

RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: GRC-F01

Do You Know What You Don't Know?

Marcus H. Sachs, P.E.

@MarcusSachs

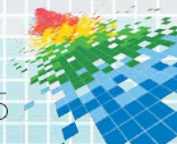
CHANGE

Challenge today's security thinking



Apply Slide

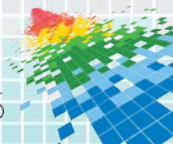
- ◆ Next week you should:
 - ◆ Identify where unknowns are hiding within your organization
- ◆ In the first three months following this presentation you should:
 - ◆ Understand where your organization fits into the proposed model
 - ◆ Develop a plan to push your organization to the upper right quadrant
- ◆ Within six months you should:
 - ◆ Begin the execution of your plan, managing the unknowns rather than focusing just on what you know
 - ◆ Demonstrate to peers and seniors how this methodology can work for other areas of risk management



Some Axioms

You cannot protect assets
you don't know about.

You cannot defend against threats
you are unaware of.



The Quote

“...there are *known knowns*; there are things that we know that we know.

“We also know there are *known unknowns*; that is to say we know there are some things we do not know.

“But there are also the *unknown unknowns*, the ones we don't know we don't know.”

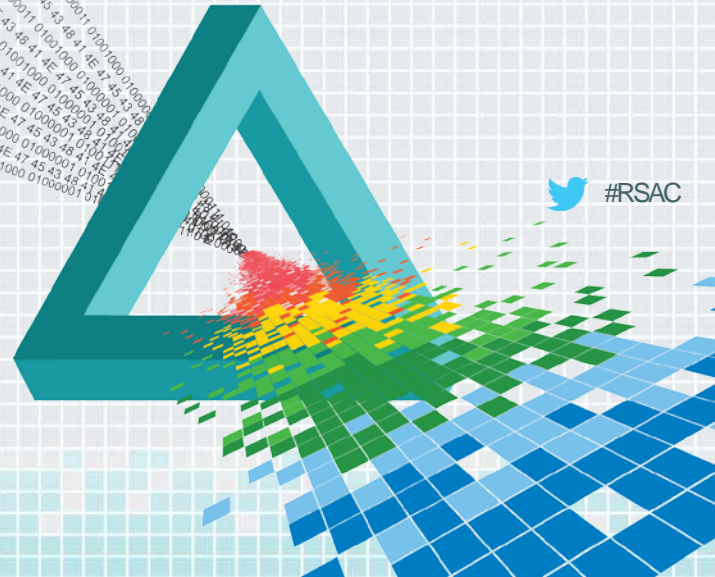
-Donald Rumsfeld, 2002



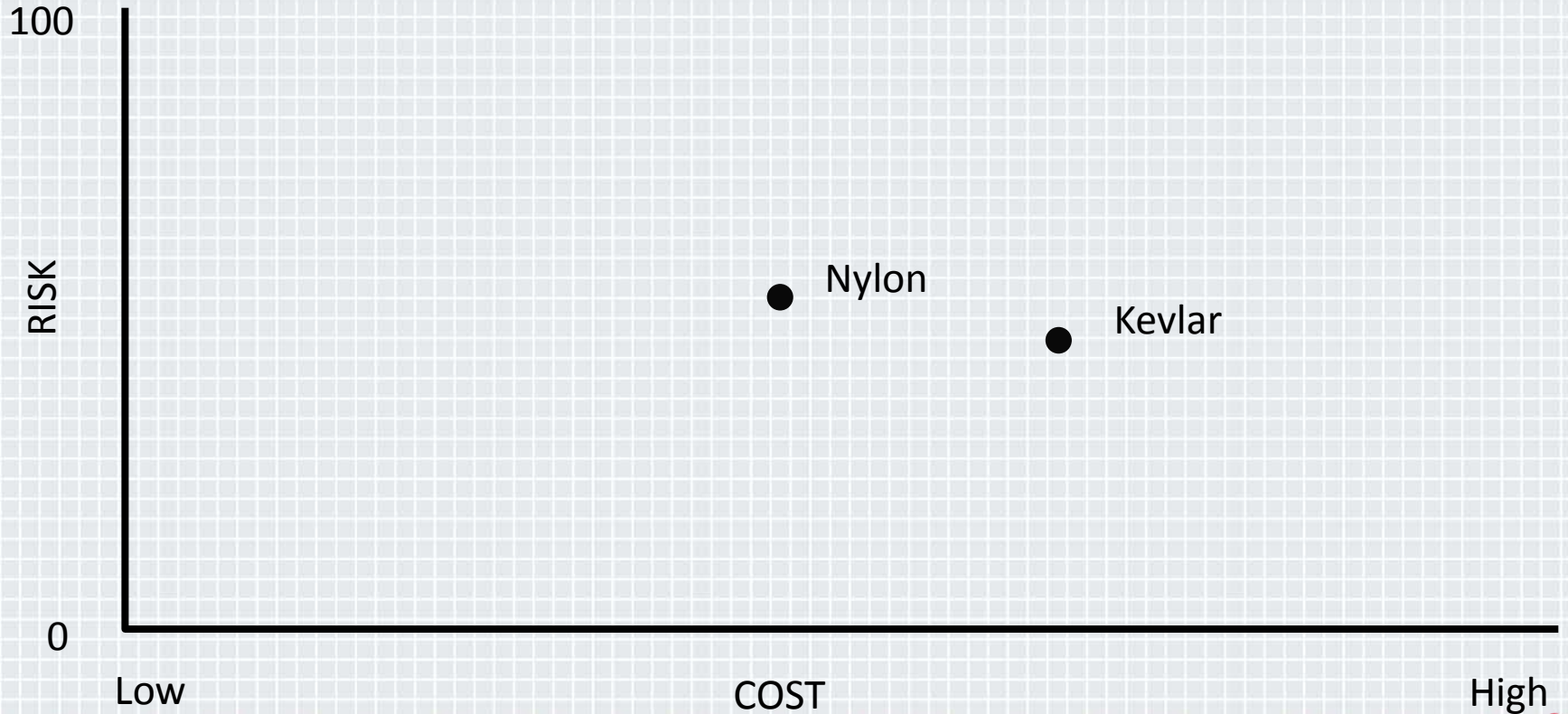
RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

