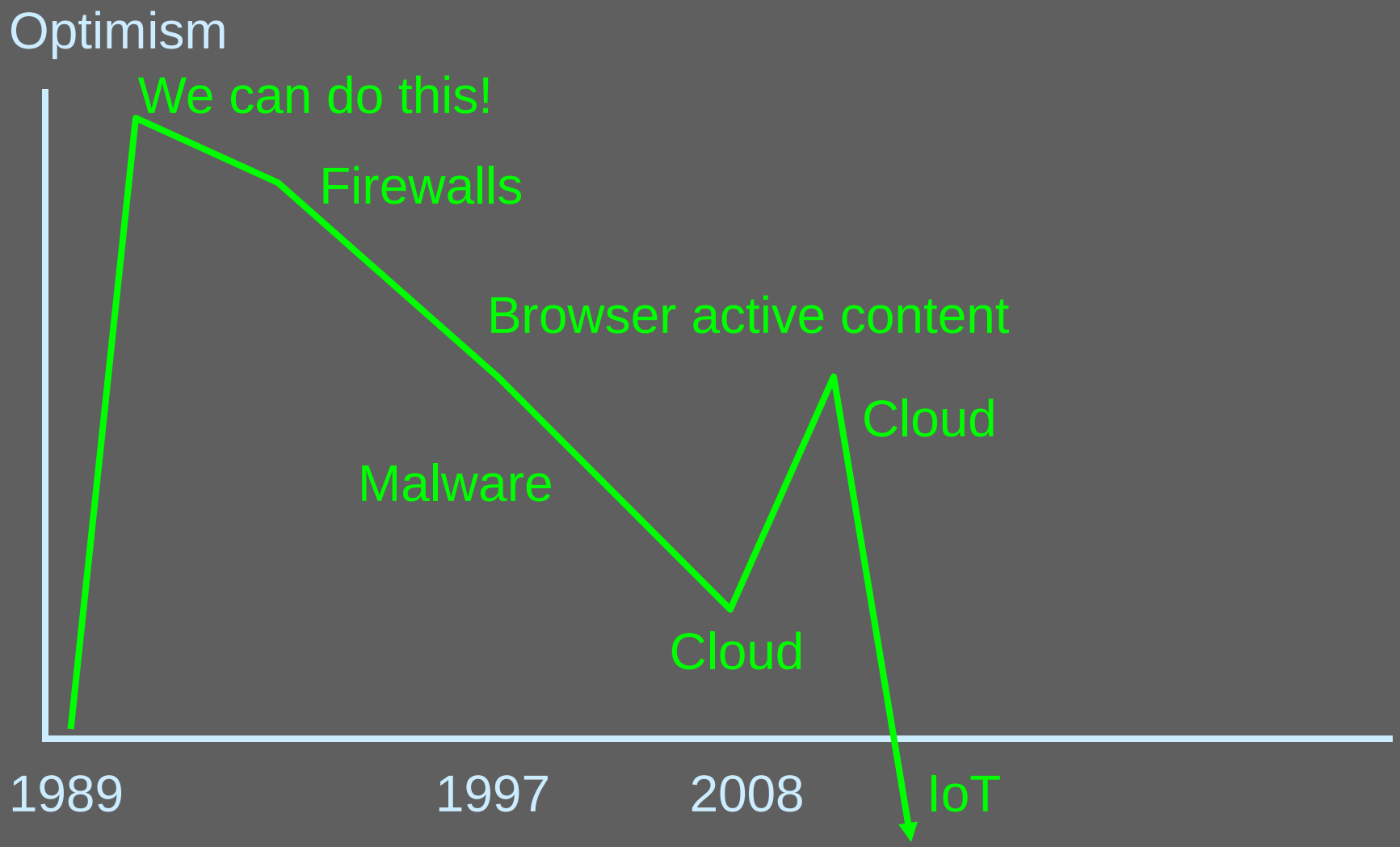
Security in My Rear-View Mirror

Marcus J. Ranum
works for
Tenable Network Security, Inc.

