



MILLER THOMSON
AVOCATS | LAWYERS

FORWARD TOGETHER

Cybersecurity 20/20

Looking back at 2019, preparing for 2020:



Clauiu Popa
President, Datarisk Canada
Chair, CybersafetyFoundation.org
Author, Canadian Cyberfraud Handbook



David Krebs, Counsel
Key Contact for Miller Thomson Cybersecurity



Claudiu Popa

Board Level Risk Advisor



*Focus on standardization & security audits
Industry focus on regulated sectors, healthcare and finance
Educator, expert witness, media contributor and professional speaker
CEO, Informatica Corporation; Chair, Knowledgeflow Cybersafety Foundation*

DAVID KREBS, CIPP/C

- Counsel in Miller Thomson's Business Law Practice Group specializing in Privacy, Technology, and Cyber Security
- Key Contact for Miller Thomson's Canadian Cyber Security Practice and editor of MT Cybersecurity Blog
- 10+ years' experience in data privacy law (Canada and Europe)

Cybersecurity Blog

Read the latest from our MT Cybersecurity blog

[More](#)



Agenda

1. Introduction: Guest Speaker, Claudiu Popa
2. Key Takeaways
3. Canadian Landscape
4. The Cost of Breaches & Security Incidents
5. Legal Risk & Considerations
6. What's the Kill Chain?
7. The Holy Grail
8. Need to know
9. Summary and Questions

Key Takeaways

- Cyber threats are real and are changing... "Third Wave" is coming...
- Cyber Incidents carry a **number of operational, reputational, and legal risks**
- **One incident....many laws** (Federal, provincial, US State, European, sector-specific...)
- **Investments in cybersecurity** are worth it – preparedness, technology/infrastructure, legal/compliance resources, training, and insurance are tools that should be considered and utilized
- Legal as **trusted advisor** – we highlight cyber security as integral part of business operations
- **Incident response** is a **team-sport** – IT security and forensics experts work hand-in-hand with legal counsel/breach coach, PR, and key management; **Communication** is King! Breach communication not intuitive...
- Consider impact of cyber risk: in contracts with vendors (sector-agnostic, not just about personal data); M&A; Enterprise Risk Management; When choosing insurance coverage

Cyber Incidents in Canada

Cyber Incidents on the rise...Changing Face of Ransomware

eHealth discovers files sent to suspicious IP address following ransomware attack

[CTVNewsRegina.ca Staff](#)
[Contact](#)

Published Friday, February 7, 2020 12:45PM CST
Last Updated Friday, February 7, 2020 6:36PM CST



Saskatchewan

Cyber attack shuts down Evraz IT systems across North America, but company says no data compromised



Company issued a three-day layoff notice that takes effect Friday

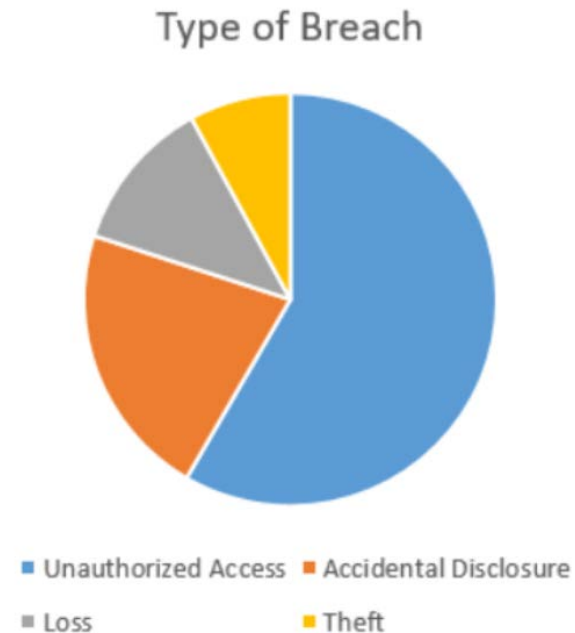
CBC News - Posted: Mar 05, 2020 12:03 PM CT | Last Updated: March 5



Evraz North America's information technology systems are down after a cyberattack late Wednesday night. (Olivia Stefanovich/CBC)

Report from the Office of the Privacy Commissioner of Canada

- *“A full year of mandatory data breach reporting: What we’ve learned and what businesses need to know”*
- The past year has seen an estimated **28 million** Canadian data records compromised in **680 reported security breaches** reported to the Privacy Commissioner's Office.
- Since new breach requirements were added to PIPEDA exactly a year ago, the number of reports by companies and individuals has **surged six-fold**, revealing **new trends** and priorities for the coming year.





