Communications Security Establishment
Centre de la sécurité des télécommunications

CYBER JOURNAL

EDITION 13 | AUGUST 2018

IN THIS EDITION

PARTNERING FOR SECURE AND RESILIENT CANADIAN SYSTEMS

Cyber security is one of the most serious economic and national security challenges we face in this digital age. Budget 2018 highlighted just how important a cyber secure Canada is to the federal government by establishing the Canadian Centre for Cyber Security. The Cyber Centre will offer a unified approach to cyber security that will build upon Canada's already world-class expertise by uniting key cyber security operational units from Public Safety Canada, Shared Services Canada and CSE.

With a public-facing posture, the Cyber Centre will offer a place where private and public sectors, including academia, can work side-by-side to tackle Canada's most complex cyber security challenges in collaborative and innovative spaces.

By working together, we can share our problems and can work towards shared solutions by developing stronger cyber defence techniques and tools. Our overall goal is to help the cyber community work smarter, not harder, in order to protect against the sophisticated threats that we all face.

The Cyber Centre will be a one-stop-shop that connects users and organizations to the proper support they need to be more secure and resilient against cyber threats. It will produce sensible, digestible, realistic and meaningful guidance for Canadians' personal use and Canadian organizations alike.

The creation of the Cyber Centre is a clear signal that the Government of Canada understands the critical nature of cyber security and is taking a leadership role in this field. This notable investment in cyber security shows that Canada is committed to making Canada more secure and resilient against cyber threats.

Originally signed by

Scott Jones
Head-Designate, Canadian Centre for Cyber Security and Deputy Chief, IT Security

cse-cst.gc.ca

Canada

THE CANADIAN CENTRE FOR CYBER SECURITY

This is an exciting time to be in the cyber security business in Canada. With Budget 2018, the government recognized the importance of investing in cyber security. Cyber security is one of the most serious economic and national security challenges the country is facing, and we can only meet that challenge by working together. The government has cemented its commitment to creating a strong federal governance system to protect Canadians and their sensitive personal information.

The Budget highlighted the funding for the new National Cyber Security Strategy, which will include many initiatives involving several federal organizations. Public Safety Canada is the lead for this strategy, which was drafted following the 2016 Cyber Review Consultations. A key initiative is the creation of the Canadian Centre for Cyber Security, which will be housed within CSE. The Budget allocates $155.2 million over five years for the creation of the Cyber Centre, with $44.5 million ongoing.

The Cyber Centre will offer a unified approach to cyber security that will build on Canada's already world-class cyber security expertise. The Cyber Centre will be this country's federal authority on cyber security as the single, unified Government of Canada source of expert advice, guidance, services and support on cyber security operational matters.

Together with our partners, the Cyber Centre will be best-placed to take on evolving and complex cyber security challenges. The Cyber Centre will advance partnerships and dialogue with other jurisdictions, the business community, academia and international partners.

By consolidating operational cyber expertise from across the federal government under one roof, the new Cyber Centre will provide Canadian citizens and businesses with a clear and trusted place to turn to for cyber security advice.

The Cyber Centre will shape the future of cyber security in Canada by taking a proactive, innovative and collaborative approach to cyber defence by drawing on the strengths found within the Government of Canada. The Cyber Centre will unite 750 employees from existing cyber security operations units at Public Safety Canada, Shared Services Canada, and CSE into one unique, innovative, and forward-looking organization. When the Cyber Centre opens in October 2018, Scott Jones will lead the newly formed organization as the head-designate of the Cyber Centre.

From Public Safety Canada, all functions of the Canadian Cyber Incident Response Centre (CCIRC) and the Get Cyber Safe public awareness campaign will be transferred to the Cyber Centre.

From Shared Services Canada, some of the functions of the Security Operations Centre will be transferred to the Cyber Centre.

From CSE, the entire IT Security branch will be transformed to become part of the Cyber Centre.

