



Blake, Cassels & Graydon LLP | blakes.com



The Threat Of Our Virtual Reality:
Protecting your organization against
the wave of cyber attacks

October 7, 2020

ACC Ontario Chapter
www.acc.com

Presenters



ROBERT TREMBLAY
Legal Counsel, Corporate
Healthcare of Ontario Pension Plan



ALI ARASTEH
Managing Director
Mandiant/FireEye, Inc.



IMRAN AHMAD
Partner
Blake, Cassels & Graydon LLP



On the Agenda

1. Cyber Trends Overview
2. Data Breaches and Cyber Incidents in Review
3. Cyber Breach Response Scenario

Blakes

1

Cyber Trends Overview

Blakes Cyber Trends Study

- Designed to be a tool for businesses to:
 - Canada specific data
 - have snapshot of Canadian cyber landscape
 - Identify trends across industries and geographic regions
- Study has four parts:
 1. Cyber trends
 2. Privacy trends
 3. Public company trends
 4. Litigation trends

Blakes

Common Types of Cyber Threats



THEFT OF DATA



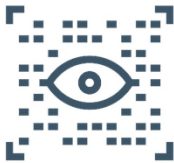
RANSOMWARE



INSIDER THREAT



DDOS ATTACK



CRYPTOMINING



PHISHING & SOCIAL
ENGINEERING



BOTNETS

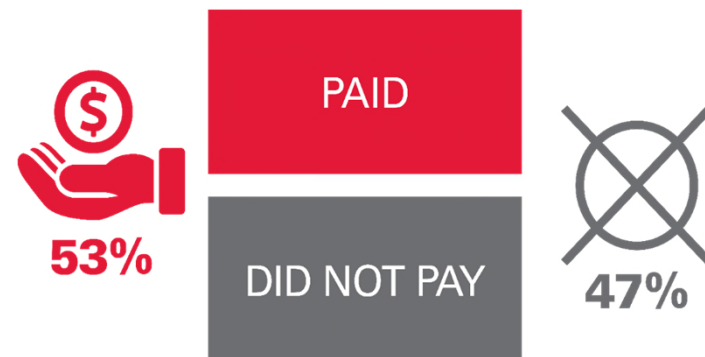
Participant Question

Q: What cyber threats are you most concerned about?

- Ransomware
- Bot attack
- Data theft
- All of the above
- Other

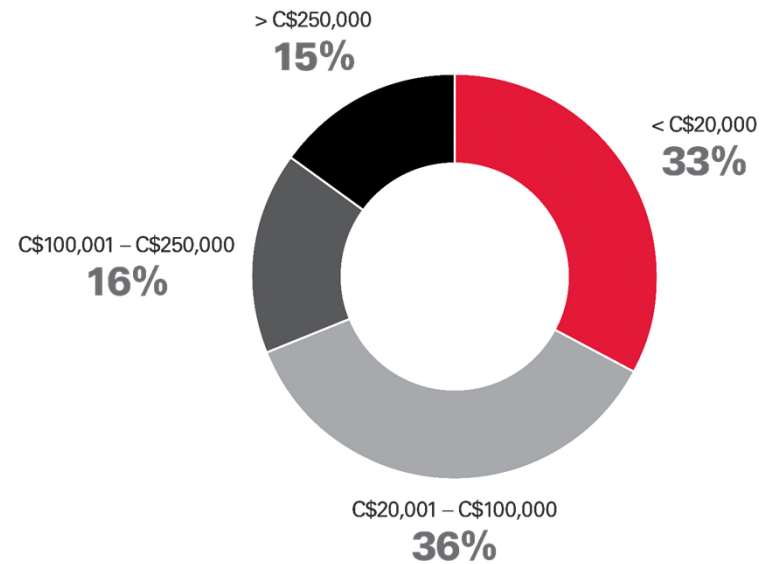
Blakes

In the event of ransomware attacks, what percentage of organizations paid the ransom?



