Everywhere you export

The Canadian Trade Commissioner Service

SPOTLIGHT ON CYBERSECURITY

TCS

Global Affairs Canada
Trade Commissioner Service

Affaires mondiales Canada
Service des délégués commerciaux

Canada

Engaging in cybersecurity practices protects one's self and one's business from the threats of cyber-crime, identity theft, and other dangers of operating online.

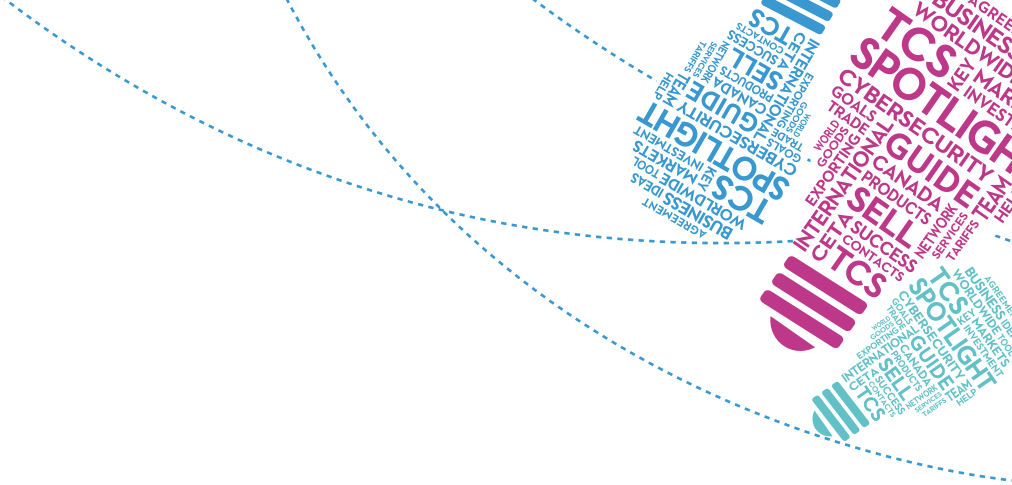
The following *Spotlight on Cybersecurity* is intended to provide Canadian exporters with the background knowledge and tools necessary to protect their business against cyber threats. From understanding who commits cyber-crimes and their motives, to what can be done to prevent them, this short guide can help you to understand and employ cybersecurity measures.

Did you know?

In 2016, there were nearly 24,000 cyber-related violations reported in Canada.

Source: **StatsCan**

Table of contents



What is cybersecurity?

Cybersecurity is generally understood to encompass any measure taken to protect online information and any asset connected to a network (e.g. data, information, hardware, among others), and secure the infrastructure on which it resides.

The Canadian Trade Commissioner Service (TCS) is pleased to introduce the following *Spotlight on Cybersecurity* to help Canadian exporters to take preventative measures to mitigate risks and protect their interests digitally or in person when conducting business outside of Canada and engaging in commercial exchanges with potential buyers, suppliers or partners.

Marketplaces

Cyberspace is the electronic world created by interconnected networks where more than three billion people are linked together. Canadians are embracing cyberspace (88.5% of Canada's population uses the internet). The worldwide embrace of cyberspace in recent decades, though, has not come without its dangers. One's personal or professional data online might be compromised by a cyber-attack. ***Cyber-attacks*** include the unintentional or unauthorized access, use, manipulation, interruption, or destruction of electronic information and/or the electronic and physical infrastructure used to process, communicate, and/or store that information. Therefore, it is important for users of cyberspace to protect themselves against potential cyber-attacks – efforts to do this fall under the term cybersecurity.

Return to Table of Contents

Common cyber-attacks:

- ***Phishing*** involves sending emails to large numbers of people asking for sensitive information or encouraging them to visit a fake website;

- ***A watering hole*** involves setting up a fake website or compromising a legitimate one in order to exploit visitors;

- ***Ransomware*** may include disseminating disk encrypting extortion malware;

- ***Spear-phishing*** involves sending emails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software; and

- Deploying a ***botnet*** may involve delivering a DDOS (Distributed Denial of Service) attack or subverting the supply chain to attack equipment or software being delivered to the organization.

Tips and tricks to safeguard against cyber-attacks:

- **Your password** – One hacker reported that the way he entered most secured websites was by exploiting people's weak passwords. Passwords should be at least eight characters in length; include a combination of numbers, letters, and symbols; and not be words related to you.

- **Keep it safe** – Don't allow others to access your password protected sites without you being present. After they do, change your password. Even the most well-meaning person can accidentally make you the victim of a cyber-attack if their computer is infected.

- **Go low tech** – If you have a spreadsheet of passwords or other digital files that are highly sensitive, consider keeping them on an old computer not connected to the Internet. If you don't have an extra computer, encrypt the files using one of the many free file encryption tools.

