ELECTRO FEDERATION CANADA

ACHIEVING A SECURE STATE:

Cybersecurity Best Practices IT Resource Guide

INTRODUCTION

Achieving a secure state for your IT environment takes time, investment, collaboration and resources. Multiple layers of protection across computers, networks and programs, along with well-established safety protocols, are critical to ensuring your organization is continually 'cybersafe'.

EFC's Cybersecurity Best Practices and Cybersecurity Measures of Success task groups, comprising IT experts from our industry, have developed this guide as a roadmap to steer your organization's cybersecurity priorities and investments. This report provides best practices and guidance on:

- Establishing a shared vision for outcomes with executive leaders
- Uncovering different types of cybersecurity threats
- Understanding the business implications of cyber-attacks
- Considerations for cybersecurity investments
- Nine key pillars for cybersecurity planning
- Charting and mobilizing your cybersecurity journey
- Employing a risk assessment method that's right for your business

Toolkit of Resources

To supplement this guide, EFC has assembled a toolkit of other resources to help your organization plan, prepare and improve your cybersecurity strategy. The toolkit includes:

1. A sample presentation framework to share with your executive team to establish common ground for cybersecurity planning
2. An executive summary to share with your executive leadership team to level-set their understanding of cybersecurity threats and actionable approaches
3. A full framework detailing 18 cybersecurity controls with actions and tools to safeguard your company (developed by the Center for Internet Security)

These resources are available for download – follow this link (note: you will be prompted to enter your contact information to protect the security of these resources. The information will not be used for solicitation purposes).

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. Often, there is a division of understanding between executives and IT leaders; executives might be unfamiliar with the types of cyber threats and system requirements, while IT teams might be unaware of business and financial implications.

The following chart outlines common questions that executives and IT teams can address together to interpret and define a cybersecurity business 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?

Download the sample presentation framework to establish a common ground for cybersecurity planning with your executive team.

TYPES OF CYBERSECURITY THREATS

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 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 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.

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 **$200,000**

The average downtime after an attack is **21 days**

Only 8% of victims who pay up recover all encrypted files

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

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

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

BUSINESS IMPLICATIONS OF CYBER-ATTACKS

Cyber-attacks directly impact a company's bottom line, yet many leaders are unaware of the **cost of inaction** to their organization.

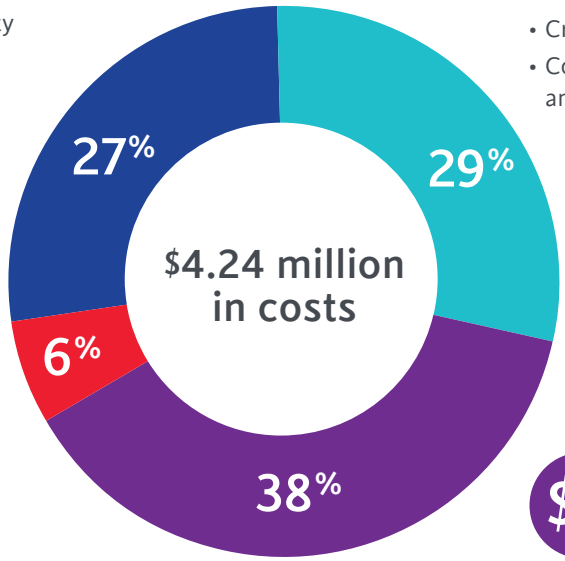
According to an IBM study, businesses that fall victim to security breaches can incur $4.24 million in costs, on average, largely attributed to four factors: **post-breach response costs, detection and escalation costs, notification costs, and lost business costs.**

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.[2]

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.

[2] 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)

