Potter Anderson Corroon LLP

YOUR DELAWARE ADVANTAGE

Threats to Data: Legal Compliance Challenges at the Intersection of Privacy and Security

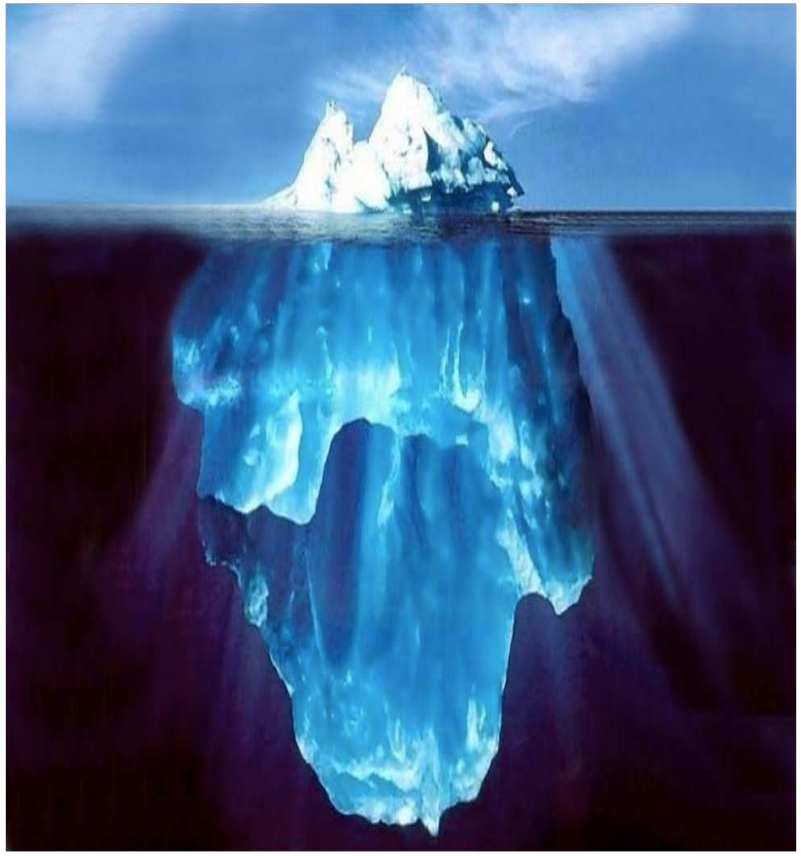
William Denny

Secure Delaware Workshop

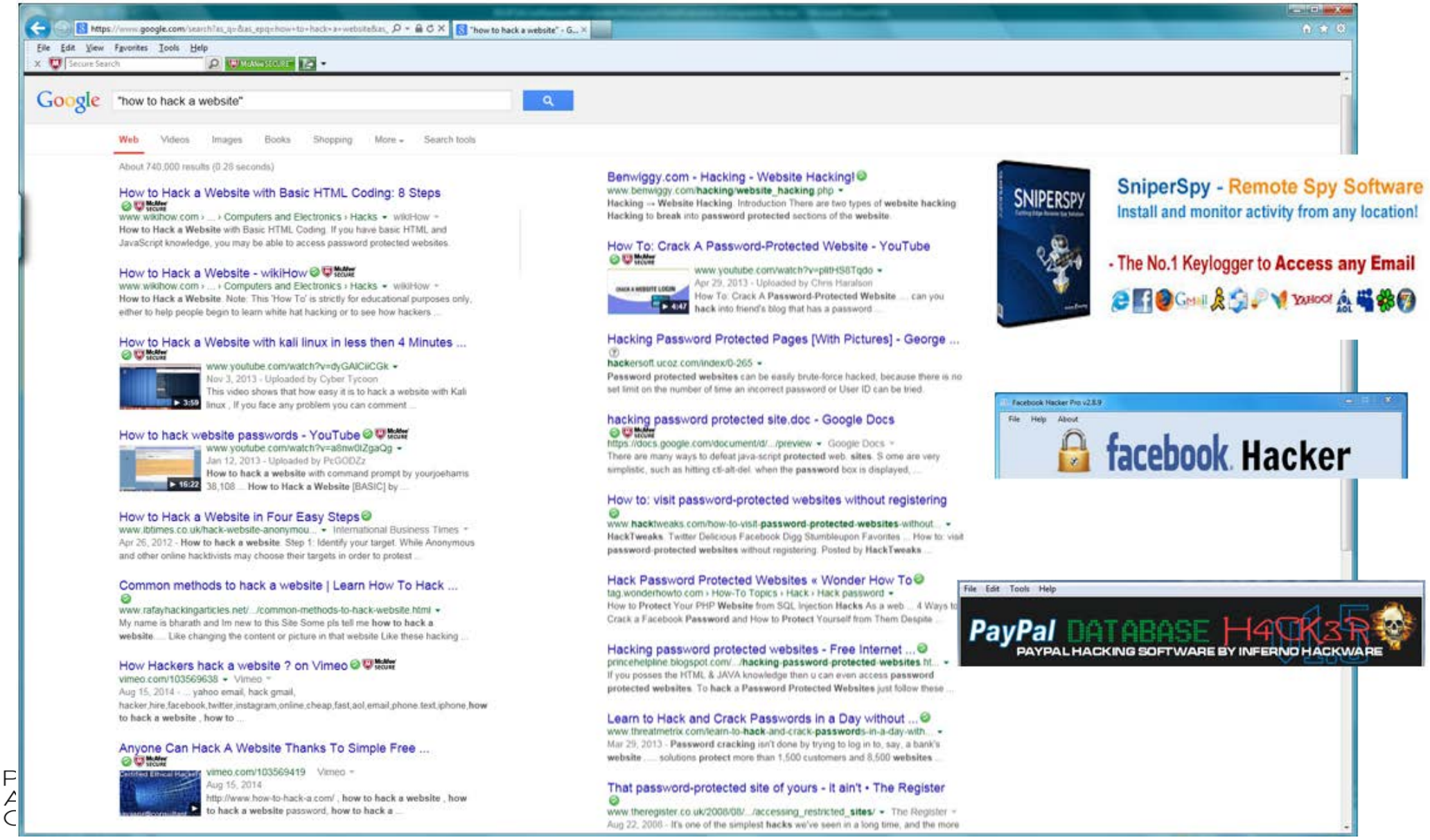
September 24, 2019

Common Cyber Incidents

- Espionage & surveillance
- Business email compromise
- Ransomware
- Formjacking
- Cryptojacking
- Credential stuffing attack
- Misconfigured devices
- Disinformation campaigns
- Negligent or malicious insiders



Why Are There So Many Data Breaches?



Data Security Breaches Dominate the Headlines

- First Half of 2019: 3,813 incidents publicly reported
  - Up 54% compared to same period in 2018
  - Number of exposed records up 52% to 4.1 billion
- 53% of firms reported at least one cyberattack
  - Only 11% of firms qualified as experts based on preparedness and response
  - Down from 26% in last year's survey
- 69% of breaches perpetrated by outsiders, most by email compromise

Ransomware

- One of the top cyber threats
  - Attacks increased 105% in first quarter 2019 compared to same period in 2018
  - 92 state, county and local governments hit in 2019 (including Baltimore, Atlanta)
  - Financial damage expected to exceed $11 billion in 2019
- Easy crime to commit
  - Limited risk of prosecution
  - Attackers pricing at level businesses are willing to pay
- Best ways to defend against ransomware
  - Train employees never to click suspicious links
  - Update and patch software
  - Restrict user permissions to install and run software
  - Back up data regularly and store on separate device offline

Attacks through Vendors

Action Item: Examine your Vendor Relationships

- Assess your vendor risk
- Conduct due diligence on new vendors
- Negotiate contracts / review existing contracts
  - Data privacy and security obligations
  - Data security audits and certifications
- How do you manage?
  - Standardize common responses by solution/offering
  - Create security/privacy descriptions share with clients
  - Comply with industry-recognized standards
  - Use standard contract terms where possible
  - Develop parameters for handling different contract terms

Credential Stuffing Attacks

- Attackers use previously stolen addresses and passwords, coupled with automated tools, to attempt millions of log-ins to a consumer-facing website.
- Costs as little as $550, criminals can earn at least 20x profit.
- Websites vulnerable because users re-use passwords.

