ELECTRO
FEDERATION
CANADA
EFC

ACHIEVING A SECURE STATE:

Cybersecurity Best Practices IT Resource Guide

EXECUTIVE SUMMARY

Cybersecurity is essential for today's connected world. Every facility can become the target of a cyberattack – businesses, factories, banks, institutions, homes and even infrastructure such as electricity transmission grids. Cyberattacks are typically aimed at accessing, changing or destroying sensitive information; extorting money from people; or interrupting normal business processes.

Cybersecurity experts agree that experiencing a compromise is not a question of if, but rather, when. When a compromise occurs, organizations with an effective cybersecurity plan can quickly detect and respond to the issue, will maintaining business continuity and preventing the potential loss of money, intellectual property, stakeholder confidence and brand reputation. The financial impact of a breach to organizations is significant, often resulting in lost business and detection, escalation and other response measures that can cost an organization, on average, $4.25M[1].

> Organizations must "assess the risks to information and systems with the same vigor [they] would for legal, regulatory, financial or operational risks."
>
> Source: National Cyber Security Centre (UK)

This document recommends best practices and actionable steps organizations can take to establish safety protocols to keep their data and systems safe. The cost of inaction can be substantial – outlined below, are key implications and measures to consider as your organization builds out its cybersecurity action plan:

$4.24 million

Data breaches can cost companies $4.24 million

IBM

38%

Lost business accounts for 38% of data breach costs

IBM

10–15%

10-15% of IT budget on cybersecurity spend

Deloitte

22 days

Average cost of downtime following ransomware attack: 22 days

Statista

31%

31% of customers discontinued relationships with companies that had a data breach

CIO Insight

To access the full toolkit of resources, follow this link. You are strongly encouraged to share these resources with your IT team. If you or your team have any questions, please contact EFC at **info@electrofed.com**.

[1] IBM Cost of Data Breach Report 2021

GETTING STARTED TAKES A SHARED VISION

Cybersecurity is a business imperative that is *everyone's responsibility*. For a cybersecurity strategy to be effective, business leaders and IT personnel must have a shared understanding of their organization's risks, challenges, priorities and action plan. The following chart outlines common questions that executives and IT teams can address together to interpret and define a cybersecurity plan that is best suited for their organization:

Key questions	What this involves
Are we compliant?	• What cybersecurity standards do we need to meet or exceed? • Have we met the standards? • **If yes**, what measures do we have in place to ensure we maintain compliance? • **If no**, what do we need to have in place to achieve compliance?
Are we secure?	• Do we understand our risks and threats? What are they? • Do we know what our key assets are? • How are we protecting them?
How has our security evolved from last year?	• What has changed in our security landscape, or within our organization, in the last 12 months? • How are we addressing new security challenges? • Where did we improve? • What more can we do to mitigate risks? What resources or costs are required?
What do we do in the case of a breach or attack?	• What security incidences have occurred in our organization? • How were they handled? • What did we learn? • How did we adapt?

TYPES OF CYBERSECURITY THREATS

The first step to protecting your business, is understanding the most prevalent types of cybersecurity threats:

Data Breaches

A data breach occurs when sensitive data is stolen from a system without authorization from the system owner. Cybercriminals search for weaknesses in a company's security settings within network or point-of-sale (POS) systems and then exploit the weakness to access confidential user information, credit card and social security details as well as usernames and passwords. Data breaches can also occur as social attacks: cybercriminals trick users into granting access to the organization's network by having them download harmful attachments or retrieving login credentials. When a data breach occurs, businesses must take immediate action to contain the breach and resolve the issue to prevent system downtime and service interruption.

Data breach costs significantly increased year-over-year from **$3.86 million** in 2020 to **$4.24 million** in 2021

Source: Cost of Data Breach Report (IBM, 2021)

Compromised Passwords

Passwords are most often compromised when a user enters their login credentials unknowingly on an illegitimate website. Default and common username and password combinations can also leave accounts vulnerable to attacks. Using the same password across multiple platforms can make systems even more susceptible to hackers, leaving multiple accounts at high risk. Reports suggest that over half of users apply the same passwords for both their work and personal accounts, so instruct staff to create unique passwords for company accounts. When possible, provide a password manager service to staff to help them manage and protect their password.