Our collective expertise will allow us to build strong partnerships, innovate new and necessary cyber security techniques and drive resilience for a secure cyber ecosystem. With this investment in Canada's cyber security ecosystem, and by continuing to work together, we can and will make Canada stronger and more resilient against cyber threats.

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

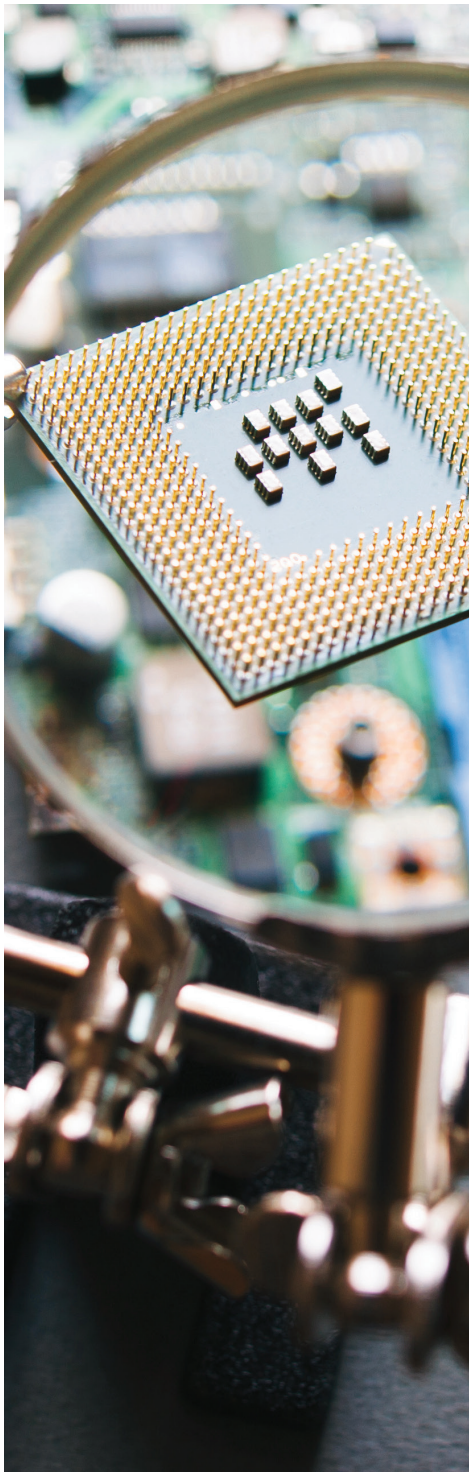
MELTDOWN AND SPECTRE: TWO VULNERABILITIES THAT CHANGE THE CYBER THREAT LANDSCAPE

This past January, the world was rocked by the news that virtually every processor chip used in computing devices had two critical vulnerabilities: Meltdown and Spectre. These flaws can be exploited by threat actors granting access to a computer's protected memory, putting encrypted and sensitive information at risk. What makes the issue even more serious is the revelation that these flaws have existed in nearly every processing chip manufactured since 1995.

Since the news broke, many operating system vendors and system manufacturers have released patches to ensure their software cannot be exploited through these vulnerabilities; however, there is no simple patch to fix the fact that your computer is likely using a chip containing one of these flaws. So what are the long-term implications of this problem?

For starters, major hardware overhauls may be needed sooner rather than later, especially for some Government of Canada departments. A report from Bloomberg explains that regulated sectors, such as government offices and public health institutions, are more likely to be affected by these bugs than others. Part of the problem stems from the widespread use of older systems by organizations within these sectors; they're outdated, and patches developed to mitigate these vulnerabilities could slow these aging systems down even more.

What's far more significant is the fact that threat actors now have a new avenue to search for vulnerabilities: not in software, but physically within computers themselves. Flaws in computer hardware have been discovered before, although nowhere near the scale of Meltdown and Spectre. This means that searching to exploit vulnerabilities in hardware, as opposed to just software, could become the new norm.



