

# Compliance: The Enterprise Vulnerability Roadmap

...

Weasel

Nomad Mobile Research Centre

[weasel@nmrc.org](mailto:weasel@nmrc.org)





# Introduction

# The Semi-Security State of Compliance

- Overview of Compliance Benefits and Standards
- Things Compliance Gets Wrong
- Detrimental effects of Compliance

# Compliance Benefits

- Old, hard-to-sell controls finally being implemented
- Standardization of common controls
- Credentials for lazy people who don't want to work or go to school (OK, so that's not a benefit...)

# Compliance Standards

- COBIT
- PCI DSS
- HIPAA

# Compliance Standards (Cont)

- GLBA
- SOX
- ISO
- ITAF

# The Psychological Impact of Compliance on the Enterprise

- False Senses of Security
- Misinterpretations of concepts
- Budgetary and Resource Shifting and Mayhem
- The “Pass the Audit” vs. “Secure the Systems” Paradox

# Compliance brings us a new fingerprinting foundation

- Standards == Defined Attack Matrix
  - Passwords (length, complexity, age, etc), Data Retention, Encryption Standards, Focal Points
- Data retention
  - What data is known to exist before it is even found
- Configuration Management
  - Workstation, Server, Data Centers, Infrastructures
- Policy
  - Policy-level weaknesses and vulnerabilities

# Other Standardizations

- Encryption requirements
  - standard algorithms
    - No time wasted forcing non-compliant algorithms
  - sensitive data flagging
    - Encryption flags the “juicy stuff”
  - Key management

# Compliance is the Self-Devouring Serpent

- Misrepresented/Misinterpreted Postures
- Conflict of Interests
- Governance Hypocrisies
- "Secure" vs. "Passing Audit" paradox
- Things you may not have known about compliance boards

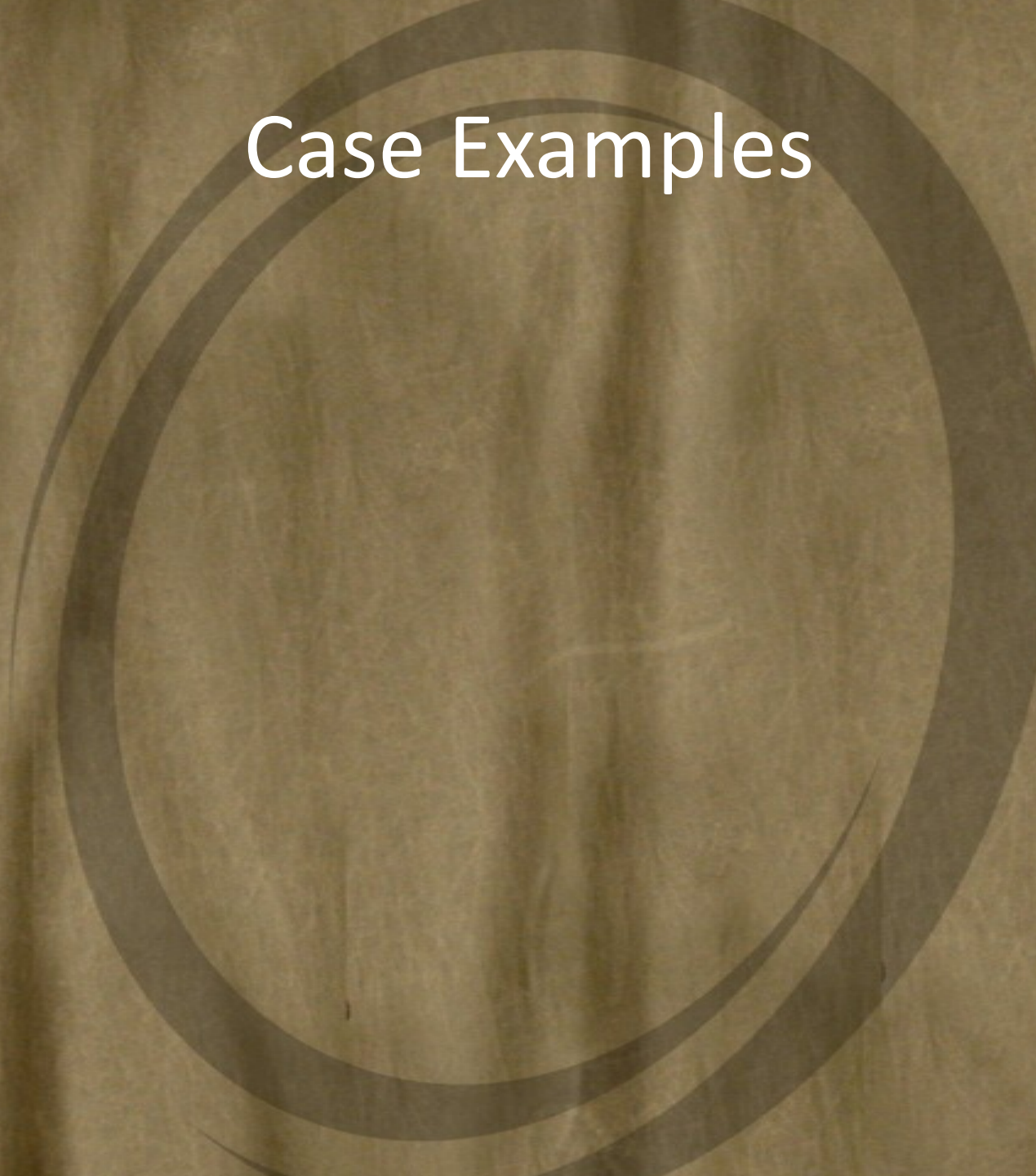
# The Anti-Progression Trap

- Compliancy can lock organizations into “old” technologies and architectures
  - Requiring Firewalls where emerging concepts don’t call for one
  - “Anti-virus is Dead”


# Notes on the "Risk Bandwagon"

- Definition
- A new mentality is evolving
  - Knowing the enemy before you know who it is

# Case Examples



# Conclusion



Q&A

Credits



Links

