Gaining Buy-in

Resources to Manage Cybersecurity Risk in OT Environments

Jason Tugman
Vice President, Cyber Risk
Axio

Maggy Powell
Sr. Manager, Real Time Systems Security
Exelon

Gaining Buy-in

Resources to Manage Cybersecurity Risk in OT Environment

- Defining the current communication landscape
- What is Risk Debt and why should I care about it?
- Quantifying the “So what”
- Communicating the risk to gain buy-in

Jason Tugman
Vice President, Cyber Risk Engineering
Axio
jtugman@axio.com
571.251.8177

Maggy Powell
Sr. Manager, Real Time Systems Security
Exelon
Margaret.Powell@exeloncorp.com
410.470.3382 (desk)
410.949.7048 (cell)

The Communication Landscape

Starting with the end in mind … Gaining Buy-In

People – Who needs to understand?

- Decision Makers
- Other Impacted Partners
- Performers
- Competitive Dynamic
    - Comparative Advantage
    - Competing priorities
    - Decision making Hierarchy

Presentation –What is the story you need to tell?

- Understand Risk Management … one concern is relative to others
- Speak security, but put it in operational/business context
- Be Open
- Avoid fueling fear
- Don’t speak geek (at least not too much)

Analysis –Why does it Matter?

- Answer: “So What?” or “Why should I care?”
- Anticipate and explain the consequences of NOT taking action
- Be explicit about the costs over time

Risk Debt

What is it, why should I care, and what’s it have to do with gaining buy-in for OT resources?

Understanding Risk Debt in ICS Environments

What is Technical Debt

Technical Debt

Tech Debt is a concept in software development that reflects the implied cost of additional rework caused by choosing an easy solution now instead of using a better approach that would take longer.

Software Entropy

As a system is modified, its disorder, or entropy, tends to increase.
– Ivar Jacobson

Technical Debt

"Shipping first-time code is like going into debt. A little debt speeds development so long as it is paid back promptly with a rewrite. Objects make the cost of this transaction tolerable. The danger occurs when the debt is not repaid. Every minute spent on not-quite-right code counts as interest on that debt. Entire engineering organizations can be brought to a stand-still under the debt load of an unconsolidated implementation, object-oriented or otherwise."

- Ward Cunningham (1992)

Understanding Risk Debt in ICS Environments

What is Risk Debt?

Risk Debt

[Cyber] Risk Debt is the compounding cyber risk introduced into an environment due to a lack of asset visibility and the variance in which assets are configured, deployed, and maintained.

Risk vs Risk Management

> *"The amount of risk an organization has today is a lagging indicator of how it managed risk in the past."*
>
> *- Jack Freund & Jack Jones*

Risk Debt can also be expressed as 'Cyber Risk Entropy'

Risk Debt Interest Rate

Risk Debt, like financial debt, has a principal balance, an interest rate, and a compounding value:

- Principal Balance = number of assets
- Interest Rate = sum of the variations in asset deployment and configurations
- Compounding value = asset vulnerabilities*

*system, software, and process vulnerabilities

Understanding Risk Debt in ICS Environments

What's the 'So what' of Risk Debt?

Risk Debt

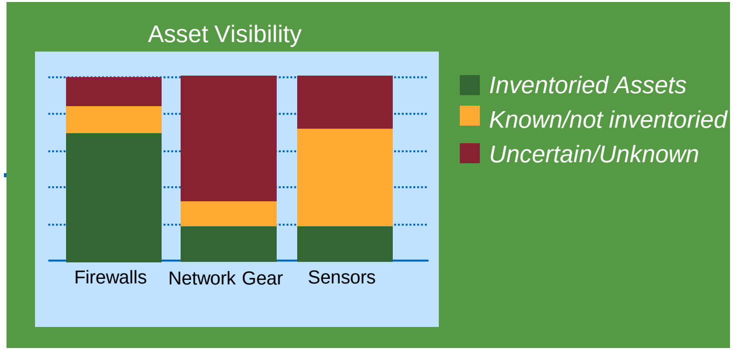
[Cyber] Risk Debt is the compounding cyber risk introduced into an environment due to a lack of asset visibility and the variance in which assets are configured, deployed, and maintained.

Measuring Risk Debt

Answering the question of what is known and what is unknown about the environment

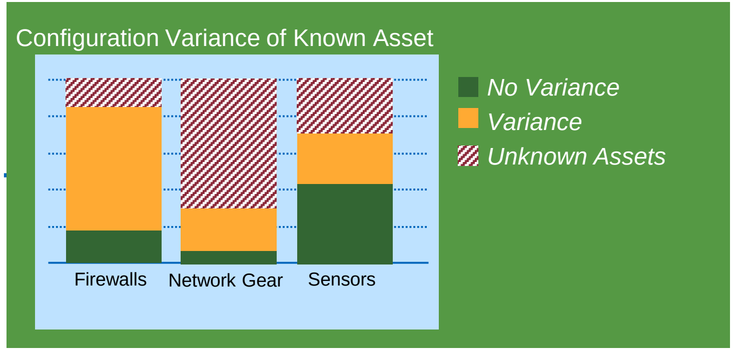
Visibility Metrics

- Assets that are known and inventoried
- Assets that are known but not inventoried
- Assets that are notionally known
- Assets that are unknown



Variance Metrics

- For all known assets within an asset-class configured the same?
- Are all known assets deployed in the same way?
- For all known assets maintained the same?



Quantifying Buy-in

How to answer the ’So what’

Quantifying Buy-in

Yes, but what about the next Zero Day?

