Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

# The data grab: Cybersecurity risk, protection and response

Tony Morris, Partner
Jordan Deering, Partner

January 31, 2018

*motion*2018
discussing what matters

# Join the conversation

Tweet using #NLawMotion and connect with @NLawGlobal

Connect with us on LinkedIn
linkedin.com/company/nortonrosefulbright

# Speakers

## Tony Morris

Senior Partner
Calgary

Tony Morris assists technology suppliers and users in structuring, negotiating and implementing technology-related corporate and commercial transactions, including business process and information technology outsourcing and service agreements, competitive procurements, investment and finance and the reworking of information technology relationships. Mr. Morris provides guidance on technology licensing and development, electronic commerce, cloud computing and “software as a service” applications, privacy, product acquisition, reseller and distribution arrangements and other commercial transactions. He has also advised clients on issues of copyright, trade secrets, and trade-marks and is a registered trade-mark agent.

Mr. Morris has lectured regularly on various aspects of outsourcing, technology, privacy and electronic commerce law.

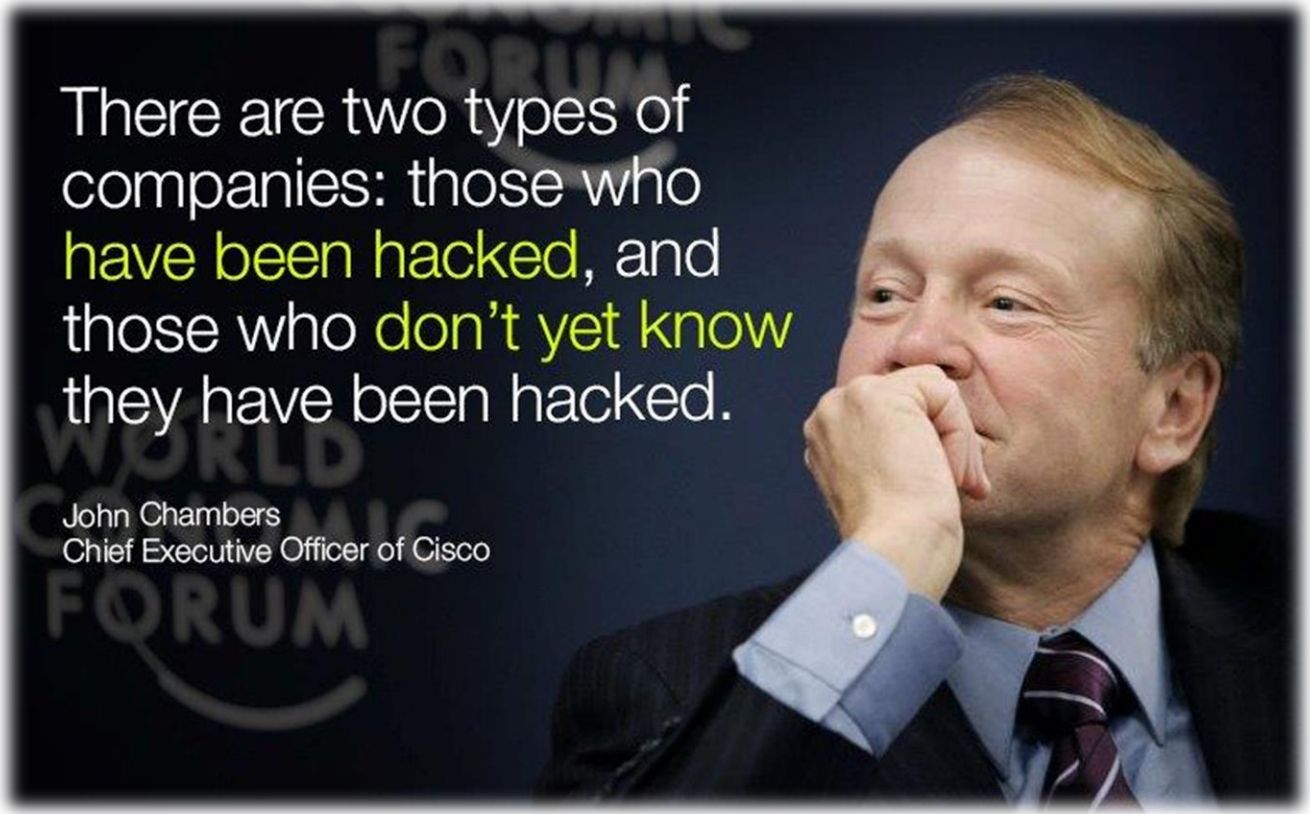
In addition to his law degree from the University of Alberta, Mr. Morris holds an MBA (Alberta) and an LLM in the "Law and Business of E-Business" (Osgoode Hall).

# Speakers

## Jordan Deering

Partner
Calgary

Jordan Deering represents corporate clients and investors relating to all aspects of fraud, bribery, corruption, white collar crime, and corporate investigations. She acts for victims of Ponzi schemes, mortgage fraud, employee theft, and other fraud schemes. Jordan provides advice to her clients respecting compliance with and investigations pertaining to the Corruption of Foreign Public Officials Act. She is regularly called upon by clients to assist in developing fraud and corruption prevention policies and programs, including whistleblower programs, compliance officer training, and risk assessment.


There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco

# One definition of “cybersecurity”

*The ability to protect or defend an enterprise’s use of cyberspace from an attack, conducted via cyberspace, for the purpose of: disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or, destroying the integrity of the data or stealing controlled information.*

– US Committee on National Security Systems (CNSS-4009)

# Increased stakes and some numbers

- Norton Rose Fulbright “2017 Litigation Trends Annual Survey”:

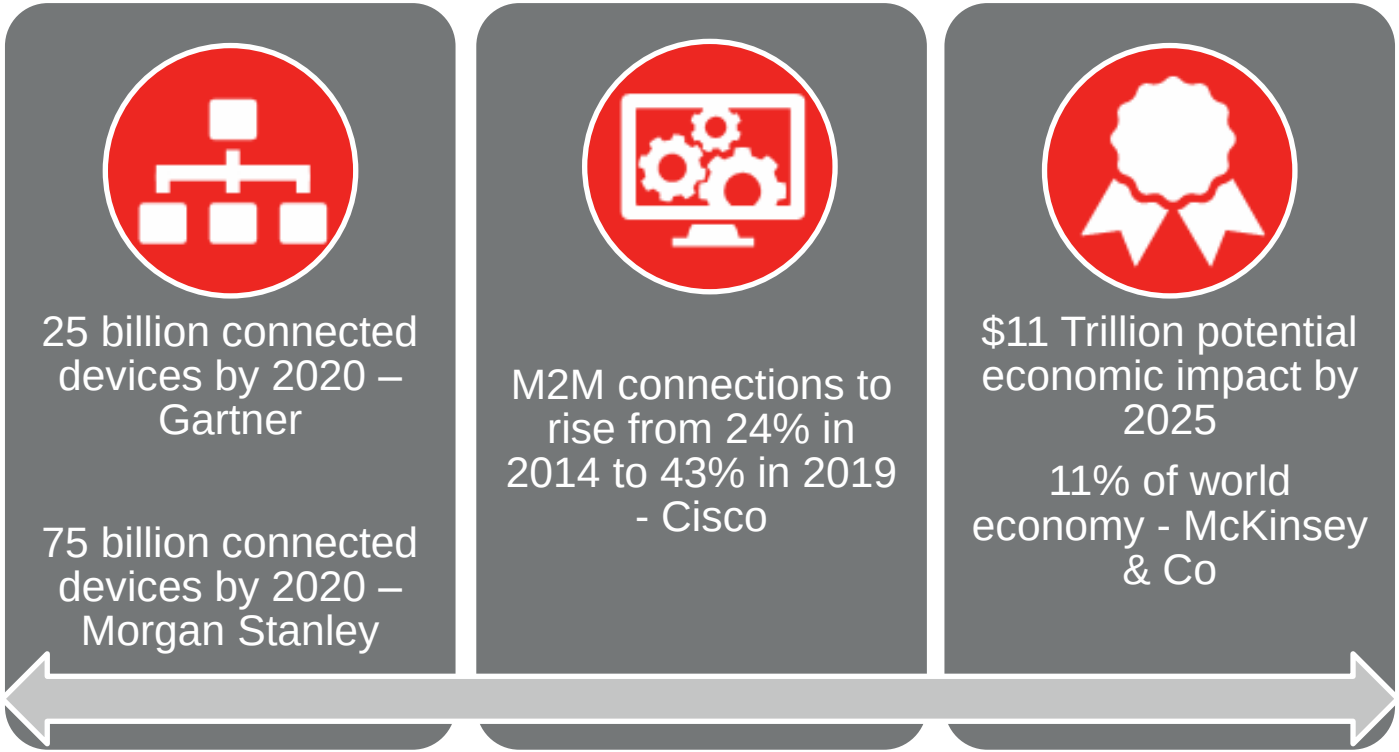
  “63% of respondents have become more exposed to disputes concerning cybersecurity and data protection over the last 12 months”

