be copied, transmitted, stolen and perused by unauthorized individuals or large state actors.

There is no doubt all institutions and regulatory bodies are aware of the likelihood and susceptibility of data breaches; however, the key is to properly ensure businesses and institutions are tying the likelihood with the financial impact a data breach can have. In addition, the consumers who are at a loss because of a data breach are left out in the cold, considering their information is in the hands of someone who can potentially cause reputational and financial damage.

The business-to-external parties (such as consumers) or other third parties (such as regulatory bodies) all have a responsibility and have to pay in terms of reputational, financial or regulatory backlash when a breach occurs. It is not like no one understands the cost side of breaches; however, it is something of a reactionary response that money talks and once a monetary figure is tied to a breach, everyone pays attention. After all, it takes money to reduce the likelihood of data breaches, and for this there is a fiscal aptitude one must have to register the impact of a data breach.

Breach of Data

"Data breach" has been loosely defined in various ways, but the simplest definition is the unlawful and unauthorized acquisition of personal information that compromises that information's security, confidentiality or integrity. Personal information, which is the individual's name and government-issued identification data, financial account numbers and personal identification numbers (PINs), are all termed as computerized data that include personal information. Note that lawfully made public information does not qualify for a breach since it is not subjected to the same level of privacy regulation.

What Does a Breach Cost?

One of the most valued research studies in data breach cost, which is regarded by most industry experts as noteworthy, is that sponsored by IBM Security and performed annually by the Ponemon Institute. The 2017 study was conducted across 11 countries and two regions, involving a total of 419 organizations. The global average cost of a data breach was approximately US $3.62 million and the average cost for each stolen record containing sensitive and confidential information was US $141.[1] Naturally, the cost of the average data breach will vary based on the location of the breach and the industry or the various unique factors tied to each organization. The Ponemon Institute report also shows that institutions spent, on average, US $4.5 million to resolve data breaches; institutions with losses greater than 50,000 records spent approximately US $10.3 million (**figure 1**).

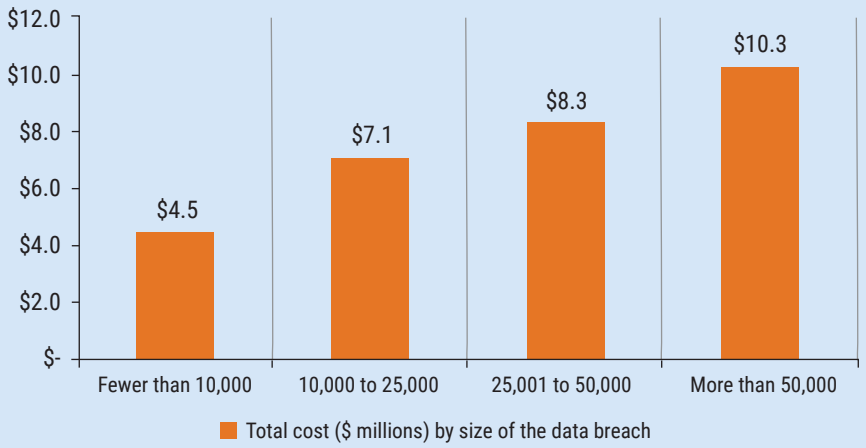
Mohammed J. Khan, CISA, CRISC, CIPM
Is a global head of IT audit at Baxter, a global medical device and healthcare organization. He works with C-suite offices across audit, security, medical device engineering (cyber) and privacy. He has spearheaded multinational global audits and assessments in several areas, including enterprise resource planning systems, global data centers, cloud platforms (i.e., Amazon Web Services, Salesforce.com), third-party manufacturing and outsourcing reviews, process re-engineering and improvement, global privacy assessments (EU Data Protection Directive, the US Health Information Portability and Accountability Act [HIPAA], the EU General Data Protection Regulation [GDPR]), and medical device cybersecurity initiatives in several markets over the past five years. Most recently, he has gained further expertise in medical device cybersecurity. Khan has previously worked as a senior consultant for Ernst & Young and Deloitte and as a technology expert for global enterprise resource planning/supply chain systems at Motorola. He frequently speaks at national and international conferences on topics related to data privacy, cybersecurity and risk advisory.

