Vendor Security Alliance:
Finally Fixing Third Party Cybersecurity

Ken Baylor, Ph.D.
President,
Vendor Security Alliance
@baylorsecurity

Nathan McCauley
Director of Security, Docker
Vendor Security really?
Data is the most important thing you have

Most valuable companies 2007

1. Exxon Mobil
2. Petrochina
3. General Electric
4. China Mobile
5. Industrial and Commercial Bank of China
6. Microsoft
7. Royal Dutch
8. China Petroleum
9. GazProm
10. AT&T

Most valuable companies 2017

1. Apple
2. Alphabet/Google
3. Microsoft
4. Amazon.com
5. Facebook
6. Berkshire Hathaway
7. Alibaba Group
8. Johnson & Johnson
9. Exxon Mobil
10. JP Morgan Chase
63% # of data breaches linked to third-party vendors

Trustwave Global Security Report
Who gets blamed?
$4 \text{mm/breach on average (2016)}
The Vendor Security process is VERY broken
Stages in buying a product

- Identify a need
- Identify vendors
- Test products or services (Proof of Concept/PoC)
- Vendor due diligence
- Pricing & contracts
Corporate Vendor Security Perceptions

1) Add no business value, has no real risk reduction
2) Expensive in time and money
3) Adds no insight to vendor decisions
4) Ask random questions, too many and too late

⇒ The focus of the group should be to protect your brand, by protecting your most important asset, customer information, via weeding out weak vendors
Real life: Scenario 1

Last day of quarter:
Approached by SVP who ‘requires’ you to sign off on a major purchase. They have completed an in-depth PoC (which you are just hearing about now)
If you slow down or kill this deal you will suffer

⇒ Only the product has been tested you have no idea what data is being shared or how it is being protected.
There are 10 PoCs occurring simultaneously
Each has 6 vendors. 
A vendor assessment costs $6.5k if done in-house, $13k if outsourced. 
You have only 2 assessors and assessments keep falling through the cracks
Average turnaround time is 8 weeks: several weeks AFTER the decision to purchase has been made.
⇒ Critical vendors are never periodically reviewed as you are swamped
Regulations require better due diligence
Europe is implementing the EU General Data Protection Regulation (GDPR) in May 2018. Risk-based due diligence required for all data processors. Breach fines of 2-4% of global revenue.

Many US companies are signing up for Privacy Shield in order to do business with the EU. Many GDPR requirements being placed on US companies. Privacy Shield revision due in Sept 2018.

If you do business with companies in the EU or USA, GDPR will likely impact you.
Asia standards changing

- Philippines Data Protection Act comes into full force in September 2017. Criminal liability in event of a breach up to 7 years (inc CEO & Board)
- India, Philippines applying for data privacy ‘adequacy’. Must implement controls similar to GDPR
- APEC CBPR – Governs cross border data transfers (South Korea, USA, Mexico, Canada, Japan)
- Singapore ‘Cyber Security Bill’ data breach notification requires tight control of vendors
- Japan updated it’s privacy laws on May 30 2017 to include ‘sensitive information’, establishment of a Privacy Commission and other GDPR concepts.
No one vendor can fix it, but together we can
Solving this problem is very hard

1) Need a new questionnaire driven by industry, not a vendor in a vacuum
2) This questionnaire must be flexible and risk proportionate
3) Focus on security practices (i.e. data protection)
4) Scope must be JUST the service we are purchasing
5) The questionnaire must be regularly updated
6) It must be widely adopted (free is a good start)

Others have tried similar things before: Shared Assessments SIG, Cloud Security Alliance, Google, PCI. None of them meet all criteria. But the questionnaire is only the start.
How to scale it:

a) Stop duplication: If a recent review has been done by another trusted party, we can access it immediately
   i) Allows rapid acceptance or rejection of PoC candidates
b) You need a network of trusted Auditors who you can outsource the audit to. This will allow you to find and focus on critical risk vendors
   i) Auditors must speak multiple languages
   ii) The cost of a report must be low (> $1200)
c) If we compare competing vendor security practices, we can find and eliminate weak links in your vendor ecosystem
   i) This is the ultimate goal of vendor risk management
Creating an alliance focused on Vendor Security
2017

- Adobe
- Taskus
- Coinbase
Solution Phase I

Create a non-profit. Owned by all members.

MISSION: Measure and improve vendor risk

Create a FREE questionnaire that is data-security centric and focuses on real risk
Large companies have downloaded it, and replaced their current methods
Startups are using it to build good security practices early
Scaling it via shared reports by trusted assessors

1. Real time vendor risk decisions
2. Lower costs compared to doing it yourself
3. Faster than doing it yourself
4. Ability to scale (all vendors can be audited within a year)
5. Ability to audit in multiple languages
6. Realize you have better vendor options, and who they are
7. Make vendor management highly relevant to business decisions
Choosing between vendors
Corporate Vendor Security Perceptions

1) Add no business value, as no real risk reduction
2) Expensive in time and money
3) Adds no insight to vendor decisions
4) Ask random questions, too many and too late

⇒ The focus of the group should be to protect your brand, by protecting your most important asset, customer information, via weeding out weak vendors
‘To Do’

- Examine your current vendor due diligence program, and ask:
  - Does our risk methodology make sense?
  - Are we finding high risk vendors?
  - Are vendors being assessed appropriately?
  - Is it fast enough?
  - Is the fully loaded cost per audit?

- Examine regulatory changes:
  - If you do business with EU, US, Philippines or India more diligence needed
  - Are there more secure vendors that can replace ours?
  - Are we weeding out high residual risk vendors?