Phishing

This hacking scheme tricks users into downloading harmful messages, in turn, exposing organizations to massive risks. Fraudulent emails that appear to come from a reputable source and contain legitimate-looking links, attachments, business names and logos are sent to users. The message persuades users to take some form of action – whether it's clicking a link or downloading an attachment – with the goal of stealing sensitive data such as credit card and login information or installing malware on the user's machine. Most breaches involve some form of phishing. According to Cisco, 86% of organizations have reported having at least one user connect to a phishing site.[2]

Malware

Also known as 'malicious software', malware is designed to damage and destroy computers and systems by slowing them down or stopping them from working entirely. Common types of malware include: trojan viruses, spyware, adware, worms and ransomware. Malware is released into a computer when users either click on an infected link, click on a pop-up ad or download an email attachment from an unknown sender. Once malware infects a computer system, hackers can gain access to company passwords, credit card numbers, banking data, personnel files, etc.

Ransomware

This is a type of malware that blocks users from accessing systems or files until ransom payment is made to cybercriminals. Ransomware often spreads through a malicious download in a phishing email. An attack can either target individual employees or entire organizations.

Ransomware attack costs are higher than other forms of breaches and can range from hundreds to millions of dollars. Unfortunately, many companies that pay ransom still don't recover access to their systems from perpetrators.

> Two-thirds (66%) of organizations said they suffered significant revenue losses as a direct result of a ransomware attack.
>
> Source: Ransomware: The True Cost to Business (Cybereason, 2021)

RANSOMWARE NUMBERS FOR 2021

Malicious emails are up 600% due to COVID-19

The average ransom for businesses is	The average downtime after an attack is	Only 8% of victims who pay up recover all encrypted files
$200,000	21 days	8%

Source: phoenixnap.com/blog/what-is-ransomware

80% of victims who paid ransom suffered another attack

46% of victims who paid ransom recovered corrupt data

60% of victims experienced revenue loss due to an attack

The largest paid ransom was $40 million

[2] Banks, Joe "5 cybersecurity threats for businesses in 2021." Security Magazine, September 12, 2021.

BUSINESS IMPLICATIONS

Cyber-attacks directly impact a company's bottom line, yet many leaders are unaware of the cost of inaction to their organization. According to an IBM study, businesses that fall victim to security breaches can incur $4.24 million in costs, on average, largely attributed to four factors: **post-breach response costs, detection and escalation costs, notification costs, and lost business costs.**

Post breach response

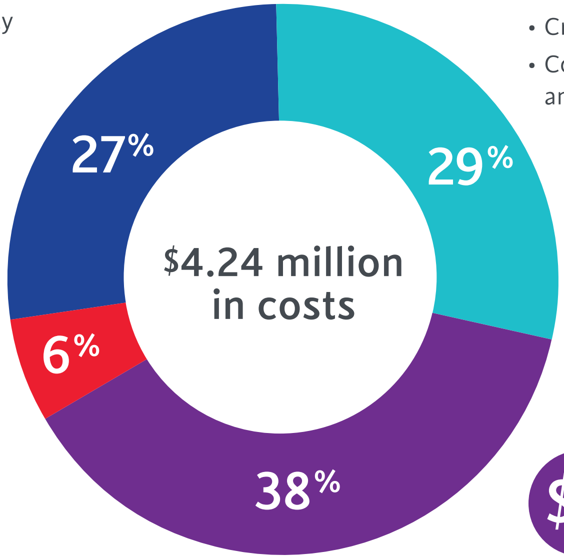
Activities to help victims of a breach communicate with the company and redress activities to victims and regulator

- Help desk and inbound communications
- Credit monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory fine

Detection and escalation

Activities that enable a company to reasonably detect a breach

- Forensic and investigative activities
- Assessment and audit services
- Crisis management
- Communications to executives and boards