VANCOUVER

CALGARY

EDMONTON

SASKATOON

REGINA

LONDON

KITCHENER-WATERLOO

GUELPH

TORONTO

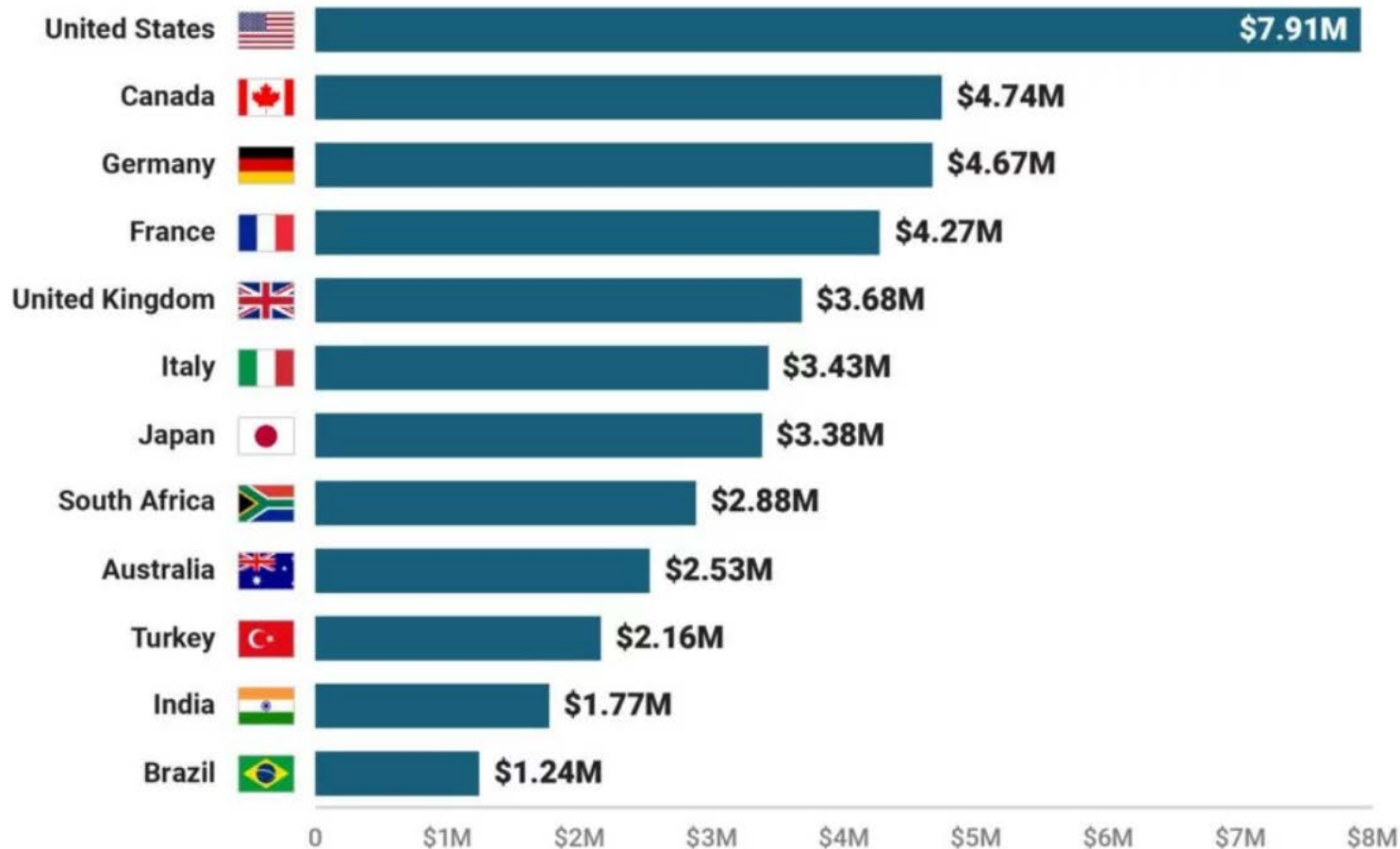
VAUGHAN

MARKHAM

MONTRÉAL

Canada Second Highest in Cost of Breaches: IBM

Average total cost of a data breach by country, 2018



Source: IBM

statista | BUSINESS INSIDER



Protecting the intangible
Since 1989

TRUST  INFORMATICA



2019 Cost of a Data Breach Report

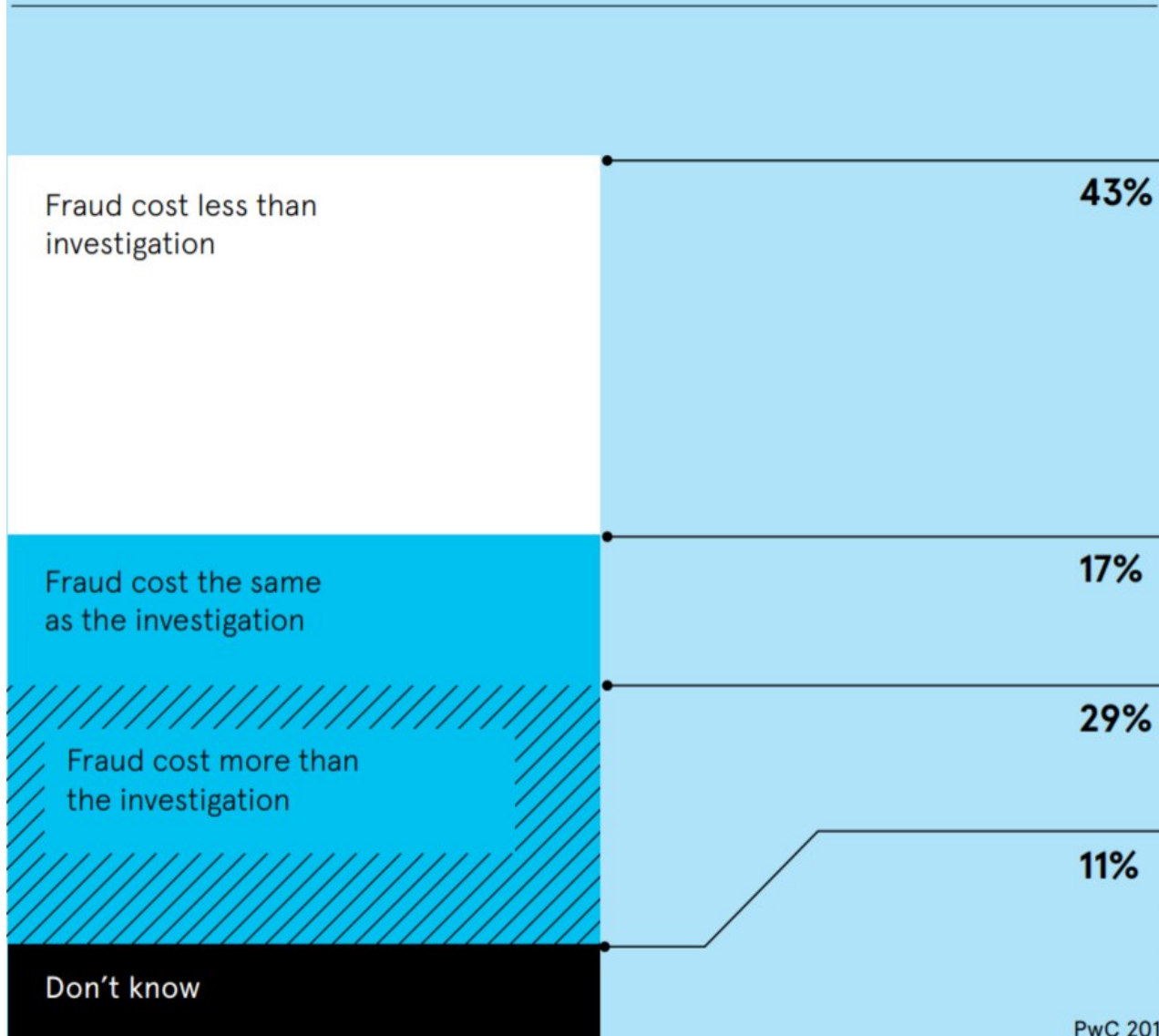
Global average total cost of a data breach
Measured in US\$ millions



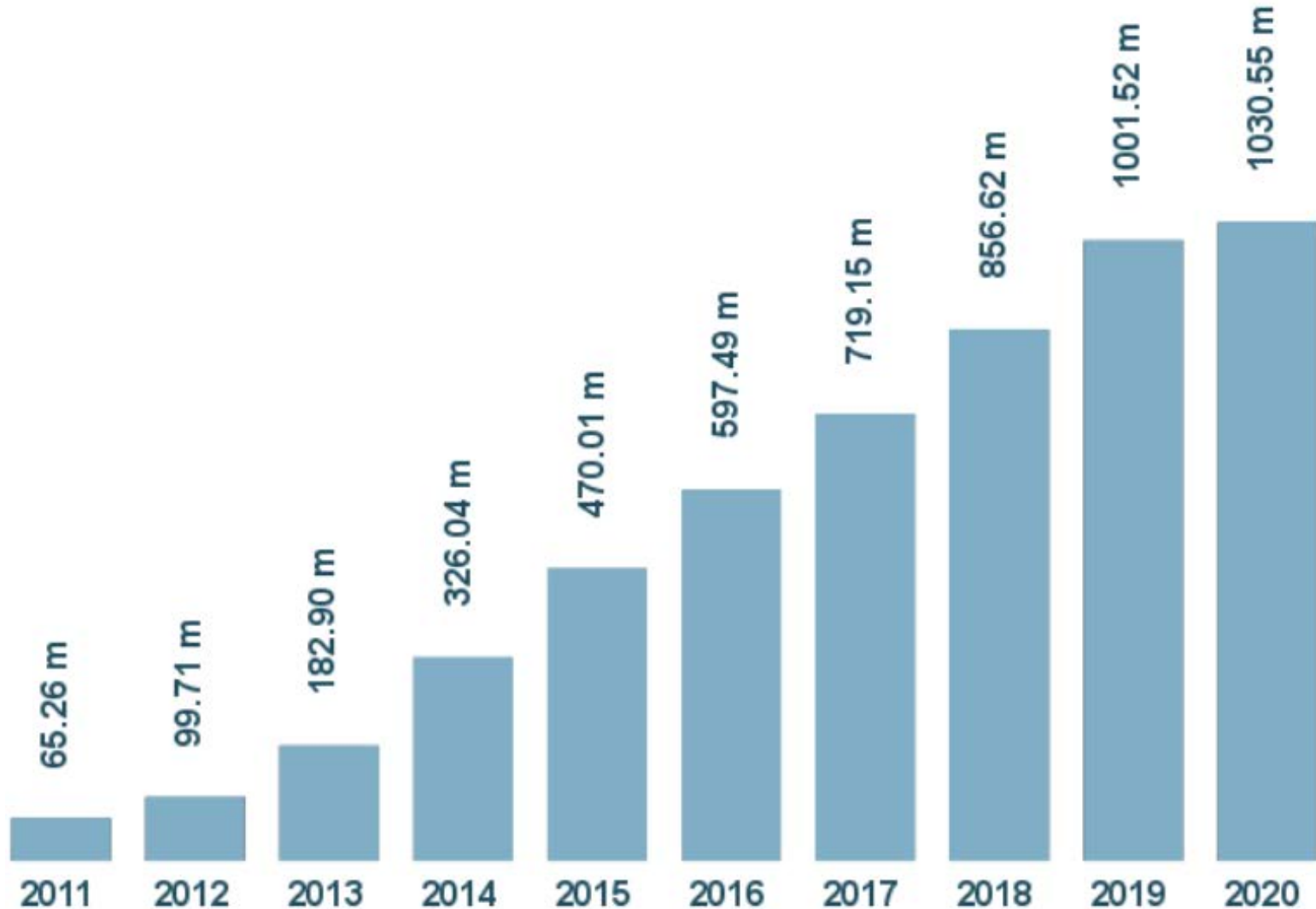
The latest annual Cost of a Data Breach report by the Ponemon Institute and funded by IBM. Source: IBM



