WEBINAR

CYBER SECURITY AND PRIVACY RISKS IN A REMOTE WORK ENVIRONMENT

BRENT J ARNOLD | CINDY KOU | CHRISTOPHER OATES

GWLG, APRIL 9, 2020

GOWLING WLG

LEGAL DISCLAIMER

- The presentation today is not intended as legal advice.
- Because this is a high level overview, it is impossible to cover all relevant details, and your available rights and remedies will depend on the unique facts of each situation, your applicable contract or subcontract, or the nature of your project.
- For specific advice, please contact your qualified legal counsel before making any decisions or taking any action. This is of particular importance as every province and territory has its own legal regime.
- As you know, the situation is extremely fluid and is changing on a daily basis. As things evolve, your best course of action could also evolve. Please follow up to date and reliable sources for your information.

AGENDA

Topic	Speaker
Cyber Security Risks	Brent Arnold
Privacy and Regulatory Issues	Christopher Oates
Commercial Contract Considerations For Privacy And Data Security	Cindy Kou
Questions?	

REMOTE WORK CYBER RISKS

- **Existing Risks Exacerbated by Remote Work**
- **Intensification of Cyber Attacks**
- **Risks Caused by Departure from Internal Controls**

EXISTING RISKS EXACERBATED BY REMOTE WORK

- **Loss / theft of hardware containing corporate data, e.g.:**
  - Leaving laptops in cabs
  - Dropping USB keys
- **Carelessness around communications**
  - Cell / Zoom calls around other people
  - Client documents / emails left in view of others
  - Use of videoconferencing platforms without proper controls in place around recording, access

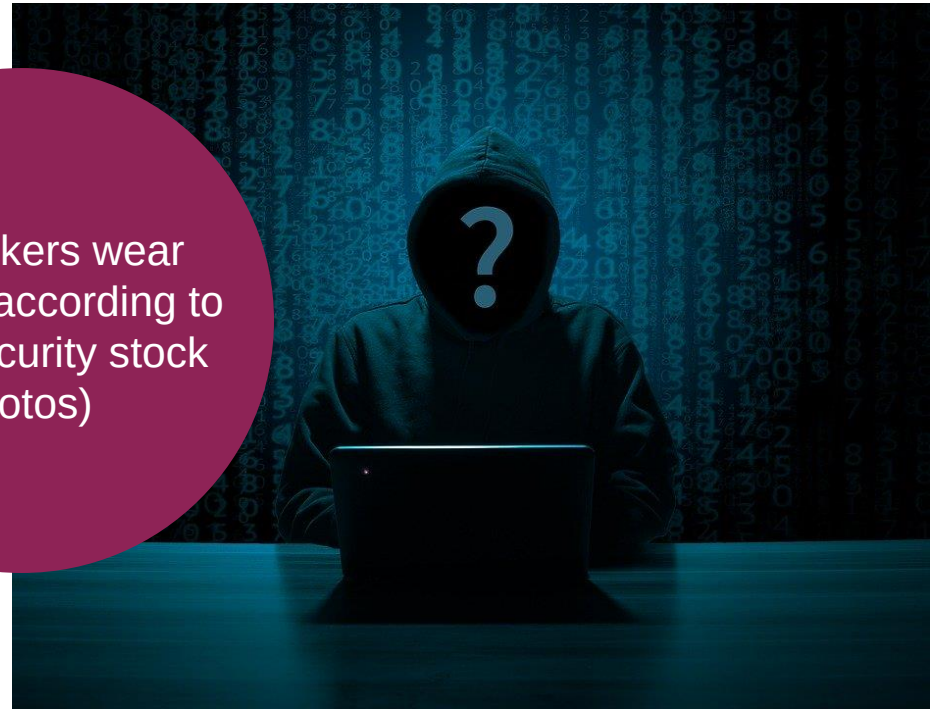
EXISTING RISKS EXACERBATED BY REMOTE WORK

- **Bring-your-own (or, now, use-your-own device)**
  - Employees forced to use of own computers / tablets / phones that operate outside the company's security umbrella
  - Or, other employees *electing* to use own devices to work around inconvenience posed by remote use of office-issued equipment
  - These devices *may* be operating without virus protection, firewalls, login access controls
- **Unsecure wi-fi**
  - More of a risk in post-social distancing period when employees may able to work in coffee shops, libraries, etc., or as people become overconfident and begin to "bend" the distancing rules
  - Wi-fi "pineapples"