CONSIDERATIONS FOR CYBERSECURITY INVESTMENTS

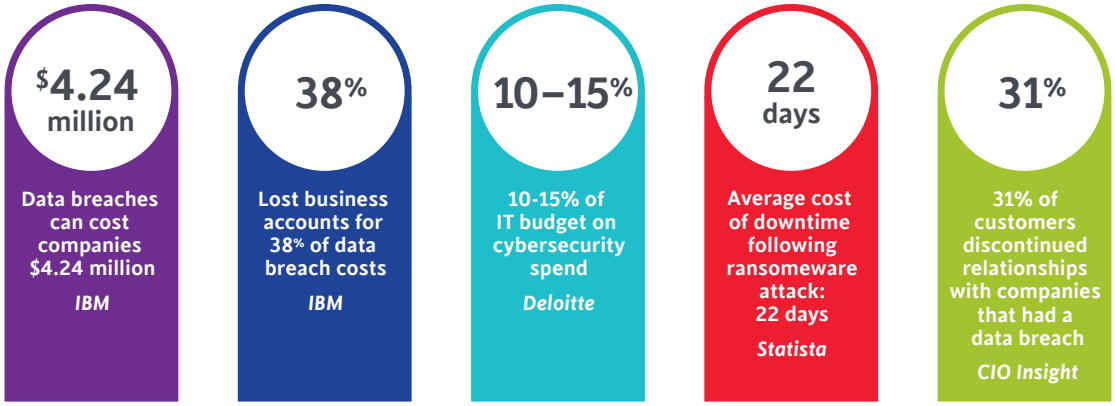
Cybersecurity is an investment in risk mitigation; it is an actionable approach to protecting systems and applications from malicious attacks. When it comes to Cybersecurity investments, ROI is not the metric to track. If your company maintains a secure state with a well-planned recourse plan when a 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.[3] (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.[4] 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.

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

The cost of inaction can be substantial – outlined below, is a snapshot of the key implications and measures to consider as your organization builds out its cybersecurity action plan:



The investment in cybersecurity is critical. It is also wide-ranging; cybersecurity planning 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.

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:

CYBERSECURITY BEST PRACTICES	ACTIONABLE STEPS
1 **Empower Your Security Team:** ensure that the person leading the security team has the ear of the business leader and not just the IT leader. Give them the budget and resources commensurate with the risks and the tools needed to mitigate the risks that your company faces.	
2 **Endpoint Protection:** this practice involves securing devices such as desktops, laptops, mobile devices and servers from cyber threats. This level of protection typically includes software programs that are installed on devices and centrally- managed by security administrators to protect endpoints on a network (or on the Cloud) from cybersecurity threats. Endpoint security has evolved from traditional anti-virus software to modern machine learning-based threat detection systems that provide comprehensive protection from sophisticated malware threats. Many systems offer automatic responses that not only flag malware but also shut it down completely to prevent further spread.	✓ Review software to ensure all devices on the network are updated with the latest updates from the provider. ✓ Implement staff training to help users identify threats and understand how to report suspected threats. Test and track user activity to monitor progress.
3 **Network and Perimeter Protection:** represents the most important and basic lines of defense as these systems filter and examine the packets that flow in and out of the corporate network as well as between different components or branches of the network. Firewalls are a primary example of these systems. Firewalls are your first (inbound traffic) and your last (outbound traffic) lines of defense. Other systems include Intrusion Detection Systems (IDS), which monitor network traffic and provide remediation tactics when malicious behaviour is detected, and Behavior Monitoring Systems which use machine learning algorithms to track network traffic and flow between systems to establish a baseline of normal activity and then look for anomalies.	✓ Conduct regular Intrusion Detection Systems (IDS) tests to analyze network traffic for signatures that match known cyberattacks. ✓ Isolate networks with sensitive information. ✓ Implement URL filtering. ✓ Deploy anti-spam and email filtering. ✓ Secure Wi-Fi networks (access control, encryption).

4 **Account & Identity Management:** this involves the implementation of tools and processes that grant, restrict, monitor and remove user-level access to protected information, systems or assets within an organization. This is a security framework that authenticates and authorizes 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.

Multi-Factor Authentication (MFA) is an example of this type of management. It involves an authentication method that requires users to provide their username and password as well as another identify verification method (e.g., entering a code or acknowledging a prompt sent to their smartphone). Given the relative ease with which passwords can be hacked or stolen, MFA remains the most reliable way to verify user identity before granting access to corporate systems and data. Password managers are another protocol to be considered, which encrypts and safely stores user passwords, recalling them as needed.

- ✓ Develop processes and technical controls to manage users and accounts.
- ✓ Centralize systems and tools to minimize the complexity of managing user accounts.
- ✓ Ensure end-point devices or user identities are verified frequently when accessing systems and sensitive data.
- ✓ Prevent unauthorized access to sensitive information by limiting user privileges to only the areas that they need.
- ✓ Secure user accounts that have access to sensitive data with MFA.
- ✓ Audit user access to protect against unauthorized escalation of privileges, and the removal of inactive accounts.

