ISSUE 3

Securely Speaking:

Your Privacy & Security Bulletin

BY REBOOT COMMUNICATIONS LTD.

1. **The Power and Limitations of AI in Cybersecurity**
2. **How to Increase Your Cyber Security Resilience in Canada/ Comment augmenter votre résilience en matière de cybersécurité au Canada**
3. **Honouring Excellence:** *PICCASO Awards Canada Celebrates Champions of Data, Privacy, and Information Security*

reboot COMMUNICATIONS LTD

info@rebootcommunications.com

Forward

Welcome to ***Securely Speaking: Your Privacy & Security Bulletin***, a regular quarterly publication provided by Reboot Communications Ltd. The bulletin's objective is to explore the latest trends and developments in privacy and security, including the challenges and opportunities that arise from new technologies like artificial intelligence, the Internet of Things, and blockchain. We also examine the legal and ethical implications of data collection and use, and look at how organizations and individuals can take steps to protect themselves and their information.

We invite you to review articles and interviews which will provide our readers with a comprehensive understanding of the complex and evolving landscape of privacy and security, as well as actionable advice and best practices for navigating it.

We believe that a better understanding of these issues is crucial for all individuals, organizations, and governments, and that by fostering a dialogue around privacy and security, we can work together to create a safe, more secure, and more ethical future for all. We hope you enjoy reading this bulletin and join us in this important conversation.

We focus on these strategic pillars to provide a comprehensive and valuable resource for staying informed and protected in the digital age:

OUR KEY STRATEGIC PILLARS

Education & Awareness/ Best Practices

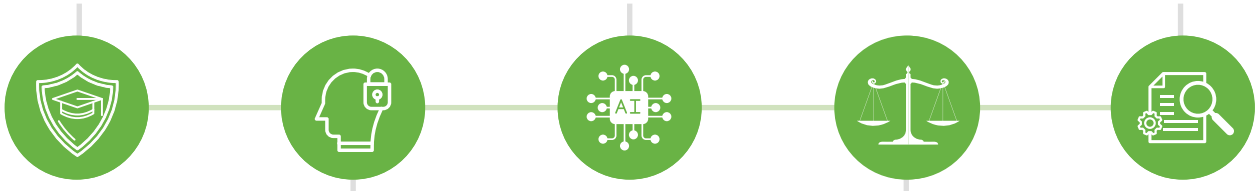
Educating readers on the latest privacy and security threats, best practices, and emerging trends.

Emerging Technologies

Emerging technologies and their potential impact on privacy & security (ie AI, IoT, blockchain).

Case Studies

Real world examples of privacy and security breaches and how they were addressed.



Thought Leadership & Industry News

Articles and interviews with experts in the privacy and security field.

Regulatory Developments

Information on the latest privacy and security regulations and laws.

Acknowledgments

ARTICLE 01

The Power and Limitations of AI in Cybersecurity

By: Jim Richberg | Head of Cyber Policy and Field CISO, Fortinet

ARTICLE 02

How to Increase Your Cyber Security Resilience in Canada ENGLISH »

Comment augmenter votre résilience en matière de cybersécurité au Canada FRANÇAIS »

By: The Canadian Centre for Cyber Security | Le Centre canadien pour la cybersécurité

ARTICLE 03

Honouring Excellence: ***PICCASO Awards Canada Celebrates Champions of Data, Privacy, and Information Security***

By: Nicholas Cheung | VP Privacy Training, The Privacy Pro and Advisory Board member, PICCASO Canada