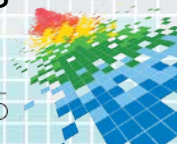
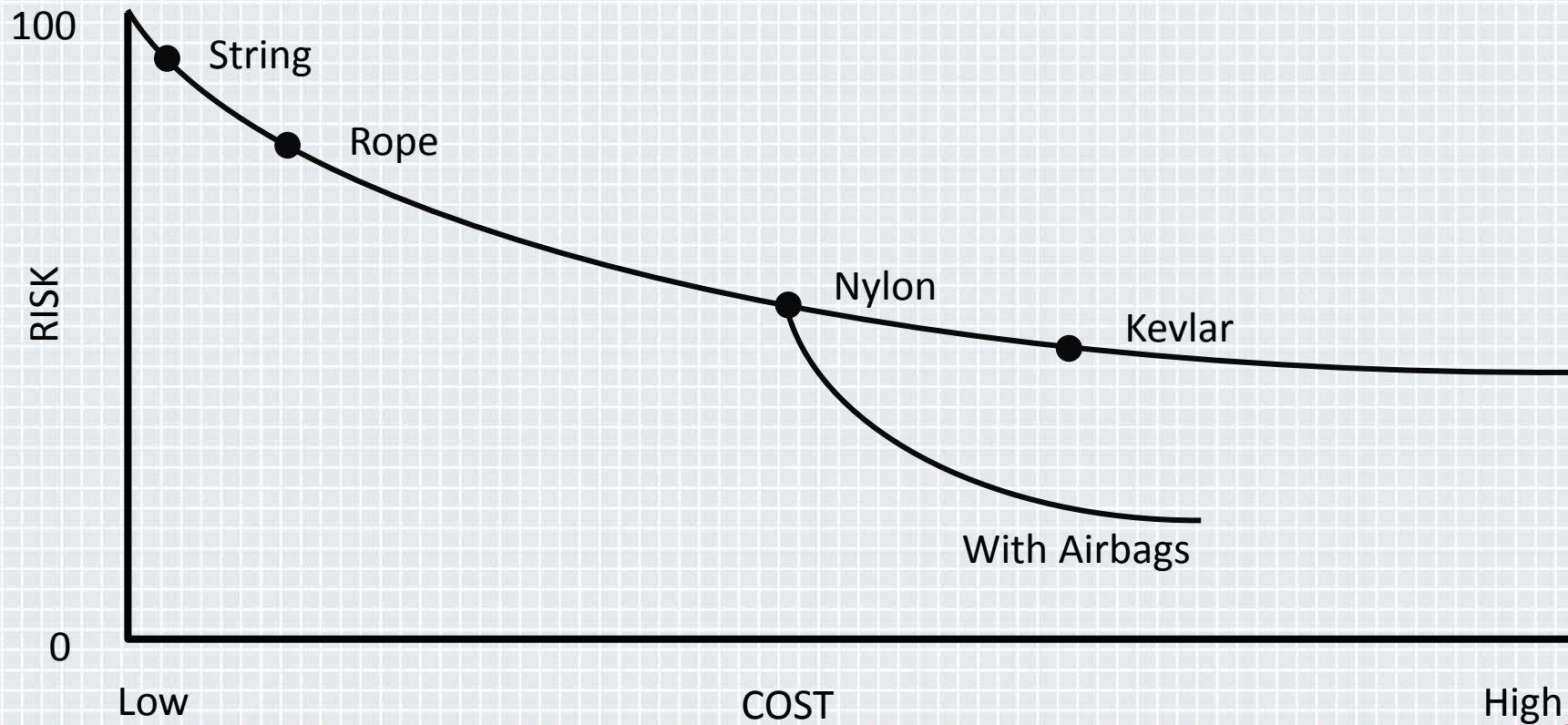
Let's Do An Exercise



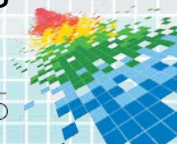
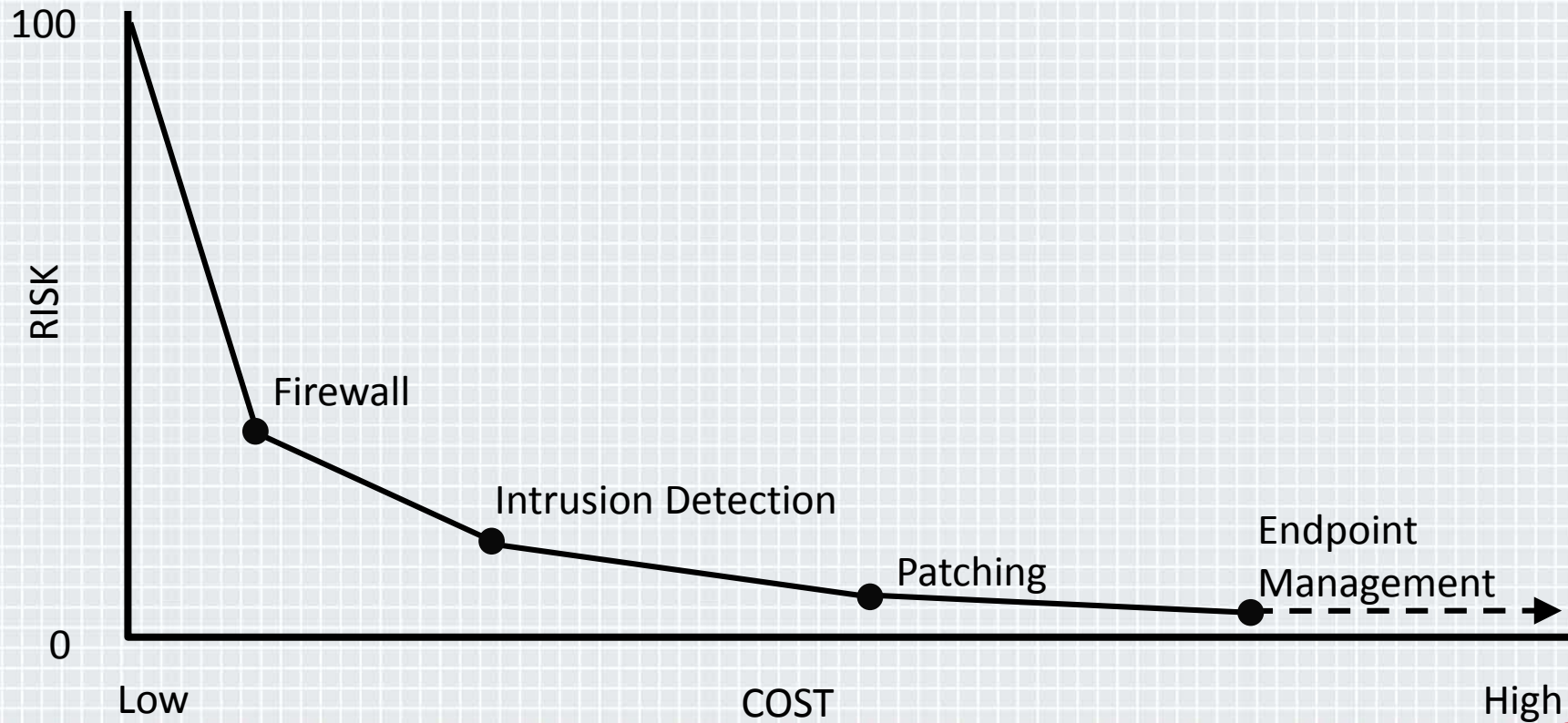
The Seatbelt Project



