FORUM: General Assembly I

ISSUE: Measures to Protect Electronic Devices from Security Breaches

STUDENT OFFICER: Michelle (Min Joo) Kim

POSITION: Deputy President of General Assembly I

Introduction

According to the 2017 Data Breach Year-End Review released by the Identity Theft Resource Center and CyberScout, the number of U.S data security breach incidents tracked in 2017 hit a new record high of 1,579 breaches, which is a drastic upturn of 44.7 percent increase over the high figures reported for 2016. Before getting into this topic, we need to thoroughly understand what security breach is.

Security Breach, also known as a security violation, is an incident that results in an unauthorized access of data, applications, services, networks, and devices by bypassing their underlying security mechanisms. It usually occurs when an individual or an application illegitimately enters a private, confidential and unauthorized logical IT perimeter. Generally, security breach is monitored, identified and mitigated by a software or hardware firewall. If an intrusion or violation is detected, the firewall issues a notification to the network or security administrator.

As we are entering an unlocked community that everyone can easily connect and communicate, a security breach is becoming a fundamental problem which people are directly facing in their daily life such as when they are surfing on the Internet, chatting on their phone, calling to their parents, or even taking photos with their friends. Thus, there is no doubt that not only the United Nation should take the responsibility to prevent this issue, but also for us to think of diverse kinds of ways to minimalize security breaches.

Background

In these days, a security breach could be divided into 5 areas: banking (credit and financial), business, government and military, educational, medical and healthcare. The disparity is mainly due to the lack of disclosure in baking, business, and education It is alarming to see how little is being made public about breaches in these sectors. That, of course, means that organizations would have to formally disclose a breach in order for it to be counted, which we know is not happening as often as it should. As Adam Levin, Chairman of ITRC report sponsor CyberScout noted back in 2016, "Many breaches continue to fly under the radar because many businesses aim to avoid the financial dislocation, liability, and loss of goodwill that comes with disclosure and notification."

While cybercriminals are certainly working overtime to infiltrate organizations, the rise in data breaches is partly due to a lack of cybersecurity awareness and knowledge among end users. Hacking, a category that includes phishing, ransomware, malware, and skimming, was the primary method of attack in 63% of the overall breaches.

Among all of the types of security breaches, hacking continues to rank the highest in the type of attack. Hacking incidents had a significant impact on the Business sector this year, with nearly 40 percent of the breached businesses identifying this type of attack as the cause for the breach. So, to surely prevent the issue of the security breach, make sure to prevent the problem of blocking hackers from entering and accessing peoples' information. Next, employees-driven factors, such as error, negligence, improper disposal and loss, were the root cause of 9% of breaches. Then, accidental online exposure of data following it by 7%. The industries with the highest number of data breach incidents were healthcare, which was 27%, then financial services 12%, education 11%, and government, which was 11%. In terms of the number of records lost, stolen or compromised, the most targeted sectors were government, financial services, and technology, followed by the number of 18%, 9.1%, and 16%.

From 2015 to 2017, 2017 has been the worst year that has the highest amount of security breaches happened. As an example, on December 20, 2016, E-Sports Entertainment Association (ESEA), one of the largest video gaming communities, issued a warning to players after discovering a vast breach. It revealed that 1,503,707 ESEA records had been added to its database and that leaked records included a great deal of private information such as registration date, city, state, last login, username, first and last name, email address, zip code, website URL, relate ID, etc. It has been a worse data breach since it accessed a lot of personal information to the social services including all the hackers on the cyberspace, resulting in the occurrence of cybercrimes. Another example would be university students' personal information have been uploaded to the cyberspace and to the entire internet, causing the security breach. According to The Oklahoma Daily and Washington State University storage unit in Olympia, WA, it claimed that approximately total 7,500 people were unintentionally exposed through incorrect privacy settings. They reported that there were more than 29,000 instances in which students' private information was made public to users through the email system. Sensitive information, including social security numbers, financial aid information, and grades, was also included.

