DSi INTERNATIONAL SECURITY DIVISION

Protect your organizations against cyber threats

US$ 6 trillions

in direct, indirect cost and revenues for cybercriminals in 2021. Equivalent GDP of the world's third largest economy.

(WEF Global Risk Report 2020)

42%

of Canadians are victims of cyber attacks, phishing, fraud, malware, hacking of online accounts.

(StatCan, September 2020)

4 times more

cyber attacks since the beginning of the pandemic. A frightening and continuously rising stats.

(FBI, 2020)

> *"The threat landscape has changed, but more importantly, the pandemic has created an environment of anxiety and uncertainty that cyber criminals exploit. Now more than ever, cybersecurity is a concern organization cannot ignore."*
>
> Jacques Latour, Chief Technology Officer CIRA

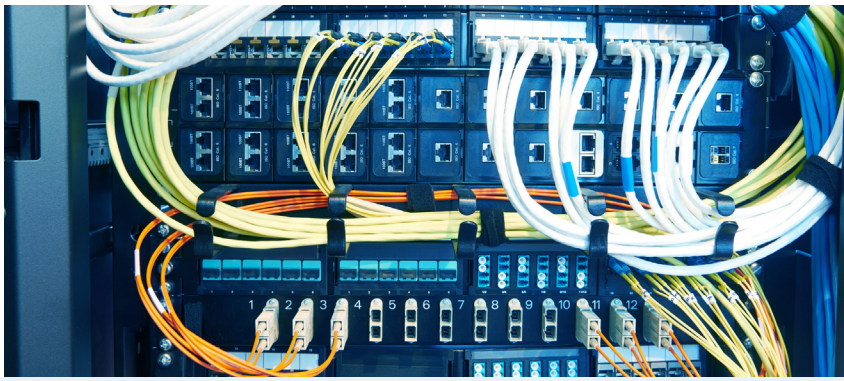
Undergoing a cyber attack means you expose yourself to multiple risks.

- Personal and confidential data loss.
- Financial loss (ransom, investigation, prevention).
- Time loss (daily activities and operations shutdown).

It is now crucial to review the security state of your organization in order to take all possible precautions.

Together, let's set up a good security hygiene for your organization.

- Fraud prevention.
- Protection of your organization's reputation.
- Protection of personal data theft and confidentiality of employees, students, parents, partners and providers.



Take advantage of our adapted and above all affordable 360° service offer.

Our objective : democratize the security industry.

Division Sécurité International (DSI), composed of 13 founding members, provides to you a variety of specialists from all sectors of security in order to offer you optimized 360° solutions. Our expertise includes cybersecurity, protection of individuals and data, as well as physical security.

Vulnerabilities tests
Determination and elimination potential security exposures
Implementation of appropriate controls

Setting up of an action plan and deployment
Determination of objectives and desired security infrastructure according to the appropriate deadlines

Assessment of current security posture
Policies and procedures review (technologies and human)

Protection of infrastructure and information systems
Acquisition of hardware and computer equipment
Acquisition of software

Cybersecurity education*
Cyberthreats training for employees
Strategic cybersecurity training for executives
Crisis simulation (phishing, cybersecurity)

* Accredited trainings by EC-Council and PECB in Cybersecurity and ISO Compliance

Service offer

Phase 1 – Define the current security context and document the needs including physical, information and technology protection assets

Continuation of needs analysis

- Inventory of assets (Human, Physical, Procedures, Technologies, Infrastructures et Partnerships).
- Documentation of existing relationships between processes and technologies (Data Flow).
- Analyze the “flow” and produce a functional architecture (High level).
- Discuss and promulgate the applicable recommendations with the person in charge.
- Document and record the decisions and orientations adopted.
- Document the current security posture with a gap analysis against the established target.

DSI INTERNATIONAL SECURITY DIVISION

info@dsi.group
www.dsi.group