Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

A Strategy to Get Started with a Cybersecurity Program: Cybersecurity Awareness Training

Patrick Rost prost@dopkins.com

This is the second in Dopkins series of Cybersecurity posts. These blogs will introduce various topics, related terms, importance of reviewing the topic and hopefully raise some questions you should be asking.

Read our last issue on Data Backups

Published November 25, 2020 – In this month's issue, we will be discussing the vital role Cybersecurity Awareness Training plays in your business strategy. Cybersecurity Awareness Training is a way to ensure that all employees in an organization are knowledgeable of the cybersecurity threats they face every day, including:

- How many employees in your organization would be able to recognize an email that is a phishing attempt, trying to get them to click a link that would compromise your entire system?
- How many would even be aware of what a phishing attempt is?

Maybe while answering the previous questions you realized that you don't understand the term "phishing" or you do recognize it but are unsure of the ways to identify a phishing attempt. Before we move forward let's define **phishing** as "the social engineering attack that utilizes email or SMS [text message] to scam individuals into divulging sensitive information or clicking on malicious links." This is just one example of information that all employees need to know to be able to effectively keep their systems guarded from attacks. Some other examples are password best practices, working from home, public Wi-Fi security, etc. There is an ever growing and changing list of what employees need to be knowledgeable about in the IT and cybersecurity world.

It is important to continually train employees due to this consistent change. Employees who sit through a one-time training may not effectively learn everything; it is a lot to take in all at once. Then, what they did learn may not be relevant after a couple years, or even months. A recurring training and testing program will allow employees to learn pieces at a time, reinforce what they learned at a later date, and then be updated on new technology, terms, and recommendations.

So, what happens when someone interacts with that phish attempt? This will vary depending on the goal of the threat actor. But, in every instance it will open the door for an unauthorized person to have some level of access to your system. Ransomware is one of the most frequent attacks. Ransomware was discussed in October 2020 blog about **backups**. In that blog we mention how having a good backup will allow you to restore your data after an attack. While this still remains true, a new threat has emerged in early 2020. These individuals who develop the ransomware software now snoop around your system before starting the encryption process. They will transfer your data out of your network and then threaten to release it to the public if you do not pay them. Even if you do pay there is no guarantee they do not release the data and destroy the copies they have. Once you are compromised

there is no real way to recover from this attack. This change in how ransomware is functioning is what is driving the increased requirement to disclose ransomware attacks as a breach.

At this point you might be wondering about the security of your technology and thinking that your firewall, patching, endpoint protection, etc. is enough to stop anything thrown your way. However, these attacks are designed to bypass these controls and count on the human error being the weak point in your network's defense. Consider the following:

- A **2018 survey conducted by Sophos Security** found that "more than 77 percent of those impacted by ransomware were running up to date endpoint protection, confirming that traditional endpoint security is no longer enough to protect against today's ransomware attacks."
- In addition, **SC Magazine recently covered research** published in **the Journal of Computer Information Systems** that states "Security safeguards alone will not protect a company from phishing scams. Organizations and individuals substantially invest in security safeguards to protect the integrity, availability, and confidentiality of information assets. However, our study supports the findings of recent studies that these safeguards are not adequate to provide the ultimate protection of sensitive and confidential information."
- This is even more important to address now because cybersecurity firm **CrowdStrike released a study earlier** this year which found threat activity throughout its customers' networks has shown more intrusion attempts within the first half of 2020 than in all of 2019.

While it is still important to invest in the appropriate technical controls, overlooking the Cybersecurity Awareness Training component of your overall cybersecurity plan could ultimately lead to those investments being ineffective. It is time to start training and testing your employees if you are not already.

HOW DO YOU GET STARTED?

Dopkins has partnered with KnowBe4, the world's first and largest new-school security awareness training and simulated phishing platform, to provide training and testing for your employees. Visit our KnowBe4 page for more information and to set up a free demo. A subscription to KnowBe4 is included in our STARTegy program, where we setup and manage everything for you. Check out our STARTegy page for more information about our Strategy for Getting Started with Information Security.

Stay tuned for our next blog about working from home!

For more information, contact Patrick Rost at prost@dopkins.com.

Reference Links:

Dopkins October 2020 blog: A Strategy to Get Started with a Cybersecurity Program: Are you prepared with a Data backup?

Sophos Security survey: https://www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx

SC Magazine article: https://www.scmagazine.com/home/security-news/phishing/you-clicked-on-what-shaming-among-the-most-effective-deterrents-phishing-scams/

Research published in the Journal of Computer Information Systems, performed at University of Sussex and University of Auckland:
https://www.tandfonline.com/doi/full/10.1080/08874417.2020.1812134?scroll=top&needAccess=true

CrowdStrike report: https://www.crowdstrike.com/resources/reports/threat-hunting-report-2020/

Dopkins KnowBe4 Security Awareness training: https://www.dopkins.com/services/it-systems-consulting/knowbe4-security-awareness-training/

Dopkins STARTegy: A strategy for getting started with Cybersecurity: https://www.dopkins.com/services/it-systems-consulting/startegy-a-strategy-for-getting-started-with-information-security/