Problems Raised

Personal Information and Data Leakage

The major problem of a security breach would be personal information and data leakage. As it is mentioned in the previous section, any information from different branch such as business, government, education, etc., is lacked if the security breach occurs. So, the biggest problem is definitely personal information and data leakage. Since security breaches increased enormously in 2017, in the first three-quarters of the year, 3 billion accounts leaked their personal information only because of security and data breaches.

Moreover, hundreds and thousands of people are suffering from personal information leakages after they experience security and data breaches. Using apps and mobile websites are normal for smartphone users, especially for 21st-century people. However, some applications that people trust are leaking their personal information, hacking their personal account to get their information and use it in negative ways, which could be called cybercrimes. More than 200 apps were found to be exposing sensitive consumer information, with close to 60 percent of the leaks coming from news, sports and shopping apps. More than a million social media users in the UK are believed to have been affected by the data breach, affected by data leakage, storing their personal information to all of the people who are using the Internet, including phone, tablet, and computer. Thus, the cause of security and data breach lead to personal information and data leakage to happen.

Weak Security Controls and Internal Threats

Weak security control is arguably straightforward of the common cause of data breaches. There is no surprise that this is among the common problem with it. There are three different groups that weaken security, including weak and stolen passwords, overly complex access permission, and not forcing security policy on including mobile devices, tablets, and computers.

First, weak and stolen passwords. This situation happens a lot in our life. While hacking and are often the top concern for protecting an organization's data, more often than not a weak or lost password is the vulnerability that is being exploited by the hacker. When a device such as laptops, tablets, cell phones, computers, and email is protected with weak passwords, hackers can easily break and come through into the system. This reveals subscription information, including personal and financial information, sensitive business data. Second, overly complex access permission. Incorrectly managing access to applications and different types of data can result in employees being able to view and transport information they don't need to do their jobs. Third, by not forcing security policy, starting from 2014, several issues that have been discussed include: lack of passwords, out-of-date software, non-encrypted wireless transmissions, Malware, App Vulnerabilities, and Physical Device theft or loss.

Internal threats can be broken down into two broad categories: accidental and intentional. Accidental happens by sending a document to the wrong recipient or not understanding the security protocols and procedures. According to the survey conducted by Verizon, this was the most common type of data breach resulting from a mental error. Another one called intentional breach can happen for several reasons. The biggest reasons could be an ex-employee or contractor who is disgruntled causes problems and getting around permissions and protocols that are in place.

International Actions

The United Nations Public Administration Network (UNPAN)

The United Nations Public Administration Network uses the UN E-Government Survey to provide new analysis and evidence to utilize better technologies to build sustainable and resilient societies. In other words, it also includes cybercrimes and security breaches. They use this E-Government to fill up the role of its governance, to bridge the gap between control requirements, technical issue, and business risks. After the establishment, the organizations undergoing change management become the easy targets of cybercriminals. As an example, since 2011, Bangladesh Bank was busy modernizing its payment and settlement system. The overall banking functions of the central bank had been brought under automation by implementing the banking application package. Usually, this transformation remains risk-prone, as hackers take this chance of transition.

Moreover, the organization made 2018 UN E-Government Survey available, the Sustainable Development Goals (SDGs), which is the 2030 agendas for all parts of government, parliaments, supreme audit institutions as well as non-state actors, based on the information provided by the 64 countries that presented voluntarily reviews of implementation of the SDGs. It includes all the information, of course, the policy about cybercrime (data and security breach). In addition, it also creates the World Public Sector Report 2018 (WPSR 2018), which examines how government, public institutions, and public administration can foster integrated approaches to the implementation of the 2030 agenda and the Sustainable Development Goals. The report thus aims to produce a comprehensive empirical analysis of policy integration for the SDGs at the national level, on how emerging initiatives aiming to enhance policy and institutional integration might lead to long-term success in achieving the SDGs, in different developmental and governance contexts. It includes how they approach the issue of creating the security breach policy and cybercrime policy.