- Dark Web value as low as $1 per credit card or $10 for health information
- 2015 Global Internet economy: $4.2 Trillion

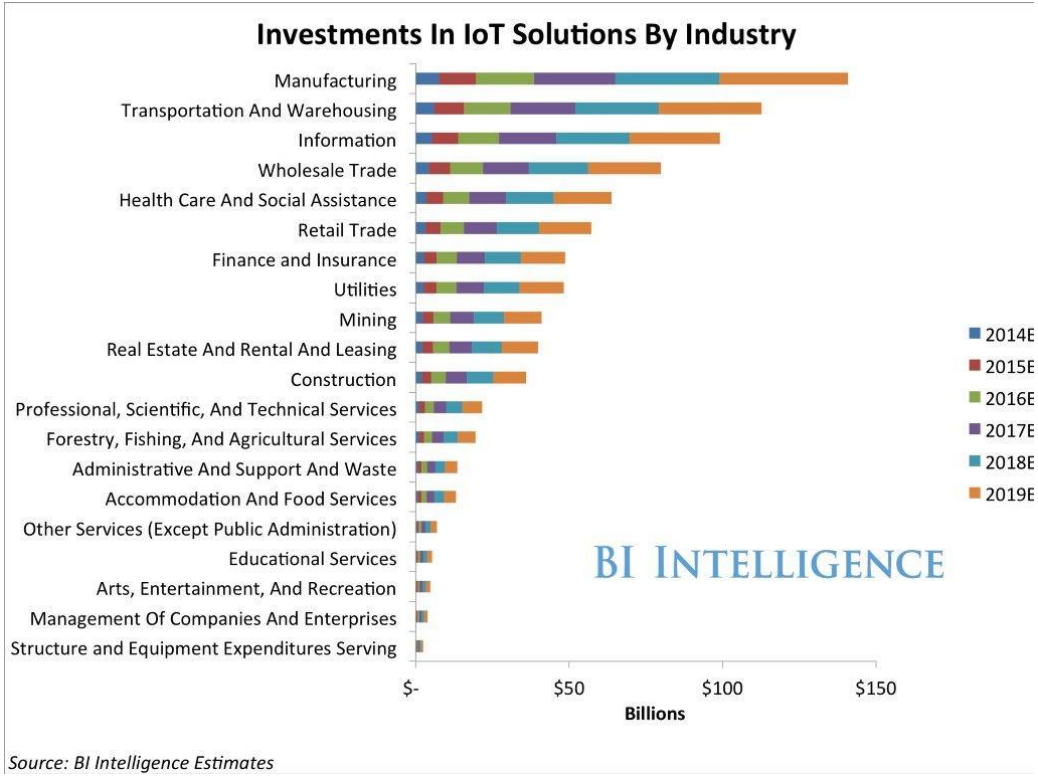
# Increased stakes and some numbers (cont'd)

- Cybercrime extracts 15-20% of that
- Canada loses 0.17% of GDP to cybercrime, or $3.12 Billion/year
- Ponemon Institute:
  - $3.62 million/breach
  - $141/record lost
  - +24,000 records/breach
  - 28% of recurring material breach over 2 years

# The Internet of Things by the numbers



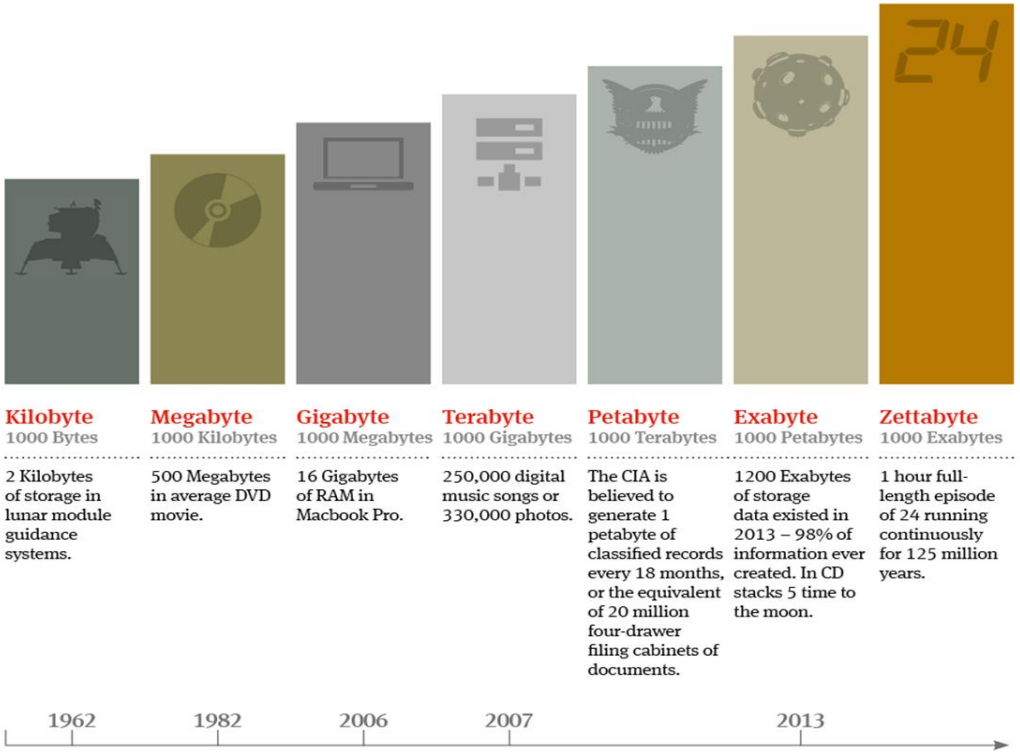
# Internet of Things sector opportunities



# What is big data?

- Big Data “is shorthand for the aggregation, analysis and increasing value of **vast exploitable datasets of unstructured and structured digital information**”.
- More data has been created in the past **two years** than in the entire previous history of the human race.
- By 2020, we will have over **6.1 billion smartphone** users globally.
- Within 5 years there will be over **50 billion smart connected devices** in the world, all developed to collect, analyze and share data.
- By 2020 our accumulated digital universe of data will grow from 4.4 zettabytes today to **~ 44 zettabytes.**