- Basic Safeguards
  - Use multi-factor authentication
  - Check logs to see if there are massive, failed log-in attempts
  - Limit login attempts and lock out
  - Use “Captcha” defensive tool
  - Implement mandatory password reset if you discover customer’s credentials have been stolen

Business Email Compromise

- Two variants:
  - Perpetrators purporting to be company executives use spoofed email addresses and direct company's finance personnel to make large wire transfer to third-party bank.
  - Perpetrators impersonate the victim's vendors and request that the victim initiate changes to the vendor's banking information and then make large wire transfers.
- Losses to U.S. financial institutions over $9 million since 2016.
- Prevention tips
  - Enhance payment authorization procedures and verification requirements for vendor information changes.
  - Examine account reconciliation procedures and outgoing payment notification processes to detect and stop fraudulent payments
  - Train employees about BECs and update internal policies and procedures

FTC Enforcement Actions

Privacy v. Security

- ***Data Privacy*** focuses on the use and governance of personal data, including the laws and regulations requiring companies to protect personal data.
- ***Data Security*** refers to the ways organizations protect their data: administrative, technical, and physical safeguards

"You can have security without privacy,
but you cannot have privacy without security."

Major Developments in 2019

- CCPA amendments and deadline for implementation
- New York SHIELD Act and tighter data security requirements
- Nevada Internet Privacy Law
- BIPA liability for use of facial recognition technology
- Delaware Supreme Court case on directors' fiduciary duties
- GDPR enforcement actions

CCPA and the Re-Engineering of Data Handling Practices

- Comes into force January 1, 2020.
- Applies to any for-profit business that collects data on California residents, and:
  - Annual revenue tops $25 million, or
  - Holds personal information on at least 50,000 customers, or
  - Generates at least 50% of annual revenue from selling user data.
- High fines and private causes of action for non-compliance
- In a survey conducted by PricewaterhouseCoopers, only 52% of respondents expected their companies to be compliant by January 2020.

CCPA and the Re-Engineering of Data Handling Practices

- Definition of “Personal Information” is incredibly broad.
  - “Personal Information” means information that identifies, relates to, describes, is ***reasonably capable of being associated with***, or could reasonably be linked, directly or indirectly, with ***a particular consumer or household***.”
  - **Exception**: *publicly available* or *deidentified* information
  - **Complication:** limited applicability to *employee data* for one year
- Greatest challenges to businesses:
  - Detailed recordkeeping is required going back to January 1, 2019.
  - New mandatory disclosures must be added to privacy notices.
  - New mandatory procedures are required for responding to consumer data requests.
    - Right to opt out of sale of data, require correction or deletion
    - Right to see what has been collected, to whom shared

Action Item: Update Privacy Notices

- Many organizations' privacy notices fail to meet principles outlined in GDPR, CCPA, PIPEDA
- Common Deficiencies:
  - Not understandable or clear
  - No description of which types of third parties could access user data
  - Failure to notify users if their information was sold or shared
  - Failure to hold third parties to same data sharing standards
  - No explicit language about data retention
  - No effective date
- User Access to Data
  - Explicitly state how users can access data and request its deletion

New York SHIELD Act

- Stop Hacks and Improve Electronic Data Security ("SHIELD") Act places increasing obligations on businesses that handle personal data.
  - Applies to any business that owns or licenses computerized data that includes private information of a New York resident.
  - Broadens the definition of "data breach" to include situations where data is merely *accessed* by an unauthorized person, not just situations where data is *acquired*.
- New security requirements
  - Each business must develop a *data security program* that employs administrative, technical and physical safeguards to protect the security, confidentiality and integrity of the private information.
    - Risk assessments, employee training
    - Careful selection of vendors
    - Document retention programs and network security and incident response plans

Nevada Internet Privacy Law

- Goes into effect October 1, 2019
- Applies to “operators” who (1) own or operate an internet website for commercial purposes, (2) collect and maintain covered information from Nevada consumers, and (3) purposefully direct their activities towards Nevada or consummates some transaction with a Nevada resident.
- Consumers have the right to opt-out of the sale of their covered information.
  - Operators must establish a procedure to allow consumers to opt out of the sale of their data.
  - Operators must respond to requests and honor consumers’ directives within a time table prescribed by the law.

