



IT RISK MANAGEMENT

Mick DiGrazia

CEN Member Conference
May 10, 2013



ABOUT ME

- UConn IT Risk and Compliance Manager
- UConn IT for 15 years
- Risk management, PCI compliance, incident handling, forensic examinations, security awareness, DLP, security policy
- My contact information
 - mick.digrazia@uconn.edu
 - @yemick
 - 860-486-1336



THE NEXT 60 MINUTES

1. What risk management is
2. What risk management is not
3. Why think about risk?
4. Risk management case studies
5. UConn's risk management program
 1. Our history & outcomes
 2. Our lessons learned
 3. Our next steps

3



WHAT RISK MANAGEMENT IS...

1. Cyclical
2. Proactive
3. Pervasive
4. Strategic -> Operational
5. Mindset/Philosophy
6. Problem solving

4



WHAT RISK MANAGEMENT IS...

Three Essential Components:

- **Evaluate:** Identify your assets and evaluate their properties.
- **Assessment:** Systematically discover threats and vulnerabilities that pose risk to assets.
- **Mitigation:** Address risk by transferring, eliminating or accepting it.

5



WHAT RISK MANAGEMENT IS NOT...

1. Static (BYOD)
2. A destination
3. A firewall (or encryption, or...)
4. Elimination of all risk
5. Breach free guarantee
6. A reason to spend \$100,000 to Avoid A \$50,000 risk

After Checking Your Bank Account, Remember To Log Out, Close The Web Browser, And Throw Your Computer Into The Ocean

COMMENTARY Opinion · ISSUE 49-18 · Apr 30, 2013
By Karen Seubert, Privacy And Security Expert, Chase Bank



At Chase Bank, we recognize the value of online banking—it's quick, convenient, and available any time you need it.

Unfortunately, though, the threats posed by malware and identity theft are very real and all too common nowadays. That's why, when

Source: the onion
<http://www.Theonion.Com/articles/after-checking-your-bank-account-remember-to-log-6,32260>

6



WHY THINK ABOUT RISK?

©Cartoonbank.com



"All I'm saying is now is the time to develop the technology to deflect an asteroid."

Risk \ˈrɪsk\:

1. possibility of loss or injury
2. someone or something that creates or suggests a hazard
3. the chance of loss or the perils to the subject matter

Merriam-Webster.com

<http://www.merriam-webster.com/dictionary/risks>

7



WHY THINK ABOUT RISK?

- It's not all bad - there may be opportunity in risk
- Helps prioritize, gain support for your initiatives
- It exists, even if you don't acknowledge it
- You have important data to protect!
- Find risks before your adversaries do

8



RISK MANAGEMENT CASE STUDIES

- Server administrator places low priority on patching servers, leaving servers unpatched for several years
- IT organization forgoes upgrade of important reporting system due to high expense. Legacy server requires older operating system and web server
- IT security implements strong password controls, encryption, firewalls, standards, policies, and logging. Security awareness is not prioritized over these technical initiatives.

9



RISK MANAGEMENT CASE STUDIES

- Business unit refuses to fund upgrade of application, causing legacy database dependency. Database contains PII (of course!)
- Project management is a priority – schedule, scope, and budget are critical. Applications are moved to production before security testing is complete
- Firewall rules are overly permissive, allowing server administrators, application developers, and users access system components “easily”

10



RISK MANAGEMENT CASE STUDIES

What do these cases have in common?

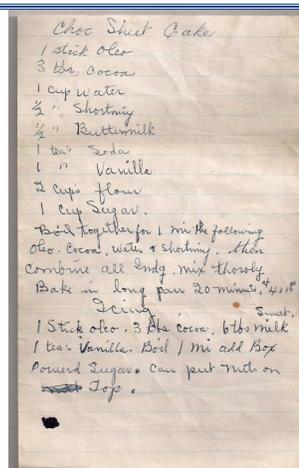
- Risk mitigation decisions put in the wrong place
- Risk decisions were made by indecision
- Security concerns outweighed by convenience, speed, or resource constraints
- I have a personal connection with each of them!

11



RISK MANAGEMENT CASE STUDIES

More Familiar...



12



UConn's RISK MANAGEMENT PROGRAM

From humble beginnings...

- Regular incidents, data breaches, & system compromises throughout the years
- 2012 breaches were a turning point – we need to pay closer attention to the infrastructure
- Vulnerability management, php applications, poor data management practices, legacy systems & configurations, standardization
- Support of CSO, CIO, and Provost!

13



UConn's RISK MANAGEMENT PROGRAM

What we've accomplished since October 2012

- 90% reduction in vulnerabilities with CVSS score 7-10
- 85% reduction in vulnerabilities with CVSS score 4-7
- 65 servers decommissioned
- 20% of total servers were on legacy OS – upgrade/migration almost complete
- Systematic system upgrades and compensating controls

14



UConn's RISK MANAGEMENT PROGRAM

What we've accomplished since October 2012

- Windows & Linux hardening standards developed (collaboratively!)
- Logging standard created
- Patch management policy created
- **Risk Management Advisory Counsel** meeting weekly – policy exceptions, documentation, standards reviewed & approved

15



UConn's RISK MANAGEMENT PROGRAM

What we've learned since October 2012

- We know where our PII is located
- We know which systems are “critical”
- We know which systems have (severe) vulnerabilities
- Together this gives us a good picture of the environment

16



UConn's RISK MANAGEMENT PROGRAM

What was different this time?

- Provost was invested
- IT management was invested – weekly dashboards and meetings. They owned the resource issues and accommodated getting the work done.
- Server administrators don't want another breach or outage!
- Patching became part of job performance

17



UConn's RISK MANAGEMENT PROGRAM

What have we learned so far?

- Reporting properly to management is essential
- Reporting properly to system administrators is essential
- Doing this right takes resources, commitment, time, effort, and long-term view

18

 **UConn's RISK MANAGEMENT PROGRAM**

Where we need to go



- Application vulnerability assessments
- Server/application vulnerability assessments for distributed IT systems
- Improved security awareness
- Risk assessment service/procedures

19

 **UConn's RISK MANAGEMENT PROGRAM**

Where We Need To Go



20



HOW CAN YOU GET STARTED?

Slow & Steady...

- Inventory systems
- Perform a risk assessment

⊕ Risk analysis worksheet (Range of 0.0 to 1.0 for P and I)

| Threat | Probability (P) | Impact (I) | Risk = P x I |
|---------------------------------------|-----------------|------------|--------------|
| IT – Viruses | | | |
| IT – Hacking, Unauthorized Intrusions | | | |
| IT – Hardware | | | |
| Flooding – Internal | | | |

- Involve administrators – provide proactive reports and get input & buy in

21



HOW CAN YOU GET STARTED?

Next steps

- Establish roles, responsibilities, levels of authority
- Understand service criticality & data sensitivity
- Allow community to report risks and you prioritize against risk repository (Excel)
- Security awareness training
- Appropriate Use Policy & other security policies

22



HOW CAN YOU GET STARTED?

Vulnerability management

- Regular vulnerability scans
 - Nessus subscription - \$1,500/year
- Reports for sysadmins
- Reports for administration

23



STAY IN TOUCH

mick.digrazia@uconn.edu

@yemick

860-486-1336

<http://security.uconn.edu>

24