RSΛCONFERENCE2013

Living Below The Security Poverty Line:

Coping Mechanisms

Andy Ellis
Akamai

Wendy Nather
451 Research

Session ID: SECT-F41

Session Classification: Intermediate

Akamai 451 Research

SPL:
Outside View

Security Poverty Line

Organizations that don't have enough resources to implement perceived basic security needs.

Security Subsistence Syndrome

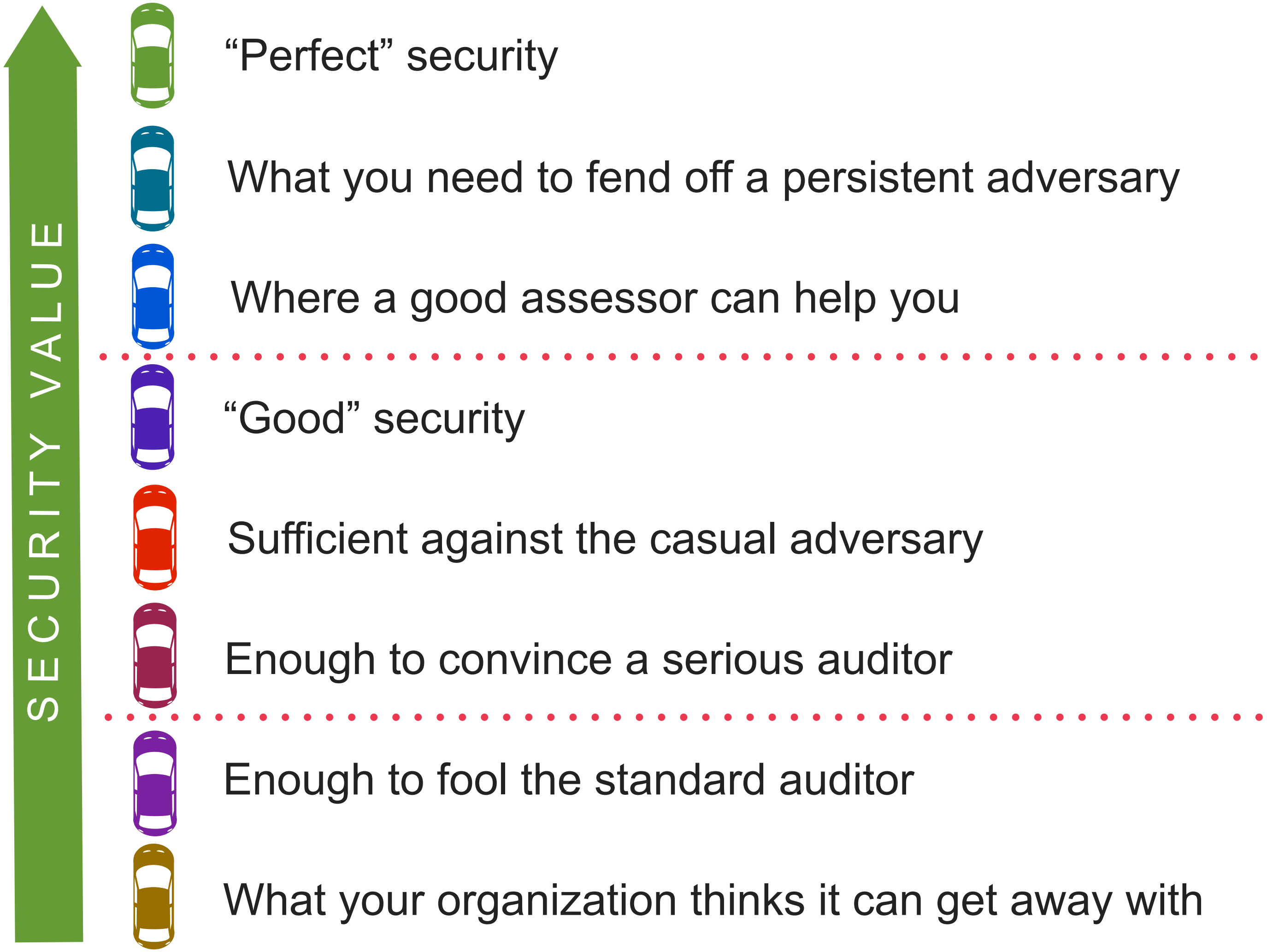
"I can't even do the barest minimum to cover my ass, so I'd better not do anything **but** cover my ass."

