What keeps me up at night? The thought that your money may be stolen. The odds are only rising.

We are just at the start of a cybersecurity crisis. The cost of cybercrime is exploding, and by 2026 will exceed $20 trillion. Today, the Dark Web generates enough cybercrime to make it the third largest economy on earth. **Don't be a victim**. The first step to arm yourself, and your organization, is to know where you are vulnerable. By completing this assessment, you will immediately know where the gaps in your security may lie. Fill in these holes, and you can **protect yourself from 99%** of cyberattacks.

1. Password Management: Is your password strong enough?

- ☐ Are passwords complex (at least 12 characters, including letters, numbers, and symbols)?
- ☐ Are unique passwords used for different accounts?
- ☐ Are passwords stored securely, such as in a password manager?
- ☐ Are passwords changed regularly?

2. Multi-Factor Authentication (MFA): Do you use second level authentication everywhere?

- ☐ Is MFA enabled for all critical accounts and systems?
- ☐ Are users educated on the importance of MFA?
- ☐ Are backup methods (like recovery codes) securely stored?
- ☐ Is MFA regularly reviewed and updated?

3. Internet Hygiene: Are you cautious with every online connection?

- ☐ Are users trained to recognize phishing and social engineering attacks?
- ☐ Are security measures like anti-virus, and anti-malware software in place and up to date?
- ☐ Do you avoid dangerous websites that offer exploitative content?
- ☐ Are you cautious on social media? Do not overshare personal information.

4. Network Security: Have you invested in network cybersecurity?

- ☐ Are network security tools properly configured and maintained?
- ☐ Is network segmentation implemented to limit access to sensitive data?
- ☐ Are regular network security assessments and penetration tests conducted?
- ☐ Are security patches and updates applied promptly?

5. Internet of Things (IoT) Security: Are the devices that connect to your network secure?

- ☐ Are devices like cameras, doorbells, WIFI lights, etc.) regularly updated and patched?
- ☐ Are default credentials (username and password) changed on all IoT devices?
- ☐ Is network access for IoT devices restricted and monitored?
- ☐ Are IoT devices assessed for vulnerabilities before being integrated?

Bring Eric to your organization: Contact@EricONeill.net

WWW.ERICONEILL.NET

6. Data Protection and Encryption: Is all your sensitive data encrypted?

- ☐ Is sensitive data encrypted both at rest and in transit?
- ☐ Are data backups regularly performed and securely stored?
- ☐ Is there a data classification policy to identify and protect sensitive information?
- ☐ Are access controls in place to limit who can view or modify sensitive data?

7. Incident Response Plan: Are you ready for a cyberattack?

- ☐ Is there an established incident response plan (IRP)?
- ☐ Are IRP drills and simulations conducted regularly?
- ☐ Is there a communication plan for incident reporting & during an ongoing attack?
- ☐ Are roles and responsibilities defined and understood by all employees?

8. Employee Training: Do you train on cybersecurity awareness?

- ☐ Are regular training sessions conducted for all employees?
- ☐ Is there ongoing education on new and emerging threats?
- ☐ Are phishing tests and other exercises used to gauge employee awareness?
- ☐ Is cybersecurity culture promoted throughout the organization?

9. Access Management: Are there controls for access to your confidential data?

- ☐ Are least privilege principles applied to user accounts?
- ☐ Are access rights regularly reviewed and updated?
- ☐ Is there a process for quickly revoking access for terminated employees?
- ☐ Are privileged accounts monitored and audited for suspicious activity?

10. Vendor and Third-Party Risk Management: Are those who connect to your data secure?

- ☐ Are third-party vendors assessed for cybersecurity risks?
- ☐ Are contracts and agreements in place to enforce cybersecurity requirements?
- ☐ Is there continuous monitoring of third-party activities and access?
- ☐ Have you considered a strategy for the use of generative AI?

Bring Eric to your organization: Contact@EricONeill.net

WWW.ERICONEILL.NET