CYBERSECURITY

Achieving a Secure State for IT Environments

ELECTRO
FEDERATION
CANADA
EFC

Cybersecurity is essential for today’s connected world.

ELECTRO FEDERATION CANADA EFC

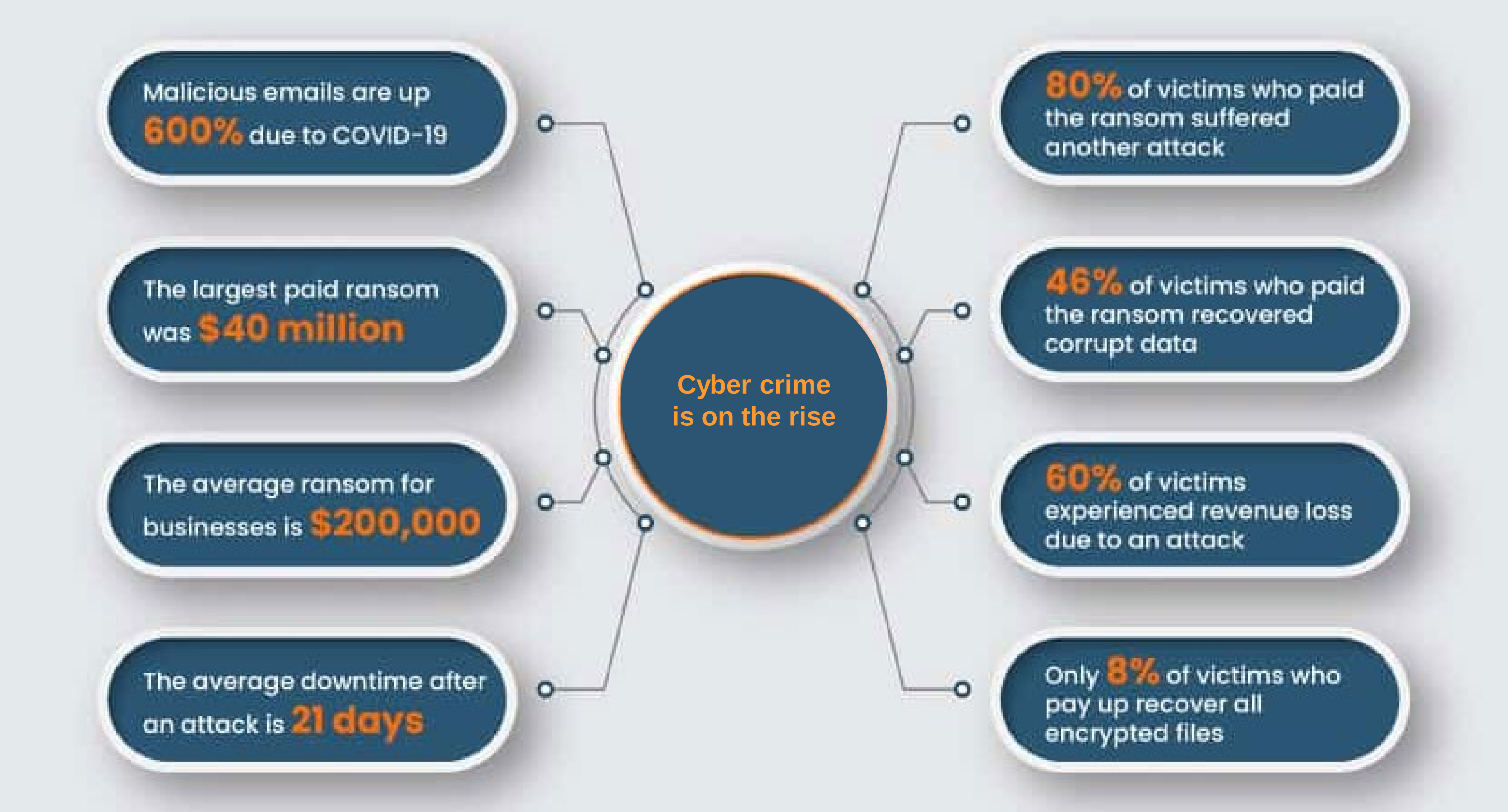
Every facility can become the target of **cyber crime**…
businesses, factories, banks, institutions, homes and electricity transmission grids

What is Cyber Crime?