Return to Table of Contents

- **Two places** – another layer of protection could involve keeping the files in two locations. Copy the encrypted files to a flash drive. If your computer is infected by a virus and temporarily unusable, those files are still available to you.

- **Don't fall for a pop-up** – If an e-mail or pop-up window asks you to enter your username or password, don't do it. Instead, open your browser and go to the site directly. Reputable companies will never ask you for your login information through an e-mail.

Did you know?

You can insure your business against cyber-attacks. Cyber liability insurance will help you handle the associated costs that come along with a breach.

Sector focus:

Manufacturing

Manufacturers are increasingly being targeted, not just by traditional malicious actors such as hackers and cyber criminals, but by competing companies and nations engaged in corporate espionage. Motivations range from money and revenge to competitive advantage and strategic disruption. Auto manufacturers were the top targeted manufacturing sub-industry, accounting for approx. 30% of total attacks against the industry in 2015.

Return to Table of Contents

Understanding cyber threats

Most cyber-attacks share four (4) common characteristics that account for their growing popularity (among hackers) and their increase in the frequency of occurrences.

- **Inexpensive** – many attack tools can be purchased for a modest price or downloaded for free from the internet.
- **Easy** – attackers with only basic skills can cause significant damage.
- **Effective** – even minor attacks can cause extensive damage.
- **Low risk** – attackers can evade detection and prosecution by hiding their tracks through a complex web of computers and exploiting gaps in domestic and international legal regimes.

Did you know?

Hackers do not just focus on large corporations. Small and medium-sized enterprises (SMEs) are commonly targeted as they are less prepared for an attack making their data more vulnerable. SMEs also offer a back-channel entrance to larger players in their respective value chains.

Return to Table of Contents

Sector focus:

Retail

Retail organizations are increasingly being targeted, primarily for credit card data. Cyber criminals are becoming more sophisticated, tapping into an ever-expanding toolkit of new techniques to access massive quantities of confidential records more efficiently than ever. Threats to retail may include data breaches, denial of service, third party payment breach, and insider man-in-the-middle attacks. The U.S. is typically one of the largest targets in this underground market.

Return to Table of Contents

Who is carrying out cyber-crime?

Today, hackers are divided into four (4) categories:

- **Individual hackers** – generally act alone and are motivated by being able to show what they can do. In essence, this is someone who exploits weaknesses in a computer system or computer network. They may be motivated by challenge or enjoyment, or to evaluate those weaknesses to assist in removing them (i.e. a "white hat" hacker).

- **Activist** – often referred to as "hacktivism," these hackers are primarily focused on raising the profile of an ideology or political viewpoint, often by creating fear and disruption. They are generally non-violent in nature. Some examples may include the promotion of internet freedom and freedom of speech.

- **Organized crime** – This hacker is focused solely on financial gain through a variety of mechanisms. Some examples may include identity theft, theft of credit card information, extortion (via ransomware of DDoS), click-jacking, pirating software, monetizing computer data in any way possible.

- **Nation state** – These hackers are sponsored by nation states and are generally focused on improving the geopolitical position and/or commercial interests of that state. Some examples include obtaining intelligence from adversaries, cyber espionage, stealing secrets from adversaries, disrupting or damaging an enemy's military infrastructure, propaganda, and distracting an enemy during a real attack.

Terrorist use of the internet:

Terrorists are aware of the potential for using the Western world's dependence on cyber systems as an exploitable vulnerability.

Return to Table of Contents

Sector Focuses:

Critical Infrastructure

Attacks on critical infrastructure have become a growing cause of concern for governments and private providers around the world – whether inflicted by cybercriminals seeking financial gain or by hackers as political acts aimed at undermining governments' and companies' credibility. The increase of infrastructures running on internet-facing networks has led to an increase in the number of cyber-attacks to the same infrastructures.

Government

Threats may include cyber espionage, national security information loss, disruption of critical infrastructure and national defence, disclosure of tax payers personal and business information, loss or theft of resources, insider man-in-the-middle attack, or hacktivism.

High Tech

Unlike the previous examples, ICT companies are often the organizations making it possible for the previously mentioned companies to manage, process, and share data. Cyber criminals are targeting their networks to obtain sensitive data. The most recent breaches were the result of attacks that exposed financial and credit card data, and volumes of personally identifiable information.