Focusing more on individual industries, in 2017, the business sector topped the list at 54.7 percent of the total number of breaches, followed by the healthcare/medical industry at 22.6 percent. The education sector ranked third at 11 percent of the total number of breaches, followed by the banking/credit/financial industry at 5.8 percent and the government/military at 5.6 percent.[2] These data put into perspective the fact that most of the breaches occurring are in institutions that operate as data processors or data controllers. As the research also indicates, the amount of hacking, which includes campaigns such as phishing and ransomware, were primary causes of the data breaches.

The cost of the breach can vary from industry to industry, but generally, there are similar themes in terms of main areas (**figure 2**). They can be categorized into three main areas—business, litigation and customer—as follows:

- **Loss of business**—This area tends to be the most relevant from a financial perspective since it eliminates the operation of the business or part of a business, resulting in lost revenue. Depending on the industry, the type of loss-of-business areas within the organization can add up fairly quickly and can eat into profits.
- **Legal costs**—This can be a heavy financial burden for most organizations victimized by a data breach. Absent a cybersecurity insurance policy covering legal fees in the event of a breach, the cost of hiring a firm and/or firms to manage the litigation side of the breach can add up. One study found that

Figure 1—Cost of Data Breach by Size



Source: IBM and Ponemon Institute, "2017 Ponemon Cost of Data Breach Study," USA, 2017. Reprinted with permission.

Figure 2—Data Breach Key Impact to Organizations

healthcare organizations ranked at the top of the list for costs, incurring an average cost of US $380 per lost or stolen record. Other leading targets were financial services at US $245 and media at US $119. The public sector had the lowest average cost per lost or stolen record at US $71.[3]

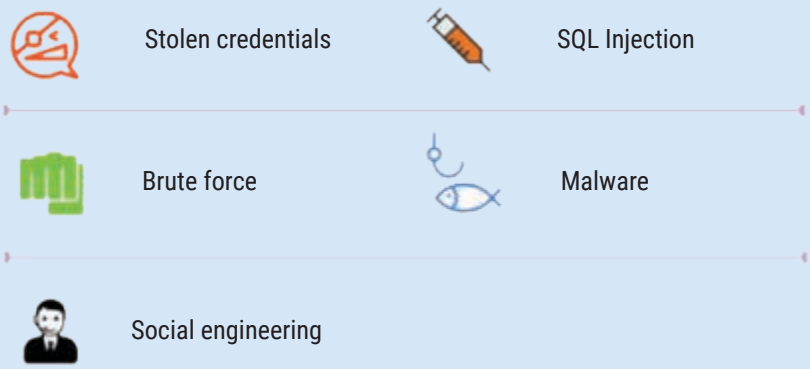
- **Loss of customers**—This will inevitably occur, and it is impossible to place a monetary value on loss of customers since part of the loss is losing consumer faith and, thus, depletion of the brand value on both Main Street and Wall Street. A recent study performed across 10,000 people worldwide found that if an organization were to suffer a data breach, 70 percent of its consumers would stop doing business with it.[4] Interestingly enough, another study found that customers are more likely to leave a bank after experiencing fraudulent charges on an account. However, other industries, such as healthcare providers and insurers, may be harder to leave after a breach due to limited choices or time-based agreements.[5]

Methods of Breaches

The typical vectors utilized by threat actors are normally fairly basic and low-level, taking advantage of small openings that can result in a disastrous ending (**figure 3**):