TIME SPENT INVESTIGATING FRAUD CAN COST MORE THAN THE FRAUD ITSELF



Total Active Malware in the World



Last update: March 06, 2020

Copyright © AV-TEST GmbH, www.av-test.org

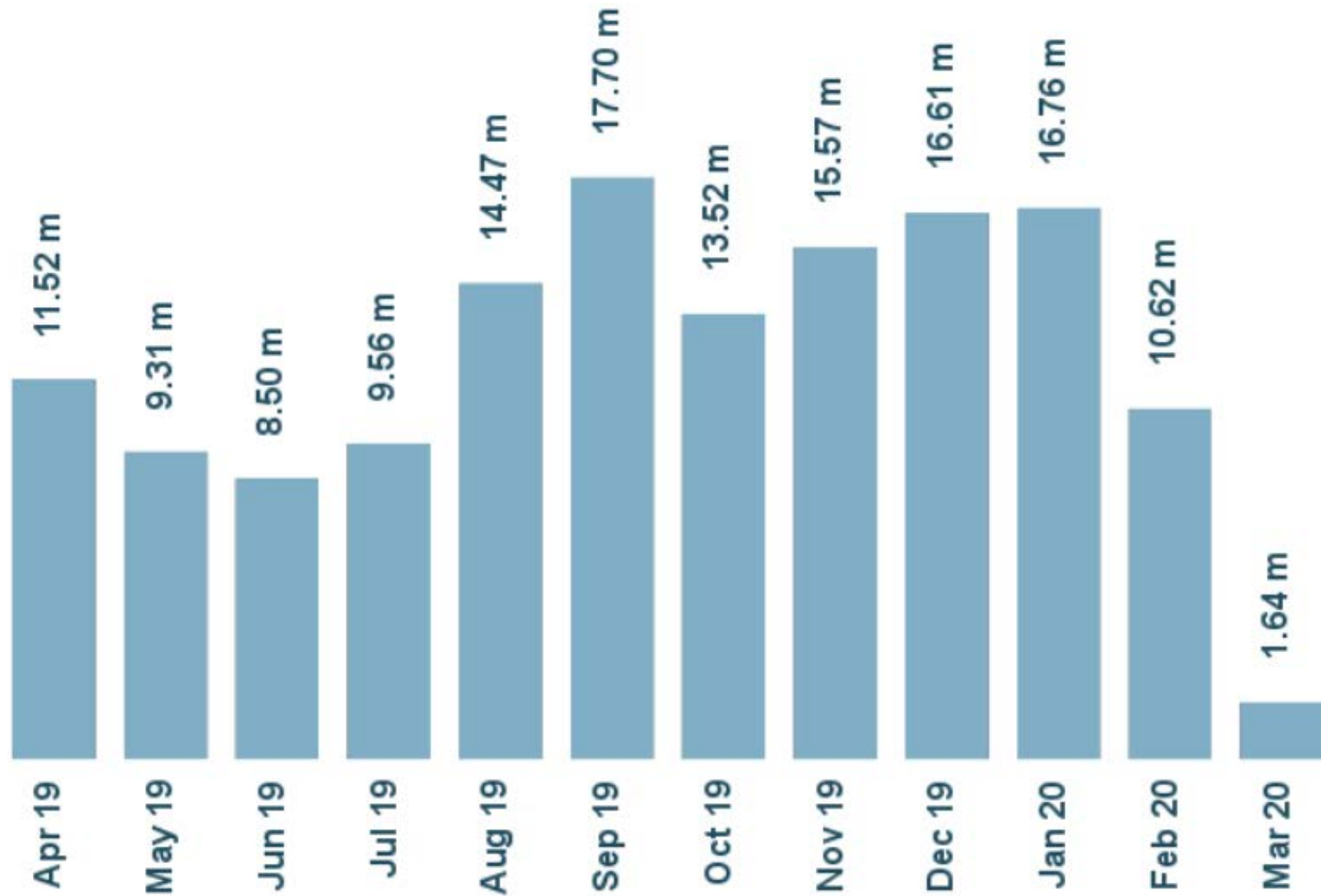


Protecting the intangible

Since 1989

TRUST  INFORMATICA

New Malware Strains Per Month



Last update: March 06, 2020

Copyright © AV-TEST GmbH, www.av-test.org

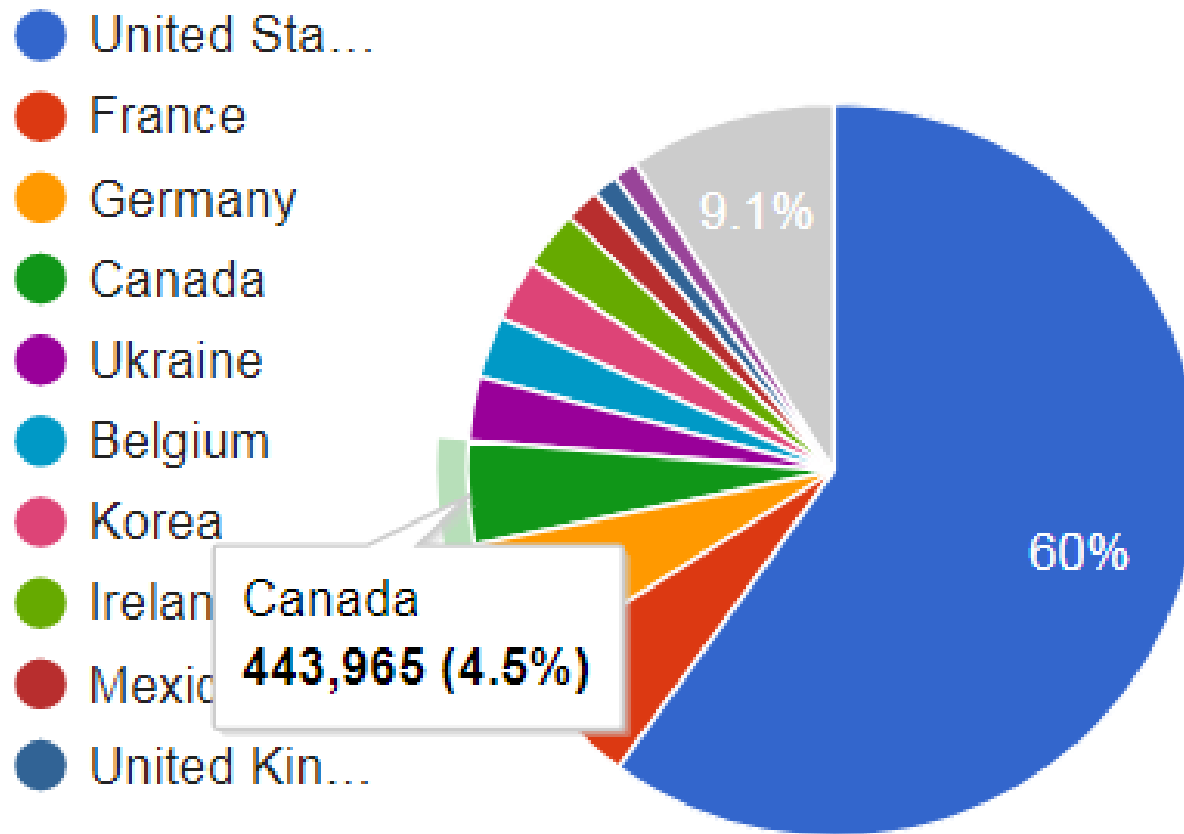


Protecting the intangible

Since 1989

TRUST  INFORMATICA

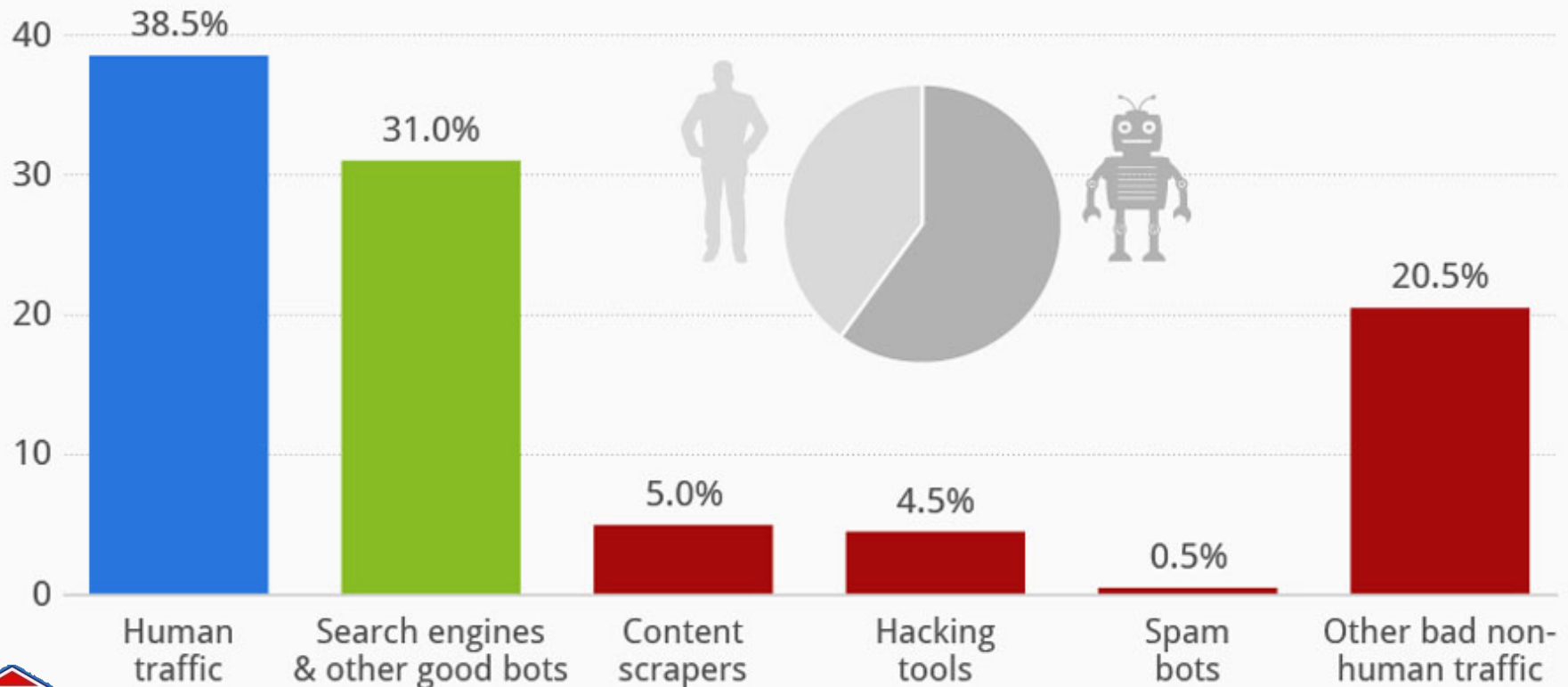
Weekly Virustotal Uploads



Humans Account for Less Than 40% of Global Web Traffic

Breakdown of global website traffic by source* (2013)