BIPA Liability for Use of Facial Recognition Technology

- Illinois' unique Biometric Information Privacy Act requires businesses to:
  - Inform individual that his or her biometric information is being collected or stored;
  - Inform individual of the purpose of the collect, storage or use and timing of retention;
  - Receive a ***written release*** from the individual to collect the information.
- Illinois Supreme Court in *Six Flags* lawsuit ruled that aggrieved persons **did not** need to allege injury to have standing to sue.
  - Illinois has the only biometric privacy law with a private right of action.
  - Other states, such as Texas and California, also restrict use of biometric information.
- Critical safeguards:
  - Secure your biometric data
  - Know your applicable state law restrictions
  - Get consent

Personal Liability of Corporate Directors for Failure to Ensure Proper Oversight of Risk

- Directors of Delaware corporations owe fiduciary duties to the corporation and all stockholders:
  - Duty of Care, *and*
  - Duty of Loyalty (including a duty to act in good faith)
- Fiduciary duties give rise to oversight obligations
  - Make sure policies and procedures are in place to ensure that the corporation complies with applicable regulatory, legal, and financial requirements
- *Marchand v. Barnhill*, Delaware Supreme Court (June 19, 2019)
  - Directors breached duties of loyalty by failing to make good faith efforts to ensure that company's regulatory compliance programs were adequate.
  - Reasoning applies directly to cybersecurity risk.

Director Oversight: Practical Guidance

- Understand applicable laws, regulations and guidance
- Ensure that an organizational risk assessment has been conducted and understand company's cyber risks
- Ensure organization has and implements robust cybersecurity and privacy policies tailored to risk profile
- Build compliance into governance structure
- Require cybersecurity updates as part of agenda at board meetings
- Ensure organization has adequate incident response plan and that it is updated and practiced

Director Oversight: Practical Guidance

- Ensure effective controls and procedures to make accurate and timely disclosures relating to cybersecurity
- Ensure employee training on cyber risk, data protection policies and identification of red flags
- Conduct risk assessment of third party vendors
- Review insurance coverage for cyber-related incidents

GDPR Enforcement Actions

- Ponemon Institute Study in 2019 showed:
  - 50% of respondents experienced at least one personal data breach that was required to be reported under the GDPR
  - 25% of respondents ranked their readiness and confidence to respond to a GDPR data breach as *very low!*
  - Only 18% of organizations were highly confident in their ability to communicate a reportable data breach within 72 hours.
  - Only 1/3 of companies had cyber risk insurance and only 43% of those had coverage for GDPR fines
- Polish Data Protection Office fined an organization $700,000 for not appropriately protecting data of about 35,000 people collected from installment loan applications.
- Fines for collecting *publicly available data* without notifying data subjects.

Action Item: COPPA Compliance

- Determine what information is being collected in connection with content directed at children
- Re-evaluate criteria for designating content as “child-directed” in light of FTC enforcement action
- Ensure you are not inadvertently collecting personal information through third-party platforms
- Confirm that data collection practices of third-party service providers are compliant
- Make changes to production practices so content posted on YouTube will be less likely to be considered targeted to children

Tips for Updating your Cybersecurity Program

1. Identify the Personal Information you are holding.
2. Prepare incident response plan and conduct tabletop exercises.
3. Use clear, consistent language in your data security policies.
4. Regularly download and install software updates.
5. Segregate your system's databases and networks.
6. Commit adequate resources.
7. Encrypt sensitive data
8. Regularly change passwords
9. Insulate sensitive data and network locations from public access points.
10. Suspend inactive accounts after termination or lack of use.
11. Provide training.
12. Evaluate and improve vendor management.

Resources

- Delaware Attorney General's Consumer Protection Unit https://attorneygeneral.delaware.gov/fraud/cpu/securitybreachnotification/
- Delaware Small Business Development Center - Datassured https://delawaresbdc.org/special-programs/data-assured/
- FTC Protecting Small Businesses https://www.ftc.gov/tips-advice/business-center/small-businesses
- U.S. Small Business Administration - Cybersecurity https://www.sba.gov/managing-business/cybersecurity
- Small Business Development Center http://www.sbdcnet.org/small-business-cybersecurity/cybersecurity-resources-small-business
- Department of Homeland Security https://www.dhs.gov/publication/stopthinkconnect-small-business-resources
- Federal Communications Commission Cybersecurity for Small Business https://www.fcc.gov/general/cybersecurity-small-business

To Contact Us

William R. Denny
Direct dial: (302) 984-6039
wdenny@potteranderson.com

Potter Anderson & Corroon LLP
1313 North Market Street
P.O. Box 951
Wilmington, DE 19899-0951
www.potteranderson.com

Presenter: William R. Denny

- Partner and Chair of the Cybersecurity, Privacy and Data Governance Practice at Potter Anderson & Corroon LLP
- Certified Information Privacy Professional (CIPP/US) and Certified Information Privacy Manager (CIPM) by the International Association of Privacy Professionals
- Member of the ABA Cyber Security Legal Task Force
- Licensed in Delaware