ARTICLE 1

The Power and Limitations of AI in Cybersecurity

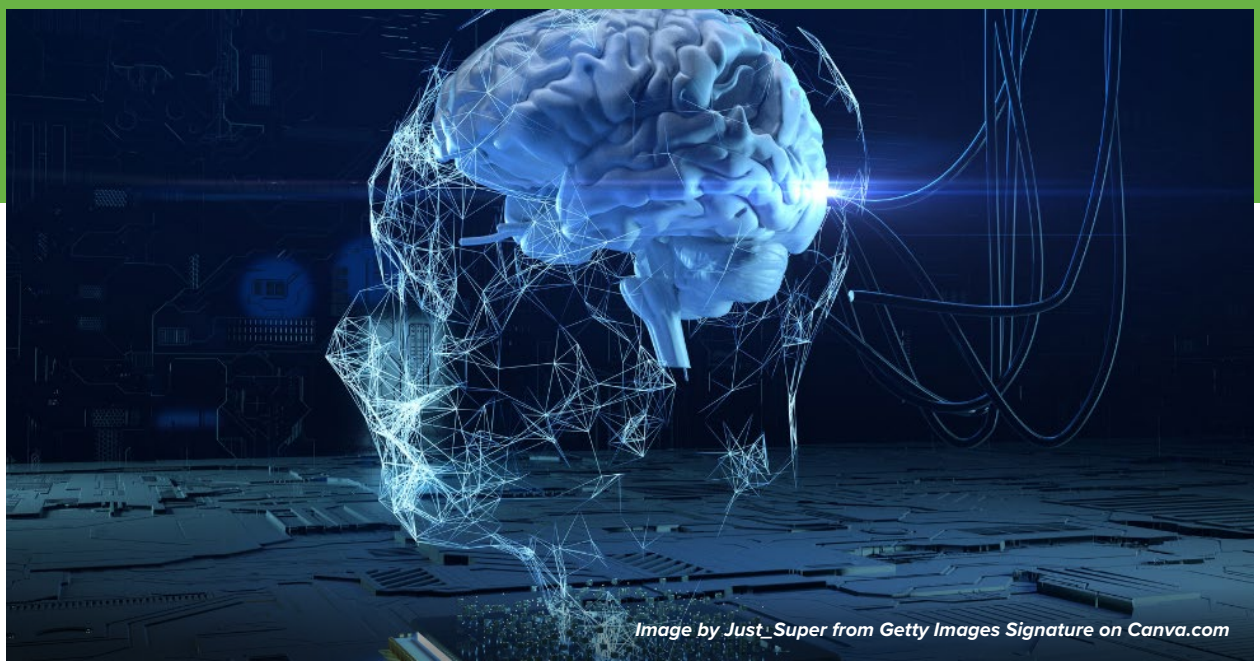


Image by Just_Super from Getty Images Signature on Canva.com

Today's security officers face new cybersecurity challenges because of the increasing use of artificial intelligence (AI), particularly generative AI (GenAI). This is not a surprise given the growing use of GenAI in the workplace, with fully two-thirds of organizations last year reporting that they were already beginning to use it and only 3% of enterprises not planning to adopt it.

AI has become a double-edged sword for cybersecurity. On the one hand, it has lowered the barrier to entry into cybercrime, enabling would-be criminals to generate malware even when they lack programming skills and providing more sophisticated criminals with capabilities few could have imagined a relatively short time ago. On the other hand, cyber defenders can take advantage of AI for intelligent automation and defense strategies.

AI Challenges and Impact on Cyberthreats

A would-be malicious cyber actor no longer needs any programming skills using GenAI because large language model (LLM) AI tools can be used to write malware. GenAI can dramatically increase the sophistication of spear-phishing attacks, elevating them above the content and spelling errors or awkward grammar that organizations often teach users to look for. Now, when a malicious actor harvests a victim's address book, they may also take email content and use it to generate tailored emails that match the syntax and subjects the compromised sender has used with each addressee.

AI-driven data analytics have given malicious cyber actors new tools for exploitation that make new classes of data attractive targets. A decade ago, only nation-states had the data centers and computing power to make it possible to exploit large data sets. The AI-driven revolution in data mining and the growth of pay-as-you-go computing power and storage mean that massive data sets have become exploitable and attractive targets for criminal actors and nation-states.

Using AI for Cyber Defense

Cybersecurity professionals use the term *attack surface* to describe the size and complexity of the digital environment and their difficulty in mapping or even fully understanding it. AI and the growing use of cybersecurity mesh architectures provide the opportunity to turn the size and complexity of this digital environment liability for network defenders into a potential advantage. Sensors linked in a common architecture allow network operators and defenders to generate data in real time, and increasingly powerful AI and ML can make sense of it in real time.

