Scholarly Research Journal for Interdisciplinary Studies,
Online ISSN 2278-8808, SJIF 2019 = 6.380, www.srjis.com
PEER REVIEWED & REFEREED JOURNAL, JAN-FEB, 2021, VOL- 8/63

IMPORTANCE OF CYBERSECURITY

Jasraj Singh Johal
Jaishree Periwal High School

Paper Received On: 21 FEB 2021
Peer Reviewed On: 28 FEB 2021
Published On: 1 MAR 2021
Content Originality & Unique: 99%

Introduction

Cybersecurity means protecting data, networks, programs and other information from unauthorized or unattended access, destruction or change. In today's world, cybersecurity is very important because of some security threats and cyber-attacks. For data protection, many companies develop software. This software protects the data. Cybersecurity is important because not only it helps to secure information but also our system from virus attack. After the U.S.A. and China, India has the highest number of internet users. It is also important because it encompasses everything that pertains to protecting our sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems from theft and damage attempted by criminals and adversaries.

Cybersecurity risk is increasing, driven by global connectivity and usage of cloud services, like Amazon Web Services, to store sensitive data and personal information. Widespread poor configuration of cloud services paired with increasingly sophisticated cyber criminals means the risk that your organization suffers from a successful cyber attack or data breach is on the rise. Gone are the days of simple firewalls and antivirus software being your sole security measures. Business leaders can no longer leave information security to cybersecurity professionals. Cyber threats can come from any level of your organization. You must educate your staff about simple social engineering scams like phishing and more sophisticated cybersecurity attacks like ransomware attacks (think WannaCry) or other malware designed to steal intellectual property or personal data.

GDPR and other laws mean that cybersecurity is no longer something businesses of any size can ignore. Security incidents regularly affect businesses of all sizes and often make the front page causing irreversible reputational damage to the companies involved. If you are not yet worried about cybersecurity, you should be.

What is Cybersecurity?

Cybersecurity is the state or process of protecting and recovering computer systems, networks, devices, and programs from any type of cyber attack. Cyber attacks are an increasingly sophisticated and evolving danger to your sensitive data, as attackers employ new methods powered by social engineering and artificial intelligence to circumvent traditional security controls. The fact of the matter is the world is increasingly reliant on technology and this reliance will continue as we introduce the next generation of smart Internet-enabled devices that have access to our networks via Bluetooth and Wi-Fi.

The Importance of Cybersecurity

Cybersecurity's importance is on the rise. Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow. Data leaks that could result in identity theft are now publicly posted on social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive.

The fact of the matter is whether you are an individual, small business or large multinational, you rely on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones and the Internet of Things (IoT) and we have a myriad of cybersecurity threats that didn't exist a few decades ago. We need to understand the difference between cybersecurity and information security, even though the skill-sets are becoming more similar.

Governments around the world are bringing more attention to cybercrimes. GDPR is a great example. It has increased the reputational damage of data breaches by forcing all organizations that operate in the EU to:

- Communicate data breaches.
- Appoint a data-protection officer.
- Require user consent to process information.
- Anonymize data for privacy.

The trend towards public disclosure is not limited to Europe. While there are no national laws overseeing data breach disclosure in the United States, there are data breach laws in all 50 states. Commonalities include:

- The requirement to notify those affected as soon as possible.
- Let the government know as soon as possible.
- Pay some sort of fine.

California was the first state to regulate data breach disclosures in 2003, requiring persons or businesses to notify those affected "without reasonable delay" and "immediately following discovery". Victims can sue for up to $750 and companies can be fined up to $7,500 per victim. This has driven standards boards like the National Institute of Standards and Technology (NIST) to release frameworks to help organizations understand their security risks, improve cybersecurity measures and prevent cyber attacks.

Why is Cybercrime increasing?

Information theft is the most expensive and fastest growing segment of cybercrime. Largely driven by the increasing exposure of identity information to the web via cloud services. But it is not the only target. Industrial controls that manage power grids and other infrastructure can be disrupted or destroyed. And identity theft isn't the only goal, cyber attacks may aim to compromise data integrity (destroy or change data) to breed distrust in an organization or government. Cybercriminals are becoming more sophisticated, changing what they target, how they affect organizations and their methods of attack for different security systems. Social engineering remains the easiest form of cyber attack with ransomware, phishing, and spyware being the easiest form of entry. Third-party and fourth-party vendors who process your data and have poor cybersecurity practices are another common attack vector, making vendor risk management and third-party risk management all the more important.

According to the Ninth Annual Cost of Cybercrime Study from Accenture and the Ponemon Institute, the average cost of cybercrime for an organization has increased by $1.4 million over the last year to $13.0 million and the average number of data breaches rose by 11 percent to 145. Information risk management has never been more important.

