CYBERSECURITY 2021 – THREATSCAPE & PROTECTING YOUR INTERNAL BUSINESS CLIENT

BRENT ARNOLD, HENRY HARRIS

January 21st, 2021

GOWLING WLG

GET YOUR CPD / CLE CREDITS

- **For all registrants seeking California MCLE credit please visit this link (https://www.ivyevents.com/allhands/webinar_login.php?segment_code=210114GOW01) within 15 minutes before the start of the webinar. The linked page contains a form including fields for entering name, California bar number, email address, and electronic signature.**
- **Please note: MCLE credit for viewing the recording will be available only when it is viewed on the All Hands Meeting CLE server**

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
Cyber Risk: The 2021 Threatscape
The Increasing Complexity of Compliance
Anatomy of a Cyber Breach and Response
Law Firms: Protecting Clients' Crown Jewels
In-House Counsel: Protecting Your Internal Client
Questions?

CYBER RISK: THE 2021 THREATSCAPE

- **2020, only more so…**
  - Continued—for some, permanent—remote deployment
  - Vastly increased threat surface
  - New and improved attack vectors

CYBER RISK: THE 2021 THREATSCAPE

- **Continuation, possibly expansion of remote deployment**
  - Millions were remote-deployed during the pandemic; mass vaccinations will take months
  - Companies and professional firms have discovered efficiencies in remote deployment
    - Employees remain unexpectedly productive
    - decreased overhead, e.g. potential for reduced rent and associated costs
  - World Economic Forum—survey of 1,200 CIOs worldwide (from cross-section of industries):*
    - 48.6% of study respondents report *increase* in productivity since remote deployment
    - Number of *permanent* remote workers expected to ***double in 2021***—increase **from 16.4% to 34.4%**

*Source: World Economic Forum, https://www.weforum.org/agenda/2020/10/permanent-remote-workers-pandemic-coronavirus-covid-19-work-home

GOWLING WLG

CYBER RISK: THE 2021 THREATSCAPE

- **Vastly expanded threat surface**
  - **Remote workers = less supervision and control over device use**
    - More company devices in the field with less oversight
    - Risk due to hastily installed VPN and other remote access solutions
  - **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

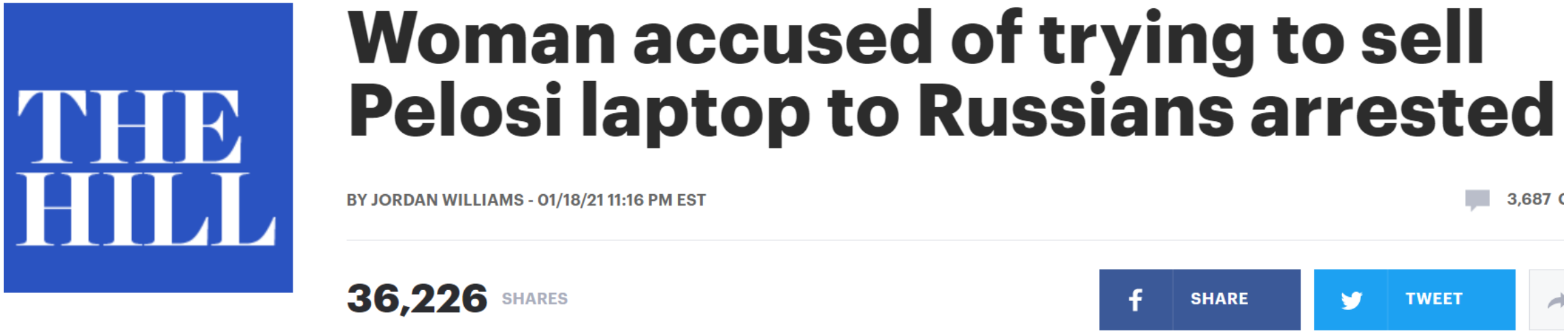
CYBER RISK: THE 2021 THREATSCAPE

- **Vastly expanded threat surface**
  - **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

