



MAGNET
FORENSICS®

The Erosion of Social Capital Online and How We Can Revive It
2022 Cybersecurity and Privacy Institute Conference // Waterloo, ON
Neil Desai, VP, Magnet Forensics // Senior Fellow, CIGI



Magnet Forensics

Digital Investigation Solutions used by the global public safety community to assist in their criminal investigations and enterprises in incident response



**Built by Police
for Police**



Committed to Giving Back



Proudly Canadian

MISSION:

To impact people's lives by uncovering the truth and empowering others to make a difference.

VISION:

**Help modernize policing for the 21st century:
Equipping law enforcement agencies with the necessary tools to combat the crimes of today to help them more effectively serve and protect their citizens.**

Magnet Forensics Core Capabilities

Current solutions being used by in investigations with digital evidence

COLLECTION



- Get data off PCs, smartphones, tablets, IoT devices and the cloud

PROCESSING



- Piece together critical evidence from hundreds of apps

ANALYSIS



- Help make sense of all the data
- Give investigators a better start with AI and visualization tools

REPORTING



- Prosecutor and jury friendly reports
- Forensically sound to hold up under scrutiny

Trusted by over 4000 agencies in over 100 countries

Police, national security and other agencies with investigative authorities

Municipal/Provincial Federal US Global



OPP



Waterloo Regional Police Service



Toronto Police Service



Barrie Police Service



London Police Service



Hamilton Police Service



CBSA



RCMP



CFNIS



DND



Department of Finance

Government of Canada

Competition Bureau

CRA



DHS



DOD



USSS



FBI



DIA



NYPD



UK National Crime Agency



Hong Kong Customs & Excise



French National Police



London Met Police



Singapore Police Force



Dutch National Police

Global Private Sector Adopting Magnet's Solutions

Fortune 500, Pro-Services Firms and Digital Forensics/Cyber Specialists



vodafone



Shell



US-Terrorism Case

Magnet Forensics' products making a tangible impact



30 devices confiscated in the investigation



Living suspect's motive was established through digital evidence recovered by a Magnet tool.

Communication/internet activity across multiple apps/languages



“Tsarnaev had extremist material on multiple devices, FBI Agent Testified”

– Boston Globe



6.7 terabytes of discovery

1 month to analyze the digital evidence.



“Thousands of gigabytes of digital evidence”



Indian Fraud Case

Magnet Forensics' products making a tangible impact



Kolkata Police outsourced fraud investigation to "Truth Labs" who have technical digital forensic expertise

Suspects accused of impersonating Microsoft support workers.



“Digital investigators recovered instruction documents outlining how to speak with victims...”

100s of victims' PII and banking information found in recovered evidence



Canadian-Child Exploitation Case

Magnet Forensics' products making a tangible impact



18 computers and hard-drives
confiscated in the investigation

Attempts to lure minors over
multiple social media applications



“Jail for teacher who lured kids online”


- CP24



Conviction secured of a local
teacher who had taught children
whom he was communicating with.

2,000 child pornography video
9,500 child pornography image
recovered using Magnet's tool



An aerial night view of a city skyline, likely New York City, featuring numerous skyscrapers and illuminated buildings. The scene is dark, with the city lights providing the primary illumination. The text is centered over the image.

The Realities of Cybercrime and Policing Today

Cyberattacks are growing in number and complexity

Police agencies are limited in their ability to investigate



PRIVACY & SECURITY

Northern Ontario police force recovering from ransomware attack

[Home](#)



TORONTO | News

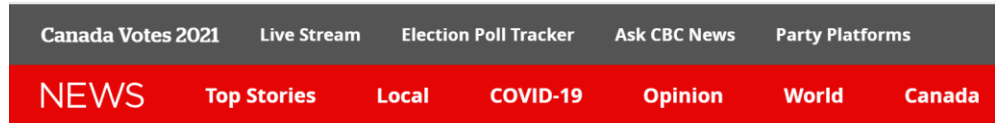
Toronto hospital working to restore systems after being struck by cyber attack



Canada's federal election could be a target for cyber attacks: expert

BY KELLYTURNER
POSTED SEP 3, 2021 10:33 AM EDT LAST UPDATED SEP 3, 2021 AT 1:58 PM EDT

CBC | MENU | Canada Votes 2021



World

Major ransomware attack aimed at tech provider leaves other companies scrambling



Cybercrime

Entering the Canadian political discourse

▼ Open letter to Canadian organizations about ransomware

RE: Protecting yourself from the threat of ransomware

December 6, 2021

Fellow Canadians,

Since the beginning of the COVID-19 pandemic, we have all been reminded of how crucial the internet is to our way of life. More and more of us have been working and studying from home and conducting business online, and it is therefore more important than ever that we take steps to remain cyber safe.

Across the world, we have seen a marked rise in the volume and range of cyber threats – and Canada is no exception. This includes a surge in ransomware incidents – a tactic wherein threat actors deny access to an organization's most important informational or vital systems until organizations pay the threat actor, usually in digital currency. This year, we have seen a growing number of ransomware threats targeting Canadian small and medium-sized businesses, health care organizations, utility organizations, and municipalities.

There is, however, good news. By adopting basic but appropriate cyber security practices, we can all help stop the vast majority of cyber incidents targeting Canadians.

You, and your organization, are not alone.

The Communications Security Establishment's Canadian Centre for Cyber Security (the Cyber Centre) and the Royal Canadian Mounted Police (RCMP) urge all Canadian organizations and businesses to take steps to review and strengthen the cyber security of your networks, systems, and information – and we are here to help.

