21 Cybersecurity Best Practices for Your Hybrid Workforce

THE COVID-19 PANDEMIC UNARGUABLY SHOOK THE WORLD LIKE NO OTHER EVENT BEFORE IT. ITS IMPACT WAS FELT IN EVERY SECTOR, WITH MOST BUSINESSES RELYING ON REMOTE WORK TO STAY AFLOAT DURING THE CHAOS.

However, with the recent rollout of vaccines, there is hope that businesses can do away with the fully remote model since it provides less space for collaboration. Many companies have touted hybrid work environments as the best option moving forward.

A hybrid environment brings together elements of traditional on-site work and remote work. Employees will have the choice to work from home, at the office or split time between both. While hybrid environments have advantages such as flexibility and good productivity, there are disadvantages like heightened cyber risks. These risks are especially conspicuous since many endpoints operate outside the secure corporate perimeter in a distributed work environment.

THAT'S WHY IT WOULD BE IN YOUR BEST INTEREST TO GO THROUGH THE CHECKLIST BELOW THAT HIGHLIGHTS 21 CYBERSECURITY BEST PRACTICES FOR YOUR HYBRID WORKFORCE:

01. Regular Risk Assessment

This process helps detect, estimate and prioritize risks to an organization's individuals, assets and operations.

02. Business Impact Analysis (BIA)

BIA helps quantify the impact of a disruption (due to an accident, disaster, etc.) on critical business operations.

CHECKLIST

03. Asset Management (Inventory and Mapping)

Keeping an in-depth inventory of digital assets (model number, serial number, location, the operating system, the patch levels, the configurations and even the state of known vulnerabilities, etc.) is vital from a security and data breach protection perspective.

04. Virtual Private Network (VPN)

To avoid a security incident, you need to install a business VPN that will secure connections with encryption. Make sure your employees test it at their respective locations to avoid any hassle.

05. Continuous Monitoring (Health and Vulnerability) for Network and Endpoint Devices

Around-the-clock monitoring is essential to defend endpoint devices and networks against malicious threats and suspicious user behavior. Keeping track of the health and vulnerabilities of endpoints and networks can help deflate data breach attempts.

06. Strong Identity Controls - Multifactor Authentication (MFA)

Strong identity controls that go beyond the traditional username-password authentication are essential to tackle the current threat landscape. Multifactor authentication, with features like one-time passwords (OTPs) and security questions, fits the bill.

07. Access and Permissions Management

Every employee should not have the same access rights within any business, including yours. By deploying an apt access and permissions management solution, you will no longer have to worry about what an employee has access to and what they can/cannot do.

08. Threat Intelligence, Investigations and Hunting (real-time)

It is crucial to proactively detect and block threats that are lurking undetected in your business' network. Threat Intelligence, Investigations and Hunting helps you achieve that.

09. Security-Driven Internal Network Configurations

This enables businesses to weave together the dynamic networks and static security tools set up to secure them. By converging security and networking functionality into an integrated system, you can speed up your business-critical applications and keep them secure.

10. Network Segregation

By applying network segregation, you can isolate your critical networks from other unimportant and less business-sensitive networks. It helps you keep cyberthreats in check.

11. Strict Password Policies/Management Tools

Implementing strict password policies and deploying the right password management tools helps your business improve overall password hygiene. It is, in a way, the first line of defense against intruders.

12. Secure and Guard Home Routers/Wi-Fi Connections

Ramping up the security of home routers and Wi-Fi connections must be a key consideration in a hybrid work environment because cybercriminals are waiting to seep in through the cracks.

CHECKLIST

13. Security Operations Centre (SOC) for Core Operations

It is necessary to set up a security operations center with people, processes and technology to monitor and improve the security of core operations. It helps identify, analyze, respond to and block cyberthreats.

14. Secure Cloud-Powered Systems/Solutions

Although the cloud is an integral element of hybrid work environments, it is not safe from risks. Mitigating those risks is essential for a seamless experience in distributed workspaces.

15. Backups and Disaster Recovery Systems

It does not matter if data loss happens because of human error, cyberattack or natural disaster. In the absence of a robust BDR solution, a data loss incident can have consequences such as severe downtime, reputation damage, regulatory penalties or even permanent closure.

16. Business Continuity Strategy

A good business continuity strategy ensures that business-critical functions carry on unhindered when disaster strikes and IT systems, software and applications are accessible and recoverable.

17. Clear, Documented Policies and Procedures

The policy and procedure documentation concerning the security of hybrid work environments should be brief but comprehensive to avoid crisis-hour hassles.

18. Define Incident Notification and Response Plans

This ensures that the right personnel and exact procedures are in place to tackle a malicious actor effectively in the event of a security breach.

19. Continual Security Awareness Training

This helps develop a transformative security culture within your business by empowering your employees to detect sophisticated cyberthreats and take adequate action.

20. Transparent Communication

Employees can't thrive working in silos. Deploy the right communication tools that enable collaboration and get everyone on the same page.

21. Security-First Culture

Your business' security must be top-of-mind for every employee. Therefore, make building a security-first culture a priority.

CONTACT US TO LEARN MORE ABOUT
EACH OF THESE SECURITY BEST PRACTICES
AND MORE FOR HYBRID WORK ENVIRONMENTS.

ALARIS

Alaris Threat Mitigation Consultants
contact@alaristmc.com 727-400-6259 alaristmc.com