Securing the Smart Municipality

With digital transformation comes great responsibility

About David

- Bachelor of Arts, Information and Communications Studies

- Master of Business Administration

- Certified Information Security Manager

- Former journalist, soldier
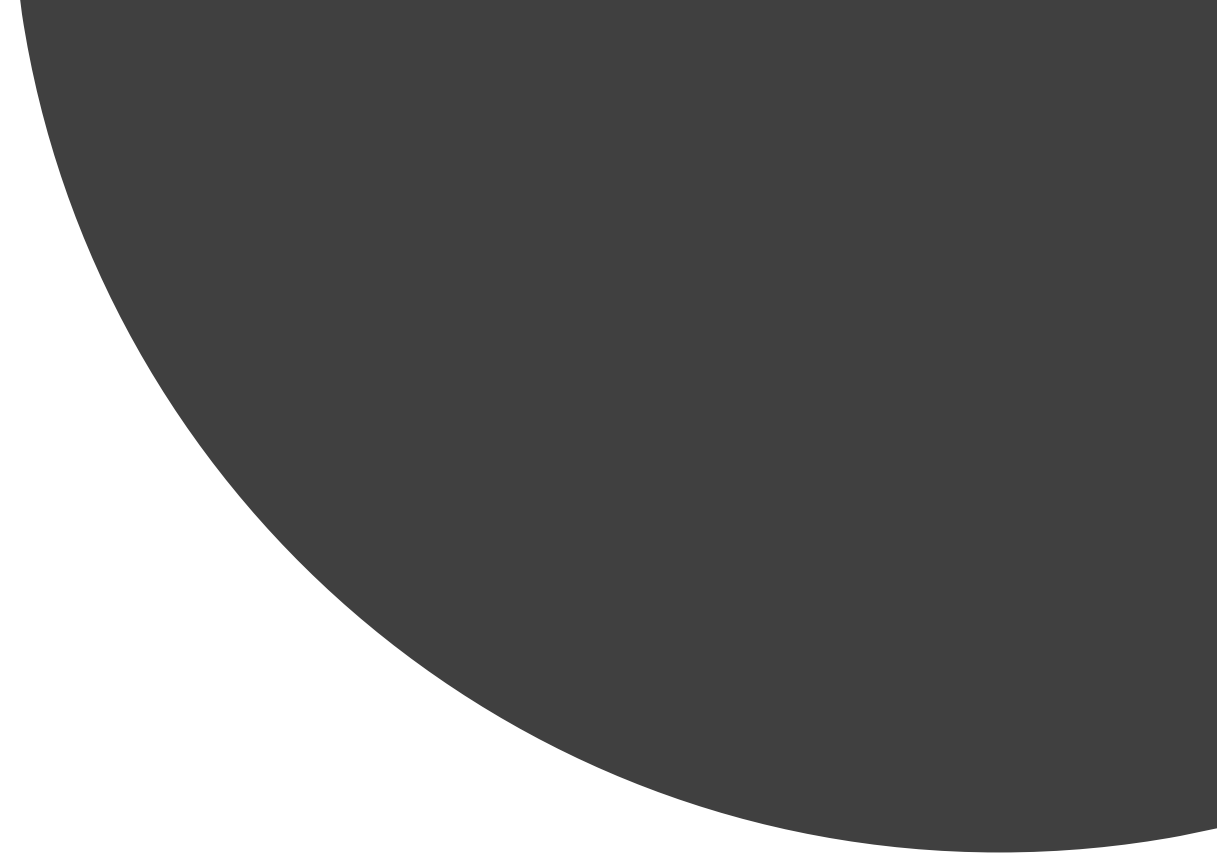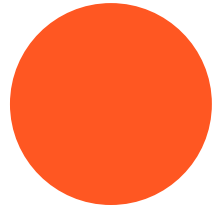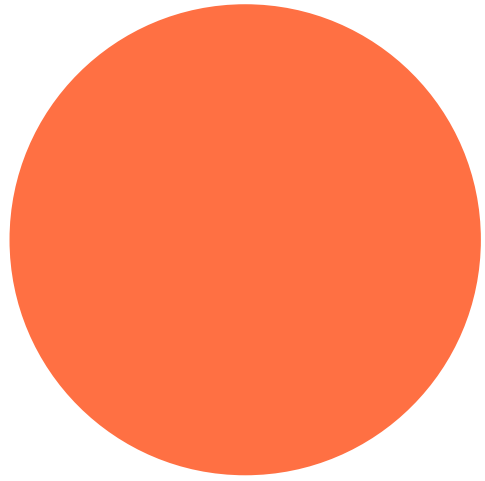
BEAUCERON

