k

by S J

Submission date: 05-May-2021 07:51PM (UTC-0500)
Submission ID: 1579131115
File name: Implementing_Effective_Cybersecurity_programs.edited.docx (13.74K)
Word count: 718
Character count: 4351

Effective Cybersecurity Programs for Employees and Contractors

Name

Institution

Course

Instructor

Date

Effective Cybersecurity Programs for Employees and Contractors

Employees are the greatest asset a company can have, but they also present some of the notable risks associated with cybersecurity. Over the last decade, some of the notable cybersecurity breaches, whether accidental or intentional, have all been associated with employees. Previously, companies trained their workers annually on the best practices for cybersecurity, thinking that was enough. Organizations must adopt people patching strategies. Similar to updating the software and hardware existing systems. Businesses need to progressively update their employees and their contractors regarding the latest security threats and vulnerabilities and train them to avoid them.

According to Schreider (2019), employees are the single most important asset an organization can have, hence the importance of ensuring they are updated regarding the cybersecurity issues that are recognized. For instance, when a user clicks on a malicious email that infects a company's network with a malicious virus, people will be quick to point an accusing finger, ignoring that the organization was already under attack when such an email was sent and opened. It also means that any other cybersecurity strategy adopted by the company has failed. In this regard, it is important for entities to properly update their employees and contractors regarding emerging threats on cybersecurity and what can be done to counter these issues (Schreider, 2019). The best form of training involves live simulation. The stakeholders become victims of cyberattacks orchestrated by the organization's information technology department, and employees get to witness first-hand new emerging issues in cybersecurity.

Data protection is key for any organization to ensure the security of its information technology systems is protected. Lefever (2019) argues that employees and contractors must not share sensitive information with unauthorized persons. For instance, when an employee shares a

photo that shows a whiteboard in the background or a computer screen behind them, they could accidentally reveal information that hackers could use to gain access into an entity's systems. According to Lefever (2019), companies can adopt policies covering issues touching on the destruction of data that is no longer useful. The steps are taken when an individual comes across malicious ransomware and email.

In addition to installing anti-malware programs like the common antivirus, employees and contractors should avoid clicking pop-ups and unknown links. Phishers try to rick system users into clicking links and pop-ups that can lead to security breaches. Intrusion detection software may be successful in blocking malicious pop-ups and other programs sent by phishers, but they have proved to be ineffective in the past. Also, Yıldırım & Mackie (2019) suggest that companies must develop a policy regarding the types of passwords employees and contractors are allowed to use. Some individuals use simple passwords like their birth dates, their names, and their children or pets. These simple passwords are easy to figure out, exposing entities to cybersecurity vulnerabilities (Yıldırım & Mackie, 2019). A good password policy ensures that letters, numbers, capitals, uppercase, lowercase, and special characters are used, making it hard for someone with malicious intentions to figure out. In this manner, the company's systems are assured of some level of security. In addition to that, organizations can also adopt multi-factor authentication, where those allowed to access their system follow multiple authentication procedures. For instance, system entry requirements can include passwords, biometric details, and voice recognition. A combined multi-access approach ensures it is difficult for unauthorized personnel to access a company’s network or systems.

To sum it up, whereas the cybersecurity strategies discussed in this paper can help achieve system security, there is no perfect solution that fits all the network security

requirements of any organization. That is why cyber-attacks are still happening daily. However, the most important thing is for businesses to ensure that their employees and contractors do not make it easy for malicious individuals trying to break into the networks and systems of an organization. The strategies discussed in this paper, if properly adopted, can offer significant security to a company's information technology network.

References

Lefever, D. (2019, March 22). Building an effective cybersecurity program. Forbes. Https://Www.Forbes.Com/Sites/Forbestechcouncil/2019/03/22/Building-An-Effective-Cybersecurity-Program/?Sh=2b0b096a185d

Schreider, T. (2019). *Building an Effective Cybersecurity Program*. Rothstein Publishing.

Yıldırım, M., & Mackie, I. (2019). Encouraging Users to Improve Password Security and Memorability. *International Journal of Information Security*, *18*(6), 741-759.

k

ORIGINALITY REPORT

1%	0%	0%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Roehampton University Student Paper	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		