Malicious activity during which the internet, computers, tablets or mobile devices are used to commit a criminal offense.

Typically aimed at:

- ✓ accessing, changing or destroying sensitive data
- ✓ extorting money from people
- ✓ interrupting normal business processes



Cyber crime is on the rise

Malicious emails are up **600%** due to COVID-19

The largest paid ransom was **$40 million**

The average ransom for businesses is **$200,000**

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

80% of victims who paid the ransom suffered another attack

46% of victims who paid the ransom recovered corrupt data

60% of victims experienced revenue loss due to an attack

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

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

‘Organizations must assess the risks to information and systems with the same vigor they would for legal, regulatory, financial or operational risks.’

National Cybersecurity Centre (U.K.)

Getting Started Takes a Shared Vision

ELECTRO
FEDERATION
CANADA
EFC

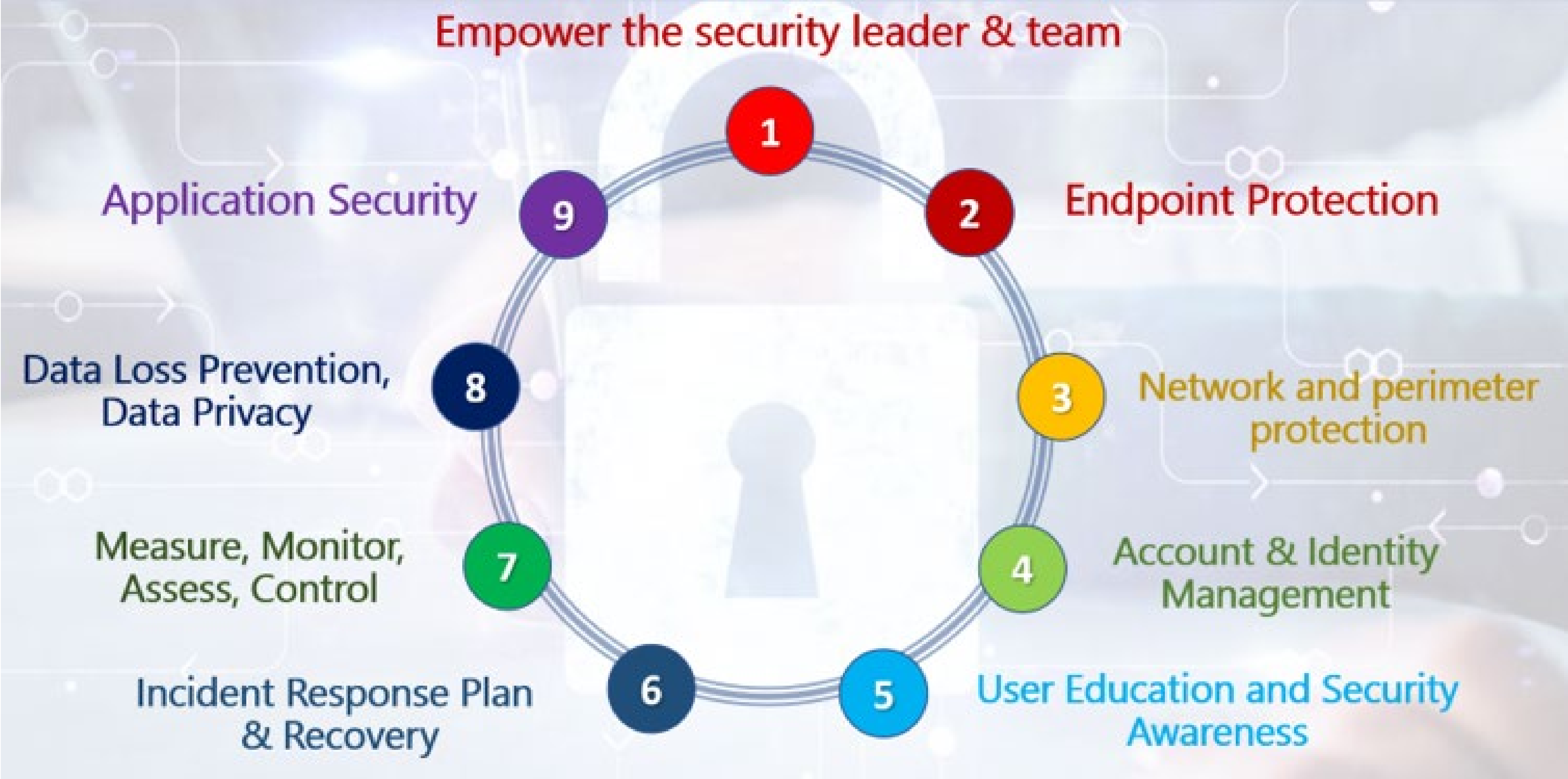
Questions to Address: IT and Executive Teams