AI helps spot anomalous activity, determine which anomalies are attacks, generate a real-time response to block the attack and inoculate the rest of the organization's digital assets against further attacks. Remember, AI and ML are fueled by data – and the more data they have to train on and work with, the more effective they are.

As empowering as AI, enterprises face other challenges relating to using AI in the workplace. A key concern is that data contained in GenAI queries becomes part of the large language model (LMM) dataset used by these models. Other common problems include copyright infringement, revealing personal information, unknown use of biased or objectionable data, which is glib but patently wrong output. Many organizations are proceeding cautiously in their use of GenAI; but in most cases, the workforce does not understand the reasons. They are becoming accustomed to using GenAI in their private lives and experimenting with it independently in the workplace. GenAI has become the latest form of shadow IT that the security officers must deal with.

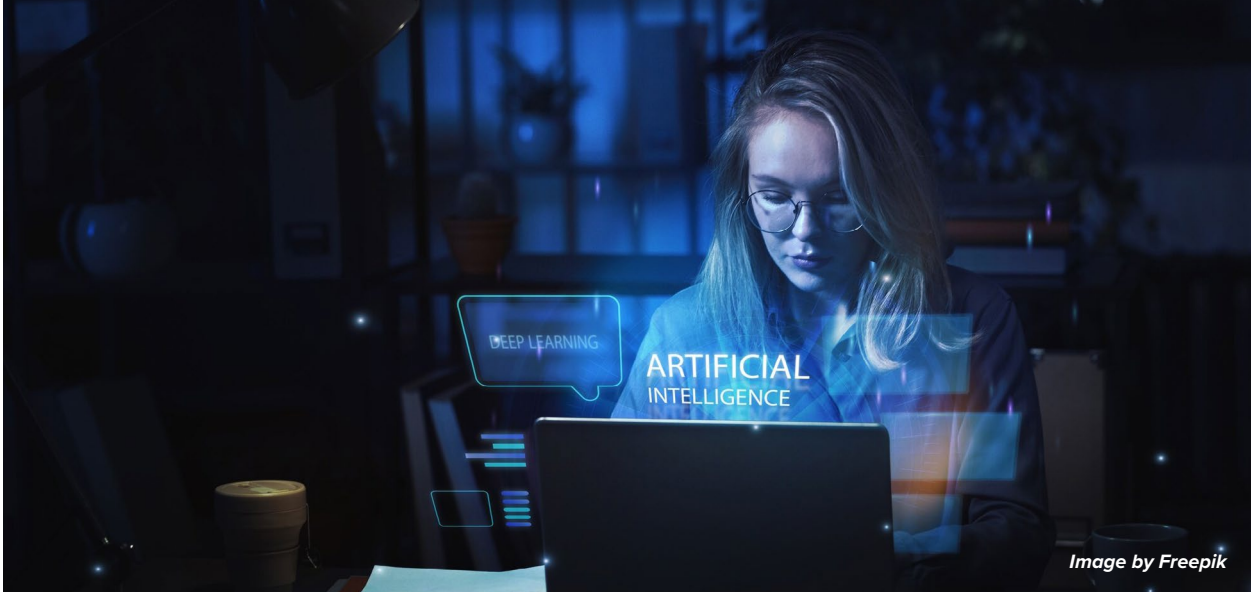


Image by Freepik

AI Best Practices

You should look at taking advantage of AI but be smart about it. Look to implement GenAI solutions using one of these options:

- **Run a foundational model in a private environment** so the training data and output remain segregated, ensuring your queries will not expose your organization's sensitive data to outsiders.
- **Run data loss prevention** as a filter on input into public LMM.
- Talk to your GenAI provider and **tailor your use cases with data security in mind. Look into privacy and security settings.** Can you prohibit your data from being saved? Can you do it manually? On a timed basis? Can you run queries with anonymized data?
- If you use third-party apps or Software-as-a-Service providers that have embedded GenAI into their tools, **ask questions and determine how they safeguard your input and results.**
- **Incorporate strict access controls.** Limit the use of specific datasets to authorized users.
- **Use privacy-enhancing technologies** with data obfuscation, encrypted data processing, federated/distributed analytics on centralized housed data, and data accountability tools.
- **Take a hard look at the volume of data.** The more data you provide, the greater the likelihood of leakage.
- **Train the team** using the model to reflect best practices, compliance, and threats.

