Communications Security Establishment
Centre de la sécurité des télécommunications

CYBER JOURNAL

EDITION 12 | OCTOBER 2017

IN THIS EDITION

BUILDING STRONGER CYBER SECURITY

At CSE, we recognize that cyber security is everyone's responsibility, regardless of position, profession, organization or industry. October is Cyber Security Awareness Month, which serves as a great reminder of how important it is to get involved in your organization's cyber security initiatives. Strong cyber security requires continual and dedicated investments. No single entity can solve every cyber issue alone. It takes widespread collaboration and partnerships between all sectors to develop innovative solutions to today's cyber threats. We must understand that practicing good cyber security is not just a concern for the IT team; it should be treated as a strategic business issue by all levels of the organization. Learn more about the importance of investing in cyber security in this edition of Cyber Journal.

You may have noticed CSE in the media recently for our public report on cyber threats to Canada's democratic process. Read our featured article for a brief overview of this threat assessment and the findings that could impact the 2019 federal election. You may have also noticed some proposed changes to CSE's governing legislation with the *CSE Act*. This legislation, if passed by Parliament, would allow CSE to better protect Canadians at home and abroad by further clarifying our authorizations and operations.

Moving forward, it is crucial for CSE to keep pace with emerging technologies to better protect Canada's sensitive information. There are many technologies, such as cloud computing, that CSE has been investigating in order to determine how our organization can safely benefit from them in a secure way. It is through CSE's dedication to innovation that we are able to secure Canada's position as a leading force in the global fight against cyber threats. We encourage everyone to get involved in finding innovative solutions to cyber security issues. Every industry, organization and individual must work together to create and maintain a safe cyber environment for all Canadians.

Originally signed by

Scott Jones
Assistant Deputy Minister, IT Security

cse-cst.gc.ca

Canada

Guidance contained within should not be considered comprehensive and all encompassing.

CYBER JOURNAL

OCTOBER 2017

CYBER SECURITY IS EVERYONE'S RESPONSIBILITY

October is Cyber Security Awareness Month, an internationally recognized campaign held each October to inform the public on the importance of cyber security. This annual event encourages Canadians and organizations of all sizes, including Government of Canada (GC) departments and agencies, to promote strong cyber security practices. Take time this month to evaluate your online security habits and see how your cyber hygiene measures up. Remember, cyber security is everyone's responsibility because the basic principles of good cyber security matter.

So what can happen when an organization's level of preparedness is nonexistent? Well, that's the thing: anything could happen. When organizations' networks connect to the internet, they're connecting to a world that cyber criminals and other threat actors have access to as well. Something as simple as unpatched software or an easy-to-guess password could result in malware being installed on an organization's system, potentially resulting in hours of lost productivity and money spent fixing the problem. This is why it's important to evaluate your organization's cyber security measures and determine your organization's level of preparedness.

Remember, broadly applying cyber security guidance does not necessarily mean your organization promotes an effective cyber security culture. Sometimes it's just not enough to tell employees to never connect to public Wi-Fi using enterprise devices; they need to be taught about what could happen should they do so. To combat this problem, see if there are targeted training and awareness courses available for employees. If so, will these programs likely lead to behavioural changes in employees by offering training and cyber-specific guidance relevant to their specific jobs? System safeguards are vital to the protection of importantIT networks and systems, but a workplace can only be secure if the employees understand the exact purpose for maintaining good security.

Without proper training, staff could create vulnerabilities that may affect online operations. This risk can be avoided by building a stronger first line of defence by fostering a culture of security awareness. By applying action #6 of CSE's Top 10 IT Security Actions, *"Provide tailored awareness and training"* GC departments can better understand what threats are specific to individual departments or agencies, as well as their potential business impacts.

Educating staff members on a wide range of IT security topics and providing regular updates to users can greatly improve employees' understanding of current cyber trends that could affect your organization. To learn new ways to protect against cyber threats in today's dynamic threat environment, visit Get Cyber Safe online to find educational materials and resources to help protect your online security.

