FUSION Computing

☎ 416-566-2845
www.FusionComputing.ca

CONSTRUCTION

Construction companies are fast becoming a favoured target among cybercriminals. Construction firms are currently dealing with a huge array of new risks – both on and offsite. A threat can expose all of a company's digital assets, including business plans and acquisition strategies; proprietary construction plans and designs; customer, contractor, and supplier lists and pricing; personally identifiable information (PII) of employees and contractors; protected health information of staff as well as facilities security information. Threats can also severely interrupt the manufacturing and building process, hit profit margins, and cause reputational damage.

Some Key Areas To Review:

INADEQUATE DEFENCES

Construction companies often have inadequate firewalls or defences against cyber-attacks.

Consumer-grade antivirus software is often used but is generally insufficient to thwart determined attackers.

VULNERABILITY MANAGEMENT

Companies use multiple digital systems, complex software and communication devices across multiple job sites.

Devices and applications must be continuously patched and updated with the latest security fixes.

REMOTE WORK

Employees take their devices home or on the road at various sites, conferences and remote areas.

Unsecured public wifi, different cellular providers or having other people access their devices can pose a security threat.

According to one study, construction companies were the third most common industry targeted by hackers. In 2020-2021 nearly one out of six construction companies reported a ransomware attack.

SUBCONTRACTORS AND VENDORS

Construction companies can be heavily reliant on subcontractors and vendors.

If subcontractors and vendors have unrestricted access to your systems or applications, it can pose a serious security threat.

LEGACY DEVICES

Use of certain devices or applications that may no longer be supported in the market.

This means the device/application will no longer have applicable updates and security fixes, leaving it vulnerable to attacks.

RANSOMWARE AND PHISHING

Attackers can access and lock down important data, demanding large sums of money to release it without guarantee.

It might not lead to a loss of information, but it can cause an enormous amount of lost productivity and business delay.

Malicious emails designed to look genuine, can only take one unsuspecting employee to click on a link or attachment.

FUSION Computing

CONTSTRUCTION

Key NIST/CyberSecure Canada control points:

NIST

MOBILE COMPUTING

Ensure your laptop and personal digital assistant (PDA) are encrypted and password-protected.

If a computer or PDA uses wireless connections, ensure all wireless communications are encrypted.

Ensure encrypted backups are in place.

When using USB flash drives, use only devices that have built-in encryption and require passwords.

Implement mobile device management to deploy org-wide configuration and compliance policies.

PASSWORD GUIDELINES

Ensure your computer has a user profile lockout policy in place that requires reentering a password to gain access.

Have strong password policies in place, including password complexity, password age and use of MFA.

Use of password managers in accordance with NIST and Cyber Secure Canada guidelines.

EMAIL SECURITY

Use appropriate signatures and standard disclaimers on email messages, faxes and other documents.

Report spam/junk emails immeditely.

Carefully address emails and double-check names in the address lines.

Be cautious when communicating sensitive information via email.

GENERAL

Perform weekly scans to ensure endpoints are up to date and unauthorized software is not installed.

Make weekly backups and keep backups securely offsite.

Ensure policies are in place preventing access to restricted websites and software.

STAFF EMPOWERMENT

Educate staff and end users about cybersecurity.

Require regular security awareness trainings.

CYBER INSURANCE

Cyber Insurance generally covers your business's liability for a data breach involving sensitive customer information.

Cyber insurance and cybersecurity frameworks have a symbiotic relationship, with one enabling and reinforcing the other.

FUSION COMPUTING targeted remediation:

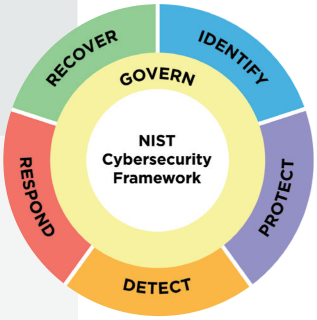
RISK ASSESSMENTS

Risk must be gauged and prioritized based on factors such as probability of occurrence, impact on the organization, and prioritization.

Risk assessments should be conducted or reviewed regularly and at least once per year.

SECURITY CONTROLS

- ✓ Anti-virus and MDR
- ✓ Secure encrypted backups
- ✓ Data Loss Prevention
- ✓ Encryption at rest and in transit
- ✓ Firewall
- ✓ Incident Response Plan
- ✓ Mobile Device Management
- ✓ Policies and procedures
- ✓ Security Awareness Training
- ✓ Vulnerability Management
- ✓ Multi-Factor Authentication



CIS Controls