- **Stolen credentials**—Research conducted between March 2016 and March 2017 identified 788,000 credentials stolen via key loggers, 12 million credentials stolen via phishing and 3.3 billion credentials exposed by third-party breaches. Also, in the case of the third-party data breaches, 12 percent of the exposed records included a Gmail address serving as a username and a password.[6] Transitive trust causes a severe case of downstream impact on credential integrity across multiple platforms, and this study proves this point, which provides perspectives on some of the reasons why there are so many breaches and they are increasing year over year.
- **Malware**—Malicious software has been around since the advent of computing technology, and it has grown to become among the primary ways breaches occur. One of the leading organizations in the area of cybersecurity, Kaspersky Lab, noted, "Computer viruses are probably the most familiar type of malware, so named because they spread by making copies of themselves. Worms have a similar property. Other types of malware such as spyware are named for what they do; for example, spyware transmits personal information, such as credit card numbers."[7]
- **Social engineering**—Employees in many organizations have a social media presence on major sites such as Facebook, LinkedIn, Quora and Twitter. Each platform has the potential to provide a hacker several key data points about employees, which can enable use of the data to hack the employee account at the enterprise layer by spoofing and launching a social engineering attack

Figure 3—Methods of Breaches



on the organization. By leveraging the multitude of options of going through social media accounts with exposed data, attackers can gather these data to further their advances in terms of hacking into accounts.

- **Brute force**—The concept is simple: Attack the source of the data with as much persistence as possible and try every permutation to get through the password control. Distributed computing increases the likelihood and success of breaches due to this method.
- **SQL injection**—This attack forms through a database-connected mechanism, which invariably is connected to a web application. A fragment of the Structured Query Language (SQL) code is entered into a field on the web page and directs to another URL. The concept is simple, but very effective. Based on Ponemon Institute's SQL injection survey, "65 percent of respondents experienced one or more SQL injection attacks that successfully evaded their perimeter defenses over the previous 12 months, and it required organizations an average of nearly 140 days to discover that a SQL injection attack had breached their databases."[8]

> "THE UPSIDE TO ALL THE DATA BREACHES OCCURRING IS THERE IS ROOM TO HELP REDUCE THE RISK OF A DATA BREACH BASED ON ALL THE EXAMPLES TO STUDY."

These methods of breaches help outline the basic principles all organizations should consider when investing resources in security. Part of the cost of data breaches inevitably results in ramping up the security and privacy front of the organization that had a data breach. The upside to all the data breaches occurring is there is room to help reduce the risk of a data breach based on all the examples

to study. There can be further reduction in the cost of a breach by simply paying attention to the methods of the breach.

Conclusion

The cost of a breach has proven it can be disastrous for the institutions and, more important, the data subjects who lose their personal and private information. As understanding of the costs involved with data breaches across the globe grows, it is clear that even further understanding and knowledge of how best to reduce this cost by preventive measures and educating the board, business leaders, technology companies and the authorities about the risk are required.

Cyberattacks will continue to increase and breaches will occur and then fade away when another news story of a breach takes the spotlight. There will not be a one-stop solution to stopping breaches; however, being aware of the costs of data breaches will help in assessing the risk and mitigating threats to avoid breaches occurring in the first place.

Endnotes

1 IBM and Ponemon Institute, "2017 Ponemon Cost of Data Breach Study," USA, 2017, *https://www.ibm.com/security/data-breach*
2 Identity Theft Resource Center, "At Mid-Year, U.S. Data Breaches Increase at Record Pace," 18 July 2017, *https://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release*

3 Cooper, C.; "What Is the Cost of a Breach?" *CSO*, *https://www.csoonline.com/article/3234332/data-breach/what-is-the-cost-of-a-breach.html*
4 Noll, M.; "Data Breach Cost: When You Lose Your Customers," IT Security Central, 20 December 2017, *https://itsecuritycentral.teramind.co/2017/12/20/data-breach-cost-when-you-lose-your-customers/*
5 Telang, R.; S. Somanchi; "Security, Fraudulent Transactions and Customer Loyalty: A Field Study," Carnegie Mellon University, USA, November 2016, *https://www.ftc.gov/system/files/documents/public_comments/2016/10/00062-129181.pdf*
6 Thomas, K., *et al*; "Data Breaches, Phishing or Malware? Understanding the Risks of Stolen Credentials," Research at Google, 2017, *https://research.google.com/pubs/pub46437.html*
7 Kaspersky Lab, "What Is Malware and How to Defend Against It?" *https://usa.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it*
8 Ponemon Institute, "The SQL Injection Threat Study," *www.dbnetworks.com/form/Ponemon_SQL_Injection_Threat_Survey.htm*