think CSC | Your Chief Technology Office

15 WAYS TO PROTECT YOUR BUSINESS FROM CYBERATTACK

RISK ASSESSMENT

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

WRITTEN SECURITY POLICY

Policy guides employee behavior and sets expectations for prioritizing cybersecurity in your company strategy. It can be used to guide you through a breach (incident response).

SECURITY AWARENESS

Most cyber breaches are caused by employees who engage with phishing emails that ask them to wire money or open a malicious attachment. Training your team is critical.

PASSWORDS

Password managers like LastPass should be used by all employees. This guarantees passwords are long, complex, unique, and safely stored while being manageable.

MULTIFACTOR AUTHENTICATION

MFA prevents hackers from brute-force VPN attacks and online account credential theft. Hardware tokens are the most secure.

ADVANCED ENDPOINT PROTECTION

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

Nearly 70% of internet traffic comes in via HTTPS. In addition to enabling web content filtering, you must also set your WCF up to decrypt, inspect, and re-encrypt HTTPS traffic.

The total cost of a successful cyber-attack is

$301 per employee

– Ponemon Institute

ENCRYPTION

On servers, file-level encryption protects against data scraping malware attacks. On mobile devices, encryption protects against hard drive theft and other risks.
You need both.

FIREWALL

Firewalls are more effective when properly used. This means configuring IDS, IPS, and other advanced security features. Firewalls that talk to endpoints are the most effective in preventing and combatting attacks.

BACKUP

Good backups follow the 3-2-1 rule: 3 copies of the data, 2 different media, and 1 offsite. Attackers will target NAS devices and back-up appliances, so make sure these have MFA enabled.

UPDATES

Windows updates are crucial, but so are updates to third-party apps like Chrome and Adobe Reader. Attackers can easily create a PDF embedded with malicious JavaScript, run it through multiple encoders and move right through your firewall. Patch early and often.

ACCESS CONTROL

Implement the policy of “least privilege” everywhere—on premise and in the cloud. Only give users privileges who need them to perform their jobs.

PENETRATION TESTING

Required by most cybersecurity regulations and frameworks, you must perform penetration testing to determine how hackable your business is. Ethical hackers attempt to gain footholds in your network to identify weaknesses.

INCIDENT RESPONSE

Even with the best planning, your organization may experience a breach. Incident response allows you to mitigate the impact by determining how to respond, who to involve, how to restore operations, and how to protect your reputation.

Cyber Insurance is a last line of defense if all else fails

thinkCSC.com 7420 Worthington Galena Rd. Worthington, Ohio 43085 (614) 786-7100