# Just how big is a zettabyte?



# Big data often characterized by the “3 Vs”:

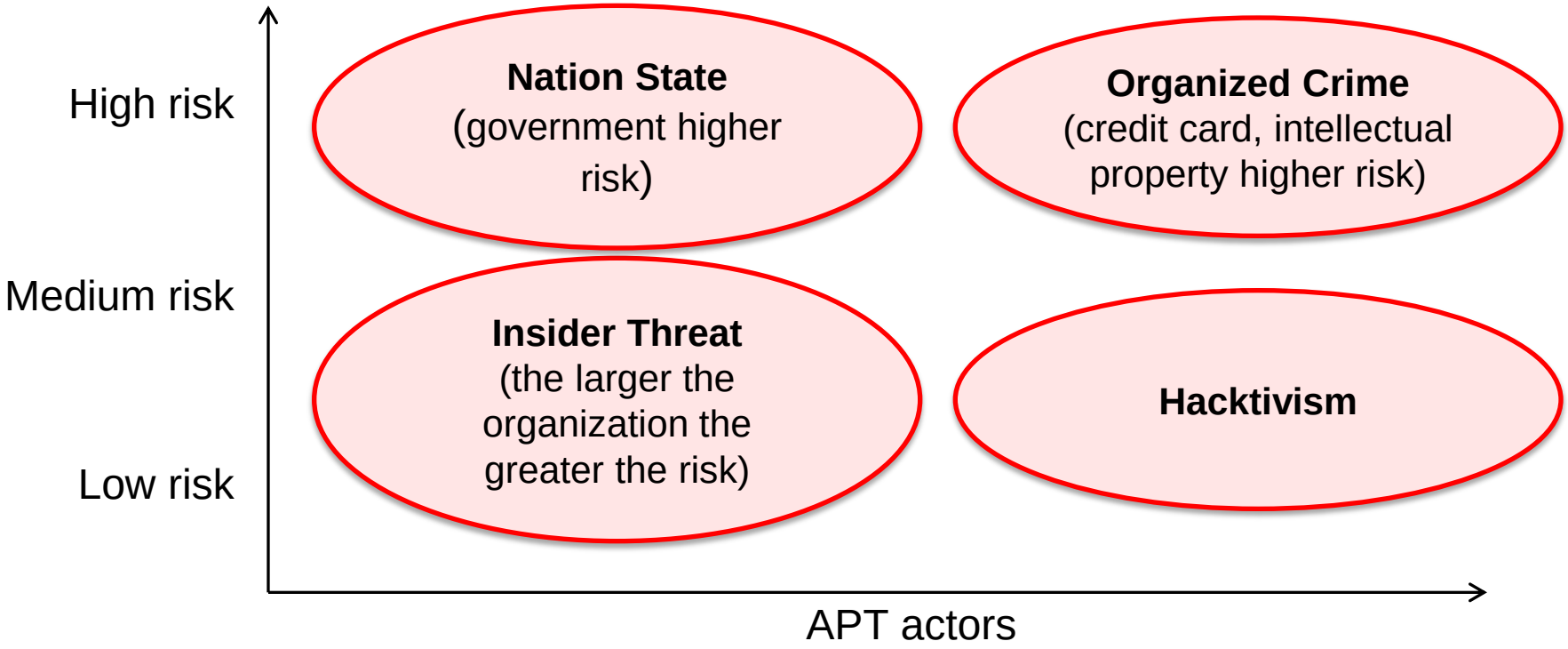
- **Volume**: the vast quantity of data that can be gathered and analyzed effectively
- **Velocity**: the speed at which new data can be accumulated, analyzed and utilized
- **Variety**: the breadth of data that can be effectively analyzed

# Sources of cyber attacks

- State-sponsored
- Organized crime
- Hacktivists
- Adversaries
- Insiders
- Competitors
- Skilled hackers
- Not-so-skilled hackers

# Cyber threats

# Advanced Persistent Threat (APT) actors

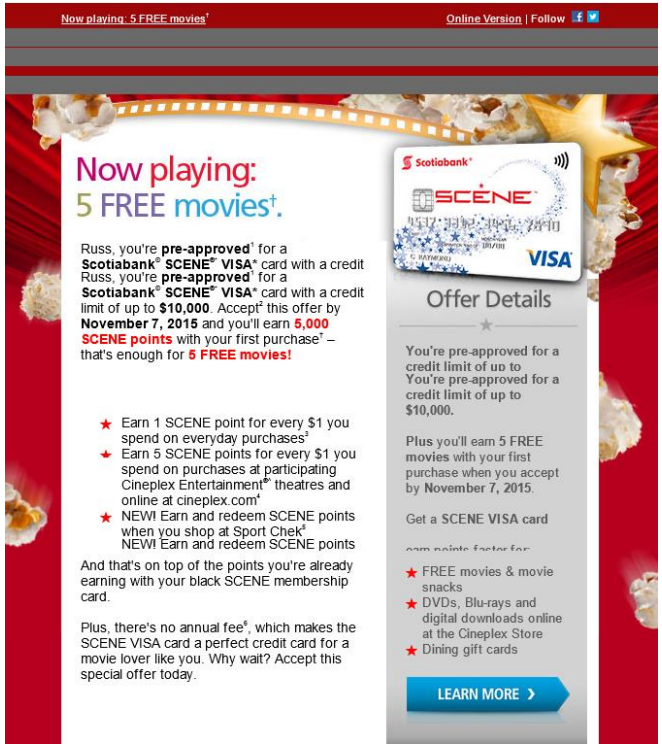


# Types of cybersecurity threats

- Phishing and s  pear-phishing
- Distributed denial of service
- Malvertising
- Watering holes
- Ransomware, malware and spyware
- Botnet (zombie army)
- Brute force

These are the primary strategies because **the interface between the keyboard and the chair** is the **most vulnerable** and weakest link that **no security technical layer can defend against**.

**From:** "Scotiabank" <noreply@yourcard.scene.scotiabank.com>
**To:** "russ g thomson" <russ.g.thomson@shaw.ca>
**Sent:** Friday, September 11, 2015 12:28:02 PM
**Subject:** Russ, say yes to 5 FREE movies with a SCENE VISA card.