ELECTRO FEDERATION CANADA EFC

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?

Cybersecurity Planning

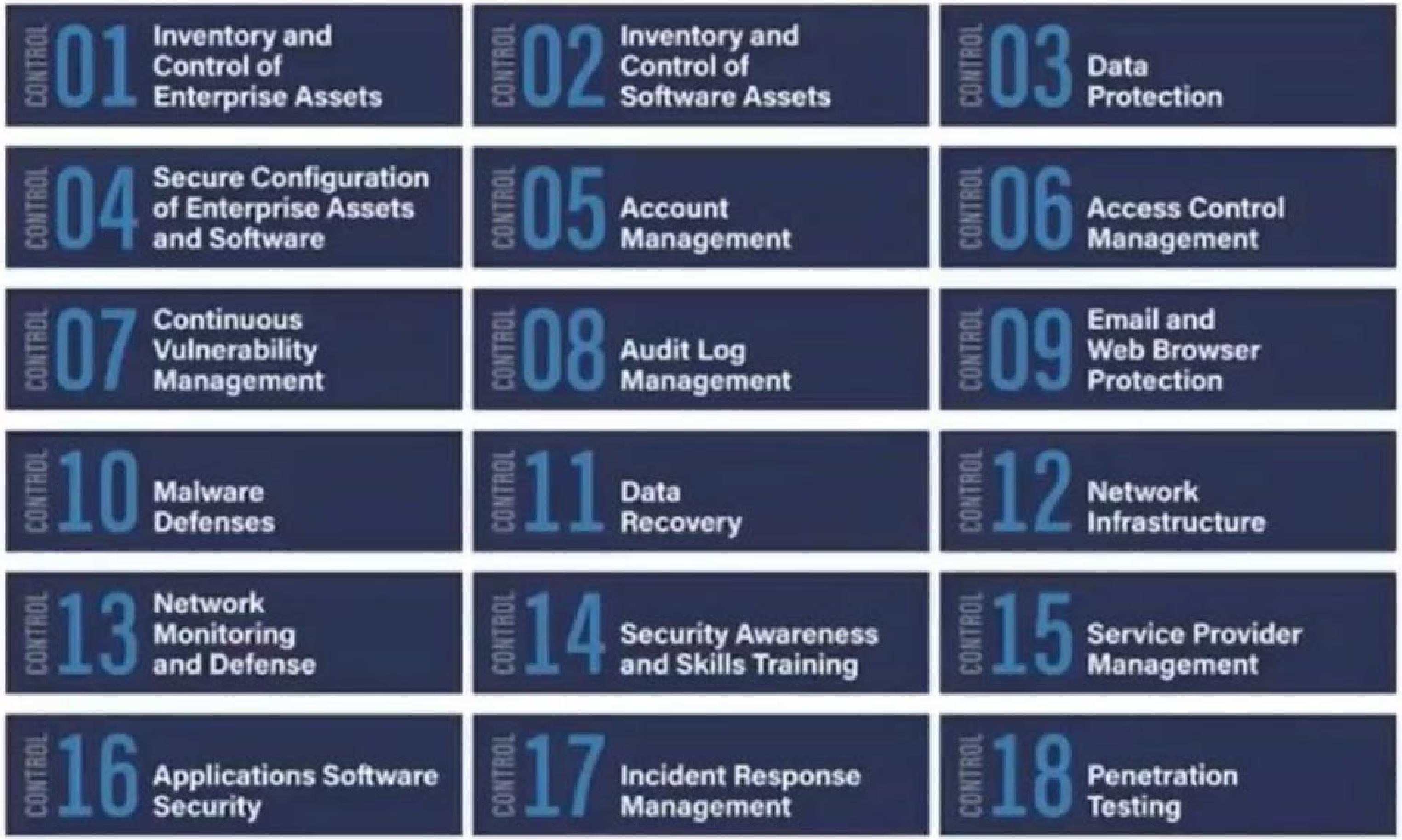
Nine Pillars for Cybersecurity Planning



Empower the security leader & team
1
2
Endpoint Protection
3
Network and perimeter protection
4
Account & Identity Management
5
User Education and Security Awareness
6