Our story

- Born from experience at the University of New Brunswick

- Dozens of clients across North America with users in 30+ countries

- Proudly Canadian

Cyber history

- "Cyberspace" - William Gibson, '82 – Burning Chrome

- Cybernetics – Norbert Weiner, 1948

- Kubernétēs – Greek for steersman or helmsman

"The trouble with our times is that the future is not what it used to be. "
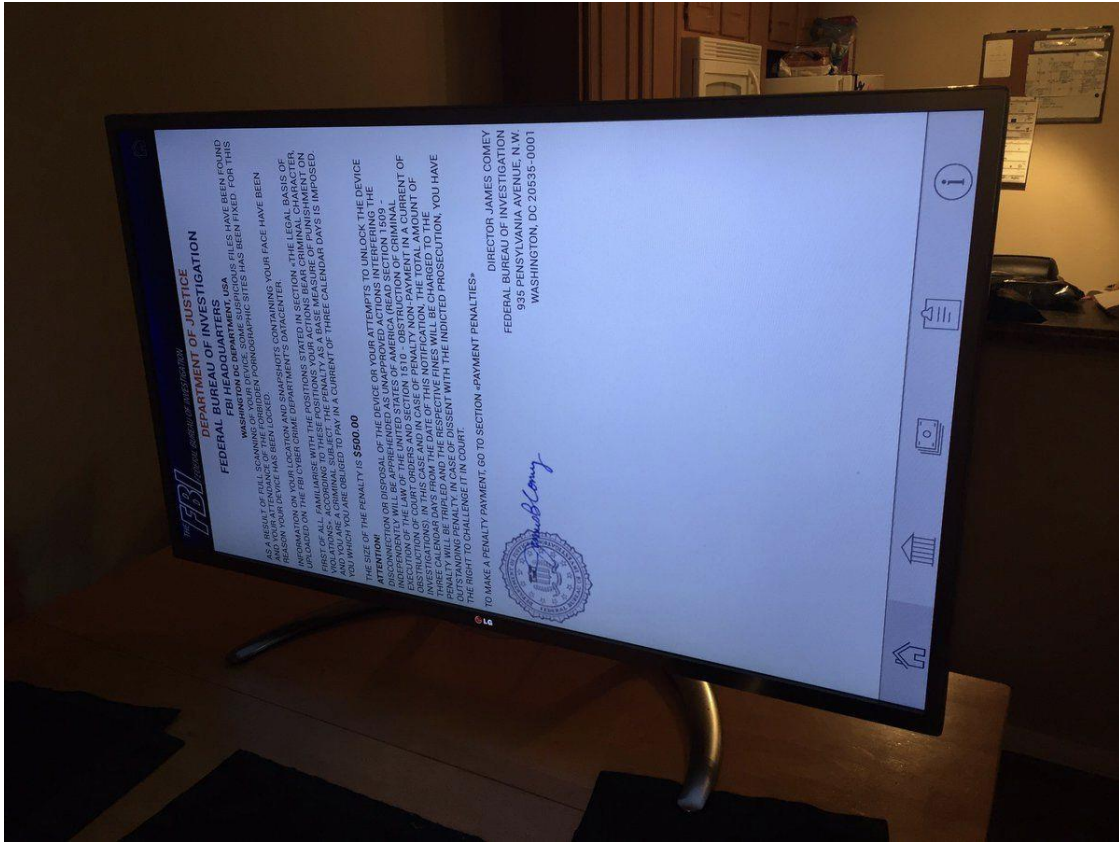
— **Paul Valéry**