Human Good non-human Malicious non-human



Professional Grade Cybercrime



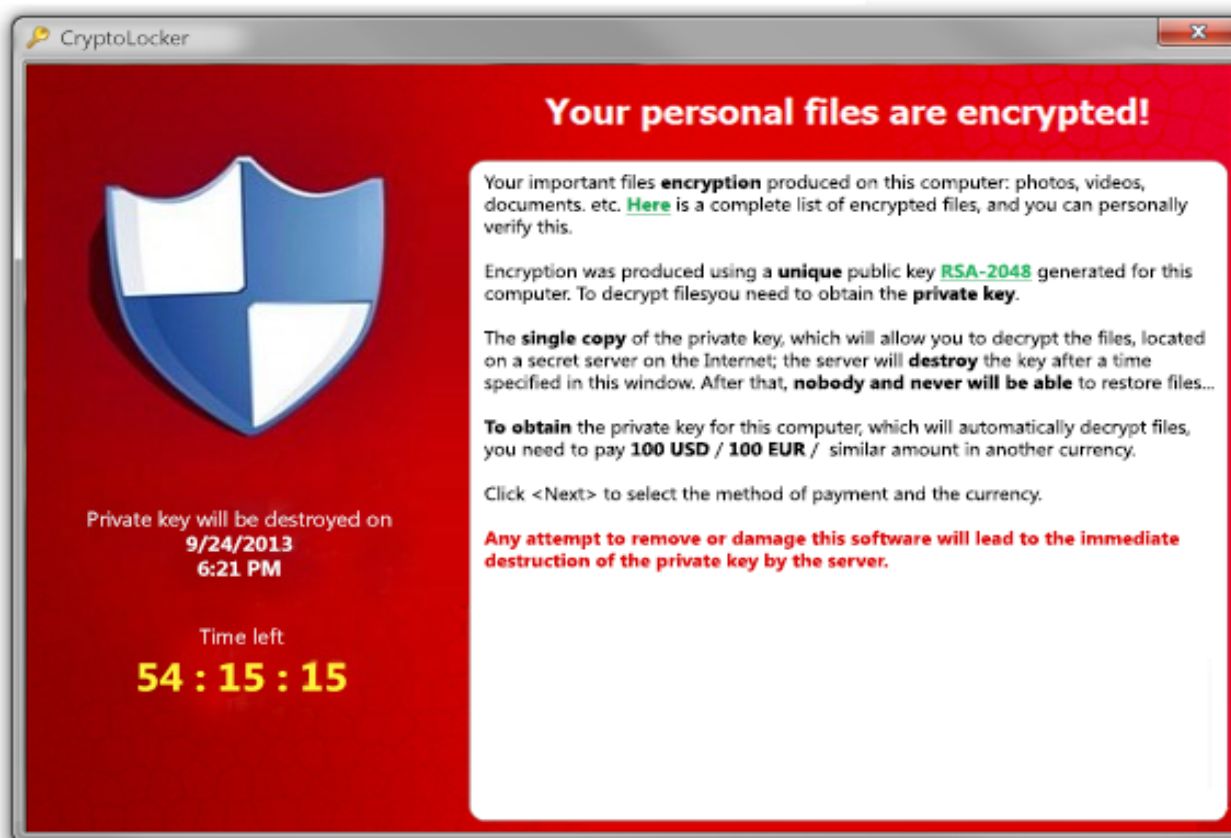
Protecting the intangible

Since 1989

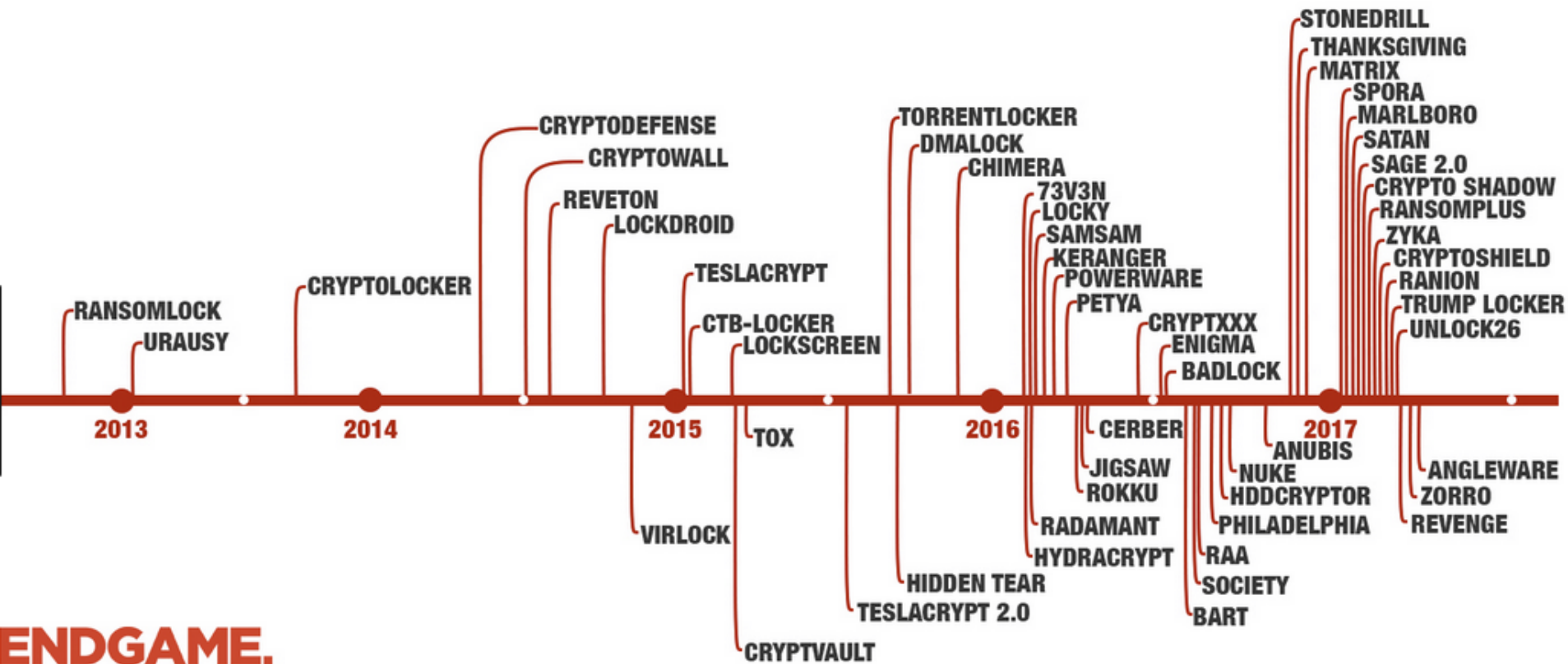
TRUST  INFORMATICA



The Firewall is now human



no experience required





All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ≈ 550 USD.

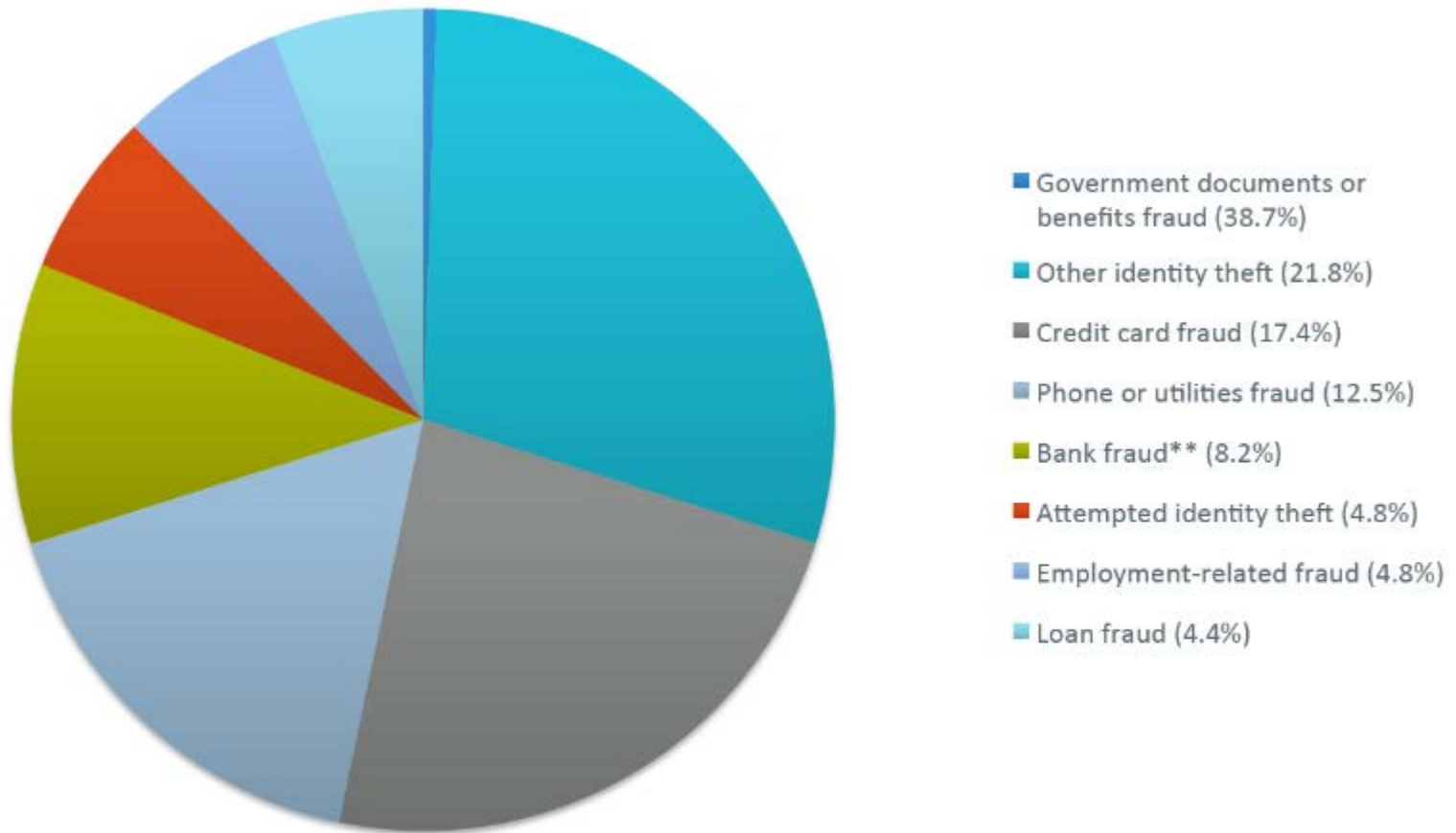
Your Bitcoin address for payment: 1J7H9WwPZ8mTtUdFzYKZLAeRACuBvXUjD6