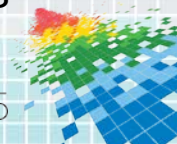
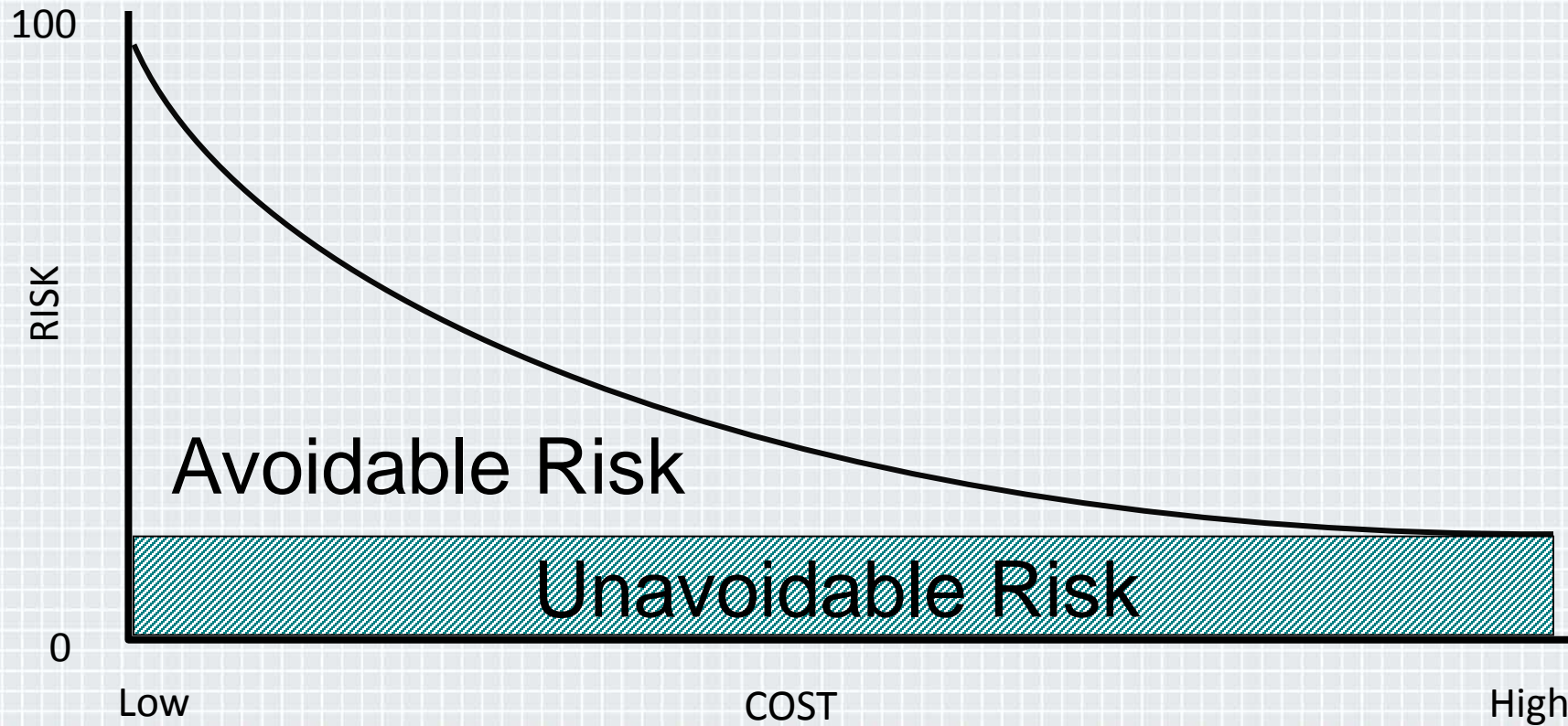
The Seatbelt Project



The Security Project

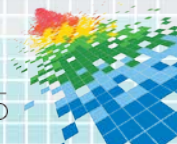


Managing Risk



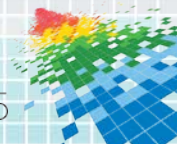
Is Cyber Risk Something That Can Be Measured?

- ◆ Perhaps, but you first have to define “risk”
- ◆ Some say it is this:
$$\text{Risk} = \text{Threats} \times \text{Vulnerabilities} \times \text{Impact}$$
 - ◆ What numbers do you use? What does it mean?
- ◆ Others say risk is related to uncertainty
 - ◆ If you can determine with precision the outcome of a series of events, then the risk of something else happening is low
 - ◆ Does that mean that jumping out of airplane at 10,000 feet without a parachute is not a risky venture?



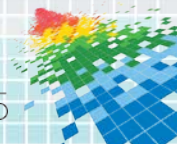
Perhaps Risk is Something Else

- ◆ In the Market, risk is the potential of losing something of value weighed against the potential to gain something of value
- ◆ Another approach is to let risk be a function of what you don't know
 - ◆ How do you determine what you don't know?
 - ◆ Can you measure how much you don't know?
 - ◆ What about not knowing about what you don't know?



