Cyber Risks, AI, Impacts Lessons Learned from Recent Attacks

Ann Wyganowski, MBCP, CCRP

HZX Business and Cyber Resilience Planning

Recent Attacks and Lesson Learned

- Cyber Security versus Cyber Resilience
- Canadian Landscape (hotter than climate change)
- Cyber Risk Assessment
- Case Studies
- Artificial Intelligence – friend or foe?
- What is the way forward?

What’s going on in Canada?
Here’s a small selection, seems daily

Date / Timeline	Victim	Type of Cyber Attack
Mar 11, 2024 (ongoing)	Town of Huntsville	Unknown maybe ransomware
Mar 6, 2024 (ongoing??)	FINTRAC; **Canada's financial intelligence unit. It is engaged in money laundering investigations, tracking millions of suspicious transactions annually and making thousands of disclosures about illegal money flows to the police**	Unknown; impact to the stock market may be unknown?
Mar 4, 2024 (ongoing)	City of Hamilton, ON	Ransomware
Feb 24-26, 2024	RCMP	Website – hosted by Shared Services Canada; DOS maybe?
Oct 11, 2023	Air Canada	Ransomware
Oct 23, 2023 (ongoing)	Bluewater Health, Chatham-Kent Health Alliance, Erie Shores HealthCare, Hotel-Dieu Grace Healthcare and Windsor Regional Hospital	Ransomware
Oct 27, 2023 – Mar 15, 2024	Toronto Public Library	Ransomware
June 26, 2023; April 24, 2023	Suncor, Petro-Canada	unknown
April 24, 2023	Yellow pages	Black Basta Ramsonware finally confirmed data leaked 2022 to 23
Feb 9, 2023	Indigo Chapters	Ransomware

What are we doing wrong?

Cyber Security versus Cyber Resilience

Cybersecurity

- **Prepare before the event**
- The prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.

CNSSI 4009

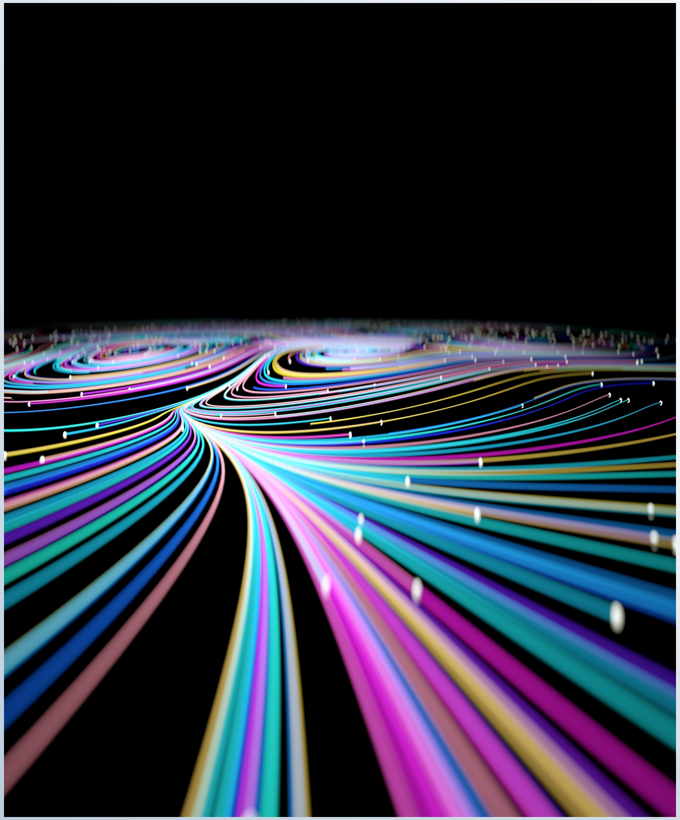
Cyber Resilience

- **Once you discover the breach!**
- An entity's ability to continuously deliver their products and services despite any adverse cyber events by actively preparing, planning, reacting, responding, and recovering the entity from cyberattacks. In addition, adapting to changing threat landscapes; effectively training personnel; and ensuring that response and recovery plans are maintained and exercised.