AI-driven innovation is happening across the technology landscape, and it's up to organizations to take advantage of it. While an AI arms race is occurring between cyberattackers and defenders, the defense is well positioned.

By: Jim Richberg | Head of Cyber Policy and Field CISO, Fortinet | in linkedin.com/in/jim-richberg

Jim Richberg's role as Fortinet's Head of Cyber Policy and Global Field CISO leverages his nearly 40 years' experience driving innovation in cybersecurity and threat intelligence. Prior to joining Fortinet, Jim served as the US National Intelligence Manager for Cyber, the senior Federal Executive focused on cyber intelligence within the $80B+/100,000 employee US Intelligence Community (IC). He led the creation and implementation of cyber strategy for the 17 departments and agencies of the IC, set integrated priorities on cyber threat, and served as the senior advisor to the Director of National Intelligence on cyber issues.

Since joining Fortinet, Jim has been named a "Fed 100" and a "Pinnacle" awardee for his influence on technology in the U.S. Federal government, a "State Scoop 50" leader for driving innovation in state IT, and he was nominated as a "Security Pioneer" for his sustained contribution to cybersecurity. He is a member of the US IT Sector Coordinating Council, the CNBC Technology Executive Council, the Forbes Technology Council, and the World Economic Forum's Cybersecurity Leadership Community. He leads industry working groups focused on national cyber strategy, implementing Federal cybersecurity initiatives with the private sector, and on helping state and local government improve their cybersecurity. Jim received his undergraduate degree at the Honors Tutorial College of Ohio University and attended graduate school at M.I.T. and Stanford.

ARTICLE 2

ENGLISH

How to Increase Your Cyber Security Resilience in Canada

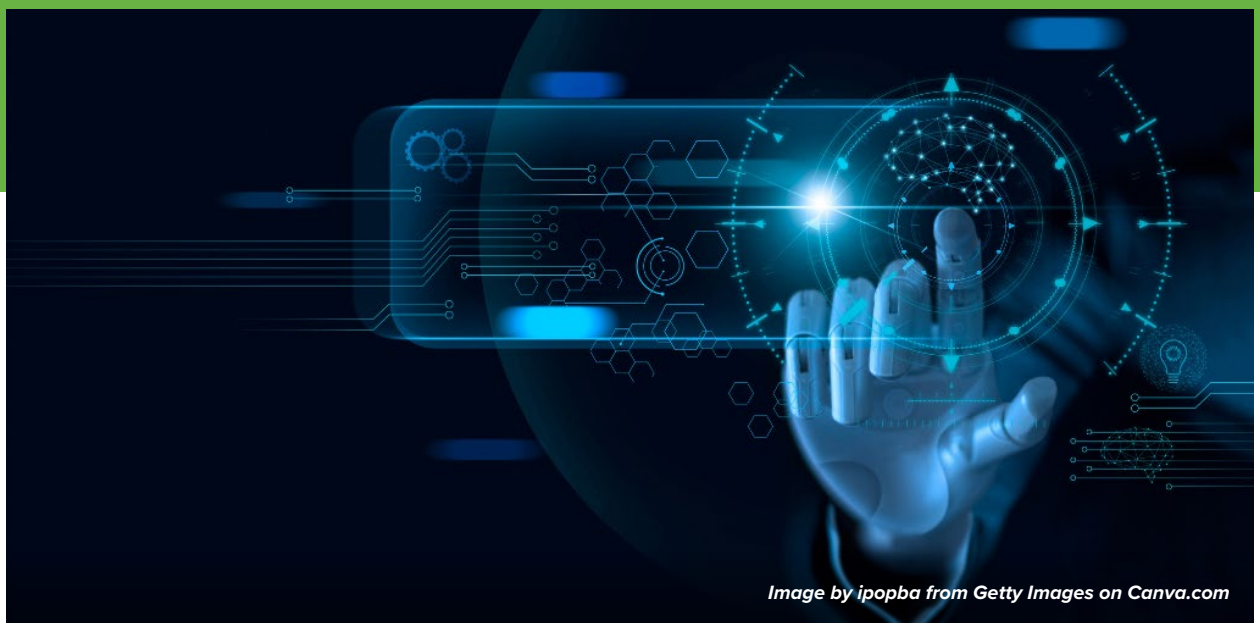


Image by ipopba from Getty Images on Canva.com

Digital technologies are now an integral part of our daily lives, with new developments emerging every day. Technologies connect Canadians from coast to coast to coast while linking us into a dynamic global network. Virtually everything Canadians do is touched by technology in some way – on a per capita basis, we spend the most time online of any country in the world, at 43.5 hours per Canadian per month.

