Managing the Security Unknowns
Do We Know What We Don’t Know?

Marcus H. Sachs, P.E.
SVP and CSO, North American Electric Reliability Corporation
October 27, 2015
You cannot protect assets you don’t know about

You cannot defend against threats you are unaware of
“...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
LET’S DO AN EXERCISE....
The Seatbelt Project

RISK

COST

Low

High

String

Rope

Nylon

Kevlar

With Airbags

E-ISAC

Electricity Information Sharing and Analysis Center

Resiliency | Reliability | Security
The Security Project

E-ISAC

RESILIENCY | RELIABILITY | SECURITY
Managing Risk

Avoidable Risk

Unavoidable 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?
• 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
“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.”
• In nearly half of Verizon’s 2009 data breach forensics cases, investigators observed what are 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*
• Rather than counting what you know, risk management works better 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*
Unknown:
Who is Giving Away Your Passwords?
What Are Your Employees Doing?
Breaking News

Official Interest Rate remains unchanged at 3.75%.
Outer case says 50v 6800μF
Strange Item in the Equipment Yard
• 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....
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**

**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: 1  
[Add To Cart](#)

**ADD-ONS**

No accessories available.

*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.
<table>
<thead>
<tr>
<th>eBay Used Cisco Parts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Systems WIC-1DSU-T1-V2, 1-Port T1/Fractional T1 DSU/CSU Interface Card: V2</strong></td>
</tr>
<tr>
<td>Used Top Rated Plus</td>
</tr>
<tr>
<td><strong>Cisco T1 DSU/CSU WAN Interface Card - DSU/CSU - plug-in module - WIC - 1.544 Mbp</strong></td>
</tr>
<tr>
<td>Used Manufacturer refurbished</td>
</tr>
<tr>
<td><strong>Cisco T1 DSU/CSU WIC-1DSU/CSU-T1 1700 2600 3600 Interface Module Card</strong></td>
</tr>
<tr>
<td>Used Top Rated Plus</td>
</tr>
<tr>
<td><strong>Lot of 50- Cisco WIC-1DSU-T1-V2 T1 DSU/CSU WAN Interface Card + 90 Day Warranty</strong></td>
</tr>
<tr>
<td>Used</td>
</tr>
<tr>
<td><strong>Cisco 1-port T1/fractional T1 Dsu/csu Wan Interface Card</strong></td>
</tr>
<tr>
<td>New</td>
</tr>
<tr>
<td><strong>Cisco WIC-1DSU-T1-V2 T1 DSU/CSU WAN Interface Card + 90 Day Warranty</strong></td>
</tr>
<tr>
<td>Used</td>
</tr>
</tbody>
</table>
## Amazon’s Prices

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

by Cisco

*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](https://www.amazon.com/a-to-z-safe-buying-guarantee). Never respond to requests to send funds via wire transfer. Learn more about [Safe Online Shopping](https://www.amazon.com/safety).

### 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](https://www.amazon.com/sell).

### Showing: Used (22 from $4.00)

#### Sorted by: Price + Shipping

<table>
<thead>
<tr>
<th>Price + Shipping</th>
<th>Condition</th>
<th>Seller Information</th>
<th>Buying Options</th>
</tr>
</thead>
</table>
| **$4.00**        | **Used - Very Good** | Seller: **SAM Networks LLC**  
Seller Rating: **Just Launched** ([Seller Profile](https://www.amazon.com/seller/sam-networks-llc))
Ships in 1-2 business days. Ships from VA, United States.  
[Domestic shipping rates](https://www.amazon.com/delivery) and [return policy](https://www.amazon.com/returns). | [Add to Cart](#) or [Sign in](https://www.amazon.com/signin) to turn on 1-Click ordering. |
| **$7.50**        | **Used - Very Good** | ![DTS-HARDWARE](https://www.amazon.com/dts-hardware)  
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](https://www.amazon.com/delivery) and [return policy](https://www.amazon.com/returns).  
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](https://www.amazon.com/signin) to turn on 1-Click ordering. |
| **$8.40**        | **Used - Like New** | ![Genuine](https://www.amazon.com/genuine)  
Seller Rating: ★★★★ 95% positive over the past 12 months. (157 total ratings) | [Add to Cart](#) or [Sign in](https://www.amazon.com/signin) to turn on 1-Click ordering. |
Counterfeit Versus Genuine

http://www.andovercg.com/services/cisco-counterfeit-wic-1dsu-t1.shtml
• 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*)
We don’t know much about risks that are identifiable

We don’t know what risks exist

We know a lot about risks we can identify

We know risks exist that we can’t identify

What we know about things we know

A Lot

Nothing

Unknown Knowns

Known Knowns

Unknown Unknowns

Known Unknowns

E-ISAC

Electricity Information Sharing and Analysis Center

RESILIENCY | RELIABILITY | SECURITY
• 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
• 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
• **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
• **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

<table>
<thead>
<tr>
<th>What we know</th>
<th>We don’t know much about what we know</th>
<th>We know a lot about what we know</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System and machine logs</td>
<td>Internal/External Audit results</td>
</tr>
<tr>
<td></td>
<td>Calls to the help desk</td>
<td>Business records</td>
</tr>
<tr>
<td></td>
<td>Internal discussions</td>
<td>Lawsuits</td>
</tr>
<tr>
<td></td>
<td>Lessons learned but not shared</td>
<td>Press (good and bad)</td>
</tr>
<tr>
<td></td>
<td>Encrypted data/files</td>
<td>Measured impact of service loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>How long to recover from failure</td>
<td>Counterfeit/inferior hardware</td>
</tr>
<tr>
<td></td>
<td>Existence of undocumented devices, networks, or data</td>
<td>Social media postings</td>
</tr>
<tr>
<td></td>
<td>Dependencies on others</td>
<td>Unauthorized software</td>
</tr>
<tr>
<td></td>
<td>Former employee accounts</td>
<td>New versions of malware</td>
</tr>
<tr>
<td></td>
<td>Zero-days in software</td>
<td>Intentions of malicious insiders</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nothing</td>
<td>We don’t know what we don’t know</td>
<td>We know there are things we don’t know</td>
</tr>
</tbody>
</table>

**RESILIENCY | RELIABILITY | SECURITY**
• **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
• 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

RISK vs. COST

- **Knowns**
  - Low Risk, Low Cost
  - High Risk, High Cost

- **Unknowns**
  - Low Risk, High Cost
  - High Risk, Low Cost
• 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!
Questions and Answers

DBIR available at: http://www.verizonenterprise.com/DBIR
Mandiant Reports:  https://www.mandiant.com/resources/mandiant-reports