
Cyber Security Integration into PM Methodology

Doug Ascoli – Ameren

Liz Lahm – Ameren

Bruce Tons - Rabo AgriFinance

Do these look familiar ?

How are they similar ?

❑ Super Bowl 2013

Baltimore Ravens versus
San Francisco 49ers



❑ Toyota Prius



Definitions

- ❑ Cyber security - the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
- ❑ Hacker - a term used by some to mean "a clever programmer" and by others, especially those in popular media, to mean "someone who tries to break into computer systems."
- ❑ Cracker - someone who attempts to crack someone else's system or otherwise uses programming or expert knowledge to act maliciously

Cyber Security Regulations

- Cyber Security Act 2012
 - A bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States – Not passed

- Cyber Security Act 2013
 - A bill to provide for an ongoing, voluntary public-private partnership to improve cyber security, and to strengthen cyber security research and development, workforce development and education, and public awareness and preparedness, and for other purposes - Pending

Cyber Security Impacts

- Ensuring cyber security requires coordinated efforts throughout information systems.
- Impacts include:
 - Application security
 - Information security
 - Network security
 - Disaster recovery / business continuity planning
 - End-user education
- Project Management is not immune !

Cyber Security in Projects

- Types of Projects Impacted - Any scope that delivers digital technology:
 - IT Infrastructure
 - Software Applications / Web Apps
 - Plant Equipment
 - Facilities – Management systems
 - ???

Cyber Security in Projects

- Implications to project management:
 - Risk Management – security risks
 - Project Team – add Information Security
 - Scope Management - scope can be difficult to establish; can be dynamic
 - Cost Management – added cost of controls
 - Communications – protect vulnerability information

Cyber Security in Projects

- Implications to project lifecycle & cost
 - Bring Security in EARLY and include throughout lifecycle
 - Initiation Phase
 - Business Case - Total Cost of Ownership
 - Scoping
 - Sustainment plan
 - Planning Phase
 - Regulatory requirements
 - Security requirements
 - Design Phase
 - Security controls
 - Build/Test Phase and/or Post-Implementation
 - Vulnerability Tests
 - Penetration Tests

Cyber Security in Projects

- ❑ Addressing Business Risk (implications of external corporate data cyber-breach) AND business cost
 - Loss of information
 - Protecting company assets / physical damage
 - Impact to Operations
 - Impact to Physical Security

Key Issues

Evolving Scope

Regulatory Changes

- Not as specific as needed, lends itself to interpretation

Court Judgments

- What are enough layers
- What extent of monitoring
- Customer/client responsibilities and EULA

Key Issues

□ Resources

- Scarce resources that understands regulatory requirements and are kept current
- Internal Requirements to satisfy frequency of events – Daily, Weekly, Monthly, Quarterly, Annually
- Changes to core system, new products, new vendors

Key Issues

- Shortcuts
 - Internal pressure to take shortcuts
 - Place a check in the box and move-on
 - Exposure
- New threats – zero-day attacks, new attack vectors and vulnerabilities
- **How do we know if we are protected?**

Q&A