Trajectory


Optimism
We can do this!
Firewalls
Browser active content
Cloud
Malware
Cloud
IoT
1989
1997
2008

Current Trends

- Management:
  - Do more with less
  - Process not people
  - Off the shelf software
  - No in-house development capability

A Problem

- Everything I advocate is the opposite of “do more with less”

The Problem

- Management is chasing fads and engaging in false optimism
  - Keep buying anti-malware products “maybe the next one will work”
  - Keep freeform data-sharing “maybe we’ll figure out where it is someday”
  - Keep desktop systems administration “configuration management is hard”

Market Dynamics

- The security world is getting crushed from 3 sides at once:
  - Top
  - Bottom
  - Flank

Market Dynamics

- From the top, the security market is getting crushed by cloud computing
  - Cloud *is* configuration management and automation
  - If you won't/can't/are too stupid to do it, we'll do it for you, and aggregate the cost

Market Dynamics

- From the bottom, the security market is getting crushed by the apparent savings of BYOD
  - Not, you know, the *reality* of BYOD
  - It's just a way of pushing the cost of management onto the user

Market Dynamics

- From the side, the security market is getting crushed by new management models
  - Apple walled garden software (but knowing Apple, it’s not too late to screw up)
  - Software as a service

If You Were Paying Attention

- You may have noticed that I just said that security is almost entirely being driven by management costs
  - Specifically system administration / configuration management

If You Were Paying Attention

- This is why current focus on standards and compliance (PCI, etc) is ill-advised
  - It is *another* management cost
  - If organizations realize this, they'll figure out how to game compliance
    - Switch to cloud
    - Switch to configuration management and automation

Digging Out Of The Hole

- Stop doing “penetrate and patch”
  - The industry must/will switch to streaming software updates with version repudiation
  - It’s heading that way for everything, it probably won’t be good enough
  - Switch to whitelisting applications *and* traffic *and* storage
- Focus on aggregate management cost

How to Talk to Managment

- Use small words

How to Talk to Managment

- Joking aside:
  - Use comparative results
  - “we did X, and it resulted in Y”
  - “we spend X amount of time on each incident, compared to Y amount of time in aggregate configuration management”
- Help them understand where the effort is going

How to Talk to Managment

- This applies to software, as well!!
  - “I know you say ‘we don’t do software development’ but Oracle and Arcsight and everything we have to configure *is* software development. We need to look at long-term maintenance and management costs, not top line cost.”

How to Talk to Managment

- Eventually someone must ask:
  - “Are cheaper Windows/PC combinations actually cheaper than a Mac, if we look at them over a 5-year cycle including maintenance and management costs as well as add-on software and management of add-on software?”
  - Do you know the true cost of malware?

All of This Means:

- Maintain metrics
  - It is effectively impossible to make honest cost-based system projections without data about current outcomes
- “When is the best time to plant a mighty oak tree?”

My Advice To You

- If you’re working in security, work with a focus on management and automation
  - That’s mostly what we do, anyway
  - Forms of management that can be, will be ditched
  - Forms of management that can be, will be automated

My Advice To You

- If you're working in software, work with a focus on management and automation
  - CASE tools failed in the 80s and 90s because they made writing bad code harder
  - Make it easier to write good code faster and you will get rich*

* If you don't die of frustration, first

My Advice To You

- Avoid “forensic management” careers
  - Vulnerability management
  - Asset management
  - Penetration testing
  - Compliance auditing
- These are fields that are targeted for cost-cutting (which will mean increased competition)

My Advice To You

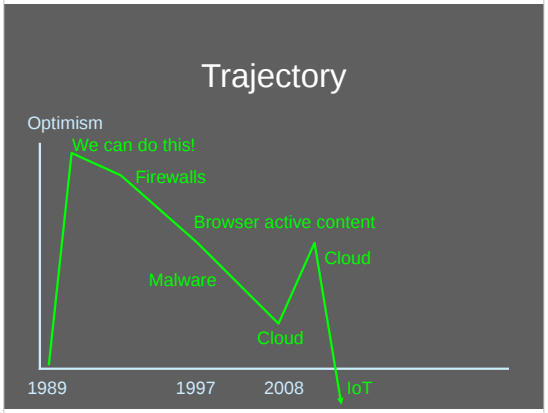
- Want to make a ton of $Euro?
  - Application whitelisting as a service
  - Storage management as a service

Summary

- It probably sounds like I am “big” on configuration management
  - Yes
- Why?
  - Security is properly a sub-discipline of systems and network administration
  - We exist as an industry because they suck

Security in My Rear-View Mirror

Marcus J. Ranum
works for
Tenable Network Security, Inc.