§ PURCHASE PRIVATE KEY WITH BITCOIN

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards)

how stolen information is abused

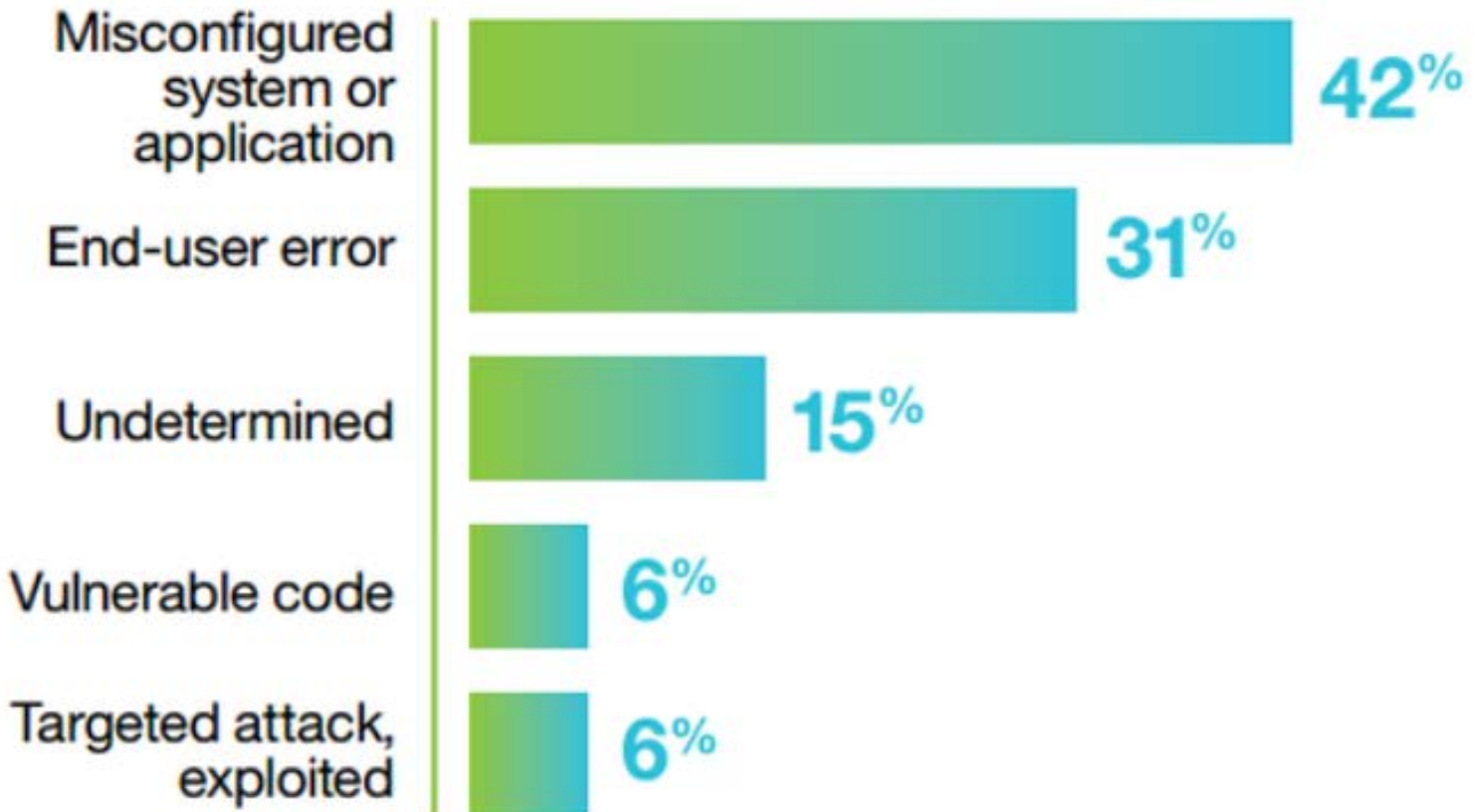


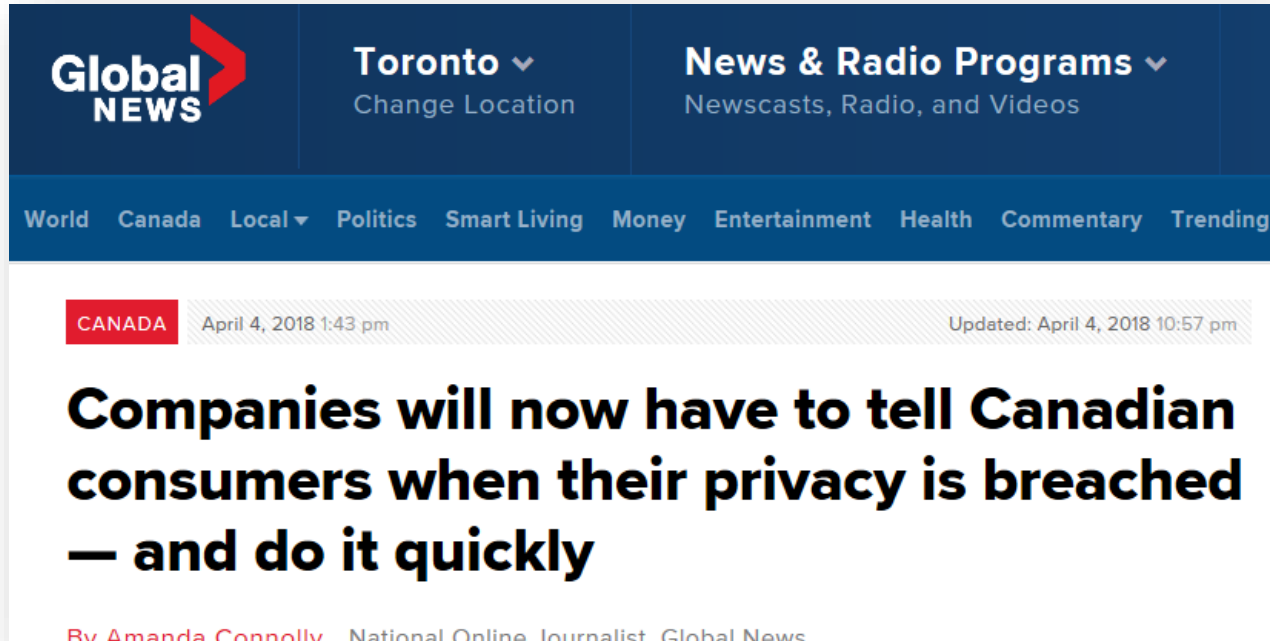
* Percentages are based on the total number of complaints in the Federal Trade Commission's Consumer Sentinel Network (332,646 in 2014). Percentages total to more than 100 because some victims reported experiencing more than one type of identity theft (17% in 2014).

** Includes fraud involving checking, savings, and other deposit accounts and electronic fund transfers.

Source: FTC

crimes of opportunity?





The image is a screenshot of a news article from Global News. The top navigation bar is dark blue with the Global News logo on the left, 'Toronto' with a dropdown arrow and 'Change Location' in the center, and 'News & Radio Programs' with a dropdown arrow and 'Newscasts, Radio, and Videos' on the right. Below this is a lighter blue bar with category links: World, Canada, Local (with a dropdown arrow), Politics, Smart Living, Money, Entertainment, Health, Commentary, and Trending. The article itself has a red 'CANADA' tag, a timestamp of 'April 4, 2018 1:43 pm', and an 'Updated' timestamp of 'April 4, 2018 10:57 pm'. The headline is in large, bold black text. The byline at the bottom reads 'By Amanda Connolly, National Online Journalist, Global News'.

Global NEWS

Toronto ▾
Change Location

News & Radio Programs ▾
Newscasts, Radio, and Videos

World Canada Local ▾ Politics Smart Living Money Entertainment Health Commentary Trending

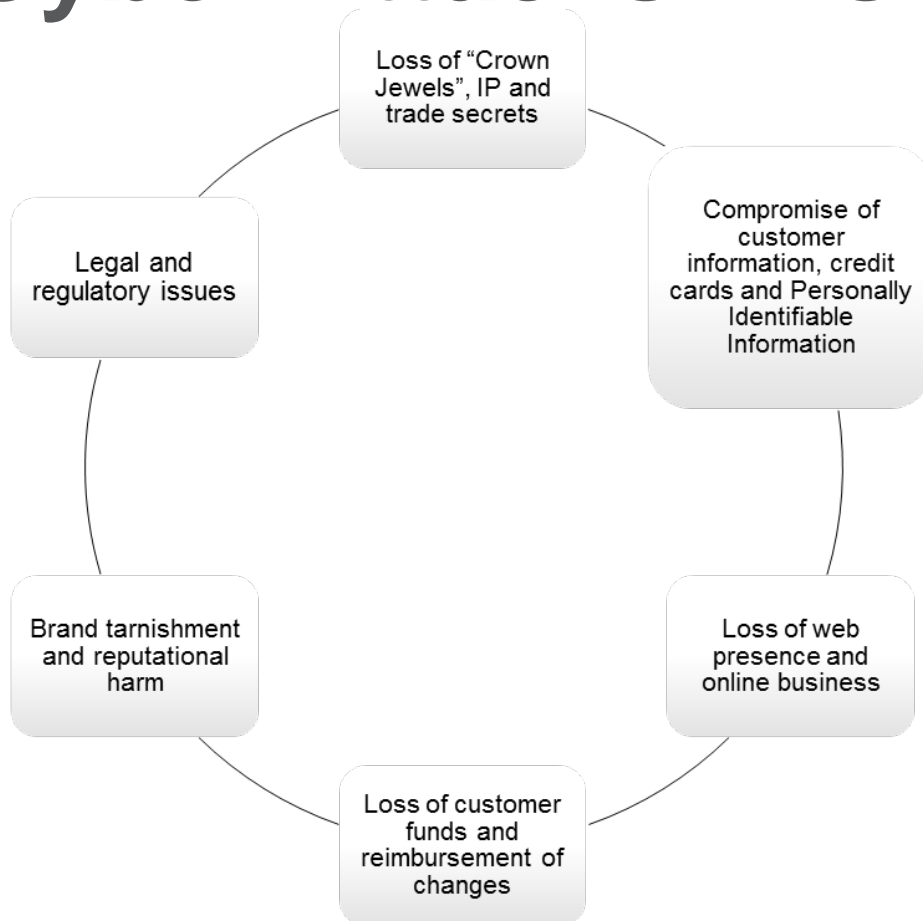
CANADA April 4, 2018 1:43 pm Updated: April 4, 2018 10:57 pm

