FUSION Computing

416-566-2845
www.FusionComputing.ca

FINANCE

Financial institutions are among the leading targets of cyber attacks. Banks are where the money is; for cybercriminals, attacking banks offers multiple avenues for profit through extortion, theft, and fraud. At the same time, nation-states and hacktivists also target the financial sector for political and ideological leverage. Cyber-attacks in the financial sector have tripled over the past five years, and the average cost of containment has increased by 40%. Today, the assessment that a major cyberattack threatens to financial stability is axiomatic- not a question of if, but when.

Some Key Areas To Review:

RANSOMWARE & MALWARE

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

There is a costly process of notifying clients, analyzing the attack, remediating the business and paying for monitoring.

Malicious emails are designed to look genuine

SOCIAL ENGINEERING

Phishing or whaling attacks, sending bogus invoices that purport to be from a trusted source.

People are often the most vulnerable link in the security chain.

DATA ENCRYPTION

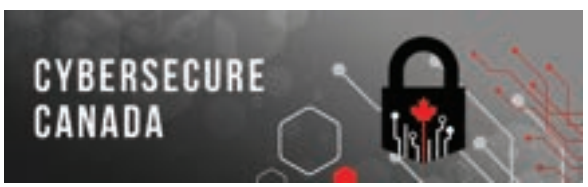
Unprotected mobile applications and unencrypted data are a massive threat to financial institutions

FRAUD & IDENTITY THEFT

These are constantly evolving through more digital channels.

Implement cybersecurity strategies that actively search for suspicious account activity.

More and more banking transactions are now conducted online, with 78% of Canadians primarily banking online or through mobile devices. After data breaches, it could be challenging to trust financial institutions. That's a significant issue for banks. Data breaches caused by a shoddy cybersecurity solution may easily lead to their consumer base moving their business elsewhere.



FUSION Computing

FINANCE

Key NIST/CyberSecure Canada control points:

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.

SECURITY AWARENESS

Educate staff and end users about cybersecurity.

Require regular security awareness trainings.

Test staff progress and knowledge by deploying phishing campaigns.

ANTIVIRUS & EDR

Endpoint Detection and Response, works with antivirus solutions.

EDR collects data from the endpoint and examines it in real-time for malicious or anomalous patterns.

PASSWORDS & AUTHENTICATION

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

Have strong pasword 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 is 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