Vendors & Data Security:
How to Assess Your Risk & Protect Your Data

Matt Kelly
Radical Compliance
mkelly@RadicalCompliance.com

Edwin Broecker
Quarles & Brady
Ed.Broecker@quarles.com

Fernanda Beraldi
Cummins Corp.
fernanda.beraldi@cummins.com

Who are these people?

Matt Kelly, editor
Radical Compliance

Ed Broecker, partner
Quarles & Brady

Fernanda Beraldi
Cummins Inc.

Agenda

- How bad is it? A look at precarious state of vendors & data security
- Regulatory burdens: what agencies are saying about data security risk, and what they expect from companies
- Put it into practice: how Cummins manages vendors & data security risk across one whole planet
- Q&A

Part I:

Lay of the Land

Matt Kelly
Radical Compliance

Q: How bad is your exposure to cybersecurity risk through vendors, anyway?

RADICAL COMPLIANCE
SHARP THINKING ABOUT COMPLIANCE. AUDIT. AND RISK

5

A: Pretty bad

From Ponemon Institute report Sept. 2018:

- 59 pct of companies experienced breach via third parties
- 42 pct suffered breach **within the last 12 months**
- Avg. number of third parties with access to sensitive data: 583
- 57 pct can't determine whether vendor's safeguards will work as promised
- **Only 34 pct have full inventory of all vendors with whom they share sensitive data**

Source: Ponemon Institute, 'Data Risk in the Third-Party Ecosystem,' Sept. 2018

RADICAL COMPLIANCE
SHARP THINKING ABOUT COMPLIANCE. AUDIT. AND RISK

6

A: Pretty bad

Or, from Deloitte report in Feb. 2019:

- 70 pct of companies have 'moderate to high level of dependency on external entities'
- Top worry about those third parties for coming year: cybersecurity, cited by 38 percent; next was compliance at 20 percent
- (Survey of 2,300 webinar participants)

Source: Deloitte, 'Extended Enterprise Risk Management to Be Focus in 2019'

RADICAL COMPLIANCE
SHARP THINKING ABOUT COMPLIANCE. AUDIT. AND RISK

7

Q: Where are the regulators on this issue, anyway?

RADICAL COMPLIANCE
SHARP THINKING ABOUT COMPLIANCE. AUDIT. AND RISK

8

SEC tip-toes toward taking action

- April 2018: Fines Yahoo $35 mill for failing to disclose breaches
- Sept. 2018: Fines Voya Financial Advisers $1 mill for violating Red Flags Rule
- June 2019: Fines Facebook $100 mill for failing to disclose data breaches via Cambridge Analytica
- Oct. 2018: Special report on business email exploits

"Our report emphasizes that all public companies have obligations to maintain sufficient internal accounting controls and should consider cyber threats when fulfilling those obligations."

— SEC Enforcement Director Stephanie Avakian

Source: Securities & Exchange Commission Special Report, Oct. 2018

RADICAL COMPLIANCE
SHARP THINKING ABOUT COMPLIANCE. AUDIT. AND RISK

9

SEC also has some guidance

- New guidance on how to assess, disclose security risks
- What to disclose generally; what to disclose specifically
- **Closely tying disclosure risks to internal controls**
- **Escalation policies to prevent insider trading**

What the SEC doesn't say: how to assess those risks.

Source: Securities & Exchange Commission Interpretive Guidance (Feb. 2018)

RADICAL COMPLIANCE
SHARP THINKING ABOUT COMPLIANCE. AUDIT. AND RISK

10

Financial regulators worried about tech vendors

- 'Maintaining confidence in the security practices of third-party service providers has become increasingly important…'
- 'Recommend that **Congress pass legislation that grants examination and enforcement powers** … to oversee third-party service providers'
- Uneasy with small number of key providers servicing many financial firms
- Capital One breach in July: Fed examiners had been inspecting Amazon Web Services

Source: Financial Stability Oversight Council (December 2017)

RADICAL COMPLIANCE
SHARP THINKING ABOUT COMPLIANCE. AUDIT. AND RISK

11

Defense Dept. worried about tech vendors

- DFARS compliance deadline: 31 Dec. 2017
- Spoiler alert: we missed it
- Implementation of NIST 800-171:
  - Controlled, unclassified information (CUI)
  - Prime DOD contractors, pushing to sub-contractors

Source: NIST Guidance on DFARS, 800-171

RADICAL COMPLIANCE
SHARP THINKING ABOUT COMPLIANCE. AUDIT. AND RISK

12

Meanwhile, the audit firms…

'The auditor does **not** broadly evaluate the company's overall cybersecurity risk or the design and effectiveness of operational and other non-financial controls adopted by the company to mitigate that risk.'