Accruing Technical Debt

With every step forward, the undone work increases risk and makes future steps harder.

This is a dangerous way to operate!

How much is “good enough”?



“Perfect” security

What you need to fend off a persistent adversary

Where a good assessor can help you

“Good” security

Sufficient against the casual adversary

Enough to convince a serious auditor

Enough to fool the standard auditor

What your organization thinks it can get away with

How much is “good enough”?

SECURITY VALUE

“Perfect” security

What you need to fend off a persistent adversary

Where a good assessor can help you

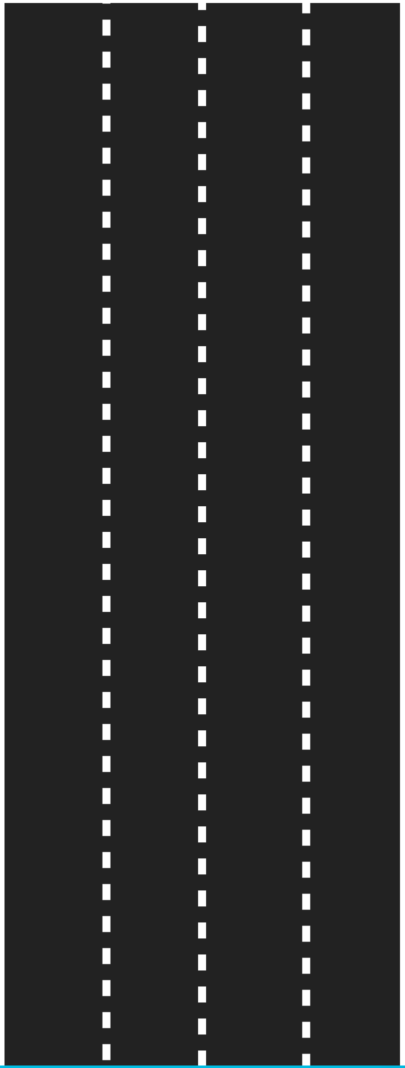
“Good” security

Sufficient against the casual adversary

Enough to convince a serious auditor

Enough to fool the standard auditor

What your organization thinks it can get away with



SPL:
Inside View

Below the Security Poverty Line …

- Little to no IT expertise
- Can’t follow through on long-term recommendations of consultant
- Can’t update security software installations
- Can’t tune SIEM or IPS
- Maintenance takes back seat to outages and new installs

Below the Security Poverty Line …

- Disproportionately dependent on third party vendors
  - Limited span of control
  - Configuration and tuning decisions
  - Architecture and strategy decisions
  - Risk management

- Information asymmetry

Technical debt below the SPL …

- Default settings
- Workarounds (such as remote access programs)
- Lots of sharing (vendors, servers, code, data, other resources)
- Limited span of control
- Limited span of attention
- “We’ll fix that later”
- No logs

Why defer risk?

What your **organization thinks** it can get away with

Organizations don't think:

People do.

The business defers risk ...

“Let’s wait until we actually get attacked.”
– CIO to law enforcement officer, in a briefing about threat activity

... so we enter CYA mode.

Business Owner
Here is my project.
Is it safe?

Security
Here's our ISO 27002
checklist of every
mistake anyone's ever
made. Prove you haven't.

That's really long.
Can you fill it out
for me?

