RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

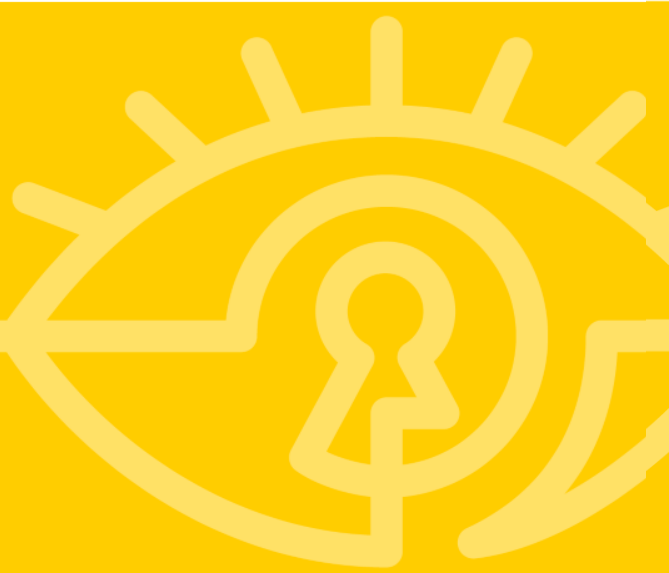
Connect to Protect

SESSION ID: STR-FO2

Vendor Security Practices: Turn the Rocks Over Early and Often

Michael Hammer
Web Operations Security
American Greetings
@MichaelHammer

Martin Andrews
Director of Web Operations
American Greetings



Why Vet Vendors for Security and Compliance?

So why vet vendors for security & Compliance?

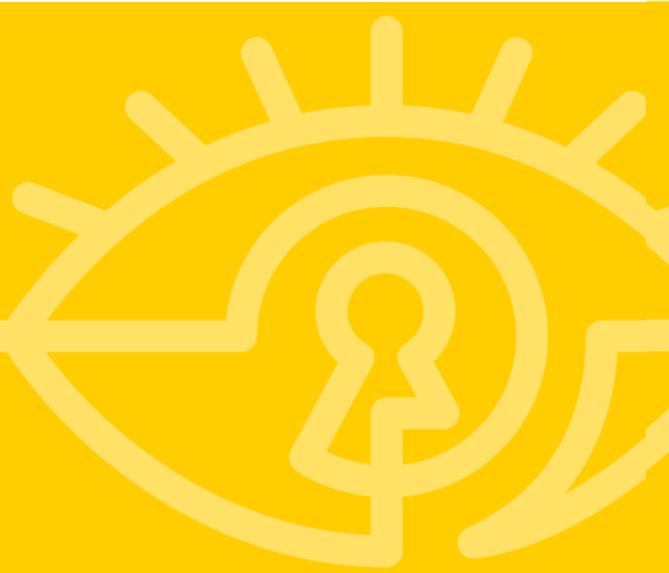
- Compliance
  - PCI, HIPAA, GLBA, SOX
  - FTC Section 5
- Security - don’t want that CNN moment
- Stewardship - it’s the right thing to do

The bar is getting higher – PCI-DSS v3.1

- 12.8.2 - Requires written agreement with vendor including responsibility acknowledgement
- 12.8.3 – Due diligence requirement prior to engaging vendor
- 12.8.4 – Program to monitor vendor compliance
- 12.8.5 – Maintain information about responsibilities

Sample Breaches Involving Vendors

- Target – December 2013 (HVAC Vendor)
- Dairy Queen – July 2014 (POS Vendor)
- JPMC – Disclosed November 2015 (**G2 Web Services LLC hacked**)
- ? – November 2015 (LanDesk)
- ? - Disclosed December 2015 (Juniper) – malware in code



Typical selection process at many organizations…

Typical Process for Vendor Selection

- Business person identifies perceived need
- Identifies potential vendors based on business needs
- Spends time gathering info and negotiating
- Maybe brings in security for review before signing agreement
  - – or not!
- 7 Stages of Grief

7 Stages of Grief

- Shock or Disbelief
- Denial
- Bargaining
- Guilt
- Anger
- Depression
- Acceptance

Typical results

- Lots of time and energy invested in vendors that may have issues and can't be used.
- Security and compliance viewed as a blocker if vendor rejected during vetting.
- Unhappiness and frustration all the way around.