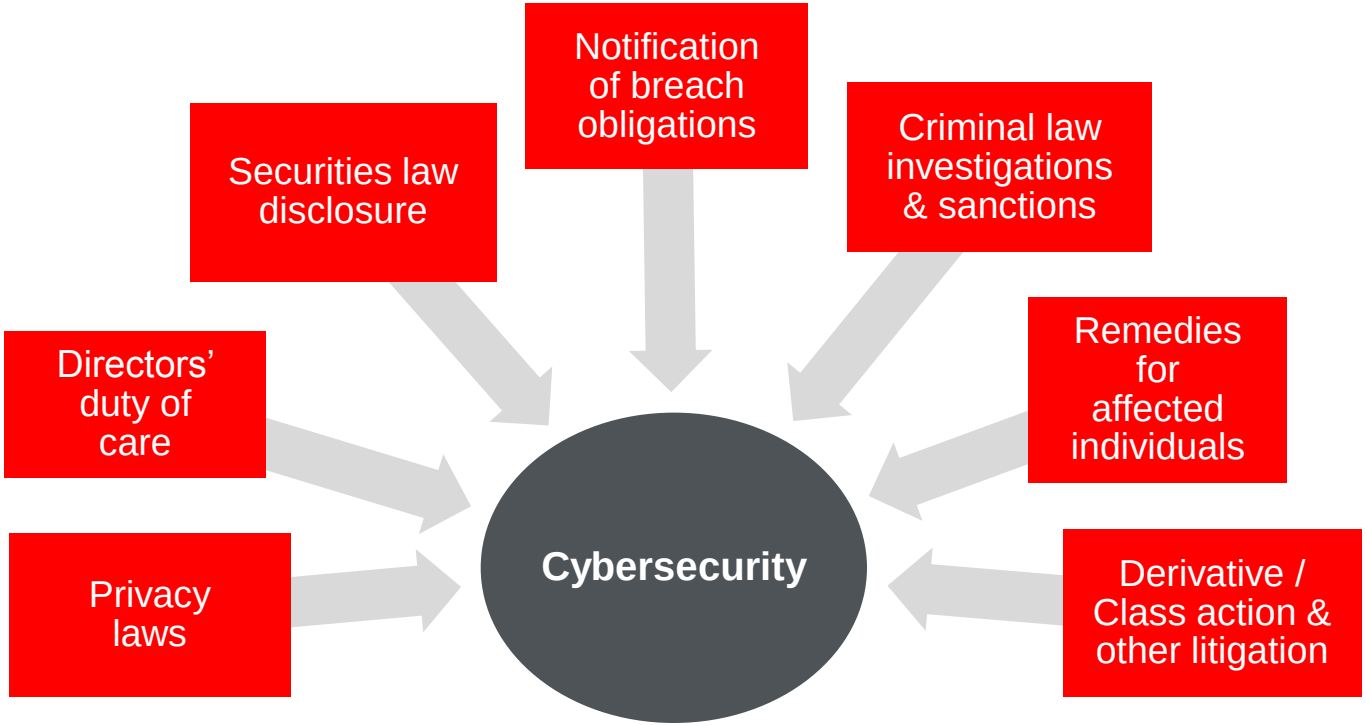

# Consequences

- Financial theft/fraud
- Theft of IP, proprietary data
- Business disruption
- Destruction of critical infrastructure
- Reputational damage
- Threats to life/safety
- Third party liability
- Class actions

# North American cybersecurity regulatory landscape

- There is **no overarching cybersecurity legislation** in either Canada or the US.
- A cybersecurity breach is generally not reportable to government authorities unless personal information has been compromised, as required by most states and some provinces.
- Civil liability is a concern in both jurisdictions. New causes of action emerging.
- Rise in **class actions** and **derivative actions** by shareholders against directors and officers.

# Canadian legal framework



# Criminal Code provisions

- Section 184(1): Interceptions
  - a “wilful interception of private communications” by means of an electronic device
  - 5 year imprisonment
- Section 342.1: Unauthorized use of a computer
  - wrongfully obtaining directly or indirectly a “computer service”
  - wrongfully intercepts any function of a computer system
  - wrongfully uses, possesses or traffics in computer passwords to enable the foregoing
  - 10 years imprisonment

# Criminal Code provisions (cont'd)

- Section 342.2: Possession of device to obtain unauthorized use of computer system or to commit mischief
  - makes, uses, sells, etc. a device to commit a s. 342.1 or s. 430 offense
  - 2 years imprisonment
- Section 402.2: Identity theft
  - fraud, deceit or falsehood to obtain or possess another's "identity information"
  - possesses, transmits, sells, etc. another's "identity information"
  - 5 years imprisonment

# Criminal Code provisions (cont'd)

- Section 403: Identity fraud
  - "fraudulently personates another person, living or dead" to gain advantage, obtain property, etc.
  - 10 years imprisonment
- Section 430: Mischief to Data
  - the wilful destruction or altering of computer data, or its obstruction or interruption, or rendering it meaningless or useless
  - 10 years imprisonment

And there are other relevant Criminal Code provisions

# Canada's Anti-Spam Legislation* ("CASL")

- Section 7: Altering transmission data
  - Without the express consent of the sender or receiver, altering the transmission of an electronic message such that it is delivered to a destination other than or in addition to that specified by the sender, is prohibited
  - To address "hacking" and "phishing"
  - Special "express consent" rules apply

*Not its real name!

# Canada's Anti-Spam Legislation (cont'd)

- Section 8: Installation of computer program
  - Without a person's express consent, installing a computer program on that person's computer, or sending electronic messages from that computer, is prohibited
  - To address "malware" and "spyware"
  - While exceptions apply, this is a **broad provision**. For businesses that install software remotely, **must consider CASL** and its special "express consent" rules.

# Canada's Anti-Spam Legislation (cont'd)

- Administrative Monetary Penalties: up to $1M for an individual or $10M for an organization, per violation, imposed by the CRTC
- Private Right of Action: damages and up to $1M per day [Enactment currently suspended]
- Director/Officer Liability if "directed, authorized, assented to, acquiesced in or participated in" a CASL violation
- Due diligence defences, so CASL compliance processes are key
- Class actions a real concern
- Need a "Chief CASL Compliance Officer"?

# Canadian Securities Administrators

- Staff Notice 11-326 “Cyber Security” (2013)
  - Public companies, registrants, regulated entities…basically market participants
  - “Strong and tailored cyber security measures”

- Staff Notice 11-332 “Cyber Security” (2016)
  - Comprehensive guidance regarding cyber security risk management:
    - Manage cyber security at an organizational level
    - “Identify, Protect, Detect, Respond, and Recover”
    - Robust awareness program for staff

# Canadian Securities Administrators (cont'd)

- Staff Notice 33-321 "Cyber Security and Social Media" (2017)
  - A survey of cyber security and social media practices at public firms (1000 surveys, 63% response)
  - 51% had a cyber security incident (43% phishing, 18% malware, 15% impersonate a client)
  - Most had cyber security policies but only 57% regarding how to ensure continual operation and 56% regarding employee training
  - 66% have an IRP which is tested at least annually
  - 30% use NO encryption of data
  - 59% have NO cyber security Insurance

# Canadian Securities Administrators (cont'd)

- Multilateral Staff Notice 51-347 "Disclosure of Cybersecurity Risk and Incidents" (2017)
  - Reviewed 240 issuer disclosures
    - 61% addressed cyber security issues
    - 20% identified those responsible for strategy management
    - 0% of breaches reported as "material"
  - Provides guidance concerning reporting issuers disclosure of cybersecurity risks if considered to be "material". Risk factors listed.
  - Provides guidance on when a particular cybersecurity incident must be disclosed. NP 51-201 Disclosure Standards for "material fact or material change"

# Key Canadian privacy laws: What law applies?

| Legislation | Applicable to |
|---|---|
| *Personal Information Protection and Electronic Documents Act* (Canada) (PIPEDA) | • Federal undertakings (i.e. banks) and employees of federal undertakings<br>• An organization conducting commercial activity within a province in which a law substantially similar to PIPEDA does not exist (which are all provinces except Alberta, BC, and Quebec)<br>• Interprovincial and international transfers of information<br>• PIPEDA does **not** apply to employee information except for that of federally regulated organizations |
| *Personal Information Protection Act* (British Columbia and Alberta) (PIPA) | • Any organization in British Columbia and Alberta, respectively, including its employees (deemed substantially similar to PIPEDA in October 2004) |
| *Act Respecting the Protection of Personal Information in the Private Sector* (Québec) | • Private sector enterprises in Quebec (deemed substantially similar to PIPEDA in December 2003) |
| *The Personal Information Protection and Identity Theft Prevention Act* (Manitoba) | • Any agency in Manitoba (Act not yet in force) |
| *The Privacy Act* (Saskatchewan) | • Any person who violates the privacy of another person. Provides a civil right of action. |

