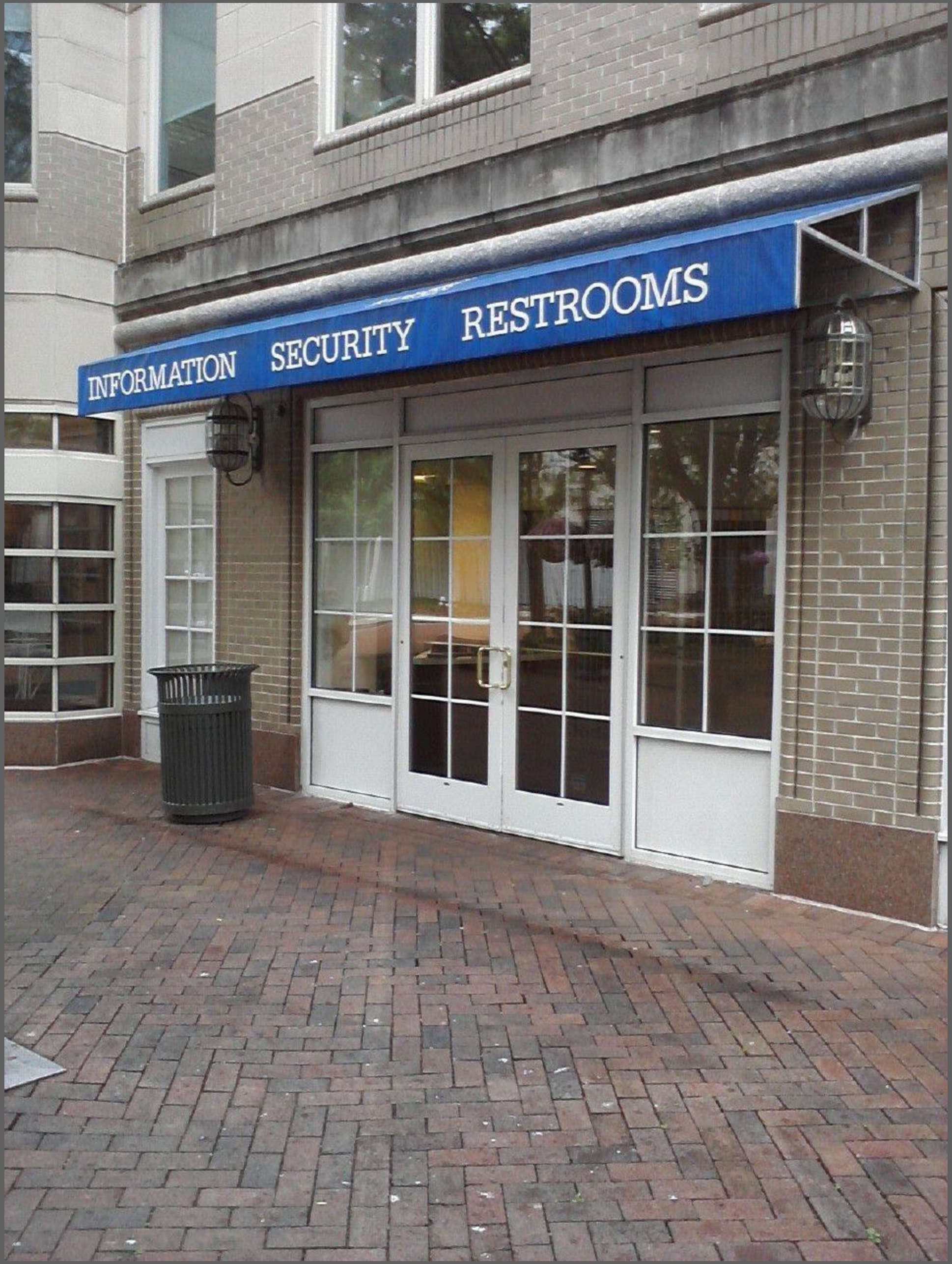
We’ve Done The Easy Stuff

Marcus J. Ranum
(mjr@tenable.com)
CSO
Tenable Network Security, Inc.



Reston, VA
last Tuesday; right across from where I ate breakfast.

They ***respect*** INFOSEC in Reston!

Warning

- When you do a lot of public speaking, your talks turn into a series of ongoing pieces of inner monologue
  - Sometimes
  - This is one of those
    - This is to explain ***why*** I am so depressed about where computer security is going

Security As Knowledge-Base

- Consider most of what we have been doing in security as knowledge-base management
  - Put another way: “You have stuff. Generally you don’t know what stuff you have, or what it does.”
  - And: “You have data. Generally you don’t know who is its custodian, or where it has propagated to.”
  - Or: “Something is wrong in a way that you don’t understand, with a piece of software you know nothing about.”

