RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: MASH-F01

Doin' the Regulatory Rumba

Mary Ann Davidson
Chief Security Officer
Oracle Corporation

A Few Caveats…

- "No regulators were harmed during the making of this presentation…"
- No disrespect is intended *nor should be inferred* towards regulatory bodies
- But… "you don't ask, you don't get!"

How Did We Get Here?

- Y'all know why…more Internet-connected stuff, more breaches, more data at risk…!
- Regulatory entities want to improve the ecosystem
  - …and can't be experts on everything
- Practitioners want "broadly better security in an achievable, effective and cost-effective way …"

How I Became A Regulatory Crank…

- Impossible-to-meet uniform requirements in the U.S. Navy
  - “Hard hat, steel-toed pumps, white gloves and a purse, really?”
- Contracting officer experience in the U.S. Navy
  - “106 general provisions…enough to skewer anyone with …”

What is a “Regulation?”

- Law
- Procurement requirement
- Contractual obligation or market requirement
- Something you gotta do … *or else!*

Why Stuff Is “Regulated”

- Public policy, e.g.
  - Safety
  - Address externalities
  - …
- Other
  - Standards
  - Competitive advantage
  - Successful regulatory capture

“Houston, We Have A Problem”

- Ambiguous requirements may be impossible to meet
- Cost may not be commensurate with benefit
- Preclusion of better solutions
- Scope creep
- Failure to keep pace with change
- “Unfortunate, unintended consequences”

Audience Participation…

- Have you been asked to comply with a regulatory requirement that was unclear?
- Have you been asked to comply with *conflicting* requirements?
- Have you ever have gone back to the regulatory body and expressed your concerns?

On the Positive Side…

When More Government Is A Good Thing

Before We Get To Examples…

- Caveats
  - “Lessons from history”
  - National Institute for Standards and Technology (NIST) is one of the *most* responsive organizations in seeking and taking industry feedback

Here We Go…

- Payment Card Industry (PCI) Payment Applications Data Security Standard (PA-DSS)
  - "Payment application" is narrowly defined
  - Third party qualified security assessors (QSAs) conduct reviews of payment applications
  - PA-DSS simplifies PCI-DSS certification
- Issues
  - Notification of vulnerability
  - …and what PCI could do with information
- Newer requirements are less draconian

Another Example…

- NIST Special Publication 800-160 (Systems Security Engineering)
- Request for “assurance artifacts”
  - Core intellectual property?
  - Development needs aren’t “standard” needs
- Root cause analysis of defects
  - Impractical at scale
  - Focused triage/deep dive?
- Security functions should monitor threat actions and sources
  - How to make applications “threat-aware and self defending?”

What To Do, What to Do…

No Man Is An Island

- Consult others to understand "broader picture"
  - Employer "position" on X
  - Other implications?
  - Look before leaping!
- Potential allies
  - Legal department, government relations…
  - Trade associations (e.g., Information Technology Association of America (ITAA))
  - Associations of security professionals (e.g., Information Systems Security Association (ISSA))
- "Practitioners' voices" are *critical!*

Weighing In


COMPLAINTS
CARTOONSTOCK.com
"It has to be something specific, sir — You can't just stand there and groan."

Kvetching 101 – How to “Express Concern”

- Be specific!
  - What is the problem?
  - Why is it a problem?
  - What might fix it?
- Are key terms defined?
- Is it leverageable?
- Be polite!

Kvetching 101 (cont'd)

- Describe "potential unfortunate, unintended consequences"
- Especially economic ones …
  - Suboptimal resource allocation
  - Regulatory capture
  - Crowding out effect
  - Opportunity cost
  - Costs of compliance vs. benefits
- React *positively* to *positive* proposals

Constructive Comments Example

- *Page B-12 Security Risk Assessment*
- *"Process and associated techniques to identify: (i) threats to the operations, information, systems, assets, and individuals of the organization; (ii) vulnerabilities associated with the operations, information, systems, assets, and individuals associated with the organization; (iii) consequences/impact to the mission/business should a threat successfully exploit a vulnerability; and (iv) the likelihood that a specific vulnerability will be exploited and a threat will be realized. "*
- Comment: For COTS, vulnerabilities found during the initial development process tend to be triaged and fixed prior to product release or service delivery. However, many vulnerabilities may be found later since the use of static and dynamic analysis tools is difficult and often has a very high rate of false positives. It is reasonable to validate that a supplier has a reasonable method for looking for security vulnerabilities and triaging them (e.g., via use of CVSS base score). However, customers do not get access to vulnerability details (to do detailed analysis) because COTS vendors typically only provide a standardized amount of information on vulnerabilities to all customers, at the same time, typically with patch availability.

Last Thoughts…

- “You don’t ask you don’t get!”
- Find common ground *and common language*
- Try to be constructive, not destructive
- Point out larger issues

Questions?