Keeping Biohealth Data Secure

March 2017

EY Building a better working world

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Agenda

1. Cyber Threat Landscape
2. Managing Cybersecurity Risk—Key Concepts
3. The Path Forward—"Real World" Considerations

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

The Threat

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

Your facilitators

Heather L. Fields
Shareholder
Healthcare, Data Privacy & Security
Reinhart Boerner Van Deuren
hfields@reinhartlaw.com

Justin Webb
Attorney
Litigation, Data Privacy & Security
Reinhart Boerner Van Deuren
jwebb@reinhartlaw.com

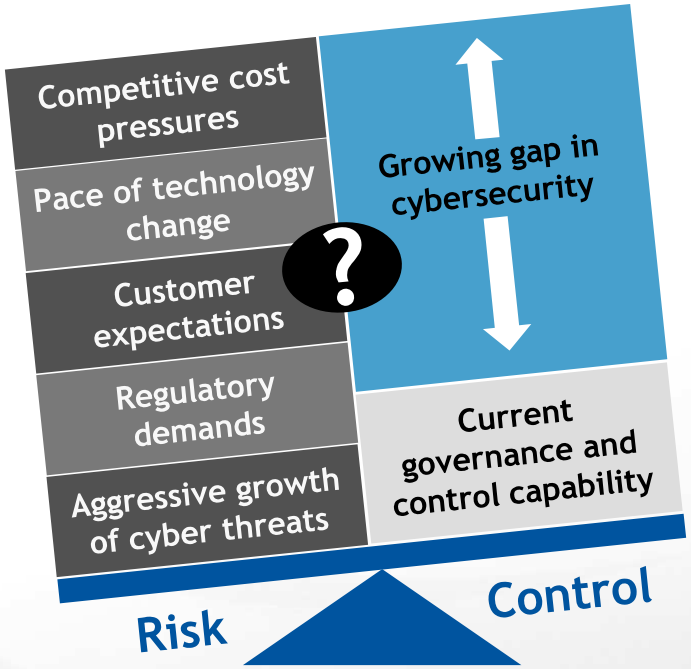
David Shade
Partner
Ernst & Young LLP
david.shade@ey.com

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

Cyber Threat Landscape

A variety of concerns affecting the marketplace



87%

Number of board members and C-level executives who said they lack confidence in their companies' level of cybersecurity[1]

The stark reality[2]

- 89% of breaches had a financial or espionage motive
- 82% took less than a day
- Less than 20% are discovered by the intended target

[1] *EY's 19th Global Information Security Survey 2016-17.*

[2] *2016 Verizon Data Breach Investigations Report.*

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

Cyber Threat Landscape

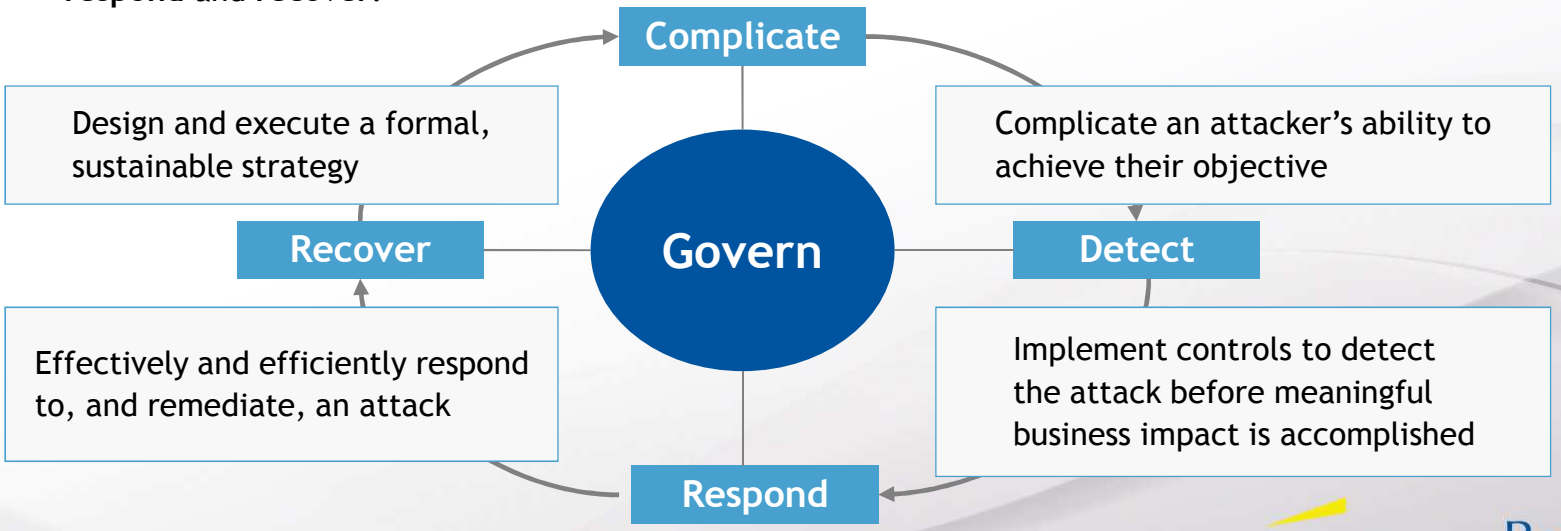
What are the potential risks to your business?

