Improving Third Party Risk Management with Cyber Threat Intelligence

Norman W Menz III, CTPRP
CTO, Prevalent
Third-Party/Vendor Risk Management is...
... while dealing with tectonic technology shifts.
3rd Party Cyber Risk is a Hot Topic

“It is abundantly clear that, in many respects,” Mr. Lawsky (New York State’s top financial regulator) said in the letter, “a firm’s level of cybersecurity is only as good as the security of its vendors.”

NYTimes.com: After JPMorgan Cyberattack, a Push to Fortify Wall Street Banks 10/21/14

• The breach at Target Corp. that exposed credit card and PII data on more than 70MM consumers began with a malware-laced phishing attack sent to a third party vendor” KrebsOnSecurity

• “PCI 3.0, HIPAA Omnibus, OCC, CFPB, FFIEC and the Federal Reserve have changed the way organizations in many industries need to think about IT & data supply chain risk management”

• "If not managed effectively, the use of service providers may expose financial institutions to regulatory action, financial loss, litigation, and loss of reputation.“ Federal Reserve

• “Institutions under the jurisdiction of the CFPB will have to evaluate the risk profile of vendors and retain evidence of risk & compliance activities of those 3rd parties,” Risk & Compliance Journal

• The Office of the Comptroller of Currency (OCC) issued new standards and requirements for banks regarding the upfront and ongoing management / monitoring of third party risk – October 2013
Living in a post-Target, post-Heartbleed world...
Companies with red logos... potentially a huge risk!
2015 – The Year of the Orange Logo
Mega Breaches

<table>
<thead>
<tr>
<th>Year</th>
<th>Breaches</th>
<th>Identities Exposed</th>
<th>Breaches &gt;10M</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>208</td>
<td>232M</td>
<td>5</td>
</tr>
</tbody>
</table>

2013 was the Year of the Mega Breach
Breaches by Sector

Data Breaches by Sector, 2013
Source: Symantec

Healthcare, education and the public sectors accounted for 72% of all data breaches

But, the retail, computer software and financial sectors accounted for 77% of all identities exposed in 2013
Targeted Organization by Size

Spear Phishing Attacks by Size of Targeted Organization, 2011 - 2013

Source: Symantec
3rd Party Error and Data Loss Cost

Figure 9. Impact of eight factors on the per capita cost of data breach

- Lost or stolen devices: $16.10
- Third party involvement: $14.80
- Quick notification: $10.45
- Consultants engaged: $2.10
- CISO appointed: $(6.59)
- BCM involvement: $(8.98)
- Incident response plan: $(12.77)
- Strong security posture: $(14.14)

Source: 2014 Cost Data Breach Study; Ponemon Institute; May 2014
Regulatory Pressure Increasing

1996

• HIPAA

1996

• GLBA

2001

• OCC Bulletin 2001-47

2002

• OCC Bulletin 2002-16

2002

• CS Privacy SB 1386

2003

• HF 1758 MN Plastic Card Security Act

2007

• HITECH Act

2009

• NRS 603 NV Data Security

2010

• 201 MA Code Reg 17

2010

• WA HB 1149

2011

• PCI DSS 2

2012

• CFPB Bulletin 2012-03

2013

• Omnibus HIPAA Rule

2013

• OCC Bulletin 2013-29

2014

• PCI DSS 3

Protected Data Types

• Intellectual Property (IP)

• Personally Identifiable Information (PII)

• Payment Card Industry (PCI)

• Protected Health Information (PHI)
PCI 3.0 - 3rd Party Risk Highlights

12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.

12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
PCI 3.0 Con’t

12.8.4 Maintain a program to monitor service providers’ PCI DSS compliance status at least annually.

12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

12.9 Additional requirement for service providers: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.

Note: This requirement is a best practice until June 30, 2015, after which it becomes a requirement.
OCC and 3rd Party Risk - Highlights

- A bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.
- A bank should ensure comprehensive risk management and oversight of third-party relationships involving critical activities.
- An effective risk management process throughout the life cycle of the relationship includes:
  - Plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.
  - Proper due diligence in selecting a third party.
  - Written contracts that outline the rights and responsibilities of all parties.
  - Ongoing monitoring of the third party's activities and performance.
  - Contingency plans for terminating the relationship in an effective manner.
  - Clear roles and responsibilities for overseeing and managing the relationship and risk management process.
  - Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management.
  - Independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.

Source: OCC
HIPAA Privacy, Security, and Enforcement Rules

• **Business Associates**
  – Direct Liability
  – Expanded Definition
  – BAA
• Marketing & Fundraising
• Prohibition on Sale of PHI without individual auth.
• Expansion of Individuals Rights to restrict Use, Disclosure & Access
• Modifications to & Redistribution of NPP

• Modifications to Individual Authorizations for Research
• Child Immunization Records
• Decedent Health Information
• **Additional Changes to Enforcement Rule**
  – Formal Investigations
  – HHS Authority to Release PHI during an Investigation
  – Liability for Agents
  – Affirmative Defenses
• Patient Safety Activities
New Focus on Willful Neglect

- Willful neglect: Conscious, intentional failure or reckless indifference
  - No policy = reckless indifference
- OCR will investigate all cases of possible willful neglect
- OCR will impose penalty on all willful neglect violations
- OCR may proceed to penalty without seeking informal resolution (settlements)

- Other Enforcement Changes
  - Change in definition of “reasonable cause” (fills the gaps between “did not know” and “willful neglect”)
  - Revised factors to calculating Civil Monetary Penalty
  - Covered Entities and Business Associates are liable for agents acting within scope of agency, even if a BAA is in place
The Data Supply Chain
3rd Party Assessment – Program Requirements

**Compliance Assessment** - Scale third party assessment process to provide full visibility through risk scoring, evidence de-duplication, and tracking with industry standard content.

