15 Must-Do Things to Protect Your Business From a *Cyber Attack*

GREAT LAKES
Computer
Corporation

□ RISK ASSESSMENT

You need to establish a baseline understanding of the risks facing your organization before you can effectively write security policies and spend money on technical controls.

□ WRITTEN SECURITY POLICY

Policy guides employee behavior and sets expectations for how cybersecurity fits into your company's strategy. It can also be used to guide you through a breach (incident response plan) when your hair is on fire.

□ SECURITY AWARENESS

It's well-known that most cyber breaches are caused by employee misbehavior as they engage in phishing emails asking them to wire money or open a malicious attachment. Training employees on what to look out for will significantly reduce your likelihood of a breach.

□ PASSWORDS

Password managers such as LastPass should be used by all employees. This guarantees that passwords are long, complex, unique, and stored in a more manageable and simple way than having to remember passwords for disparate systems. Screen timeouts and setting the max failures before lockout are also important.

□ MULTIFACTOR AUTHENTICATION

MFA will prevent hackers from brute-forcing into your VPN, from stealing online account credentials, and from accessing any other system you protect with MFA. Hardware tokens are the most secure, but soft tokens and other options are available as well.

□ ADVANCED ENDPOINT PROTECTION

Your endpoint protection should include protection against file-less threats, behavior detection, and anti-ransomware functionality. Endpoints that "talk to" next-gen firewalls can help contain threats to a particular network zone.

□ WEB CONTENT FILTERING

Almost 70% of all Internet traffic comes in via HTTPS (not HTTP). You need to enable web content filtering but be sure to also set your WCF up to decrypt, inspect, and re-encrypt HTTPS traffic. Otherwise, your security posture is dubious at best.

The total cost of a successful **cyber-attack is**

$301

per employee

– Ponemon Institute

□ ENCRYPTION

There are two encryption use-cases. On servers, file-level encryption protects against data-scraping malware attacks. On mobile devices, encryption protects against attacks such as a hard drive getting removed from a laptop and inserted into the attacker's system for their prying eyes.

□ FIREWALL

Everyone has a firewall, but not everyone configures IDS, IPS, and other advanced security features. Firewalls that "talk to" endpoints are becoming increasingly useful in combating attacks.

□ BACKUP

Good backups follow the 3-2-1 rule: 3 copies of the data (prod + 2 backups), 2 different media (disk/cloud/flash), and 1 offsite (cloud). Attackers have also started to target NAS devices and backup appliances, so make sure these things have MFA enabled, where possible.

□ UPDATES

Windows updates are important but so are updates to third-party apps such as Chrome and Adobe Reader. Attackers can easily create a PDF, embed it with malicious JavaScript code, then run it through multiple encoders to let it march right through your firewall. To address this, ensure all Windows & 3rd-party apps are patched early and often.

□ ACCESS CONTROL

Implement the concept of "least privilege" everywhere, both on-premise and in the cloud. Only give users the privileges needed to accomplish their job function. If they're in HR, don't give them write access to the Engineering department's file share. The key here is "If you can't write to it, ransomware can't encrypt it."

□ PENETRATION TESTING

This valuable exercise answers the questions "how hackable am I?" and "how effective are my security controls?" Penetration testing is also required by most cybersecurity regulations and frameworks. Ethical hackers attempt to gain footholds in your network then provide remediation recommendations where weaknesses are found.

□ INCIDENT RESPONSE

Even with good planning, your organization will eventually get breached. Incident response involves key items such as:

-How do we respond?
-How gets involved?
-How do we restore business operations?
-How do we retain our reputation?

□ Cyber Insurance – Use this as a last line of defense if all else fails.

greatlakescomputer.com | 800-899-4522 (800-899-GLCC) | sales@grlakes.com