THE JOURNEY TO INFORMATION SECURITY

Martin J. McLaughlin
414-298-8219
MMcLaughlin@reinhartlaw.com

Paloma A. Kennedy
414-298-8344
PKennedy@reinhartlaw.com

Reinhart Boerner Van Deuren s.c.
1000 North Water Street, Suite 1700, Milwaukee, WI 53202
www.reinhartlaw.com

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Agenda

- Managing cybersecurity
  - C-suite oversight
  - Determine what data needs to be protected
  - Assess and manage risk
- Practical steps to increase your security profile
  - Develop plans and policies
  - Implement Reasonable Security
  - Prepare for breach
  - Manage vendor/customer contracts
  - Evaluate cyber coverage
  - Educate
- The emerging legal landscape
  - Laws governing data privacy and security

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Managing Cybersecurity

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

C-Suite Oversight

- Do you have information security procedures, incident response plan, information security policy, crisis management team? Are they embracing best practices?
  - Factors that reduce the cost of a breach:
    - Formation and testing of incident response team
    - Use of encryption
    - Business continuity management
  - Automation technologies [Cost of Data Breach Report, Ponemon Institute, 2019]
- Does your management team review and approve top-level policies on privacy and IT security risks?
- Does your management team review and approve annual budgets for privacy and IT security programs?
- Security training
- Exposure to and education concerning budgets and risks related to data security

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

What "Data" Must be Protected?

- PII: Typically, state laws define personally identifiable information (PII) as an individual's first name or initial with last name, and one or more of the following (unencrypted) data elements:
  - Social Security number
  - Driver's license number or state or military identification card number
  - Financial account, credit card or debit card number, in combination with any required security code, access code or password that permits access to an individual's account
- However, some states define PII more broadly to include:
  - Medical information
  - Health insurance information
  - A user name or e-mail address, in combination with a password or a security question and answer that permits access to an online or financial account or resource
  - Credit or debit card number without security information
  - Biometric information (such as fingerprints or facial measurements)
- Other confidential information
  - Intellectual property, trade secrets and other proprietary information
  - Third-party confidential information

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Know Your Data

- Know your data:
  - What kind(s) do you collect?
  - Why is it collected?
  - Where is it stored and for how long?
  - Who has access (and who *should* have access)?
  - How is it used?
  - How is it secured?
- Consider the entire life cycle of data and risks associated with each step
  - Data collection, use, sharing, transfers and destruction
- Analyze each division/department's specific cybersecurity requirements by considering:
- Review, assess policies and practices for data:
  - Collection, storage, use, disclosure, protection, destruction
  - Consent for collection
- Scale down
  - Collect only what you need
  - Restrict access
  - Keep only as long as you need it

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Assess and Manage Risk

Steps to Take

- Know your data
- Know your vulnerabilities
- Develop and revise plans and policies
- Consider established frameworks as a roadmap
- Testing

Guidelines to Remember

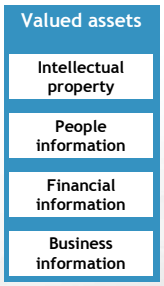
- Security is a journey, not a destination
- Consider role of attorney-client privilege
- Continuous quality improvement is key

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

What Are the Risks to Your Business?

- Business e-mail compromise—targets executives
- Wire transfers (*e.g.*, banks, intercompany transfers, title companies, deal closings, payments to foreign vendors)
- Access to financial systems to execute unauthorized financial transactions
- Denial of service/ransomware
- Theft of trade secrets, intellectual property, and sensitive business information (such as customer lists or product pricing) that can be monetized
- VPN usage
  - Fortinet bug (usernames and passwords of active users) [*VPN users: If you're on Fortinet, Palo Alto, Pulse Secure, patch now, warns spy agency*, ZDNet]



© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Know Your Vulnerabilities

- Employees
- Third-party service providers
  - (*e.g.*, cloud service providers, payroll, plan administrators, etc.)
- Physical environment
  - Firewalls, network infrastructure, Wi-Fi
  - Outward facing interfaces (webpages, portals, etc.)
  - Endpoints (desktops, laptops, printers, cell phones)

[*Scoring Methodology*, Aug. 2017 SecurityScorecard]

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Practical Steps to Increase Your Security Profile

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Develop Plans and Policies

- Develop a proactive, not reactive, information security plan and team—an equal balance of individuals yelling “Fire!” and telling everyone to calm down
- Unless you have an underdeveloped program, avoid hyper-focus on operational aspects of InfoSec
- Know and minimize your attack surface
- Establish a baseline
- Enforce record retention and destruction policies

