COVID-19 PRIVACY AND CYBERSECURITY CONSIDERATIONS FOR LAWYERS

Authors

Nathan Schissel & Kristél Kriel

Law Society of Saskatchewan

PRESENTATION OUTLINE

- Threat Landscape
- Legal Framework
- Phases of a Cybersecurity Incident
- Things You Can Do
- Other Hot Topics
- Q & A

THREAT LANDSCAPE

Law Society
of Saskatchewan

CYBERSECURITY ISSUES

- Cybercriminals exploiting fear and reactions to COVID-19
  - Increased vulnerability with work-from-home arrangements and new technologies
  - Psychological impact of COVID-19
- Various strategies
  - Phishing and fraudulent email campaigns
  - Wire Fraud
  - Text message scams
  - Ransomware
  - Constantly evolving…
- Increasing number of attacks – interrelated
- Lawyers and law firms are targets!

WHAT IS THE IMPACT?

- Financial losses
- Business interruption
- Damage to brand and reputation
- Regulatory investigations and proceedings
- Litigation

LEGAL FRAMEWORK

Law Society
of Saskatchewan

LEGAL FRAMEWORK

- Privacy
- Regulatory/ Ethical Considerations
- Common Law
- Other

PRIVACY LEGISLATION

- The collection, use and disclosure of personal information (PI) is governed by a number of federal and provincial laws
- Which law applies to an organization will depend on where it is located and the industry it is engaged in
- PI = essentially any information about an identifiable individual
- Range of sensitivity of PI (name vs. financial)

PRIVACY LEGISLATION CONT'D

- *The Personal Information and Protection of Electronic Documents Act* (PIPEDA)
- Changes pending
  - Bill C-11: the *Digital Charter Implementation Act, 2020*
  - *Consumer Privacy Protection Act* & the *Personal Information and Data Protection Tribunal Act*

KEY PRINCIPLES FOR CYBERSECURITY

- Responsible for PI when transferred to third party
- Contractual or other means to provide comparable level of protection
- Security for information appropriate to sensitivity of information
- Physical, organizational, and technological measures
- Breach = unauthorized disclosure → be open and responsive
- Others …

BREACH NOTIFICATION REQUIREMENTS

- PIPEDA Breach Notification and Record Keeping Requirements
  - Assess breaches on a case-by-case basis
  - Can be much harder than it sounds – whether or not notification is required will depend on the facts but requires legal analysis

FOUR MANDATORY REQUIREMENTS

1. Notification to Affected Individuals
2. Notification to the Office of the Privacy Commissioner of Canada (OPC)
3. Notification to Other Organizations
4. Maintenance of Records

- Note: A “trigger” is applicable to requirements 1 and 2:
  - *Reasonable to believe in the circumstances that the breach poses a real risk of significant harm to the affected individual(s)*

REGULATORY/ ETHICAL CONSIDERATIONS

- Hold information concerning business and affairs of clients in strict confidence
- Care for property as careful and prudent owner
- Take all reasonable steps to ensure privacy and safekeeping
- Duty to report (e.g., trust monies, material prejudice)
- Direct supervision of students, staff, others
- Client identification and verification
- Others

PHASES OF A CYBERSECURITY INCIDENT

Law Society
of Saskatchewan

PHASES OF A CYBERSECURITY INCIDENT

Law Society of Saskatchewan

PHASE 1: PREPARATION

- A cybersecurity preparedness strategy has two main objectives:
    1. Minimizing the chance of a successful breach
    2. Mitigating the effects of a breach
- Cybersecurity is not just an IT issue
- Cybersecurity preparedness is focused on risk mitigation – not perfection
- No cybersecurity strategy will eliminate all risk

PHASE 1: PREPARATION (CONTINUED)

- Assess legal and regulatory requirements
- Map out networks
- Identify threats and vulnerabilities
- Prepare protective measures
  - Incident Response Plan & Team
  - Third Party Security Reviews, Recommendations and Remediation
  - Privacy and Security Policies, Procedures and Safeguards
  - Employee Training and Awareness
  - Contracts (Due Diligence, Data Protection Schedules, Security Requirements)
- Cybersecurity insurance

SPECIFIC PROTECTIVE MEASURES

- Backups!
- Remote work policies
- Communication and agreements with staff
- Antivirus monitoring
- Review technology infrastructure
- Review money transfer protocols
- Verify sources of information
- Approach requests for information with caution
- Incident response planning