Notification

Activities that enable the company to notify data subjects, data protection regulators and other third parties

- Emails, letters, outbound calls or general notice to data subjects
- Determination or regulatory requirements
- Communication with regulators
- Engagement of outside experts

Lost business

Activities that attempt to minimize the loss of customers, business disruption and revenue losses

- Business disruption and revenue losses from system downtime
- Cost of lost customers and acquiring new customers
- Reputation losses and diminished goodwill

Adapted from: Cost of Data Breach Report (IBM, 2021)

Aside from the bottom-line impacts, cyberattacks can also compromise a company's intellectual property, brand reputation and may introduce legal and regulatory implications. Let's examine some of these other factors:

Brand Impact

We all want to conduct business with organizations that are capable of keeping our information safe. One of the most important assets that a company has is the trust it establishes with customers. The impact that a cyber-attack may have on a brand can be dire. According to a survey conducted by CIO Insight, 31% of customers surveyed said they discontinued their relationships with companies that had a data breach. Of these customers, 65% said they lost trust in the breached organization.[3]

To mitigate this loss of brand reputation and trust, companies must be transparent with customers and partners on what actionable approaches they are taking to protect their data. When your company invests in security improvements and goes the extra mile to keep user data safe, take the opportunity to let your customers and partners know. It should be a standard part of your value proposition.

It's essential for marketing teams to be involved in developing a customer communication plan *before* a breach occurs. Marketing departments are uniquely positions to understand stakeholders' interests and can help protect the trust companies have spent decades building with customers and partners.

Legal Ramifications

A data breach may compromise sensitive information, resulting in the loss of intellectual property and significant legal ramifications. Legal teams are required to adhere to provincial and federal laws governing data breach notifications, and if applicable to their customer base, international laws as well.

Organizations are required to report data breaches under the Personal Information Protection and Electronic Documents Act (PIPEDA), involving breaches of personal information that pose a risk of significant harm to individuals. Affected individuals must be notified and a record must be kept of all breach activities. As shown earlier, notification costs account for approximately 6% of cyber-attack costs, which involves expenses related to informing regulatory agencies, partners, customers and the general public about a data breach.

[3] Frenkel, Karen A. "Linking Breaches, Brand Reputation & Stock Prices," CIO Insight, June 2017.

When an organization undergoes a data breach, the case will go to litigation and the company will be asked to demonstrate “due care.” This is the language judges use to describe “reasonableness” – businesses must demonstrate they implemented safeguards that are reasonable to the enterprise and appropriate to other interested parties at the time of the breach. It’s important for your organization to assess the level of sensitive data your company collects and to keep record of ‘due care’ safeguards that are in place to protect the data.

CASE STUDY: YAHOO

One of the largest company data breaches recorded involved Yahoo. In 2016, Yahoo reported that an estimated 500 million user accounts had been stolen two years prior. Yahoo’s challenge was escalated when officials indicated that the company had been aware of the breach three months earlier and had failed to notify customers. Yahoo’s mishandling of this situation and slow disclosure had significant business and brand implications: multiple lawsuits were filed and Yahoo’s stock price plunged, losing $1.5 billion in market value.

Source: ResearchGate: Journal of Advertising Research (March 2017)

Legal Ramifications

A data breach may compromise sensitive information, resulting in the loss of intellectual property and significant legal ramifications. Legal teams are required to adhere to provincial and federal laws governing data breach notifications, and if applicable to their customer base, international laws as well.

Organizations are required to report data breaches under the Personal Information Protection and Electronic Documents Act (PIPEDA), involving breaches of personal information that pose a risk of significant harm to individuals. Affected individuals must be notified and a record must be kept of all breach activities. As shown earlier, notification costs account for approximately 6% of cyber-attack costs, which involves expenses related to informing regulatory agencies, partners, customers and the general public about a data breach.