This page offers blog posts, infographics and videos that provide additional background information on the importance of practicing good cyber security. Implementing these tips is a great place to start when it comes to raising awareness of cyber security among employees, colleagues, friends and family.

Stay cyber secure. Don't forget to follow CSE on Twitter to stay informed on cyber security best practices.

Guidance contained within should not be considered comprehensive and all encompassing.

CYBER JOURNAL

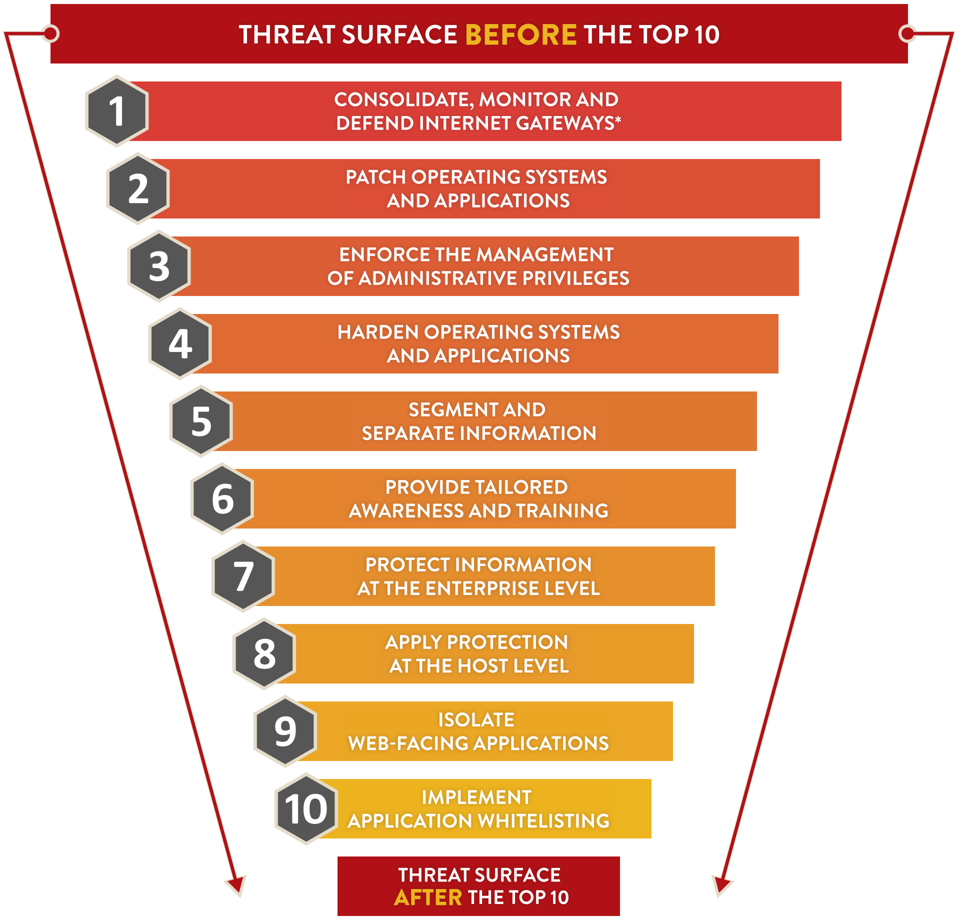
OCTOBER 2017

CSE'S TOP 10 IT SECURITY ACTIONS ARE NOW FOR EVERYONE

Cyber incidents continue to grow in scale and complexity every day. There are many different mitigation actions publicized online as the best ways to protect your system. It can be overwhelming deciding exactly what advice to follow. This is why CSE originally created the Top 10 IT Security Actions. They are based on CSE's hands-on knowledge and many years of experience mitigating thousands of cyber incidents that impact Government of Canada (GC) departments. The Top 10 have dramatically reduced the threat surface for the GC. They are the best defence against cyberattacks.

But the question remains - how can non-GC organizations mitigate their risk?