# Key Canadian privacy laws: What law applies? (cont'd)

| Legislation | Applicable to |
|---|---|
| *Personal Health Information Act* (Newfoundland and Labrador) | • Health information custodians in Newfoundland and Labrador |
| *Personal Health Information Act* (Nova Scotia) | • Health information custodians in Nova Scotia |
| *Personal Health Information Protection Act, 2004* (Ontario) | • Health information custodians in Ontario |
| *Personal Health Information Privacy and Access Act* (New Brunswick) | • Health information custodians in New Brunswick |
| *Health Information Protection Act* (Saskatchewan) | • Health information trustees in Saskatchewan |
| *Health Information Act* (Alberta) | • Health information custodians in Alberta |
| *The E-Health Act (Personal Health Information Access and Protection of Privacy Act*) (British Columbia) | • Data Stewardship Committee for information in health information bank or ministry database |
| Memorandum of Understanding between Alberta and British Columbia Information and Privacy Commissioners and Federal Commissioner | • Co-operation and collaboration in Private Sector Privacy Policy, Enforcement and Public Education |

# Privacy breach reporting summary: As of Nov 1, 2017

| Action | AB | ON* | NB* | MAN | NL* | NS* | CAN |
|---|---|---|---|---|---|---|---|
| **Mandatory** notification to applicable privacy commissioner | X†† | X | X | | X** | | X†† |
| **Mandatory** notification to affected individual | X† | X | X | X††† | X | X†† | X†† |
| Indirect notification is permitted (by conspicuous message or advertising) | X‡ | | | | | | X |
| Complaint possible*** | X | X | X | X* | X | X | X |
| Civil damages possible*** | X | X | X | X | X | X | X |
| Class action*** | X | X | X | X | X | X | X |

*Applicable to health care sector

**Material breaches only

***Exists even in jurisdictions where breach reporting/notification is not mandatory

‡ Indirect notice must be approved by Information and Privacy Commissioner

†If required by Information and Privacy Commissioner and real risk of significant harm

† †If real risk of significant harm

†††Does not apply if the organization is satisfied that it is not reasonably possible for the personal information to be used unlawfully

Not yet adopted or in force

# Breach notification: Regulatory requirements

## Alberta – Personal Information Protection Act (PIPA)

- Section 34.1: Notification of loss or unauthorized access or disclosure

  34.1 (1) An organization having personal information under its control must, **without unreasonable delay**, provide **notice to the Commissioner** of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a **reasonable person** would consider that there exists **a real risk of significant harm** to an individual as a result of the loss or unauthorized access or disclosure.

- "Real Risk"
  - Reasonable degree of likelihood that harm could result
  - Risk of harm is not hypothetical or theoretical, and is more than merely speculative
- "Significant Harm"
  - Material harm with non-trivial consequences
  - Examples: financial loss, identity theft, physical harm, humiliation, damage to one's professional or personal reputation

# Breach notification: Regulatory requirements (cont'd)

## Alberta – Personal Information Protection Act (PIPA)

- Section 37.1: Power to require notification

37.1 (1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the **Commissioner may require** the organization to notify individuals to whom there **is a real risk of significant harm** as a result of the loss or unauthorized access or disclosure

(a)in a **form and manner** prescribed by the regulations, and

(b)within a **time period** determined by the Commissioner.

[…]

(7) **Nothing** in this section is to be construed so as to restrict an organization's ability to **notify individuals on its own initiative** of the loss of or unauthorized access to or disclosure of personal information.

# Regulatory fines

## Alberta – Personal Information Protection Act (PIPA)

- Section 59(2): Failure to provide notice to Commissioner:
  - Up to $10,000 per offence for an individual
  - Up to $100,000 per offence for an organization
- Section 59(3) and (4): No offence if relying on the Commissioner's direction or if deemed to be "acting reasonably in the circumstances"
- Section 60: Certain rights for personal action claims to recover "loss or injury" damages, for orders made or offense convictions
- Given low bar to RRSH test by the Commissioner, often best to notify individuals promptly
- Strategy may be shifting as "liability goal posts" shift

# Breach notification: Regulatory requirements

**Federal –** Select amendments to PIPEDA under the *Digital Privacy Act*:

- Requires an organization to notify individuals and organizations of certain “breaches of security safeguards” that create "a real risk of significant harm" and report them to the PCC
- Requires an organization to maintain a record of every breach of security safeguards involving PI under its control
- Creates offences for contravening obligations, similar to Alberta, but no defense of relying on PC’s direction

Note: These amendments are not yet in force.

# Regulatory fines

**Federal –** Select amendments to PIPEDA under the *Digital Privacy Act*:

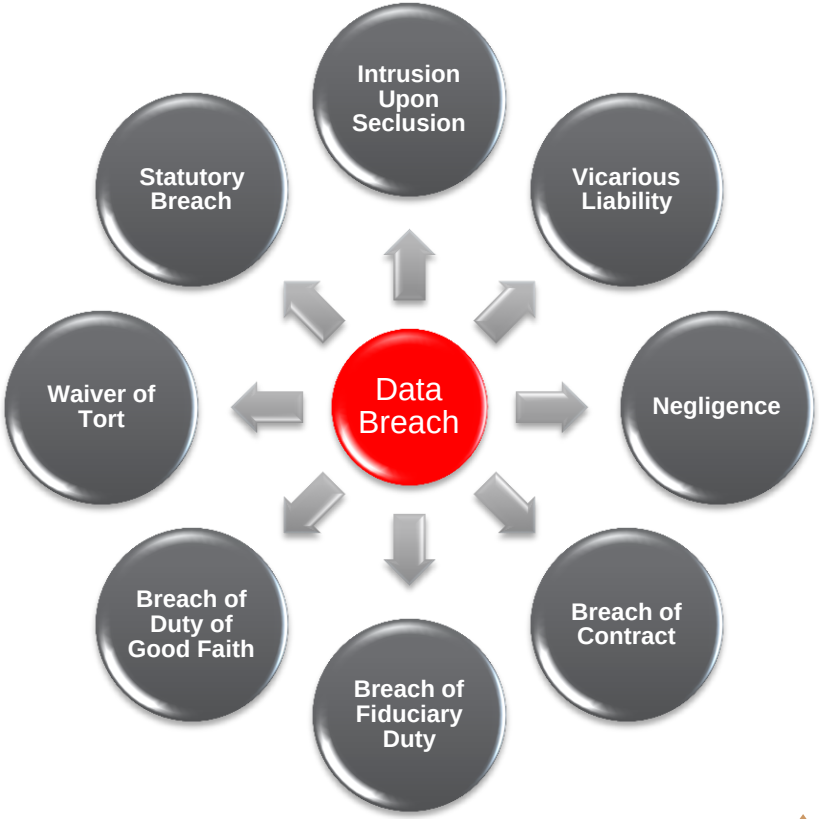
- Failure to provide notice to PCC and affected individuals, and failure to maintain records of every breach of security safeguards:
  - Up to $10,000 per offence punishable on summary conviction
  - Up to $100,000 per indictable offence

Note: Fines are not yet in force

# And more changes ahead

- General Data Protection Regulation (“GDRP”) in May 2018
- Much tougher than the “EU Data Protection Directive” (95/46/EC)
- Applies to both data “controllers” and “processors”
- Fines are significant:
  - first tier – up to €10M or 2% of total annual revenue
  - second tier – up to €20M or 4% of total annual revenue
- New breach notification obligation, to regulator and individuals
- Will PIPEDA stand? Will PIPA?

