The State of Computer Security

Marcus J. Ranum
CSO
Tenable Network Security, Inc.

Short Form

- **In 5 years, security won’t be interesting**
  - **That’s not the same as saying it’ll be a solved problem!**

Who Am I?

- Industry (?what?) analyst / curmudgeon
  - Firewall researcher/product developer late 1980s
  - VPN product designer early 1990's
  - IDS researcher / CEO of NFR mid 1990's
  - Consultant, teacher, writer, other stuff

Disclaimer

- This is an "industry" view
- Much of what I'm talking about will ripple down to the individual practitioner in the form of changes to their:
  - Budgets
  - Products to choose from
  - Leverage within the organization

This talk

- Some History
- Current State of Security
- Some Extrapolation

Some History

- **The early days of computer security:**
  - **Audit function - oversight**
  - **Mainframe usage accounting and system log analysis**
  - **Often an accounting function separate from IT**

Early Golden Age

- **The firewall and the internet**
  - **Everyone going online**
  - **Everyone getting hacked**
  - **Wild west attitude and lots of attention**
  - **Security IPOs in the mid 1990s trigger a rush of $$$ from venture community into security**

Late Golden Age

You are here

- **The worm and the pro hacker**
  - **Everyone is online**
  - **Horrible levels of vulnerability everywhere**
  - **Exposure of data and professionalization of cybercrime**
  - **Venture community pulls up stakes and leaves**
  - **Lawmakers stake out turf and arrive**

Current State of Security

- Industry Changes
- Regulatory Changes
- Technology Changes

Industry Changes

- Consolidation is everywhere
  - ISS -> IBM
  - Betrusted -> Verizon
  - RSA -> EMC2
  - IDS industry collapses into IPS (I.e.: gets bought by the firewall industry)
  - Log analysis and event management is next

Drivers

- Overinvestment to Exit in late 1990s
- VCs fund (approximately) 200 security start-ups
- Security market is (approximately) $20 billion
- Subtract Cisco, IBM, Oracle, Symantec, Microsoft, McAfee
  - Top 5 vendors account for all the industry except for about $1billion

TopHeavy

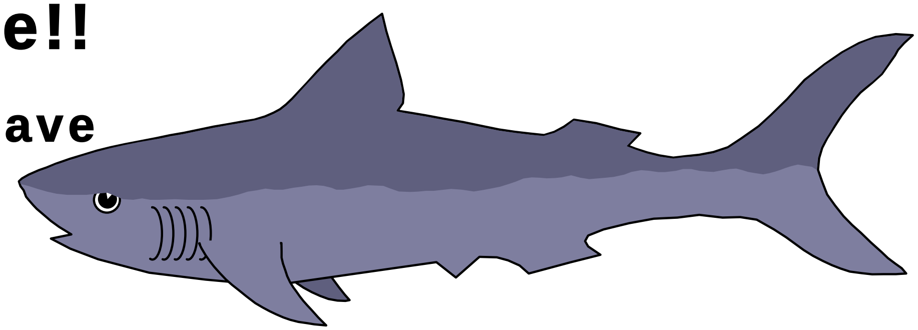
- **$1 billion divided among 190 start-ups**
  - **Not good**
  - **"That's not a market; that's a hobby" (Peter Kuper, Morgan Stanley)**
  - **Further pressure on the "little guys"**
    - **Odd to think of Checkpoint and ISS as "little guys" but really where can they go? Up-market and compete with Cisco? There *is no* down-market**

Industry Changes: Summary

- **More consolidation**
  - **It'll get frantic over the next 5 years as the industry wraps itself up**
- **More big one stop shops**
- **50% of the products you know and love today will disappear in next 10 years**
  - **The good news is, it will be worse for the ones you hate**

Regulatory Changes

- **The lawyers are here!!**
  - **Security practitioners have been asking for it "and now you got it!"**
  - **SarbOx, EU Legislation, GLBA, HIPAA, etc**
  - **Now *disclosure* regulation**
    - **Each state is heating up their own, slightly different!**



Regulation: Part 2 “The Devastation”

- **Here’s the problem**
  - **Security is on Capitol Hill’s radar screen**
  - **It’s an area where they can legislate that is populist, poorly understood, expensive, and the costs are borne by “the wealthy corporations”**
    - ***I.e.: it’s a regressive tax***
- **The amount and complexity of legislation will only increase**

Regulation: The Effect

- **Compliance dollars are being spent under guidance of liability (legal department)**
- **Compliance is going to report to legal department**
- **Security winds up (at least in part!) *competing* for budget dollars with lawyers**

Technology Changes

- **Consolidation drives integration**
- **Integration drives one-stop-shopping**
- **One-stop-shopping turns security into a clickbox feature**
- ***Hold* that thought…**

Some Extrapolation

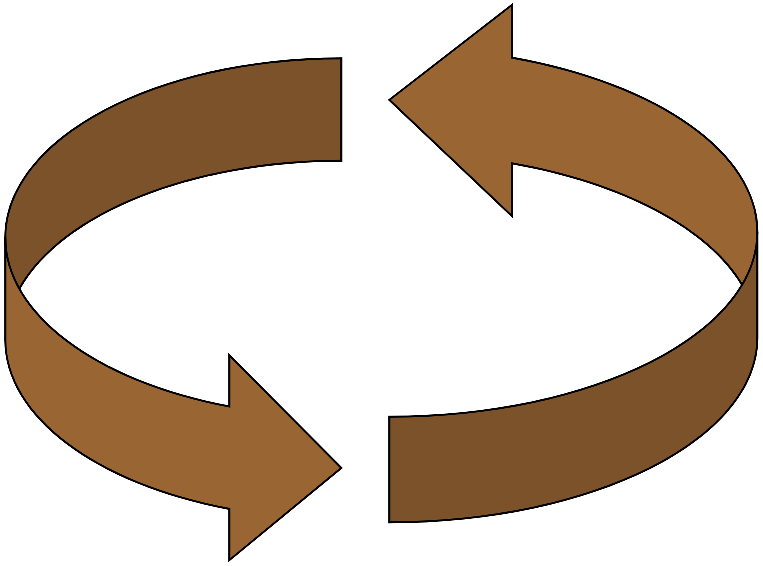
- Security gets subsumed as a “click feature” in network management
    - “Hey Bob the router guy! When you’re done with turning on the VOIP in the router, turn on the IPS security features too!”

Some Extrapolation

- **Security gets subsumed as a “click feature” in system administration**
  - **This has already largely happened in the enterprise except for website security**
  - **Patch management and antivirus *are* desktop security**
  - **System administrators will be expected to do this (along with everything else)**

Some Extrapolation

- **“Pure security” practitioners get shoehorned into audit**



My Take

- Security will become increasingly specialized and in 10 years most “pure” security practitioners will report to lawyers
- There will always be a few mercenary specialists chasing the “disaster of the day”

What's Still Hot?

- Sim / Siem pretty much works
  - That's what you'll be deploying next
  - (That market is ripe for consolidation)
- Data leakage will be next big thing
  - Prediction: Big failure, much bleeding, great sorrow
- In 5 years it'll be damage control on IP hemorrhage brought on by outsourcing

PS: I love Outsourcing

- Consider becoming a project manager to oversee outsourcing
- In 10 years you can make a fortune as a consultant being a project manager when things are “reinsourced”
- The next big area of security activity is non-technical and involves damage control for big business mistakes of early 21st century

Conclusion

- Our moment in the sun is coming to a close
  - 5 years of play left, *at most*
- Good luck!