—Kathleen Hamm, PCAOB director

- Most data breaches do **not** pose material risk to financial statements
  - Copying data, not stealing money
  - Ransomware demands = not material
  - Disruptions: new costs, not faulty financial reporting

13

Part II:

What the law & regulators require

Ed Broecker
Quarles & Brady

14

‘Cybersecurity risks pose grave threats to investors, our capital markets, and our country.’

SEC Interpretive Guidance

February 26, 2018

‘Cybersecurity is not simply a corporate concern; it is a supply chain issue.’

National Defense Industry Association White Paper

July 2018

Quarles & Brady LLP

15

Suppliers are Risky

According to a PWC report, in 2014, roughly a quarter (23%) of all cyber breaches were attributed to current service providers and contractors; 45% were attributed to past partners.

Source: PWC, Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015.

Quarles & Brady LLP

16

Most Regulation Is Industry Specific

Department of Defense- DFARS Clause 252.204-7012 (Defense contractors)

Federal Energy Regulatory Commission- Supply Chain Risk Management Reliability Standards (Power generators and transmitters)

Health & Human Services – HIPAA Security Rules (Medical professionals)

New York Department of Financial Services – Cybersecurity Regulations (Financial institutions)

Quarles & Brady LLP

17

SECURE Technology Act

- Strengthening and Enhancing Cyber-capabilities by Using Risk Exposure Technology Act (the 'SECURE Technology Act') — December 2018
- Established the Federal Acquisition Supply Chain Security Council
  - charged with steering the development of National Institute of Standards and Technology guidelines on supply chain risk management, crafting information-sharing protocols between federal and non-federal entities, establishing a lead agency to oversee the information-sharing process and looking into broadly applicable contracting solutions, such as subscription services or machine learning-enhanced analysis, that can guide procurement decisions
  - also charged with establishing procedures for and facilitate the exclusion of sources or covered articles (think ZTE, Kaspersky Labs, Huawei)

Quarles & Brady LLP

18

Other Federal Sources

Securities & Exchange Commission

- Board Guidance on Cyber Risk Management (2018)
- Guidance stresses importance of maintaining comprehensive policies related to cybersecurity risks and incidents

Federal Trade Commission

- Enforcement Actions

Quarles & Brady LLP

19

Recent FTC Data Security Enforcement Actions

Quarles & Brady LLP

20

DFARS Basics

DFARS Clause 252.204-7012: requires contractors/subcontractors to:

1. Safeguard covered defense information that is resident on or transiting through a contractors internal information system or network
2. Report cyber incidents that affect covered defense information or that affect the contractor's ability to perform requirements designated as operationally critical support
3. Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center
4. If requested, submit media and additional information for damage assessment

Quarles & Brady LLP

21

NIST SP 800-171

- As part of it obligations under the DFARS, the contractor must provide adequate security over all of its information systems
- Adequate security incorporates the protective measures of NIST SP 800-171
  - not later than Dec 31, 2017
- 'Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach'
- Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, but some may require security-related software or hardware

Quarles & Brady LLP

22

HIPAA Security Rule

- The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity
- The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information

Quarles & Brady LLP

23

Guiding Principles:

- Security must be reasonable and appropriate in light of the circumstances
- Breach doesn't necessarily = lack of reasonable security
- BUT no breach doesn't necessarily = reasonable security
- Data security is an ongoing process

Quarles & Brady LLP

24

Documentation is Critical

Behind every security compliance measure is a documentation requirement

Practically every facet of cybersecurity compliance requires that policies and procedures be created and implemented

Best practice and many regulatory bodies require flow-down of the cybersecurity obligations and certifications

Quarles & Brady LLP

25

Individualized plans

Because information and data supply chains differ across and within organizations, any information security SCRM Plan should be tailored to individual organizational contexts

Quarles & Brady LLP

26

NCSC- 13 Elements of SCRM Program

The National Counterintelligence and Security Center has articulated 13 elements to be included in an effective Supply Chain Risk Management Program (SCRM)

1. Executive level commitment
2. Communication with stakeholders – horizontal and vertical
3. Assessment of current critical assets, systems, processes and suppliers
4. Integrated risk reduction relative to critical assets, systems, processes and suppliers
5. Elevate security as a primary metric

Quarles & Brady LLP

27

NCSC Elements (cont)

6. Conduct due diligence on suppliers
7. Monitor suppliers' adherence to agreed-upon SCRM security requirements
8. Identify critical data/information about organization and customers
9. Establish processes to share information about vulnerabilities
10. Manage security risks when terminating suppliers
11. Monitor effectiveness of established risk mitigating strategies and update as necessary
12. Train employees about managing, mitigating and responding to risk
13. Plan for contingencies

Quarles & Brady LLP

28

Standards

- ISO270001/2
- NIST 800-53
- ISACA COBIT 5
- PCI-DSS
- CIS 20
- DISA
- FFIEC / GLBA / OCC / OTS
- OWASP

Why so many?

