CYBER SCEURITY ASSESMENT IN Any Organization

Dr. Preeti Bala 1, Ms. Shweta singh2

Abstract :

This paper describes about cyber security and its Impact on any organization, we are almost open when we are talk about Internet and we would online ,we should remember "OUR DATA IS OUR POWER" but how an organization can take some safety measures regarding the data and make secure Data exchange through different platform . Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many.

Key word---Cyber security, Organization, Threats, Risk.

Introduction and overview of the cyber security risks to organizations

Cyber security is the collection of tools, guidelines, risk management approaches, and technologies that can be used to protect IT systems and cyber environments from external attacks. It is based on the protection of the confidentiality, integrity and availability of an information system. Do to the increase in internet usage and continued security breaches, in the last fifteen years cyber security has been more and more prevalent. In Cyber Security there are legal, human, technical and organizational elements capable of analyzing the vulnerable points of a system, as well as the threats and the associated risks. Cyber security is necessary to operate any business efficiently, and it is also critical for protecting customers' information. Following IT best practices means not only using the latest technology at your company; it's about staying ahead of risks and disasters that might bring a company to a screeching halt.

One of the most problematic aspects of cybersecurity is the constantly evolving nature of security risks. Cyber threats continue to expand, with hackers targeting not only large businesses but also small businesses and non profit organizations. According to the National Cyber Security Alliance, research found small and medium sized organizations that incur cyber attacks are likely to be out of business within six months of an attack. And of course it's not just money that's at stake. Public trust, employee morale and customer retention can be considered additional ramifications of falling victim to cyber attacks.

Small businesses generally have less resources when it comes to data protection. These can have great products and services but do not understand the importance of cyber security. It can be truly damaging when they suffer a hack or misconfigured database which exposes sensitive information online. Ensuring cybersecurity requires the coordination of efforts throughout an information system, which includes: • Information security • Application security • Network security • Operational security • Disaster recovery/business continuity planning • End-user education

Securing a cyber infrastructure needs to have a defence in depth approach composed of different layers of security and not only an perimeter level of security.

The most common cyber attacks that businesses experience --------------------

Regardless of the type of business, the most common cyber attacks include:

Ransomware - This type of malware does not allow users to access their system or personal data and demands ransom payment in order to regain access. Ransomware attacks are typically spread through phishing attacks, email attachments, infected websites and inadvertent malware downloads.

Phishing - These attacks attempt to trick a person into clicking a link within a fake email or website, so that cyber criminals can access a computer or network. A successful phishing cyberattack can allow attackers to access passwords, private data, credit card information, social security numbers and financial records. The weakest link in many organizations is people, criminals are aware of this and that's why phishing is one of the most popular cyberthreats businesses have to face.

Malware - Malware, also known as malicious software, can inflict damage on networks and/or gain access to that network and digital devices attached to it. This is one of the biggest threats to small and medium sized businesses. Usually, a malware successfully breaches a system security due to humans that download an infected file by clicking on a bad link which was placed with nefarious intent by cyber attackers.

Social Engineering - Social engineering is about manipulating people to divulge private information or click an infected link. Infected links are disguised by including them in emails, unscrupulous websites, and even legitimate websites that have been infected themselves.

DDoS - A distributed denial of service (DDoS) attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server. Typically the target is businesses, but personal computers can be used en masse to execute a DDoS cyberattack without the innocent individual even knowing it.

Website Hijacking / URL Poisoning - This is when a website is compromised by hackers who have set it up to download malware to any device that connects to it. These attacks are quite sophisticated and could be leveraging crosssite scripting (XSS), URL poisoning, or other.

User-Initiated Website Visit - When a user visits a website and inadvertently downloads malware it infects his endpoint system. Sometimes it can also affects the network to which the device is connected. This may happen even on known safe sites in a variety of situations such as website hijacking or URL poisoning.

Email Initiated Infections

- These attacks occur when a person clicks on an email attachment or some link in an email, either in error or thinking they are truly clicking on a legitimate link/attachment. Some legitimate looking emails may contain an attractive and convincing link that either collects personal data, downloads malware, or deploys a small “dropper” file which calls back to the command server for more instructions.

Insider breaches

Insider breaches are those caused by employees or leaders within an organization. These are among the hardest data breaches to detect and often the costliest ones. Around two-thirds of all data records compromised in 2017 were

actually the result of inadvertent insiders, according to the "2018 IBM X-Force Threat Intelligence Index". Insider threats are the cause of 60% of cyberattacks.