- Theft of research and clinical trial data that can be monetized or used to perpetrate financial fraud, blackmail and corporate espionage
- Access to sensitive data to facilitate market manipulation:
  - Contract bids
  - M&A activity
  - Succession plans
  - Financial forecasts
  - Business plans
- Access to financial systems to execute unauthorized financial transactions (e.g., SWIFT – Society for Worldwide Interbank Financial Telecommunication)
- Manipulation of automated processes:
  - Modification of programming to industrial control systems, robotic systems, etc.
  - Modification of business rules utilized in processing (e.g., calculations, interfaces, detection and monitoring thresholds)

Managing Cybersecurity Risk – Key Concepts

The 'new normal' for cyber security

- It is no longer feasible to effectively prevent cyber attacks from occurring, especially those initiated by a sophisticated attacker.
- Since absolute prevention is not feasible, companies must move to a posture of **preparedness** and **timely response,** or as we have advocated, an approach that focuses on four main tenets – **complicate**, **detect**, **respond** and **recover**.



EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

The Path Forward….

Pragmatic guidance to combating cyber threats

Focus on real risks … it is more than legal compliance

Protect the information … not the infrastructure

Governance matters … aligned and enterprise focused

Plan and be intentional … nibble your way to success

Less about the big things … master the little things

EY Building a better working world

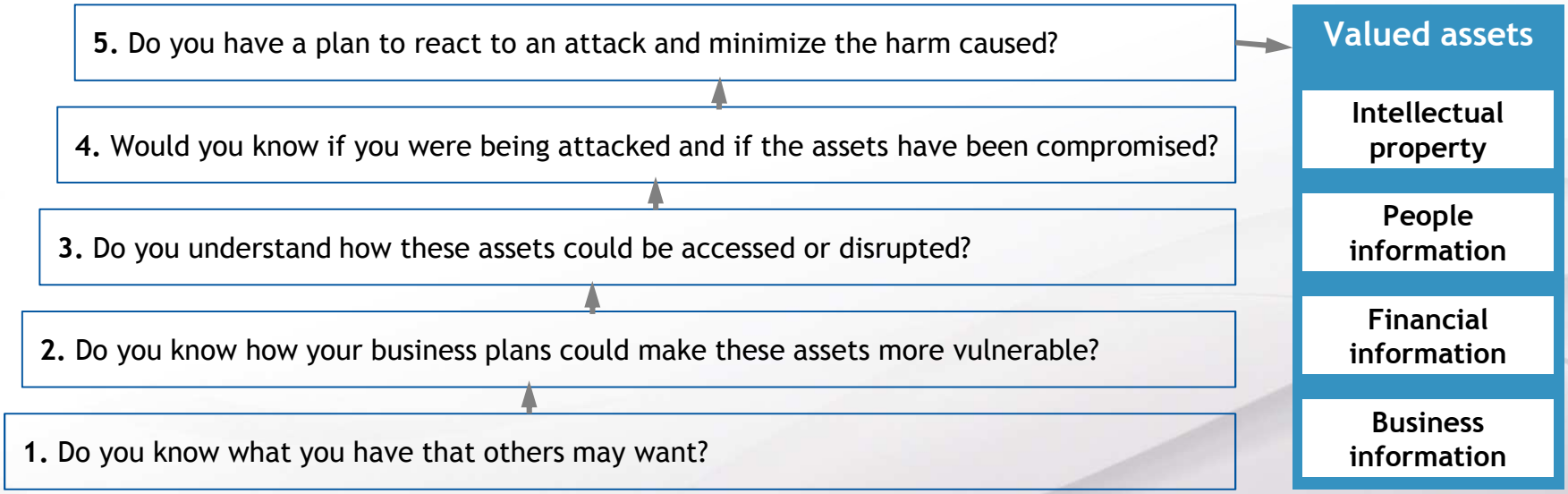
Reinhart Boerner Van Deuren s.c. Attorneys at Law

The Path Forward....

Protect the information

Being attacked is unavoidable, so how prepared are you?

Can you answer "yes" to these five key questions?



EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

The Path Forward….

Protect the information

- 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:
  - Type and sensitivity of data handled or managed
  - Applicable laws and standards
  - Contractual commitments and internal policies and procedures
  - Internal capabilities
  - Flexibility needed with data security measures
- Cost/Benefit assessments

The Path Forward….