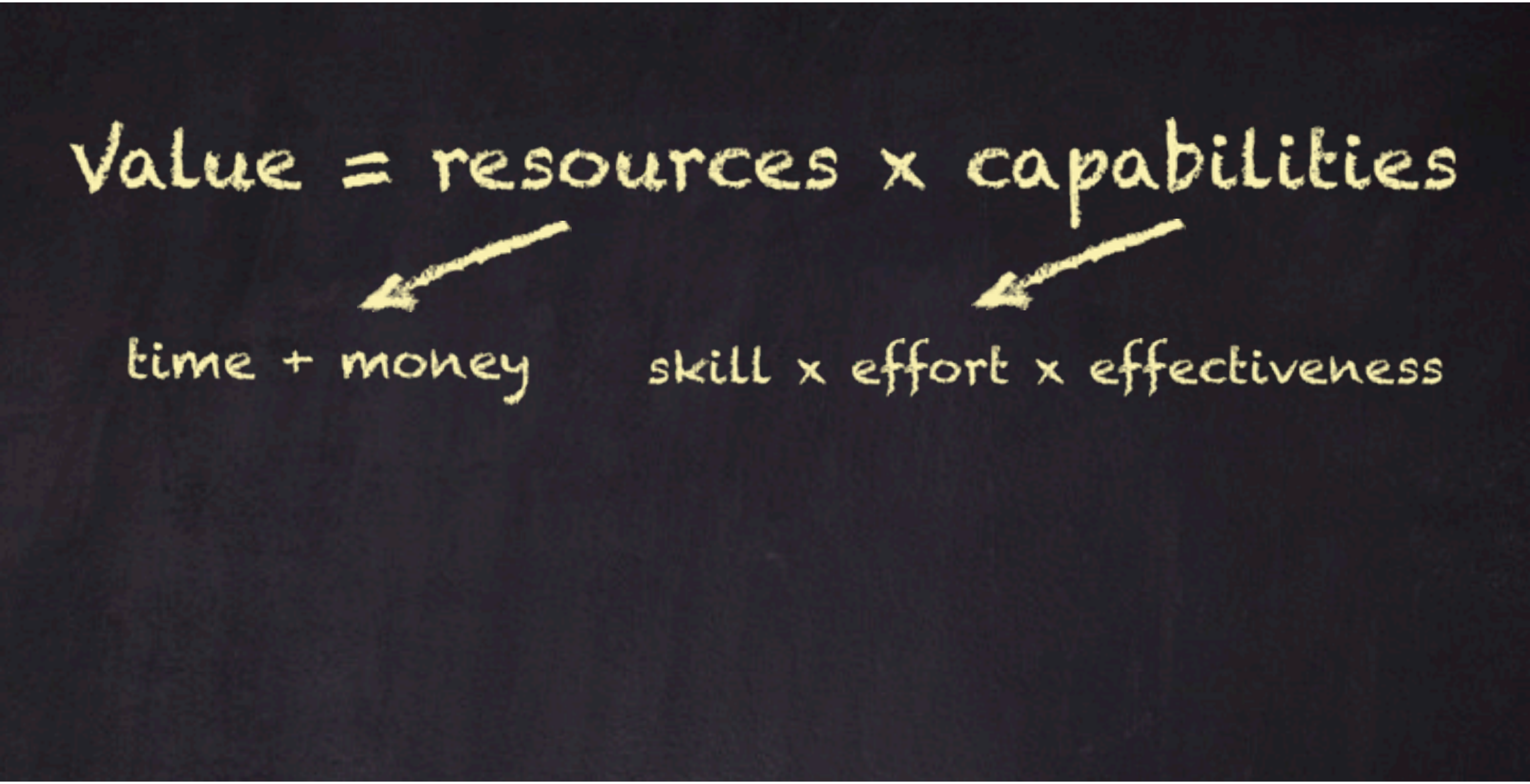
Sure. You have a bunch
of esoteric risk here.

Really? Is that a
showstopper?