- Vary by industry & regulatory oversight
  - Defense / Government
  - Manufacturing
  - Financial Services
- Generally, standards are only a framework for controls that must be tailored to the organization.

Quarles & Brady LLP

29

Cybersecurity Maturity Model Certification

The DoD has been exploring options for validating and certifying cybersecurity compliance.

In May 2019 event, Katie Arrington, special assistant to the Assistant Secretary of Defense for Acquisition for Cyber, announced a new certification standard called the 'Cybersecurity Maturity Model Certification' (CMMC).

It's no longer acceptable to say your company is compliant; soon, you will have to prove it!

Quarles & Brady LLP

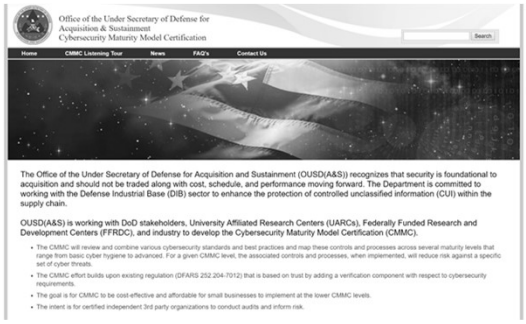
30

CMMC

Still in development

There is a website that provides additional background on the proposed CMMC, including FAQs and details about a Listening Tour that is intended to solicit feedback from key stakeholders

Version 1.0 the CMMC framework expected in January 2020 with requirement in Requests for Proposals (“RFPs”) beginning in June 2020



Quarles & Brady LLP

31

Credit Cards

- PCI DSS sets forth requirements about how to manage risks in the supply chain, whether that includes an internal process or involvement of third party service providers, merchants etc.
- PCI DSS 3.0 includes requirements like penetration testing, application development lifecycle security, and threat modeling

Quarles & Brady LLP

32

Part III:

How Cummins Inc. manages risk

Fernanda Beraldi
Cummins Inc.

33

How does Cummins identify data security concerns among its vendors?

- Not scientific method, basically identifying suppliers/partners that hold employees' or customers' data.
  - Look to Legal and Purchasing to identify these vendors and bring E&C along.
  - Use a gatekeeper process on OneSource (HR system - employee data) to identify transfers to vendors.

Fernanda's slides start here

- Work closely with Cybersecurity – vendor security assessment has questions about privacy and the type of data involved. If personal data included, they involve E&C.
- Privacy Program started in 2011 – 3 years to get the program to a point of good awareness, process and procedures around vendors handling data.
- Better with global vendors vs. local vendors, because of higher risk.
- Leveraged Safe Harbor and now Privacy Shield Certification to identify global vendors. By reviewing and identifying systems with personal data annually, we identify vendors too.

34

What does Cummins do once risk is identified?

- Once a vendor that will handle personal data is identified, it goes through a vendor security assessment with cybersecurity (very robust) and privacy questionnaire.
- Conversations with business owner to ID the specific data the vendor needs for the work. Intention: narrowing down vendor's data exposure. Also identify who at Cummins and at the vendor will have access to the data, same intention.

Fernanda's slides start here

- Training of the Purchasing Function occurs every other year, mostly due to updating of contract language. Contract language updates are typically triggered by regulations.
- One basic privacy clause in the MSA. Use several addendums attached to the MSA depending on the personal data involved.
    - If handling personal data, security and data privacy addendum.
    - If EU data, Model Clauses (2 or 3 different versions – controllers vs. processors).

35

How does Cummins monitor use of the data?

- E&C doesn't really monitor the vendors day-to-day.
- For groups that engage with vendors on long projects, as they check request additional approvals for new countries or new data fields to be included, we provide multiple checkpoints to ensure that previous approvals provided continue to be respected.

Fernanda's slides start here

- Reliance on employees who manage vendor relationships to be "eyes and ears" with their selected vendors. If something is out of control, E&C must be immediately notified.
- Data Loss Prevention program handled by CISO – emails, downloads, external drive, thumb drives. If the file involves personal data, E&C gets a call.
- General privacy training to help employees to understand issues and basic red flags.
- Best intentions for the data versus actual consequences.

36

Part IV:

Q&A: fire away!

Thank you!

Matt Kelly
Radical Compliance
mkelly@RadicalCompliance.com

Edwin Broecker
Quarles & Brady
Ed.Broecker@quarles.com

Fernanda Beraldi
Cummins Corp.
fernanda.beraldi@cummins.com