An Alternative Approach – Security First

Attitude is Everything

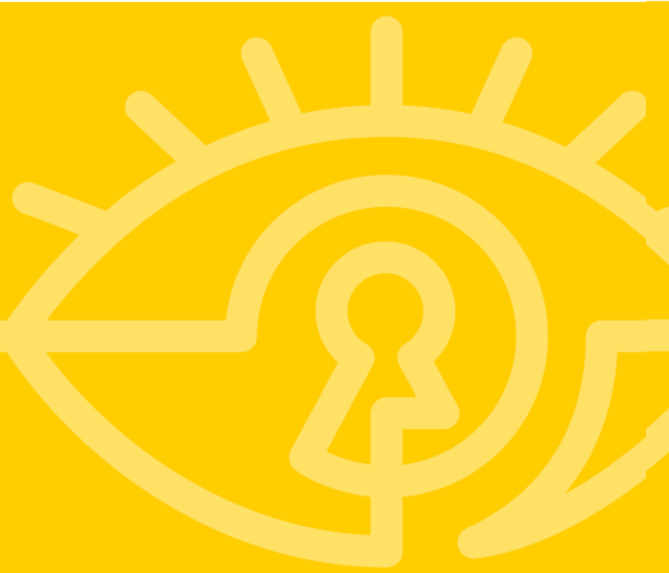
- It’s about finding ways to get to yes!
- It’s not about finding reasons to say no!

Goals

- Reduce effort vetting Vendors
- Rank acceptable Vendors on Security & Compliance Practices
- Identify potential risks
- Sets stage for contractual requirements and negotiations

Process Starts the Same

- Business person identifies perceived need
- Identifies potential vendors based on business needs
- **Security and Compliance Steps in…**



Finally, Things You Can Apply!

Initial Homework – Some tools

- Google “$VENDOR security”
- Ssllabs.com
- Senderscore.org
- Shodan
- FOCA (document exposure)
  - https://www.elevenpaths.com/labstools/foca/index.html

Interview Process

- Business person arranges 30 minute call with (vendor) person **responsible for security & compliance.** Get an NDA set up in advance.
- An hour or so before the call, email ~30 questions to vendor
- The call
- Post Mortem

Arranging The Call

- Make Sure the Vendor Representative Knows Security & Compliance for Organization
  - NOT VP of Marketing
  - NOT Sales Engineer

Ranking Criteria

Select ~4 Categories to Rank Vendors

Example: Hosting Provider

- Physical Controls
- Employee Checks
- Vendor Security
- General

The Questions

- We generally send ~30 questions (1 per call minute)
  - You probably won't get through all of them
  - Think about your criteria for ranking
- Tailor to What the Vendor is Doing/Providing.

The Call

- Not Looking for Deep Dives on Any Given Question
- Expect They May Not Have All Details At Hand
- How They Answer Can Be As Important As What They Answer.
- Consistency Across Answers
- Transparency

Questions: Documentation

Can you provide:

- Security Policy
- SOC2 Report or comparable – Take with a grain of salt.
- Employee Handbook

- How forthcoming are they?

Questions: Compliance

- Any security compliance you adhere to (PCI, HIPAA, SOX, GLBA)?
- What requirements can you fulfill?
- Will you sign agreement defining your role and responsibilities?

Questions: Incidents

- Any security incident or breach in the last 18 months?
- Any regulatory or end-user notification required?
- Any security events?
  - Lost phones or laptops?

Questions: Vendor Security

- Do you have a formal program to assess vendor security?
- Onsite assessments?
- What vendors do you use?

Questions: Penetration Test

- When was your last pentest?
  - When was the prior one?
- Organization(s) that performed them?
- Nature and scope?
- High or critical items found?
  - Entered into ticketing system?
- Remediation?