To allow for broader adoption, CSE has adapted the Top 10 to apply to any type of organization. Critical infrastructure owners, small/medium enterprises, and non-profits are just a few examples of who can now benefit from implementing the Top 10. Together, we can collectively make Canada stronger and more resilient against cyber threats.



THREAT SURFACE **BEFORE** THE TOP 10

1. CONSOLIDATE, MONITOR AND DEFEND INTERNET GATEWAYS*
2. PATCH OPERATING SYSTEMS AND APPLICATIONS
3. ENFORCE THE MANAGEMENT OF ADMINISTRATIVE PRIVILEGES
4. HARDEN OPERATING SYSTEMS AND APPLICATIONS
5. SEGMENT AND SEPARATE INFORMATION
6. PROVIDE TAILORED AWARENESS AND TRAINING
7. PROTECT INFORMATION AT THE ENTERPRISE LEVEL
8. APPLY PROTECTION AT THE HOST LEVEL
9. ISOLATE WEB-FACING APPLICATIONS
10. IMPLEMENT APPLICATION WHITELISTING

THREAT SURFACE **AFTER** THE TOP 10

**Government of Canada to use Shared Services Canada Internet Gateways.*

Learn more about our new Top 10 for everyone:
ITSM.10.189–Top 10 IT Security Actions to Protect Inter-Connected Networks and Information

For GC departments, continue to follow:
ITSB-89 v.3 – Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information

CYBER JOURNAL

OCTOBER 2017

PUT YOUR MONEY WHERE YOUR DATA IS – INVEST IN CYBER SECURITY

Major cyber breaches continue to hit the news, making it apparent that organizations are still not adequately investing in cyber security. It is critical for all organizations to adopt a cyber security mindset and make investments accordingly. Canadian organizations must think of cyber security not only as an IT issue, but also as a risk management issue.

No matter the size of your organization, big or small, if you have data to protect and it's stored on an electronic network, threats will find you. In fact, 71% of data breaches in Canada affect small businesses.

It's important to remember that when a system is compromised, stopping and repairing the damage is expensive. According to a recent IBM study, the average cost of a data breach to a Canadian organization is $6 million, a number that grows every year. This doesn't include the costs incurred by business disruption, such as lost productivity, after a breach has occurred.

It is critical for all organizations to adopt a cyber security mindset and make investments accordingly. As you can see, recovering from a breach is not cheap. However, proactively investing in cyber security can protect your organization and can save you from the bigger costs associated with cleaning up after a breach.

It's important to realize that the choices organizations make regarding cyber security can have a direct impact on their reputation, which can be even more damaging than just the financial costs associated with a breach. Furthermore, by employing strong cyber security practices, an organization can gain an advantage over competitors, while also building confidence with stakeholders.

No one can afford to be unsecure. Investing in cyber security should be a priority for all Canadian organizations.

To help all organizations in protecting their networks, CSE has developed the Top 10 IT Security Actions.

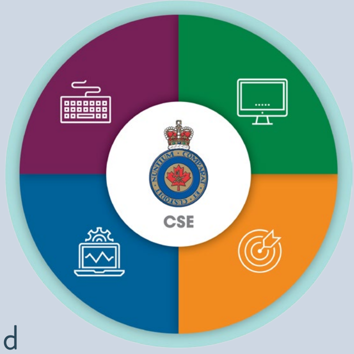
The Top 10 has been built upon years of CSE's mitigation advice to Government of Canada departments and agencies.

The Top 10 has been prioritized in a way that each action builds on the previous one to continually diminish the threat surface and, in turn, increase the difficulty and level of effort required by threat actors to compromise networks.

The Top 10 has proven to be a good investment to make and yields a strong return by protecting networks against the most challenging cyber threats.

Invest in cyber security and implement the Top 10 so that, collectively, we can make Canada stronger and more resilient against cyber threats.

PROPOSED CSE ACT



CSE is at the forefront of cyber security, operating in a technological world that is rapidly evolving. In June 2017, the Government of Canada tabled Bill C-59, the new national security legislation.