How we perceive the Internet

What it's really like

The Internet was never designed to be secure

Hacking the home

How we ended up with hackable cars
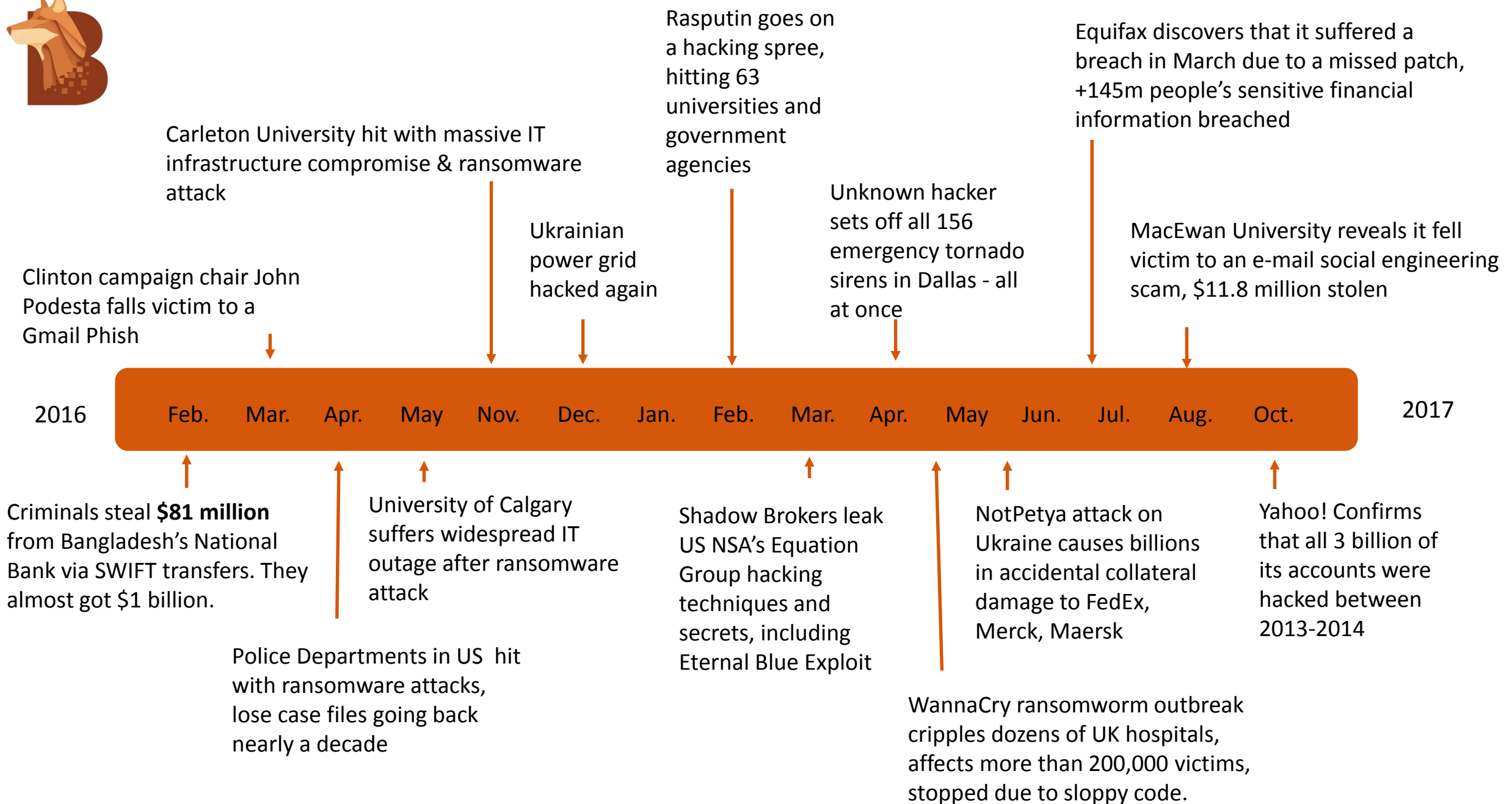
It started with a business decision

World's First

Power Outage
Caused by Hackers

Sending a message

When cyber truly gets personal

Carleton University hit with massive IT infrastructure compromise & ransomware attack

Rasputin goes on a hacking spree, hitting 63 universities and government agencies

Equifax discovers that it suffered a breach in March due to a missed patch, +145m people's sensitive financial information breached

Ukrainian power grid hacked again

Unknown hacker sets off all 156 emergency tornado sirens in Dallas - all at once

MacEwan University reveals it fell victim to an e-mail social engineering scam, $11.8 million stolen

Clinton campaign chair John Podesta falls victim to a Gmail Phish

2016

Feb. Mar. Apr. May Nov. Dec. Jan. Feb. Mar. Apr. May Jun. Jul. Aug. Oct.

2017

Criminals steal **$81 million** from Bangladesh's National Bank via SWIFT transfers. They almost got $1 billion.