There are advantages to having more people publicly discuss issues related to computer hardware. We can now expect cyber security researchers, government departments, and various organizations to research the impact of Meltdown and Spectre for years to come. However, it also means cyber threat actors will be doing the same, which could require security practitioners to redefine their craft to keep up with entirely new threats.

Even though Meltdown and Spectre may have disrupted the cyber landscape, there are ways for organizations to take control. The Canadian Cyber Incident Response Centre (CCIRC) issued an alert that includes suggested actions and links to recommended mitigation guides. These references can help both Government of Canada departments and private industry reduce their threat surfaces and better prepare for the changing cyber threat landscape.

While there is no immediate fix for the problems posed by Meltdown and Spectre, CSE urges organizations to continue being proactive and aware of new vulnerabilities. Implement robust patching plans and IT-ever greening processes as defences against aging IT infrastructures. If you follow CCIRC's suggested actions, implement CSE's Top 10 and practice good cyber hygiene, you are less likely to face the spectre of a cyber meltdown.

CLOUD BENEFITS: EVERY CLOUD HAS A SILVER LINING

Ask not what you can do for the cloud, but what the cloud can do for you. Cloud computing offers many benefits that can transform daily operations by enabling convenient, on-demand access to a shared pool of configurable computing resources. The cloud has become an increasingly popular IT tool for government, business and personal use due to its productivity, security and economic advantages. It allows users – both business and personal – to develop more targeted and creative solutions to everyday business problems.

There are some inherent benefits of switching to the cloud that have the potential to revolutionize the way you use IT:

SERVICE PERFORMANCE

Self-service provisioning of computing resources can dramatically reduce the time to meet a requirement. Metrics-based service levels that are contractually enforced help ensure consistent performance levels.

SECURITY

Cloud service providers hold internationally recognized security certifications that are assessed by third-party security professionals. These certifications include robust security features that would be a challenge for any one consumer to fund individually.

