FINANCIAL AND CONSUMER SERVICES COMMISSION

COMMISSION DES SERVICES FINANCIERS ET DES SERVICES AUX CONSOMMATEURS

Notice Regarding Cybersecurity Risk

Introduction

Cyber threats are a growing risk for organizations within FCNB's regulated sectors.[1] Proactive management of this risk is increasingly important to protect against attacks seeking to compromise or disrupt computers systems or steal data and information stored.

FCNB has resources to help strengthen risk-management practices and increase cybersecurity preparedness.

This notice identifies important first steps organizations in our regulated sectors can take toward that goal.

Managing the cybersecurity risk

A number of best practices standards for cybersecurity risk management exist. FCNB employs a modified National Institute of Standards and Technology (NIST) framework[2] to manage its cybersecurity risks.

Many of these best practice standards set out important steps which an organization should take to manage risk in different areas within an organization:

Area	Key risk management steps
Cybersecurity planning	The organization has committed to improving its cybersecurity posture, has put appropriate personnel in charge and has committed resources. A plan is in place to identify assets, assess risks to those assets and take remedial steps where necessary.
People security	Employees are trained to adopt security conscious behaviour. A cybersecurity culture exists within the organization. Everyone is aware of their responsibility to maintain a cybersecure environment. The organization has a robust employee entry and exit process and employees only have access to the IT resources required to do their work.

[1] The 2019 Accenture Cost of Cybercrime Study identifies significant and growing cybersecurity risks to organizations. The study demonstrates an increasing focus on information theft and disruption of core systems and data, as well as more aggressive and sophisticated techniques targeting the "human layer" through phishing and social engineering techniques. See https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[2] The NIST Cybersecurity Framework provides organizations with a structure for assessing and improving their ability to identify, prevent, detect, respond to and recover from cyber incidents. See https://www.nist.gov/cyberframework

Organizational policies	Policies are in place to identify best practices in the use of IT resources and data management.
Operational security	The organization has operational awareness of cybersecurity threats and vulnerabilities, and how its IT resources and data are used and accessed. It can take effective action when a risk materializes. Incident response and business continuity plans are in place. The organization learns from its experiences.
Software development	New software is assessed for cybersecurity risks before use. Software developed in-house meets appropriate security standards and testing requirements before implementation.
Physical security	Systems and processes are in place to prevent unauthorized physical access to the organization's offices and assets. Appropriate access logs are maintained where appropriate.
Third-party relationships	The organization verifies the cybersecurity posture of any third parties who may have access to the organization's IT systems and data. The organization has commitments from these parties to be notified if any fall victim to a cybersecurity breach.
Network security	The organization's network is structured to protect against external threats. Appropriate firewall solutions, server configurations and encryption mechanisms are in place. Controls are ready to manage connection of foreign devices to the network (such as USB drives).
Platform security	All computer and server operating systems on the network are patched and updated as required. Appropriate anti-virus/malware software is installed on each device on the network. Mechanisms are in place to ensure all users are authenticated and authorized before accessing the network. Users have robust passwords.
Application security	User applications are tested for cybersecurity risks before use and are updated as required.

How to start

Not all risks are the same. Some risks pose a bigger threat than others. Some risks are easy to address while others are more complex to manage. Identifying the biggest risks with the easiest fixes first is a good strategy.

Below is a simple initial cybersecurity checklist for an organization without a current cybersecurity risk plan or strategy. This checklist is not comprehensive and does not cover all potential risks to an organization. However, it should help in identifying and addressing the "low hanging fruit" risks.

An organization that has addressed the steps in the list should have confidence it has materially improved its cybersecurity posture and preparedness.

After addressing all the steps on this checklist, organizations are encouraged to pursue a broader cybersecurity plan covering additional risk areas identified in more formal frameworks. Additional resources and details of how to develop a broader cybersecurity plan are available on the FCNB website.

A first run through of the checklist will likely identify numerous gaps. These gaps should be prioritized based on the risk posed and resources available, and preferably assigned for remediation to a specific employee with a specific completion timeline.

The checklist

- ☐ Assign a person or persons the responsibility of managing the organization's cybersecurity risks.
- ☐ Make an inventory of all computing devices used within the organization, and identify for each device:
    - the type of device (smart phone, tablet, desktop, laptop, server, etc.) and the model number
    - a serial number available or placed on the device
    - the user responsible for the device
    - the operating system and relevant applications installed on the device
    - whether the device is encrypted
- ☐ Make a list of all types of electronic records and data maintained on the organization's computer systems ("electronic assets") and identify where they are stored.
- ☐ Classify the electronic assets based on whether they contain any of the following:
    - personally identifiable information (PII)
    - proprietary information
    - sensitive financial information (for example, credit card information)
    - transaction data
- ☐ Identify electronic records and data on the list that are important to the organization's ability to operate.
- ☐ Create a network topology for the organization (for example, how are its computer and other computing devices connected, what servers/storage devices are on the network, how is the network connected to the Internet, etc.)
- ☐ Conduct a risk assessment of computing devices, electronic assets and network topology by identifying:
    - Which devices and assets are attractive attack targets?

- What attack vectors are there for gaining access to these devices and/or assets?
- Which actors may be seeking to attack the organization?
- What is the likelihood of a breach via a particular attack vector?
- What is the impact of such a breach?
- How can the risk of a breach be reduced or perhaps eliminated?

- ☐ Consider adopting a remote management tool to manage the organization's computing devices used outside the organization's offices.
- ☐ Review who has access to the organization's electronic assets and ensure "least privilege"[3] access.
- ☐ Review, update and test the back-up and recovery process for electronic records and data.
- ☐ Offer cybersecurity awareness training to employees, preferably on an ongoing basis.
- ☐ Review or create key cybersecurity policies for the organization:
  - Cybersecurity best practices
    - Authentication
    - Passwords
    - Clean desk
    - Using computing devices outside the office, etc.
  - Acceptable use of IT resources
  - New employee intake and exit
  - Third parties and IT vendors
- ☐ Review the organization's physical security posture. Are appropriate controls in place to limit physical access to the organization's office(s)/building(s) to only the appropriate employees?
  - Key card access?
  - ID badges?
  - Visitor access rules?
- ☐ Verify that the disposal process for physical assets (old hardware, paper records, etc.) ensures all important records are properly destroyed or shredded at end of life.
- ☐ Review the organization's network architecture. Are appropriate firewall solutions, server configurations and encryption mechanisms in place?
- ☐ Review the operating systems and network enabling applications in use to ensure they are up-to-date and properly patched, and that an appropriate update schedule is in place and being followed.
- ☐ Ensure up-to-date anti-virus/malware software is installed on all devices that have access to electronic assets.
- ☐ Create a cybersecurity breach incident response plan and test it.
- ☐ Create a business continuity plan and test it.

[3] An employee only has access to the information needed to do his or her work, and nothing more.