Companies will now have to tell Canadian consumers when their privacy is breached — and do it quickly

By Amanda Connolly, National Online Journalist, Global News

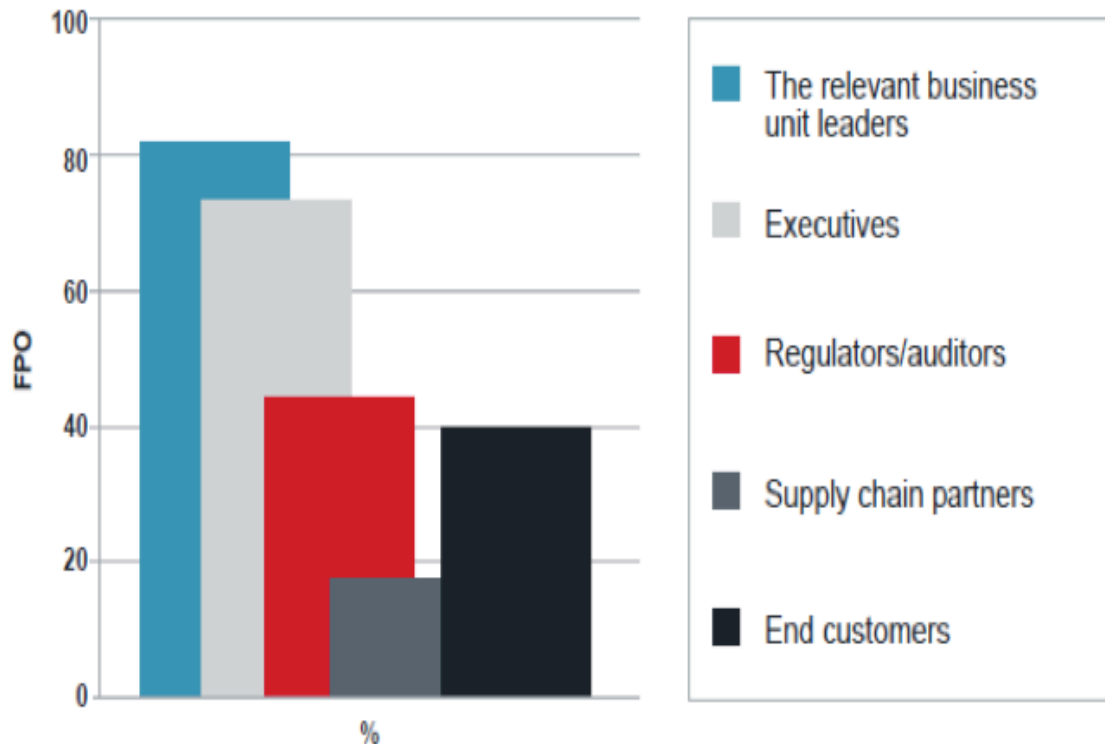
Canada: Data Breach Reports Skyrocket In First Year Of Mandatory Breach Reporting

Cyber Attacks' Risk to Business



- Director and Officer liability
- **Legal liability including litigation**
- **Regulator enforcement and investigations**
- Failure to meet key contract terms
- Economic harm (e.g. loss of confidential information/IP)
- **Reputational harm**
- **Business interruption**
- Physical harm

Who do you notify when a breach occurs?



Breach Coach/Counsel's role:

- Coordinate - urgency without panic, help assess the facts
- Review relevant contracts
- Work with forensics – did the breach result in data access or extraction? Was there a bad actor? Internal vs external threat?
- Work with PR; Communicate with stakeholders
- Advise on risk
- Where required – prepare notifications; review which law(s) apply (cross-border!)



Ransomware and reporting

- Many ransomware cases traditionally not reported – intent was \$ not exfiltration of data.
- Caution: Do the analysis; review the facts and the law
- Law not settled – very fact specific
- 100% certainty is an illusion
- Learnings from recent HIPAA (US) Guidance:
 - Whether or not the presence of ransomware would be a breach under the HIPAA Rules is a fact-specific determination. A breach under the HIPAA Rules is defined as, “...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” See 45 C.F.R. 164.402.6
 - When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, **a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a “disclosure” not permitted under the HIPAA Privacy Rule.**
 - **Unless the covered entity or business associate can demonstrate that there is a “...low probability that the PHI has been compromised,”** based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred. The entity must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements. See 45 C.F.R. 164.400-414.

Assessing probability of compromise (HIPAA)

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. the unauthorized person who used the PHI or to whom the disclosure was made;
3. whether the PHI was actually acquired or viewed; and
4. the extent to which the risk to the PHI has been mitigated.

Personal Information

- What is “Personal Information”?
 - **PIPEDA** defines PI as “information about an identifiable individual”
 - excludes business card information
 - According to the **OPC***, personal information includes any factual or subjective information, recorded or not, about an identifiable individual.
- Examples:
 - age, name, ID numbers, income, ethnic origin, or blood type;
 - opinions, evaluations, comments, social status, or disciplinary actions; and
 - employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs)



Breach notification

- **Under PIPEDA: Breach of security safeguards** means the loss of, unauthorized access to or unauthorized disclosure of “personal information” resulting from a breach of an organization’s security safeguards – being “accessible” can be sufficient
 - Organization must determine if the breach poses a **“real risk of significant harm”** to any individual whose information was involved in the breach by conducting a risk assessment
 - The assessment of risk must consider the **sensitivity** of the information involved, and the **probability** that the information will be misused
 - When the organization considers that a breach poses a real risk of significant harm, **it must notify affected individuals and report to the Commissioner** as soon as feasible
- Depending on location(s), sector, and impacted population, a number of different laws may come into play.
- Assess all potential obligations in determining strategy.

Data breach record keeping (PIPEDA)

- Organizations must maintain sufficient information in a data breach record to demonstrate that they are tracking data security incidents that result in a breach of personal information.
- Broad interpretation of what information would constitute a “record” for the purpose of PIPEDA.
- Organizations must hold data breach records for a minimum period of time; specifically **24 months**.
- Oversight by the Commissioner to ensure compliance with the requirements to report to the Commissioner and notify affected individuals of significant breaches.

APRIL 4, 2017 / INSIGHTS

The Next Big Hacking Target: Law Firms

The lure of hacking law firms is clear: they are privy to companies' most sensitive data

BY STEVEN S. MCNEW



Protecting the intangible

Since 1989

TRUST  INFORMATICA

Heightened Risk of Cyberattacks Puts Pressure on Law Firms to Bolster Defenses

Considering 80 of the 100 biggest law firms have been hacked since 2011, **it stands to reason** yours could be next.

Hacking of law firms highlights serious [security breaches](#) for companies entrusting them with sensitive data. A report by Citigroup urged their employees to **be mindful of the risks of trusting law firms** with sensitive digital data for three reasons:

1. Law firms continue to be a high value target for hackers and foreign entities
2. Law firm security is below industry standards--given the assets they hold
3. Law firms have been unwilling to disclose when they have been breached, and the severity of breaches, despite ongoing pressure from clients and law enforcement officials.

Daniel Garrie, of the [Journal of Law & Cyber Warfare](#), states, "Law firms represent, in today's information security environment, **the easiest and richest** target to go after...Law firms have no incentive to protect themselves from being attacked because, to date, there has been no meaningful financial impact to the law firms' bottom line."

what *other* threats do law firms face?

66%

of law firms have reported a breach of some type, with varying levels of compromise.

- spear phishing (malicious hyperlink)
- ransomware (weaponized attachment)
- drive-by downloads (autoinstalls)
- watering hole attacks (hijacked website)
- 3rd party breaches (VoIP, mobile & storage)

More Than 100 Law Firms Have Reported Data Breaches. Is Your Firm Next?

Unfortunately, these rules do not include any specific technical requirements that attorneys can reference. This puts attorneys in the difficult position of trying to determine what is sufficient when it comes to cybersecurity.