Organizations generally focus significant resources on the reduction of external threat actors, but insider risks are likely to pose even a greater financial threat to the business. According to the Ponemon Institute's "2018 Cost of Insider Threats" report, in 2017 the average cost of insider-caused incidents was $8.76 million, which is more than twice the $3.86 million global average cost of all breaches occurred during the same year.

We can list 5 types of insider threats: ---------------------

1. Non-responders

A significant percentage of the employees is made up of non-responders to awareness training exercises. These users perhaps do not intend to behave negligently, but they're among the riskiest members for businesses since their behaviours can fit consistent patterns.

2. Inadvertent Insiders

Negligence is the most popular form of insider threat, and is also the single most expensive category of employee risk. The insider threats might usually exhibit secure behaviour and comply with policy, but they cause breaches due to isolated errors. Basic misjudgment such as storing intellectual property on insecure personal devices or falling for phishing schemes caused two-thirds of breached records in 2017, according to the X-Force report.

3. **Insider Collusion**

Insider collaboration with external threat actors is probably the rarest form of criminal insider risk, but it is still a relevant threat due to the increased frequency of attempts by professional cybercriminals to recruit employees in the dark web.

4. Persistent Malicious Insiders

Very often, criminal insiders exfiltrate data or commit other malicious acts in order to obtain financial rewards or other personal gain. A Gartner study on criminal insider threats found that around 62% of insiders with malicious intent can be categorized as "second streamers" (people seeking a supplemental income). So-called "second streamers" could remain undetected to maximize the personal benefits of data theft. These individuals may exfiltrate data slowly to personal accounts to avoid detection, and not complete large data exports which could raise flags in common network monitoring tools.

5. Disgruntled Employees

Disgruntled employees who commit deliberate sabotage or intellectual property theft are among the costliest risks to a business. The Gartner analysis of criminal insiders reported 29% of employees stole information after being fired or quitting for future gains, while 9% were just motivated by simple sabotage.

Critical assessment of the organization's vulnerabilities -------------------------

We have completed a deep analysis of the client's organization in terms of cyber security, and we found the following vulnerabilities:

Generally speaking, security passwords are quite weak and old. Users should change their passwords every 2 months.

- Operation systems not updated. It is important to run updates whenever these are available, so that computers can run smoothly and more secure.

- Wi-Fi available for employees' personal devices. To establish more security in the organization, only the authorized business computers should be able to connect to the network. External devices may cause risks and threats to the entire system. - Stickers and notes on desk. Lots of these papers include personal passwords/codes, which

can be potentially stolen by someone within the company. - Mobile devices are used inside the working office. The devices can be used to capture data displayed on the computer or to audio-record sensitive data in a conversation. - Internet is often slow due to the fact that some employees watch videos/movies with the computers. Websites like Youtube, Vimeo or Dailymotion should not be accessible.

Social media such as Facebook and Instagram might be blocked, as well as various online games. These can be a big distraction to the users. - Possibility to use any external hardware such as pen drives with the organization's computers. This can raise the level of risks and threats since the hardware might contain malwares.

Physical authorization key for each employee, in addition to personal security passwords, would establish more security in the whole system.

The organization should do regular security risk assessments internally. This has to be a joint effort between the IT staff and business unit leaders. Security assessments are periodic exercises that test the organization's security preparedness. These include checks for vulnerabilities in the IT systems and business processes, and also recommending steps to reduce the risk of future attacks. Security assessments can be also useful to keep systems and policies up to date.

If the IT security strategy simply relies on installing an anti-virus software with no further checks or training, the organization is vulnerable to an attack. You may have the best security software installed in your company, but an aggressive hacker or an inadvertent employee is enough to bring the whole system down.

To mitigate the risk of a cyberattack, it is important to build a culture of information security within the organization. This can be done by regularly monitoring the security posture through security assessments.

Security assessments help a company identify risky behaviour of employees and take actions to better train them, in addition to testing the IT systems for vulnerabilities.

Affordability of security assessments for small businesses

Many small businesses never conduct security assessments, either because they believe it to be too expensive, or because they are not really familiar with the process for carrying an assessment out. To reduce costs, businesses might conduct security assessments internally using in-house resources. Even then, seeking a third party specialist to assess a security posture on a less frequent basis is always a good practice.

A security assessment should broadly include the following:

Security review: A collaborative process that includes the identification of security issues and their level of risk, and also the preparation of a plan to mitigate these risks.