Data breaches can involve financial information like credit card numbers or bank account details, protected health information (PHI), personally identifiable information (PII), trade secrets, intellectual property and other targets of industrial espionage. Other terms

for data breaches include unintentional information disclosure, data leak, cloud leak, information leakage or a data spill.

Other factors driving the growth in cybercrime include:

- The distributed nature of the Internet.
- The ability for cybercriminals to attack targets outside their jurisdiction making policing extremely difficult.
- Increasing profitability and ease of commerce on the dark web.
- The proliferation of mobile devices and the Internet of Things.

What is the Impact of Cybercrime?

A lack of focus on cybersecurity can damage your business in a range of ways including:

- Economic Costs: Theft of intellectual property, corporate information, disruption in trading and the cost of repairing damaged systems
- Reputational Costs: Loss of consumer trust, loss of current and future customers to competitors and poor media coverage
- Regulatory Costs: GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cybercrimes

All businesses, regardless of the size, must ensure all staff understand cybersecurity threats and how to mitigate them. This should include regular training and a framework to work with to that aims to reduce the risk of data leaks or data breaches. Given the nature of cybercrime and how difficult it can be to detect, it is difficult to understand the direct and indirect costs of many security breaches. This doesn't mean the reputational damage of even a small data breach or other security event is not large. If anything, consumers expect increasingly sophisticated cybersecurity measures as time goes on.

How to protect your organization against cybercrime

There are three simple steps you can take to increase security and reduce risk of cybercrime:

1. Educate all levels of your organization about the risks of social engineering and common social engineering scams like phishing emails and typo squatting.
2. Invest in tools that limit information loss, monitor your third-party risk and fourth-party vendor risk and continuously scan for data exposure and leak credentials.
3. Use technology to reduce costs like automatically sending out vendor assessment questionnaires as part of an overall cyber security risk assessment strategy.

Companies should no longer be asking why is cybersecurity important, but how can I ensure my organization's cybersecurity practices are sufficient to comply with GDPR and other regulation and to protect my business against sophisticated cyber attacks.

Examples of damages to companies affected by cyber attacks and data breaches

The amount of cyber attacks and data breaches in the recent years is staggering and it's easy to produce a laundry list of companies who are household names that have been affected.

Here are a few examples:

- Equifax: The Equifax cybercrime identity theft event affected approximately 145.5 million U.S. consumers along with 400,000-44 million British residents and 19,000 Canadian residents. Equifax shares dropped 13% in early trading the day after the breach and numerous lawsuits were filed against Equifax as a result of the breach. Not to mention the reputational damage that Equifax suffered. On July 22 2019, Equifax agreed to a settlement with the FTC which included a $300 million fund for victim compensation, $175m for states and territories in the agreement and $100 million in fines.
- eBay: Between February and March 2014, eBay was the victim of a breach of encrypted passwords, which resulted in asking all of its 145 million users to reset their password. Attackers used a small set of employee credentials to access this trove of user data. The stolen information included encrypted passwords and other personal information, including names, e-mail addresses, physical addresses, phone numbers and dates of birth. The breach was disclosed in May 2014, after a month-long investigation by eBay.
- Adult Friend Finder: In October 2016, hackers collected 20 years of data on six databases that included names, email addresses and passwords for The FriendFinder Network. The FriendFinder Network includes websites like Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com. Most of the passwords were protected only by the weak SHA-1 hashing algorithm, which meant that 99% of them had been cracked by the time LeakedSource.com published its analysis of the entire data set on November 14.
- Yahoo: Yahoo disclosed that a breach in August 2013 by a group of hackers had compromised 1 billion accounts. In this instance, security questions and answers were also compromised, increasing the risk of identity theft. The breach was first reported

by Yahoo on December 14, 2016, and forced all affected users to change passwords, and to reenter any unencrypted security questions and answers to make them encrypted in the future. However, by October of 2017, Yahoo changed the estimate to 3 billion user accounts. An investigation revealed that users' passwords in clear text, payment card data and bank information were not stolen. Nonetheless, this remains one of the largest data breaches of this type in history.

While these are a few examples of high profile data breaches, it's important to remember that there are even more that never made it to the front page.

Cyber Crime

Use of cyberspace, i.e. computer, internet, cellphone, other technical devices, etc., to commit a crime by an individual or organized group is called cyber-crime. Cyber attackers use numerous software and codes in cyberspace to commit cybercrime. They exploit the weaknesses in the software and hardware design through the use of malware. Hacking is a common way of piercing the defenses of protected computer systems and interfering with their functioning. Identity theft is also common. Cybercrimes may occur directly i.e, targeting the computers directly by spreading computer viruses. Other forms include Denial of Service (DoS) attack. It is an attempt to make a machine or network resource unavailable to its intended users. It suspends services of a host connected to the internet which may be temporary or permanent.

