Why You Should Care about Cybersecurity

Cybersecurity is regrettably easy to ignore—until it's too late. Once an incident occurs, costs are baked in; there's no way to put the genie back in the bottle. The right time to prepare is before an incident occurs.

How much do breaches cost businesses?

$9.4 million (USD)

In 2022, the average cost of a data breach in the United States was $9.44m. (Ponemon and IBM)

In recent years, the cost of a data breach has continued to increase, with no reprieve in sight. As companies continue to take more and more work online, this trend will likely continue.

$5.6 million (USD)

In 2022, the average cost of a data breach in Canada was $5.64m USD. (Ponemon and IBM)

Companies in every nation around the world are being similarly affected. As a company, you're facing figures like these if you do not make cybersecurity a long-term company focus item.

How much cybercrime?

$8 trillion

Projected global 2023 cybercrime damage. (CyberSecurity Ventures)

- ~20x global illicit drug revenue (UN)
- Nearly half of European Union GDP

Six Practical Steps to Stay Secure

Fortunately, you can achieve a significant security upgrade just by engaging in a number of best practices that impose minimal new costs. How do you or your business score on this checklist?

Fix Passwords

✓ **Use strong passwords.**
They should be long, unpredictable, and unique for each login.

✓ **Get a password manager.**
If you can remember all your passwords, they're not good enough.

Adopt 2FA/MFA

✓ **Enable 2FA/MFA everywhere.**
Use mobile authenticator apps or YubiKey—on every login you have.

✗ **Avoid unless no other choice:**
Email-based 2FA, which is inherently insecure.

Make Backups

Keep all of your data securely backed up at all times, so that if the worst happens your data is safe.

✓ **Rely on daily automation.**
Backups should not be manual or left to manual or ad-hoc processes that can miss data or be forgotten.

✓ **Consider cloud services.**
Cloud storage, applications, and backups are significantly safer and easier to manage than costly and fragile onsite backups.

Stop Account Sharing

Make sure that no "shared" accounts are in use. Every user should have his or her own login and password.

✗ **Don't cheat.**
Storing accounts in a password manager, then using it to enable many users to "securely" share an account isn't actually secure.

Run Updates

Keep your hardware and software up-to-date at all times.

✓ **Implement a process.**
Create a process or calendar item for assets that need manual checks.

✗ **No EOL software/hardware.**
Retire assets when updates end.

Limit Admin Access

Ensure that there is only one user with administrative access in any multi-user accounts.

✓ **Use regular accounts if possible.**
Even for services with only one user, create separate "admin" and "daily use" accounts when possible, then use admin only for admin tasks.

How to Respond to an Incident

1. Insurance

It is likely that your policy imposes particular notification requirements. Be sure to adhere to them.

✓ **Understand requirements.**
Know who should be notified and what must accompany your notification.

✓ **Notify promptly.**
Most policies require timely or prompt notification.

2. Legal

Begin communication with your legal team or representation about the incident immediately.

✓ **Be transparent.**
Do your best to answer questions and provide information requested.

✓ **Follow recommendations.**
To avoid making a bad situation worse, carefully adhere to legal recommendations.

3. Law Enforcement

If recommended by legal, notify law enforcement and/or intelligence agencies.

✓ **Do involve legal.**
Rely on legal guidance for agency or agencies to notify and how to notify.

✗ **Don't expect miracles.**
Law enforcement's role is to prevent future crimes, not to improve your current situation.

4. Notifications

Under guidance from legal, make any notifications to third parties or to the public that you're required to make.

✓ **Do involve legal.**
Rely on legal guidance for who to notify.

✗ **Don't head straight to social.**
Public notifications may be required, but plan carefully—don't "live tweet" the incident on Twitter.

5. Preserve Evidence

Think "evidence" from day one so that as it's required by insurance, legal, or law enforcement, it's available.

✗ **Don't rush.**
Remediate rapidly, but not so rapidly that forensic data is destroyed.

6. DFIR Specialist

Either engage a digital forensics and incident response (DFIR) specialist or appoint an internal investigation and remediation stakeholder.

7. Negotiation Specialist

If you have been the victim of a ransomware attack, consider engaging a boutique specialist in ransomware negotiaton.

✗ **Don't immediately pay.**
Your best chance to retrieve data is with a specialist, not in acquiescing right away to ransom terms.

Security Rollout Sequence

A. Identity Protection

Identity is the foundation of cybersecurity; no other strategy matters if identity is insecure.

✓ **Implement password security.**
Use or require strong passwords and a password manager.

✓ **Deploy multi-factor.**
Deploy a secure 2FA/MFA soltuion like authentictor app(s) or YubiKey(s).

B. Governance

After passwords and 2FA/MFA, implement identity and data governance.

✓ **Centralize identity.**
Manage identities from a central providerlike Azure AD; deploy a single sign-on solution like Plurilock AI.

✓ **Prevent data loss.**
Deploy a data loss prevention (DLP) solution like Plurilock AI to ensure that sensitive data isn't shared.

C. Governance Training

Identity solutions are only as good as your users' dedicated use of them.

✓ **Provide reasons.**
Users are more likely to comply if they understand the reasons for doing so.

✗ **Don't accept shadow IT.**
Ensure that users understand that creating new accounts outside of this framework is forbidden.

D. Email Security

Implement email security to ensure that employee email interactions and behavior don't eventually lead to an incident.

✓ **Deploy a dedicated platform.**
Deploy an email security platform like Proofpoint to scan incoming email for malicious code, URLs, or attacks.

✓ **Hold phishing workshops.**
Ensure that your users understand how to avoid getting phished.

E. Endopoint Protection

Deploy detection and response—EDR, XDR, or MDR—for endpoint safety.

✗ **Don't allow unsafe endpoints.**
Ensure that every endpoint is protected; do not allow work on unprotected systems.

✓ **Consider a managed service.**
A managed service is more effective if you don't have a security team.

F. Network Security

Deploy, configure, and mandate firewall and VPN solutions.

✗ **Don't allow off-VPN work.**
Limiting work to only VPN endpoints provides an additional, robust layer of network security.

✗ **Don't start here.**
Having or installing "a firewall" does not provide you with "enough security" to skip all the preceding items in this list.