An initial cybersecurity program assessment

The cybersecurity program assessment is based on a cybersecurity program maturity model that has been adapted to address the unique context of many SMBs.

The results will allow you to consider where your organization lies along a continuum of cybersecurity program maturity and guide where you may be able to make investments to bolster your program, make your organization more secure, and reduce the risks to an acceptable level.

Below there are six sections that provide an indication of the maturity of your overall program. Within each section, choose the response which most closely applies to the practices in your organization.

Section 1 - Critical information and assets of business value

- ☐ We are aware that some of the information and assets of the business hold more value than others.
- ☐ We have identified information and assets of business value.
- ☐ We have identified and categorized information and assets of value within the organization based on its business value as well information that must be protected to be in compliance with local laws and regulatory requirements.
- ☐ We have an IT asset management program that includes identifying all information and data inventory which includes the value of all information and assets as well as the protections required.

Section 2 - Appreciation of the threat context

- ☐ We are aware of the general cyber threats to our organization.
- ☐ We have identified specific threats to our business / sector.
- ☐ We have conducted a threat assessment to our business / sector.
- ☐ We have ongoing monitoring of active and emerging threats to our business / sector.

Section 3 - Risk management

- ☐ We understand that there are cyber risks to our organization.
- ☐ We have identified general cyber risks to our organization that we have acted upon.
- ☐ We have a conducted a risk assessment and applied appropriate risk treatments to reduce the risks to an acceptable level.
- ☐ We have an integrated risk management program in place that is monitored and updated as the business, technical or threat context changes.

Section 4 - Cybersecurity Protections/Security Controls

- ☐ We are not aware of what cybersecurity controls are in place within our organization.
- ☐ We have some basic cybersecurity controls in place that address some threats.
- ☐ We have basic cybersecurity controls in place that respond to our appreciation of the common threats posed to our business.
- ☐ We have a tailored suite of cybersecurity controls in place that are responding to the dynamic threat environment experienced in our business / sector.

Section 5 - Cybersecurity governance and management

- ☐ We understand that we should have some form of cybersecurity governance and management.
- ☐ We have a senior member of our organization assigned as the cybersecurity leader and they understand who does what within the organization and can make the decisions needed to maintain a basic level of security.
- ☐ We have a governance body in place for cybersecurity and have guidance available to employees. We have occasional meetings.
- ☐ We have a governance body in place as well as a policy that defines organizational cybersecurity roles and responsibilities. We also have associated plans to support incident response and business continuity. We are monitoring and measuring key aspects of the program and annually review policies and plans to ensure that they are up to date.

Section 6 - Security awareness and employee behaviours

- ☐ We do not have a security awareness program in place and hope that employees know what to do.
- ☐ We have a security awareness program in place that provides a general overview of the threats and suggested employee best practices.
- ☐ We have ongoing security awareness throughout the year and regular updates. Those with specific cybersecurity responsibilities are aware of those responsibilities.
- ☐ We have an ongoing security awareness program that is monitored and measured against employee behaviours. Those with cybersecurity responsibilities have had the necessary training to support their roles.

Feedback on completion of the assessment

Level 1

The important thing now is that you are aware that there is work to do. As you progress through this program, ensure that you consider your own organizational context and focus on the cybersecurity basics to get you to the next level.

Level 1.1 – 2.5

You are progressing on your program and have basic protections within your organizations. As you progress through the modules, identity the next steps that will help you further mitigate risks and elevate your program to the next level.

Level 2.5 – 3.5

Your program is quite mature and you should be looking at where you can refine your security controls and explore opportunities to create a more robust program. Accordingly, as you progress through the modules, critically assess your organization's practices against what is laid out in the modules to see where you might make some improvements.

Level 3.6 – 4

Congratulations, you've done a great job of bringing your cybersecurity program to a level that most rarely achieve. However, you should keep in mind that there is no such thing as 100% security. So, the emphasis should be on monitoring and continuous improvement while ensuring that you are able to adapt to a change in business, technological or threat context. As you progress through the modules consider what other areas that may help you sustain your program and address the evolving future.