The NYS Forum, Inc.

Third Party Risk Management

John Verry, Managing Partner
john.verry@pivotpointsecurity.com
Startling Statistics

- 74% think that 3rd Parties will provide highly important or critical services in the next year
- 26% have suffered reputational damage due to a third party security incident in the last year
- 87% of organizations have been impacted by a third party security incident in the last year
Startling Statistics

• 74% think that 3rd Parties will provide highly important or critical services in the next year
• 26% have suffered reputational damage due to a third party security incident in the last year
• 87% of organizations have been impacted by a third party security incident in the last year
• Only one problem, they are not “real”, :>
Knowing Where We Are And Where We Are Going ...

1. Cost & complexity drive cloud & outsourcing
2. Evolving threat vectors result in events
3. Events result in regulations
4. Regulations drive changes in practices and the development of technology solutions (see step 1)
5. Repeat steps 1 – 4
Knowing Where We Are And Where We Are Going ...

1. Greater understanding of Third Party/Vendor Risk
   1. Including Shadow IT

2. Greater expectation of managing Third Party/Vendor Risk

3. You end up at a NYSICA event listening to me drone on ...
For Today, Two Overlapping Audiences

1. Risk Officers need to understand and analyze Third Party Risk and insure that it is being managed in accordance with the entity’s risk appetite

2. Auditors need to assess the effectiveness of the design and operation of the Third Party Risk Management Program
Tomorrow, Six+ Overlapping Participants

1. TPRM (often procurement) operates the program
2. Information Security which may/should play some role
3. Enterprise Risk Management which may/should play some role
4. Auditors which may/should play some role
5. Third Parties
   1. Vendors
   2. Other Agencies
   3. Regulators
   4. Insurers
6. Fourth Parties (Third Parties to your Third Party)
Risk Realization

**IT/Infosec**
- Confidentiality
- Integrity

**TPRM**
- Availability
- Breach

**ERM**
- Reputational Impact
- Financial
• Common Data & Risk Classification & Appetite (ERM, ISMS, TPRM)
• Internal Risks Inform Third Party Risk Consideration
• CLI Informs ISMS & TPRM
• TPRM Informs CLI Selection
• Incident Response -> Crisis
• Incident Response Plan (3rd Party Integration)
• Vendor’s TPRM
• PSPs Inform TPRM
• Your & Their BIAs Inform TPRM (DRBCP Testing?)
Risk Officers

• Normalize risk identification, analysis, and acceptable risk across
  • IT/InfoSec
  • TPRM
  • ERM
  • Impact criteria and probability are key
• Insure TPRM & Info Sec Risks inform Enterprise Risk and vice versa
Auditors

• Need to identify a suitable standard for Design audits:
  • ISO-27001/2 provides limited guidance
  • Shared Assessments VRMM is great if you are a member
  • OCC:2013:29 can be used as a framework
• Key Areas include: Governance, PSP’s, Contract, Vendor Risk (4th Party & Resilience), Skill/Expertise, Reporting, Tool Use, Ongoing Monitoring
If You Are Green - Fielding
Tidbits & Gotchas

• Prevailing “Good Practice” on TPRM (10% H, 40% M, 50% L)

• Build your program before you buy your tools
  • Capabilities, Process, Pricing, Population, and Staffing all impact choice

• Some TP Risks are more challenging to identify and/or monitor
  • Concentration risk – What if the wrong combination of suppliers use AWS, a particular ISP, or Florida?
  • Geographic risk – Does your supplier move data geographically for BC? Are the wrong combinations of vendors subject to political/geographic turmoil?

• TP Exit Strategy is critical
  • Address time-frames, data “recovery,” and transition support
  • Include T&Cs that trigger Exit (breach, business conditions, etc.)
Questions & Additional Help

• [https://sharedassessments.org/](https://sharedassessments.org/)
  • Packaged VRM (SIG, AUP, VRMMM)
  • Certified Third Party Risk Professional Certification

John Verry
Pivot Point Security
888.PIVOTPOINT
john.verry@pivotpointsecurity.com
Threat, Vulnerability, Risk, Compliance –
What do I do first to protect my agency?

William (Bill) Harrod
Advisor, CA Technologies
Public Sector, Cyber Security Practice
William.Harrod@ca.com
What is Risk?

Threat x Vulnerability x Cost = Risk

Where Threat and Vulnerability are probabilities of successful attack
Federal Government requires seat belts -

Title 49 of the United States Code, Chapter 301, Motor Vehicle Safety Standard, which took effect on January 1, 1968, that required all vehicles (except buses) to be fitted with seat belts in all designated seating positions¹

Seat Belts Save Lives!

58% of teen drivers killed in car accidents were not wearing a seat belt.

The largest number of people are killed between 5 p.m. and 6 p.m.

On average, 6.6 million people are killed during each of these hours.

2,228 teenagers died in motor vehicle accidents in 2012.

29% of wrecks happen 2-5 miles from home

23% of car wrecks happen less than 1 mile from home.

1. https://en.wikipedia.org/wiki/Seat_belt_legislation_in_the_United_States

Why do we allow convertibles?

