volcorp
JULY 2021

THE FRONTBURNER

Welcome to the July edition of *The FrontBurner*! 2021 continues to be incredibly busy as we continue to work with compressed rates, bloated balance sheets, and plenty of unknown. We also have a lot of bold initiatives underway while maintaining focus on the daily operations that must be delivered at a high level for you. By now, you should have noticed our rebranding and, hopefully, you have heard about our new CUSO, Symphony, which has hit the ground running. We also have some other exciting things going on behind the scenes that we will introduce you to in due time.

All of this busyness can cause an organization to lose its laser-like focus on the all-important topic of cybersecurity. However, in the midst of all that we have going on, protecting your corporate is paramount, as we know protecting your organization is to you as well. As such, this month's edition of *The FrontBurner* will focus on some of the most common cybersecurity myths we feel must be better understood in order to maintain a high-level cybersecurity program. With that, I hope you enjoy this month's edition of *The FrontBurner*.

We'll see you in August at Forum'21!

Jeff Merry, President/CEO

Cybersecurity continues to be a hot topic across multiple industries with the ever-changing cyber threat landscape. As new breaches and attacks are featured in the daily headlines, there seems to be a battle to see who can hold the title for the worst breach ever.

Despite the increased focus on securing organizations, you might be wondering why or how businesses continue to fall victim to cyber-attacks. There are several misconceptions about cybersecurity that can prevent organizations from effectively safeguarding their data. Here are three of the most common fallacies regarding cybersecurity:

Common Misconceptions About CYBERSECURITY

1 Misconception #1 – We have an expert(s), cybersecurity is the responsibility of IT

Not many will argue IT bears the brunt of responsibility for managing cybersecurity and implementing safeguards for an organization. However, IT is not solely responsible for cybersecurity. Real cybersecurity preparedness is the responsibility of every employee within the organization.

A cybersecurity breach can have a lasting effect on a business. In fact, some organizations fail completely and are unable to recover. A company that prepares each employee to have their own cybersecurity sword and shield stands a better chance of defending their network than those who are relying on just one expert or an understaffed IT department.

Continued...

Misconception #2 – Cybersecurity threats come from external actors

External threats are a serious concern for any organization and should be monitored on a continuous basis. The threat landscape is constantly changing with advancement in technology creating new attack surfaces. However, insider threats are equally dangerous and disruptive to an organization's mission.

Insider threats via accidental, negligent, and malicious behaviors pose a higher security risk than outside threats because these users are already behind layers of security controls. It is estimated that insider threats accounted for 60% of all cyberattacks.[1] Any business can suffer an attack from an insider threat. Your credit union should extensively monitor for insider threats to quickly identify events that will require an immediate response.

> *Cybersecurity misconceptions...present a belief that things are better than they are, or that the unimaginable is impossible.*

Misconception #3 – That won't happen to us, we are too small

Many organizations assume they are not a target. Why would an attacker target me? We have nothing of value, we are a small business, or we operate in a niche industry. The truth is, every business is a target and very likely to suffer a security breach at some point. Today's businesses are operating in a connected world. Multiple devices can be used to access data outside of brick and mortar buildings.

According to Verizon's Data Breach Investigation Report[2], 56% of cyberattacks involved small businesses. These attacks are successful because small businesses often lack advanced security software and security teams, making the entity an easier target for bad actors. Every organization needs an incident response plan to act swiftly against cyberattacks and reduce the impact on the business.

Cybersecurity misconceptions are very common and present a real threat to an organization's cybersecurity posture. They present a belief that things are better than they are, or that the unimaginable is impossible. Empowering end users with knowledge is the first step towards breaking down misconceptions and developing a mature cybersecurity program.

If you have questions regarding your credit union's cybersecurity structure, please contact Tyler McNair, Director, Enterprise Risk, at *tmcnair@volcorp.org* or 615-232-7948. You can also hear one of the nation's leading authorities on cybersecurity, Jim Stickley, at Forum'21 at the Loews Vanderbilt Hotel in Nashville, August 18-20. Register today at *volcorp.org/forum21/*.

[1] *IBM Threat Intelligence Report*

[2] *2021 Verizon Data Breach Investigation Report*