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Essential Policies and Procedures

- General information security policy
- Privacy policy
- Privacy notices
- Incident response plan
- Mobile device management
- Bring your own device policy
- Updated employee handbook
- Acceptable use policy
- Business continuity policy
- User agreements
- Website terms and conditions
- Disaster recovery policy

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Implement Reasonable Security

- States are requiring that Companies implement reasonable administrative, physical and technical safeguards
- In the event of a breach, regulators want to know what security procedures were in place
- Consider adhering to established cybersecurity framework
  - **COBIT**: Best practices for governance and control processes for information systems and technology, one aspect of which is the control of information system and technology risk
  - **HIPAA**: Provides a series of security standards and implementation specifications
  - **ISO**: International, ISO/IEC 27001 and 27002 provide a comprehensive baseline set of controls that can be implemented by any type of organization; healthcare-specific considerations are addressed in ISO/IEC 27799 (Expensive)
  - **NIST**: Intended for federal agencies, the NIST SP 800-53 controls, and supporting 800-series publications provide, a comprehensive information security risk management framework; healthcare-specific considerations are addressed in NIST SP 800-66 (the bell cow among the frameworks)
  - **PCI**: Intended for payment card information, but scope sufficiently comprehensive to provide a reasonable baseline for the protection of any type of sensitive information
  - **HITRUST**: Formed specifically to support the healthcare industry
  - **Center for Internet Security Critical Security Controls**: Designed to automate the implementation, enforcement and monitoring of security controls

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Best Practices for Testing

Consider retaining an outside consultant to perform tests of your systems

- Vulnerability scanning
- Spear phishing
- Penetration testing

Internal exercises you can perform

- Tabletop exercises
- Phishing tests

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Pop Quiz!

How much longer does it take to crack a 12-character password drawn from upper case and lower case letters including numbers and symbols versus one with just six lower case letters?

a. 62 times longer
b. 62,000 times longer
c. 62 million times longer
d. 62 trillion times longer

[Chris Kornelis, "Test Your Knowledge of Passwords," *Wall Street Journal*, Sept. 18, 2019]

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Answer: D

It would take a computer 62 trillion times longer to run through all the 12-character possibilities than it would for a password of only 6 lowercase letters.

[Chris Kornelis, "Test Your Knowledge of Passwords," *Wall Street Journal*, Sept. 18, 2019]

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Recommendations

Network

- Encryption
- Intrusion detection/ prevention
- Data loss prevention software
- Locked-down firewalls
- Penetration testing
- Desktop modeling
- Patching moving to cloud

User

- Password protocols
  - No reuse
  - 14-character minimum
- Multi-factor authentication
- Mobile device management
- Skills-based user education (*e.g.*, Barracuda PhishLine, LLC)
- Social media monitoring
- Limited access
- Restricting applications

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Prepare for a Breach

- Are you prepared for a breach?
- How and where are your backups?
- Do you have cyber coverage?

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

How Data Breaches Occur

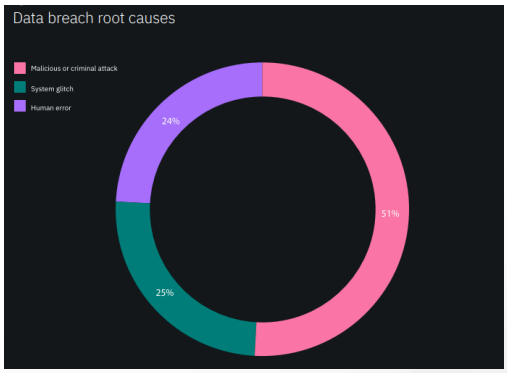
1. Malicious Internet attacker/APT
2. User error
3. Loss/theft of device
4. Disgruntled employee
5. Third-party mistake
6. Network intrusion

[Cost of Data Breach Report, Ponemon Institute, 2019]

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

How Data Breaches Occur (cont.)



It takes substantially longer to identify and contain a breach for a malicious attack (approximately 314 days), which is why these types of breaches are 27% more costly than those caused by human error ($4.45 MM vs. $3.5 MM). [Cost of Data Breach Report, Ponemon Institute, 2019]

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

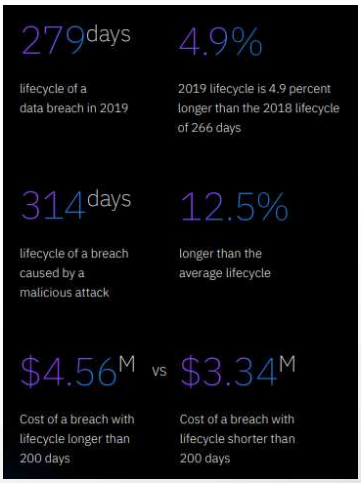
Being attacked is unavoidable, so how prepared are you?
Can you answer "yes" to these six key questions?