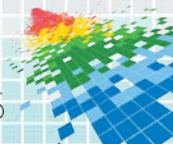
Cyber Risk is Everywhere (what we DO know)

- ◆ Insiders doing legitimate work insecurely
- ◆ Outsiders interacting with our systems
- ◆ Technology innovation and change
- ◆ IT supply chain complexity
- ◆ Old protocols and assumptions
- ◆ Government regulation
- ◆ Determined adversaries

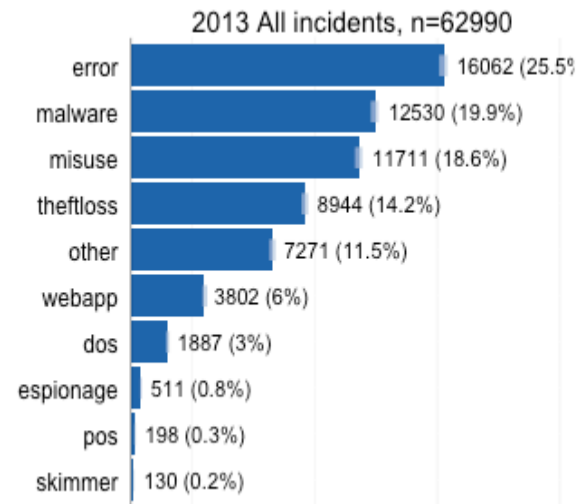
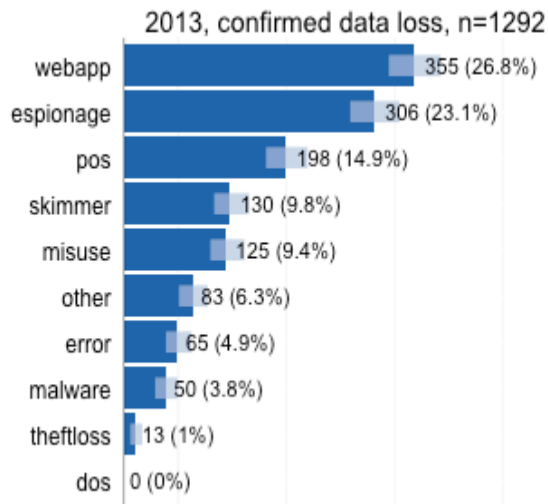
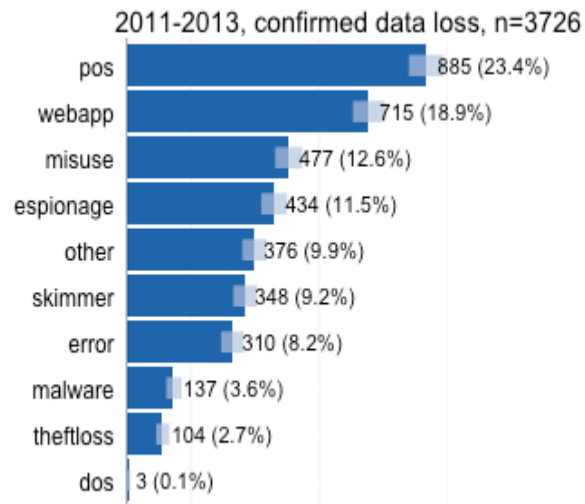


Guidance From a Security Professional for Measuring Cyber Risk (Focused on Knowns)

- ◆ “**Quarterly Statement of Risk** which outlines all the risks that have been identified for that quarter and any exceptions granted so that senior management can understand how much risk they have.”
- ◆ “**Monthly Vulnerability Report** that gets delivered to all levels within the enterprise with specific remediation metrics such as 30, 60, 90 days for high, medium and low risks.”
- ◆ “**Monthly Exception Report** that shows how many policy exceptions have been requested, how many have been granted, and when they expire.”
- ◆ “**Access Review Summary** for all applications that house highly confidential data, which details who has access to what, for what reason and has an audit trail back to the date of employment.”
- ◆ “**A Monthly Incident Report** should be delivered to senior management that shows how often the enterprise comes under attack and the kinds of attacks they are under.”

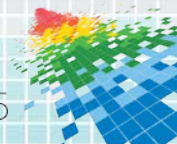


An Example of What We Know: The 2014 Verizon DBIR Findings



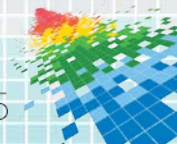
2010 DBIR: The Unknown Unknowns

- ◆ In nearly half of Verizon's 2009 cases, investigators observed what were not so affectionately called the "unknown unknowns."
- ◆ These were classified as meeting at least one of the following conditions:
 - ◆ **Assets unknown or unclaimed** by the organization (or business group affected)
 - ◆ **Data** the organization **did not know existed** on a particular asset
 - ◆ Assets that had **unknown network connections** or accessibility
 - ◆ Assets that had **unknown user accounts** or privileges