This bill includes the *CSE Act*, which would clarify how we are authorized to operate in cyber space, protecting Canadians at home and abroad from threats to our security, stability, and economic prosperity.

To learn more, click here to read the proposed *CSE Act*.

CYBER JOURNAL

OCTOBER 2017

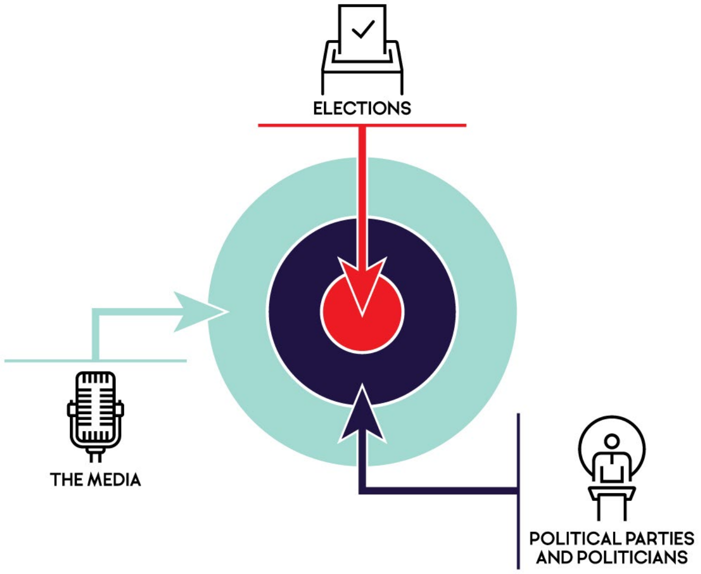
CYBER THREATS TO CANADA'S DEMOCRATIC PROCESS

CSE'S ASSESSMENT ON CYBER THREATS TO CANADA'S DEMOCRATIC PROCESS

The recent cyber threat activity against the democratic process in the United States and Europe has raised concerns about similar threats to Canada. In response to a request from the Minister of Democratic Institutions, CSE conducted a threat assessment on cyber threats to Canada's democratic process. This information is available in a report entitled *Cyber Threats to Canada's Democratic Process*. To better understand the threat environment, CSE examined cyber threat activity against democratic processes, both in Canada and around the world, over the past ten years.

In this assessment, we considered the cyber threats to Canada's democratic process at the federal, provincial/territorial, and municipal levels of government. Additionally, we reviewed cyber capabilities and how adversaries use these capabilities in sophisticated ways to influence a democratic process. We provided our assessment of cyber threat activity targeting democratic processes – both around the world and in Canada – and what we expect to see against the 2019 federal election, political parties and politicians, and the media relevant to the election.

Over the past five years, there has been an upward trend in the amount of cyber threat activity against democratic processes globally. At the time of publication, 13 percent of countries holding federal elections had had their democratic process targeted. However, to date, we have not observed nation-states using cyber capabilities with the purpose of influencing the democratic process in Canada during an election.



We assess that whether this remains the case in 2019 will depend on how Canada's nation-state adversaries perceive Canada's foreign and domestic policies, and on the spectrum of policies espoused by Canadian federal candidates in 2019. These trends impact all of us. No one can do this alone; we all have a role to play in cyber security.