Questions: Security Assessments

(pretty much the same as Pentest questions)

Questions: Logging

- What logs are collected?
- How long are access and audit logs maintained?
- What controls to preserve integrity?
- How are logs reviewed?

Questions: Intrusion Detection/Prevention

- Do you utilize NIDS/HIDS?
- IPS?
- WAF?
- What traffic/locations are covered?
- Who responds to events? SLA?

Questions: Endpoint Security Software

- Do you use endpoint security? Which?
- What systems are covered?

Questions: Employee Checks

- Background check and drug test required?
- All employees?
- Contractors?

Questions: Incident Response

- Who is in your incident response team?
- How often do they meet?
- Training/Exercises?
- Describe (provide?) your incident response plan.

Questions: Physical Controls

- Describe office and datacenter physical controls
- Are visitors required to check-in and wear badges?
- Video monitoring? How long is it retained?
- Card access log retention?

Questions: Software Development

- What parts of applications are internally developed?
- How is security included in your SDLC?
- Do you use
  - Static analysis?
  - Code reviews?
  - Vulnerability assessment tools?
  - Web application firewall?

Questions: Change Control

- Formal change control process?
- Who can move to production?
- Rollbacks?

Questions: Cloud

Multiple layers = less transparency

- What components and data are in the cloud?
- Who is responsible for what?
- What is covered by Letter of Compliance, SAS 70, etc.
  - And what is not!
- Which regions is vendor hosted in?
- How are access keys managed?

Questions: Wireless

- Do you maintain wireless network(s)
- What authentication?
- What access is allowed?
- Rogue wireless detection?

Questions: Remote Access

- VPN for remote access?
- Are there systems that don't require VPN?
- Multi-factor authentication? What components?

Questions: Patching

- What 3rd party software do you use?
- What notification sources do you track?
- Process for patching 3rd party software?

Red Flag Examples

- Most stringent audit ever
- Never had a security event (in 10 years?)
- We deal with many large companies and they have never asked us these types of questions.
- We ARE a large well known company and we don’t give out this information.

Post-Mortem

- Acceptable?
- Ranking + “the story” in business language
  - What are the most important issues/priorities
  - Consistency across questions
  - Feedback to help selection process

Once “the vendor” is identified

- You still need to do additional due diligence
  - Validate assertions – may include onsite
  - Contractual requirements
  - Remediation

Now

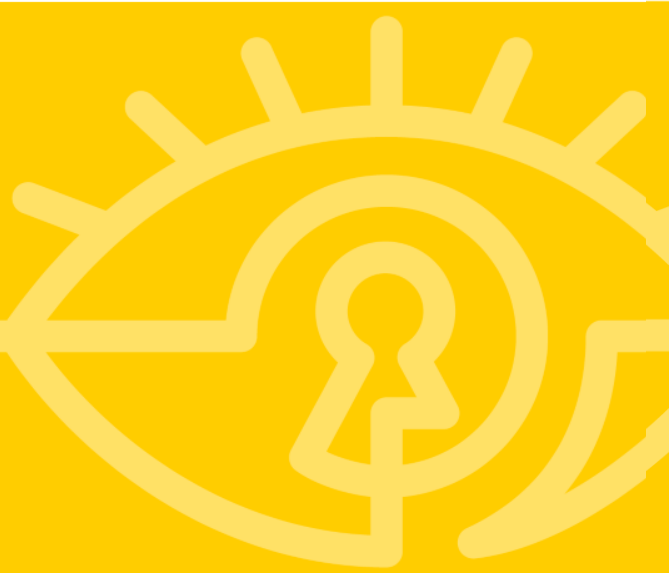
- Get Senior Management Buy-in & Support
- Evangelize the benefits of this approach
  - Time savings for business
  - Shortens selection life cycle

Now

- Meet with business contacts
  - What vendor searches are ongoing/upcoming
  - Tell them you want to help (and how)
  - Lunch and Learn about the process
- Create an interview template
- Build a portfolio of tools

Next 3 Months

- Interview vendors for a new project
- Get to “yes”



Questions?

mandrews@ag.com
mhammer@ag.com