LinkPoint.
IT SOLUTIONS

1 Do you know what assets (data and devices) need to be protected and where they are located? Yes □ No □

2 Do you maintain system logs? Yes □ No □

3 How long do you maintain your system logs?

□ Less than 6 months □ 6 months - 1 year □ 1-3 years □ 3-5 years □ More than 5 years

4 Do you use anti-virus software and is it up-to-date? Yes □ No □

5 Do you use data encryption technology on your sensitive data and devices? Yes □ No □

6 Is there a designated person in your organization responsible for cybersecurity? Yes □ No □

7 Do you have a training program for your employees, contractors or volunteers to maintain user awareness of cyber risks? Yes □ No □

8 Has your organization ever fallen victim to a cyber-attack in the past? Yes □ No □

9 Would you know if a security breach has occurred? Yes □ No □

10 Do you have a Cyber Incident Response Plan in place? Yes □ No □

11 Do all staff members understand their roles and responsibilities in the event of a cyber incident? Yes □ No □

12 Does your organization have Cyber Liability Insurance? Yes □ No □

13 Are you aware of any regulatory requirements regarding data protection and privacy that impact your business? Yes □ No □

Taking steps to understand your readiness to face a cyber incident can mean the difference between protecting your assets and becoming the headline of a cautionary tale. Our assessment focuses on a few core areas of cybersecurity and is meant to identify a starting point for where your organization can focus on improving in the future.

If your organization scores under 5, you rank as a **BEGINNER** in cybersecurity preparedness. Based on your responses, we recommend considering the following as you continue to refine your cybersecurity strategy:

### Protect Your Critical Assets

Identify what the most critical assets are to your organization, where they reside, and who has access to them. Leverage technology to enhance the protection of these assets through anti-virus software, encryption, and monitoring. Conduct regular assessments to pinpoint where your vulnerabilities are and develop strategies to mitigate them.

### Designate a Person Responsible for Cybersecurity

There are likely several team members whose skill sets, knowledge or capacity allow them to play a role in the overall cybersecurity strategy, but it's recommended that you designate one individual to be primarily responsible for overseeing your program. If you don't currently have the capacity to designate a team member to this area, consider whether adding an employee is an appropriate path forward or whether engaging a third-party organization to act as a virtual Chief Information Security Officer is a viable solution.

### Train Your Employees

Human error remains the leading cause of cyber incidents, and these situations often result from an end user's failure to follow policies and procedures. Employees need to understand how to identify risks and the appropriate individuals or departments where they should report findings. In addition, every employee should be taught best practices, like how to create stronger passwords or how to spot suspicious emails, so that they can use good judgment when online.

### Strengthen Your Vendor Strategy

Remember that your cybersecurity strategy is only as strong as the third-party vendors on which you rely to deliver products or services to your clients. Require that each of your third-party providers meets your defined minimum security standards, such as maintaining up-to-date virus detection software, standard device configurations, or user training best practices. Have each provider share their cybersecurity strategy with you so that you can evaluate that they meet or exceed your expectations.

### Be Ready to Respond

Creating an incident response plan guides your employees and stakeholders on what to do if the worst case scenario occurs. All plans should include key team members tasked with remediation, communication procedures, critical systems, any potential workarounds that can keep your organization functioning, and an estimated timeline to contain a breach.

### Cover Yourself with Cyber Liability Insurance

You can limit your financial, legal, and reputational damage from cybercrime through the coverage of a cyber liability insurance policy. The insurance addresses two critical risks: first, the liability risk to your business if sensitive client or employee information is compromised, and second, the substantial cost of notifying clients that their information has been compromised, credit monitoring, fines, legal fees, and forensics.

If your organization scores 5-10, you rank as a **INTERMEDIATE** in cybersecurity preparedness. Based on your responses, we recommend considering the following as you continue to refine your cybersecurity strategy:

### Designate a Person Responsible for Cybersecurity

There are likely several team members whose skill sets, knowledge or capacity allow them to play a role in the overall cybersecurity strategy, but it's recommended that you designate one individual to be primarily responsible for overseeing your program. If you don't currently have the capacity to designate a team member to this area, consider whether adding an employee is an appropriate path forward or whether engaging a third-party organization to act as a virtual Chief Information Security Officer is a viable solution.

### Train Your Employees

Human error remains the leading cause of cyber incidents, and these situations often result from an end user's failure to follow policies and procedures. Employees need to understand how to identify risks and the appropriate individuals or departments where they should report findings. In addition, every employee should be taught best practices, like how to create stronger passwords or how to spot suspicious emails, so that they can use good judgment when online.

### Hack Your Own System

Take your cybersecurity strategy to the next level by conducting social engineering or red team exercises to try and hack into your own system. This type of test will simulate an actual cyber incident to help you identify if you are using your security technologies effectively and where your system may have weaknesses. It is also a great way to test if your current employee training program is functioning effectively.

### Revise Your Response Plan

After creating an incident response plan that includes key team members, communication procedures, and a timeline for containment, it will be important to revisit it to account for changes to your organization or your risk landscape. The key is not to overcomplicate the context so that it works in multiple situations. You can apply learnings from your cyber risk assessment to add additional safeguards.

### Consider International Regulations

Any organization that conducts business internationally needs to be aware of how regulations change from country to country to remain in compliance. Unlike standards in the U.S., some countries consider the data privacy of its citizens to be a human right. Under new regulation standards like the European Union's General Data Protection Regulation (GDPR), companies are required to obtain consent to collect personal information and maintain opt-out programs in digital and telecommunications programs. You can minimize your global cyber risk exposure by gaining an understanding of how data privacy regulations extend for your international operations.

If your organization scores 10-13, you rank as a **ADVANCED** in cybersecurity preparedness. Based on your responses, we recommend considering the following as you continue to refine your cybersecurity strategy:

### Strengthen Your Vendor Strategy

Remember that your cybersecurity strategy is only as strong as the third-party vendors on which you rely to deliver products or services to your clients. Require that each of your third-party providers meets your defined minimum security standards, such as maintaining up-to-date virus detection software, standard device configurations, or user training best practices. Have each provider share their cybersecurity strategy with you so that you can evaluate that they meet or exceed your expectations.

### Revise Your Response Plan

After creating an incident response plan that includes key team members, communication procedures, and a timeline for containment, it will be important to revisit it to account for changes to your organization or your risk landscape. The key is not to overcomplicate the context so that it works in multiple situations. You can apply learnings from your cyber risk assessment to add additional safeguards

### Consider International Regulations

Any organization that conducts business internationally needs to be aware of how regulations change from country to country to remain in compliance. Unlike standards in the U.S., some countries consider the data privacy of its citizens to be a human right. Under new regulation standards like the European Union's General Data Protection Regulation (GDPR), companies are required to obtain consent to collect personal information and maintain opt-out programs in digital and telecommunications programs. You can minimize your global cyber risk exposure by gaining an understanding of how data privacy regulations extend for your international operations.

Contact our team of technology experts today to discuss how to greatly improve cyber security for your organization

604.559.TECH (8324)
Toll Free (888) 557-0259

info@linkpoint.ca
support@linkpoint.ca