DRI

DRI International Glossary for Resilience

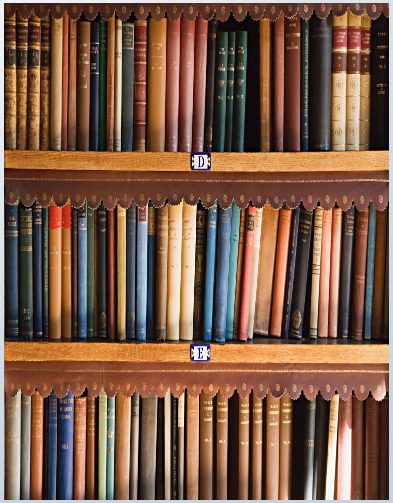
Cyber Risk Assessment



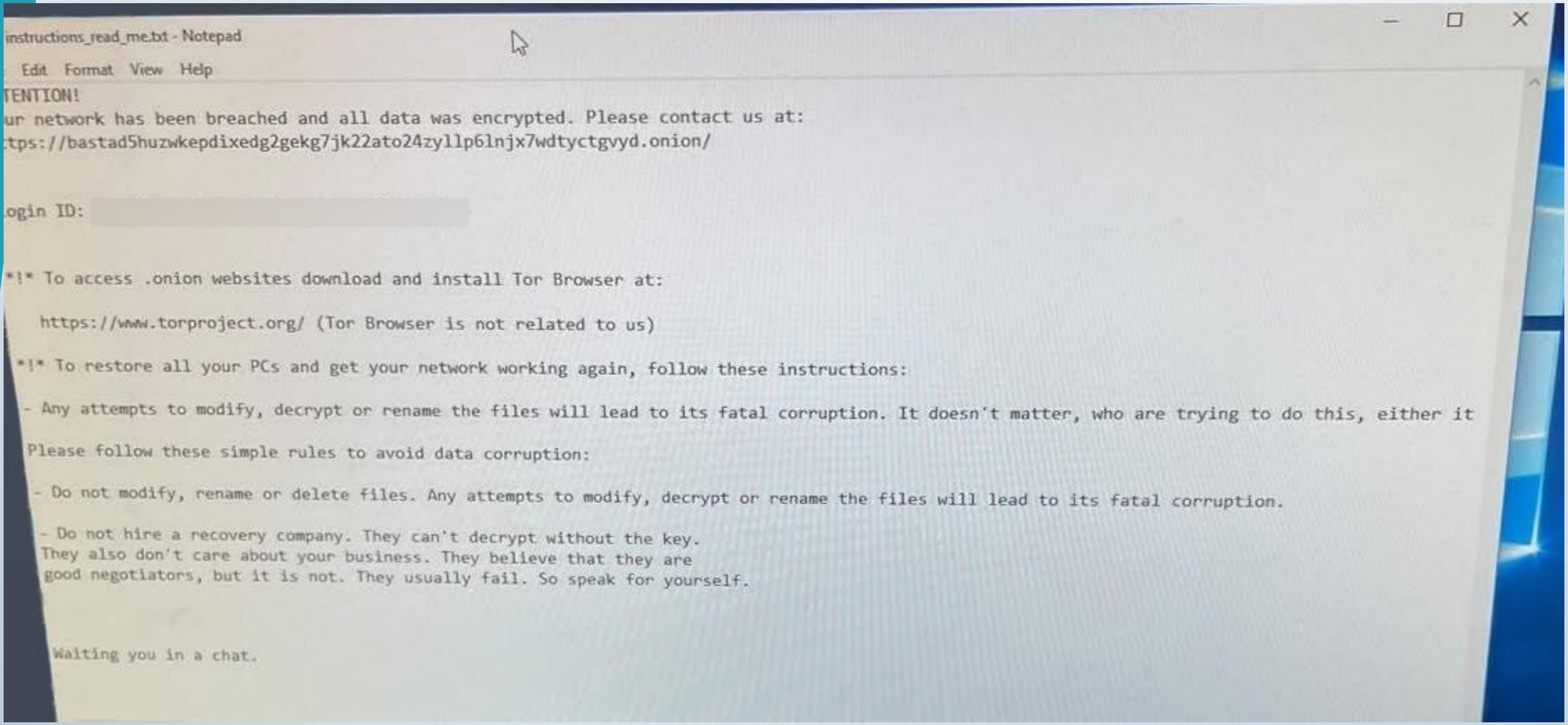
- What data do we safeguard?
- Who can do what with the types of data we hold?
- What are our endpoints?
- How up to date is our hardware, software, patch management?
- Where do we keep our encryption keys?
- Do we have a documented IT Disaster Recovery Plan?
- What do we back up and where is it?
- What do the critical business functions expect for RTOs and RPOs; do they have a plan for loss of IT Services?
- How detailed is our security incident management plan?
- Physical locations and service providers?

Toronto Public Library

- Canada's largest public library system
  - Access to 12 million books through 100 branches
  - 1,200,000 registered members
  - Annual budget over $200M.
- Oct. 27, 2023 – Overnight, attack becomes visible
- Oct 28, 2023 – Entire technical environment shut down, all internal and external networks
  - Move to shadow website
  - 3rd party cyber security technical experts and 3rd party legal counsel engaged
  - Police engaged, IMS activated, BCPs activated, Canadian Centre for Cybersecurity
- Oct 29, 2023 – Full isolation and containment
- Nov 1, 2023 "We have engaged with third-party cybersecurity experts to help us in resolving this situation. We do anticipate though that it may take several days before all systems are fully restored to normal operations."



