|  |
| --- |
| **Partner/ EQR Reviewer: Moi** |
| **PR Reviewer:** |
| **Imagery:** |
| S:\BUSINESS\Marketing\Common\NATIONAL\PHOTOS\Stock Photography\Technology Photo 495142074 |

**Cybersecurity and Protecting Your Business**

By Aish Patel, Assurance Senior

Marcum, LLP

Hartford, CT

According to the cyber education company Cybint, human error causes about 95% of cybersecurity breaches — and that vulnerability costs companies billions of dollars. In this article, we discuss the value of understanding the cybersecurity mechanism; how war and COVID-19 have intensified the cybersecurity landscape; and how employees can help protect businesses from cybercriminals and cyberattacks.

Human intelligence and greed have led the world to the cybernetic warfront. Countries are fighting to save their place in the world, and protecting against cyberattacks has become a key element of preserving their integrity, substance, and sanctity in that cybernetic battlefield.

While you’re likely aware of the Russia/Ukraine conflict, you may not realize how severely this war has impacted cybersecurity around the world. Many countries and businesses were caught in the crossfire and became victims of the ongoing conflict. According to a study published in 2022 by the Center for Strategic and International Studies, several cyberattacks that targeted Ukraine also disrupted services in America and Italy. This includes multiple private and public sector DDoS attacks that targeted personal accounts of government officials, media organizations, energy facilities, post offices, etc. For instance, the study reported, “the American company Viasat was attacked, which disrupted internet services across Europe, including Ukrainian military communications at the start of the Russian invasion. The attackers hacked satellite modems belonging to thousands of Europeans to disrupt the company’s service.”

The same study reported that one of the attacks that pushed “two of the country’s largest banks go offline was the result of an ‘information attack’ where Ukrainian citizens received spam text messages claiming that ATMs were not working.” It’s important to note that the hackers used common citizens as a medium to infiltrate banks’ network.

With the majority of the workforce working remotely, COVID-19 proved a golden opportunity for cybercriminals. From a cybersecurity standpoint, working from home is not as safe as working in an office because of a lack of protective measures. Even if you install anti-malware software and firewalls, criminals will have an easier time getting through than they would if you were in an office environment monitored by IT personnel. Also, not all businesses provide a virtual private network (VPN) to their employees. VPNs provide a secure and encrypted environment for users to enter and work in and restrict unauthorized parties, such as cyberattackers. Many people work in a cloud-based workspace that is not tunneled through a VPN. Additionally, people fell victim to fake and malicious coronavirus information websites. As the International Criminal Police Organization (Interpol) reported in April of 2020, “There has been an increase of domains registered with the key words ‘COVID’ or ‘corona’, to take advantage of the growing number of people searching for information about COVID-19.”

When employees don’t understand their role in protecting the cyber environment, it puts the entire business at risk. While humans are the weakest link, they are also the strongest firewall that can protect against cyberattacks. Jen Easterly, the United States Director of the Cybersecurity and Infrastructure Security Agency, said earlier this year in an interview with CNBC that “Cyber security is not a tech issue; it’s about people and human behavior. This is a persistent issue and so we need to focus on how we can protect ourselves.” Employees’ social behavior is the key to protecting against cybersecurity threats. According to an article published in 2021 by Columbia Southern University, “An important concept when learning about behavioral analysis in cybersecurity is understanding both how individuals create risk to organizations and how to mitigate those risks. This begins with the understanding that hackers will always seek the easiest possible path into a network, which is often through employees and other individuals.”

When we think we have all of our cybersecurity bases covered, that is when we fall victim to vulnerability. Humans are constantly manipulated, and attackers constantly evolve. Therefore, educating the human workforce on how to protect against malicious attacks is the most important path to protecting your business. It is essential for the businesses to **train** and educate employees. The scale can be small for a small business, but even smaller organizations must perform regular and timely cybersecurity risk assessments.

The rules to follow when educating employees are straightforward and include even minor precautions, such as:

* Maintaining presence of mind.
* Maintaining caution in handling emails.
* Maintaining caution while browsing the web.
* Avoiding illegitimate websites.
* Ensuring you do not pass on sensitive information while speaking to other people.
* Following the cyber rules that exist within your organization.
* Limiting access to sensitive data.

Management should also be trained and educated on:

* + What and how the IT department (whether external or internal) is managing the cyber environment and attached risks; and
	+ Subjects like securing access points and networks; how web and email filters work; how patching works; and if it has been implemented properly.

Lastly, it is important to understand that as technology becomes more sophisticated, so do the infiltrating mechanisms. For instance, a virus would be a mechanism. Therefore, organizations should not only limit use of traditional cybersecurity tools but should also implement the latest solutions that have artificial intelligence and machine learning capabilities. Understanding the facets of cybersecurity may sound esoteric, but it is straightforward and only requires awareness and a collective effort. Doing so can save billions or even trillions of dollars. Let’s not make this a forlorn hope.

Bibliography

<https://www.cybintsolutions.com/cyber-security-facts-stats/>

<https://www.youtube.com/watch?v=ZlNE9gQTBXs>

<https://www.columbiasouthern.edu/blog/blog-articles/2021/february/human-aspects-of-cyber-security/>

<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html