1. Do you know what you have that others may want?
2. Do you know how your business plans could make these assets more vulnerable?
3. Do you understand how these assets could be accessed or disrupted?
4. Would you know an attack is occurring and whether your assets are compromised?
5. Do you have a plan to react to an attack and minimize the harm inflicted?
6. Do you have independent control backup?

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Lifecycle Data Breach Findings



[Cost of Data Breach Report, Ponemon Institute, 2019]

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Cost of a Breach

Data security breaches are major risk areas for businesses. A business that suffers a data breach incident or reportable event may incur significant expenses, including costs relating to:

- Investigating and containing the breach
- Hiring third-party investigators
- Notifying affected individuals if the breach affects individuals' PII
- Determining whether existing insurance policies cover the breach
- Government fines and private lawsuits
- Reputational damage, lost customers, and lost business
- Potential lawsuits
- Contract liability and fees (Payment Card Industry fees)

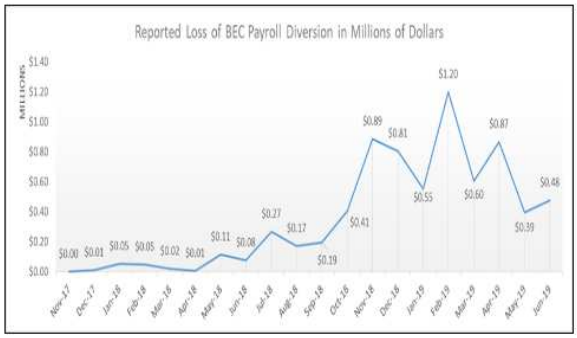
© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Business E-Mail Compromise

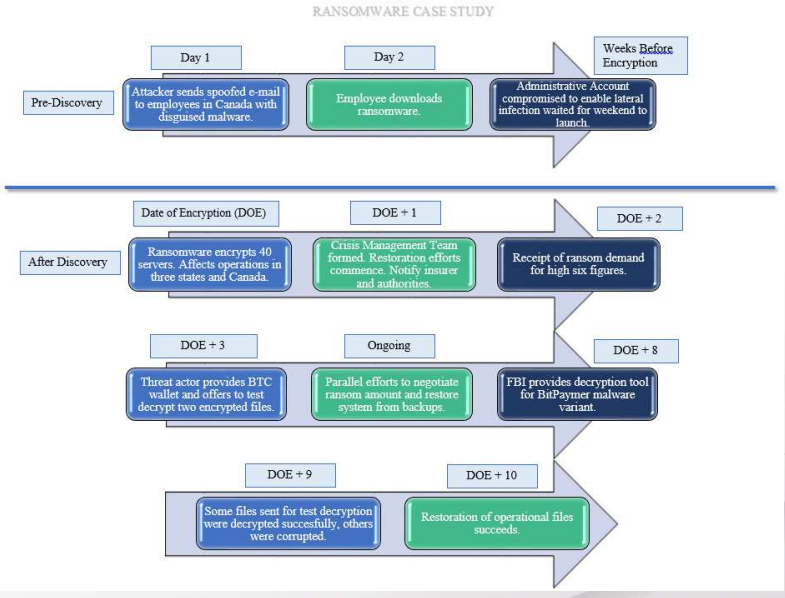
- Total U.S. victims: 69,384
- Total U.S. exposed dollars lost: $10 B
- Total victim dollar loss: $3.5 B
- Payroll diversion

[Public Service Announcement, September 10, 2019, Federal Bureau of Investigation]



© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law



© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Best Practices for Cyber Liability Insurance

- Review your policy and understand exactly what is covered
- Check endorsements and coverage limitations (some policies limit coverage for social engineering hacks)
- Review the policy with your information security team
- Does it cover hosted service providers failures?
- Does it only cover external breaches? Internal?
- Does it cover credit card expenses?
- What are the exceptions?