As our world is transformed by digital innovation, it can expand the threat surface. Criminals and other malicious cyber threat actors – many of which operate outside our borders – take advantage of security gaps, low cyber security awareness, and technological developments in an effort to compromise cyber systems. They steal personal and financial information, intellectual property, and trade secrets. They disrupt and sometimes destroy the infrastructure that we rely on for essential services and our way of life.

Image by rawpixel.com on Freepik

In our most recent National Cyber Threat Assessment, the Canadian Centre for Cyber Security (Cyber Centre) focuses on five cyber threat narratives that we judge are the most dynamic and impactful and that will continue to drive cyber threat activity to 2024.

Key judgements

- **Ransomware is a persistent threat to Canadian organizations.** Cybercrime continues to be the cyber threat activity most likely to affect Canadians and Canadian organizations. Due to its impact on an organization's ability to function, ransomware is almost certainly the most disruptive form of cybercrime facing Canadians. Cybercriminals deploying ransomware have evolved in a growing and sophisticated cybercrime ecosystem and will continue to adapt to maximize profits.
- **Critical infrastructure is increasingly at risk from cyber threat activity.** Cybercriminals exploit critical infrastructure because downtime can be harmful to their industrial processes and the customers they serve. State-sponsored actors target critical infrastructure to collect information through espionage, to pre-position in case of future hostilities, and as a form of power projection and intimidation. However, we assess that state-sponsored cyber threat actors will very likely refrain from intentionally disrupting or destroying Canadian critical infrastructure in the absence of direct hostilities.
- **State-sponsored cyber threat activity is impacting Canadians.** We assess that the state-sponsored cyber programs of China, Russia, Iran, and North Korea pose the greatest strategic cyber threats to Canada. State-sponsored cyber threat activity against Canada is a constant, ongoing threat that is often a subset of larger, global campaigns undertaken by these states. State actors can target diaspora populations and activists in Canada, Canadian organizations and their intellectual property for espionage, and even Canadian individuals and organizations for financial gain.

- **Cyber threat actors are attempting to influence Canadians, degrading trust in online spaces.** We have observed cyber threat actors' use of misinformation, disinformation, and malinformation (MDM) evolve over the past two years. Machine-learning enabled technologies are making fake content easier to manufacture and harder to detect. Further, nation states are increasingly willing and able to use MDM to advance their geopolitical interests. We assess that Canadians' exposure to MDM will almost certainly increase over the next two years.
- **Disruptive technologies bring new opportunities and new threats.** Digital assets, such as cryptocurrencies and decentralized finance, are both targets and tools for cyber threat actors to enable malicious cyber threat activity. Machine learning has become commonplace in consumer services and data analysis, but cyber threat actors can deceive and exploit this technology. Quantum computing has the potential to threaten our current systems of maintaining trust and confidentiality online. Encrypted information stolen by threat actors today can be held and decrypted when quantum computers become available.

Image by da-kuk from Getty Images Signature on Canva.com

Thankfully, you are not alone when facing these cyber threats.

The Cyber Centre is the single unified source of expert advice, guidance, services and support on cyber security for Canadians and Canadian organizations. The Cyber Centre welcomes partnerships that build a stronger, more resilient Canadian cyberspace.

The Cyber Centre's free services include:

- Sharing awareness reports and cyber threat intelligence notifications;
- Providing tools to strengthen your cyber defence;
- Leveraging its expertise to provide you with actionable information to resolve a cyber incident; and
- Hosting regular engagements to improve the cybersecurity of Canadian organizations.