5 **User Education and Security Awareness:** training provides formal cybersecurity education to your workforce so they can assess potential security threats. Security awareness training is most useful when approached as a critical ongoing practice and included in individual and corporate objectives. Formal training programs from third-party providers are designed to engage and test users and also provide IT administrators with feedback on potential user weaknesses/threats. In addition to formal training platforms, security awareness can also be shared through webinars, lunch and learn sessions, and other internal programs to reinforce knowledge and create a culture of cybersecurity in the organization.

With training, organizations should also consider security policies that include a framework of definitions, rules, processes and expected behaviours that need to be followed in order to make the organization more secure. The policies must be circulated to everyone in the company and needs to be reviewed and updated regularly.

- ✓ Simulate a variety of phishing attacks using e-mail campaigns that are similar to real-life hacking attempts.
- ✓ Create a baseline score to measure the effectiveness of training programs and to identify areas that require more attention.
- ✓ Track and measure multiple metrics to monitor staff's security awareness, such as the number of phishing incidents, malware infection rates and user actions.
- ✓ Regularly review test email campaigns to ensure it is relevant and effective.

6 **Incident Response Plan & Recovery:** this involves a set of instructions designed to help companies prepare for, detect, respond to, and recover from major security incidents. Most plans are technology-centric and address issues such as malware detection, data theft and service outages. However, any significant cyber-attack can affect an organization across functions in multiple ways, so the plan should also encompass HR, finance, customer service, internal communications, legal, insurance, public relations, regulators, suppliers, partners, local authorities and other entities. The main objectives are to minimize damage, protect your data and reputation, and to help your organization recover from an incident as quickly as possible. Some organizations may be legally required to have an Incident Response Plan in place, for instance, as part of PCI-DSS compliance.

- ✓ Create a secure backup plan and incident response plan and review both periodically (Note: there are several industry-standard incident response frameworks (e.g. NIST and SANS) that provide general guidelines on how to respond to an active incident. However, your organization's plan should be much more actionable, detailing who should do what, and when.
- ✓ Test the restore procedures, evaluate timeframes and adjust accordingly.
- ✓ Identify key resources and clarify roles (response team).
- ✓ Prepare a communications plan, and list contact information (internal, partners, law enforcement).
- ✓ Secure an alternate location for storing key contact info and critical docs.
- ✓ Build partnerships with a breach coach, forensic experts, public relations firm and legal counsel.

7 **Measure, Monitor, Assess & Control:** it is critical to continually observe and test IT networks, systems, data usage, applications, and infrastructure in order to proactively detect vulnerabilities, potential threats or breaches is cyber monitoring. Testing methods include:

(continued on next page)

- ✓ Conduct a vulnerability assessment to gain a systematic review of security weaknesses in information system.

Vulnerability Assessment and Penetration Testing (VAPT): the most common type of testing that involves having a trained professional detect and exploit vulnerabilities in your systems and networks to identify insecure business processes and security settings.

Security Information and Event Management (SIEM) platform: centralizes all audit logs and security data, and conducts forensic analysis to identify malicious incidences.

Security Operation Center (SOC): a centralized function within an organization that is the central command post, continuously monitoring an organization's security posture by preventing, detecting, analyzing, and responding to cybersecurity incidences. Essentially, the SOC is the correlation point for every event logged within an organization that is being monitored.

To establish the scope of cyber testing, assess your IT ecosystem as such:

- Which IT systems are essential for operating your business and cannot sustain any downtime?
- If there are vulnerabilities in your system, which ones might be the most exploitable?
- Are there any loopholes in your network that are easily discoverable by external people?

✓ Refer to the Common Vulnerability Scoring System (CVSS) or National Vulnerability Database (NVD) to explore which vulnerabilities are present (do not differentiate between flaws that can be exploited to cause damage and those that cannot.

✓ Conduct a penetration test to simulate a cyber-attack against your systems to check for exploitable vulnerabilities.

✓ Identify which flaws pose a threat to the application and measure the severity of each.

8

Data Loss Prevention (DLP), Data Privacy: refers to a set of tools and processes that protect sensitive data from becoming lost, misused or accessed by unauthorized users. DLP software classifies regulated, confidential and business critical data and identifies violations of policies defined by organizations or driven by regulatory compliance such as HIPAA, PCI-DSS, or GDPR. If violations are identified, DLP enforces remediation with alerts, encryption and other protective actions. DLP provides reporting to meet compliance and auditing requirements and identify weaknesses and anomalies for forensics and incident response.

✓ Implement data sensitivity classifications.

✓ Develop data access policies, roles and responsibilities.

✓ Secure encryption and segregation.