Trajectory
Optimism
We can do this!
Firewalls
Browser active content
Cloud
Malware
Cloud
1989
1997
2008
IoT

Current Trends

- Management:
  - Do more with less
  - Process not people
  - Off the shelf software
  - No in-house development capability

A Problem

- Everything I advocate is the opposite of “do more with less”

The Problem

- Management is chasing fads and engaging in false optimism
  - Keep buying anti-malware products “maybe the next one will work”
  - Keep freeform data-sharing “maybe we’ll figure out where it is someday”
  - Keep desktop systems administration “configuration management is hard”

Market Dynamics

- The security world is getting crushed from 3 sides at once:
  - Top
  - Bottom
  - Flank

Market Dynamics

- From the top, the security market is getting crushed by cloud computing
  - Cloud *is* configuration management and automation
  - If you won't/can't/are too stupid to do it, we'll do it for you, and aggregate the cost

Market Dynamics

- From the bottom, the security market is getting crushed by the apparent savings of BYOD
  - Not, you know, the *reality* of BYOD
  - It's just a way of pushing the cost of management onto the user

Market Dynamics

- From the side, the security market is getting crushed by new management models
  - Apple walled garden software (but knowing Apple, it's not too late to screw up)
  - Software as a service

If You Were Paying Attention

- You may have noticed that I just said that security is almost entirely being driven by management costs
  - Specifically system administration / configuration management

If You Were Paying Attention

- This is why current focus on standards and compliance (PCI, etc) is ill-advised
  - It is *another* management cost
  - If organizations realize this, they'll figure out how to game compliance
    - Switch to cloud
    - Switch to configuration management and automation

Digging Out Of The Hole

- Stop doing “penetrate and patch”
  - The industry must/will switch to streaming software updates with version repudiation
  - It’s heading that way for everything, it probably won’t be good enough
  - Switch to whitelisting applications *and* traffic *and* storage
- Focus on aggregate management cost

How to Talk to Managment

- Use small words

How to Talk to Managment

- Joking aside:
  - Use comparative results
  - “we did X, and it resulted in Y”
  - “we spend X amount of time on each incident, compared to Y amount of time in aggregate configuration management”
- Help them understand where the effort is going

How to Talk to Managment

- This applies to software, as well!!
  - "I know you say 'we don't do software development' but Oracle and Arcsight and everything we have to configure *is* software development. We need to look at long-term maintenance and management costs, not top line cost."

How to Talk to Managment

- Eventually someone must ask:
  - “Are cheaper Windows/PC combinations actually cheaper than a Mac, if we look at them over a 5-year cycle including maintenance and management costs as well as add-on software and management of add-on software?”
  - Do you know the true cost of malware?

All of This Means:

- Maintain metrics
  - It is effectively impossible to make honest cost-based system projections without data about current outcomes
- “When is the best time to plant a mighty oak tree?”

My Advice To You

- If you're working in security, work with a focus on management and automation
  - That's mostly what we do, anyway
  - Forms of management that can be, will be ditched
  - Forms of management that can be, will be automated

My Advice To You

- If you're working in software, work with a focus on management and automation
  - CASE tools failed in the 80s and 90s because they made writing bad code harder
  - Make it easier to write good code faster and you will get rich*

* If you don't die of frustration, first

My Advice To You

- Avoid “forensic management” careers
  - Vulnerability management
  - Asset management
  - Penetration testing
  - Compliance auditing
- These are fields that are targeted for cost-cutting (which will mean increased competition)

My Advice To You

- Want to make a ton of $Euro?
  - Application whitelisting as a service
  - Storage management as a service

Summary

- It probably sounds like I am “big” on configuration management
  - Yes
- Why?
  - Security is properly a sub-discipline of systems and network administration
  - We exist as an industry because they suck