withum

TIP SHEET

Today's Cybersecurity Best Practices: Protect Your Business and Financial Systems

Do you have a viable cyber strategy and a good understanding of cyber threats facing your business?

Businesses must understand that during COVID-19 and the New Norm, your organization's attack surface has significantly expanded, especially with a distributed workforce and technology. A reporter asked Mike Tyson whether he was worried about Evander Holyfield's fight plan. Tyson said, "Everyone has a plan until they get punched in the mouth."

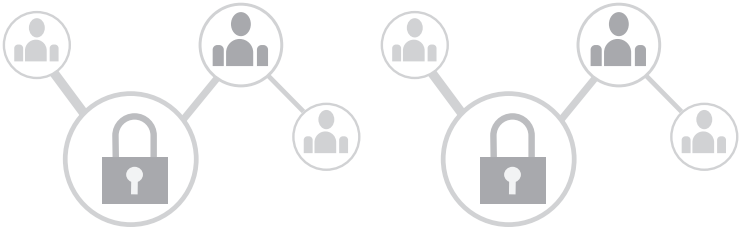
AVERAGE COST OF A DATA BREACH IN THE UNITED STATES: **$8.19M**

APPROXIMATELY **73%** OF CRITICAL BACKUPS FAIL DURING A CYBER-ATTACK.

RANSOMWARE ATTACKS OCCUR EVERY:

14 SECONDS AND EVERY 11 SECONDS BY 2021

THE AVERAGE COST OF A COMPROMISED RECORD IS **$242** PER RECORD EXPOSED DURING A DATA BREACH.



It is a misconception to think data breaches occur only to collect a ransom. Modern cyber-attacks are often after more than just a ransom. Although training may help reduce the number of users who fall victim to phishing attempts, it is certainly not the fix. Consider that if a single user alone falls victim to a phishing email, the entire organization can be impacted. That single user needs not be an IT Administrator with domain admin or superuser credentials for the entire environment and/or critical business assets to be compromised.

Cyber intrusions are about the confidentiality, availability and integrity of the systems and data. Modern cyber threats to business are external hackers and even an internal threat actor, as well as government and legal actions in the form of violations and sanctions. In terms of internal threat actors, an independent poll was conducted during COVID-19 that found that ~57% of employees felt that they could engage in nefarious activities against the company they work for and get away with it, simply because they were working from home.

withum

WHAT SHOULD YOU DO?

Cloud does not automatically equate to better security. Cloud is simply someone else's computer. Merely because your cloud provider is secure does not make your company secure. Next-generation cyber-attacks are here now, and they are not science fiction either. They are called cyber kinetic attacks. These types of attacks cause physical damage to environments. So, regardless of whether backups are 'good', cyber kinetic attacks can brick environments. Thus, rendering physical, electronic equipment and data useless like a physical brick. Secure your environment via independent third-party audits.

HERE ARE SEVERAL CYBERSECURITY CONSIDERATIONS YOU SHOULD ADOPT:

Apply Security Controls and Filtering w/Artificial Intelligence Integration
Virtual Tripwires (Identifies Anomalies in the Environment) Implement Self-Healing Smart Backups (Backups are typically poisoned by intruders)
Conduct a 3rd Party Threat Emulation aka authorized hacking of environment, Business Continuity and Security Gap Assessment to verify the business's confidentiality, availability, and integrity
24/7/365 Independent 3rd Party Monitoring and validation of environments to provide a constant 'checks-and-balance' against people, processes, and technologies. This assures internal and external policy, data privacy and compliance adherence

DON'T WAIT UNTIL AN INCIDENT OCCURS. For additional information about Withum's Cybersecurity Services, contact our experts now.