When an organization undergoes a data breach, the case will go to litigation and the company will be asked to demonstrate “due care.” This is the language judges use to describe “reasonableness” – businesses must demonstrate they implemented safeguards that are reasonable to the enterprise and appropriate to other interested parties at the time of the breach. It’s important for your organization to assess the level of sensitive data your company collects and to keep record of ‘due care’ safeguards that are in place to protect the data.

CYBERSECURITY INVESTMENTS

Cybersecurity is an investment in risk mitigation; it is an actionable approach to protecting systems and applications from malicious attacks. When it comes to Cybersecurity investments, ROI is not the metric to track. If your company maintains a secure state with a well-planned recourse plan when a breach occurs, your investments have been successful.

But how much cybersecurity spend is recommended? While there is not a one-size-fits-all budget for cybersecurity operations, companies should expect to spend **10–15% of their IT budget** on cybersecurity. According to a recent study by Deloitte, companies in the financial services sector spend, on average, 10% of their IT budgets on cybersecurity. That equates to approximately $1,300 to $3,000 per full-time employee.[4] (Note: this benchmark may be higher for smaller companies because they cannot take advantage of scale or volume).

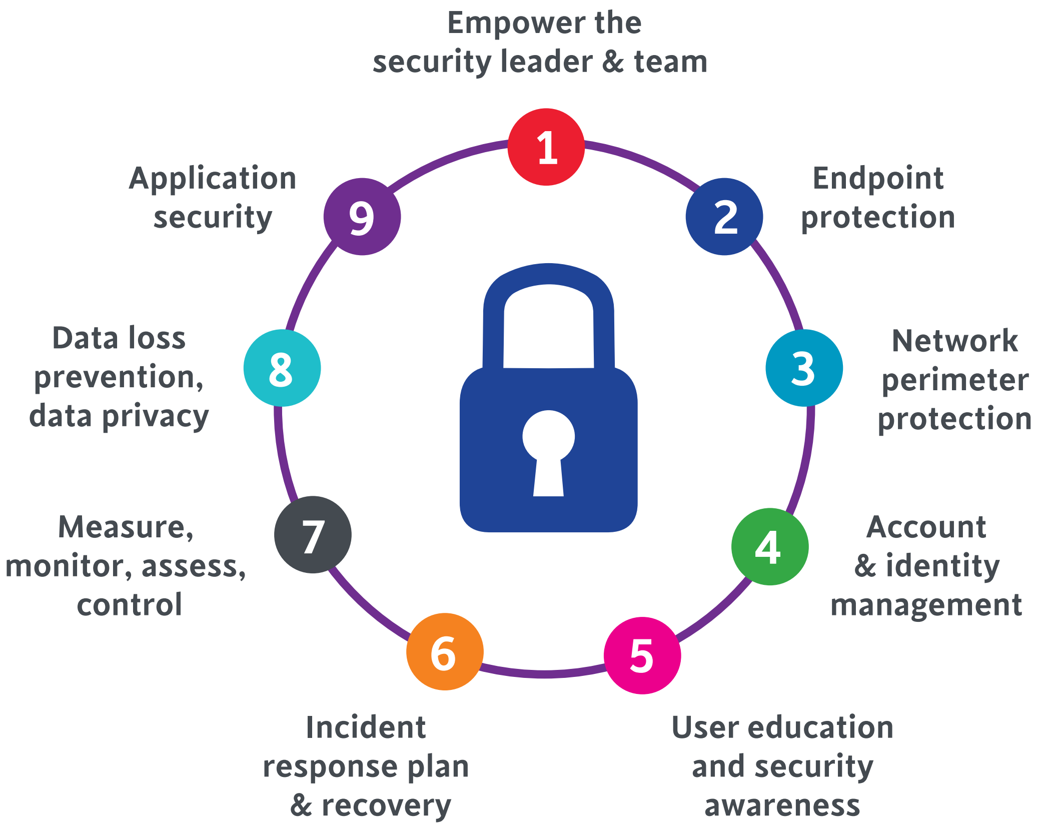
The allocation of 10–15% on cybersecurity spend might seem high to some, but the ramifications of not investing sufficient funds can be dire to business continuity. Over a 1½ period, Statista tracked businesses that had experienced a ransomware attack and found the average duration of downtime they experienced was 22 days.[5] Even well-prepared businesses experience downtime for 14 days on average, resulting in substantial lost sales which equates to more than the amount spent on cybersecurity measures.