CYBER RISK: THE 2021 THREATSCAPE

GOWLING WLG

CYBER RISK: THE 2021 THREATSCAPE



GOWLING WLG

CYBER RISK: THE 2021 THREATSCAPE

- There will be huge security impacts in the coming year from the move to work from home (WFH) fueled by COVID-19. More attacks will occur on home computers and networks, with bad actors even using home offices as criminal hubs by taking advantage of unpatched systems and architecture weaknesses.
- The rush to cloud-everything will cause many security holes, challenges, misconfigurations and outages.
- More growth in the security industry. Our numbers of new products and new year mergers and acquisitions will cause network complexity issues and integration problems and overwhelm cyber teams.
- Privacy will be a mess, with user revolts, new laws, confusion and self-regulation failing.

Source: Government Technology, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-21-security-predictions-for-2021.html

CYBER RISK: THE 2021 THREATSCAPE

- Identity and multi-factor authentication (MFA) will take center stage as passwords (finally) start to go away in a tipping-point year.
- Tons of high-profile Internet of Thing (IoT) hacks, some which will make headline news.
- Ransomware will get worse and worse — with new twists, data stealing prior to encryption, malware packaging with other threats and very specific targeting of organizations.
- Lots of 5G vulnerabilities will become headline news as the technology grows.

Source: Government Technology, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-21-security-predictions-for-2021.html

GOWLING WLG

CYBER RISK: THE 2021 THREATSCAPE

- Advanced Persistent Threats (APT) attacks will be widely available from criminal networks. The dark web will allow criminals to buy access into more sensitive corporate networks.
- Mobile devices, including smartphones, will be attacked in new ways, including app stores.
- Cryptocurrencies will play new roles, with criminals switching often for hiding advantages.
- As digital transformation projects grow, many plans will implode as security challenges mount.

Source: Government Technology, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-21-security-predictions-for-2021.html

GOWLING WLG

CYBER RISK: THE 2021 THREATSCAPE

- Ransomware gangs develop new tactics to force payment
- New ways to exploit remote workers
- Close co-operation between cyber criminals (e.g. some of the largest botnet operators and ransomware authors are now collaborating)

Source: Broadcom (Symantec), https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-2021-cyber-security-predictions-looking-toward-future

GOWLING WLG

CYBER RISK: THE 2021 THREATSCAPE

- Supply chain backdoor techniques to proliferate
- Hacking the home to hack the office
- Attacks on cloud platforms become highly mechanized and handcrafted
- New mobile payment scams
- QR code abuse
- Social networks as workplace attack vectors

Source: McAfee, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/2021-threat-predictions-report/

GOWLING WLG

CYBER RISK: THE 2021 THREATSCAPE

SECURITY

- Increased social engineering attacks
- Exposure of known and unknown internet-facing vulnerabilities
- Exploitation of system administration tools
- Lack of instrumentation and monitoring of critical systems
- Human-operated ransomware on the rise

Source: Security, https://www.securitymagazine.com/articles/94343-five-cyber-threats-to-watch-in-2021

GOWLING WLG

THE INCREASING COMPLEXITY OF COMPLIANCE

- **New cases:**
  - *California Consumer Privacy Act* (*CCPA*) came into effect January 1, 2020
  - Retroactive effect
  - First wave of adjudicated cases arising from breaches of *CCPA* privacy guidelines, and attempts to stretch the application of the law and of the private right to sue
- **New laws:**
  - Expect copycat *CCPA*-style legislation in other states
  - International Association of Privacy Professionals believes the Biden administration may move to implement a comprehensive federal privacy law*

