IMAGINE

i/+^ 2014

Data Security Concerns: Law Departments and Service Providers

Panel Discussion

Moderator:

Joseph Abrenio

VP Advisory Services & General Counsel
DeltaRisk

Panelists:

Brett Tarr	**Mike Russell**
Caesars Entertainment	*Liberty Mutual Insurance*

Thank you for being here today!

August 18, 2014

LEGAL DEPARTMENT CONCERNS

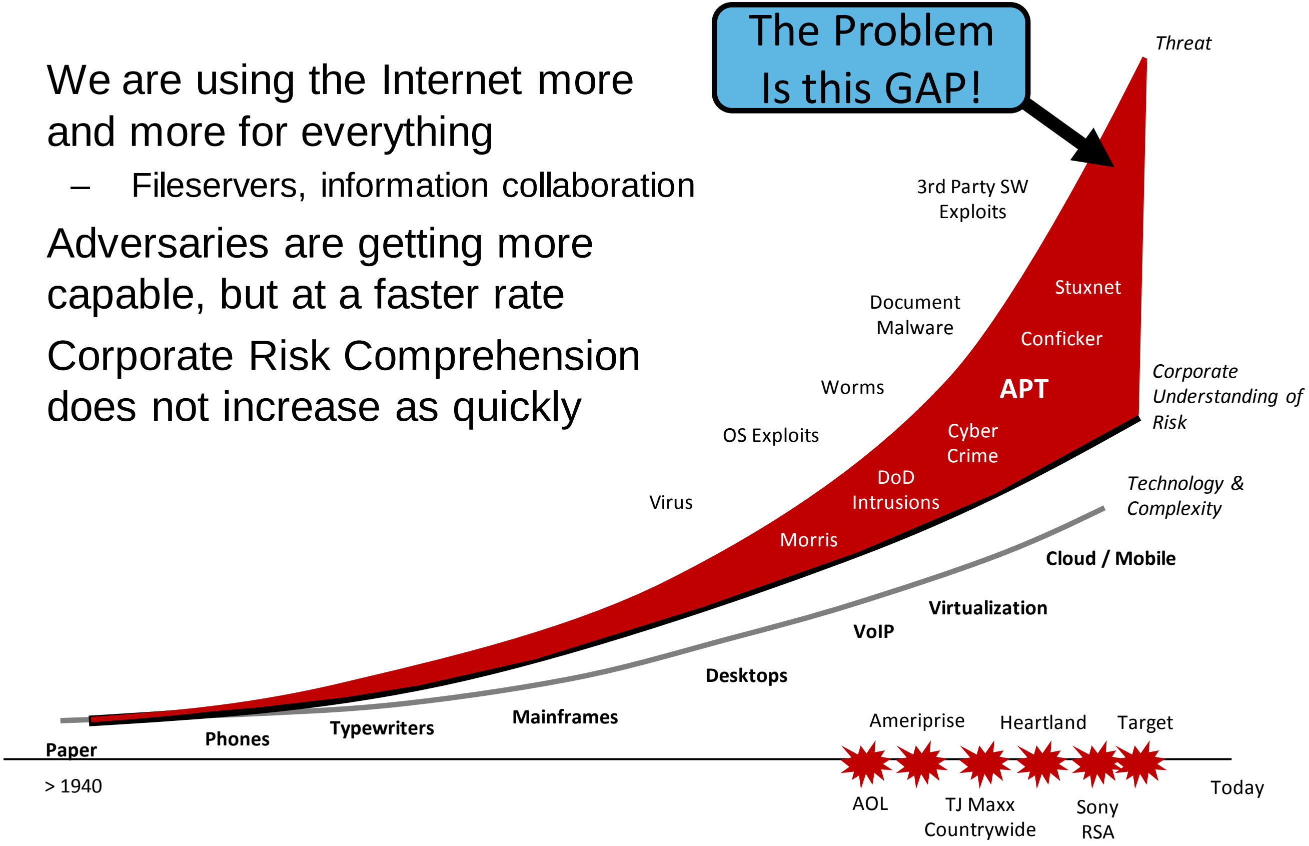
“What’s keeping the GC up at night?”

We’ve all heard the horror stories; what should we be doing to avoid one of our own?

- The Why is obvious… practical implications
- Audits – a false sense of security?
- Risk Assessments
- HIPPA & PCI
- Cloud Environments
- Q&A - takeaways