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Vendor Management

- Identify the third parties your organization relies on to collect, access, process, disclose, transmit, or host sensitive or confidential data (payroll processors, cloud service providers, plan administrators, etc.)
- Vendor due diligence is a must
- Require service providers by contract to implement appropriate security measures to protect against unauthorized access
- With increasing frequency, clients are seeking security representations and warranties in agreements
- Consider risk-based approach to managing vendor security agreements/contract standards
- Implement vendor oversight and contract enforcement
- Maintain vendor contact information and ensure key vendors are represented and included as part of incident response team

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Vendor Management (cont.)

Review contracts with vendors that collect, provide, access, use, store, disclose, or otherwise process PII

- Do your vendors have resources to indemnify?
- Do your vendors have cyber liability insurance coverage? Do you have coverage?
- Data breach clause essential:
  - ✓ Indemnification provisions
  - ✓ Notification process and timing
  - ✓ Cooperation during investigation
  - ✓ Who notifies affected parties?
  - ✓ Who pays for notice?
  - ✓ Clear delineation of responsibility
  - ✓ Limitation of liability (double-edged sword)
  - ✓ Confidentiality
- Monitor continually

A source impacted by the ransomware tells ZDNet that the two companies opted to pay the ransom demand. The Digital Dental Record and PerCSoft have been sharing a decrypter with impacted dental offices since Monday, helping companies recover encrypted files.

The recovery process has been slow, as most ransomware recovery operations tend to be, with some dental offices claiming on a Facebook group that the decrypter either didn't work, or didn't recover all their data.

[Ransomware hits hundreds of dentist offices in the US, ZDNet]

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

CEO Scams

- https://www.youtube.com/watch?v=_oqXcx3bRD8

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Educate

- Education and training is key
  - Employee education upon hire, at least annually thereafter, notice of updates to procedures
  - Document
- Update employee handbook and policies
  - Keep information confidential
  - Assignment of intellectual property
  - Fair use for work and technology
- Well-understood and publicized reporting procedures essential
- Resources:
  - Anti-phishing.org
  - Phishme.com

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Emerging Legal Landscapes

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Laws Governing Data

- State data breach and privacy laws
- New York Financial Services Regulation (23NYCRR 500)
- Fair Credit Reporting Act
- Gramm-Leach-Bliley Act (GLBA)
- Financial institutions
- Children's Online Privacy Protection Act (COPPA)
- Health Information Portability and Accountability Act (HIPAA)
  - PHI: Protected Health Information
- California Consumer Privacy Act (CCPA)
- Foreign Laws: General Data Protection Regulation (GDPR); APEC Privacy Framework; China's data security law

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Wisconsin Privacy Laws

- "Personal Information" means an individual's last name and first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:
  1. The individual's social security number
  2. The individual's driver's license number or state identification number
  3. The number of the individual's financial account number (*i.e.*, credit or debit card number)
  4. The individual's deoxyribonucleic acid profile
  5. The individual's biometric data

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Illinois Biometric Information Privacy Act

- Entities must obtain written consent from consumers prior to collecting any biometric information, such as fingerprints, voiceprints, or scans of hand or face geometry
- Good faith compliance = best practices:
  - Implement information security policies and procedures
  - Prepare and regularly review incident response policies and procedures
  - Review contracts involving the use or disclosure of personal information
  - Educate employees

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

The CCPA

- Who must comply?
- Am I doing business in California?
  - Headquartered in California
  - Employees are in California
  - Business is required to qualify in California as a foreign entity AND/OR
  - Repeated sales into California
- What happens if I don't comply?

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

The CCPA (cont.)

- "Personal information" is "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly" with a particular household
- Includes:
  - Identifiers (legal name, postal address, etc.)
  - Commercial information (purchase history)
  - Biometric information
  - Internet activity (browsing history, search history, etc.)
  - Geolocation data
  - Education information
  - Professional and employment information
  - Audio, electronic, visual, thermal, olfactory or similar information

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Consumer Rights Under the CCPA

- Right to receive notice at or before collection
- Right to request personal info be deleted
- Right to prohibit the sale of personal information
- Right to request a digital copy of information to be transferred to another entity
- Right to receive equal service and price

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Questions?

Thank You!

This presentation provides information of a general nature. None of the information contained herein is intended as legal advice or opinion relative to specific matters, facts, situations or issues. Additional facts and information or future developments may affect the subjects addressed in this presentation. You should consult with a lawyer about your particular circumstances before acting on any of this information because it may not be applicable to you or your situation.

© 2019 All Rights Reserved
Reinhart Boerner Van Deuren s.c.
42532141
Reinhart
Boerner Van Deuren s.c. Attorneys at Law