Governance Matters - Security is an Enterprise Risk

- Security risk management must be part of existing organizational governance, leadership and operational structures
  - Governance: board, compliance committee, operational committees
  - Leadership: general counsel, CEO, CIO/CTO, CFO, COO, CISO, compliance officer, risk manager
  - Operational Divisions/Departments: finance, billing, purchasing, HR, PR/communications, gov't relations, clinical research, medical staff, CIN/ACO, payroll

Allocation of cybersecurity risk management activities: a point of view

Function (stakeholder)	Risk management for cybersecurity risks		
	Govern (ongoing)	**Respond** (incident and breach)	**Contain** (damages and liabilities)
Board of directors and audit committee	▪ Set standard of due care ▪ Periodically evaluate cybersecurity risk governance and review annual cybersecurity risk assessment ▪ Oversee management's cybersecurity risk disclosures per US Securities and Exchange Commission (SEC) guidance	▪ Monitor breach notifications and governance processes and updates	▪ Re-evaluate cybersecurity risk governance oversight ▪ Re-evaluate standard of due care ▪ Re-evaluate cybersecurity risk disclosures
Executive management	▪ Identify critical assets ▪ Prepare cyber risk assessment ▪ Prepare incident response plan ▪ Prepare cybersecurity risk disclosures per SEC guidance	▪ Categorize and assess incidents	▪ Develop short-term and long-term remedial actions
Risk management (e.g., Chief Risk Officer)	▪ Define and oversee ongoing cybersecurity risk management program	▪ Monitor breach and cybersecurity risk trends and measure risk management execution	▪ Evaluate effectiveness of cybersecurity breach response and technology risk management

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

Allocation of cybersecurity risk management activities: a point of view

Function (stakeholder)	Risk management for cybersecurity risks		
	Govern (ongoing)	**Respond** (incident and breach)	**Contain** (damages and liabilities)
Legal (e.g., general counsel)	▪ Develop cybersecurity risk legal response strategy ▪ Approve cybersecurity breach response program	▪ Execute breach communications plan ▪ Execute authority and regulator response plan	▪ Perform cybersecurity risk liability control (long-lived)
Information security (including incident response team) (e.g., CISO)	▪ Build threat mitigation program to plan and protect most critical assets ▪ Establish incident, investigation and forensics response programs and conduct tests	▪ Detect and respond to incident ▪ Execute investigation plans, including incident forensics	▪ Assess effectiveness of cybersecurity incident response ▪ Execute incident remediation plan and assess effectiveness

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

The Path Forward….

The variety of laws impacting cybersecurity

- **Must Comply With …**
  - HIPAA Security Rule and Related Guidance from OCR
  - Payment Card Industry Data Security Standards (PCI DSS)
  - 21 CFR Part 11
  - Applicable State Law
- **Highly Recommend …**
  - NIST Special Publication, 800-53 and other related NIST documents
  - NIST "Framework for Improving Critical Infrastructure"
  - FDA Guidance regarding Cybersecurity and Medical Devices
- **Review and Consider ...**
  - DOJ Cybersecurity Unit Best Practices for Victim Response and Reporting of Cyber Incidents
  - FTC Data Breach Response – A Guide for Business

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

The Path Forward….

Less about technology … more about the task

Cybersecurity Frameworks:

- **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
- **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
- **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

The Path Forward….

Less about technology … more about the task

Cyber Liability Coverage:

- Periodically review for adequate coverage as risks evolve and change
  - Evaluate coverage based on actual (and desired) level of risk exposure
  - Negotiate coverage to fit your specific needs
    - Insurance standards are not yet set for cyber liability which gives more negotiation power to policy holders
- Understand your coverage
  - Note exclusion clauses that eliminate coverage for specific events
  - Evaluate scope of coverage to determine which networks and control systems are covered

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

The Path Forward….

Less about technology … more about the task

Cyber Liability Insurance (cont.):

- Coverage options to consider:
  - Event Response Services
  - Business Interruption Expenses; Dependent Business Interruptions
  - Network Security Liability
  - Data Restoration/Digital Assets
  - Network Extortion
  - Coverage for intentional acts by employees or insiders
- Evaluate various layers of coverage
- Ensure broker knowledgeable and individual preparing applications has working knowledge of current security program and controls

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

The Path Forward….

Less about technology … more about the task

Vendor Contracting:

- Contracting parties should consider seeking additional protections for PHI beyond HIPAA's requirements
- Security provisions should be based on the on the parties' business relationship and extent of use and disclosure of PHI
- Scope of services may merit separate data security agreement (e.g., hosting services)
- BUT, contractual protections do not equate to a vendor management program

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

The Path Forward….

Less about technology … more about the task

Vendor Management:

- Identify your organization's full scope of dependencies on third-party service providers or vendors that collect, access, process, disclose, transmit, or host sensitive or confidential data
- Develop formal privacy and data security vendor management processes, such as:
  - Vendor due diligence process
  - Vendor oversight and contract enforcement
  - Maintain vendor contact information and ensure key vendors are represented and included as part of incident response team

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law

The Path Forward….

Less about technology … more about the task

Vendor Management (cont.):

- Ideally, management of contracts involving or affecting sensitive or regulated data should be:
  - Centralized
  - Risk-based
    - Tiered approach to allocation of review resources may save expenditure of resources, however, cannot be based on "dollar value of the contract"
  - Involve a multi-disciplinary review process
    - Security team review important step – not only expertise, but also ability to spot interplay with other arrangements, products, etc.
    - Need review by attorney(s) with expertise in security

Questions?

EY Building a better working world

Reinhart Boerner Van Deuren s.c. Attorneys at Law