Together with law enforcement agencies, and other federal and international partners, we are working hard to make threat information more publicly available and provide you with specific advice and guidance to help you stay safe from the impacts of ransomware. Canada is also working closely with our allies to pursue cyber threat actors and disrupt their capabilities. We are also assisting in the recovery of organizations compromised by ransomware, and helping them to be more resilient going forward.

To keep yourselves and all Canadians safe, we're asking you to take action. Our national cyber security must involve efforts from industry partners, small and medium sized businesses, and all Canadians. Our message is clear: taking basic steps to ensure your organization's cyber security will pay swift dividends.

Taking action is worth it.

To assist your organization, the Cyber Centre has published best practice guidelines. As Canada's national technical authority for cyber security, the Cyber Centre provides extensive advice and [recommended IT actions](#) to organizations to help mitigate the threat of ransomware. Canadian organizations should invest in these inexpensive but effective [baseline cybersecurity controls](#) to limit their exposure to cyber attacks. You can refer to the [Ransomware Playbook](#) for specific advice. Once you have implemented these practices, we encourage you to register with the [CyberSecure Canada](#) program, thus attesting to your cyber security status and certifying that protective measures are in place.

If your organization is threatened with or falls victim to ransomware, you should implement your recovery plan, seek professional cyber security assistance, and immediately report the incident to the Cyber Centre's [online portal](#) as well as your local police. Timely reporting is critical to help us identify the threat vector and update our guidance, make linkages across separate incidents, launch law enforcement investigations and take action against cybercriminals, and ultimately reduce the risk to other Canadians.

It's time to think seriously about cyber security. We urge you to take stock of your organization's online operations, protect your important information and technologies with the latest cyber security measures, build a response plan, and ensure that your designated IT security personnel are well-prepared to respond to incidents.

Your government is here to help.

Together, we can make Canada the most cyber secure place to conduct business and other activities online.

Sincerely,

The Honourable Anita Anand, PC, MP
Minister of National Defence

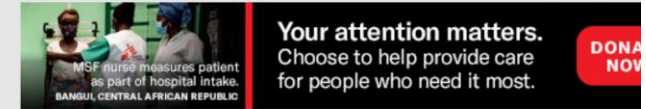
The Honourable Marco E. L. Mendicino, PC, MP
Minister of Public Safety

The Honourable Bill Blair, PC, MP
Minister of Emergency Preparedness and President of the Queen's Privy Council for Canada

The Honourable Mary F. Y. Ng, PC, MP
Minister of International Trade, Export Promotion, Small Business, and Economic Development

CBC | MENU ▾

NEWS Top Stories Local Climate World Canada Politics



Politics


Federal government may make reporting cyberattacks mandatory: Mendicino

"Increasingly, criminality is conducted on the internet and investigations are international in nature, yet investigative tools and RCMP capacity have not kept pace. Growing expectations of policing responsibilities and accountability, as well as complexities of the criminal justice system, continue to overwhelm the administrative demands within policing."



-RCMP Memo to Commissioner Lucki

Public Reporting of Cybercrime

Are police agencies able to maintain the public's trust under the status quo?

 Communications Security Establishment Centre de la sécurité des télécommunications

Q English Sign in

[My Cyber Portal](#) / Report a cyber incident

Report a cyber incident

1. Disclaimer 2. About You 3. About the Incident 4. Review and Submit

This form will take approximately five minutes to complete.

You are about to report a cyber incident to the Canadian Centre for Cyber Security (Cyber Centre).

Reporting a cyber incident helps the Cyber Centre keep Canada and Canadians safe online. Your information will enable us to provide cybersecurity advice, guidance and services.





We recommend that this form not be completed on a network or device that you believe has been compromised.

Information provided to the Cyber Centre, including personal information, is protected in the same way we protect our own confidential information: held securely, with strictly limited access. We may share any such derived cyber threat information with domestic and international partners involved with cyber security (both in the public and private sector), as well as with operators of other information infrastructures of importance to the Government of Canada, for the purposes of protecting those infrastructures.

[Privacy Statement](#)

I have read and accept the above Disclaimer and terms of the Privacy Statement. *

[Next](#)

Canadian Centre for Cyber Security Terms and Conditions    

The Cyber-Talent Crunch

Can police agencies keep pace?

There will be 3.5 million unfilled cyber-security jobs by 2021, up from 1 million positions in 2014.



Cybercrime

The face(less) suspects and victims



An aerial night view of a city skyline, likely New York City, featuring several prominent skyscrapers illuminated against a dark sky. The city lights create a dense pattern of small points of light, with larger, brighter structures standing out. The overall tone is dark and futuristic.

Technology Trends and its Trajectory for Public Safety

Technology Transforming the Rule of Law

Encryption



Technology Transforming the Rule of Law

Cloud Computing



Technology Transforming the Rule of Law

The Dark Web



Technology Transforming the Rule of Law

Artificial Intelligence



Technology Transforming the Rule of Law

Web 3.0 - Cryptocurrencies / Blockchain / Metaverse



An aerial night view of a city skyline, likely New York City, featuring numerous illuminated skyscrapers and a dense urban landscape. The image is dark with blue and white highlights from the city lights.

The Opportunities

Opportunity to build public trust, safety and prosperity

General purpose, policing technologies and platforms for the vulnerable



Opportunity to build public trust and safety

Innovation in public policy



Opportunity to build public trust and safety

Innovation in career opportunities



Thank you // Discussion

Contact Details:
neil.desai@magnetforensics.com

