VENDOR SECURITY RISK MANAGEMENT: How to Handle the New Normal

“Some Important Lessons Learned From Both Directions”

Presented by:
Joe Filer, CISSP, PMP, CRISC

June 23, 2015

Who Is this Guy?

• BA in Math, Masters in Operations Research
• More than 20 years as an information security professional
  • Increasing levels of global security leadership with extensive compliance focus
• CISSP/CRISC – Security and Risk Experience
• PMP – Project Management Experience
• ISSA Distinguished Fellow
• Currently – VP, CISO at Harland Clarke Holdings Corp.
  • Multi-company, global footprint
• Resident of San Antonio, TX (almost 30 years)
Ground Rules

Some of the information provided will be identified as “my personal or professional opinion” and should not be considered as reflective of my employer’s position.

Any aspect of this presentation that might be considered to address legal issues reflect summaries and should not be considered legal advice.

Overview

• What Is Vendor Security Risk Management (VSRM)?
• Overview of the Key Concepts
• Perspective/Premise
• Changing Landscape and Forecasts
• Issues and Lessons Learned
• Solutions
• Conclusions
DEFINITION:

Vendor Security Risk Management

Structured approach to ensure that relevant vendor security risk postures are understood, DOCUMENTED and validated to an appropriate level.
Key Components of Effective VSRM

**Vendor Security Risk Management**

- Required confidentiality components in contracts
- Confidence that all “relevant” vendors are subjected to program’s oversight
- Approach where vendor security postures are understood, documented and validated when appropriate
- Feedback to the vendor to facilitate remediation when required
Key Concepts

Risk – potential harm that could occur from a future event
Risk Management – the process of understanding risk and determining how best to handle exposure
Compliance – meeting all the requirements of a standard
Certification – authority attesting to a level of compliance
Unique Perspective

Own vendor security risk management for
~50 CRITICAL VENDORS

MY TEAM

Support client requirements as a critical vendor to
HUNDREDS OF FINANCIAL INSTITUTIONS

P R E M I S E : As an industry, we need to recognize
the importance of doing vendor security risk
management better....

“Vendor Security Risk Management (VSRM/Due Diligence)
efforts can be very costly and may not lead to confident
visibility into the security posture of our critical vendor
relationships.”

“We have not embraced the key
lessons learned from doing VSRM for
several years.”

“There has to be a better
(cost-effective) way to meet this
important objective.”
Changing Landscapes and Forecasts

OCC Guidelines Oct 2013

- Establishes clear requirement for third-party oversight
- Emphasis on risk management and due diligence
- Considered somewhat ambiguous and subject to misinterpretation

The weaknesses associated with “payment card industry approach” will be addressed

- Expect more comprehensive requirements including vendor security management
- More stringent assessor expectations
- VISA Validation effort – Jan 2015
Changing Landscape and Forecasts

Consumers are sick of “holding the bag”
- Companies will be held accountable for security decision-making
- Too many vendors do not have a good “history”
- Class action lawsuits

Federal legislation is coming!
- Tech savvy generation in leadership influencing direction
- Lots of new regulations (See OCC 10/2013)
- Legislation has been “bubbling under the surface” for several years (See http://fas.org/sgp/crs/natsec/R42114.pdf)
- Response to consumer lack of confidence
### Issues and Lessons Learned #1

**Vendors are not your enemy! They are not trying to hide things from you and you should not fear them.**

**Lesson 1:** If we need to be “afraid” of our vendors, why have them?

- Build relationships with good partners
- Invest in good up-front vetting that starts the process on a solid footing
- There is too much focus on people trying to “pull the wool over our eyes”

### Issues and Lessons Learned #2

**The PROCESS is not more important than the objective.**

**Lesson 2:** We need to recognize the impact that this process has on our vendors and our business elements

- Excessively burdensome requirements can impact the willingness of the vendor to “participate” in the effort
- We don’t all have unlimited security budgets and “Time Is Money”
- Vendors are not impressed by fancy collection tools, overly comprehensive surveys, etc.
**Issues and Lessons Learned #3**

*Inconsistent guidance to Vendor Security Management is reflected in extraordinary document requests*

**Lesson 3:** Vendor Security Management has lost sight of the original objective – confidence with the security posture of key vendors

- Piles of documents cannot really support an effective evaluation of security posture
- Approach probably increases overall risk as many documents reflect SENSITIVE information on their own

---

**Issues and Lessons Learned #4**

*Not every “gap” is HIGH risk*

**Lesson 4:** We need to be realistic about the sensitivity we attach to risk issues

- Threat consideration is a key piece of the process
- Effective risk assessment allows for business prioritization and remediation
- Credibility with the business is at stake
Issues and Lessons Learned #5

Compliance has become a CheckBox exercise in many cases.

Lesson 5: We have lost sight of something learned long ago – “There is no such thing as One Size Fits All Security”

- PCI and “compliance versus security” failures
- The “qualitative” aspect of reviews began to erode with SOX reviews
- Risk context is very important

SOC 2 could be the best thing to happen to VSRM in some time

Lesson 6: We have to rely on comprehensive security reviews whenever possible.

- SAS70 was not the answer – not always measured to same level
- SOC 2 is a viable solution for non-validated control visibility – a good, cost-effective starting point for vendor security awareness
- Mentioned directly in OCC Guidelines as viable oversight
Solutions

Maintain the focus on **Security Risk Management**
- Keep process on target and in a “box”
- We cannot over-rotate on parts of the issue (e.g., scanning)
- Limit document exposure
- Trust but verify while keeping validation at an appropriate level

We do **NOT** need to re-invent the wheel
- Effective Vendor Security Risk Management has been going on for more than 15 years
- Success starts with clear requirements in contracts
- Understand and respect the impact on the vendor

Be **proactive** as a vendor
- “Build once, use many” documents provide efficient visibility
- Confidence goes a long way
- Stand firm when you have to
Solutions (Generally)

Focus on effective security posture NOT compliance
- Comprehensive and secure programs lead to compliance BUT not the other way around
- Recognize the importance that risk plays in the process

Document the risk management decision process
- Capture why things were (or were not) done
- Ensure the business owns/drives the risk-based decision
- Security should be a consultant in the process
- Understand and advocate for your vendors/clients/customers

Own your compliance/audit relationships
- Push them beyond the checkbox mentality
- Think quality
- And, make them add value to your awareness
Conclusions

- Vendor security risk management is an absolute requirement today and we must **DO IT RIGHT**
- Working together as **PARTNERS** is essential
- Process is an enabler not the objective
- As an industry, we have to get better at understanding and **LEVERAGING** risk management
- There is **NO SUCH THING** as “one size fits all security”
- We must address the rising **CHECKBOX MINDSET** and its impact on security/compliance
- **SOLID SECURITY PROGRAMS** reflect foundation for compliance successes – not the other way around
- We must determine some alternatives – **SOC 2 – YES!**
- Fundamental Philosophy has not changed – **EFFECTIVE SECURITY** must enable the business

Questions
For more information

Joe Filer, CISSP, PMP, CRISC
VP, Chief Information Security Officer

15955 La Cantera Parkway
San Antonio, TX  78249
210.694.1560 (office)
210.475.1920 (cell)
joseph.filer@harlandclarke.com

29