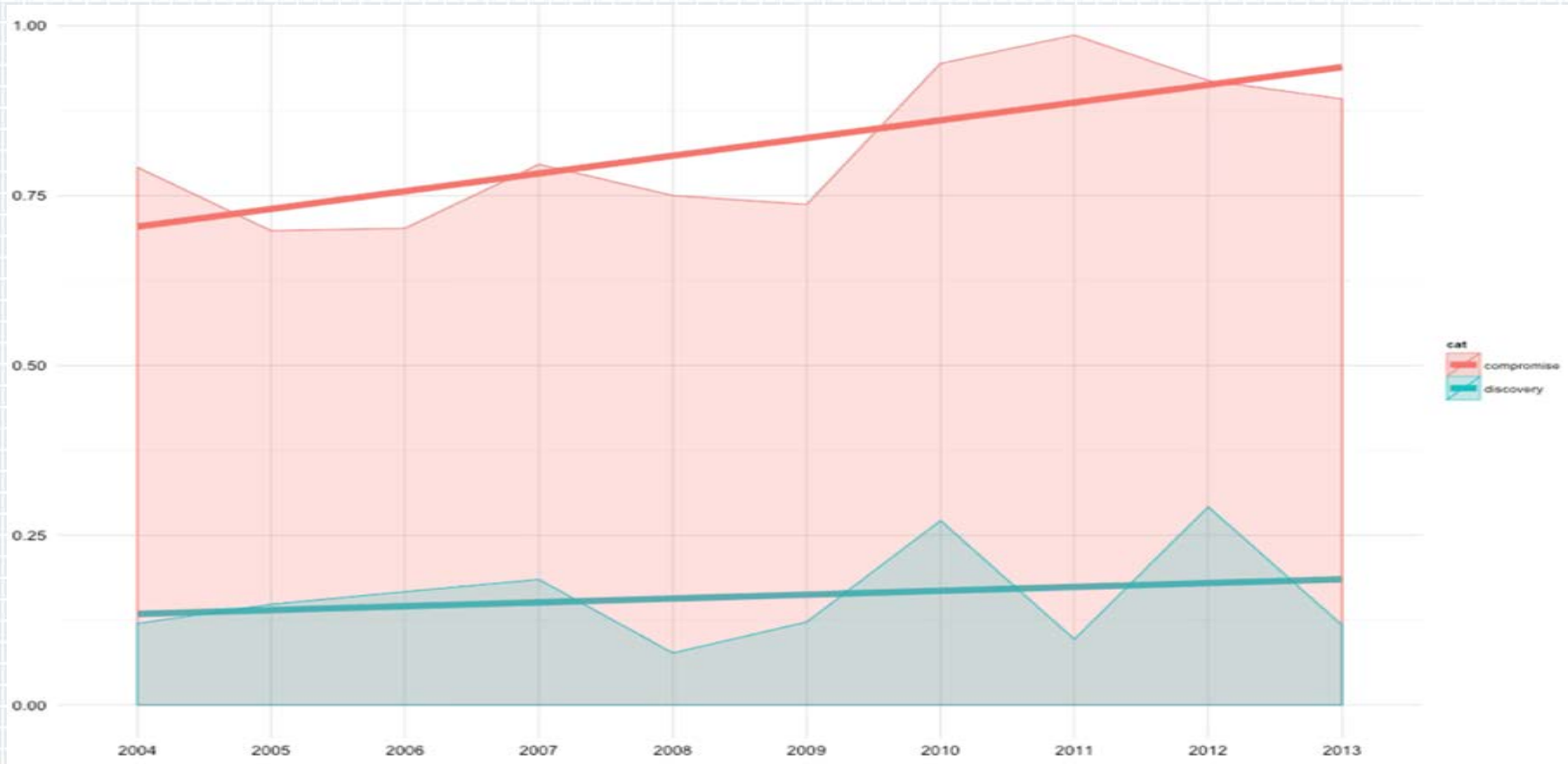


Measuring the Unknowns

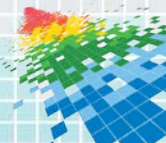
- ◆ We have found that rather than counting what you know, risk management works best when you identify and reduce what you don't know
- ◆ A personal example:
 - ◆ When was the last time a house in your neighborhood caught fire?
 - ◆ Do you know how long it takes for a fire truck to arrive?
 - ◆ Do you know if your nearest fire hydrant has water in it?
- ◆ These are the ***unknowns*** – you want to identify and convert them into ***knowns***



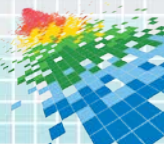
Consequence of an Unknown: Time-to-compromise vs. Time-to-discovery



Unknown: Who is Giving Away Your Passwords?

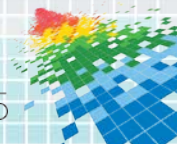


Unknown: Who is Giving Away Your Passwords?

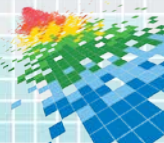


Unknown: What Are Your Employees Doing Online?

#RSAC

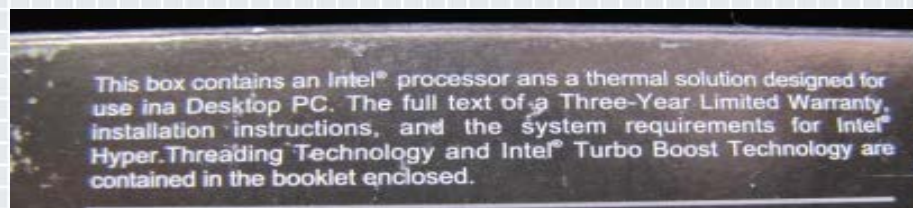


Unknown: BUSTED!



Unknown: Counterfeit Technology

- ◆ Fake Intel Core i7 CPUs sold at Newegg.com



Unknown: Component Mis-Match

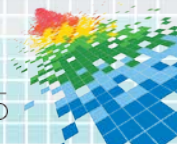


Outer case says 50v 6800µF



Unknown: Employees Using Malicious Mobile Phone Apps

- ◆ <http://www.networkworld.com/news/2014/030514-pre-installed-malware-turns-up-on-279401.html>
- ◆ <http://www.symantec.com/connect/blogs/will-your-next-tv-manual-ask-you-run-scan-instead-adjusting-antenna>



Dangerous Unknowns: The Case of the Cisco T1 WAN Interface Line Card

- ◆ Networking department wants to purchase a new WAN interface card to update their Cisco 1760 routers
 - ◆ They recommend the WIC-1DSU-T1-V2 card
 - ◆ Cisco suggested retail price is about \$1000
- ◆ Recommendation is approved and the parts request goes to the ordering department
- ◆ Ordering department, knowing that the organization is not made of money, goes online to research a few sources
- ◆ Let's see what they find....



Legitimate Used Cisco Parts?

Cisco WIC-1DSU-T1 Card

1-Port T1/Fractional T1 DSU/CSU WAN Interface Card ...

Condition: **Certified Pre-Owned** ?

UC Part #: 213262

Availability: **In Stock - Ready to ship**



[Be the first to write a review](#)

Actual item may differ from photo shown. UsedCisco.com does not sell or include licensed software of any kind. All products are [tested](#) and updated with the latest manufacturer's firmware.

EXTEND YOUR WARRANTY

- 1 Year Warranty **Free**
- 2 Year Warranty **\$10.00**
- 3 Year Warranty **\$20.00**

PRODUCT PRICING

List Price: ~~\$1,000.00~~
You Save: \$900.01 (90%)

Today's Price: \$99.99

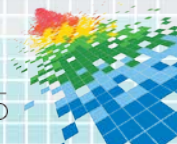
QTY:

Add To Cart 

ADD-ONS

No accessories available.