By Kevin Baker | February 13, 2020 at 01:15 PM

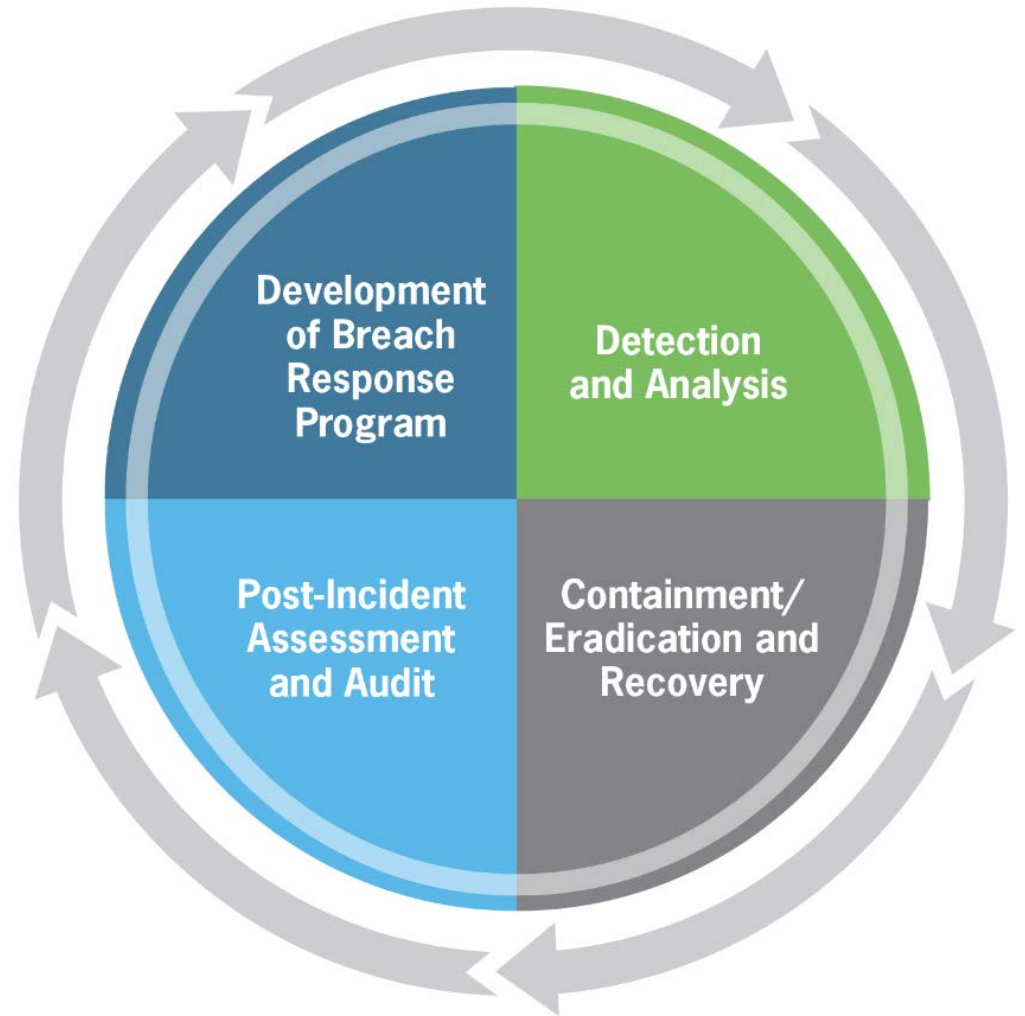


Protecting the intangible

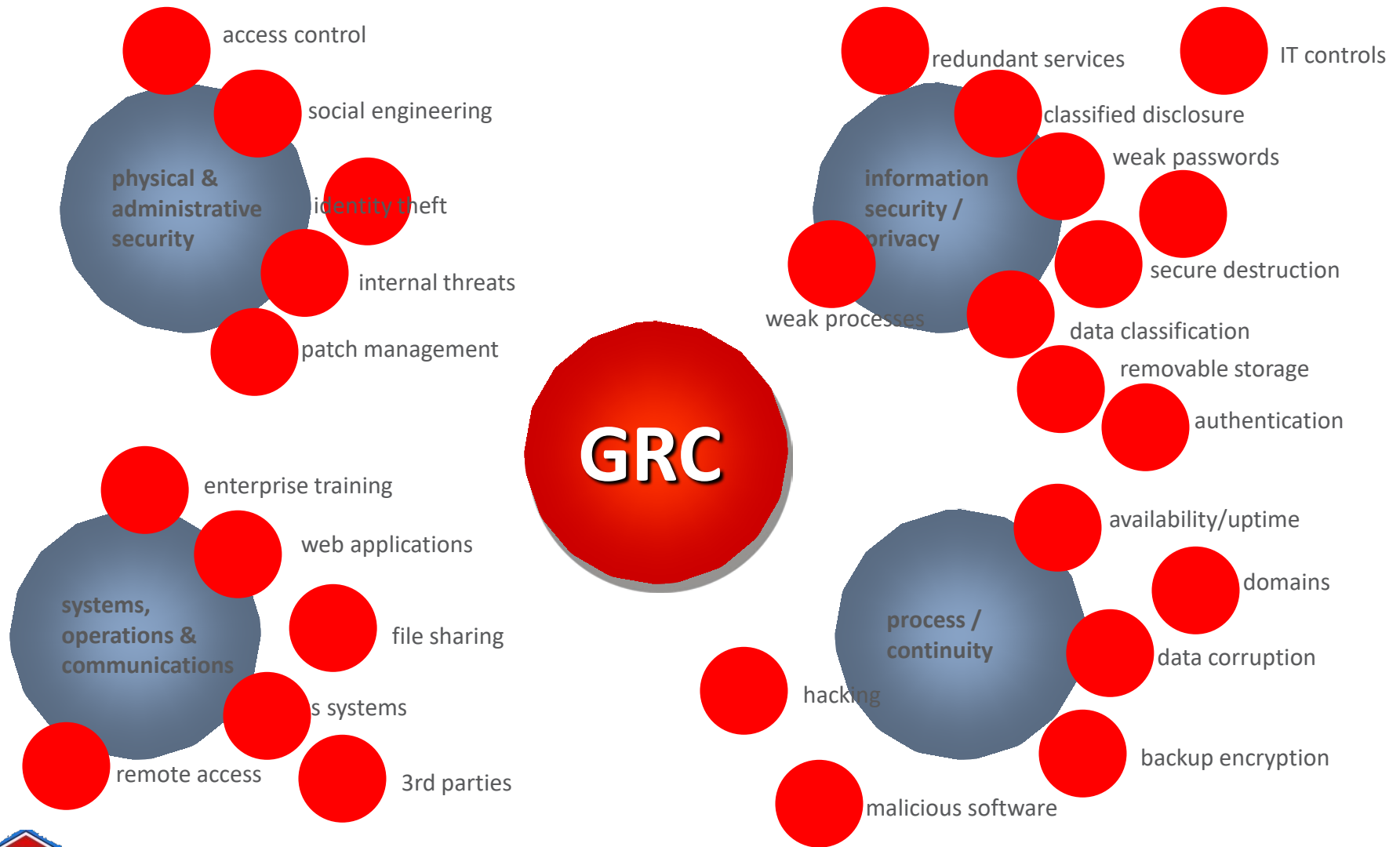
Since 1989

breach response planning

1. response
2. recovery
3. remediation
4. reporting
5. review



Real cybersecurity expertise needed for breach management

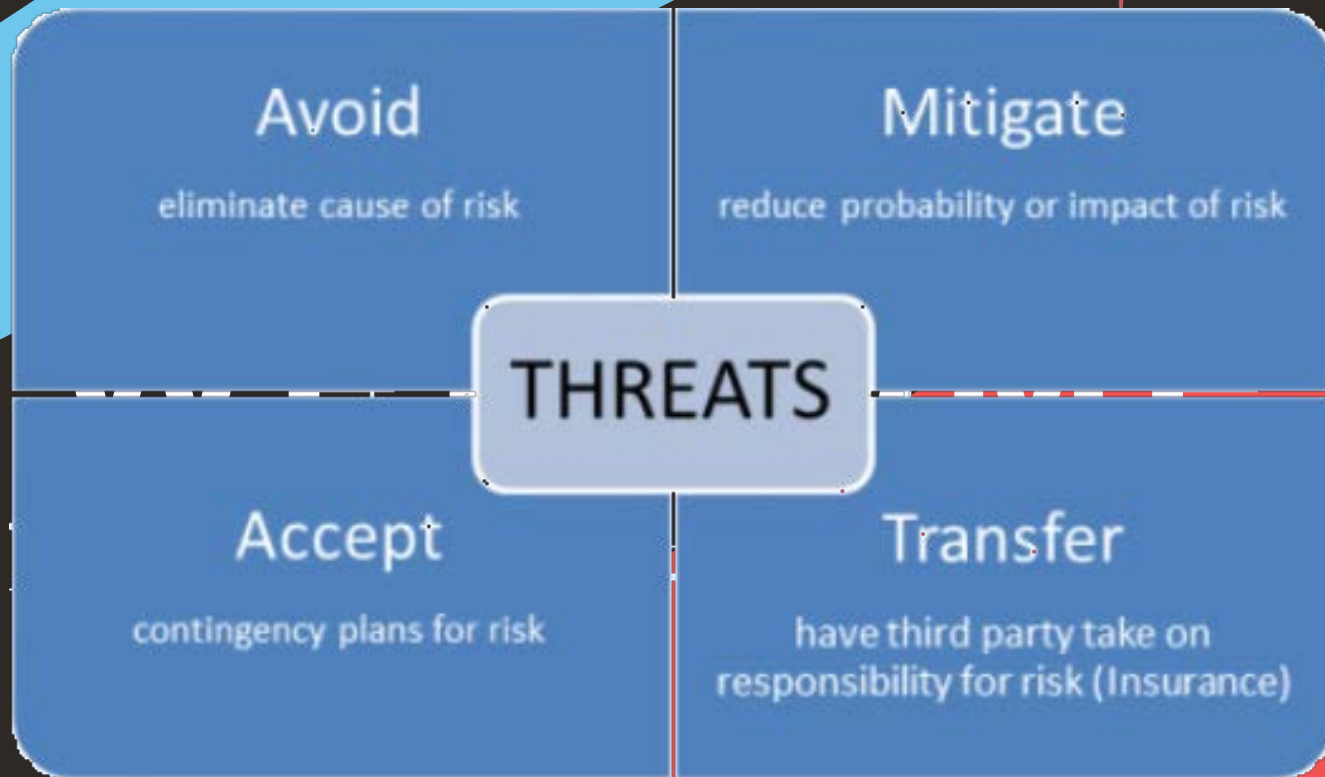


Protecting the intangible

Since 1989

TRUST  INFORMATICA

risk treatment options



Protecting the intangible

Since 1989

TRUST  INFORMATICA

FBI: Business Email Compromise Cost Businesses \$1.7B in 2019

BEC attacks comprised nearly half of cybercrime losses last year, which totaled \$3.5 billion overall as Internet-enabled crimes ramped up.