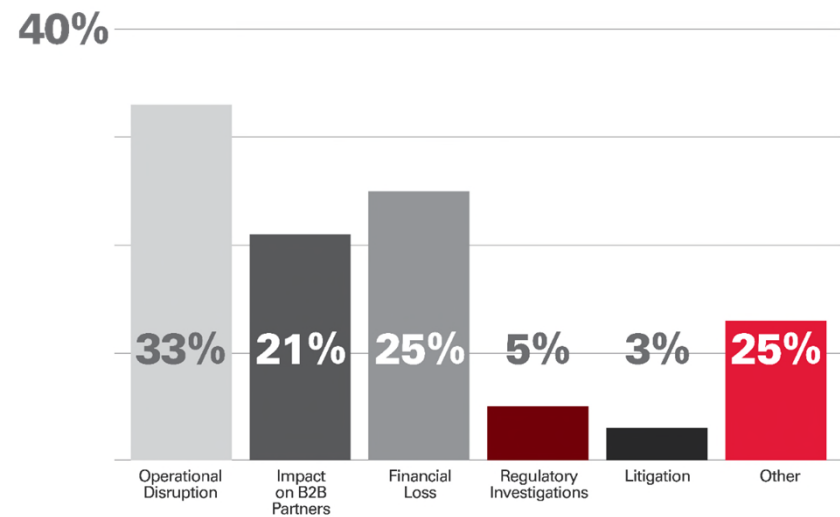
Blakes

Where a ransom payment was made, what was the average payment amount?



Blakes

What was the primary impact of the cybersecurity incident on your organization?



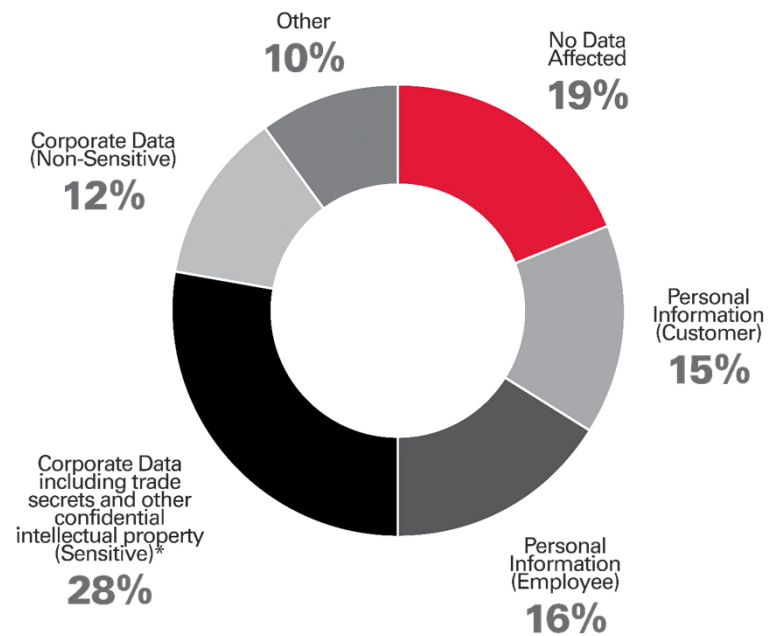
Blakes

What is the average time for a business to recover from a cybersecurity incident?

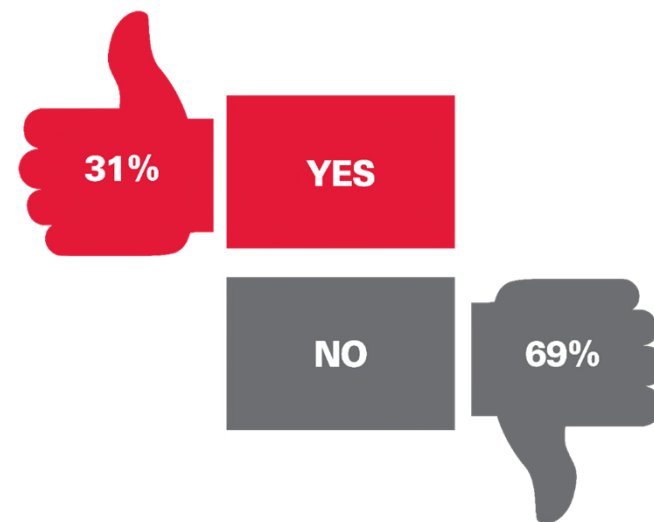


Blakes

What type of data did hackers have access to?



Was the cybersecurity incident reported to law enforcement?



Did the organization
have standalone cyber
insurance in place?

YES
14%

NO
86%

Blakes

Participant Question

Q: What percentage of companies have a cybersecurity incident response plan in place?

- < 20%
- 20 – 40 %
- 40 – 60%
- > 60%

Blakes

Did the organization have a Cybersecurity Incident Plan (CIRP) in place that it followed when dealing with a cybersecurity incident?