University of Calgary suffers widespread IT outage after ransomware attack

Shadow Brokers leak US NSA's Equation Group hacking techniques and secrets, including Eternal Blue Exploit

NotPetya attack on Ukraine causes billions in accidental collateral damage to FedEx, Merck, Maersk

Yahoo! Confirms that all 3 billion of its accounts were hacked between 2013-2014

Police Departments in US hit with ransomware attacks, lose case files going back nearly a decade

WannaCry ransomworm outbreak cripples dozens of UK hospitals, affects more than 200,000 victims, stopped due to sloppy code.
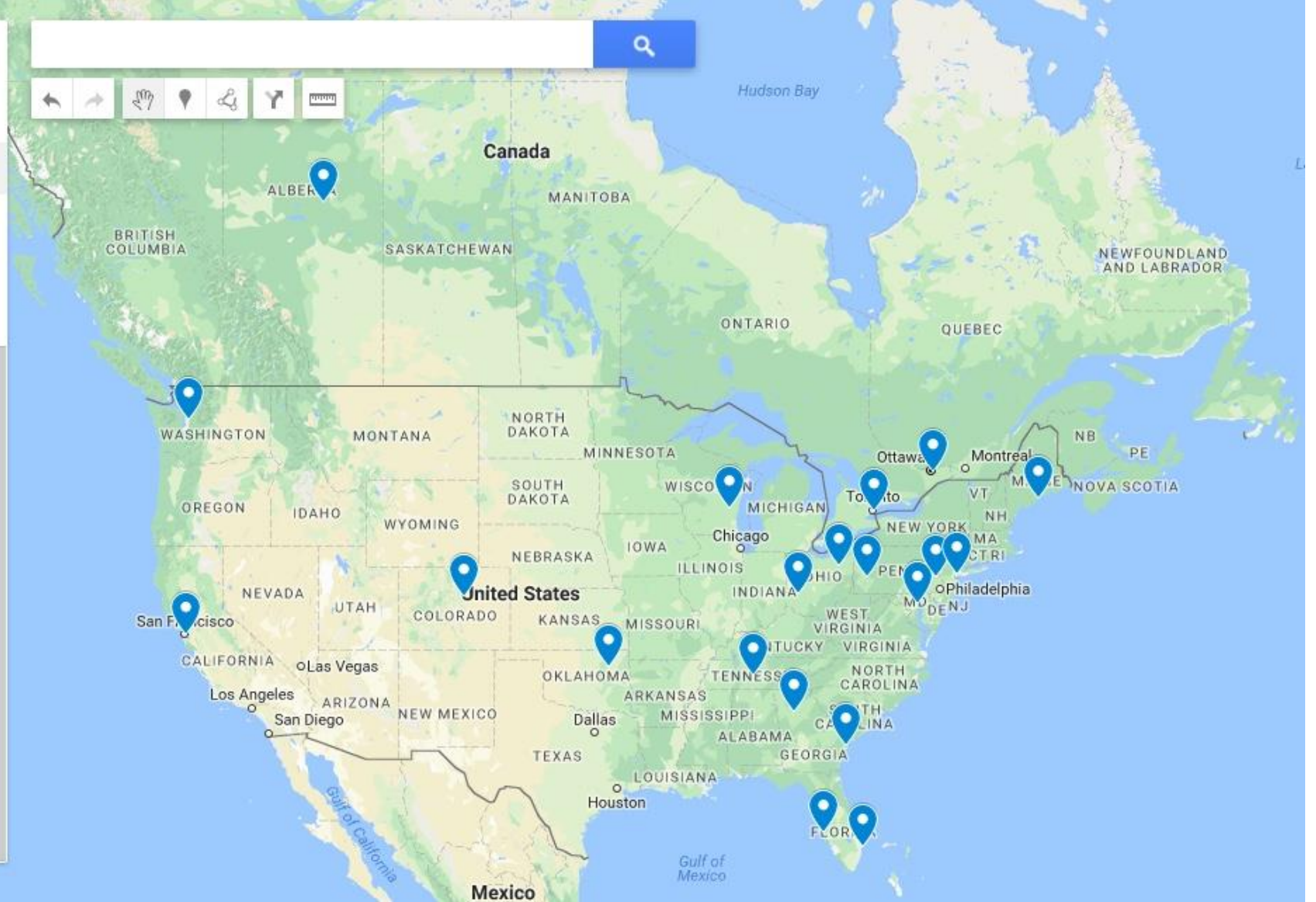
Municipal Cybersecurity Incident...