Add To Cart 



Google Is Your Friend

Google

Web Images Maps **Shopping** More ▾

Electronics Sort: Default ▾ View: Grid ▾

Audio
Computers & Devices
Photo & Optics
TV & Video
More









Bernards, NJ
Change

Show only
 In stock nearby
 New items

Price
 Up to \$100
 \$100 – \$250
 \$250 – \$600
 Over \$600
\$ to \$

Category
 Bridges & Routers
 Modems

Merchant links are sponsored ⓘ

 <p>Cisco Module WIC-1DSU-T1-V2 \$25.00 from Triton Datacom Online</p>	 <p>Cisco 1-Port T1 CSU/DSU Card, WIC-1DSU-T1-V2, NEW \$229.95 from CablesAndKits.com</p>	 <p>Genuine Cisco Systems Wic-1dsu-t1-v2 Interface Card For Router T1 ... \$18.99 used from eBay - citirom</p>	 <p>Cisco WIC-1DSU-T1-V2 - Cisco T1 DSU/CSU WAN Interface Card \$20.00 from CPU Medics</p>
 <p>Cisco Systems Cisco 1841 Router - with Cisco T1 DSU/CSU WAN ... \$699.85 from 10+ stores</p>	 <p>Cisco - 1.5 Mbps DSU/CSU - PC \$94.14 from 25+ stores</p>	 <p>Genuine Cisco Wic-1dsu-t1-v2 Warranty 50 Available \$15.50 used from eBay - certlabkits</p>	 <p>WIC-1DSU-56K Cisco Systems One Port 4-wire 56/64 CSU/DSU WAN Interfac \$64.64 from 10+ stores</p>



eBay Used Cisco Parts



Cisco Systems WIC-1DSU-T1-V2, 1-Port T1/Fractional T1 DSU/CSU Interface Card: V2

Used



25d 0h 55m left

US \$5.00

Buy It Now
or Best Offer



Cisco T1 DSU/CSU WAN Interface Card - DSU/CSU - plug-in module - WIC - 1.544 Mbps

Manufacturer refurbished

5d 3h 12m left

US \$198.10

Buy It Now
or Best Offer



Cisco T1 DSU/CSU WIC-1DSU/CSU-T1 1700 2600 3600 Interface Module Card

Used



29d 0h 59m left

US \$18.99

Buy It Now



Lot of 50- Cisco WIC-1DSU-T1-V2 T1 DSU/CSU WAN Interface Card + 90 Day Warranty

Used

23d 9h 43m left

US \$350.00

Buy It Now
or Best Offer

Free Shipping



Cisco 1-port T1/fractional T1 Dsu/csu Wan Interface Card

New

2d 6h 16m left

US \$37.00

Buy It Now



Cisco WIC-1DSU-T1-V2 T1 DSU/CSU WAN Interface Card + 90 Day Warranty

Used

23d 9h 43m left

US \$7.00

Buy It Now
or Best Offer



Amazon's Prices



Cisco WIC-1DSU-T1-V2 DSU/CSU WIC Card

by Cisco

★★★★★ (1 customer review)

[Return to product information](#)

Always pay through Amazon.com's Shopping Cart or 1-Click. Your purchase will be protected by the [A-to-z Safe Buying Guarantee](#). Never respond to requests to send funds via wire transfer. Learn more about [Safe Online Shopping](#).

Price at a Glance

List Price: \$1,000.00

Used: from **\$4.00**

Refurbished: from **\$8.90**

New: from **\$25.99**

Have one to sell? [Sell yours here](#)

All

New (13 from \$25.99)

Used (22 from \$4.00)

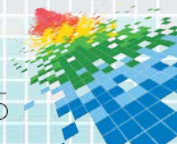
Refurbished (10 from \$8.90)

Show Used FREE Super Saver Shipping offers only

Sorted by Price + Shipping ▾

Used 1-15 of 22 offers

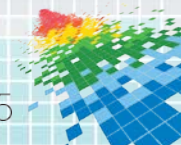
Price + Shipping	Condition	Seller Information	Buying Options
\$4.00 + \$5.49 shipping	Used - Very Good	Seller: SAM Networks LLC Seller Rating: Just Launched (Seller Profile) Ships in 1-2 business days. Ships from VA, United States. Domestic shipping rates and return policy .	Add to Cart OR Sign in to turn on 1-Click ordering.
\$7.50 + \$5.49 shipping	Used - Very Good	DATAHARWARE Seller Rating: ★★★★★ 100% positive over the past 12 months. (4 total ratings) Ships in 1-2 business days. Ships from CA, United States. Expedited shipping available. Domestic shipping rates and return policy . Items undergo 100% testing by certified technicians. Test reports and serial #'s are available upon request. 1 yr. warranty provided.	Add to Cart OR Sign in to turn on 1-Click ordering.
\$8.40 + \$5.02 shipping	Used - Like New	GENUINE DATAHARWARE Seller Rating: ★★★★★ 95% positive over the past 12 months. (157 total ratings)	Add to Cart OR Sign in to turn on 1-Click ordering.



Counterfeit Versus Genuine

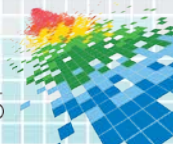


<http://www.andovercg.com/services/cisco-counterfeit-wic-1dsu-t1.shtml>



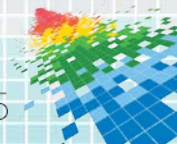
One More Example Of An Unknown: What The Heck Is BASH?