# Asserted causes of action



# Common law liabilities in Canada

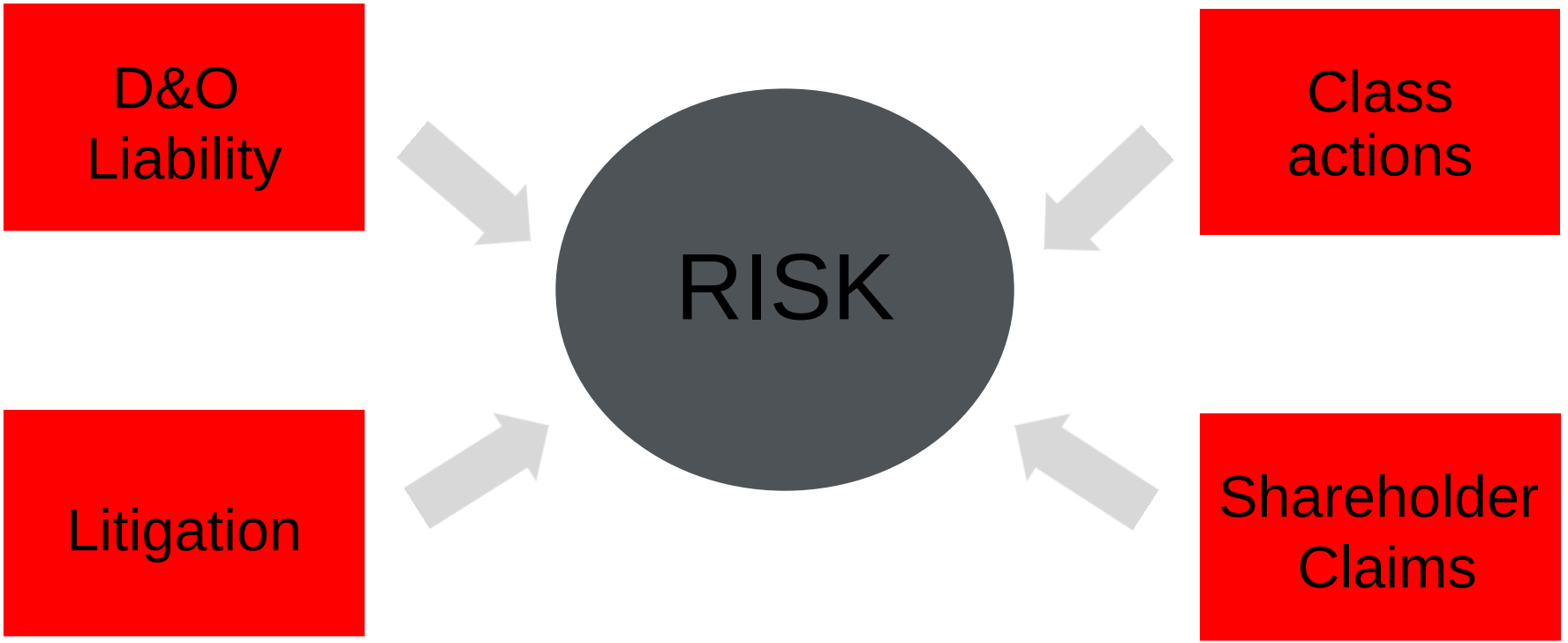
## Jones v Tsige, 2012 ONCA 32

- Intrusion upon Seclusion", new tort of invasion of privacy
  - Elements of the tort:
    - The Defendant's conduct must be intentional or reckless
    - The Plaintiff's private affairs must have been invaded without lawful justification
    - A reasonable person would view the invasion as being highly offending, causing distress, humiliation, or anguish
- Intrusion must be deliberate and significant (financial or health records, sexual preference and practices, employment, diary or private correspondence)

# Common law liabilities in Canada (cont'd)

## Jones v Tsige, 2012 ONCA 32

- Actionable without economic harm; however upper limit on damages set at $20,000
- Punitive aggravated damages available
- Damages assessment factors:
  - nature, incidence and occasion of act
  - effect a plaintiff's health, welfare, social, financial position
  - any relationship between the parties
  - distress, annoyance or embarrassment
  - conduct of parties before and after the act


D&O Liability
Class actions
RISK
Litigation
Shareholder Claims

# Class action litigation

- Conduct of company
- Report to privacy commissioners
- Timely response/ notice to customers
- Free offers to customers
- Damages suffered

# Director & Officer liability

# Becoming informed

Just a few Government publications on point:

- “Cyber Security in Canada: Practical Solutions to a Growing Problem”, Canadian Chamber of Commerce, 2017
- “Getcybersafe Guide for Small and Medium Businesses”, Government of Canada
- “Fundamentals of Cyber Security for Canada’s Critical Infrastructure Community”, Public Safety Canada, 2016
- “Getting Accountability Right with a Privacy Management Program”, The Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia

# Becoming informed (cont'd)

- "Privacy and Cyber Security Emphasizing Privacy Protection in Cyber Security Activities", Office of the Privacy Commissioner of Canada
- "Cyber Security Self-Assessment Guidance", Office of the Superintendent of Financial Institutions Canada, 2013
- Visit the "Canadian Cyber Incident Response Centre (CCIRC) website, and the Federal Privacy Commissioner's website

# Staying informed

Membership in cyber-security associations can help an organization stay informed about latest developments:

- Canadian Cyber Threat Exchange (CCTX)
- Canadian Centre for Cyber Risk Management (C3RM)
- Canadian Cybersecurity Alliance (CCA)
- American Society for Industrial Security (ASIS)
- The SANS Institute (SANS)
- Information Systems Security Association (ISSA)
- Cloud Security Alliance (CSA)

And many others

# The lifecycle of data loss: 8-step action plan

1. **Prevent** through policies, procedures, testing, audit and training
2. **Detect** through vigilance, safeguards and technological tools
3. **Contain** through immediate safeguards and “fixes”
4. **Assemble** breach response team per “Incident Response Plan”
5. **Investigate** breach
6. **Triage** breach through immediate containment measures
7. **Notify** and **Report** where required, necessary or prudent (regulators, individuals, insurers and others)
8. **Prevent** through post-mortem investigation and assessment and through the implementation of remedial measures

# Preventing data loss

- Identify
  - Privacy risks and security gaps, based on datasets in question
- Establish
  - Incident Response Plan, policies and procedures, update regularly
  - Cyber-insurance
- Conduct
  - Regular audits on systems and processes
  - Staff training on risks, procedures and policies
- Use
  - Encryption, access controls, authentications, etc.
  - Caution in giving network and building access to third party contractors

# Developing an incident response plan

- Establish an Incident Response Team (members, contact information, reporting lines and responsibilities)
  - Company privacy officer – should always be informed of security breaches
  - Internal team leads (e.g. executive, IT, finance, compliance, legal, HR, etc.)
  - External contacts (e.g. third party forensics provider, legal counsel, law enforcement, experts, credit monitoring service providers, broker, insurance company, etc.)
  - Ensure clear “chain of command”
  - Consider multijurisdictional team
  - Consider the maintenance of “legal privilege” throughout response

# Developing an incident response plan (cont'd)

- Identify data repositories and protections
  - Where data is stored, the nature of the information, the affected individuals, who has access and who is responsible
  - Reporting and notification protocols- internal, external, regulatory authority and affected individuals (who to notify and when)
- Consider key digital channels:
  - Point-of-sale security
  - Email security
  - Data security
  - Remote access security
  - Mobile device security
  - Physical security

