Cyber Security and Project Planning: How to "Bake It In"

Tim Jacks, PhD, CMIS, **SIUE**

Bruce Tons, VP, Security Officer, IT Privacy Advisor, **Rabo AgriFinance**

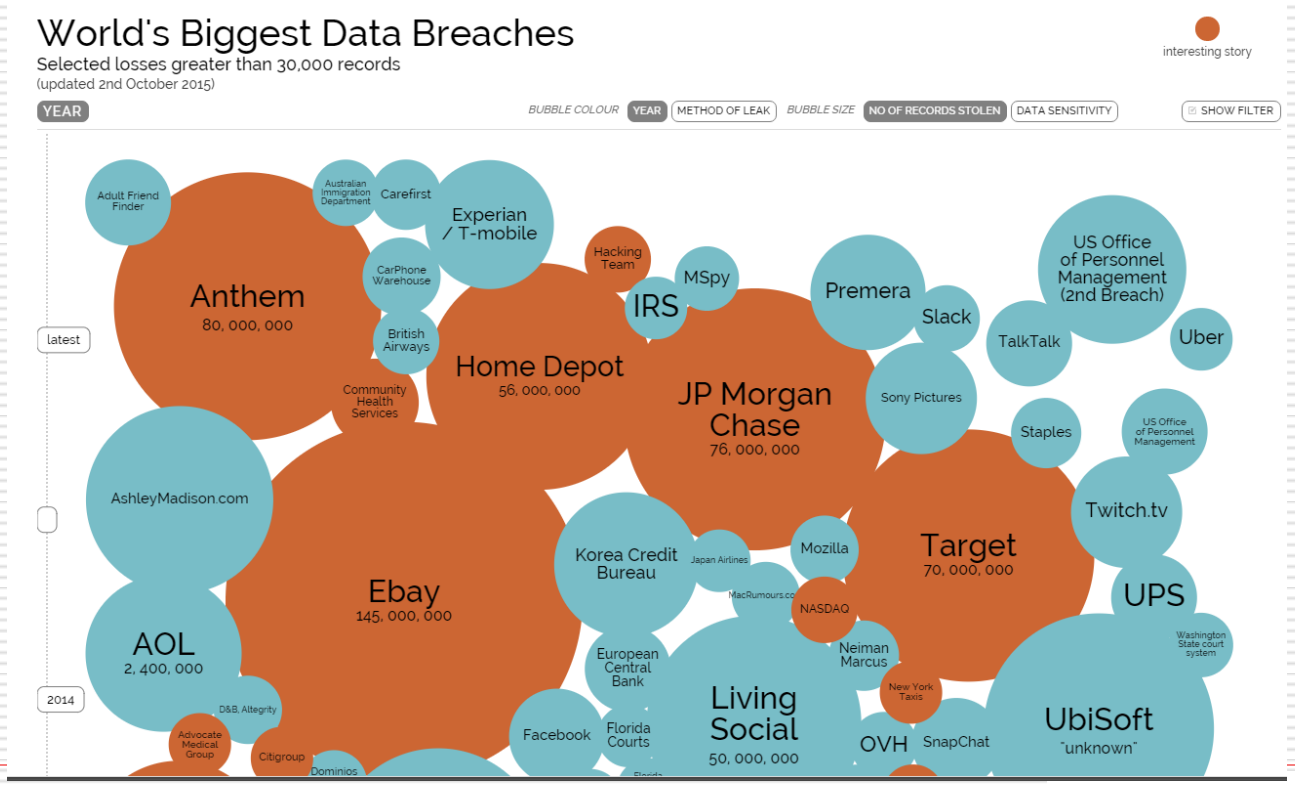
Doug Ascoli, Sr. Project Manager, **Ameren**

Tonya Munger, Sr. Mgr Manufacturing Execution Systems, **Boeing**

SOUTHERN ILLINOIS UNIVERSITY EDWARDSVILLE
SCHOOL OF BUSINESS

Why do we care?