Incident Response Plan & Recovery
7
Measure, Monitor, Assess, Control
8
Data Loss Prevention, Data Privacy
9
Application Security

Each Pillar Coincides with CIS Controls®

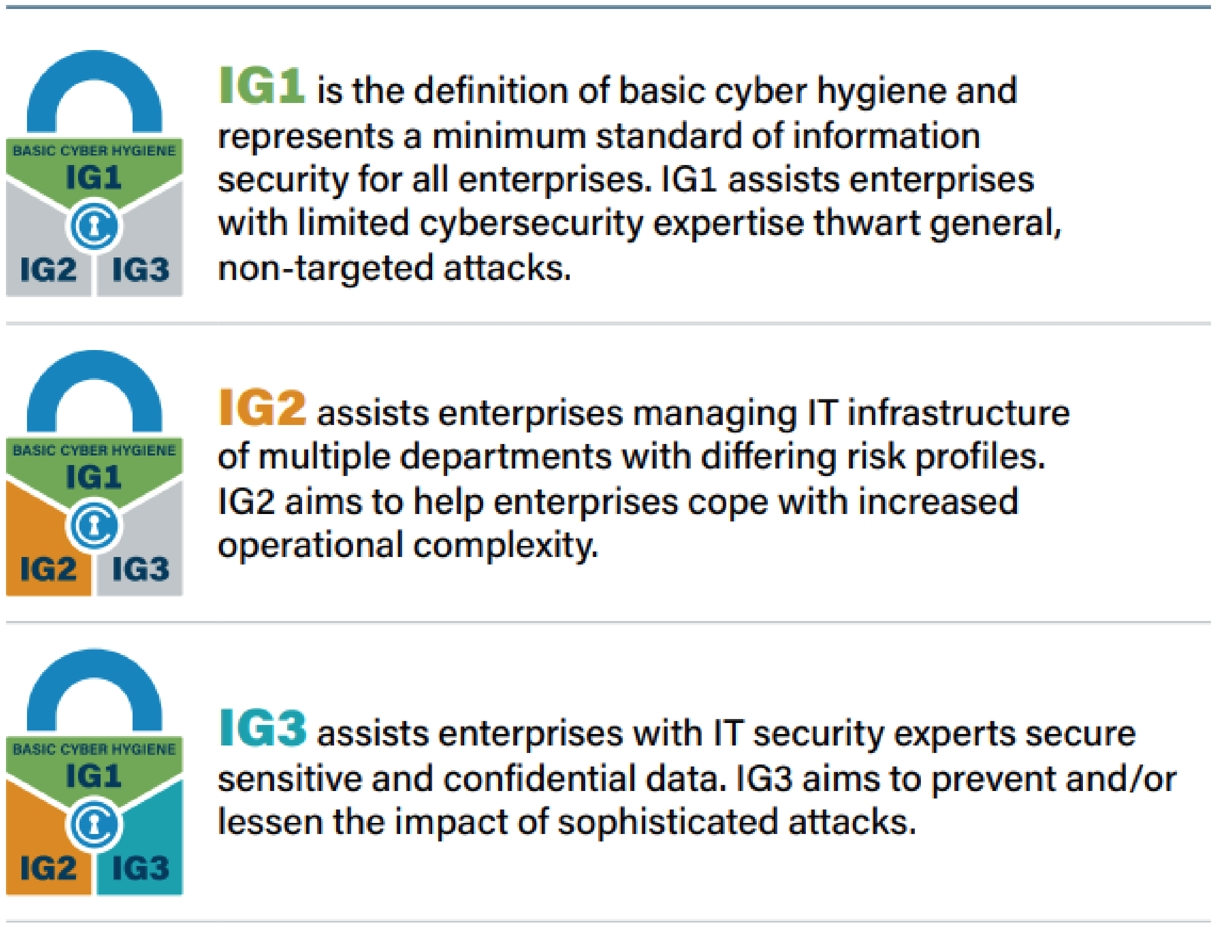
CIS Controls = 18 globally-recognized security controls developed by the Center for Internet Security (CIS) to help mitigate prevalent cyber-attacks on systems and networks.