All changes saved in Drive

Add layer   Share   Preview

- Tulsa
- City of Baltimore
- Fond du Lac
- New Kensington
- Riverside
- Spring Hill
- San Francisco
- Toronto
- Ottawa
- Rockport
- Yarrow Point
- Englewood
- Sarasota
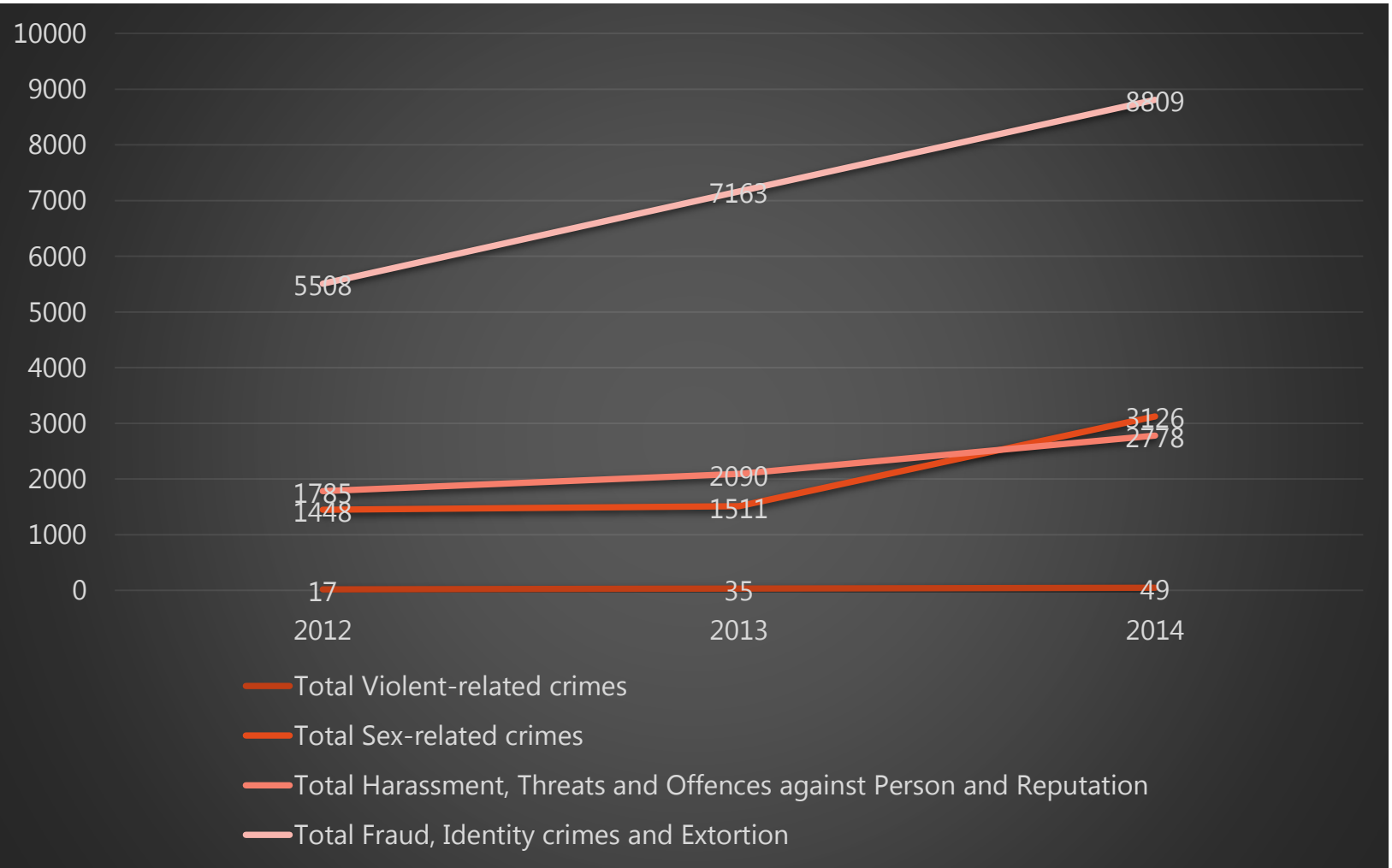- Allentown
- Newark
- Savannah
- Wabasca-Desmarais

Base map

In only 6% of police reported cybercrimes are suspects ever identified

Police Reported Cybercrime in Canada

DATA BREACH SUPPLY
HAS SIGNIFICANTLY OUTPACED DEMAND

9,198,580,292
Data Records Lost or Stolen Since 2013

In the past year the pace for data breaches has grown

26%

THE RISE OF RANSOMWARE

THE PERFECT CYBER CRIME

___

- It's easy - Crimeware-as-a-Service with 24-hour support chat lines and money back guarantees.