Key Players

The Information Systems Security Association (ISSA)

The Information Systems Security Associations (ISSA) is a nonprofit, international organization, or information security professional and practitioners. Its primary goals are to promote management practices that ensure the confidentiality, integrity, and availability of information resources. Their members include all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial and government. By the use of the Information Systems Security Association, it is much easier to get help to learn the steps of preventing data and security breaches before it occurs. They organize international conferences meetings and seminars that offer educational programs, training and valuable networking opportunities, provide access to information through the ISSA Website as well as online E-Newsletters and in the monthly ISSA Journal, earn CPE credits by attending chapter meetings, and enhance professional stature and advance the profession by sharing your expertise as an event speaker or contributor ISSA Journal, etc. While they do such activities, they continue these activities to promote a secure digital world.

The International Information System Security Certification Consortium Inc (ISC)2

The International Information System Security Certification Consortium Inc (ISC)2 generally offers education and certification programs for information security professionals in all career stages related to cybersecurity including security breaches. With a membership of over 100,000 (ISC)2 provides access to a large network of industry professionals worldwide. By providing up-to-date information and education related to date and security breach, they support us to be well prepared before security breach happens. In addition, they also created programs and softwares that are used to stop breaches when people are facing breaches.

Possible Solutions

Preparation-Risk Assessment and Risk Evaluation

OTA analyzed reported breaches through Q3 2017 and found that 93% were avoidable, which is consistent with previous years' findings. 52% were the result of actual hacks, while 11% were due to lack of internal controls. Analysis reveals that these too are avoidable, by blocking fake messages and training users to recognize spear phishing attacks.

In addition to better processing of email, there are several other steps that can prevent or limit the impact of ransomware, which include updated system and security software as well as regular data backups Since security breach lacks a strong security program, we need to first consider developing an effective data security program. The first step is to identify foreseeable

internal and external threats to information attests in need of protection, also known as risk assessment or examine each major area of data operations. Companies, organizations, or countries should examine each major areas of data operations, including information storage, network security, regularity compliance, and employee training. While they examine each area, they should consider if the information system is ready to fend off a hacker's attack or not, if the company's employees have sufficient knowledge or not and if they have they awareness about data security attacks or not. In addition, I suggest the expert assistance to help to identify all potential risk to an information system; several companies specialize in cyber-crime response and computer forensics, and internal date security assessments may also be conducted on a regular basis while they do it.

After the risk assessment, once potential threats are identified, companies, organizations, or countries should evaluate the potential damage that could result, and assess the sufficiency of policies, procedures, and safeguards in place to guard against foreseeable threats such as hacker. As an example, if consumer information stored in computers and mobile data systems such as laptops is not encrypted, the likelihood of a threat materializing may be significant, and potential damage may be great, even huger than you thought. As a result, it may choose to implement a policy requiring data encryption, or some other procedures to safeguard such information.

Creating Security Policies

To prevent security breaches, we always need to remember that policy making is the fastest way to prevent breaches created by using technology. With implementing date security technologies, a country, company, or an organization may reduce risk by creating clear date security policies and enforcing them effectively. One important data security that everyone should strive to follow is removal of obsolete records. Many companies keep enormous stores of sensitive data that provide marginal business benefit but create huge risks that damage them. In more detail, retailers keep databases of highly sensitive credit card data even though it is unnecessary. Best security practices should require a thorough policy spelling out how such data should be stored and how frequently it should be deleted. Those security policies could include the cause of security breaches such as: lack of complete risk assessment, including internal third-party and cloud base systems and services, not promptly patching known, public vulnerabilities, misconfigured devices and servers, unencrypted data or poor encryption key management and safeguarding, use of end of life devices, operating system and application, employee errors and accidental disclosures (lost data, files, devices, computer, improper disposals), failure to block malicious email and users succumbing to business email compromise, etc.