Where Have We Succeeded?

- The easy stuff

- What does that mean?
  - The stuff where knowledge-bases can be executed simply
  - And obtained by someone else

  - I.e.: Where we can remain ***ignorant***

What Does That Mean?

- Consider antivirus as:
  - Outsourcing our understanding of our runtime environment
- Consider SIM/SEIM as:
  - An exploratory tool for visually identifying outliers
  - Haystack metaphor: a SEIM automates your search for needles in a haystack
  - And what does ***that*** say about how well we understand “the hay”? Which is really the important part of the equation!

Another Possibility

- Perhaps the hay stack is mostly composed of needles

More

- Consider the “next generation firewall” as:
  - Outsourcing our understanding of what good apps and bad apps look like on a network
  - Simplifying our network access control policies even further (in search of the point where we cease to comprehend them)
    - The state of the art of home user firewalls is “this is my inside interface, everything is OK”
    - Meanwhile I’ve seen corporate firewalls with 5,000+ rules

Still More

- Consider vulnerability management as:
  - Outsourcing our understanding of the priority we should assign to fixing the horrible masses of software we run on our systems
  - System administration has become so difficult because of shifting goal-posts and releases that the cost of system administration is “unacceptable” and triggers a veto-vote called “cloud computing”

That Was the ***Easy*** Stuff

- I am not saying building a firewall, a/v system, SEIM, etc, is trivial!
  - Far from it!

- But they are tractable problems:
  - Execution/evaluation engine that drives:
  - A deep, complex, problem-specific knowledge-base

So, That’s the Set-up

- The ongoing trend since the mid 1990s has been to dumb down security in the face of exponentially increasing complexity elsewhere in IT
  - This makes sense; any other approach would break violently
  - Maybe “dumb down” isn’t the right word: we’re leveraging externally-provided knowledge-bases more and more and letting go of comprehension of local terrain

Now For Some Cheerful Ideas

The Trend is Accelerating

- “Cloud Computing” means “acknowledge that we can’t do cost-effective system administration”
  - What’s next?
  - Well, it’s sort-of also outsourcing network administration (because large-scale fault-resistant data networks are really ***hard*** to build!)
- “Mobile Devices” represent throwing our hands up in despair

The Trend is Accelerating

- App stores represent giving up controlling our runtime/software environment
  - The final stage of a trend that began in the late 1990s (aka: “the endless beta-test”)

Convergence

Noun:

The process or state of converging.

The tendency of unrelated animals and plants to evolve superficially similar characteristics under similar environmental conditions.

Convergence 2.0

- Convergence
  - As in “the freight train moving at 80mph *converged with* the car that was parked on the track.”

Compliance

- The old “new thing” in security is *compliance*
  - Consider as:
    - Outsourcing your idea of what “good security” looks like to a *committee* that knows nothing about how your organization actually works

Oh, that’s going to work.

Get More Done With Less

- 2008 financial crash coupled with cost savings offered by “cloud computing” are going to apply across-the-board pressure on staffing for IT security
  - The “golden age” of persistently spiralling IT security infrastructure ended in November 2008

  - All those knowledge-based solutions? They’re expert systems that amortize small numbers of experts across large numbers of organizations

Get More Done With Less

- Amortizing more experts across large numbers of organizations is the *only* way to keep costs down*

*This is great if you’re an expert!

High Intellectual Cost Attacks

- Dealing with a targeted attack (let alone one from a well-funded or highly motivated attacker) will quickly allow you to realize that ***all the knowledge-based expert systems everyone is building and deploying are not worth their weight in rotten bananas***
  - Sure, they may help, but only if they're being used by skilled, clued-in, motivated, creative technical people