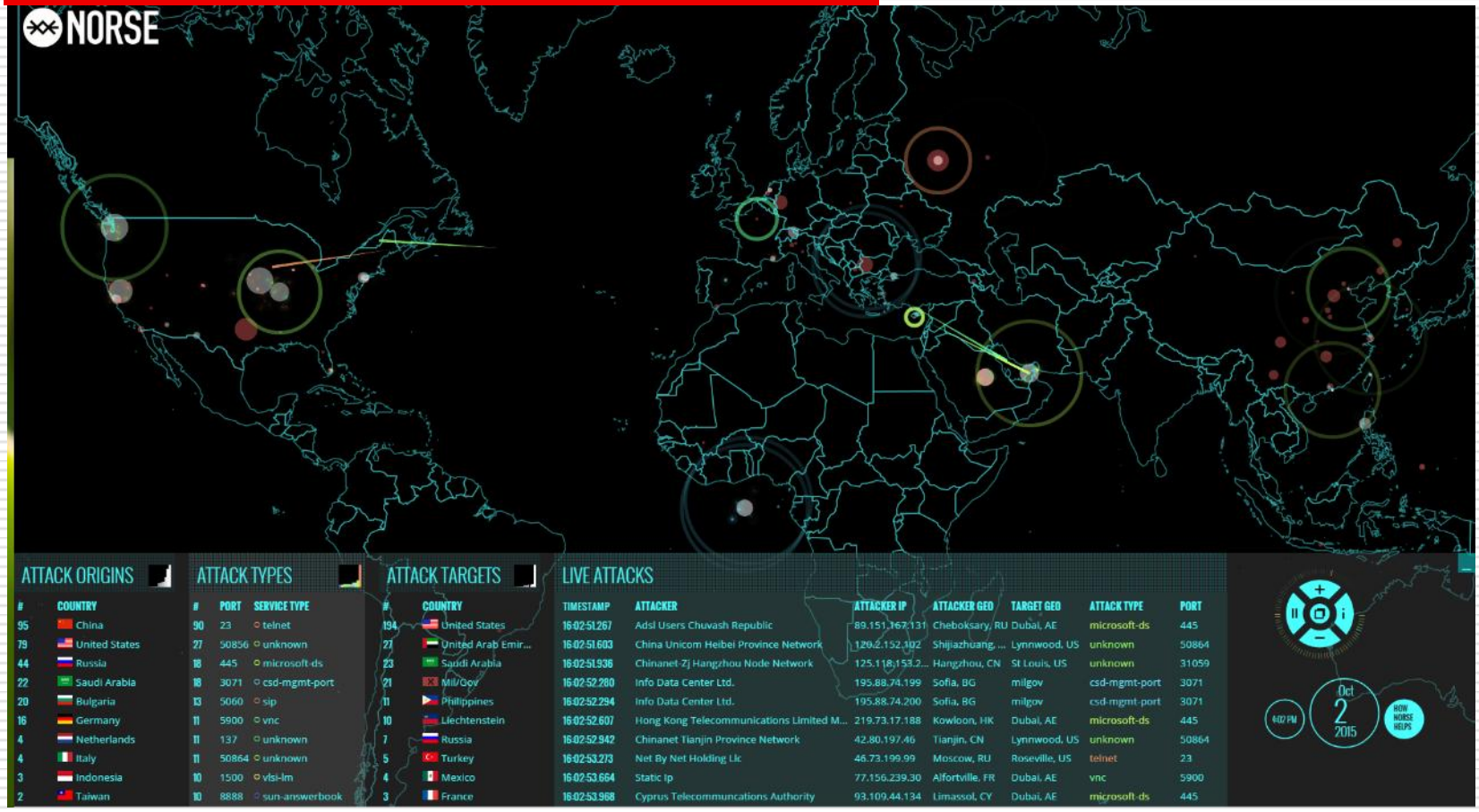
- http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Cyber Security and PM role

- PMs are not expected to be Cyber Security experts
- *"By including security considerations in every phase of a project, PMs have the opportunity to deliver more secure systems in a more secure manner." (Pruitt, 2013)*
- Is security a problem in St. Louis?

http://map.norsecorp.com/



How can PM's "bake it in"?

- Ensure these 10 ingredients are baked into your project plan!

Preview of 10 ingredients

1. Operational handoff
2. Security Impact Analysis
3. Know your data
4. Secure communications
5. Risk management
6. Access management
7. Questions for vendors
8. Weakest link
9. Becoming a "top chef"
10. Sharing lessons learned

#1 Plan for a great operational handoff!