Return to Table of Contents

Administering cybersecurity prevention (5 key areas):

- **Identification:**
  - The first core function of cybersecurity is to identify the organization's cyber risk, which is the amount of risk posed by the organization's activities, connections, and operational procedures.
  - **Examples of solutions:** vulnerability assessment; proactive cyber intelligence; governance, risk & compliance; asset management.
- **Protection:**
  - The next core cybersecurity function is to ensure that the organization has the appropriate safeguards or controls in place to mitigate the various types of threats. This is the first line of defence.
  - **Examples of solutions:** threat prevention; access control; data security; patch management.
- **Detection:**
  - These solutions should help monitor for deviations from the normal state of activity. This would be the reinforcement to the first line of defence mentioned above.
  - **Examples of solutions:** Continuous (24/7) monitoring; anomaly & threat
- **Response (or level of responsiveness):**
  - It is important that an organization prepare for an incident, including knowing how the organization will respond if an incident occurs.
  - **Examples of solutions:** incident response; malware analysis; forensic remediation.
- **Recovery:**
  - The development and implementation of a recovery plan includes appropriate processes and procedures for how one intends to restore confidence in the recovered systems and data.
  - **Examples of solutions:** continuity of operations; disaster recovery; threat mitigation.

Return to Table of Contents

Sector Focus:

Healthcare

Healthcare records represent an attractive target for cyber criminals, containing as they do various bits of sensitive information, such as social security numbers, all in one place. The global healthcare cybersecurity market size was valued at nearly USD $5.5 billion in 2014. Key factors attributing to its rapid growth include the threat of cyber-attacks, regulatory and security compliance related issues, and data leaks from within the organization triggered by external or internal factors. Furthermore, increasing instances of patent infringement, theft of intellectual property, business secrets, medical identity fraud, and loss of electronic patient health records (E-PHI) and social security records are also expected to boost the usage of products in the field of healthcare.

Return to Table of Contents

International issues related to cybersecurity:

- **Trade & investment** – Having a secure and open internet is fundamental to the Canadian and global economies.

- **International Law** – Canada is active in seeking to establish and promote acceptance of peacetime norms for state behaviour in cyberspace.

- **Security issues** – Canada is working to develop confidence-building measures to reduce tensions and the risk of conflict stemming from the use of cyberspace.

- **Human Rights** – The internet can be used as a tool to promote human rights & democracy, or as a tool of repression.

- **Development perspective** – Much work remains to build an inclusive cyberspace in which everyone stands to benefit.

Return to Table of Contents

Sector Focus:

Banking and Financial Services

The banking and financial services sector has been a prime target for cyber criminals over the last five years. Some examples of the methods cyber criminals use to target this sector include: account takeovers, third party payment breach, market trading exploitation, ATM skimming, mobile banking exploitation, and insider man-in-the-middle attack.

Return to Table of Contents

How the TCS can help

The Canadian Trade Commissioner Service (TCS) can provide owners and representatives of SMEs with valuable insight into new markets that takes into account cyber risks. Most notably, the TCS connects clients with qualified contacts so as to prevent interactions with fraudulent websites and companies, and reduce the risk of identity theft.

TIP:

Cyber-attacks can result in more than monetary losses due to lost time and data recovery. Invest in security training to avoid potential damage to your company's reputation and relationships with customers and partners.

Return to Table of Contents

Are you export ready?

The Step-by-Step Guide to Exporting will help you to:

- **Sell to more customers.** Target global buyers online.
- **Enter more markets.** Leverage the benefits of free trade.
- **Save time & avoid risks.** Learn the legal aspects of trade.

Download this free guide and gain access to all TCS export publications through **MY TCS.**

Additional Resources on cybersecurity:

- Canadian Trade Commissioner Service (TCS)
  - Cyber Crime
  - Spotlight on E-commerce
  - Cybersecurity Law - China
  - China – Market Facts
    - Fraud Awareness in China
    - Fraud and Scams in China
    - Recommendations for Protecting Your Intellectual Property Rights in China
- Canada Business Network
  - Online Sales
  - E-business security, privacy, and legal requirements
- National Research Council of Canada (NRC)
  - Quantum solutions
- Public Safety Canada
  - Cybersecurity
  - Get Cyber Safe
  - Canada's Cybersecurity Strategy
  - National Strategy for Critical Infrastructure
  - Action Plan for Critical Infrastructure (2014-2017)
  - Cyber Review Consultations Report
- Other
  - Privacy and Cybersecurity Emphasizing privacy protection in cybersecurity activities
  - Cybersecurity in Canada: Practical Solutions to a Growing Problem
  - Security Best Practices for Canadian Telecommunications Service Providers (TSPs)
  - Payment Card Industry (PCI) Security Standards

Return to Table of Contents

Trade Commissioners are on-the-ground in more than 160 cities in Canada and worldwide.

The Canadian Trade Commissioner Service (TCS) is gaining market intelligence and insight, and uncovering opportunities for Canadian companies.

Our export experts can help your company:

- Prepare for international markets
- Assess your market potential
- Find qualified contacts
- Resolve business problems

tradecommissioner.gc.ca

LinkedIn Twitter Facebook