RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CXO-W14

MONTY PYTHON AND THE HOLY RFP

Mary Ann Davidson

Chief Security Officer
Oracle Corporation
@heenaluwahine

How Did We Get Here?

- Explosion in security-related questionnaires
- Scope is …the moon, the stars, the known universe
- No clear risk concern behind many questions
- No clear “driver”
- Result
  - Long, expensive sales cycles
  - Potentially worse security from “crowding out effect”
  - Statistically significant increase in Scotch consumption

A Theory…

- History of “demand better assurance…”
- With cloud, security is a shared responsibility
- However, natural need to assess the processor of sensitive data is now skewed:
  - Assessing everything
  - Neglecting basics

Learning Objectives

- Understand why “checkbox-based security” isn’t necessarily good security
  - “Look both ways before crossing the road…”
- How to ask legitimate, clear questions internally and externally to advance your ability to assess risk

Sound Familiar?

- HEAD KNIGHT: The Knights Who Say Ni demand a sacrifice!
- ARTHUR: Knights of Ni, we are but simple travelers who seek the enchanter who lives beyond these woods.
- HEAD KNIGHT: Ni! Ni! Ni! Ni!
- ARTHUR and PARTY: Oh, ow!
- HEAD KNIGHT: We shall say 'Ni' again to you if you do not appease us.
- ARTHUR: Well, what is it you want?
- HEAD KNIGHT: We want... a shrubbery!

A Few Caveats

- Assessing *relevant* risk management concerns is good and useful
- Regulated industries have more questions they *believe* they need answered
- No shrubberies or herrings were harmed during the making of this presentation

Reasonable Expectations

- Gauging supplier's risk management practices…
  - ***…as they specifically affect the purchaser***
- Scoped questions related to specific products and services
- Alignment with relevant, recognized, international, independently-developed standards

Unreasonable Expectations

- Asking questions about **all** business risk of the supplier
- Questions relating to “all products and services”
- Demands that are vague, unmeetable or that enable “another shrubbery” ask
- Requiring “assessments” by specific contractors or auditors against their proprietary, non-standard “frameworks”

In Other Words…

Examples

- “Provide the patching status of every Windows server in your enterprise.”
- “Provide a patch for anything we deem critical so we can apply it within 3 days.”
- “Answer this service-oriented questionnaire for on premises products.”
- “Your entire security team needs to fly to < > to explain your assurance program.”

….And Why They Are Problematic

- "Patching status"
  - Server hosting customer data patched against ransomware != entire enterprise
- "3 day patching"
  - Third party library, architectural changes required, "community issues…"
  - "We know nobody can meet this."
  - Pulling the plug for a DOS vulnerability
- "Service-oriented questionnaire"
  - Renter vs. hotel
- "Fly to <x>"
  - 10-20 people for 3 days for *one* customer?

Sound Familiar?

ARTHUR: You silly sod!
TIM: What?
ARTHUR: You got us all worked up!
TIM: Well, that's no ordinary rabbit!
ARTHUR: Ohh.
TIM: That's the most foul, cruel, and bad-tempered rodent you ever set eyes on!
ROBIN: You tit! I soiled my armor I was so scared!
TIM: Look, that rabbit's got a vicious streak a mile wide! It's a killer!

More Painful Examples

- “We want to pen test *any* internal system.”
- “You must agree to <non-standard assurance certification>, provide development artifacts including security design, architectural analysis, static analysis results…”
- “You must meet with our auditor.”
- “You must notify us immediately of any CVSS 7 or greater or any zero day.”
- “Your security policies must have a watermark on them.”

….And Why They Are Problematic (1 of 2)

- "Pen test *any* internal system"
  - Our internal systems contain… **none** of your data
  - Multitenant clouds containing a competitors' data, really?
- "Non-standard certification, development artifacts…"
  - *No contractual restrictions* on "asks" for more artifacts, or third party code analysis
  - Access to core IP would "bleed"
  - Attestations to documented assurance practice would be reasonable

….And Why They Are Problematic (2 of 2)

- "Auditor"
  - On site auditor didn't know scope of audit, asked customer audit support person, who didn't know…
- "Vulnerability notification"
  - Watch and learn from PCI…
  - Notification without a patch doesn't solve the problem
  - Attestation that security issues are (generally) fixed in severity order is reasonable
- "Watermark"
  - On non-printed material?

Even More Painful Examples

- “We found a severe CSRF: you must provide static analysis results for each release and patch.”
- “You must review each of 120 documents (1000 pounds, printed).”

….And Why They Are Problematic

- "Static analysis results"
  - Wasn't a CSRF and issue had already been fixed
- "120 documents"
  - Each organization agreed we align with ISO27001:2013, NIST, other standards
  - Extremely costly exercise that added no value but deducted from bottom line

Considerations

- Spending resources on “shrubbery” uses scarce resources that could be spent making security better *for everybody*
- Specific risk concern to a purchaser != any and all business risk
- Nobody should contractually commit to something that is vague or cannot be done
- Unclear/bad regulations should be pushed back on, not kowtowed to

Sound Familiar?

Old Man from Scene 24: Stop! WHAT is your name?
King Arthur: It is Arthur, King of the Britons!
Old Man from Scene 24: WHAT is your quest?
King Arthur: To seek the Holy Grail!
Old Man from Scene 24: WHAT is the airspeed velocity of an unladen swallow?
King Arthur: What do you mean? African or European swallow?

Finding the Holy Grail – Vendors (1 of 2)

- Provide “rules of engagement”
  - Ask about specific products/services
  - Submit via X not Y
- Roadmaps help everyone get to the finish line faster
- Provide “self service” materials as publicly as you can
- Use/train account teams on expectations management and eliciting core risk management concern

Finding the Holy Grail - Customers (2 of 2)

- Eliminate the middleman and accompanying “translation problems”
- Push back on vague/unclear/unworkable “regulation”
- Focus on meaningful, cost-effective risk mitigation
  - Compliance *may* be necessary, but it is not sufficient
  - …especially if it crowds out actual security
- Buy…a shrubbery! (Not too big.)

Lessons from the Trenches

- Published “rules of engagement” for customers
- Creating more online information about security practices
- Providing FAQs on “why we won’t provide X, and why it’s in your interests”
- Exploring if there are regulatory requirements behind some of the stranger asks
- The above can work for companies of any size

Apply What You Have Learned Today

- Next week you should:
  - Watch *Monty Python and the Holy Grail*
- In the first three months following this presentation you should:
  - Ensure all your vendor security questionnaires have a clear, prioritized “risk management concern” behind each item
- Within six months you should:
  - Review relevant regulatory areas driving security questions
  - Identify problematic areas that need clarification or revision
  - Determine whether African or European swallows are faster