Shouldn’t all cars have steel reinforced roofs with extra protection against meteor strikes?
Threat x Vulnerability x Cost = Risk

Seat Belts
.011 x .95 x $25,000 = $261.25

Meteorites striking a car
.0000000000000000001 x .99 x $35,000 = $0

Cyber Risk
.99 x .7 x $550,000 = $381,150

https://business.kaspersky.com/cost-cyberattack-enterprise/5195/
INAMOIBW

28

?
28 Months
28 Months is the Average Tenure for a Large Agency CISO
IT’S NOT A MATTER OF IF BUT WHEN

That you will be attacked NOT, that the bad guys will succeed, in other words your THREAT is nearly 100%
Gartner predicts there will be 6.8 billion connected devices in use in 2016.
The Rapid Escalation in Threat, and Vulnerability is driven by:
Current Top Security Threats

Extortion Attacks
- Ransomware
- Exposure Threats – DNC, WikiLeaks, Russian Hackers “Fancy Bears”

Phishing Attacks and Identity Fraud
- Credential Captures
- Unauthorized / unknown / ghost software

IoT Zombie Botnet Attacks
- Machine to Machine Attacks (Dyn DDoS DNS attack on 10/21/16)
- PoC attacks against cars, medical devices, HVAC systems

Advanced Persistent Threat
- Change or manipulate data
- Gathering & exfiltrating data
- Accounting changes
- Sabotage

Retail Sales Attacks
- POS Attacks (outdated OS, lack of controls)
- Online Transaction Attacks
- App Payment System Attacks (Starbucks, Apple Pay)
What do all of these companies have in Common?

1. They were PCI Compliant
2. They suffered significant breaches
Heartland Payment Systems Hacked

Heartland’s Data Breach: What Happened?

II.

The method used to compromise Heartland’s network was ultimately determined to be SQL injection. Code written eight years ago for a web form allowed access to Heartland’s corporate network. This code had a vulnerability that (1) was not identified through annual internal and external audits of Heartland’s systems or through continuous internal system-monitoring procedures, and (2) provided a means to extend the compromise from the corporate network to the separate payment processing network. Although the vulnerability existed for several years, SQL injection didn’t occur until late 2007.

* Heartland Payment Systems: Lessons Learned from a Data Breach
  Julia S. Cheney
Standards compliance does not equal sound information security risk management

The question "how much is enough" in regard to security spending has been explored by many researchers. Industry seems to have answered the question simply as "spend just enough to pass the next regulatory examination." Regulatory security standards are intended to provide a generalized baseline for information protection and organizations are failing to recognize their own security requirements do not directly map to any single standard or set of standards. In fact, the very elements within an organization that do not overlap with a standard may present the most challenging risks.

Unfortunately, it appears many institutions have settled on the misguided notion that compliance and security are essentially synonymous and as a result have significant unmitigated risks. Simply stated, the checklist security audit approach is easy to understand and budget for, but the result is inadequate security. The Heartland Payment Systems breach demonstrated how an emphasis on compliance may not be reasonable as the company was damaged by a huge breach despite apparent compliance with the PCI...
We have a Proliferation of Standards and Regulations and Frameworks

ISO 27001 Certified

COBIT

SARBANES-OXLEY

COSO

HIPAA Compliance

GLBA

PCI DSS COMPLIANT

NIST

Gramm-Leach Bliley Act

Department of the Treasury Internal Revenue Service

2016 NYSICA Annual Conference
A “Head Start” for Cyber Risk – Prioritized Steps

Originating in 2008 as the SANS Top 20 Security Controls, the Center for Internet Security (CIS) has published The Critical Security Controls (CSC) a prioritized list of actionable steps that organizations can implement to reduce cyber-security risk.

1. (http://www.cisecurity.org/critical-controls.cfm)

“Organizations that apply just the first five CIS Controls can reduce their risk of cyberattack by around 85 percent. Implementing all 20 CIS Controls increases the risk reduction to around 94 percent.”
## A “Head Start” for Cyber Risk – 5 Prioritized Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Can be Automated</th>
<th>Supported Automating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Inventory of Authorized and Unauthorized Devices</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>2.</td>
<td>Inventory of Authorized and Unauthorized Software</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>3</td>
<td>Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>4</td>
<td>Continuous Vulnerability Assessment &amp; Remediation</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>5</td>
<td>Controlled Use of Administrative Privileges</td>
<td>✅</td>
<td>✅</td>
</tr>
</tbody>
</table>
Call to Action: Move from “NO” to “KNOW”

• Know who your users are and what they can access
  • Limit Scope and clean up “ghost” accounts

• Know what is on your network – software and hardware inventory

• Know who your privileged users are and what they can actually do

• Know how users authenticate – Passwords are dead
  • Risk based Authentication – Risk Score
  • Behavior Based Authentication – Is this typical
Know who your users are and what they can access!
Our System Administrators are the Good Guys

“We only have a few privileged users”

“They are background checked”

“Our SysAdmins are the Good Guys”

“We don’t allow shared account access (do we?)”
How Many Times Has Your Personal Information Been Exposed to Hackers?

http://www.nytimes.com/interactive/2015/07/29/technology/personaltech/what-parts-of-your-information-have-been-exposed-to-hackers-quiz.html?_r=1
Be Flexible, Nimble, and Adapt

1. Adopt and implement the first 5 Critical Security Controls

2. Follow a DAPE Model – Deny All, Permit Explicitly

3. Leverage Stronger Authentication - Passwords are out

4. Prioritize Security Actions - Address the top 5, then the top 20, then ....

5. RINSE, LATHER, REPEAT
William (Bill) Harrod
Advisor, CA Technologies
Public Sector, Cyber Security Practice
William.Harrod@ca.com
703.708.3863