INTENSIFICATION OF CYBER ATTACKS

- **Dramatic increase in cyber attacks during pandemic**
- **Hackers exploiting:**
  - Employee panic over COVID-19
  - Lack of cyber sophistication of employees unused to working from home
  - Lack of employee training and enterprise controls

(All hackers wear hoodies, according to cyber security stock photos)



GOWLING WLG

INTENSIFICATION OF CYBER ATTACKS

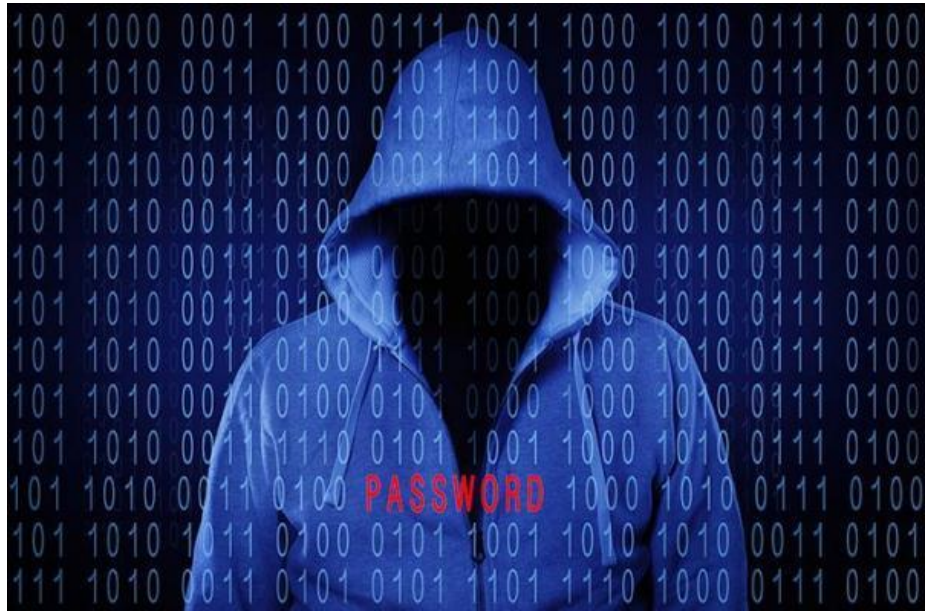
- **Scope:**
  - Cybersecurity provider Kaspersky has reported a spike in South Africa in devices affected by cyber-attacks, from the norm of under **30,000 daily to 310,000** on 18 March
  - **71% of security professionals reported an increase in security threats or attacks since the beginning of the Coronavirus outbreak.** The leading threat cited was phishing attempts (cited by 55% or respondents), followed by malicious websites claiming to offer information or advice about the pandemic (32%), followed by increases in malware (28%) and ransomware (19%).*
  - SANS: The **number of source IP addresses attackers used** to scan the internet for RDP **increased by about 30%** during March, from an average of **2,600 attacking IP addresses to around 3,540** each day in March

Source: GlobeNewswire, https://www.globenewswire.com/news-release/2020/04/07/2012660/0/en/Increase-in-Remote-Working-and-Coronavirus-Related-Threats-Creating-Perfect-Storm-of-Security-Challenges-for-Organizations-New-Survey-Finds.html

GOWLING WLG

INTENSIFICATION OF CYBER ATTACKS

- **Types:**
  - Fake COVID-19 info maps that download malware to user devices
  - Phishing emails purporting to be from legitimate organizations (including the World Health Organization and the Center for Disease Control) promising critical COVID-19 updates but installing malware or ransomware
  - Fake web conferencing meeting links that install malware
  - Exploitation of publicly known vulnerabilities in hastily deployed VPNs and other remote working tools and software



