FUSION Computing

☎ 416-566-2845

www.FusionComputing.ca

ACCOUNTING

As the rate of cyberattacks grows, hackers know vulnerable systems that contain important financial information are easy targets. Accounting cybersecurity practices ensure that your firm protects sensitive data, not only for your firm's compliance, but also for the safety of your clients who have entrusted you with their financial, personal and professional information.

Some Key Areas To Review:

PHISHING

Accounting organizations are increasingly being targeted by phishing attacks.

Cybercriminals contact users, impersonating legitimate business contacts.

Lure targets into giving up sensitive data and access to company resources.

RANSOMWARE

It locks down systems and prevents access until a ransom is paid.

It is one of the fastest-growing types of cybercrime.

CLIENT RISK

Accounting firms hold important information for individuals and businesses.

Accounting firms have a duty to protect this information at all costs.

FINANCIAL & REPUTATIONAL RISK

The financial consequences of a cyberattack are considerable.

If exposed to an attack, it may lead to significant reputational risk.

Recovering some reputational losses can be difficult and as costly as the financial losses.

Many people believe that cyber-attacks are solely the domain of multibillion-dollar corporations. This is a faulty assumption, as ransomware attacks on small and medium-sized businesses were reported by 85 percent of managed service providers (MSPs).

CYBERSECURE CANADA

FUSION Computing

ACCOUNTING

Key NIST/CyberSecure Canada control points:

NIST

NETWORK PERIMETER & ARCHITECTURE

The Network needs to be configured, organized, and connected so as to ensure security and operability.

use next-generation firewalls that continuously monitor activity and detect intrusions.

BACKUPS

Plan to back up your data, operating systems, and applications.

Ensure that data and information are stored in the cloud and backed up regularly.

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.

PASSWORDS & AUTHENTICATION

Ensure your computer has a user profile lockout policy, which 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.

PATCH MANAGEMENT

It's important to update devices and software on a regular basis.

Ensures devices and applications are protected from attacks and operating efficiently.

Restricting unauthorized software applications can help mitigate exposure to potential attacks.

FUSION COMPUTING targeted remediation:

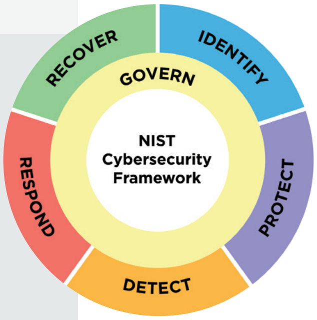
RISK ASSESSMENTS

Risk must be gauged 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