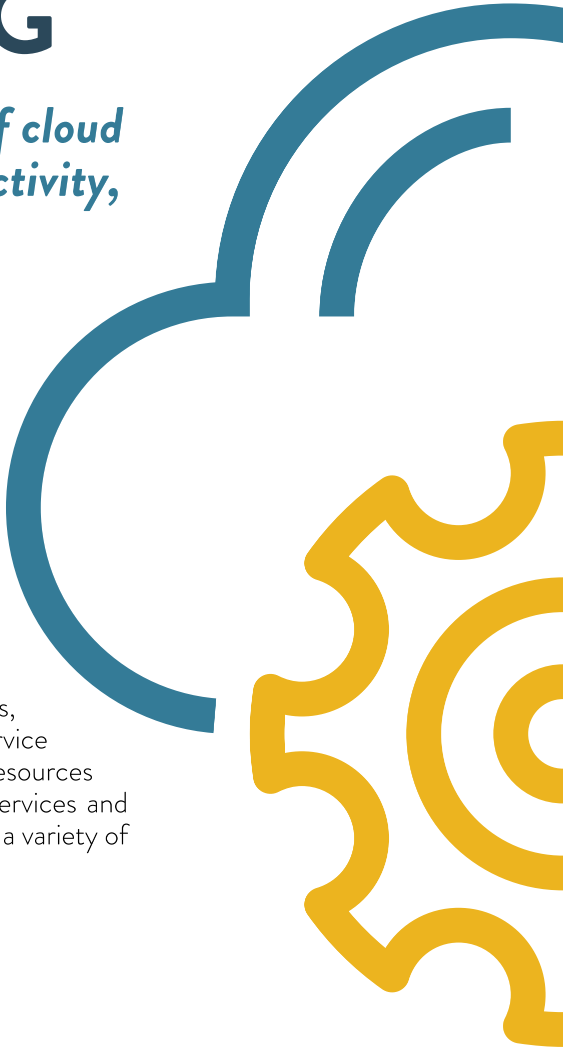
Click here to read the entire report.

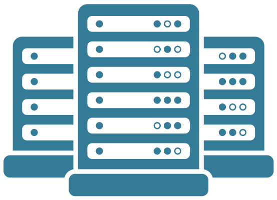
CYBER JOURNAL

OCTOBER 2017

THE FORECAST ON CLOUD COMPUTING

Whether or not you realize it, you are using a form of cloud computing almost any time you perform an online activity, from checking your e-mail to logging in to an online shopping account. Cloud computing is becoming an increasingly popular IT tool for both business and personal use due to its productivity, security and economic advantages.





SO WHAT IS CLOUD COMPUTING?

Cloud computing is the sharing of IT applications, infrastructure and services over a network that is, in many cases, owned and operated by a third-party service provider. This service provider invests heavily in infrastructure and then shares its resources among many clients. This outsourcing helps reduce the cost and maintenance of IT services and infrastructure for businesses. We can think of the cloud as a large data centre that hosts a variety of computing services to help facilitate IT and business operations.

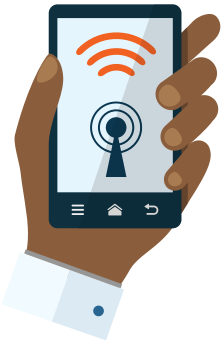
CLOUD COMPUTING IN THE GC

Canadians continue to demand IT-enabled government services. These increasing demands for technology can only be met by implementing relevant and practical solutions, such as cloud computing. The Government of Canada (GC) is keeping pace with emerging cyber trends by moving towards cloud-based technologies.

Treasury Board of Canada Secretariat (TBS), Shared Services Canada (SSC) and CSE are working together to leverage cloud services for the GC. TBS recently launched the Government of Canada's Cloud Adoption strategy with the goal of bridging the supply and demand gap for cloud services, while providing a consistent approach to managing the risks of cloud adoption. The objective is to prepare the IT workforce for cloud adoption by making services more accessible and efficient for government departments and Canadians.

WHY USE CLOUD

Canadians are increasingly dependent on technology and online services to perform daily tasks. The cloud plays a major role in many of these, including online banking and shopping, social media, tax returns, student loan applications… the list goes on. Cloud services offer unique benefits that help address our increasing need for technology. Service performance is one benefit. Self-service provisioning with computer resources can dramatically reduce the time required to complete a task, making cloud an efficient business option. Additionally, cloud service providers are known for their security standards, which are often assessed by third-party security professionals. This allows organizations to employ robust security systems that may not have been financially feasible without the support of a third-party service provider. The cloud's flexibility makes it a cost effective IT solution by allowing organizations to save time and, therefore, money. Organizations only have to pay for the services they use, which can easily be modified to grow or shrink with the organization's demand for IT services.