- Minimize last minute security fixes and oops's
- Invite security to the party early, not late.
- Get your firm's Operational Acceptance Testing checklist ahead of time and bake it in from the beginning of the project!
- Be a superhero! ☺

#2 Do a security impact analysis

- Determine the value of information to the firm
- Determine costs of preventative measures and costs of failure
  - Average firm cost of responding to a data breach = $4.5 million in the U.S.
  - Average damage to firm reputation = $3 million in the U.S.
- www.ponemon.org
- Include your Security Department in your planning meetings

#3 Know and Protect your Data

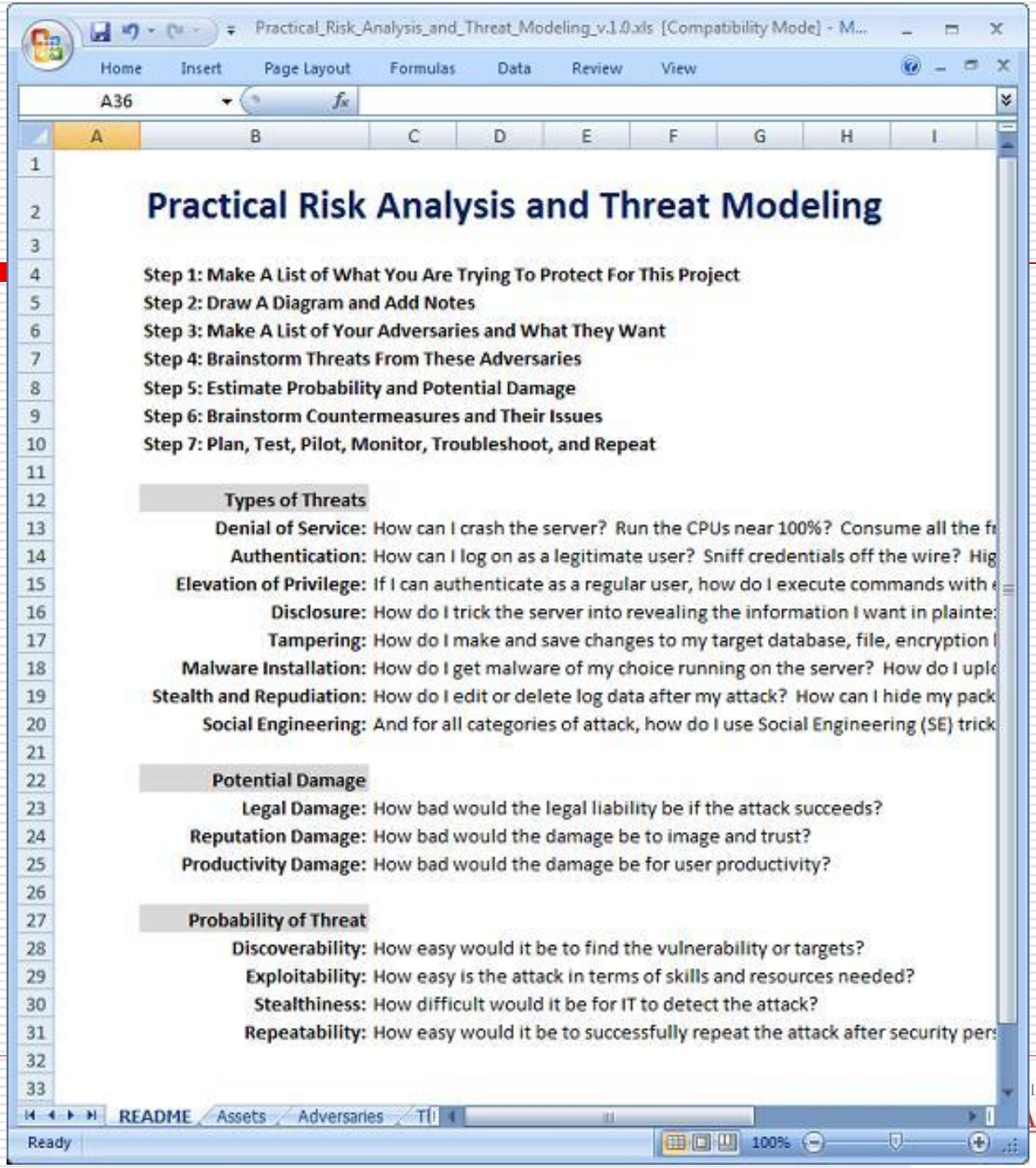
- Any external regulatory/ compliance concerns? Any internal?
- Examples of protected data: healthcare, financial, military, government, personal, proprietary, social security #, credit card #, international, employee, grades, etc.
- The PM may not know the answers but has to ask the right questions and include others

#4 Plan for secure communications

- Communications plan + security = secure communications
  - PMBOK says "Communication has been identified as one of the single biggest reasons for project success or failure."
- Communications Plan needs to include how to secure the following:
  - Online project documentation, passwords for conference calls, email, IM, backups, printed documents, configuration documentation (F/W, VPN, outbound email, thumb drives)
  - Are you guarding your "keys to the kingdom" or "Crown Jewels"?

