IP SERVICES

ipservices.com 866.226.5974

Is your Cybersecurity posture ready for remote workers?

Shifting operations to a work from home (WFH) model introduces new cybersecurity considerations to your company/organization. Use this checklist to get ahead—and stay ahead—of new risks.

✓ **Instigate a cybersecurity health checkup** during and after the shift to WFH. Review all cybersecurity controls to identify gaps, prioritize, and remediate accordingly.

✓ **Update your Technology & Data Use Policy** to include remote workforce considerations like non-company owned Wi-Fi, VPN usage, USB and connected drives, and Bring Your Own Device (BYOD).

✓ **Update your Incident Response Plan** to include common and key WFH scenarios that may impact your organization, including lost or stolen devices.

✓ **Send regular awareness training videos to employees**, depicting important cybersecurity topics for a remote workforce, such as Wi-Fi usage and actively protecting company devices.

✓ **Hold group training sessions via remote webinar** with employees on best practices to help protect the company, specifically on phishing style and similar attacks. Include a short quiz to gauge learning.

✓ **Get regular cybersecurity threat alerts** that feature emerging cybersecurity topics, attacks, and vulnerabilities—including those related to remote workforce, this is often accomplished through a good Security Event Information Management (SEIM) service or solution.

✓ **Run vulnerability scans on networks** (internally and externally) any time you make configuration changes to firewalls and other devices, including VPN, to quickly identify critical vulnerabilities to patch.

✓ **Scan the Dark Web for stolen passwords** for all employees. If any are found, have employees change passwords immediately on all systems, devices, and applications.

✓ **Activate ongoing phishing tests** on employees simulating how cyber-attackers use fear, uncertainty, and doubt. Employees should confirm requests and verify links or attachments before opening, there great automation tools to provide this continual testing and validation.

✓ **Consider hiring ethical hacking on your networks** after reconfiguring systems to identify weaknesses attackers could exploit. This is generally called Penetration Testing or “PEN” Testing.

About IP Services

IP Services manages IT systems and applications spanning from Desktop to Datacenter, and we literally wrote the book – “The VisibleOps Handbook” – on best practices based IT Management. We have spent 15 years maturing the VisibleOps methodology into a true Quality Control System for IT Management. The VisibleOps approach uses a specific set of best practices for optimally managing every IT service.

Questions? Need assistance? Contact Toni.Overton@ipservices.com | 541-359-3146