YES
29%

NO
71%

Blakes

Key Takeaways

- Cyber risks are quick evolving
- Cyber criminals using new tactics to force payment
- “Return to normal” can be lengthy process
- Preparation materially reduces negative impacts of a cybersecurity incident

Blakes

2

Data Breaches and Cyber Incidents in Review

Understanding Legal Risks & Damages

- Current trends in data breach litigation
 - What are plaintiff's class action lawyers looking for?
 - What activities and breaches have given rise to claims?
 - How have claims been framed?
 - How are defendants responding to such claims?
- Damage awards
 - What can be claimed?
 - What has been successful?
 - How much has been obtained through recent settlements?
- Coverage litigation
 - Does the act of war exemption apply?

Blakes

Causes of Action Alleged

- Tort of intrusion upon seclusion
- Tort of public disclosure of private facts
- Breach of privacy statutes
- Breach of confidence
- Negligence
- Breach of contract/warranty
- Breach of fiduciary duty
- Unjust enrichment
- Vicarious liability for conduct of employees
- Note that the Supreme Court has recently held that waiver of tort is not an independent cause of action

Blakes

Damages Sought in Civil Litigation

- Compensation for mental distress
- Compensation for identity theft/fraud
- Costs of credit monitoring
- Out-of-pocket costs
- Disgorgement of profits
- Symbolic/moral damages for intrusion on seclusion
- Aggregate awards of monetary relief where no proof of loss by individual class members is required
- Punitive damages

Blakes

Tucci v. Peoples Trust Company, 2020 BCCA 246

- Unencrypted database breached by Chinese hackers from Peoples Trust, a federally-regulated trust company
- PII included dates of birth, social insurance numbers, occupations, and, in some cases, mothers' birth names
- The company had failed to apply patches and software updates on the server
- Some of the stolen data used in “phishing scams”, but not established at this stage whether the information was misused for any other purposes

Blakes

Tucci v. Peoples Trust Company (BCCA)

BCCA held:

- PIPEDA is not a complete code that precludes common law remedies for breaches of privacy
- There is no “federal common law” of intrusion on seclusion
- Its own prior decisions that there is no cause of action for breach of privacy or intrusion upon seclusion in BC beyond the limited statutory claim provided for in the *Privacy Act*, should be revisited in a future case
- Breach of contract and negligence claims were properly certified
- Breach of confidence not certified, as the cause of action requires intentional misuse of confidential information (refused to follow FCA in *Condon* and *Doe*, in which intention not required)

Blakes

Kaplan v. Casino Rama, 2019 ONSC 2025

- Action not certified
- Class action arising out of a criminal cyberattack
- A “very convoluted class action”: no provable losses and the real intruder (the hacker) was not a defendant
 - Publicity given to private life and breach of confidence claims struck
 - Intrusion upon seclusion, negligence, and breach of contract claims not “doomed to fail” but court noted defendant was not the intruder

Blakes

Kaplan v. Casino Rama

- Class action “collapsed in its entirety” on commonality – type and amount of information stolen varied considerably from individual to individual
 - Some stolen information was sensitive, much of it not inherently private
- Positive commentary about defendants’ response to cyberattack

Blakes

Broutzas v. Rouge Valley Health System, 2018 ONSC 6315 and 2018 ONSC 6317

- Action not certified
- Alleged unauthorized disclosure of hospital patient contact information
- Affirmed that parameters of intrusion upon seclusion are “tight and narrow” and not established by “guilt by association”
 - Only actual “intruders” were rogue hospital employees
 - Information intruded upon – contact information – not inherently private
- Negligence should not be used as a “backstop” where requirements of intrusion upon seclusion not made out

Blakes

Broutzas v. Rouge Valley Health System

- Class action not the preferable procedure
 - Behaviour modification unnecessary
 - Small claims court actions could provide access to justice for few class members who may have experienced harm
- Privacy Commissioner order did not create an issue estoppel against the hospital

Blakes

Lessons Learned

- Value of effective breach response in mitigating litigation risk
 - Comprehensive notice program
 - Offers of credit monitoring in appropriate circumstances
 - Cooperation with law enforcement/regulators
 - Use of takedown notices
- Intentional torts not suited to many privacy breach cases
- Preferable procedure is a live battleground in cases with no or few provable losses
- Plaintiffs' counsel very focused on finding a path to aggregate damages
- Privacy Commissioner findings not determinative of civil liability

Blakes

Questions?



Blakes



Blake, Cassels & Graydon LLP | blakes.com



Association of
Corporate Counsel
ONTARIO



Thank you for joining us today

ACC Ontario Chapter
www.acc.com