> *OK, so Risk Debt is all fine good and wonderful, but all my Board/CIO/CISO want to know is how do we protect ourselves against the next Not Petya?*
>
> \- You, probably

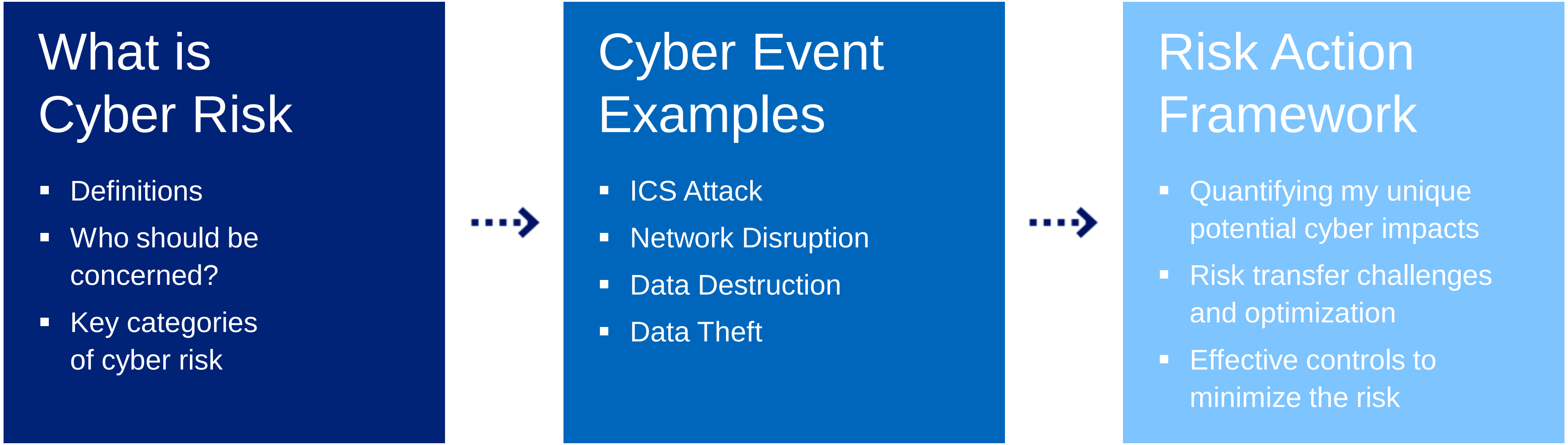
Quantifying Buy-in

Yes, but what about the next Zero Day?

> *If there is a problem to big to solve, there is a smaller problem you can solve; find it.*
>
> \- How to Solve It, George Polya (1945)

Quantifying Buy-in

Find the smaller problem and solve for it



What is Cyber Risk

- Definitions
- Who should be concerned?
- Key categories of cyber risk

Cyber Event Examples

- ICS Attack
- Network Disruption
- Data Destruction
- Data Theft

Risk Action Framework

- Quantifying my unique potential cyber impacts
- Risk transfer challenges and optimization
- Effective controls to minimize the risk

The objective is to make sense of a challenging problem space and leave you with a framework for action.

Quantifying Buy-in

Find the smaller problem and solve for it

ICS Attack

- Customer and Employee bank account info (ACH),credit cards, and other identity information is stolen (SSNs, address)
- Proprietary exploration and financial data is also suspected to be stolen

Network Disruption

- Attacker compromises network communications used to control field assets
- Production operations are impacted due to inability to control remote assets

Data Destruction

- A Shamoon-style attack deletes hard drive contents on every desktop and laptop computer in the enterprise overnight
- Business operations are severely impacted for 2 (or more) weeks while machines are either replaced/restored

Data Theft

- Customer and Employee bank account info (ACH),credit cards, and other identity information is stolen (SSNs, address)
- Proprietary exploration and financial data is also suspected to be stolen

Bringing It All Together

Risk Debt & Loss Scenarios

Analysis –Why does it Matter?

- Answer: “So What?” or “Why should I care?”
- Anticipate and explain the consequences of NOT taking action
- Be explicit about the costs over time

Communicating the risk to gain buy-in

Preparation Checklist

Are you ready to make the request?

ANALYSIS

- Can you explain the Analysis Process?
- Do you know the math? Are the numbers accurate, complete, and current?
- Can you show current and future costs?
- Have you considered alternatives?
- Can you convey the consequences of no action?

PEOPLE

- Is your boss aware, on board, and able to promote the project?
- Do you know the other impacted divisions/resources? Can you count on their support or do you need to address/pre-empt their concerns?
- Do you know who is making the decision?
- Do you know the decision makers' priorities and how this can fit in?

PRESENTATION

- Are you articulating a specific 'ask'?
- Have you articulated value in terms of the business?
- Are you showing why it is important, how it ranks relative to other priorities, and the consequences of denial?
- Is the request documentation clear, thorough and in the correct templates?
- Have you rehearsed with a trusted sounding board person?
- Have you run Spell Check?

REMINDER: Relax if it doesn't go your way … ask for feedback, cyber risks are never one and done.

Summary

This presentation:

- Established the Communication Landscape and the details important to gaining buy-in
- Discussed Risk Debt and Loss Scenario quantification concepts to convey the risks deserving of resources to mitigate

Questions?

Thank You!

Jason Tugman
Vice President, Cyber Risk
Axio
jtugman@axio.com
+ 1 571 251 8177

Maggy Powell
Sr. Manager, Real Time Systems Security
Exelon
Margaret.Powell@exeloncorp.com
410.470.3382 (desk)
410.949.7048 (cell)