Black Basta Ransomware Attack



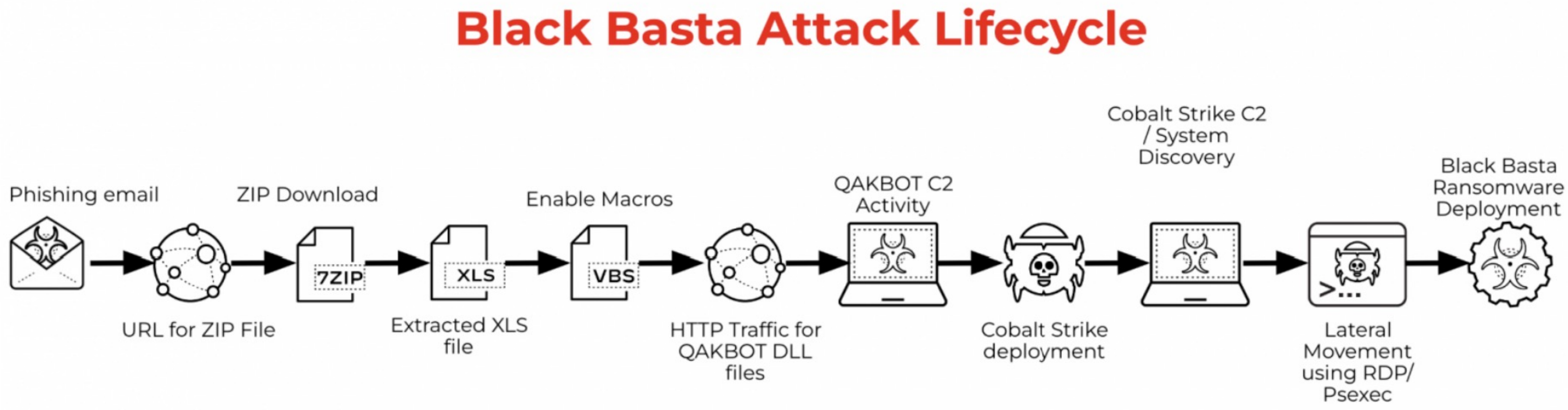
```
TENTION!
ur network has been breached and all data was encrypted. Please contact us at:
tps://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/


ogin ID: [redacted]


*!* To access .onion websites download and install Tor Browser at:

   https://www.torproject.org/ (Tor Browser is not related to us)

 *!* To restore all your PCs and get your network working again, follow these instructions:

 - Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it

  Please follow these simple rules to avoid data corruption:

  - Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption.

  - Do not hire a recovery company. They can't decrypt without the key.
  They also don't care about your business. They believe that they are
  good negotiators, but it is not. They usually fail. So speak for yourself.



   Waiting you in a chat.
```

Black Basta ransomware ransom note created on TPL workstations

Source: BleepingComputer

What is Black Basta???

- 2nd week of April 2023 gang launches several ransomware attacks globally
- Experts speculate a rebrand of a top tier ransomware gang
- File encryptor needs admin privileges to run
- Hijacks existing Windows service


Black Basta Attack Lifecycle
Phishing email
URL for ZIP File
ZIP Download
7ZIP
XLS
Extracted XLS file
Enable Macros
VBS
HTTP Traffic for QAKBOT DLL files
QAKBOT C2 Activity
Cobalt Strike deployment
Cobalt Strike C2 / System Discovery
Lateral Movement using RDP/ Psexec
>...
Black Basta Ransomware Deployment

