CYBERSECURITY CHECKLIST

Eliminate the most common mistakes and missteps made by even the largest companies that are hit with cyberattacks. Ransomware hits businesses big and small every 11 seconds, that statistic beats the rate of car crashes in the US... Don't end up as a statistic, use and abuse this list for your company's health and reputation.

Cyber Insurance

If cyber hell breaks loose, is your company covered? Be prepared to repair the damage as a result of a cyber attack - P.S. most cyber insurance policies require each item in this list before your company can be covered.

Email Protection

Over 90% of hacks originate through email. Every company big or small needs to have AT LEAST an up-to-date Spam Filter and Advanced Threat Protection, or more commonly known as "ATP".

MFA Login Policy

Multi-Factor Authentication, also known as Two or Dual-Factor Authentication needs to be utilized on EVERY available application. This additional layer will protect you even if your password is compromised.

System Updates

Keep your office and personal technology updated, and turn on auto-update if available. Typically every software update includes new security protections designed to protect against the latest known cyber attacks.

24/7 Monitoring

Do you have a solution in-place that monitors your network 24/7 to detect and respond to cyber threats? Breaches happen at all hours so a 24/7 vendor or in-house tech security is vital to your company's safely.

Dark Web Scans

Real-time monitoring of the Dark Web to actively respond to stolen credentials that are listed for sale. This tool is one of our top, most cost-efficient, recommendation in preventing a company-wide data breach.

Team Awareness

Are your employees trained on cybersecurity practices? Does your company have phishing simulations and a training solution in place? Your company's data and reputation is only as strong as its weakest link.

Admin Controls

Are your admin accounts constantly locked down and only strategically accessed? You can significantly reduce the chances of entire networks being compromised by managing who has access and placing them on strict cybersecurity

CHECKLIST CONT'D

Antivirus SW

Is there active company-wide antivirus software that is constantly updated? This is a huge step in protecting company data from malware and viruses that can track and store valuable data.

Modern Firewall

Outdated firewalls are the equivalent to last year's flu shot, though it may have little strength remaining, it will make your company much more prone to cyberattacks and intrusions that could be avoided.

Data Backups

If your network was breached and data held hostage, you could still be on your merry way if you have proper data backups. External drives and/or cloud platforms could save your company from complete disaster.

4G Failover

Is your company prepared if your internet and phones go down? Whether from a cyber attack or bad weather, a down network could cost you more than you realize. Many providers offer 4G auto-failover to keep you up and running.

Response Plan

I'm sure your office has an emergency fire plan, but does it have an emergency cybersecurity plan? If your company goes under attack, an internal response plan is a must to find and regain access to your sensitive data.

PEN Tests

Penetration tests dive deep into your network, its configurations, and your users' behaviors to help uncover the issues that could lead to a cyberattack. These tests provide real-time vulnerabilities and cybersecurity risks.

Missing Any Checkmarks?

If this checklist is having you question your company's cybersecurity status and processes, schedule a cybersecurity assessment with us to see how we can help. Chances are, a **free cybersecurity assessment** from our team may uncover more vulnerabilities than expected.