CONTROL 01 Inventory and Control of Enterprise Assets	CONTROL 02 Inventory and Control of Software Assets	CONTROL 03 Data Protection
CONTROL 04 Secure Configuration of Enterprise Assets and Software	CONTROL 05 Account Management	CONTROL 06 Access Control Management
CONTROL 07 Continuous Vulnerability Management	CONTROL 08 Audit Log Management	CONTROL 09 Email and Web Browser Protection
CONTROL 10 Malware Defenses	CONTROL 11 Data Recovery	CONTROL 12 Network Infrastructure
CONTROL 13 Network Monitoring and Defense	CONTROL 14 Security Awareness and Skills Training	CONTROL 15 Service Provider Management
CONTROL 16 Applications Software Security	CONTROL 17 Incident Response Management	CONTROL 18 Penetration Testing

CIS Controls & Implementation Groups

Each organization belongs to an Implementation Group (based on their risk profile, resource capacity and budget)


BASIC CYBER HYGIENE
IG1
IG2
IG3

Foundational level

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.

Intermediate level

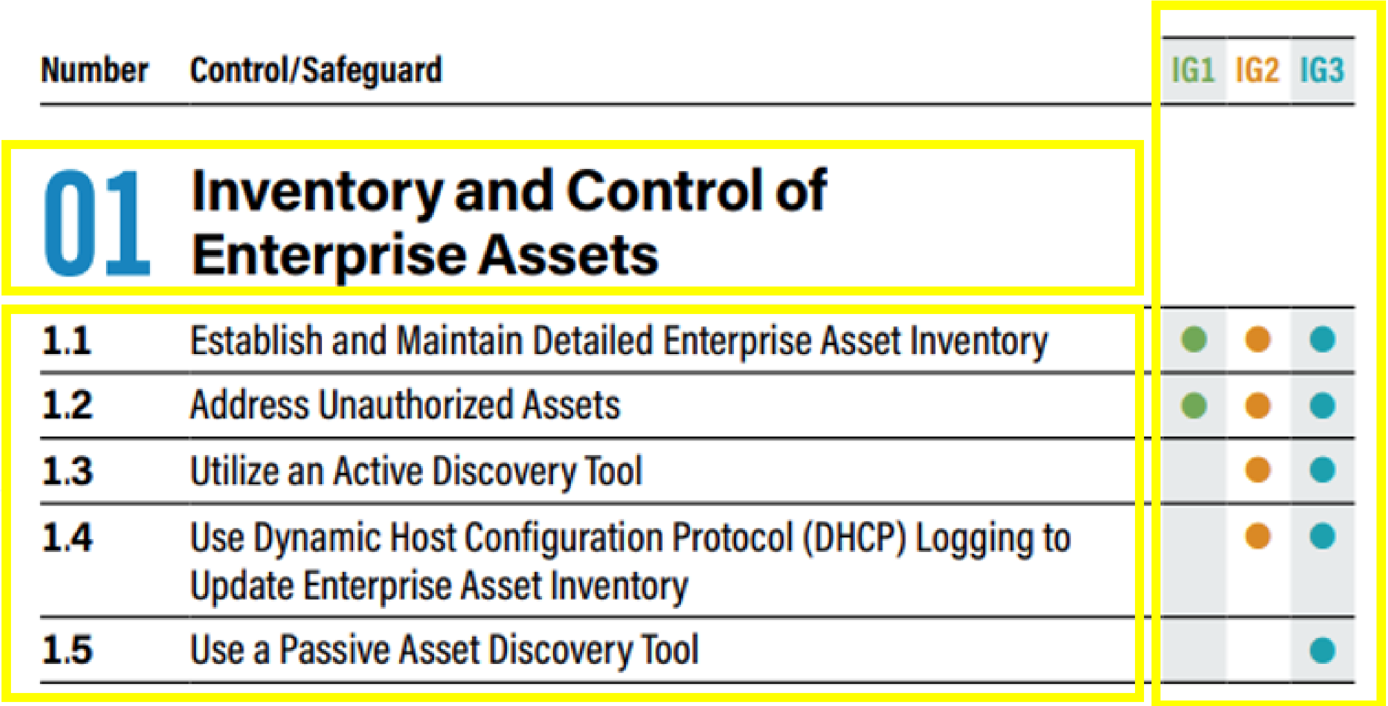
IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