INNOVATION

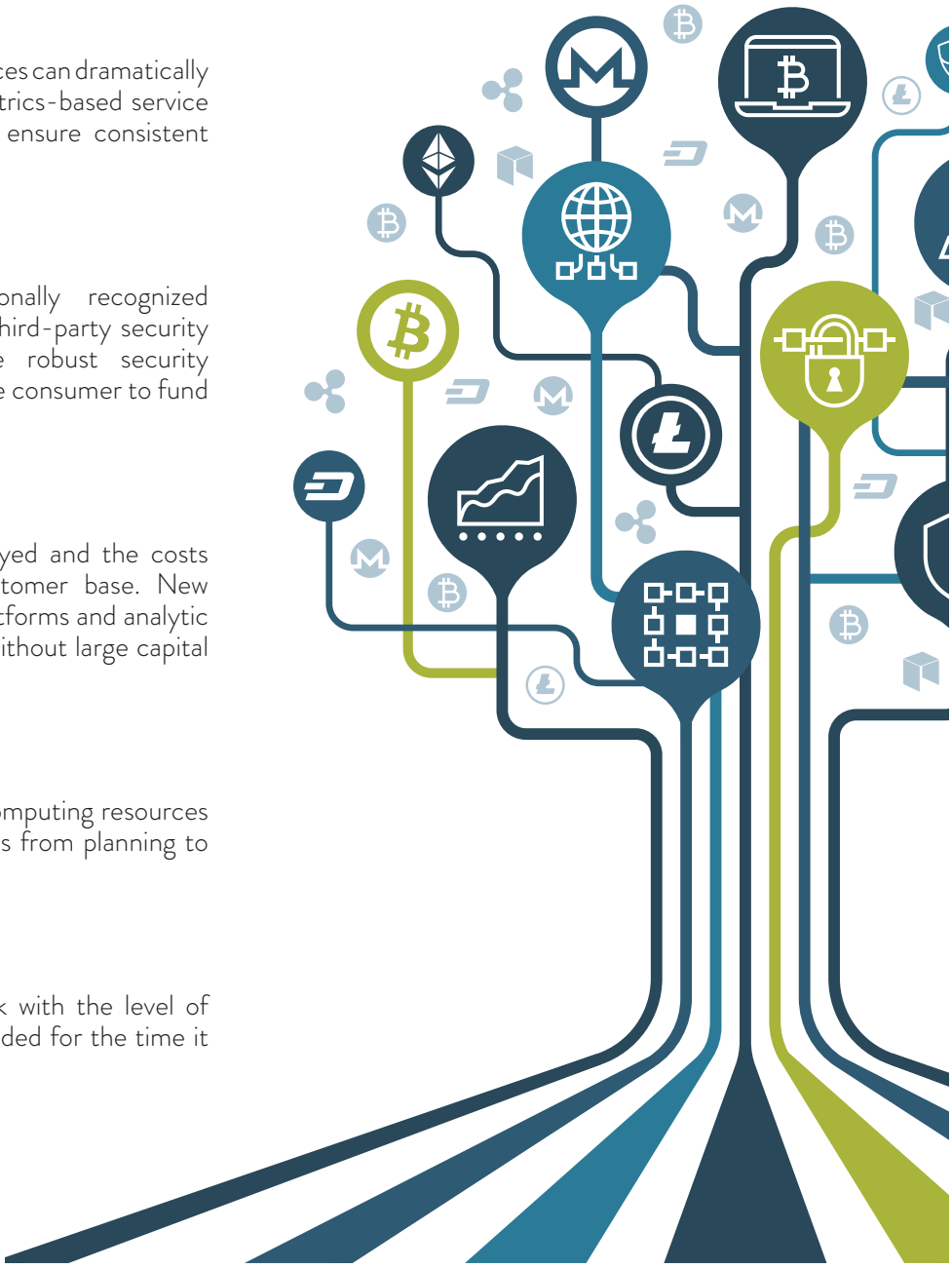
New features are continuously being deployed and the costs are amortized across a global service customer base. New technologies such as social media, mobile platforms and analytic tools are all available through subscriptions without large capital investments.

AGILITY

Rapid access is available to multi-featured computing resources at the required capacity to carry out projects from planning to full operation.

ELASTICITY

Commoditized services can grow and shrink with the level of demand; consumers pay only for what is needed for the time it is needed.



THERE ARE PLENTY OF CLOUDS IN THE SKY. SO WHAT'S YOUR TYPE?

You've decided the cloud is right for you, so now what? The next step is to research different service and deployment models, and then decide which would benefit your organization the most. Think wisely when choosing a cloud service model: there are several different models to choose from, and your decision will have a lasting effect on your organization. It is important to note that there is no 'one-cloud-fits-all' solution, since not all cloud services are created equal. Knowing which cloud service and cloud deployment model is right for you is important. Although this list is not all-encompassing or inclusive, it summarizes the most common models.

SERVICE MODELS

SOFTWARE AS A SERVICE (SaaS)	PLATFORM AS A SERVICE (PaaS)	INFRASTRUCTURE AS A SERVICE (IaaS)
SaaS is a software distribution model where applications are purchased or hosted by a cloud service provider, and then made available for customers to use over the internet. This reduces the need to install and maintain the software on local computers. Many Government of Canada departments use a similar type of service, but they use a network instead of the internet.	PaaS is a platform model that provides a safe development, testing, and deployment environment for application developers. This service model is very flexible and can allow you to scale deployments quickly. It can provide add-on features to aid in the application development and deployment processes.	In an IaaS model, users pay for cloud storage space on a consumption basis. Users are also responsible for accessing, monitoring, and managing their own data remotely stored on the infrastructures. IaaS Cloud Service Providers generally manage hardware, storage and networking, as well as other services at an additional cost.

