RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: CXO-R04

When Will InfoSec Grow Up?

MODERATOR:

John D Johnson

Global Security Strategist
John Deere
@johndjohnson

PANELISTS:

Alex Hutton

VP of Information Security
A Large Financial Institution
@alexhutton

David Mortman

Chief Security Architect
Dell
@mortman

Jack Jones

President
CXOWARE, Inc.
@jonesFAIRiq

Questions

- Why does InfoSec need to grow up?
  - How do threats, regulations and business opportunities demand it?
  - What obstacles must we overcome?
  - How can we all get on the same page with foundational terminology?
- Do we need to be thinking more about risk (vs. Opsec)?
  - How do we improve our (mental and formal) models?
  - How can we treat the risk landscape as a system, learning from Root Cause Analysis?
  - How should we approach metrics to support good risk management? Especially in light of social, mobile, cloud, CoIT, IoT, etc.?
- Looking back and looking forward: predictions for the future

Viewpoint

(Evolve To Become The 2018 CISO Or Face Extinction, Andrew Rose, Forrester Research, Inc. (8/20/14))

- Preconceptions And An Addiction To Operations Draw Attention Away From Key Areas
  - Security leaders still tend to focus on technology
  - Security managers love the thrill of operational emergencies
  - S&R peer groups still value the CISSP above an MBA
- The Increasing Criticality of Information Will Lead To A Consolidation Of Roles
  - The CISO will become a privacy champion
  - All of IT compliance will come under the CISO's jurisdiction
  - Data governance will underpin the CISO's information risk practices
- Conclusion: CISO evolves into CIRO

Questions

- Why does InfoSec need to grow up?
  - How do threats, regulations and business opportunities demand it?
  - What obstacles must we overcome?
  - How can we all get on the same page with foundational terminology?
- Do we need to be thinking more about risk (vs. Opsec)?
  - How do we improve our (mental and formal) models?
  - How can we treat the risk landscape as a system, learning from Root Cause Analysis?
  - How should we approach metrics to support good risk management? Especially in light of social, mobile, cloud, CoIT, IoT, etc.?
- Looking back and looking forward: predictions for the future

Review

- Standardized nomenclature
- Recognition that controls != risk
  We need to improve our (mental and formal) models
- Recognition that the risk landscape is a system
  How much risk we have today is a lagging indicator of how we've managed risk in the past (thru decisions and execution). Learning from effective root cause analysis is critical to improvement.
- Controls are necessary but not sufficient
- Monitor & Measure
- Empathy not attitude

Apply What You Have Learned

- Awareness of the problems
  (awareness that you have a problem is, after all, the first step)
- Awareness of different options for addressing the problems
  (resources, pros/cons)
- Metrics are super important
- Don't put too much import on CVSS or out of the box SIEM
  (vuln scores don't express risk without context)
- Steps they can take:
  - Simple ways to evaluate what their organization is doing well/poorly on these issues
  - Simple steps for influencing change in their organizations
    (e.g., facilitating internal discussion/adjustments)
  - Security leadership is needed! Develop your skills and plan for the future!