Is Your Workforce Ready for Hybrid Working? Here's a Checklist to Help...

The Covid-19 pandemic shook the business 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 successful rollout of vaccines across the UK, there is hope that businesses can soon do away with the fully remote model, should they want to, since a return to face-to-face communication seems welcomed by employers, and employees alike. Many industry experts have touted hybrid work environments as the best overall option moving forward.

A hybrid environment brings together elements of traditional on-site work and remote work, with Employees having the choice to work from home, at the office, or split time between both. While hybrid environments have advantages such as personal flexibility and heightened productivity, there are disadvantages like an increase in cyber risks, and costs associated with asset management. These risks multiply due to many endpoints operating outside the secure business perimeter, in a distributed work environment.

Team Syn-Star have compiled this 21-point checklist to ensure you are using best security practices for your existing hybrid workforce, or to assist in creating one from scratch.

Broken into three sections: **People; Software; Hardware**, this checklist will help you ensure nothing is missed when it comes to your hybrid worker environment.

#1: People

Your staff are your biggest asset, but they can also be your biggest risk. The number one weakness targeted by hackers to gain access to a company's data is through the deliberate or unwitting errors of your employees.

- [ ] **Access and Permissions Management**

  Ensuring you have an up-to-date tiered files and folder structure with access and permissions levels defined at a corporate level, you will no longer have to worry about what an employee has access to, or what they can/cannot do.

- [ ] **Strict Password Policies / Management Tools**

  Implementing strict password policies and deploying the right password management tools help your business improve overall password health and strength. It's worthwhile implementing systems and processes that force regular password changes.

- [ ] **Have a Security-First Culture**

The security of the systems you use within your business must be at the forefront of the mind of every employee. By building a security-first culture you will minimise the impact of attacks.

- [ ] **Security Awareness Training**

Empower your employees to detect sophisticated cyber threats and take action to protect your business by training them on cyber security.

- [ ] **Transparent Communication**

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

- [ ] **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.

- [ ] **Employee Performance Monitoring**

Deploying an employee monitoring solution can not only improve productivity and employee engagement, but can also lessen the risk of infection by unauthorised website usage.

#2: Software.

Software is at the heart of every modern business, but it can also cause frustrations for users if the software you are using isn't properly set-up or integrated poorly.

- [ ] **Backups and Disaster Recovery Systems**

By having an automated backup that is monitored daily, it matters less if data loss happens because of human error, cyber attack or natural disaster, because you have the relevant systems in place to save and rollback your important information. In the absence of a robust and multi-layered solution, a data loss incident can have severe consequences such as business downtime, reputation damage, regulatory penalties, or even permanent closure. Onsite and cloud backup solutions should always be considered for hardware failures also. Ensure you have a written disaster recovery process that is regularly tested and updated.

- [ ] **Threat Intelligence, Investigations and Real-Time Hunting**

It is crucial to proactively detect and block threats that are lurking undetected in your company's network and data. Threat Intelligence, Investigations and Hunting helps you achieve that. There are hundreds or automated software products available, scalable to the size of your business.

- [ ] **Continuous Monitoring (Health and Vulnerability) for Network and Endpoint Devices**

Whether you are using smartphones, tablets, desktop or laptop connected to your network, around-the-clock monitoring is essential to defend against malicious threats and check on suspicious behaviour. Keep track of the health and vulnerabilities of your machines and networks, and help suppress internal and external data breach attempts.

#3: Hardware.

You will need to be mindful of the fixed physical assets that need to be implemented into your business for hybrid workers.

- [ ] **Asset Management (Inventory and Mapping)**

Keeping an in-depth inventory of digital assets (a register or all hardware) which includes: **The model and serial number; Location; Operating system; Patch and update levels; Specific configurations for certain hardware; State of known vulnerabilities** is vital from a security and data breach protection perspective.

Network Segregation

By applying segregation to your various networks, you can isolate your critical infrastructure from other less important and less business-sensitive networks. It helps keep threats localised.

Virtual Private Network (VPN)

To avoid a security incident, installing private network connections for your remote users will upgrade their connections with extra layers of encryption, and thus make them more secure by default. Ensure any VPNs unused for long periods are removed.

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 cyber criminals are waiting to target the holes. Your data is only as safe as the weakest vulnerable location.

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.

Security Operations Centre (SOC) for Core Operations

Although the cloud can be an integral enabling element of hybrid work environments, it should not be overlooked while assessing risk. Minimising the threat to your cloud environment is essential for a seamless experience in distributed workspaces. If your business is 'renting' cloud storage, like Microsoft 365 or Amazon Web Services, these can potentially be the most vulnerable from mass attacks.

Keeping your hybrid workers secure is an ongoing process and will require continued focus. We recommend that every business, whatever its size, should:

Regularly Review Risk Assessments

By reviewing Risk Assessments on a regular basis, you will effectively detect, quantify and prioritise action against risks to your team, digital assets and business.

Create a Business Impact Analysis (BIA)

BIA works with a risk assessment to help quantify the impact of a disruption (due to an accident, disaster, etc.) on critical business operations.

Implement Strong Identity Controls

Strong identity controls that go beyond the traditional username / password authentication are essential to tackle the current threat landscape. Multi-Factor Authentication (MFA), with features like one-time passwords (OTPs) and security questions, should keep you more secure once deployed.

Define Incident Notification and Response Plans

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

Implement a 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 remain accessible or recoverable.