DEPLOYMENT MODELS

PUBLIC CLOUD	PRIVATE CLOUD	COMMUNITY CLOUD
A public cloud provides shared resources, cost-effectiveness and efficiency. This type of cloud is external to an organization, meaning that applications and data storage are remotely-accessible. You may share the same infrastructure with many organizations, meaning your data may be stored on the same server as others.	A private cloud allows customers to have greater control over their infrastructure and computational resources. This model provides services and infrastructures that are located on private networks and deployed for a specific organization.	A community cloud has a unique infrastructure that is shared by several organizations and is restricted for use by approved community users. Generally, it supports a specific community that has shared goals. It may be managed by the organization or a third party, and can exist on or off premise.

HYBRID CLOUD

A hybrid cloud is a combination of public and private clouds. They give organizations the advantages of many different service providers and facilitate access to the most efficient options for each business requirement of an organization.

HOW TO STAY CYBER SECURE: FOLLOW THE FUNDAMENTALS OF CLOUD SECURITY

Cloud Service Providers (CSPs) offer a flexible, agile and innovative alternative to the traditional organization-owned, on-premises data centre by providing on-demand and scalable computing environments. As with any information technology (IT) area, cloud computing should be approached carefully with due consideration to IT security and the risks involved. Every organization, public or private, is advised to apply CSE's Fundamentals of Cloud Security when analyzing its own requirements, and to assess, select, engage and oversee the cloud services that can best fulfill those requirements.

Understanding the risks posed to our data by adopting cloud services can sometimes be complex and unclear. To help, CSE has outlined the fundamental security issues to consider as you integrate cloud services into your existing IT infrastructure.

THE FUNDAMENTALS OF CLOUD SECURITY

- Understand your business security requirements
- Ensure asset protection and resilience
- Assume breach and plan accordingly

- Implement robust access controls
- Audit and monitor access to services
- Use the service securely

- Procure from security-centric suppliers
- Adhere to a secure design and development lifecycle
- Ensure appropriate tenant separation

CSE will be soon publishing detailed documentation on the fundamentals, allowing organizations to consider the security risks when moving to the cloud. Understanding these fundamentals will help determine if a cloud service meets an organization's security requirements and is secure enough to handle their data. By applying these nine fundamentals, your organization's cyber security posture will be far more likely to stay on cloud nine.

CSE'S COMSEC UPDATES

Effective December 2017, CSE has a pair of directives that change how cryptographic equipment and keys are managed. These new network security directives are the culmination of a long-term, concentrated effort to reaffirm CSE's security service advice and guidance.

The first of these directives, the IT Security Directive for the Management of CSE-Approved Cryptographic Equipment and Key to Secure a Telecommunications Network (ITSD-04A), focuses on identifying the authorities for Government of Canada (GC) cryptonets.

The second, the IT Security Directive for Cryptographic Key Ordering (ITSD-09), outlines the process for ordering keymat products. Together, they provide more decisive management direction for the use of network capabilities and are better able to adapt to the increasing complexity of Communications Security (COMSEC) in the GC.

ITSD-04A	ITSD-09
• Gives the Controlling Authorities (ConAuths) and Command Authorities (CmdAuths) permission to operate within their department's COMSEC • Outlines the necessity to register cryptonets with CSE's COMSEC Client Services (CCS) • Proposes the Key Material Support Plan (KMSP) as an essential tool for COMSEC development	• Outlines the key ordering process which will implement COMSEC and maintain it over the long-term • Offers CSE's Crypto Material Assistance Centre (CMAC) for assistance in the case that any COMSEC issues arise

ASSEMBLYLINE

AUTOMATING MALWARE ANALYSIS SO YOU DON'T HAVE TO

Assemblyline is a malware detection and analysis tool developed by CSE and was released to the cybersecurity community in October 2017. The release of Assemblyline benefits the country and CSE's work to protect Canadian systems, and allows the community to build and evolve this valuable open-source software.

