

Anatomy of The Security Disaster

Marcus J. Ranum

CSO

Tenable Network Security, Inc.

The Security Disaster

- What is the problem?
 - Dangerous stuff is being done by people who think it is being done safely
 - Their incomprehension of the danger encourages increased exposure (the “it hasn’t happened yet” effect)
- We are at the point where cyberterror starts to become a legitimate fear

The Future

- “It's a problem for security people because their career depends on their ability to enable the business securely. We have had six years of "regulation-based job security" for the whiners. That era is coming to an end.”

Alan Paller, SANS

The Security Disaster

- In other words, the problem is going to get worse
- What is scary is the existing scope of the problem is already very broad; the current state of affairs has been gestating for 10+ years

What Will We Do?

(that will not work)

- Spend our way out of the hole
 - Cost of doing it right exceeds cost of re-doing it
 - Currently an installed base of doing it wrong
 - Inertia (financial and technological)

...in other words: we're already so deep into this that physics has taken over

Do We Learn?

- Do pro-active measures actually carry weight?
- Disaster-and-patch is the current strategy

Time Line of a Typical Disaster

1) Inception of bad idea

2) Identification as bad idea

3) Negotiation

4) Search for Plan B

5) Failure to re-adjust expectations

6) Initial failure conditions are noticed

7) Denial or kludging

8) **Failure**

2.2) Memos
generated!

6.2) Memos
generated!

Opportunity for
cover-up or
conspiracy

Time Line of a Typical Disaster

(cont)

9) Hunt for the guilty

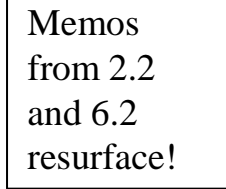
10) Finger Pointing

11) Memo Archaeology

12) Slaughter of the Innocents

13) Failure to learn

REPEAT



Memos
from 2.2
and 6.2
resurface!

Failure of Risk Management

- The premise of the “risk management” approach to security is that good thinking happens at stage #3
 - In fact, what happens is that the good thinking is largely *undone* by the time you get to stage #7
- Every organization that is performing “risk management” is currently in denial

Failure of Communication

- The premise of the “improved communication” approach to security is that good thinking happens at stage #2, #4, #6, and #7
 - That’s simply expecting too much good thinking to happen

Failure of Education

- The premise of the “educate the manager, educate the business” approach to security is the same as the “communication” idea except for the assumption that the right thing is just going to happen organically
 - That’s utter fantasy

Failure of Legislation

- The legislative approach (what is being most widely attempted right now) relies on publicly identifying organizations that have failed at stage #8 and *hoping that organizations that are already at stage #7 are going to somehow magically wind back the clock to stage #3*
 - Will always be seen as prohibitively expensive

Economic Models

- A popular fad nowadays is “economic models” of security
 - Essentially the attempt to correctly place security in the value chain
 - This almost always results in security being given a high presumed value and low cost (a nice way of saying, “highly fudged”)
 - Even so, security is a “market failure”

Epic Failures

- When failures occur, someone has to take the blame
 - Standard failure mode is management states “I take full responsibility”
 - ...but someone else takes the fall
 - In US DOD gov’t space that is virtually always a contractor (because it’s only contractors that actually *do* anything)

But let’s look closer at what’s happening...

The Middle Layer

- Discussion with a notable “CTO/CSO rountable” member
 - Security has to enable the business process
 - In *cases where failures occur it is discovered that technologists lied about how safe systems were*
- Reveals profound disconnect between what management thinks, and reality
 - This should not be news to most of you

The Middle Layer (cont)

- My observation in return was that:
 - The technologists told the truth; it's simply that management didn't hear the truth
 - Management remembers *what it asked for* not *reality*
 - Sometimes, sandwiched in the middle, is a layer of middle management
 - Result is a massive disconnect between management expectations and ground reality

The Plan A Plan B Effect

- Management asks for “(something dumb) with perfect security”
 - Technology answers “it can’t be done”
- Management then asks for “Plan B”
 - Continues shopping the idea until someone cooks up something that will mostly work

Expectation Level

- The problem is that the expectation level does not get reset in this process
 - Management simply continues to forge ahead with the idea that “perfect security” is going to be part of the equation
 - Meanwhile there are memos from technologists that say (variously) “We can do it, but there are substantial risks...”

The Space Shuttle Disasters

- The quintessential example of this kind of failure paradigm is summarized by Richard Feynman in his minority report about the Challenger disaster
 - Feynman was dead when the Columbia broke up, but the failure paradigm in the Columbia disaster was *exactly* the same
- We consistently see fundamental disconnects between expectation and reality

Breaking the Cycle

- What can we do?
 - Ensure maximum clarity at all parts of stage #2, #3, #4, #5
 - Pre-allocate blame at stage #7 and #8
- Technical / responsible individuals *must* make sure to document that they issued warnings in stage #8
 - And, if you actually want things to get better, the warnings must get high enough

Breaking the Cycle (summary)

- Key phrases:
 - “We must re-assess the decision to...”
 - “The risk estimate of regarding (blank) is optimistic...”
 - “Continuing with (blank) represents additional investment in a risky decision...”

A Grim Future

- The behaviors that I am describing are fundamental behaviors that are ingrained in human optimism
 - If I am correct, virtually all of the work that is currently being done to bring systems into compliance with regulations will represent wasted effort
 - Web2.0 rapid adoption includes the next tidal wave of bad ideas, and is already upon us

Understanding Failure as Complexity Increases

- I have already encountered 2 forensic/response cases in which the client had no interest in actually figuring out *what went wrong* they simply wanted to “fix it”
- Models of distributing and sharing risk make no sense when risk is “pick a number between 0% and 100%”

Summary

- After 20 years working in information security I am convinced that the situation is not only beyond repair; it is getting worse
- Have a nice day!