The investment in cybersecurity typically involves cyber monitoring and operations, endpoint and network security, application and data protection, identity and access management and third-party/vendor security management. The next section shares an overview of nine key pillars that organizations should include as part of their cybersecurity planning.

[4] Bernard, Julie and Nicholson, Mark, "Reshaping the Cybersecurity Landscape", Deloitte Insights: July 24 2020
[5] statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/ – data retrieved: March 2022

NINE KEY PILLARS FOR CYBERSECURITY PLANNING

A comprehensive, effective cybersecurity strategy will involve multiple touchpoints and security measures to ensure assets are secure from malicious threats and attacks. Here are nine core areas that should be incorporated into a cybersecurity action plan:


Empower the security leader & team
1
Endpoint protection
2
Network perimeter protection
3
Account & identity management
4
User education and security awareness
5
Incident response plan & recovery
6
Measure, monitor, assess, control
7
Data loss prevention, data privacy
8
Application security
9

CYBERSECURITY BEST PRACTICES

1. **Empower Your Security Team:** ensure your IT team has the budget, tools and resources to protect your company’s data and systems from security risks.
2. **Endpoint Protection:** secure desktops, laptops, mobile devices and servers from cyber threats by installing software programs which are centrally-managed by security administrators.
3. **Network and Perimeter Protection:** the most important line of defense, involving systems that filter and examine data flowing in and out of the corporate network and between different components or branches of the network. Firewalls are a primary example of these systems.
4. **Account & Identity Management:** a security framework that authorizes and authenticates user access across applications, web portals, data, systems and Cloud platforms, ensuring only the right people are being provisioned to use the right tools, for the right reasons.
5. **User Education and Security Awareness:** formal cybersecurity education allows your workforce to assess and be on-guard for potential security threats. Training is most effective when it is part of an ongoing practice and when security policies are established to provide your workforce with security definitions, rules, processes and expected behaviours.
6. **Incident Response Plan & Recovery:** a set of instructions designed to help companies prepare for, detect, respond to, and recover from major security incidents.
7. **Measure, Monitor, Assess & Control:** continuously observing and testing IT networks, systems, data usage, applications, and infrastructure to proactively detect vulnerabilities, potential threats or breaches.
8. **Data Loss Prevention (DLP), Data Privacy:** tools and processes that protect sensitive data from becoming lost, misused or accessed by unauthorized users.
9. **Application Security:** using tools and methods to protect applications once they are deployed.

CHARTING YOUR CYBERSECURITY JOURNEY

In preparing this guide, EFC's Cybersecurity Best Practices Task Groups set out with the goal to provide an easy-to-use roadmap for industry organizations to improve their cybersecurity position. The Task Group recommends an all-encompassing resource from the Center for Internet Security (CIS) to help businesses map their cybersecurity strategy. CIS is a community-driven, not-for-profit organization that is responsible for the **CIS Controls**®, a set of 18 globally-recognized security controls that help mitigate prevalent cyber-attacks on systems and networks. The CIS Controls are comprehensive and encompass multiple legal, regulatory and policy frameworks.

Scan this QR code to view a brief video about CIS Controls

The 18 CIS Controls are shown below:

01	Inventory and control of enterprise assets	02	Inventory and control of software assets	03	Data protection
04	Secure configuration of enterprise assets and software	05	Account management	06	Access control management
07	Continuous vulnerability management	08	Audit log management	09	Email and web browser protection
10	Malware defenses	11	Data recovery	12	Network infrastructure
13	Network monitoring and defense	14	Security awareness and skills training	15	Service provider management
16	Application software security	17	Incident response management	18	Penetration testing

CIS Controls & Implementation Groups

The CIS Controls are *not* a one-size-fits-all solution. Rather, they are divided into **three distinct Implementation Groups (IG1, IG2, IG3)**. All organizations belong to an Implementation Group, based on their risk profile, resource capacity and budget – providing all companies with an accessible way to achieve cybersecurity. Each of the three Implementation Groups has an assigned a list of cyber-defense **safeguards** to help prioritize which practices are essential based on their capacity, budget and scale. There are 153 safeguards in total.

IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general non-targeted attacks.

Foundational level:
Captures the most critical and essential cyber 'hygiene'. Includes 56 basic cyber-defense safeguards

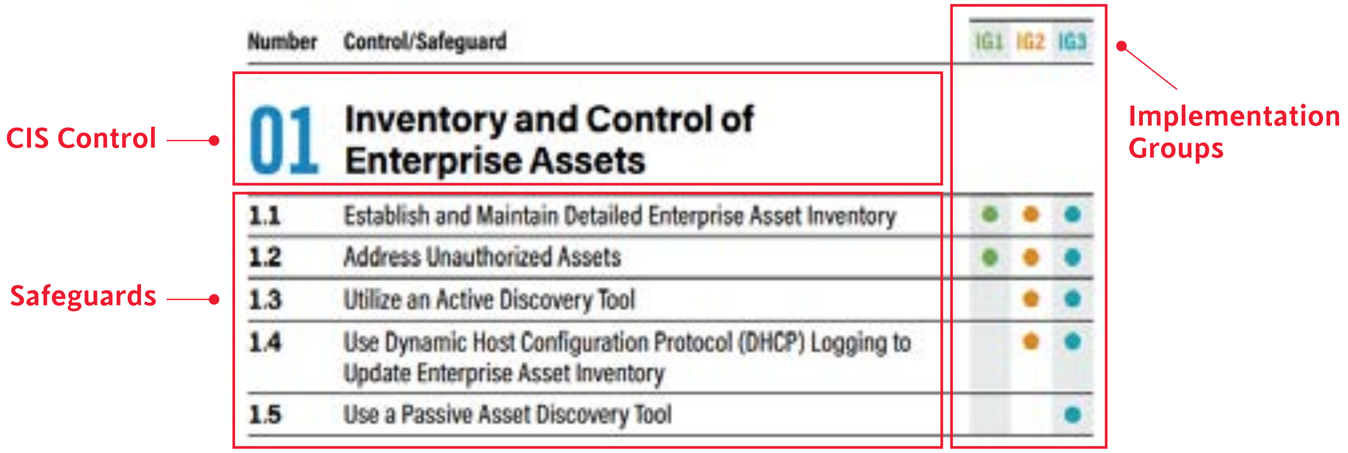
IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

Intermediate level:
Provides added layers of security and protection. Includes an additional 74 cyber-defense safeguards

IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

Advanced level:
Most comprehensive security protocols, comprising all 18 CIS Controls. Includes an additional 23 cyber-defense safeguards (captures all 153 in total)

To take this methodology one step further, the example below illustrates the first CIS Control and outlines a series of five safeguards, which are designated to relevant Implementation Groups:


CIS Control
Safeguards
Implementation Groups

Number	Control/Safeguard	IG1	IG2	IG3
01	Inventory and Control of Enterprise Assets			
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	●	●	●
1.2	Address Unauthorized Assets	●	●	●
1.3	Utilize an Active Discovery Tool		●	●
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		●	●
1.5	Use a Passive Asset Discovery Tool			●

Example of one CIS Control and the relevant safeguards and Implementation Groups

To view all 18 CIS Controls with relevant safeguards and Implementation Groups, access the Cybersecurity Toolkit (you will be prompted to enter your contact information for download access) (Note: EFC's Cybersecurity Task Groups have expanded the CIS Controls framework by flagging high-priority levels and providing a set of recommended tools to satisfy the safeguards).

CONDUCTING RISK ASSESSMENTS

A cybersecurity risk assessment describes the overall process or method used to identify risk factors that have the potential to cause harm to systems and networks. This assessment also involves analyzing and evaluating the risks to determine effective mitigation and prevention strategies.