# Developing an incident response plan (cont'd)

- Prepare
  - Protocol for initial investigation, report and proactive remedial measures
  - Provide escalation measures
  - External notification protocol
  - Post-breach review procedure, including system/internal audits if necessary
  - Predetermined "fixes"– flag files, further limit access, change codes, change account numbers, account "freeze", media lines
  - "Fixes" may be industry-based, may differ by jurisdiction and should always be "scoped out" in advance

# Developing an incident response plan (cont'd)

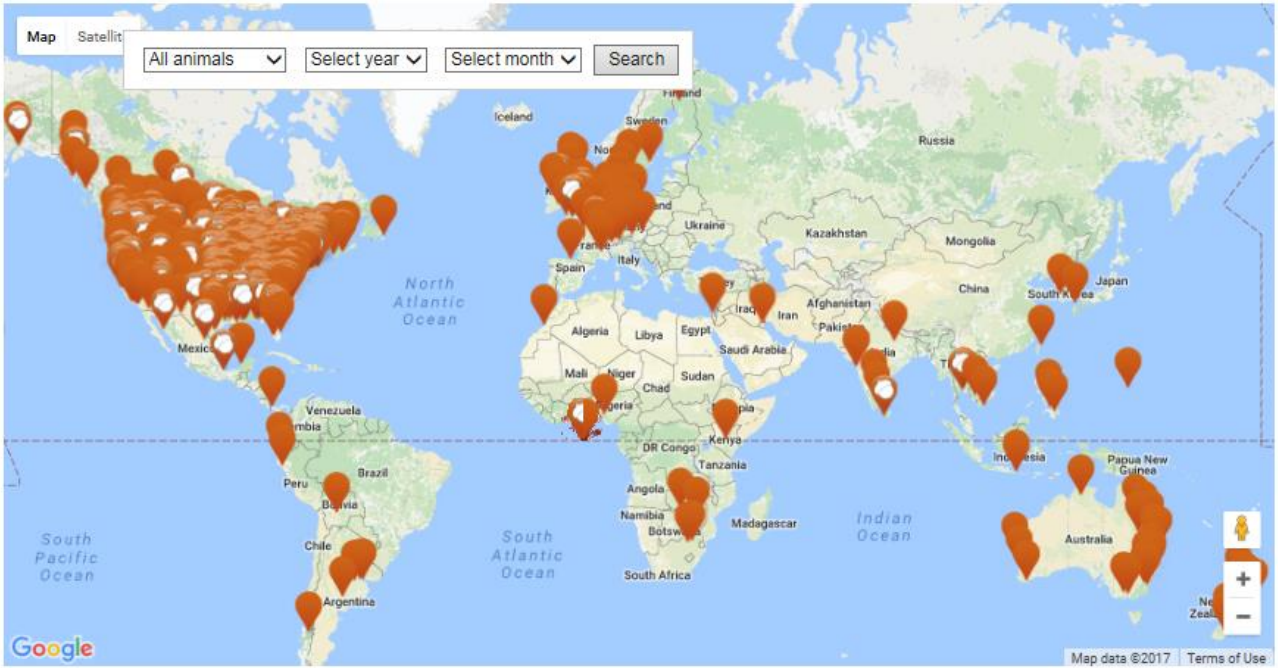
- Consolidate all relevant documents
  - Including insurance policies and key contracts - particularly where dealing with third-party suppliers who touch data
- Develop communication strategy
  - Who is involved to develop notifications?
  - Who should be notified and when?
  - Media Q&As, scripts, press releases
  - "Speaking voice" and consistency

# Data incident

| Incident identification | Containment | Investigate | Notifications | Validate & remediate |
|---|---|---|---|---|
| • Report incident response team leader and follow incident response plan<br>• Notify insurer and engage “breach coaches” under policy | • Assess the risk to continued operation (and steps to mitigate further risk) vs. preserving evidence and not alerting perpetrator<br>• Document steps undertaken | • Through forensic experts preserve evidence and assess systems & info impacted<br>• Document steps undertaken<br>• Use of privileged communication channels | • “Real risk of significant harm”<br>• Health records<br>• Voluntary notification<br>• Content requirements<br>• Mitigate class action risk<br>• Assess other disclosure obligations | • Validate systems<br>• Assess probable causes, future risks and system efficacy<br>• Learn & enhance |

# Cyber Squirrel 1

Disrupting at the highest levels, its #CyberWar4Ever!






motion2018
discussing what matters

NORTON ROSE FULBRIGHT

## TOTAL SUCCESSFUL CYBER WAR OPS AS OF 2017.04.02 - 1850

| Agent | Success |
|---|---|
| Squirrel | 927 |
| Bird | 461 |
| Snake | 84 |
| Raccoon | 76 |
| Rat | 41 |
| Marten | 23 |
| Beaver | 15 |
| Jellyfish | 13 |
| Human | 3* |

## ABOUT THIS MAP

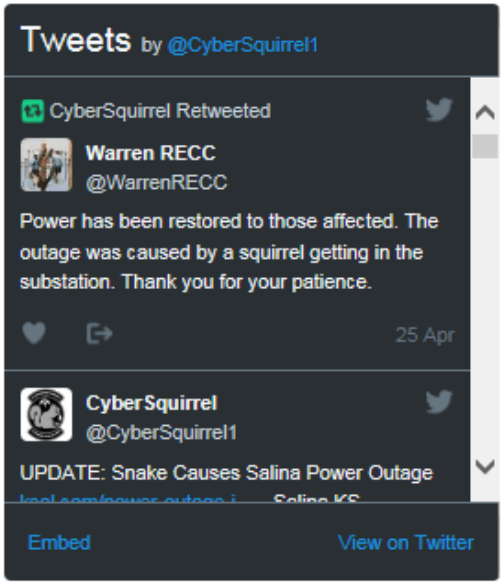
This map lists all unclassified Cyber Squirrel Operations that have been released to the public that we have been able to confirm. There are many more executed ops than displayed on this map however, those ops remain classified.

Confirmation for all ops has been preserved by the Internet Archive's WayBack Machine whenever possible.

"I don't think paralysis [of the electrical grid] is more likely by cyberattack than by natural disaster. And frankly the number-one threat experienced to date by the US electrical grid is squirrels." - John C. Inglis, Former Deputy Director, National Security Agency 2015.07.09