#5 Plan for risk management

- Different from impact analysis
  - What are the *likely* risks
- Option #1 Use internal checklist
- Option #2 Use NIST risk management framework http://csrc.nist.gov/groups/SMA/fisma/framework.html
- Option #3 Use SANS "Practical Risk Analysis and Threat Modeling Spreadsheet"



#6 Plan for authentication and access management

- Who / what / where /when / how for access
- Does it tie into A.D. for authentication?
- Role-based security
- Who's the business owner for ongoing access approval? Recertification? Frequency?
- Remote access?
- Tonya's example
  - Prod/test/dev environments

#7 Ask your vendors the right questions

- It's not <u>just</u> about price and service quality.
- *"The vendor should provide verifiable evidence that data is secure on their infrastructure like security certifications that require audits of their practices with respect to NIST and FISMA [standards] by accredited organizations like Logyx and Veris group, or via STAR or FedRAMP certs." (Pruitt, 2013)*

- External SLA's with penalties
- Right to audit
- Escalation procedures
  - Timeliness in the event of a breach
  - Communication Plan
- Review their DR plan
- Participate in their DR exercise; and vice versa
- Right to visit premises
- Understand their due diligence on their outside vendors and contractors
- Cloud usage
- Where is data stored?

#8 Plan for the weakest link in security…

- …and make sure it's not YOU or someone on your project team
- Data leakage from PM's specifically
  - PM's traveling abroad
  - Using public WiFi
  - Lost laptops, smart phones
    - use security cable and don't check your laptop
  - Written or weak passwords
- http://www.securingthehuman.org/resources
- Utilize a SETA (Security, Education, Training & Awareness) program.

#9 Become a top chef with secret recipes

- Example handouts
  - SANS Institute "Security Best Practices for IT Project Managers
    - top 20 controls
    - IT Project Security Checklist
  - SecSDLC
  - PWC Cybercrime survey

See handouts

Task Name
IT Project - Security Milestones
Initiating
Develop project charter.
Security impact assessment completed.
Planning
Develop project management plan.
Secure communications plan completed.
Collect requirements.
Security requirements collected.
Executing
Develop project team.
Security training completed.
Operational Handoff
Security responsibility transferred.
Closing
Security Lessons Learned recorded.

Figure 1-1 Example project security plan milestones or checkpoints.

Phases	Steps common to both the systems development life cycle and the security systems development life cycle	Steps unique to the security systems development life cycle
Phase 1: Investigation	• Outline project scope and goals • Estimate costs • Evaluate existing resources • Analyze feasibility	• Management defines project processes and goals and documents these in the program security policy
Phase 2: Analysis	• Assess current system against plan developed in Phase 1 • Develop preliminary system requirements • Study integration of new system with existing system • Document findings and update feasibility analysis	• Analyze existing security policies and programs • Analyze current threats and controls • Examine legal issues • Perform risk analysis
Phase 3: Logical Design	• Assess current business needs against plan developed in Phase 2 • Select applications, data support and structures • Generate multiple solutions for consideration • Document findings and update feasibility analysis	• Develop security blueprint • Plan incident response actions • Plan business response to disaster • Determine feasibility of continuing and/or outsourcing the project
Phase 4: Physical Design	• Select technologies to support solutions developed in Phase 3 • Select the best solution • Decide to make or buy components • Document findings and update feasibility analysis	• Select technologies needed to support security blueprint • Develop definition of successful solution • Design physical security measures to support technological solutions • Review and approve project
Phase 5: Implementation	• Develop or buy software • Order components • Document the system • Train users • Update feasibility analysis • Present system to users • Test system and review performance	• Buy or develop security solutions • At end of phase, present tested package to management for approval
Phase 6: Maintenance and Change	• Support and modify system during its useful life • Test periodically for compliance with business needs • Upgrade and patch as necessary	Constantly monitor, test, modify, update, and repair to meet changing threats

Table 1-2 SDLC and SecSDLC Phases Summary

#10 Document lessons learned and tell stories

- *"War stories can be one of the most effective ways to motivate secure behaviors and to establish a culture of security in your organization over the long-term."* (Pruitt, 2013)
- What are your stories?
- Your lessons learned?
- Q & A