If I say yes, you're going to
override me, aren't you?
And if I say no, I'm in
trouble if this goes wrong...

Self-improvement

Measuring a security program

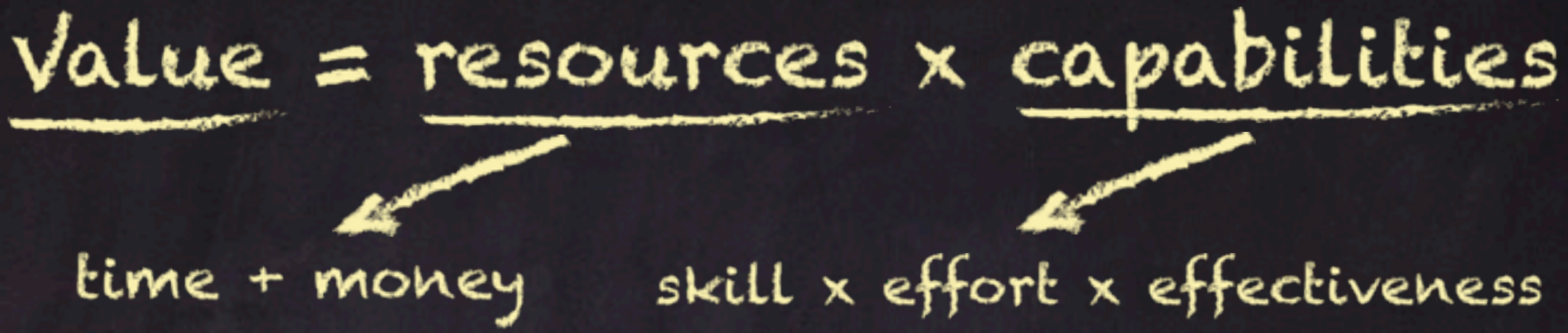


Value = resources x capabilities

time + money

skill x effort x effectiveness

INSERT SLIDE TITLE HERE


Value = resources x capabilities
time + money
skill x effort x effectiveness

Goal of any security program: **dv/dt > 0**

Below the Security Poverty Line, we see Security Subsistence Syndrome: relying on *resources*, not *capabilities*.
Goal: dr/dt > 0

A *good* security program wants to create surplus.
Goal: dc/dt > 0

Budget issues

- Budgets are low to nonexistent, or come from a different “bucket”
- Security budget can be ephemeral and last-minute
- No discretionary spending even at beginning of fiscal year

Do you know what $2,000 will buy?