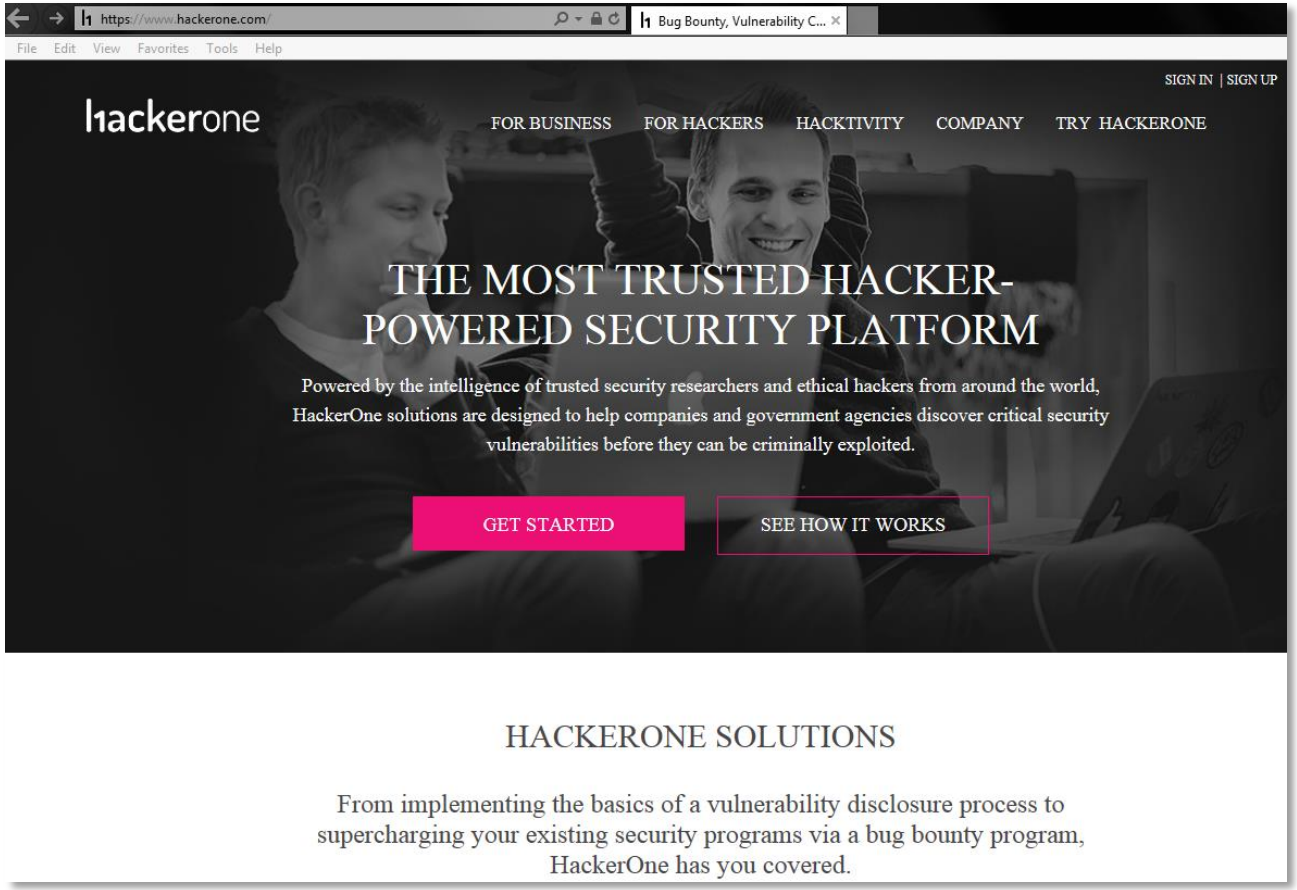
If you have confirmation of additional unclassified ops please email ops AT cybersquirrel1 DOT com

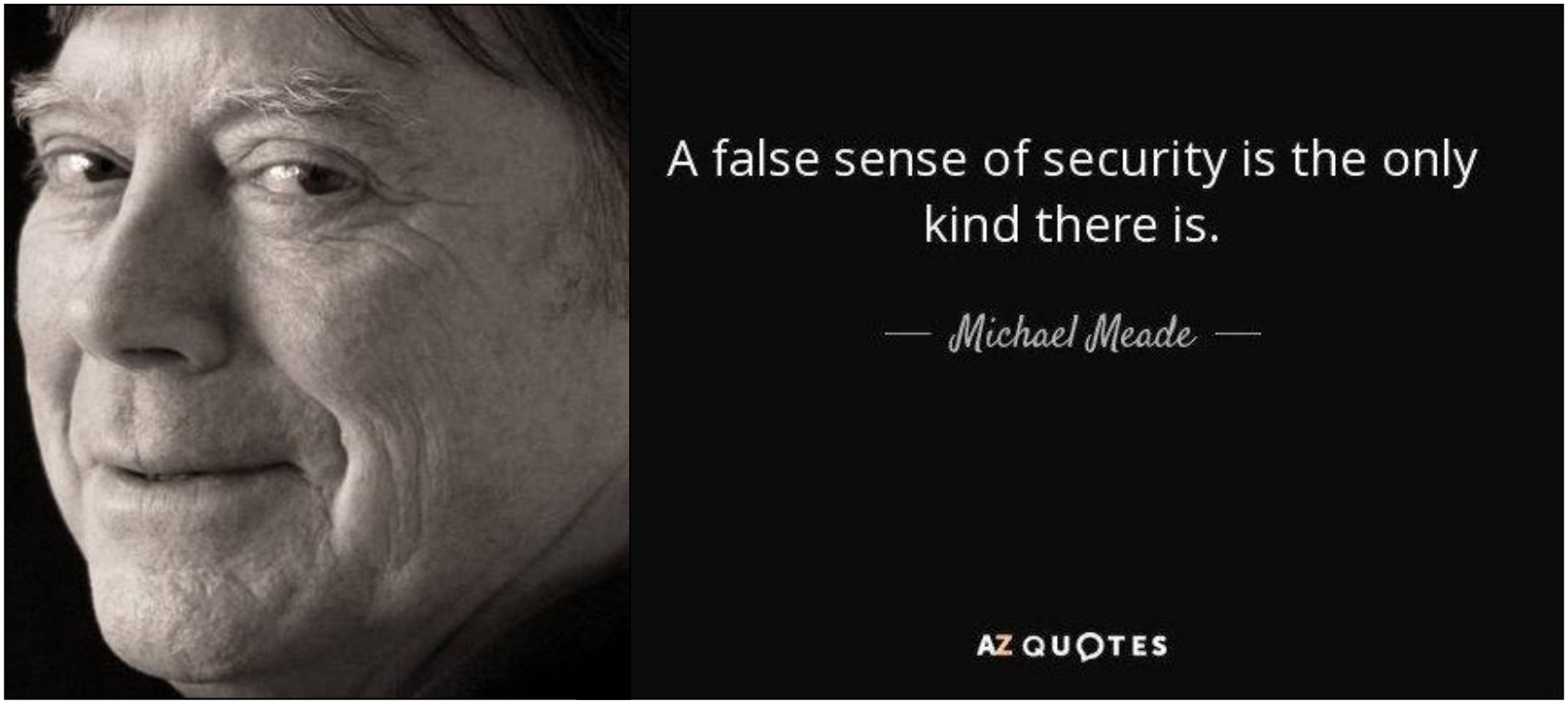
## MOST RECENT UNCLASSIFIED OPS




Tweets may be blocked by your Ad blocker

More Tweets by @CyberSquirrel1


https://www.hackerone.com/
Bug Bounty, Vulnerability C...
File Edit View Favorites Tools Help
hackerone
SIGN IN | SIGN UP
FOR BUSINESS
FOR HACKERS
HACKTIVITY
COMPANY
TRY HACKERONE
THE MOST TRUSTED HACKER-POWERED SECURITY PLATFORM
Powered by the intelligence of trusted security researchers and ethical hackers from around the world, HackerOne solutions are designed to help companies and government agencies discover critical security vulnerabilities before they can be criminally exploited.
GET STARTED
SEE HOW IT WORKS
HACKERONE SOLUTIONS
From implementing the basics of a vulnerability disclosure process to supercharging your existing security programs via a bug bounty program, HackerOne has you covered.


A false sense of security is the only kind there is.
— Michael Meade —
AZ QUOTES

# Contact

**Tony Morris**

Senior Partner, Norton Rose Fulbright

tony.morris@nortonrosefulbright.com

**Jordan Deering**

Partner, Norton Rose Fulbright

jordan.deering@nortonrosefulbright.com

motion2018

discussing what matters

NORTON ROSE FULBRIGHT