GOWLING WLG

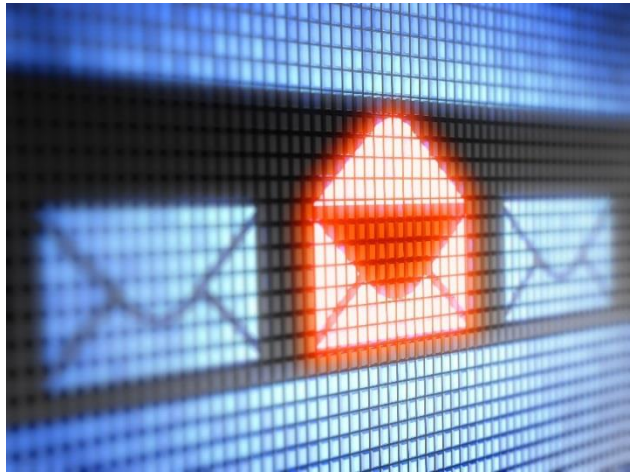
RISKS CAUSED BY DEPARTURE FROM INTERNAL CONTROLS

- **Execs, managers working remotely disrupts existing financial and other internal controls premised on in-office presence**
- **Example:**
  - “Wet” signatures required to authorize payments / transfers
  - In-person confirmation of instructions
  - Telephone confirmation of instructions where people are harder to reach / not reachable at office phones
  - Email confirmation problematic in light of greater risk of phishing attacks / compromise of corporate email systems from working remotely

PRIVACY BREACHES

- **The Commissioner has provided key steps when responding to a breach:**

1. Detect the breach
2. Contain the breach
3. Evaluate the risk
    - What information was affected?
    - What was the cause of the breach?
    - What was the extent of the breach?
    - Foreseeable harm?
4. Notifying the individuals, the Commissioner, and third parties that may reduce the risk of harm
5. Develop a plan to prevent further breaches



BREACH NOTIFICATION

- **PIPEDA requires notification for where a breach of security safeguards creates a "real risk of significant harm" to an individual. Whether there is a "real risk" of "significant harm" must be determined considering:**
  - The sensitivity of the information involved
  - The probability the information has been or will be misused
- **"Significant Harm" will include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.**

BREACH NOTIFICATION

If there is a real risk of significant harm to an individual, notification will need to be given to:

1. the affected individuals,
2. the Commissioner, and
3. any other organizations or government institutions that may be able to reduce the risk to the affected individuals

BREACH RECORDS

PIPEDA also requires organizations retain a record of all security breaches that involve personal information. Even in the absence of a real risk of significant harm.

- **Date and nature of the breach,**
- **Circumstances of the breach,**
- **Information involved, and**
- **Risk assessment leading to decision whether to notify.**

Facilitates Commissioner oversight.

RECOMMENDATIONS

- **Ensure employees are aware of *and following* corporate policies around device use and data security**
- **If you don’t have policies, now is a good time to start**
- **Make sure your incident response plan is up to date and capable of implementation without having to recall employees to the office**
- **If it isn’t capable of remote implementation, update it**
- **If you don’t have an incident response plan, now is the time**

RECOMMENDATIONS

- **Remind employees of their cyber risk and data protection training**
- **If you haven't trained employees—not just execs and people used to working remotely—on cyber risk and data protection, now is the time to source and implement training**
- **Monitor transactions closely and ensure any approved "workarounds" to adapt instruction / transaction authentication procedures for remote work still allow for proper authentication of instructions**

RECOMMENDATIONS

- Partitioning to keep corporate information separate from personal information
- Limited retention- for example, allowing personal devices to access corporate information, but not store it
- Limiting access, for example, permitting only low sensitivity information to be processed on personal devices
- Encryption of devices, limited which devices are permitted
- Up to date anti-virus software and patches
- Appropriate user authentication

PRIVACY LAW

- **Yes- it still applies.**
- **Yes- CASL also continues to apply.**
- **No- there is no COVID-19 specific exception or relaxation of its requirements.**
- **In particular:**
  - Consent is required to collect, use, or disclose information.
  - The standards for adequate security have not relaxed.

PRIVACY COMPLIANCE RISKS

- **Requests from business partners for employee health information,**
- **Increased collection of information by business that continue to operate, (e.g. screening),**
- **Relaxed or weakened security:**
  - Increased use of personal devices
  - Accessing or processing information in shared living spaces
- **Are your COVID-19 emails “Commercial”?**

PRIVACY COMPLIANCE

- **Remember:**
  - Consent to collect, use and disclose personal information remains the standard under PIPEDA,
  - Consent must be for clearly disclosed purposes,
  - Organizations must limit their collection and retention of personal information to that necessary for their disclosed purposes

COMMISSIONER GUIDANCE

The Federal Privacy Commissioner, and the Commissioners in several provinces, have issued guidance on Privacy in the context of the COVID-19 outbreak.

Themes:

- **The laws continue to apply**
- **Existing statutory exceptions allow use or disclosure of personal information without consent- but these are prescribed and limited.**

COMMISSIONER GUIDANCE

PIPEDA allows the collection, use, or disclosure of personal information without consent only in specific situations listed in the statute.

The exceptions are limited and specific.