- It's convenient - no more hunting to find a buyer and working out how to get paid

- Price and demand are both unaffected by macro trends - it doesn't matter how many other victims are dealing with ransomware, each case is a unique market

The increasing security cost of efficiency

Top line revenue pressure → Mission to reduce cost and improve citizen services → Digital Technologies and Processes → Increased Criminal Activity → Increasing Regulatory & Financial Impacts → Insufficient Resources

CITY OF ATLANTA

_____

- Dedicated professional cybercriminal group called SamSam crippled city computers, networks and online services

- Major outage lasted more than a week. Recovery continues.

- Total clean-up cost estimated at more than $4 million USD

"Over the course of our campaign, we had had at least 100 forums, and we had talked about every single thing I thought there was to talk about, and cybersecurity was not a topic of conversation," - Atlanta Mayor Keisha Lance Bottoms.

CITY OF FREDERICTON

- Launched first city-wide cybersecurity awareness and simulated phishing program in September 2017

- 75% of police department completed mandatory training in first 30 days. 100% completed in May.

- 70% of entire city team completed training by May 2018 (voluntary and mandatory)

- 91% of those who completed training found it beneficial

Managing Cyber Risk

1) What key organizational objectives and processes are vulnerable to cyber threats?

2) What is management's strategy to manage these risks effectively? What framework is being used and why?

3) How do you measure the success of your efforts?

4) What is our incident response plan? When was it last tested?

5) Do our business continuity plans / disaster recovery plans include cyber attacks?

NIST Readiness

What is NIST Readiness?

The NIST Cybersecurity Framework (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks. The NIST framework covers people, process, organizational culture and technology in a comprehensive way with references to helpful guidelines and standards such as the SANS Top 20 Critical Security Controls (CSC), ISO 27001, COBIT 5 for Security and other standards.

This NIST readiness report will help your organization understand its cybersecurity strengths as well as areas for improvement or maturity. Achieving a mature state using this framework will help your organization reduce risk and move towards more formal cybersecurity certifications such as ISO 27001.

36%
Your Organization's NIST Readiness Score

Click a category to see your NIST readiness level

Q Identify	U Protect	⊚ Detect	📢 Respond	📷 Recover

Identify

Category	Subcategory
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1** Physical devices and systems within the organization are inventoried
	ID.AM-2 Software platforms and applications within the organization are inventoried
	ID.AM-3 Organizational communication and data flows are mapped
	ID.AM-4 External information systems are catalogued
	ID.AM-5 Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
	ID.AM-6 Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

Beauceron

- 🐾 Dashboard
- 🔗 Division Management ▸
- 🎓 Education
- ☰ Risk Management ▸
- ⚠ Simulations ▸
- ⓘ Incidents
- ★ Rewards
- ☑ Reporting
- ⚙ Configuration ▸
- ⊕ Feedback

A Comprehensive, Automated Cybersecurity Management Platform

Outcomes for Organizations

- Organizational capability to identify and mitigate human centric risks of cybercrime.

- Enable executives, leaders and employees with actionable insight and intelligence to measure, manage and monitor risks.

- Reduce burden on already constrained resources and IT/Sec expertise

- Reduce exposure to unexpected risks, costs and impacts of cybercrime.