✓ Establish plans for data loss prevention and alerting.

✓ Comply with relevant regulatory legislation.

9

Application Security: this practice involves finding, fixing and improving the security of applications. Much of this happens during the development phase, but it includes tools and methods to protect applications once they are deployed. There are several approaches that can be taken to uncover security vulnerabilities in applications:

Design review: before code is written, the application's architecture and design can be reviewed for security problems. A common technique in this phase is the creation of a threat model.

Whitebox security review (code review): a security engineer analyzes the application by reviewing the source code and searching for security flaws.

Blackbox security audit: probing the application from the outside to determine security vulnerabilities; no source code is required.

Automated testing: includes three types of tools – static testing analyzes code at fixed points during its development; dynamic testing analyzes running code to simulate attacks on production systems and reveals complex attack patterns that use a combination of systems; and interactive testing, which combines elements of both static and dynamic testing.

Web application security and mobile applications security: branches of application security that deal specifically with securing websites, web applications, web services and mobile applications.

- ✓ Implement secure application development practices.
- ✓ Organize awareness training for developers.
- ✓ Deploy security testing tools for applications, web applications and mobile applications.
- ✓ Run security checks and reviews prior to selecting third-party applications and solutions.

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

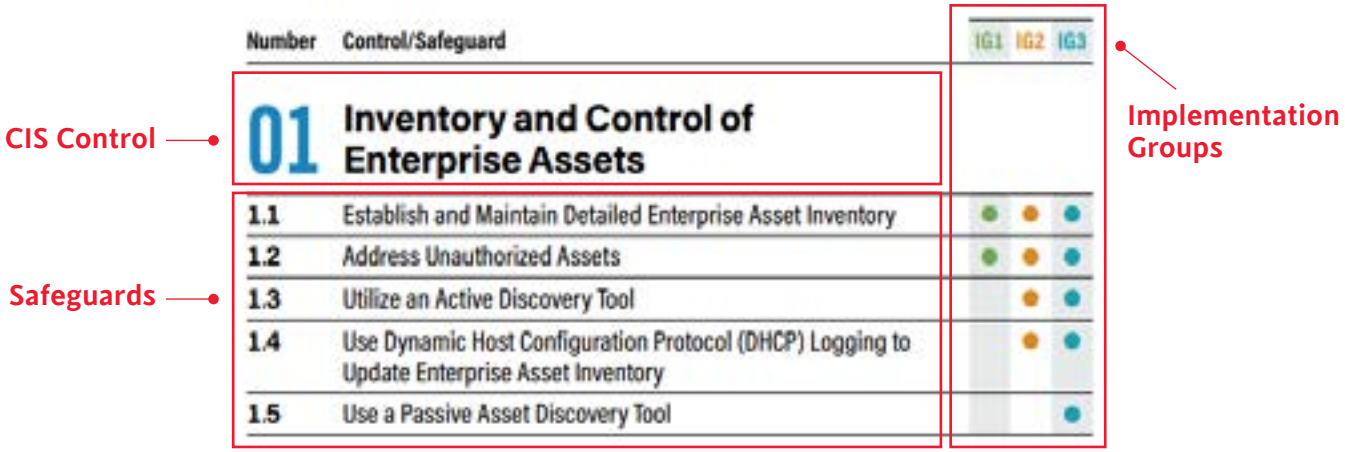
IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

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:



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

BUILDING BRIDGES: KEY CYBERSECURITY PILLARS & CIS CONTROLS

Earlier in this document, you learned about the nine pillars that should form the basis of your cybersecurity plan.

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

It is important to build bridges between the nine pillars and the 18 CIS Controls. Here's how these frameworks interplay:

Pillars	CIS controls
1 Empower the security lead and team	Ensure IT team has the budget, tools and resources to protect your company's data and systems from security risks.
2 Endpoint protection	4: Secure configuration of enterprise assets & software 10: Malware defenses
3 Network perimeter protection	9: Email & web browser protection 12: Network infrastructure management 13: Network monitoring & defense
4 Account & identity management	5: Account management 6: Access control management
5 User education and security awareness	14: Security awareness & skills training
6 Incident response plan & recovery	11: Data recovery 17: Incident response management
7 Measure, monitor, assess, control	1: Inventory & control of enterprise assets 2: Inventory and control of software assets 7: Continuous vulnerability management 8: Audit log management 18: Penetration testing
8 Data loss prevention, data privacy	3: Data protection
9 Application security	15: Service provider management 16: Application software security

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**