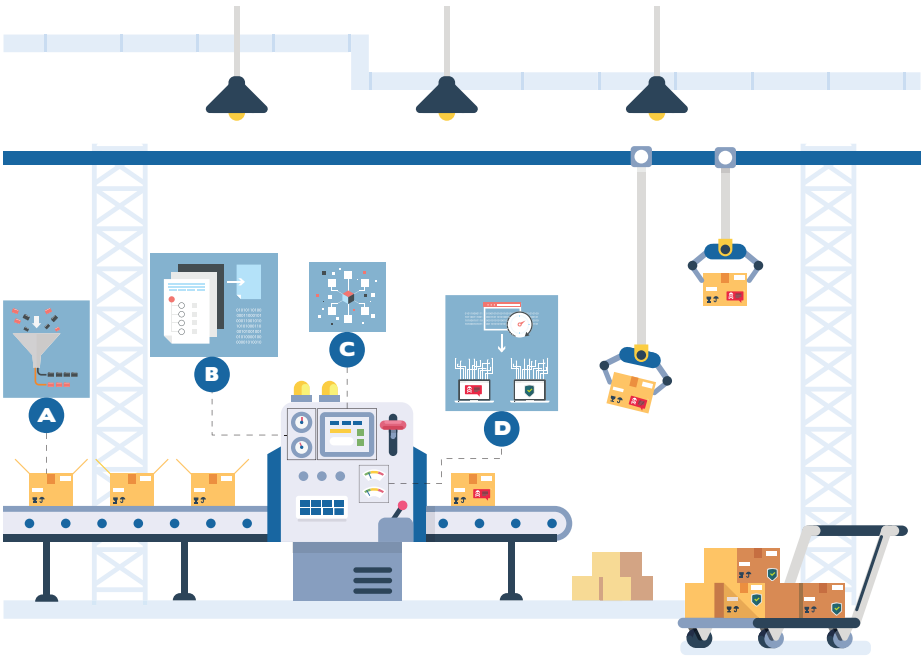
CSE, an organization once mostly known as the "super-secret spy agency," achieved a significant milestone by sharing one of its own tools with the public for the first time ever. But what's even more impressive is how it can make the jobs of cybersecurity professionals so much easier.

Assemblyline grew out of a necessity to be more transparent in how malware-related data is collected and used. As Canada continues to embrace new digital technologies, it means having significantly more data for organizations to deal with on a daily basis. However, with more than 377,000 internal users accessing government networks, it has become virtually impossible to manually handle each individual case of malware.

Now thanks to the software's automatic malware detection and sorting features, cybersecurity professionals can focus their efforts on analyzing anomalies instead of constantly dealing with routine issues. By creating an open source platform that allows others to collaborate and automate the detection of malware, the developers were able to make many peoples' jobs easier – including their own.

With Assemblyline now in use by numerous organizations, the overall cyber security ecosystem poses to be stronger than ever before. Despite this advancement, the tool can only be improved through the consistent collaboration of its users. Feedback will not only improve Assemblyline, but allow CSE to strengthen future tools and make Canada at large more resilient against cyber threats.

Assemblyline is available on BitBucket. Please note that Assemblyline is not designed as a replacement for commercial antivirus products on the desktop. Anyone interested in the field of cyber security can join the Assemblyline Google group at https://groups.google.com/d/forum/cse-cst-assemblyline



CSE IN THE COMMUNITY: CSE GOES BACK TO SCHOOL WITH HACKERGAL

Last issue, we discussed the recent efforts by CSE to address the growing skills gap in the cyber security field. By offering outreach programs in various schools and community centres, CSE has been able to introduce students and adults to the possibilities that are offered by careers in science, technology, engineering and math (STEM).

The growing gender gap is another important aspect of the skills gap that CSE is addressing. Since more cyber security organizations have been struggling to staff their positions, fixing Canada's gender disparity in STEM careers has become more important than ever.