Cloud technology offers users – both business and personal – the opportunity to access relevant IT systems and information in a timely and secure manner through shared data centres. This efficiency allows organizations to develop more targeted and creative solutions to everyday business problems.

NOW WHAT?

As with any IT service provider, organizations must be able to trust new technology before they integrate it into their daily operations. Leading cloud service providers build their business models around trust, with a focus on securing customer data. Although cloud providers follow security standards, it's important to remember that those standards are not always Canadian and may not necessarily reflect the organization's security needs here in Canada. Understanding the risks when choosing a new IT service provider and identifying business requirements can help organizations assess the acceptable level of risk with their cloud service provider. CSE is working hard to make sure there are no gaps between cloud security standards and security requirements for businesses operating in Canada.

Over the next few editions, CSE will be taking readers through a variety of different cloud-related topics and addressing the risks associated with cloud computing and other technologies. This series aims to improve your understanding of cloud technology, its security features and how it can apply to everyday personal use and business operations.

DID YOU KNOW?

According to a study by Citrix, 54% of respondents claimed to have never used cloud computing before; however, 95% of this group actually did use the cloud through daily activities like online banking, shopping and social networking sites.

Source: Business Insider, August 2012

CYBER JOURNAL

OCTOBER 2017

CYBERHYGIENE

CYBER HYGIENE SERIES: SOCIAL MEDIA

Social media has made communicating for business and personal use easier than ever before. From the photo-sharing app Instagram to the micro-blogging site Twitter, there is a platform to satisfy every taste and communication need. The proliferation of social media sites has meant an increase in usage, both here in Canada and around the world. In fact, it is predicted that the number of social media users worldwide will grow to 2.55 billion in 2018, a 25 percent increase from 2015. But with so many platforms popping up every day, one must wonder how these social media sites intend to keep up with today's constantly evolving cyber security trends.

Social media is a great communication and information sharing tool, but it also presents several security risks. There are many reports of users being tricked by fraudulent accounts designed to resemble legitimate accounts, as well as users being deceived by authentic accounts that get hacked and then send out malicious links to their followers. Simply put: it is becoming increasingly more difficult to tell which social media accounts are authentic, a fact that cyber criminals are using to their advantage.

DID YOU KNOW?

The Facebook community alone represents more than a quarter of the world's 7.5 billion population with 2 billion users worldwide – that's more than the population of any single country!

Source: CBC News, June 2017

SOCIAL MEDIA TIPS

- Use a unique password for every account
- Ensure all available security and privacy options have been applied on your account
- Review your account's website security and privacy policies regularly for changes
- Be careful when accessing unknown website links or attachments
- Report any suspected security incidents to your IT support team
- Use judgement when posting personal information on social media platforms for both privacy and cyber security reasons

Unfortunately, most social media sites do not feature security methods to indicate that a profile is authentic (although there are exceptions, such as Twitter's "verified" blue badges present on verified accounts). So no matter what social media platform you're using, it's important to be always cautious when clicking on links or hashtags present in comments and private messages. These links could contain malware, key loggers or botnets, and it's hard to know if a user's account has been hacked.

Social media can also be used as a tool to gather personal information on a user, allowing hackers to create targeted spear-phishing attacks based on the interests, ideas and information you share online. Don't forget to review your security and privacy settings on each social media account and use judgment when sharing any personal information online.

Practicing good security habits on social media is one way to keep you and your personal information secure online. Follow CSE's Cyber Hygiene fact sheet to learn how you can protect yourself from today's cyber threats.

Guidance contained within should not be considered comprehensive and all encompassing.

CSE IN THE COMMUNITY: CSE ADDRESS SKILLS GAP BY TEACHING LOCAL STUDENTS

Cyber security is a growing field, but it may be expanding at a rate that's just too fast for the job market to keep up with it. One of the greatest issues facing the future of cyber security is the lack of skilled workforce. ISACA has estimated that by 2021, there will be 3.5 million vacant cyber security jobs due to both a lack of security talent and the continuing expansion of cybercrime. Despite record security spending and appealing salaries, many hiring managers are reportedly struggling to fill positions relating to cyber security.

