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, computers, 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
<table>
<thead>
<tr>
<th>Municipal/Provincial</th>
<th>Federal</th>
<th>US</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPP</td>
<td>CBSA</td>
<td>DHS</td>
<td>NCA</td>
</tr>
<tr>
<td>Waterloo Regional Police Service</td>
<td>RCMP</td>
<td>FBI</td>
<td>National Crime Agency</td>
</tr>
<tr>
<td>CFNIS</td>
<td>DND</td>
<td>DOD</td>
<td>UK National Crime Agency</td>
</tr>
<tr>
<td>Toronto Police Service</td>
<td>DIA</td>
<td>DIA</td>
<td>London Met Police</td>
</tr>
<tr>
<td>Barrie Police Service</td>
<td>Government of Canada</td>
<td>USSS</td>
<td>Hong Kong Customs &amp; Excise</td>
</tr>
<tr>
<td>London Police Service</td>
<td>Department of Finance</td>
<td>NYPD</td>
<td>Singapore Police Force</td>
</tr>
<tr>
<td>Hamilton Police Service</td>
<td>Competition Bureau</td>
<td>French National Police</td>
<td></td>
</tr>
</tbody>
</table>
Global Private Sector Adopting Magnet’s Solutions
Fortune 500, Pro-Services Firms and Digital Forensics/Cyber Specialists
US-Terrorism Case
Magnet Forensics’ products making a tangible impact

30 devices confiscated in the investigation
Communication/internet activity across multiple apps/languages
Living suspect’s motive was established through digital evidence recovered by a Magnet tool.

"Tsarnaev had extremist material on multiple devices, FBI Agent Testified"
– Boston Globe

1 month to analyze the digital evidence.

6.7 terabytes of discovery
"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”

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

2,000 child pornography videos
9,500 child pornography images
recovered using Magnet’s tool

- CP24
The Realities of Cybercrime and Policing Today
Cyberattacks are growing in number and complexity. Police agencies are limited in their ability to investigate.

Northern Ontario police force recovering from ransomware attack.

Toronto hospital working to restore systems after being struck by cyber attack.
Cybercrime
Entering the Canadian political discourse

Open letter to Canadian organizations about ransomware

RE: Protecting yourself from the threat of ransomware
December 8, 2021

Dear Fellow Canadians,

With the rapid growth of the COVID-19 pandemic, we have all been reminded how the threat 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 surge in ransomware attacks — a tactic wherein threat actors deny access to an organization’s most important internal or vital systems, and extract a ransom demand in exchange. This year, we have seen a growing number of ransomware attacks targeting Canadian small and medium businesses, putting them at risk of financial loss and reputational damage.

There is, however, good news. By adopting best practices and adopting cyber security procedures, we can all help stop the vast majority of ransomware attacks targeting Canadians.

Yes, and we are not alone.

The Communications Security Establishment Canada Cyber Security (the Cyber Centre) and the Royal Canadian Mounted Police (RCMP) are two Canadian organizations that provide practical advice and guidance to help stop you stay safe from the threats of ransomware. Canada is also working closely with our allies to push cyber threat actors and disrupt their capabilities. We are also working in the recovery of organizations compromised by ransomware, and helping them to be more resilient going forward.

To keep ourselves and all of Canadians safe, we must all 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 secure your organization’s cyber security will pay off in the long run.

We propose a plan of action.

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 practical advice and guidance to organizations in the public sector. Government of Canada organizations should lead in these demonstrations by not prioritizing cyber security tasks, but instead preparing to respond to cyber threats.

You can refer to the Canadian Cybersecurity Challenge for more information. Once you have implemented these practices, we encourage you to register with the Canadian Cybersecurity Challenge program, thus enabling to your cybersecurity status and certifying that your protective measures are in place.

If your organization is finalized with a lab, refer to the Cybercentre, you should implement your recovery plan, as proposed by the Canadian Cybersecurity Challenge. This will help ensure that the organization is prepared to respond to cyber attacks. You can refer to the Cybercentre’s website for more information.

Your organization is not alone. We want to keep our Canadian organizations safe online, protect your information and technologies with the latest cyber security measures, and provide a robust response plan to ensure that your organization is well-prepared to respond to incidents.

Your organization is a key to our future.

Together, we can raise Canada's most cyber secure place to conduct business and other activities online.

Sincerely,

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

The Honourable Bill Blair, PC, MP
Minister of Emergency Preparedness and Minister of Border Security and Organized Crime Reduction

The Honourable Yves-François Blanchet, MP
Leader of the Opposition

The Honourable Alice Huyer, PC, MP
Minister of National Defence

The Honourable Steven Blaire, MP
Minister of National Defence

The Honourable François-Philippe Champagne, MP
Minister of Innovation, Science and Economic Development

---

"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?
The Cyber-Talent Crunch
Can police agencies keep pace?

There will be 3.5 million unfilled cybersecurity jobs by 2021, up from 1 million positions in 2014.
Cybercrime
The face(less) suspects and victims
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
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