BUSINESS E-MAIL COMPROMISE (BEC) BULLETIN

Recognize, Reject and Report it!

According to recent cybercrime statistics, BEC has stolen more than **\$5 billion** dollars from unsuspecting victims worldwide, including Canadian businesses¹. BEC is the second highest for monetary loss out of over 40 fraud types reported to the Canadian Anti-Fraud Centre (CAFC). It's real, it's growing, but with increased awareness, it can be prevented.

on the importance of awareness and vigilance

New Phoenix Keylogger tries to stop over 80 security products to avoid detection

Phoenix linked to more than 10,000 infections since the malware's launch on a hacking forum in July.



By Catalin Cimpanu for Zero Day | November 20, 2019 -- 06:00 GMT (22:00 PST) | Topic: [Security](#)



MORE FROM CATALIN CIMPANU

Security
Microsoft rebukes rumors that Microsoft Teams is being used in ransomware attacks

Security
Anonymous hacker gets a whopping six years in prison for some lame DDoS attacks

Security
New Roboto botnet emerges targeting Linux servers running Webmin

Government : US
US student was allegedly building a custom Gentoo Linux distro for ISIS

NEWSLETTERS



Protecting the intangible

Since 1989

TRUST  INFORMATICA

irresistible phishing expeditions

PUROLATOR HAVE A PACKAGE FOR YOU! HOW TO GET YOUR PACKAGE IN ONE PIECE

Please follow the steps below.

Download the Purolator Label containing your tracking number.

[Click here for your label](#)

Open the label information for your tracking number. You may reschedule a redeliver from us or arrange a pick up from our location.

*If you can't download the label, try to move this email into your inbox folder.

Purolator Your Shipping Solutions

2018 Purolator

CANADA POST
POST POSTES
CANADA CANADA



Your Xpresspost Canada Post package has been delivered!

To get the confirmation of the delivery, click on the label for your tracking number.

If you didn't receive your package, please contact us with the tracking number.

[Click here for your label](#)

*If you can't click on the label, move this email into your inbox folder.

Canada

We have a package waiting for you!



How to get your package in time?
Please follow the steps below.

Download the Purolator attachment file containing your tracking number.

Open the file for your tracking number. You may reschedule a redeliver from us or arrange a pick up from our location.

*If you can't click the label, try to move this email into your inbox folder.

*The file is only compatible with Microsoft Windows.



Purolator

www.purolator.com

| 1 888 SHIP-123

CANADA POST
POST POSTES
CANADA CANADA

We delivered your parcel

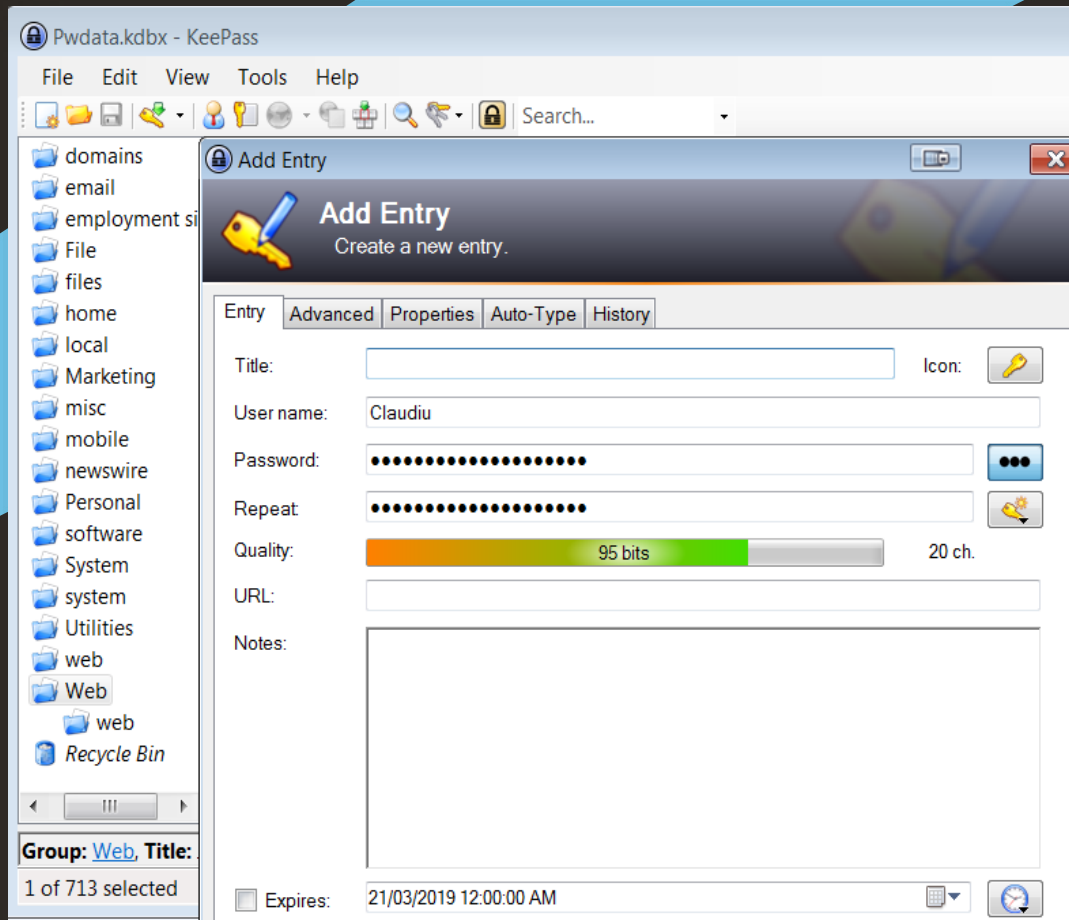
Current status

Delivered

Need help finding your parcel?

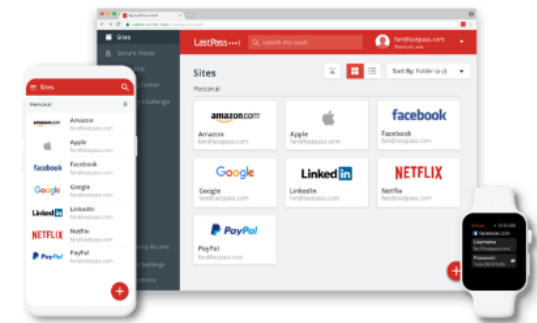


can you trust password databases?



One password. Zero headaches.

LastPass takes care of the rest.



Free features

- ✓ Secure password vault ⓘ
- ✓ Access on all devices ⓘ
- ✓ One-to-one sharing ⓘ
- ✓ Save and fill passwords ⓘ
- ✓ Password generator ⓘ
- ✓ Secure notes ⓘ
- ✓ Security challenge ⓘ
- ✓ Multi-factor authentication ⓘ
- ✓ LastPass Authenticator ⓘ



Protecting the intangible

Since 1989

TRUST  INFORMATICA

Summary & Wrap-up

- Cyber security is a key and integral part of operations – should be resourced and treated as such
- Call in the experts – legal, IT, PR – for program development, incidents, and dealing with the aftermath
- Consider cyber security/privacy/IT issues in vendor contracts, M&A transactions and when advising clients on overall risk exposure
- More data or more automation and more connectivity that is core to business operations means higher risk impact
- Advise clients to be aware, knowledgeable, and proactive

Questions?

Contact

Claudiu Popa

Email: Claudiu@SecurityandPrivacy.ca

Social Media: LinkedIn and Twitter

David Krebs

Direct Line: +1 306.667.5632

Email: dkrebs@millerthomson.com

Social Media: LinkedIn and Twitter

FORWARD TOGETHER



MILLER THOMSON
AVOCATS | LAWYERS

MILLERTHOMSON.COM



© 2016 Miller Thomson LLP. All Rights Reserved. All Intellectual Property Rights including copyright in this presentation are owned by Miller Thomson LLP. This presentation may be reproduced and distributed in its entirety provided no alterations are made to the form or content. Any other form of reproduction or distribution requires the prior written consent of Miller Thomson LLP which may be requested from the presenter(s).

This presentation is provided as an information service and is a summary of current legal issues. This information is not meant as legal opinion and viewers are cautioned not to act on information provided in this publication without seeking specific legal advice with respect to their unique circumstances.

VANCOUVER CALGARY EDMONTON SASKATOON REGINA LONDON KITCHENER-WATERLOO GUELPH TORONTO VAUGHAN MARKHAM MONTRÉAL