In addition, Information Content Management could also be used to a security policy, to secure sensitive data, involving restriction of access rights and other security protections within individual documents. The system protects document content by requiring the document creator to encrypt the document and apply rules to determine who may access to the file. Moreover, it allows the creator to specify whether the document can be printed, copied, or forwarded to others.

Creating a Security-Conscious Workforce

Another way to reduce security breach would be creating a security-conscious workforce, which means that we should make an environment that everyone is trained to protect themselves from security breach. In other words, A workforce untrained in data security protection, and unscreened for compliance, may foster data security breaches. Organization, campaigns, academies, or countries can support citizens by providing programs to remind that information related to consumers such as social security numbers, financial information and health information can be misused. Moreover, teaching them how to act when security breach has occurred while they are in the process of using a database such as Social networks service that occurs information that includes their personal information. In addition, trainers should be trained to recognize spyware, viruses, and other hacking techniques, and to report such encounters to system administrators.

Glossary

Breach

An act of breaking or failing to observe a law, agreement, code or conduct. A gap in a wall, barrier, or defense, especially one made by an attacking army.

Security

The state of being free from damage or threat, the safety of a state or organization against criminal activity such as terrorism, theft, or espionage.

Cybersecurity (CS)

The state of being protected against the criminal or unauthorized use of electronic data, or the measured taken to achieve this.

Cybercrime

Criminal activities carried out by means of computers or the Internet.

Leakage

The accidental admission or escape of a fluid or gas through a hole or crack. Capital, income, which exits an economy or system rather than remaining within it. In economics, leakage refers to outflow from a circular flow of income model.

Database (DB)

A structured set of data held in a computer, especially one that is accessible in various ways. It is an organized collection of data, an electronic system that allows data to be easily accessed manipulated and updated. In other words. A database is used by an organization as a method of storing, managing and retrieving information. Modern databases are managed using a database management system (DBMS)

Sources

Burgess, Matt. “The Biggest Hacks and Data Breaches of 2018 (so Far).” Wired, Conde Nast Traveller, 9 July 2018, www.wired.co.uk/article/hacks-data-breaches-in-2018Haiti Daitch. “2017 Data Breach

ID Experts. “Made-to-Fit Services for Breaches Large and Small.” ID Experts, ID Experts, www2.idexpertscorp.com/products-services/breach-response-service/.

McGoogan, Cara. “WhatsApp Security Problem Leaves Millions of Users Exposed to Hackers.” The Telegraph, The Telegraph, 16 Mar. 2017, www.telegraph.co.uk/technology/2017/03/16/whatsapp-security-problem-leaves-millions-users-exposed-hackers/

Rayome, Alsion Denisxo. “Report: Negligent Employees Are No. 1 Cause of Cybersecurity Breaches at SMBs.” TechRepublic, TechRepublic, 19 Sept. 2017, 6:00, www.techrepublic.com/article/report-negligent-employees-are-no-1-cause-of-cybersecurity-breaches-at-smbs/.

The Worst SO Far.” Identity Force, Data Breach & Technology, Personal, 14 Dec. 2017, www.identityforce.com/blog/2017-data-breaches.

Travis LeBlanc, Boies Schiller Flexner LLP, Jon R. Knight, Boies Schiller Flexner LLP. “A Wake-Up Call: Data Breach Standing Is Getting Easier.” CyberSecurity, Cslawreport, 17 Jan. 2018, www.bsfllp.com/images/content/2/9/v2/2995/2018-01-17-Cyber-Security-Wake-Up-Call-Data-Breach-Standing-Is.pdf.

“Security Breach Examples and Practices to Avoid Them.” UC SANTA CRUZ, Ucsc.edu, Nov. 2015, its.ucsc.edu/security/breaches.html.

United States, Iss. “Security That Delivers Peace of Mind.” ISS UNITED STATES, www.us.issworld.com/our-services/security.

https://vertassets.blob.core.windows.net/image/e0c1328a/e0c1328a-3281-4f40-98a7-015ea3dffe90/internet_lock.jpg

https://www.beencrypted.com/wp-content/uploads/security-breach.jpg