Broadly, personal information may only be collected, used, or disclosed where a "reasonable person would consider it appropriate in the circumstances".

This applies separately from the requirement for consent- and exception to the need for consent does not allow actions that are inherently inappropriate.

COMMISSIONER GUIDANCE

Consent Exceptions:

- **Collection in the interests of the individual, and consent cannot be obtained in a timely manner**
  - e.g. a person is critically ill
- **The collection and use is to make a disclosure required by law, or is to a government authority that has lawful authority to require disclosure, and the information is for law enforcement**
  - e.g. a public health authority has required the disclosure; police acting under a warrant or exigent circumstances

COMMISSIONER GUIDANCE

Consent Exceptions:

- **The organization chooses to disclose information it believes is related to a breach of the laws of Canada or a province**
  - e.g. a federal or provincial quarantine order
- **Where use or disclosure is to respond to an emergency that threatens the life, health of security of an individual.**
  - e.g. an individual required urgent medical assistance

COMMISSIONER GUIDANCE

Organizations should be cautious in relying on consent exceptions.

Generally, they should be able to clearly identify, communicate and justify their basis for doing so.

The reliance on an exceptions must be limited to that information needed to achieve the purposes for which the exception is relied on.

RECOMMENDATIONS

- Equip employees with enterprise-owned and protected devices, to the extent possible
- Use VPN (and make sure it's safe)
- Encourage employees to properly protect their own devices (and don't let them uses devices that aren't protected)
- Allow for remote updates / patching (to ensure vulnerabilities don't increase over the duration of the remote work period)
- Reduce use of paper to reduce accidental loss of data in hardcopy (not all data breaches are *cyber* breaches)
- Make sure employees are *only* working from home and, to the extent possible, observing "clean desk" (or "clean kitchen table") policies unless they live alone

1: WHO IS ENTERING INTO THE CONTRACT?

- **Contracts entered into through your normal contracting flow**
- **Remember - click throughs and acceptances through use are still considered binding**

2: WHAT DATA IS BEING COLLECTED, USED, OR DISCLOSED?

- **The contract should be very clear on how information and data move between the parties**
  - Intellectual Property vs Confidential Information vs Personal Information
- **Reminders:**
  - Personal information generally includes any factual or subjective information, recorded or not, about an identifiable individual
    - Ex: age, name, credit card number, opinions, evaluations, comments, employee files, credit records
  - If there is any personal information, that information should always remain confidential

2: WHAT DATA IS BEING COLLECTED, USED, OR DISCLOSED?

- **Examples of some key questions:**
  1. What is the flow of information?
  2. Who is collecting and sharing what information? Who owns or has the rights to the information shared or generated under the contract?
  3. If there is PII, where are the end users located?
  4. Who is allowed to use what information, and for what purposes?
  5. Who is allowed to disclose what information, and for what purposes?
  6. Where will the information be stored? Is that location allowed to change?
  7. What third parties (including contractors and affiliates) will have access to the information?
  8. What should happen to the information after the contract ends?

3: WHAT OBLIGATIONS APPLY TO THE COLLECTION, USE, OR DISCLOSURE OF THAT DATA?

- **Applicable laws, including PIPEDA and CASL**
- **Regulatory obligations**
- **Corporate policy**
- **Industry standards**
- **Existing contractual obligations with third party contracts**
- **Applicable end-user-facing privacy policies and terms of use (these may need to be updated)**

4: WHAT OBLIGATIONS APPLY IN THE EVENT OF A BREACH?

- Immediate response to the breach
- Notification of the breach and cooperation
- Insurance
- Indemnification and defense
- Mitigation
- Root Cause Analysis
- Resolution

5: I'VE ALREADY ENTERED INTO THE CONTRACT. NOW WHAT?

- **Identify the universe**
  1. Pull copies of your contracts
  2. Allow employees, contractors, subcontractors proactively disclose contracts that may have been entered into via click throughs or deemed acceptance through use
- **Review your contract terms**
  1. Can you live with the terms?
  2. Can you terminate or amend the contract?
  3. Can you restrict your the use of the technology?
- **Consider policies and processes moving forward**

QUESTIONS?

GOWLING WLG

CONTACTS

BRENT J. ARNOLD

Partner

brent.arnold@gowlingwlg.com

+1 416 369 4662

CHRISTOPHER OATES

Partner

chris.oates@gowlingwlg.com

+1 416 369 7333

CINDY KOU

Associate

cindy.kou@gowlingwlg.com

+1 416 862 5738

GOWLING WLG