*Source: IAPP, https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation/

ANATOMY OF A CYBER BREACH AND RESPONSE

1. **Stop the bleeding**
   - Identify nature of breach and contain
   - Contact:
     - Insurer (if you have cyber coverage), breach coach / legal
     - Data forensics
     - Public relations
2. **Investigate**
   - Identify source / cause of breach
   - Preserve evidence
   - Who's affected?
   - Determine potential exposure
3. **Notifications & message management**
   - Is there a "real risk of significant harm"
   - Notify affected parties & report to privacy commissioner(s)
4. **Remediation**
   - Look after the people affected
   - Plug holes in your cyber security

ANATOMY OF A CYBER BREACH AND RESPONSE

- **Don’t forget about contractual notification obligations:**
  - Client may have reporting obligations pursuant to contracts with key clients / customers, lenders, and vendors (e.g. payments vendor)
  - These may be more stringent—i.e. requiring notification regardless of whether a breach merits notifying the regulator, under applicable law—and have shorter deadlines than applicable privacy statutes
  - Consult contractual obligations to identify reporting obligations (hopefully, already tracked by client)

ANATOMY OF A CYBER BREACH AND RESPONSE

- **Lessons learned and continuous improvement**
  - Remediate security deficiencies identified by forensic investigator
  - Document changes / improvements made
  - Update incident response plan and policies as required
  - Key is to be able to show courts and regulators recognition of deficiencies in breach preparedness, responsible attitude toward affected parties, and proactive improvement of security posture

LAW FIRMS: PROTECTING CLIENTS' CROWN JEWELS

- Global law firm—over 4,000 lawyers
- June 27, 2017: global law firm DLA Piper hit by NotPetya ransomware attack
- Attack began in Firm's Ukraine office, where an employee clicked on a phishing email
- Firm shut down worldwide in 20 min. Took a week to resume operations
- Financial loss estimated to be in the millions

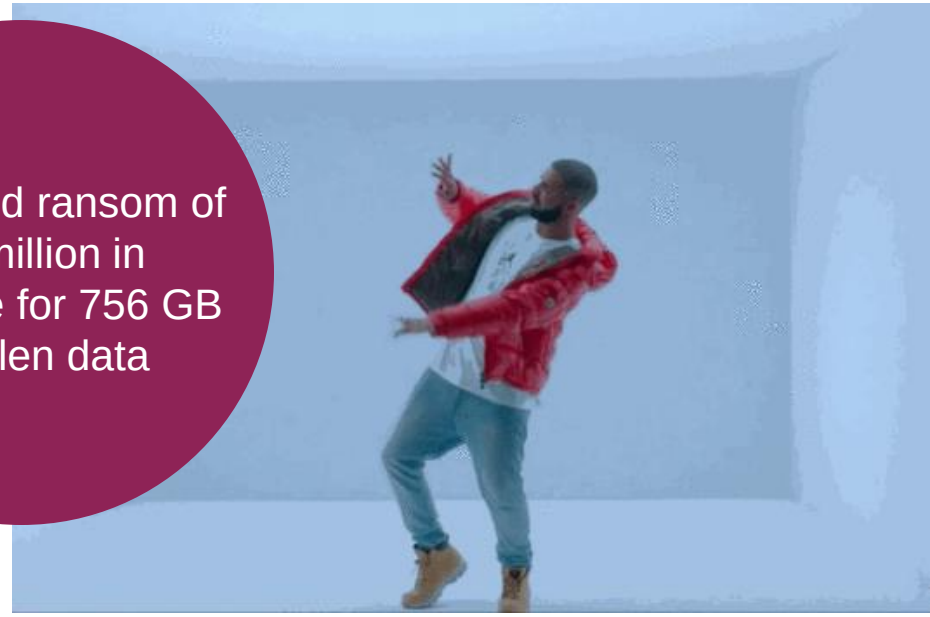
GOWLING WLG

LAW FIRMS: PROTECTING CLIENTS' CROWN JEWELS

Grubman Shire Meiselas & Sacks

- NY entertainment firm representing Drake, Lady Gaga and Bruce Springsteen
- Hackers used REvil ransomware to exfitrate and lock files
- Leaked contracts, telephone numbers, email IDs, and solicitor-client privileged communications, to show they were serious about the ransom