Ready to raise your cyber security bar? For more information on services offered, please check out our website: www.cyber.gc.ca/en. Please note, the Cyber Centre releases numerous publications throughout the year that focus on the various threats affecting different industries. We also provide guidance and best practice information material to increase the cyber security posture of individuals, small and medium sized organizations, and large enterprises. For more information, please visit our publications page: www.cyber.gc.ca/en/guidance.

For general inquiries, please contact us at contact@cyber.gc.ca.

By: The Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security (The Cyber Centre), a part of the @Communications Security Establishment (CSE) | Centre de la sécurité des télécommunications (CST)

@cybercentre_ca

Lire l'article en français

ARTICLE 2

FRANÇAIS

Comment augmenter votre résilience en matière de cybersécurité au Canada

Image by Freepik

Les technologies numériques font maintenant partie de notre quotidien, tout comme les nouveaux développements que nous constatons chaque jour. Les technologies rapprochent les Canadiennes et Canadiens d'un océan à l'autre et les relient à un réseau mondial dynamique. Pratiquement tout ce que les Canadiennes et Canadiens font est lié à la technologie d'une manière ou d'une autre. Par personne, le Canada est le pays où la population passe le plus de temps en ligne, c'est-à-dire 43,5 heures par personne par mois.

Alors que l'innovation numérique transforme notre monde, cette innovation peut accroître l'exposition aux cybermenaces. Les criminelles et criminels et autres auteures et auteurs cybermenace malveillants – dont plusieurs mènent leurs activités hors de nos frontières – se servent des lacunes en matière de sécurité, du manque de connaissances sur la cybersécurité et des développements technologiques pour tenter de compromettre les cybersystèmes.

Image by DC Studio on Freepik

Ils volent des données personnelles et financières, des éléments de propriété intellectuelle et des secrets commerciaux. Ils perturbent et parfois détruisent les infrastructures dont nous dépendons pour obtenir des services essentiels et soutenir notre mode de vie.

Dans la plus récente Évaluation des cybermenaces nationales, le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) a choisi de se concentrer sur cinq discours liés aux cybermenaces qui sont considérés être les plus évolutifs et percutants, et qui vont continuer de dominer les activités de cybermenace jusqu'en 2024.

Principaux avis

- **Les rançongiciels représentent une menace omniprésente pour les organisations canadiennes.** La cybercriminalité continue d'être l'activité de cybermenace la plus susceptible de toucher la population canadienne et les organisations canadiennes. En raison de leur incidence sur la capacité d'une organisation de fonctionner, les rançongiciels sont presque assurément la forme la plus perturbatrice de cybercriminalité à laquelle sont confrontés les Canadiennes et Canadiens. Les cybercriminelles et cybercriminels qui déploient des rançongiciels ont su évoluer au sein d'un écosystème de cybercriminalité grandissant et sophistiqué; et ils vont continuer à s'adapter de manière à maximiser les profits.
- **Les activités de cybermenace représentent un risque de plus en plus grand pour les infrastructures essentielles.** Les cybercriminelles et cybercriminels exploitent les infrastructures essentielles, car toute interruption peut être préjudiciable pour les processus industriels et leurs clients. Les auteures et auteurs de menace parrainés par des États ciblent les infrastructures essentielles afin d'obtenir de l'information en se livrant à l'espionnage, de se prépositionner en cas d'éventuelles hostilités et de faire acte de force et d'intimidation. Toutefois, selon nos observations, il est très probable que les auteures et auteurs de cybermenace parrainés par des États s'abstiennent de perturber ou de détruire intentionnellement les infrastructures essentielles du Canada en l'absence d'hostilités.