What $2,000 will buy

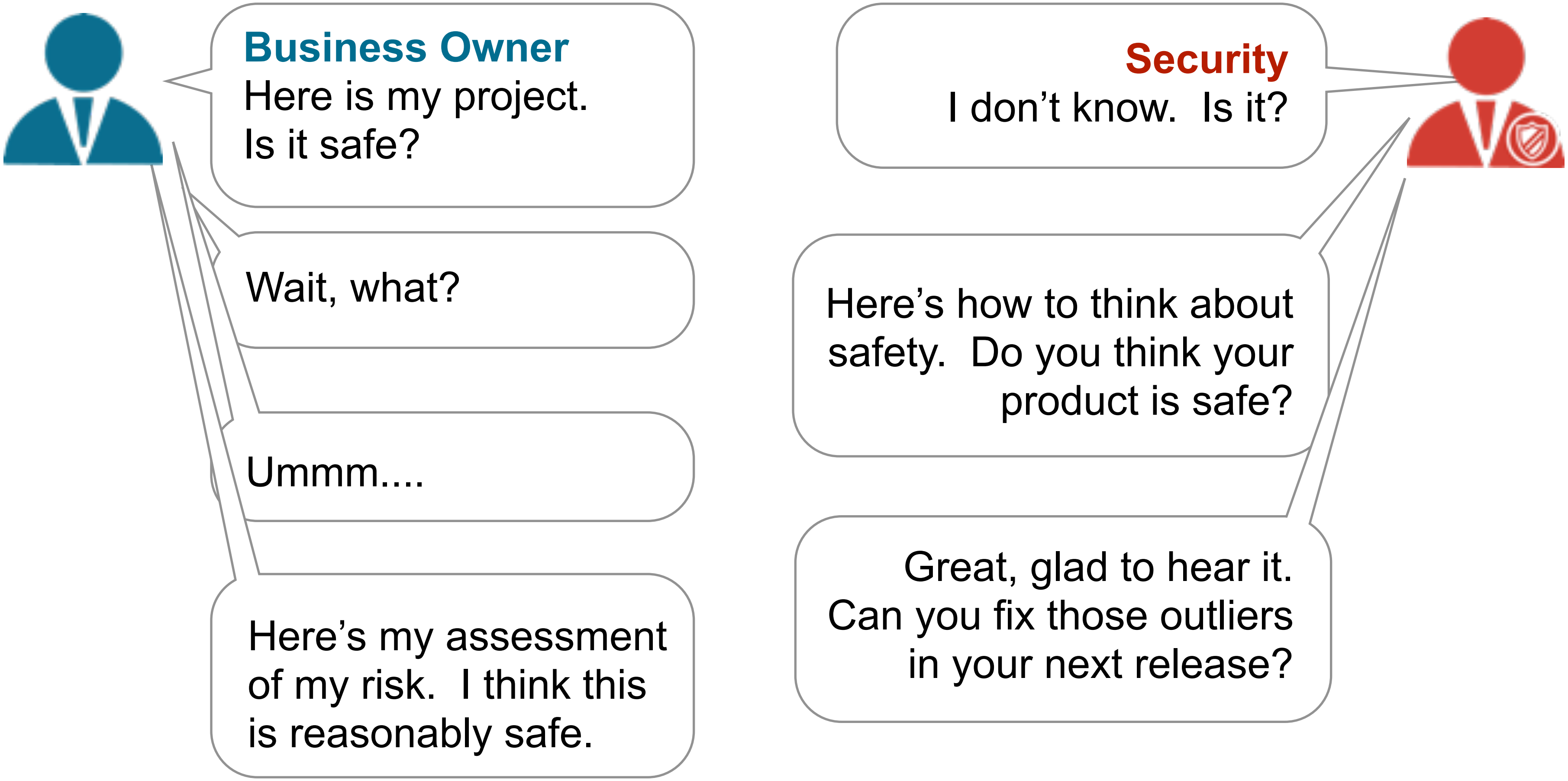
What	Details	How much
Endpoint protection suite for 25 seats, plus 2 yrs maintenance	AV, email/web filtering, desktop firewall, device control	$1,980
Web application scanning for 1 website	Permanent license (no upgrades)	$1,445
Web application scanning for 20 months, 10 sites	100 pages max/site, only 3 types of vulnerabilities checked	$2,000
Hosted email security, 85 users	1 year subscription	$2,000
Penetration testing suite that runs on a phone (qty 2)	8+ testing tools, includes wireless card	$1,920

What $2,000 will not buy

What	Details	How much
Software-based IPS	50 Mbps throughput	$2,500
File integrity monitoring	Server (no agents)	$3,999
Market leader application security testing service	1 year's subscription for 1 application	$3,000 - $7,500
SIEM for managing log collector	For 1 server, connects to 1 log appliance	$13,800*
Anti-DDoS appliance	2 Gbps throughput	$70,000

Stop Juggling!

Engage the business



Business Owner
Here is my project.
Is it safe?

Security
I don’t know. Is it?

Wait, what?

Here’s how to think about safety. Do you think your product is safe?

Ummm....

Here’s my assessment of my risk. I think this is reasonably safe.

Great, glad to hear it.
Can you fix those outliers in your next release?

RSA CONFERENCE 2013

Questions?
Answers?
Pontifications?

Akamai

451 Research