Security testing: The process of finding vulnerabilities in software applications or processes. Security testing can help you evaluate and test the security strength of your software, hardware, networks, and other IT systems.

A security test can be conducted along with the security review process, or independently.

Now let's look at a few steps you might take to test the security posture of your IT organization:

Cyberattack simulation tests. Authorized simulation attacks on a computer system help identify weaknesses and strengths of an existing system. For example, a phishing simulation tool might help identify risky users behaviour while training them to spot scam emails.

Security scanning. Use security software to run a complete scan of networks, applications, and devices at least every 30 days to identify risks and threats. Many security software provides real-time and automatic scanning features. In case you don't have security software in place, the implementation of such a system should be a priority.

Vulnerability scanning. It is often difficult to spot vulnerabilities in a system that you created or that you have been using for months or years. A vulnerability assessment is a set of procedures that help you identify vulnerabilities and rate them based on the severity of damage they can potentially cause.

For businesses aiming to reduce their security risk, a Vulnerability Assessment is certainly a good choice. It provides a complete assessment of software and hardware assets, identifying vulnerabilities, giving an intuitive risk score, and solutions to remediate the vulnerabilities. A regular assessment program always helps organizations to manage risks in the face of an ever-evolving threat environment, identifying and scoring vulnerabilities so that attackers do not meet organizations unprepared.

A Vulnerability Assessment might be done prior to product deployment or after - the earlier, the better, so that eventual holes in the system can be identified and fixed, before attackers find any opportunity to exploit or damage the system.

Training your employees

Creating an effective cyber security training for your employees starts at the top, is meaningful, just-in-time, and ongoing.

Cyber security training should not be just a phrase your employees throw around on their way to the conference room. The security and safety of your business data and your customers data depend on what your employees have acknowledged.

Survey your employees to identify weaknesses. As discussed in a previous section, human error is a major cause of cyber attacks. Interviewing your employees is useful to identify risky behaviour and correct bad practices.

At the end of their training, there are four essential things your employees should be aware of, understand, or be able to do:

1. How to update passwords regularly and responsibly. Passwords are a major issue for most employees. A 2012 analysis of passwords stolen by hackers revealed the most common passwords. The number one password of 2012 is “Password,” followed closely by “12345.”

3. How to identify various phishing attempts. Almost 91% of cyber attacks start with an email. In 2014, phishing attacks cost businesses all over the world £3.5 billion. Employees should know how to identify phishing attempts through email, text, and voicemail. It is very important to train your employees to look for unrecognized links, unidentifiable names, or thinly veiled threats, forwarding them to the IT department for investigation.

4. How to avoid downloading malicious software. Employees also need to know how to spot malicious software. One little download could infect an entire system within few minutes, burrowing deeply into sensitive files.

Trainings are extremely important to ensure business continuity and secure your assets. Cyber security education is a critical tool for business faced with an increasing volume of constantly evolving threats. IT Security staff must be skilled in the advanced techniques that form a key component of effective organization threat management and mitigation strategies. Training your team with the most up-to-date knowledge will help defend your business against the most sophisticated attacks.

CONCLUSION-

It takes the involvement of every staff from low level to high level in the organization to reinforce defence against the cyber threats. This kind of involvement will create a reasonable advantage during the worst-case scenario. However, this set of action taken by our organization preserve stakeholder value and accomplish high level in our performance wise.

References:

[1]IT Governance, *What is Cyber Security*, Retrieved from https://www.itgovernance.co.uk/what-is-cybersecurity

[2]IT Governance, *Cyber Security Risk Management*, Retrieved from, https://www.itgovernance.co.uk/cyber-security-risk-management

[3]Small Business Administration, *Protection against Ransom ware*., Retrieved from https://www.sba.gov/managing-business/cybersecurity/protect-against-ransomware.

[4]Consultancy United Kingdom, *Five reasons cyber security is more important than ever*., Retrieved from https://www.consultancy.uk/news/18435/five-reasons-cyber-security-is-more-important-than-ever

[5]Cyber security precaution, *Human Resource and Service Administration*., Retrieved from https://www.hrsa.gov/hr/cybersecurity-precautions.html

[6]Heimdal Security, *10 Critical corporate cyber security risks a data driven list*. Retrieved from https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/

[7]Cyber security skills Immediate Impact Fund, Retrieved from https://www.gov.uk/government/publications/cyber-security-skills-immediate-impact-fund