- **Les activités de cybermenace parrainées par des États ont des répercussions sur la population canadienne.** Nous estimons que les cyberprogrammes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord sont les plus grandes cybermenaces stratégiques ciblant le Canada. Les activités de cybermenace parrainées par des États visant le Canada représentent une menace constante et continue qui s'inscrit souvent dans des campagnes mondiales plus vastes qu'entreprennent ces États. Les auteures et auteurs de menace parrainés par des États peuvent cibler les populations et les militantes et militants de la diaspora au Canada, les organisations canadiennes et leur propriété intellectuelle à des fins d'espionnage, et même les particuliers et les organisations canadiennes dans le but d'obtenir un gain financier.
- **Les auteures et auteurs de cybermenace tentent d'influencer les Canadiennes et Canadiens et de briser la confiance accordée aux espaces virtuels.** Nous avons observé que ces auteures et auteurs ont de plus en plus recours à la mésinformation, à la désinformation et à la malinformation (MDM) depuis les deux dernières années. Les technologies d'apprentissage automatique font en sorte qu'il est plus facile de créer du faux contenu toujours plus difficile à détecter. Par ailleurs, les États-nations démontrent de plus en plus de capacité et de volonté envers l'utilisation de MDM pour défendre leurs intérêts géopolitiques. Nous considérons que l'exposition de la population canadienne aux campagnes de MDM devrait presque assurément augmenter au cours des deux prochaines années.
- **Les technologies perturbatrices entraînent de nouvelles possibilités et menaces.** Les actifs numériques, comme la cryptomonnaie et les systèmes financiers décentralisés, sont des cibles et des outils qui permettent aux auteures et auteurs de cybermenace de mener des activités de cybermenace malveillantes. L'apprentissage automatique est utilisé de manière courante dans les services aux consommatrices et consommateurs et l'analyse de données, mais les auteures et auteurs de cybermenace peuvent déjouer et exploiter cette technologie. L'informatique quantique pourrait devenir une menace pour nos systèmes actuels qui inspirent confiance et qui assurent la confidentialité en ligne. En effet, l'information chiffrée qui est volée par des auteures et auteurs de menace aujourd'hui pourrait être conservée et déchiffrée après l'arrivée des ordinateurs quantiques.

Heureusement, vous n'êtes pas seules et seuls lorsque vient le moment de contrer ces cybermenaces.

Le Centre pour la cybersécurité est la seule source unifiée de conseils, de services et de soutien d'expertes et experts en matière de cybersécurité pour la population et les organisations canadiennes. Il veut établir des partenariats qui aident à bâtir un cyberespace plus fort et plus résilient au Canada.

Les services gratuits que propose le Centre pour la cybersécurité comprennent :

- communiquer des rapports de sensibilisation et des notifications du renseignement sur les cybermenaces;
- fournir des outils pour renforcer la cyberdéfense;
- tirer avantage de son expertise pour fournir de l'information exploitable afin de résoudre un cyberincident;
- organiser régulièrement des événements pour améliorer la cybersécurité des organisations canadiennes.

Êtes-vous prêtes et prêts à relever la barre de cybersécurité? Pour de plus amples renseignements sur les services offerts, consultez notre site Web : www.cyber.gc.ca/fr. Il importe de souligner que le Centre pour la cybersécurité diffuse de nombreuses publications au cours de l'année qui traitent de diverses menaces pouvant toucher différentes industries. Il fournit également du matériel d'information sur les pratiques à adopter et des conseils pour accroître la posture de cybersécurité des personnes, des petites et moyennes organisations, et des grandes entreprises. Pour obtenir de plus amples renseignements, veuillez consulter notre page de publication : www.cyber.gc.ca/fr/orientation.

Pour toute demande générale, veuillez communiquer avec nous à l'adresse contact@cyber.gc.ca.

Par : Le Centre canadien pour la cybersécurité

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité), qui fait partie du @Communications Security Establishment (CSE) | Centre de la sécurité des télécommunications (CST)

@centrecyber_ca

Honouring Excellence:
PICCASO Awards Canada Celebrates Champions of Data, Privacy, and Information Security

Image by rawpixel.com on Freepik

In an age where technological progress, propelled by innovations such as artificial intelligence (AI), is advancing at an unprecedented pace, the stewardship of data privacy and information security has never been more crucial. Canada has emerged as a global and regional leader pioneering groundbreaking legislation and fostering innovative approaches such as privacy by design. And yet, media narratives often focus on cyber breaches and privacy mishaps, overshadowing Canada's successes in privacy and data security.