Demanded ransom of $42 million in exchange for 756 GB of stolen data



GOWLING WLG

LAW FIRMS: PROTECTING CLIENTS' CROWN JEWELS

- **Improving law firms' cybersecurity posture:***

1. Increase cyber awareness
2. Improve security awareness and culture
3. Increase security budget
4. Encrypt data
5. Practice secure file sharing
6. Use two-factor authentication
7. Invest in intelligent IT systems

*Sources: TitanFile, https://www.titanfile.com/blog/improve-law-firm-cybersecurity-and-privacy/; The National Law Review, https://www.natlawreview.com/article/3-cyberattacks-and-3-practical-measures-lawyers-can-take-to-protect-themselves

GOWLING WLG

IN-HOUSE COUNSEL: PROTECTING YOUR INTERNAL CLIENT

- Ensure employees are aware of *and following* corporate policies around device use and data security
- If you don’t have policies, now is the time
- 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

IN-HOUSE COUNSEL: PROTECTING YOUR INTERNAL CLIENT

- 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
- Continue to monitor transactions closely and ensure any approved "workarounds" to adapt instruction / transaction authentication procedures for remote work still allow for proper authentication of instructions

IN-HOUSE COUNSEL: PROTECTING YOUR INTERNAL CLIENT

- 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

IN-HOUSE COUNSEL: PROTECTING YOUR INTERNAL CLIENT

- 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

QUESTIONS?

GOWLING WLG

CONTACT

BRENT J. ARNOLD

Partner, Advocacy

Technology Sub-Group Leader (Com Lit)

T +1 416 347 2737
brent.arnold@gowlingwlg.com

Education

Osgoode Hall Law School (York University) J.D., 2005
Queens' University, M.A. 1999
York University, BA (Hons) (*summa cum laude*) 1994

Year of Call

Ontario Canada 2006

Brent J. Arnold is a partner practising in the Toronto office of Gowling WLG's Advocacy department, specializing in commercial litigation, data breach coaching and response, and data breach class action defence.

Brent is Vice Chair of the Steering Committee for the Cybersecurity and Data Privacy section of the U.S.-based Defence Research Institute (DRI), and sits on the executive of the Ontario Bar Association's Privacy and Access to Information Law Committee. He is corporate secretary for the Canadian chapter of the Internet Society, a global organization devoted to improving the affordability, accessibility, fairness and security of the internet.

Brent currently serves as a member of the court-appointed joint E-Hearings Task Force, whose mandate is to facilitate the modernization and re-opening of Ontario courts in the wake of the COVID-19 crisis.

GOWLING WLG

CONTACT

HENRY A. HARRIS

Partner

T +1 416-862-4393
henry.harris@gowlingwlg.com

Education

Western University, BA in Finance and Economics,
Osgoode Hall Law School, LLB, 1993
Certificate in Mining Law, Osgoode Hall PD, 2013

Year of Call

Ontario, 1995

Henry Harris is a business law partner in the Toronto office of Gowling WLG, practising in the areas of corporate finance and M&A, as well as private equity and venture capital. He regularly acts on Canada/U.S. cross-border and international transactions.

Henry represents a number of tech and e-commerce companies in the Silicon Valley/San Francisco Bay Area, and serves as Leader of the California Regional Team for the firm's US Sales Desk. In that role, he is responsible for enhancing our business dealings with clients, organizations and law firms in California and across the US.

Frequently serving in an outside general counsel role for his client base, Henry has developed innovating alternative service models for clients, such as the Virtual General Counsel and Global Coordinating Counsel service offerings. He has also served clients in managing the defence of class actions relating to consumer protection and e-commerce in various Canadian jurisdictions.

Over the past several years, he has also participated as a speaker at numerous business and legal seminars held across Canada, the United States and internationally.

GOWLING WLG

GOWLING WLG