**Technical Monitoring** - Integration with technical evidence (e.g. Veracode, Qualys) to provide risk information and allow for automated monitoring.

**Threat Monitoring** - Dynamic assessment of a third party’s risk through the analysis of public and proprietary sources of vendor threat intelligence.
Framework

- DISCOVERY
- ASSESSMENT
- RESPONSE
- MONITORING
- OVERSIGHT
Assessment

- Standardized Content (SA SIG, CSA CAIQ)
- Automate, automate, automate in software...
- Purpose built to scale.
- Centralized repository for all evidence.
- Schedule management.
How many vendor assessments can a single resources perform in a single year, and how much will each assessment cost? Well, that depends on the tool.

By leveraging VRM instead of a manual effort, a single 3rd Party Risk resource can immediately increase productivity.
Monitoring

- I have to do this again??
- Create strategies for helping minimize re-assessment efforts
  - Evidence Deduplication
  - Assessment Grouping
- Monitoring does NOT necessarily mean more assessment...
Monitoring

Technical Monitoring - Integration with technical evidence (e.g. Veracode, HP Fortify On Demand, Qualys) to provide risk information and allow for automated monitoring

Threat Monitoring - Dynamic assessment of a third party’s risk through the analysis of public and proprietary sources of vendor threat intelligence
What is Vendor Threat Monitor?

Definition

**Vendor–Threat-Monitor**

[VTM] – service

1. Dynamic assessment of a third party’s risk through the analysis of public and proprietary sources of vendor threat intelligence
2. Correlation and analysis of external events into risk categories such as Data Risk, Brand Risk, Financial Risk, Operational Risk, and Regulatory Risk
3. Provides ongoing monitoring of third parties before, during, and after an assessment
4. Helps to align organizational and regulatory objectives for ongoing and continuous monitoring of third and fourth parties

(See also: ‘vtm’, ‘prevalent’, ‘external risk’, ‘visibility’)

© Copyright 2015 Prevalent, Inc.
Risk Engine

- Feeds
- External Discovery Services
- Association
- Data Breakdown Event Identification
- Analysis
  - Relevance Rules
  - Temporal Frequency
  - Geospatial
  - Risk Areas

Risk Events

Organization Directory

Data Feed Source

Prevalent

{"risk_type": "Accidental Disclosure", "details": "Over 100,000 customer names, emails, and addresses were disclosed when an employee....", "score": 4.9}
What to Look for....Select a Cyber Threat Intelligence Platform for 3rd Party Risk

**Sources:**
- Internet/IP Reputation
- Web Presence Hygiene
- Data Breach Monitoring
- Sanctions Lists
  - OFAC
  - UK Financial Sanctions
  - EU Financial Sanctions
  - Australian Financial Sanctions
  - WorldBank Debarred List
  - etc
- Phishing Attack Monitoring
- Credit Ratings
- Financial Records

**Coverage:**
- Does the source have a broad and deep data set?
  - Broad – domestic and internal data across key sources
  - Deep – sufficient history and scope of collection

**Risk Scoring:**
- Risk Scoring Relevant to your 3rd party relationships
  - Does the tool / source consider inherent risk
  - Does it risk weight events based on the relevance to your business/3rd parties
What to Look for....Select a Cyber Threat Intelligence Platform for 3rd Party Risk

Risk Scoring:

• Risk Scoring Relevant to your 3rd party relationships
  • Does the tool / source consider inherent risk?
  • Does it risk weight events based on the relevance to your business/3rd parties?
  • Does it provide insight into impact across specific risk areas which are relevant to your relationship(s)?

Visibility:

• Beyond the risk score, can you make a decision based on the information available to you?
Risk is not a single magic number

• FICO Scores work for consumer credit but not for 3rd party risk analysis
  • Single scores provide no context, ask: “Based on the information provided do I understand where the risk is coming from and how it impacts this particular 3rd party relationship/engagement”
The Future of 3rd Party Risk

• Big Data Analytics and Continuous Monitoring
  – Gartner “predictive analytics”

• Application Security In The Spotlight

• Additional Regulatory and Privacy Coverage

• Additional Sharing Among Peers
  – Collaborative Onsite Assessments
  – ISACs
Top 5 Things Your Board Should Know

• Contracts are no longer enough to protect the business.
• A breach of your client’s or patient’s data at a third party is YOUR responsibility.
• Single, point-in-time assessment is no longer sufficient.
• Third-party risk should be part of your cybersecurity plan.
• Your CISO (or equivalent) should report those risks directly to the board.
Thank you!
VENDOR THREAT MONITOR

3.3 Billion
records lost in data breaches

13,865
data breach events

4605
sanctioned organizations

46,474
organizations monitored

473,112

It has implemented enhancements to its privacy and information security framework including the establishment of an Office of Privacy, Ethics and
Whitepaper by Brad Keller

- Available at [www.prevalent.net](http://www.prevalent.net) > Resources