Evolution of Cyber Threat

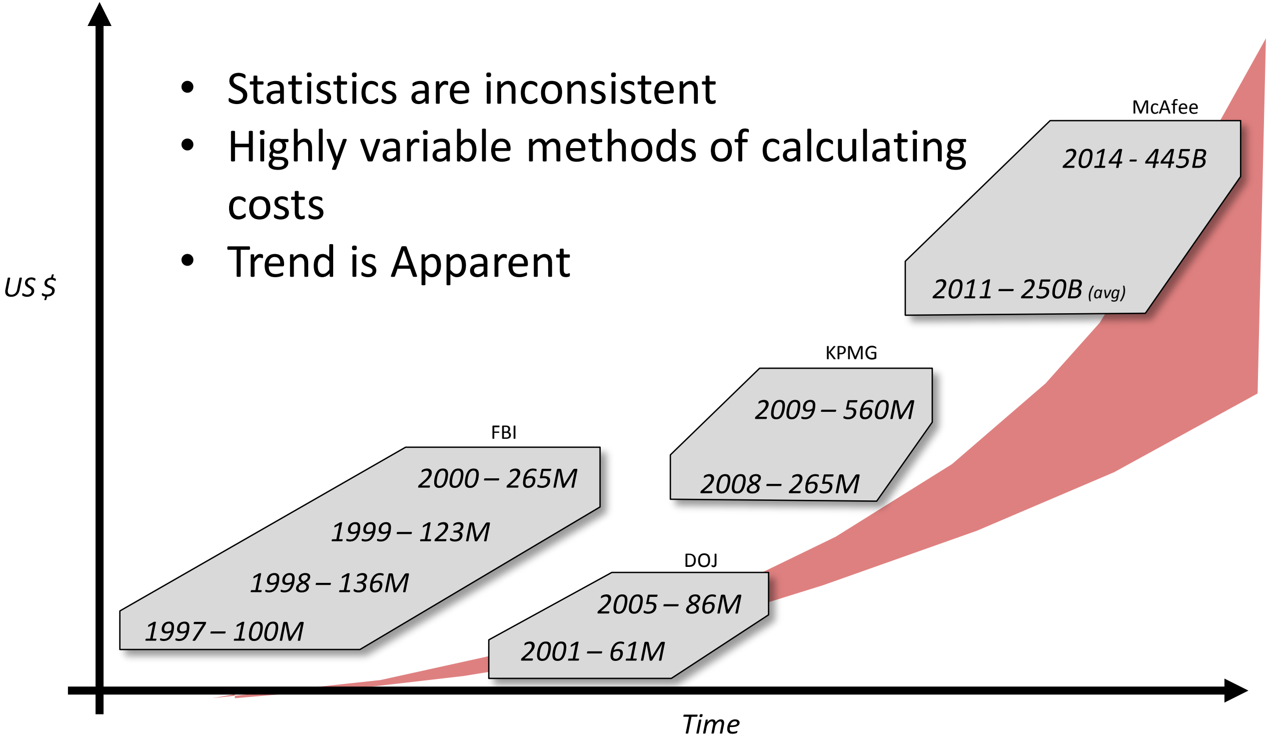
- We are using the Internet more and more for everything
  - Fileservers, information collaboration
- Adversaries are getting more capable, but at a faster rate
- Corporate Risk Comprehension does not increase as quickly



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

The Rising Costs of Cyber Crime

- Statistics are inconsistent
- Highly variable methods of calculating costs
- Trend is Apparent



Effective Security Operations Programs

- Building an effective security program requires an executive agent to commit to two areas:

Strategy

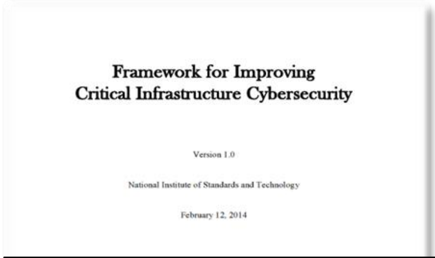
- Develop organization-wide security strategy or framework
- Define relevant, current and emergent threats to business
- Understand current security operations and process maturity
- Define and implement needed levels of information asset protection
- Educate and inform executive / board level decision making

Operations

- Organize people, process and technology to meet threats
- Conduct monitoring, detection, analysis, and response activities
- Find and address vulnerabilities
- Meet compliance and regulatory requirements and standards
- Perform audit functions

The NIST Framework - Intent

- Framework for Improving Critical Infrastructure Cybersecurity
  - Despite the name, applicable to any organization or business
- A voluntary, risk-based approach to manage cybersecurity risk, in a cost-effective way, based on business needs
- The framework is not regulation
  - There is no compliance requirement

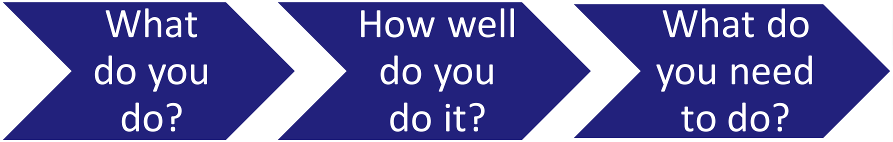


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014



It's about MANAGING RISKS and making APPROPRIATE INVESTMENTS in cybersecurity efforts

KEY SECURITY ISSUES TO CONSIDER

- Are law firms & vendors vetted for security?
  - If so, who is responsible for managing this process?
  - How are new vendor requests identified and communicated to responsible party?
  - What is the process for requesting/evaluating information from vendors and law firms?
  - Is there an established timeline SLA for approvals?
  - What types of security issues need to be considered?

For Organizations with Clients in Banking/Healthcare Industry

- What experience do you have dealing with highly confidential data, PII, PCI, PHI ?

- What level of security vetting has been performed for any subcontractors you have or plan to use?

- Does your organization manage/handle/store/process HIPAA/HITECH related data

- Have you undertaken any specific efforts to comply with the new regulations around HIPAA & HITECH?

- Is your organization considered a business associate?

- Have you undertaken efforts to achieve PCI Compliance?

Personally Identifiable Information

- What special efforts are utilized to manage communication of PII?
- Data encryption in transit?
- Data encryption at rest?
- Secured email systems that password encrypt data files/attachments?
- Limitations on sending key PII data (social security numbers, bank account numbers) via regular email?
- Confidentiality agreements
- Conflict check/management

Open Forum

We'll now open it up…

Thank You!

Please Complete your Session Evaluations – Feedback is a gift!

IMAGINE

2014