The Center for Internet Security has developed two risk assessment tools to help assess your organization's security posture against the CIS Controls:

1. **CIS Controls Self Assessment Tool (CSAT):** a foundational method for organizations with limited resource capacity or technical knowledge. CSAT supports cross-departmental collaboration by allowing users to delegate questions to others, validate the responses and create sub-organizations. CSAT is free to every organization for use in a non-commercial capacity to conduct CIS Controls assessments of their organization. View FAQs
2. **Risk Assessment Method (CIS RAM):** an advanced method that provides instructions for modeling foreseeable threats against the CIS Controls as your organization applies them. The method is consistent with formal security frameworks and helps businesses "draw a line" between which risks are below the line ("due care"), and which are above the line (require risk treatment). Organizations can also use CIS RAM's 'Duty of Care' risk methodology to weigh the risks of not implementing the controls to gauge potential outcomes. Access the RAM workbook, which includes full instructions, examples, templates and exercises for conducting a cyber risk assessment.

Another risk assessment resource that companies can consider is from the Canadian Centre for Cybersecurity, developed in partnership with the Canadian Securities Exchange's internal audit team.

3. **Cybersecurity Audit Program:** features free tools to be deployed in sequence: Placemat, Audit Guide, Preliminary Survey Tool and Audit Program, all of which is available for use by Canadian organizations. No previous IT security audit knowledge is required for using the tools. Details
4. **Third-party Service Providers:** organizations can also hire third-party partner to conduct risk assessments and implement safety measures to protect assets. Risk assessment consultants are knowledgeable experts trained in the field of risk mitigation and strategy.

Ultimately, the risk assessment method you choose will depend on your resource capacity and budget. Here's a summary of the tools for consideration based on your Implementation Group:

Tools	Implementation Group 1	Implementation Group 2	Implementation Group 3
CIS CSAT	X		
CIS RAM	X	X	X
Cybersecurity Audit Program	X	X	
Risk Consultant		X	X

Finally, even with the best laid assessments plans, it's also important to invest in an insurance plan to complete your cybersecurity strategy. Cybersecurity insurance protects your organization from potential financial risks associated with cyber-attacks (such as breaches, ransomware, DDoS attacks and regulatory compliance).

EFC CORPORATE PARTNERS

Ignite provides customized risk assessments and analytic strategies to boost cyber resilience. Learn more

Lawrie Insurance is an independent broker that has certified risk managers who will create plans to provide comprehensive cybersecurity coverage. Learn more

CYBERSECURITY TAKES A COMMUNITY

Developing and deploying a cybersecurity strategy must be a priority for every organization – extending to all employees within a company as well as all customers and partners that are part of the value chain. A cybersecurity plan will only be as strong as its weakest link. Therefore, protecting business systems and networks takes collaboration and communication across the market.

Help support your customers with their cybersecurity roadmap by sharing this industry resource guide so they can take an actionable approach to secure their systems – which by extension, will help protect your data and network assets.

RESOURCES

The following are quick links to resources shared in this guide as well as other information to help springboard and/or strengthen your cybersecurity strategy:

EFC's library of cybersecurity resources

Canadian Centre for Cyber Security

CIO Strategy Council

CIS Center for Internet Security

Data Governance Institute

IBM: Cost of Data Breach Report (2021)

Office of the Privacy Commissioner of Canada: Mandatory Reporting of a Data Breach

Public Safety Canada

If you have any questions about this resource guide, please contact EFC at **info@electrofed.com**

This resource guide is for informational purposes only and was prepared by Electro-Federation Canada (EFC) with support from the Cybersecurity Best Practices and Cybersecurity Measures of Success task groups, comprising IT experts from the Canadian electrical industry. EFC, nor any of the task group members, make any warranty—expressed or implied—or assume any legal liability or responsibility for any loss or damage suffered. This resource guide is for EFC members and respective customers and partners only. www.electrofed.com