To illustrate how large the gap is, numbers from Statistics Canada show that women made up 47% of the Canadian labour force in 2016[1]. However, only 23% were in computer and information systems jobs that year[2] . So despite a 24% increase in the number of women enrolled in STEM programs between 2010 and 2016[3], women in these fields are still greatly outnumbered by men.

In an effort to help close the gender gap, CSE played a major role in facilitating last December's Hackergal hackathon. Hackergal is a Canadian organization that aims to introduce school-aged girls to coding. The hackathon was designed so groups of girls would work together to learn the basics of coding and then create functioning animations using a simple block coding technique.

Experience levels varied among students—some already had coding experience, while others were completely new to the form. At the end of the day, the student teams shared their coding stories with their peers and were provided feedback on their storyline, logic, creativity and the quality of their code. They were also awarded certificates and badges for their hard work. But the biggest reward was each student's newly-gained confidence and the knowledge that coding can be fun.

Schools across the country participated in the all-day event, with CSE employees being on hand at many Ottawa locations to help with training and to inspire the students with stories from their own career. Approximately 2,900 girls across the country participated in the event, making Hackergal Canada's largest-ever hackathon.

While the event was designed to be fun and engaging, Hackergal's overall goal is to spark the interests of young Canadian girls in technology. By starting early to work on closing the gender gap in STEM careers, and creating more inclusive workplaces, we can strengthen Canada's future economy while fostering a workforce that truly reflects Canada's diverse population.

As an added bonus, CSE's talented employees were proud to volunteer their time, acting as mentors to local Ottawa schools on the day of the hackathon. For CSE employees that volunteered, it was a chance to go back to school. In fact, one of our volunteers was able to visit her old high school and spend the day inspiring students to pursue careers in STEM, opening their eyes to the possibilities that exist right here in Canada. Other volunteers were blown away by the willingness of the girls to learn. The positive atmosphere allowed students to tackle challenges and ask questions knowing that their fellow students would support and encourage them.

[1] Statistics Canada, International Women's Day... by the numbers, 2017

[2] Statistics Canada, Occupation data tables, 2016 census

[3] Statistics Canada, Canadian postsecondary enrolments and graduates, 2015/2016

ITSLC NEWS

Over the past several months, CSE's ITS Learning Centre (ITSLC) and Canada Revenue Agency (CRA) have successfully collaborated on the development and delivery of a custom cyber security course targeting the computer science (CS) population within CRA. ITSLC delivered this one-day course, which was tailored to suit CRA's immediate learning needs, to approximately 600 CRA employees in over 20 training sessions. The course focused on the cyber threat context specific to CRA, outlined the roles and responsibilities of various positions that play a part in the cyber security processes, and provided a role-based response to cyber security events. A team of CSE instructors, as well as experienced subject matter experts from CRA IT Security, offered best practices and practical learning experiences. This helped CRA's CS population to acquire the skills and knowledge required to better understand the cyber security context.

The ITSLC is pleased to introduce the Government of Canada Executive Cyber Security Education Program. The overall objective of this program is to provide senior departmental and agency officials with knowledge and access to tools and resources to better frame cyber/IT security-related decision-making. Intended for non-security audiences, this program includes two short e-learning modules and a facilitated, action learning session that supports better understanding of the cyber threat and IT security risk management environment. Uniquely, this program is designed to be tailored to the audience's specific business context and leverages local departmental threat and risk information to support facilitated discussions and activities.

To schedule a consultation to discuss delivery of this program within your organization, please contact the ITSLC at (613) 991-7110 or its-education@cse-cst.gc.ca

Attention IT Security practitioners! The ITS Learning Centre has scheduled its 4-day IT Security Risk Management Bootcamp on on August 20-23. This is a fantastic opportunity for IT Security practitioners outside of the NCR to come spend a week in beautiful Ottawa in the prime of summer! The 4-day course focuses on the overall concepts of IT security risk management, an introduction to ITSG-33, the risk management implementation process, and the development and application of security controls.

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