- ◆ Prior to September 26, 2014 only the Unix crowd (and a few Microsoft fans) were familiar with the Bourne Again Shell
 - ◆ But none had any idea that an enormous security hole had been lying inside of BASH waiting to be discovered for over 20 years
 - ◆ In late September millions of businesses had to scramble to figure out if they were vulnerable and how to fix the problem
- ◆ The BASH problem came only weeks after the Heartbleed issue in OpenSSL, another “unknown” concern

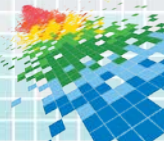


Perhaps a Model Will Help: Knowns vs. Unknowns

- ◆ Make an assertion: *there are things we know and things we do not know about cyber risks*
- ◆ Plot a range of knowledge about cyber risk (y-axis):
 - ◆ We know little to nothing about cyber risks (**low**)
 - ◆ We know a lot or everything about cyber risks (**high**)
- ◆ Then, plot how much we know about the risks we can identify (x-axis):
 - ◆ We know risky things exist, but we don't know a lot about those risks (**low**)
 - ◆ We know risky things exist, and we know a lot about those risks (**high**)

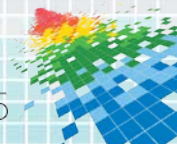
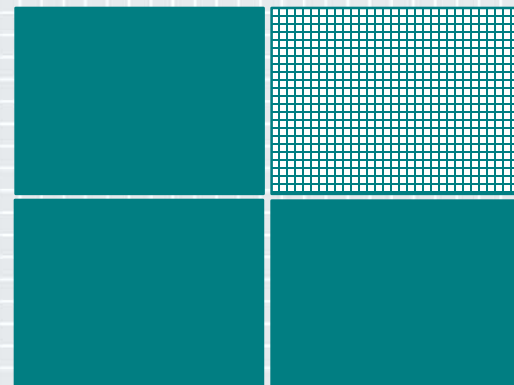


Knowns vs. Unknowns



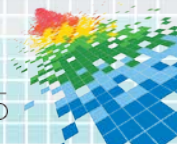
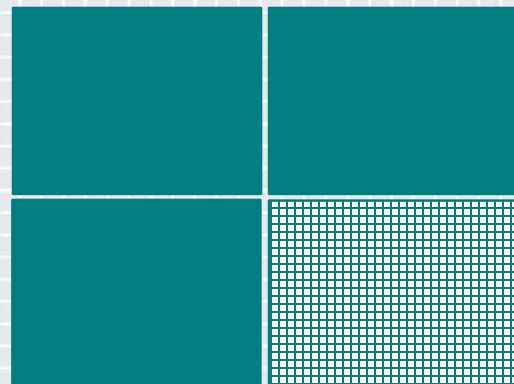
Upper Right Quadrant

- ◆ Known Knowns
 - ◆ You are aware of risks, and you know a lot about them
- ◆ Sources:
 - ◆ Internal/external audit results
 - ◆ Business records
 - ◆ Lawsuits
 - ◆ Press (good and bad)
 - ◆ Measured impact of service loss
- ◆ This is where you want to be
 - ◆ Requires high competence and plenty of resources



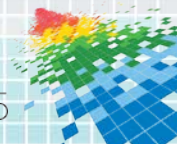
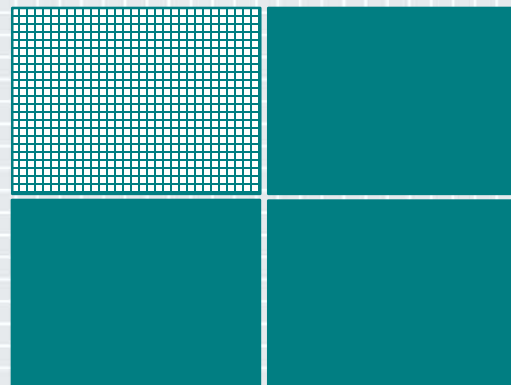
Lower Right Quadrant

- ◆ Known Unknowns
 - ◆ You know what can cause risk, but you don't know if you have any of those risks
- ◆ Types:
 - ◆ Counterfeit/inferior hardware
 - ◆ Social media postings
 - ◆ Unauthorized software
 - ◆ New versions of malware or phishing
 - ◆ Intentions of malicious insiders
- ◆ This is typical of well educated but understaffed CISOs
 - ◆ Can be improved with additional resources



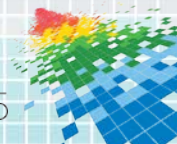
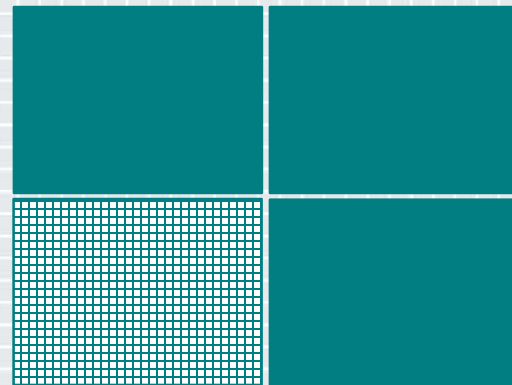
Upper Left Quadrant

- ◆ Unknown Knowns
 - ◆ Knowledge about risk is available, but you are not aware that these resources can uncover hidden risks
- ◆ Resources:
 - ◆ System and machine logs
 - ◆ Calls to the help desk
 - ◆ Internal discussions
 - ◆ Lessons learned but not shared
 - ◆ Encrypted data/files
- ◆ This is typical of large, decentralized organizations
 - ◆ Data is everywhere, but not being mined for indicators



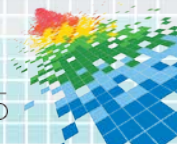
Lower Left Quadrant

- ◆ Unknown Unknowns
 - ◆ You don't know what risks exist, and you don't know where to start looking for them
- ◆ Risks you may not know about:
 - ◆ How long to recover from failure
 - ◆ Existence of undocumented devices, networks, software, or data
 - ◆ Dependencies on others
 - ◆ Former employee accounts
 - ◆ Zero-days in software you have never heard of
- ◆ This is where too many organizations find themselves
 - ◆ They are only paying attention to the things they know



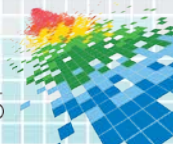
Knowns vs. Unknowns: Putting it all Together

A Lot	<p>We don't know much about what we know</p> <ul style="list-style-type: none"> - System and machine logs - Calls to the help desk - Internal discussions - Lessons learned but not shared - Encrypted data/files <p>UK</p>	<p>We know a lot about what we know</p> <ul style="list-style-type: none"> - Internal/External Audit results - Business records - Lawsuits - Press (good and bad) - Measured impact of service loss <p>KK</p>	
What we know	<ul style="list-style-type: none"> - How long to recover from failure - Existence of undocumented devices, networks, or data - Dependencies on others - Former employee accounts - Zero-days in software <p>UU</p> <p>We don't know what we don't know</p>	<p>KU</p> <ul style="list-style-type: none"> - Counterfeit/inferior hardware - Social media postings - Unauthorized software - New versions of malware - Intentions of malicious insiders <p>We know there are things we don't know</p>	
	Nothing	Nothing	What we know about things we know