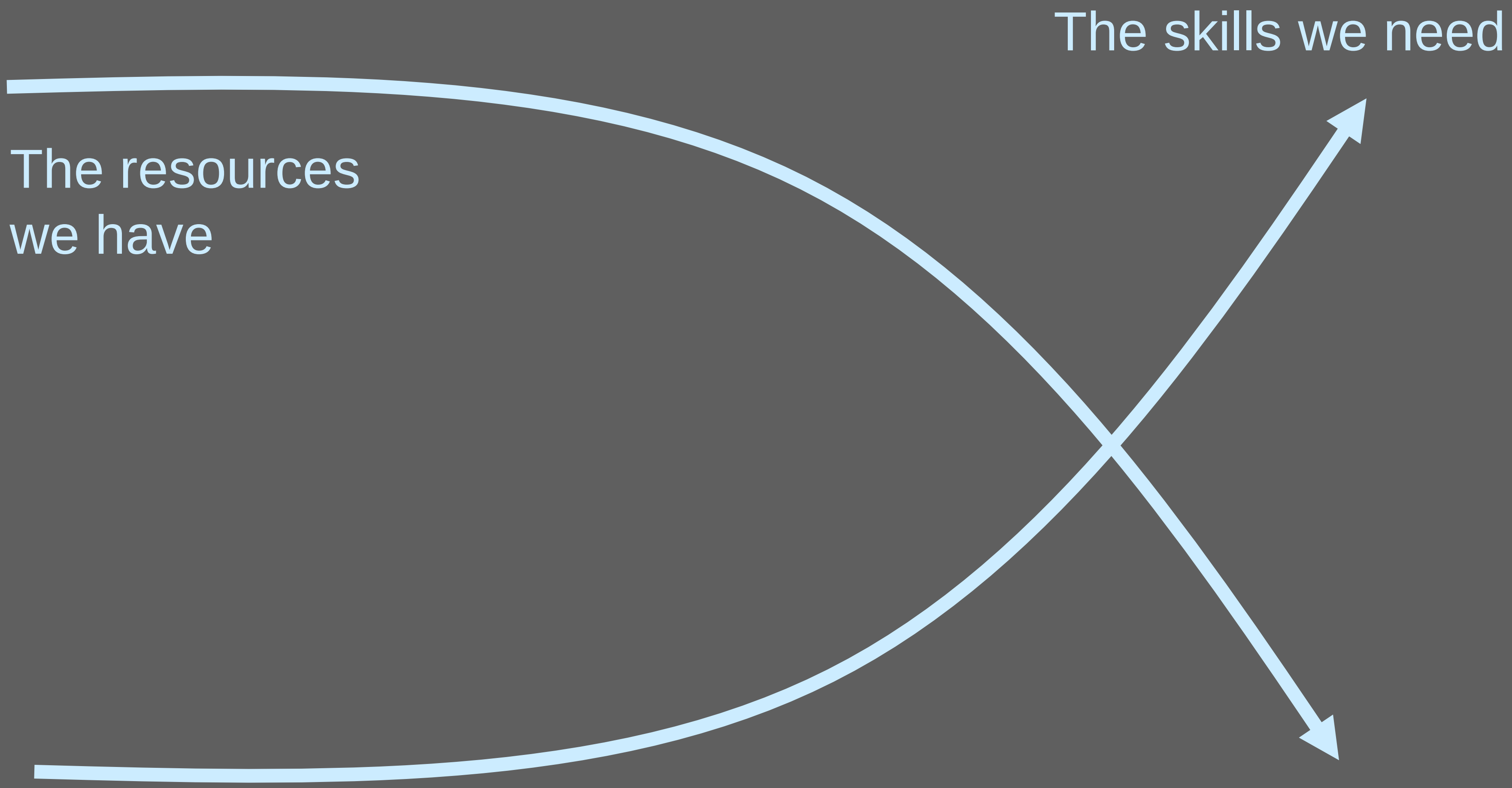
Now, The Train-wreck

- I have a unique position in the industry
  - Sometimes people call me up at 3:00am with interesting problems, just because they think I’m going to help, or will be amused, or something
  - In the last 5 years I’ve gotten sucked into 4 extremely interesting incident responses
  - Last summer’s incident response was the one which blew my mind

High Intellectual Cost Attacks

- Last Summer’s incident response project:
  - Involved me and 6 of the best technical people I know (being able to Call Tom Liston and Mike Poor and say, “hey, can you get out there?” is not an ordinary experience)
  - The fight lasted several weeks
  - We were dealing with custom code being created on the fly (Being able to call Joel Yonts and say “hey, can you decompile this? Like, now?” is also not an ordinary experience)

High Intellectual Cost Attacks



The skills we need

The resources
we have

Messages

1) You are going to ***need*** **a malware response team**
   - They will ***have*** to be able to deal with stuff that is outside of the packaged knowledge-bases
2) You are going to ***need*** to be doing monitoring and analysis above and beyond the “usual stuff”
   - The “usual stuff” simply is not good enough*
   - ***Creativity*** will be the key to success

*This is where the standards are focused

Messages

3) The trend-line of “do more with less” is going to break really hard when you have your first targeted attack (“*when*” not “if”)

4) Do full-system cost modelling

- The money you “save” by dumbing down your team will be spent in under a month by the army of expensive con$ultants you will need
- And that’s just the ***first time***

Cheerful Conclusions

- IT has done a pretty good job of avoiding tackling the hard problems
  - We’ve done such a good job that most of us haven’t realized that’s what we’ve been doing
- Targeted attacks and custom malware break the paradigm
  - The only counter-paradigms on offer are:

    a) armies of con$ultants

    b) skilled, creative, motivated generalists on staff

Cheerful Conclusions - 2

- Yeah, good luck selling that one.