Primer on Cybersecurity Risks for SMBs

As a small and medium business (SMB), you are likely using information and information systems of value that support your business which are subject to various cyber threats – deliberate, accidental or via natural events (e.g. flood, earthquake, fire). It is recommended you conduct a threat and risk assessment (TRA). While you can certainly do this yourself if you have an complete asset inventory and can either conduct or out-source a vulnerability assessment on your systems, suggest that you engage a cybersecurity service to support you in this endeavor as they have methodologies and tools to support your TRA. A fundamental challenge with TRA activities in SMBs, however, is ensuring that the business owner or senior leadership has clearly identified the business-critical information and information systems that need protection and the related business risks should these be compromised. Accordingly, this primer is focusing on the cybersecurity risks.

The risks

If your business is connected, you are at risk. Cyber risks translate to other organizational risks such as:

Financial risks – Direct or indirect financial losses or costs. Direct costs include any potential ransom, loss or theft of data, the costs associated with recover and clean up after the incident. Indirect costs can include downtime, lost opportunity, notification costs, fines, or other costs that may results as a consequence of the incident.

Operational risks - the loss of capability either through loss of data or loss of access to information systems needed to conduct business.

Legal risks- For example, loss of personally identifiable information (PII) of customers or clients can result in litigation costs.

Compliance risks – depending on your business and jurisdiction, there may be legal or regulatory compliance requirements and if you suffer a cybersecurity incident and the impact, you may be subject to fines, or sanctions, or even criminal charges.

HR risks – your organization may have employees and talent that support your operations. If you lack such resources or if they are in any way compromised such as through a social engineering attack, it will have an impact on your operations.

Supply chain risks – you likely rely on suppliers and in fact may be a supplier to another businesses. Internal or external threats to your supply chain could directly or indirectly result in impacts to your business.

Reputational risks – loss of reputation is often difficult to measure and more difficult to mitigate, but the costs can be significant if you lose client or customer trust as a result of inadequate security precautions, or failing to be transparent, or and do not take appropriate action to mitigate the impact of an incident. any threats to your business.

Value and risk

The are many ways to conduct a risk assessment and if you are not familiar or confident in conducting your own risk assessment, suggest that you contact a security or risk professional who can guide you through the process.

In basic terms, the **risks you hold are a function of the value of the information and information systems you use in your business relative to the likelihood and severity of potential cyber threats**. Be cautious when considering 'value'. Reflecting back on risk, your information and information systems can carry value well beyond the mere financial costs. Consider the value of your **intellectual property**, **business applications**, **employer or customer information**, **marketing information and website content**, **corporate secrets** or **investor information** as examples of other information or data that your business holds – it is also at risk to cyber threats.

Understanding the value of the information and information systems is the first crucial piece to knowing your risk. Another key component is appreciating your business and technical context including:

- To what extent do you rely on the internet and internet-based technologies to support your business?
- What is your market reach and primary competition?
- What level of growth are you experiencing or want to experience?
- How complex is your supply chain?

The following table* demonstrates how your business and technical context has an impact on your potential risk. For example, consider that you are the sole proprietor of a small retail outlet that primarily attracts local consumers. Additionally, for your technical context,

- your IT infrastructure consists of a laptop and you have activated automatic updates and use industry recognized security software;
- you ensure that you back up critical business information on a USB stick when it is updated, roughly once a week;
- you have a small info-only website with embedded security;
- you use accounting software that is processed across a secure connection to the vendor for updates;
- you have point of sale (PoS) device from a major banking institution; and ▪ you use a business email provider that has embedded security.

In this situation, your risks are relatively low because your business does not rely heavily on information systems for day-to-day operations with the exception of the PoS device and its security is primarily managed by the bank. Further, the remainder of your IT infrastructure has needed basic protections. So, your exposure to threats is relatively limited.

On the other hand, if you are a small tech firm scaling to the international market leveraging online sales and maintenance of your services to all clients, your risks will be inherently higher based on your investments in growth, extended reach and the increased reliance on information systems to conduct your business all which increases your threat exposure.

Business /technical context	**Typically Lower Risk** ⟷ **Typically Higher Risk**			
Internet connected technology use	None, very limited dependence	Low dependence	Medium dependence	High dependence
Market reach/ competition	Local	Provincial / regional	National	International
Growth	Limited or stable market	Low growth or emergent	Moderate growth	High growth
Supply chain complexity	Very limited or high trust	Limited, trusted suppliers	A moderate number of suppliers with some visibility and trust	Extensive with limited visibility or trust in some suppliers

* Adapted from a similar table introduced in the Canadian Centre for Cyber Security's (2019) e-learning course for small and medium organizations.

As discussed, if you are not fully familiar with your IT infrastructure and are not comfortable with interpreting vulnerability assessment results, then you should consider consulting a cybersecurity professional or similar service. Regardless, you have important data that is relevant to the risk discussion. You should ensure that you understand and can articulate:

1. the value of the information and information systems upon which your business relies and what you want to protect
2. your business context and what might increase the potential risks such as scaling up, forming new business relationships or expanding; and
3. your technical context which includes the degree of reliance on information systems and related technologies and how well they are currently protected from predominant threats.