Malware is a software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It usually appears in the form of code, scripts, active content, and other software. 'Malware' refers to a variety of forms of hostile or intrusive software, for example, Trojan Horses, rootkits, worms, adware, etc.

Another way of committing cybercrime is independent of the Computer Network or Device. It includes Economic frauds. It is done to destabilize the economy of a country, attack on banking security and transaction system, extract money through fraud, acquisition of credit/debit card data, financial theft, etc.

Hinder the operations of a website or service through data alteration, data destruction. Others include using obscene content to humiliate girls and harm their reputation, spreading pornography, threatening e-mail, assuming a fake identity, virtual impersonation. Nowadays misuse of social media in creating intolerance, instigating communal violence and inciting riots is happening a lot.

Cyber Warfare

Snowden revelations have shown that Cyberspace could become the theatre of warfare in the 21st century. Future wars will not be like traditional wars which are fought on land, water or air. When any state initiates the use of internet-based invisible force as an instrument of state policy to fight against another nation, it is called cyberwar'.

It includes hacking of vital information, important webpages, strategic controls, and intelligence. In December 2014 the cyberattack a six-month-long cyberattack on the German parliament for which the Sofacy Group is suspected. Another example 2008 cyberattack on US Military computers. Since these cyber-attacks, the issue of cyber warfare has assumed urgency in the global media.

Inexpensive Cybersecurity Measures

- The simplest thing you can do to up your security and rest easy at night knowing your data is safe is to change your passwords.
- You should use a password manager tool like LastPass, Dashlane, or Sticky Password to keep track of everything for you. These applications help you to use unique, secure passwords for every site you need while also keeping track of all of them for you.
- An easy way for an attacker to gain access to your network is to use old credentials that have fallen by the wayside. Hence delete unused accounts.
- Enabling two-factor authentication to add some extra security to your logins. An extra layer of security that makes it harder for an attacker to get into your accounts.
- Keep your Softwares up to date.

Conclusion

Today due to high internet penetration, cybersecurity is one of the biggest need of the world as cybersecurity threats are very dangerous to the country's security. Not only the government but also the citizens should spread awareness among the people to always update your system and network security settings and to the use proper anti-virus so that your system and network security settings stay virus and malware-free.

References.

An Examination of the Cybersecurity Labor Market. (n.d.). Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

Applications Now Available for City Colleges of Chicago's New Cyber Security "Boot Camp". (2017, March 18). Retrieved from http://www.ccc.edu/news/Pages/Applications-Now-Available-for-City-Colleges-of-Chicagos-New-Cyber-Security-Boot-Camp-.aspx

Apprenticeship USA Investments. (2017, June 22). Retrieved

from https://www.dol.gov/featured/apprenticeship/grants

Assante, M., Tobey, D. (2011, February 4). Enhancing the Cybersecurity Workforce. Retrieved from http://ieeexplore.ieee.org/document/5708280/

Assessment Act. Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/2007/text

ATE Centers. (n.d.). Retrieved from http://www.atecenters.org/

ATE Centers and National Science Foundation. (n.d.). ATE Centers Impact Report. Retrieved from http://www.atecenters.org/wp-content/uploads/PDF/ATEIMPACT_2016-17.pdf

ATE Centers and National Science Foundation. (n.d.). ATE Programs and Overview. Retrieved from http://www.atecenters.org/wp-content/uploads/2016/07/ATE_Overview_2016.pdf

AUSTRALIA'S CYBER SECURITY STRATEGY Enabling innovation, growth & prosperity [PDF]. (n.d.). Retrieved from https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

Baltimore Cyber Range and Cyber bit Open New Cybersecurity Training and Simulation Center. (2017, August 3). Retrieved from https://www.cyberbit.com

Bessen, J. (2014, August 25). Employers Aren't Just Whining – the "Skills Gap" is Real. Harvard Business Review. Retrieved from https://hbr.org/2014/08/employers-arent-just-whining-the-skills-gap-is-real

Best in Class Strategies for Entry-Level Employee Retention Prepared for 100K [PDF]. (2016, October). FSG Reimagining Social Change. Retrieved from https://www.100kopportunities.org/2016/10/14/best-in-class-strategies-for-entry-level-employee-retention/

Best Places to Work for Cyber Ninjas. (2017, May). Retrieved from https://www.sans.org/best-places-to-work-for-cyber-ninjas?ref=195285

Bojanova, I., Vaulx, F., Zettsu, K., Simmon, E., Sowe, S. (2016, January 21). Cyber-Physical-Human Systems Putting People in the Loop. IT Professional. Retrieved from http://ieeexplore.ieee.org/document/7389271/

Burning Glass Technologies. (2015). Job Market Intelligence: Cybersecurity Jobs, 2015 [PDF]. Retrieved from http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf