BEST PRACTICES

Cyber Risk

5 practices to mitigate exposure

Cyber risk is the risk of damage to an organization through its information systems. The risk of financial loss, business interruption, or reputation damage from a failure or breach of IT systems becomes more significant every year. All types and sizes of organizations are at risk – not just financial institutions, defense contractors, or other high-profile businesses.

When everyone involved knows what to look out for and what to do should an issue arise, organizations can more proactively manage and mitigate risks before they become bigger problems.

Start with these top 5 practices. Some address training and policies which are easier to implement and verify, while other methods will require more specialized effort and resources for implementation.

Deploy Multi-Factor Authentication (MFA)

MFA is when a user must provide two or more pieces of evidence to verify their identity to gain access to an app or digital resource. MFA is used to protect against hackers by ensuring that digital users are who they say they are.

How does it work?

MFA verification relies on three different categories of information that are unique to you.

- What you know (password or a PIN)
- Something you have (smartphone)
- Something you are (fingerprint, face ID, or voice recognition)

Set it up

More accounts and applications are moving to MFA for security. Some accounts and applications automatically require that you add another verification method.

Technical methods of protection

The five most common MFA methods are:

1. Hardware OTP (one-time password tokens)
2. Standalone OTP Mobile Applications
3. Soft token Software Development Kits (SDKs)
4. SMS-based OTP (one-time password tokens)
5. Smartcards and cryptographic hardware tokens

Update Software Consistently

Software updates replace old versions of software with newer versions that improve functionality, and most importantly, security.

Why does it matter?

Since attack methods are constantly evolving, software must also evolve to mitigate attacks. If we keep outdated software on our devices, it's like leaving a window unlocked in our building just waiting for a criminal to find it.

How does it work?

Most software will notify users of updates available, so keep an eye out for those notifications, accept them, and install them as soon as possible. Where you can, choose to make software updates automatic.

Technical methods

Anything with an Internet connection will be affected by Internet-facing vulnerabilities. Regularly scheduled vulnerability scanning and an effective patching policy should be implemented. An automatic software update and asset tracker solutions can assist with this requirement.

Make Passwords Strong

Without a strong password, criminals who spend days searching password dictionaries can easily unpack your password, and therefore your accounts.

How to make passwords strong

1. Make password unique; avoid using the same password for multiple devices and accounts.
2. Make them longer; Use between 14-16 characters that consist of upper and lower-case letters, numbers, and symbols.
3. Avoid personal information or common words; we put a lot of information on the Internet, so avoid using words or phrases that could be traced back by someone with some basic observation skills.

Additional technical protection

1. Ensure the system prevents prior passwords from being reused.
2. All electronic passwords should be encrypted.
3. Perform random visual spot-checks to ensure end-users do not write down passwords.
4. Implement a Password Manager.
5. Disable user IDs after five failed log-on attempts in the system.
6. Implement 2FA, MFA or require and implement security questions.

Encrypt and Backup Data

When you encrypt a file or an email, you secure it by requiring a password to open it. This extra step for your files or emails creates another layer of defense around sensitive materials.

Files and document drives should be backed up or copied on a regular schedule.

Why does it matter?

Encryption makes sure that only the right person opens your email documents. Backups create copies of important documents that you don't want to lose in case something happens to your device or system.

How does it work?

Tips for encrypting email in Google for end-users
Tips for encrypting email in Microsoft Outlook for users

Back up files with multiple methods and syncing services. Consider using an external hard drive or cloud storage.

Technical methods

1. Determine where server backups will be stored such as in the cloud, on-premises, offline, offsite and/or a secondary data center.
2. Ensure all backups are encrypted.
3. Use unique backup credentials stored separately from other user credentials.
4. Prevent end users from storing files local on their equipment.
5. Test backups by frequently attempting to restore them and test their integrity prior to restoration to be confident it's free from malware.

Be Cautious of Clicking on Links

Hackers impersonate entities or people you may know to try to trick you into clicking on something you.

Why does it matter?

Nearly one-third of all data breaches in the U.S. last year were the result of people clicking on

How to tell

Sometimes it's hard to tell what's real or not. If you get something suspicious, stop, don't click on it, don't share it, and contact your IT support resource for verification.

What should I do?

1. Stop here; do not enter any additional information.
2. Disconnect from the Internet.
3. Scan your machine using anti-virus and antimalware.
4. Change passwords to accounts with your password or any business-related financial information.

Technical methods of protection

1. Utilize email filtering that blocks known malicious attachments, executables, links, and messages based on the content or attributes of the sender.
2. "Tag" or mark emails coming from outside the organization.
3. Enforce MFA if end users are accessing email through a web app and/or non-corporate device.
4. Enforce Sender Policy Framework (SPF).
5. Employ DomainKeys Identified Mail (DKIM) or Domain-Based Message Authentication Reporting and Conformance (DMARC).