Black Basta attack flow

Source: Palo Alto Networks Unit 42

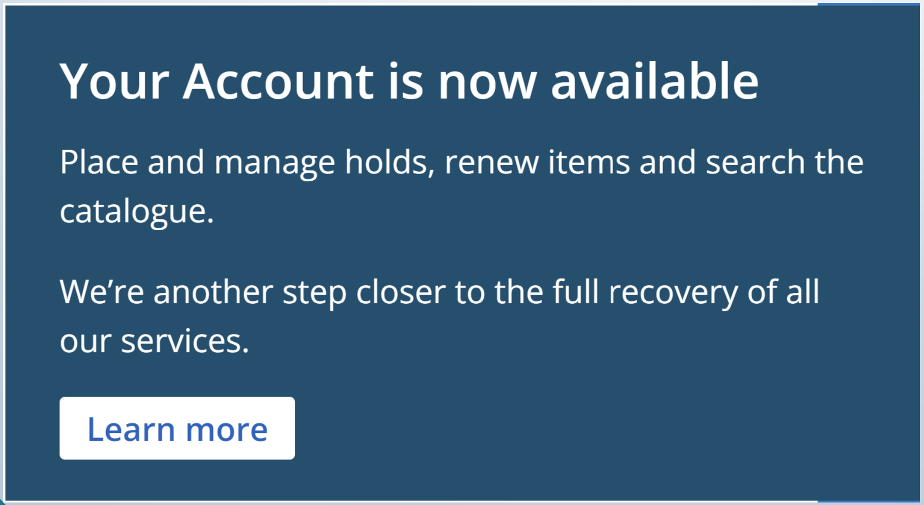
Story continues…

- Nov 15, 2023 – Privacy breach announced
  - Employees, Foundation employees, personal data dating back to 1998
    - Names, addresses, dates of birth, social insurance numbers and copies of government-issued ID
    - Two years of credit monitoring
    - Did not pay ransom, some data may be on dark web
  - Mayor Olivia Chow says still no timeline for restoration of services
- Dec 20, 2023 – City Librarian yearend report indicates interruptions will continue into 2024
  - Library remains a crime scene
- Jan 11, 2024 – Library indicates manual workarounds still in effect
- Feb 5, 2024 – Public computing resumes

The Toronto Public Library has been storing returned books in 12 offsite trailers ever since a cyberattack brought the institution to its knees on Oct. 28. (Courtesy of Toronto Public Library)

Slow return

- February 29, 2024 - restoration of catalogue, search features, and customer accounts after 4 months
  - Customers can now browse and search the catalogue, place and manage holds, renew items and view borrowing history and saved list
  - Some functionalities still not available
  - Full extent of the breach still being investigated



Your Account is now available

Place and manage holds, renew items and search the catalogue.

We're another step closer to the full recovery of all our services.

March 15, 2024
We're back to normal!

Why so long?

- Had a cyber resilience plan, BCPs, IMS, 3rd party providers
- Build back better!
  - NIST Cybersecurity Framework maturity level now improved (was at ‘Developing level’ typical of many public sector organizations)
  - Upgrades to software, servers, applications
  - Network segmentation
  - Improved patch management
  - Advanced threat monitoring and hunting, implemented SIEM (Security Information and Event Management) log management and aggregation

Still needed: Security orchestration, automation and response (SOAR) technology and AI integration with incident management

Global Team Work

- Information sharing is vital for every industry in order to gain in ISAC insight into threats, vulnerabilities, and mitigation strategies.
- In the U.S. and Canada, ISACs assist the federal government to protect critical infrastructure and the major sectors.
- Canada has more computers per capita than other country (129 devices per 100 people)
- Recent arrests and disbandments

Oct 2021 – Newfoundland & Labrador Centre for Health Information (NLCHI)

DURING COVID19 – overflowing emergency rooms, doctor shortage, surgical backlog

- Oct 15 – Attacker successfully initiates VPN connection using compromised legitimate user account
- Oct 15 – Attacker escalates privileges
- Oct 26, 29 – Attacker exfiltrated (unauthorized transfer) of personal and health data
- Oct 30 – Attacker deploys ransomware and encrypts numerous systems, widespread IT outage, ATTACK NOW DETECTED!!
- Provincial level EOC response
- Nearly all medical procedures cancelled
- Critical business functions revert to paper-based workarounds, IT rebuilds from scratch using clean backups
- May 2022 - $ 16M Cdn to date, no idea if ransom was paid
- Provincial Gov extends credit monitoring

Important considerations

- Human health and safety as ransom
- Privacy
- Artificial Intelligence use in health management
- Mental health
- Life safety

Artificial Intelligence What is the future?

Pros

- SOAR gets better at identifying attack indicators, threat detection and fast response
- Cyber threat intelligence improves
- Stronger policies for access and control
- Remember humans are still involved in the incident management but "we" can move faster

Cons

- AI needs large amounts of data to be effective
  - Data has to be clean
- Data privacy concerns, transparency
- Black hats are exploiting AI capabilities just as fast as "we" (the good) are
- AI is not perfect
  - Data poisoning can occur to manipulate the AI training data to decrease accuracy

What is the way forward?

- Cyber Resilience is different from Cyber Security
- Improve and monitor policies – face reality!
  - SIEM and SOAR
  - Need new technologies to keep up the fight
  - There is no endpoint
- Realize it’s a criminal activity and know where and how to report it
- Complete a proper risk assessment
- Make sure leadership understands they are accountable and liable for addressing risk(s)
- AI evaluation
- Data governance

Questions & Next Steps

- *Visit us at bcphelp.com*

About HZX Business Continuity Planning

- Over 30 years of experience in BCP & IT
- Certified BCP professionals (all contribute as volunteers in the industry)
- Extensive experience in BCP audits, testing & real BCP activations
- Broad industry experience ranging from small business, not-for-profits & government to large multi-nationals
- Aligned to continuity best practices
- Flexibility in approach
- Knowledge transfer to client