Advanced level

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

Example: CIS Controls & Implementation Groups

This example shows the first CIS Control which includes five safeguards that 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			●

CIS Control

Safeguards

Implementation Groups

Download all 18 CIS Controls with listed safeguards and Implementation Groups at: www.electrofed.com

Cybersecurity planning involves a phased approach

PHASE
PHASE
PHASE

CIS Controls Implementation

Risk Assessment / Penetration Test

Disaster Recovery & Business Continuity Plan

Each phase requires collaboration, planning, resources and investment.

Cybersecurity is an Investment in Risk Mitigation

There is not a one-size-fits-all budget for cybersecurity operations

Investments may be higher for *smaller companies* because of scale or volume considerations

Companies should expect to spend **10-15% of their IT budget*** on cybersecurity

EFC Cybersecurity Task Group recommendation based on industry benchmarks and cross-sector research

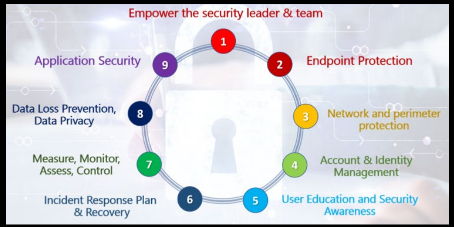
On average, businesses experience **22 days of downtime*** due to a cyberattack, resulting in substantial lost sales

*Source: Statista

ELECTRO FEDERATION CANADA EFC

Charting Your Cybersecurity Journey

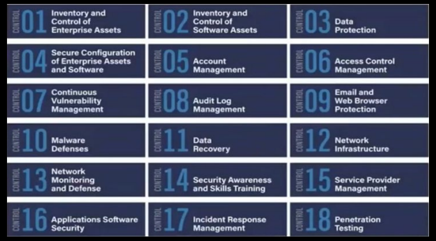
Review the **nine pillars of cybersecurity planning** and assess your company's status within each.


Empower the security leader & team
1
2
Endpoint Protection
3
Network and perimeter protection
4
Account & Identity Management
5
User Education and Security Awareness
6
Incident Response Plan & Recovery
7
Measure, Monitor, Assess, Control
8
Data Loss Prevention, Data Privacy
9
Application Security

Identify which **CIS Implementation Group** your company belongs to.
Our organization is mapped to Implementation Group X

BASIC CYBER HYGIENE
IG1
IG2
IG3

Review the **CIS Controls** for your Implementation Group and identify gaps, investment, resources and timing for deployment of safeguards.



CONTROL 01 Inventory and Control of Enterprise Assets	CONTROL 02 Inventory and Control of Software Assets	CONTROL 03 Data Protection
CONTROL 04 Secure Configuration of Enterprise Assets and Software	CONTROL 05 Account Management	CONTROL 06 Access Control Management
CONTROL 07 Continuous Vulnerability Management	CONTROL 08 Audit Log Management	CONTROL 09 Email and Web Browser Protection
CONTROL 10 Malware Defenses	CONTROL 11 Data Recovery	CONTROL 12 Network Infrastructure
CONTROL 13 Network Monitoring and Defense	CONTROL 14 Security Awareness and Skills Training	CONTROL 15 Service Provider Management
CONTROL 16 Applications Software Security	CONTROL 17 Incident Response Management	CONTROL 18 Penetration Testing

Continually engage with internal & external stakeholders to provide cybersecurity progress updates.

ELECTRO FEDERATION CANADA EFC

ELECTRO
FEDERATION
CANADA
EFC

Access EFC’s full library of cybersecurity resources:
www.electrofed.com