PHASE 2: INCIDENT RESPONSE

- Trigger your IRP
  - Consider a “Breach Coach”
  - Notify insurer
  - Assemble your Team
  - Eliminate Vulnerability and Preserve Evidence
  - Evaluate Scope of Issues and Risk
  - Communication Strategy

PHASE 3: NOTIFICATION/REPORTING

REQUIREMENT 1: OBLIGATION TO NOTIFY AFFECTED INDIVIDUALS

Content:

- Minimum requirements are imposed for content of notice
- Additional information can be added as the circumstances dictate

- Means of Notification:
  - Direct or, in some cases, indirect notice
- Timing:
  - As soon as feasible after organization determines that breach has occurred
- Note: Consider any additional obligations to notify/report in other jurisdictions

PHASE 3: NOTIFICATION/REPORTING (CONTINUED)

REQUIREMENT 2: OBLIGATION TO REPORT TO THE OPC

- Content:
  - Minimum requirements are imposed for content of notice
  - Additional information can be added as the circumstances dictate
- Means of Notification:
  - Must be in writing, direct
- Timing:
  - As soon as feasible after organization determines that breach has occurred

PHASE 3: NOTIFICATION/REPORTING (CONTINUED)

REQUIREMENT 3: OBLIGATION TO NOTIFY OTHER ORGANIZATIONS

- Who:
  - Any other organization, government institution, or part of a government institution that may be able to reduce the risk of harm that could result from that breach, or mitigate that harm
- Why:
  - To reduce the risk of harm or mitigate harm
- What:
  - Disclosure of PI – Without consent
- Timing:
  - As soon as feasible after organization determines that the security breach has occurred

PHASE 4: RECORD-KEEPING

- Requirement 4: Obligation to Maintain Records
- Important:
  - Records of ALL security breaches are to be maintained
- Purpose:
  - Compliance & oversight
  - Encourage better data security practices
- Content:
  - Broad interpretation of “breach record”
  - Must contain information sufficient to enable OPC to verify compliance with breach reporting and notification obligations
- Minimum Requirements:
  - 24 months

THINGS YOU CAN DO

Law Society
of Saskatchewan

THINGS YOU CAN DO

- Backup data (and then back it up again)
- Get Incident Response Plan (IRP) in place, updated and tested
- Ensure the right resources are available and allocated to the area of privacy and security (e.g. privacy and security officer)
- Utilize third party experts to periodically review and test your cybersecurity protection

THINGS YOU CAN DO CONT'D

- Make sure policies, procedures and training are in place for security and privacy
- When security or privacy incidents occur ensure reviews are completed
- Use privacy impact assessments to support projects & initiatives
- Create standardized reporting/ record-keeping of privacy and security incidents

OTHER HOT TOPICS

Law Society
of Saskatchewan

EMAIL HACKING ALERT

- Email accounts being compromised by hackers
- Minimum IT requirements to access coverage
  - Weekly backups of data, stored offsite, and tested at least annually.
  - Installation of critical patches, anti-virus software, and anti-spyware must be made within two weeks of release.
  - Installation and maintenance, and active monitoring within reasonable business practices, of firewalls and endpoint protection.

VIDEO CONFERENCING

- Due diligence on service provider
- Contract/ terms of service
- Practical tips
  - Strong passwords and two-factor authentications
  - Confidential User IDs
  - Host approval of guests
  - Protect calls with passwords
  - Download from trusted sources

WIRE FRAUD

- Confirm who you are dealing with
- Implement safeguards
- Limit employees' authority
- Watch for anomalies
- Educate employees
- Get insurance
- Act quickly
- Get the right help at the right time

Q&A

Law Society
of Saskatchewan

RESOURCES

- Law Society of Saskatchewan COVID-19 Updates
  - https://www.lawsociety.sk.ca/covid-19-updates/
- Canadian Centre for Cyber Security
  - https://cyber.gc.ca/
- Office of the Privacy Commissioner of Canada
  - https://www.priv.gc.ca
- Canadian Lawyer, Words of Caution for Lawyers Using Zoom
  - https://www.canadianlawyermag.com/news/opinion/words-of-caution-for-lawyers-using-zoom/328737

Thank You

- Nathan Schissel
  - T: (306) 347-8476
  - nschissel@mltaikins.com

- Kristél Kriel
  - T: (306) 347-8614
  - kkriel@mltaikins.com