

15 Years in the Computer Security Industry

Marcus J. Ranum

<mjr@ranum.com>

Personal Progression: 1

- When I began working in security, I was employed by a vendor (Digital)
- I blamed vendors for security problems
 - We sold lousy code
 - We were slow to fix bugs
 - We left security out of products
 - Products were hard to install securely

Personal Progression: 2

- Then, I became a consultant
- I blamed (though I never admitted it) customers
 - They never installed software right
 - They never read the directions
 - They were more interested in *style* than *substance*
 - They made purchasing decisions based on marketing literature

Personal Progression: 3

- I became an “industry insider”¹
- I blamed the hackers
 - After all, it’s pretty obvious that they’re causing the problem, isn’t it?
 - Hackers cashing in by becoming *part* of the security industry: biting the hand that feeds them, but justifying its existence by doing so

1) What is that? I don’t know. Someone journalists listen to? They ask questions, anyhow.

Personal Progression: 4

- I lived through the “Internet Bubble”
- I blamed the nitro-fuelled venture-funded *ship it yesterday* beta-ware hype hype hype atmosphere
 - Products in perpetual beta-test
 - “Leave security out we’ll fix it later”
 - Ridiculous amounts of money spent on ridiculous marketing

Personal Progression: 5

- Then, I became an entrepreneur
- I blamed market dynamics
 - Senseless partnerships to promote incompatible technologies
 - Mega-\$\$ marketing campaigns
 - Competitive landscape with rapid shifts of alliance or merger and acquisition makes it impossible for *good* companies to survive; only *large* ones

Personal Progression: 6

- I no longer know what I am
- I realize that, at each point in my career, I was *right* about who was to blame - and they *still are* to blame
 - In other words, we are dealing with a huge problem in multiple dimensions, all of which depend on each other
 - How do you solve such a problem?

The Current State of Affairs

- With the economy on hold, expenditures on infrastructure (security is considered infrastructure) are on hold
- Stupid companies will go out of business - This is a good thing
 - Marketeers no longer have budgets
 - New opportunity for well-focused companies in the newly hype-free industry

Things That Don't Work

- Policy
- Education
- Law Enforcement
- Patching Code
- System Administration
- Disclosing Vulnerabilities
- Mergers and Acquisitions

Things That Might Work

- Systems that pick sensible defaults
- Code reviews and coding standards
- Effective and rapid non-political vendor-neutral standards processes backed by government purchases *(unicorns are equally mythical)*
- Putting all our eggs in one basket: let's all become Windows users and live or die with Windows

Things that Would Work

(but that we won't *ever* do)

- Scrap the entire software installed base and start over
- Spend a few years reconsidering how to build software-building tools (The crud we use today, Java, C++, etc, is not *good* it's *well-marketed*)
- Kill general purpose computing
- Kill system administration

Things to Look For

- If you see these, we may be moving in the right direction
 - Application Repudiation
 - Protocol Repudiation
 - Wise distribution of computing assets (e.g.: Ebay, EverQuest)
 - Software as subscription service instead of purchased goods

The Future

- Might resemble:
 - AOL ←
 - Everquest
 - Playstation
- How to *really* terrify Microsoft
 - Playstation is the *world's most popular DVD player* - over **3 million** sold
 - Write a good office automation suite, browser, and IMAP client for it

Summary

- None of this is rocket science
 - It's actually *harder* and *more complicated*
- None of this is impossible
 - It's just a matter of willpower or a recognition of a sufficiently high pain level
- Don't despair; it's not *real life* it's just the Internet
 - *We can* do without it - we have before

Thank You

“Know what sucks; avoid it”

- Chan Suh, 1996