It is time to shift the spotlight and shine a light on the many success stories that Canada has in the privacy and data security landscape. The inaugural PICCASO Awards Canada, which is set to take place on June 11, 2024 in Toronto will honour those privacy champions who tirelessly safeguard data and information, making a significant contribution in Canada's commitment to protecting data security and privacy rights. Building on the success of the PICCASO European edition, the awards aim to shift the narrative from privacy breaches to celebrating achievements and innovations within the industry. Presented by PICCASO Canada, a non-profit collaboration of PICCASO and The Privacy Pro, this prestigious gala event, will take place at the Toronto Region Board of Trade in the presence of industry stalwarts in the data, privacy and information security space with TELUS as the founding sponsor, along with PwC Canada and AccessPrivacy by Osler as platinum sponsors.

Philippe Dufresne, Privacy Commissioner of Canada who is also the keynote speaker for the awards gala, expressed his enthusiasm for the PICCASO Awards coming to Canada *"I am pleased that the PICCASO Privacy Awards are coming to Canada. We increasingly see organizations recognizing that privacy is a strategic value, especially in this technology driven era. I believe that there is tremendous opportunity in showcasing how this is translating into concrete, positive initiatives in different sectors and industries across the country."*

Image by rawpixel.com on Freepik

The awards feature 15 categories spanning various sectors, including the public sector, not-for-profit organizations, academia and health privacy leadership. While the individual awards recognize rising stars, outstanding privacy lawyers, engineers, and thought leaders, the team accolades commend collaborative efforts and innovative initiatives in data protection.

PICCASO Awards Canada has also collaborated with a distinguished panel of judges with a remarkable background, including Elizabeth Denham, former UK Information Commissioner, Chantal Bernier, former interim Privacy Commissioner of Canada, and Dr. Khaled El Emam, Canada Research Chair in Medical AI at the University of Ottawa, for a fair and independent evaluation of nominations.

Nominations for exceptional individuals or teams are now open, inviting experts and organizations across sectors in Canada to recognize those driving innovation and excellence in privacy and security.

Nominations are **free of charge** and must be submitted by April 7, 2024.

To nominate and learn more about the awards, categories, and judging process, visit www.piccasoawards.ca. Let's come together to celebrate the champions of data privacy and security, driving innovation and excellence in safeguarding our digital future.

Reboot Communications is a proud media sponsor of PICCASO Awards Canada.

Award Categories

Sector Specific Awards	Individual Awards	Team Awards	Awards for Innovation
• Public Sector Leadership • Not-for-Profit Leadership • Health Privacy Leadership	• Rising Star • Outstanding Privacy Lawyer • Outstanding Privacy Engineer • Privacy Leader Academia/ Thought Leader • Privacy Award for Achievement • Outstanding Privacy Officer • Indigenous Leadership Award	• Data Partnership Award • Privacy Team of the Year • Best Privacy Program Award	• Most Impactful Privacy Product/ Service • Privacy Innovation Award

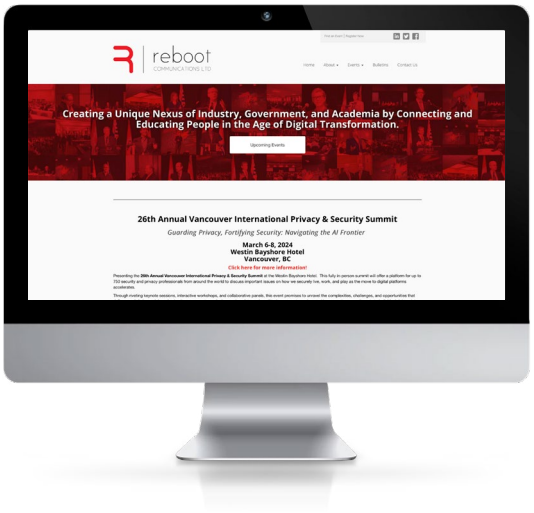
By: Nicholas Cheung | VP Privacy Training, The Privacy Pro and Advisory Board member, PICCASO Canada

info@piccaso.ca | linkedin.com/company/piccaso-canada

Copyright

ISSUE 3 EBOOK EDITION | *MARCH, 2024*

Editor: **Greg Spievak**



FIND OUT MORE & SUBSCRIBE

For more information or to subscribe and receive the ***Securely Speaking: Your Privacy & Security Bulletin*** regularly, email info@rebootcommunications.com.