How We Do It

- Proprietary Risk Score at the Individual, Division and Organization level

- Comparative Analytics

- Attitudes, Awareness and Perception Surveys

- Cyber Awareness Training

- Phishing Simulation

- Real Incident Tracking

- Assigning Rewards for Good Security Behaviour

- Custom Course Creation

- Technology & Process Self Assessments

- Insightful Dashboards and Reports

Empowering employees to manage their cyber risk

Organizational Members

Beyond Awareness: Beauceron's personal cyber risk score helps team members connect the dots between awareness and behaviour

Engaged in Security: The combination of just-in-time education, phishing simulations and timely communication creates true engagement though gamification

Rewarding Positive Behaviour: Beauceron's reward tool provides incentives and real-time feedback for reporting simulated phishes or other beneficial security behaviours
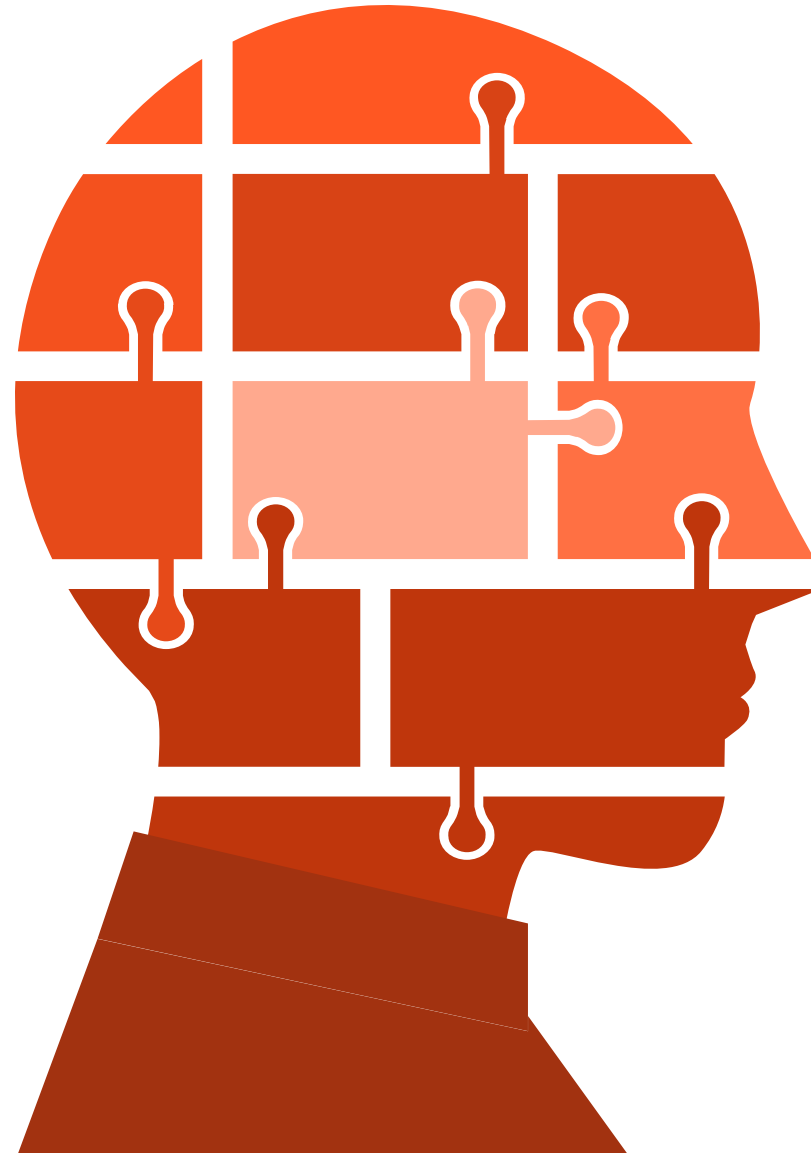
Security Awareness Team

Automated Campaigns: Beauceron's automated approach to deploying education, surveys and phishing frees up security team resources

Insightful Real-Time Analytics: Beauceron's powerful analytics, reports and dashboards makes it easier to identify security awareness strengths, weaknesses, threats and opportunities

Integrated platform: Beauceron's integrated solution provides a single platform for the team to manage with a single pane of glass for all of cybersecurity awareness

Every employee is given their own individualized dashboard which becomes their **one-stop shop** for cybersecurity awareness.

They can:

Review their personal cyber risk score,

Compare their score to others in their division,

Complete surveys,

Complete education

Learn about their exposures to cybercriminals

Learn about any simulated or real *incidents* they fell victim to

Learn about any *rewards* they've been given

Receive security news and updates

Do we have the right plan?

- How are we protecting citizen and client information?

- How much are we spending on cybersecurity and what are the outcomes?

- How are our disaster recovery, business continuity and incident response plans updated, communicated and tested?

Learn more

City of Fredericton Case Study:

- beauceronsecurity.com/fredericton

Beauceron News and Updates

- beauceronsecurity.com

Request a Demo

- beauceronsecurity.com