One way of responding to the cyber skills gap is to inspire today's students to become tomorrow's cyber security leaders. Many programs worldwide have been developed to attract young professionals to the IT world, such as the CyberFirst program in the UK, which sponsors undergraduate students in relevant fields of study and offers summer internships. Connecting with this age group is important as students in high school are either just starting to think about their post-secondary plans or have already begun applying to colleges and universities, unaware of the opportunities that exist in computer science beyond high school.

CSE is committed to addressing this skills shortage through various community outreach projects that aim to showcase the potential of careers in IT to young Canadians. CSE established a community outreach program with two clear goals in mind: to increase the interest of Canadian youth in science, technology, engineering and math (STEM) related education and careers, and to promote technical literacy for all Canadians. One example is CSE's recent pilot project at Lester B. Pearson Catholic High School in Ottawa. During a nine week course, volunteers used Raspberry Pi computers to teach useful coding skills to grade 11 and 12 students. Other outreach engagements include programs with a local senior adults centre and an ongoing partnership with a local elementary school.

The growing cyber security skills gap is a risk to all sectors in the IT security industry. Government, industry and academia must work together to identify, develop and retain talent in the field of cyber security. CSE encourages other organizations to develop similar initiatives as these programs can introduce Canadians to STEM fields and, hopefully, inspire the next generation of Canadian technology leaders.

CSE JOINS GCCONNEX

CSE has joined the Government of Canada's professional social networking platform called GC Connex. GC Connex registration is open to all federal employees.

Join here and visit our group *IT Security – Communications Security Establishment*.

Guidance contained within should not be considered comprehensive and all encompassing.

ITSLC NEWS

Over the past year, the ITS Learning Centre has worked with various departments to provide tailored training solutions to their IT security practitioners and IT business analysts. As an example, at the *Department of Fisheries & Oceans* and at the *Department of National Defence*, we delivered our five-day IT Security Risk Management Bootcamp, which provides the overall concepts of IT security risk management for the GC and the foundational knowledge and guidelines needed to contribute to the development of security control profiles.

To inquire on providing *your* IT security team with a similar group training opportunity, please contact us at its-education@cse-cst.gc.ca

For additional information or to register for a course, visit the ITSLC Web site

MARK YOUR CALENDAR!

As part of Cyber Security Awareness month, the IT Security Learning Centre is hosting their annual open house on October 19th. For more information on this event, please visit our website.

ABOUT THIS NEWSLETTER

The Cyber Journal is a newsletter prepared for Government of Canada stakeholders and Canadian organizations with a focus on current and emerging technologies. Released on a periodic basis, the publication features best practices to help departments and organizations better protect themselves in today's dynamic threat environment.

Through the Cyber Journal, CSE provides advice, guidance and tools to help secure Canada's position as a leading force in the global fight against cyber threats. As Canada's leader in cyber security, it is CSE's top priority to ensure the protection of Canada's electronic information.

CONTACT US

For general advice and security guidance support, contact:

✉ itsclientservices@cse-cst.gc.ca ☎ **General Inquiries: (613) 991-7654**

To contact the Cyber Threat Evaluation Centre:

✉ ctec@cse-cst.gc.ca

For planning, support or any issues regarding COMSEC devices, contact COMSEC Client Services:

✉ comsecclientservices@cse-cst.gc.ca

☎ **General Inquiries: (613) 991-8495**

COMSEC custodians can contact the Crypto Material Assistance Centre (CMAC):

✉ cmac-camc@cse-cst.gc.ca

☎ **General Inquiries: (613) 991-8600**

For education and training services, contact the IT Security Learning Centre:

✉ its-education@cse-cst.gc.ca

☎ **General Inquiries: (613) 991-7110**