Example: Data Breaches

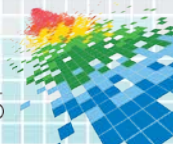
- ◆ **Unknown Unknown:** You have no idea what the term “data breach” means
- ◆ **Unknown Known:** Your organization has been breached and your computers are aware of the breach, but you are not
- ◆ **Known Unknown:** You have read about others getting breached and understand the implications of a breach, but you do not know if you have been breached
- ◆ **Known Known:** Your systems immediately alert you to a breach, you have planned for and have processes to contain breaches, and you fully understand the potential impact of a breach



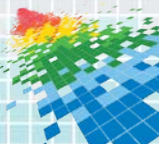
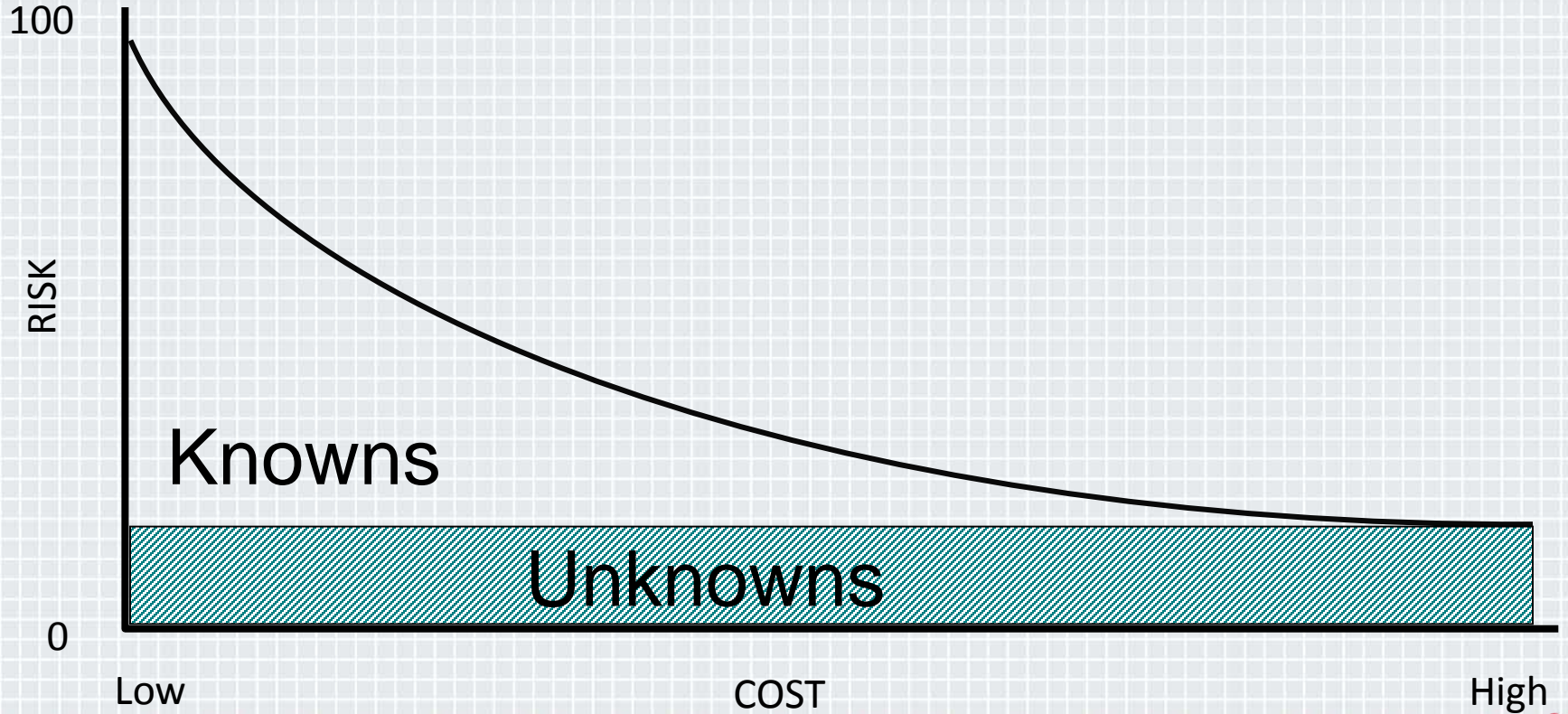
Side Case: Are We Sometimes Over Confident?

#RSAC

- ◆ What happens when there are things you think you know, but it turns out you did not know them or your information was wrong?
 - ◆ Total number of edge devices in your network
 - ◆ Complete and accurate list of all users
 - ◆ Supply sources of all equipment
 - ◆ Locations of all network connections, down to the cable
 - ◆ Names of highly trusted individuals with full access to sensitive systems
 - ◆ Time that it takes to detect and mitigate an incident
- ◆ This would be similar to a False Negative situation on an IDS or firewall
 - ◆ Bad passes through the control, but is marked as good
 - ◆ Leads to a false sense of confidence
- ◆ Some might say this is a variant of the “**unknown known**” case
 - ◆ It is certainly the worst case scenario, since you believe all is well but it's not
 - ◆ Perhaps we could call it the “**not-known known**” case

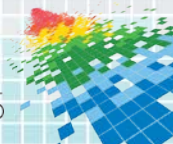


Managing Risk



Goal: Be More Secure Today Than You Were Yesterday

- ◆ Incidents by themselves are not a metric
 - ◆ Avoid focusing on how many incidents happened last year
 - ◆ Likewise, reporting the number of alerts, warnings, bulletins, etc. produced is not a measure of security
- ◆ Focus instead on awareness and reduction of the unknowns
 - ◆ Bonus: identify and reduce the unknown unknowns
- ◆ ***Since you cannot measure what you don't know, get rid of the unknowns!***





DBIR available at: <http://www.verizonenterprise.com/DBIR/2015/>

Ponemon Study: <http://www.lancope.com/ponemon-incident-response/>

Mandiant Reports: <https://www.mandiant.com/resources/mandiant-reports>

