ENERGYSEC
SERVING THE INDUSTRY´S SECURITY COMMUNITY SINCE 2004

Organizational Threat Modeling

Jack Whitsitt
jack@energysec.org | http://twitter.com/sintixerr

What is Threat Modeling? (Wikipedia)

Threat Modeling (Wikipedia)

- Threat Modeling is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, **threats** to the system.

Threat Modeling (Wikipedia)

- Addresses two distinct, but related, topics in computer security:
    1. a description of the security issues and resources the designer cares about. This is often represented as a Data Flow Diagram (DFD) that shows the potential attack points from outside the system.
    2. Threat modeling the development of attack trees, which are descriptions of a set of computer security aspects. That is, when looking at a piece of software (or any computer system), one can define a threat model by defining a set of possible attacks to consider.
- Each model defines a narrow set of possible attacks to focus on.
- Can help to assess the probability, the potential harm, the priority etc., of attacks to help security teams to minimize or eradicate the threats.
- Based on the notion that any system or organization has assets of value worth protecting, vulnerabilities, exploitation opportunities, and controls

Threat Modeling (Wikipedia)

- **Attacker-centric**
  - Attacker-centric threat modeling starts with an attacker, and evaluates their goals, and how they might achieve them. Attacker's motivations are often considered, for example, "The NSA wants to read this email," or "Jon wants to copy this DVD and share it with his friends." This approach usually starts from either entry points or assets.
- **Software-centric**
  - Software-centric threat modeling (also called 'system-centric,' 'design-centric,' or 'architecture-centric') starts from the design of the system, and attempts to step through a model of the system, looking for types of attacks against each element of the model. This approach is used in threat modeling in Microsoft's Security Development Lifecycle.
- **Asset-centric**
  - Asset-centric threat modeling involves starting from assets entrusted to a system, such as a collection of sensitive personal information.

Threat Modeling (Wikipedia)

- Define the application requirements:
  - Identify business objectives
  - Identify user roles that will interact with the application
  - Identify the data the application will manipulate
  - Identify the use cases for operating on that data that the application will facilitate
- Model the application architecture
  - Model the components of the application
  - Model the service roles that the components will act under
  - Model any external dependencies
  - Model the calls from roles, to components and eventually to the data store for each use case as identified above
- Identify any threats to the confidentiality, availability and integrity of the data and the application based on the data access control matrix that your application should be enforcing
- Assign risk values and determine the risk responses
- Determine the countermeasures to implement based on your chosen risk responses
- Continually update the threat model based on the emerging security landscape.

Threat Modeling: Other Examples

OWASP: Threat Models

- A threat model is essentially a **structured representation of all the information that affects the security of an application**. In essence, it is a view of the application and its environment through security glasses.
- Threat modeling is **a process for capturing, organizing, and analyzing all of this information**. Threat modeling enables informed decision-making about application security risk. In addition to producing a model, typical threat modeling efforts also produce a prioritized list of security improvements to the concept, requirements, design, or implementation.

OWASP Threat Modeling: Basic Steps

- **Step 1:** Decompose the Application
  - Gain an understanding of the application and how it interacts with external entities
  - Create use-cases to understand how the application is used, identifying entry points to see where a potential attacker could interact with the application
- **Step 2:** Determine and rank threats
  - Threat categorization helps identify threats both from the attacker and the defensive perspective
  - Attacker threats can be identified as the roots for threat trees; there is one tree for each threat goal
  - Defensive categorization helps to identify the threats as weaknesses of security controls for such threats
  - Use and abuse cases can illustrate how existing protective measures could be bypassed, or where a lack of such protection exists
- **Step 3:** Determine countermeasures and mitigation
  - A lack of protection against a threat might indicate a vulnerability whose risk exposure could be mitigated with the implementation of a countermeasure

https://www.owasp.org/index.php/Application_Threat_Modeling

STRIDE:

Modeling Threats from an Attacker Point of View

- Spoofing identity
- Tampering with data
- Repudiation
- Nonrepudiation
- Information disclosure
- Denial of service
- Elevation of privilege

https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

“Whole System”

But...

Why just applications?

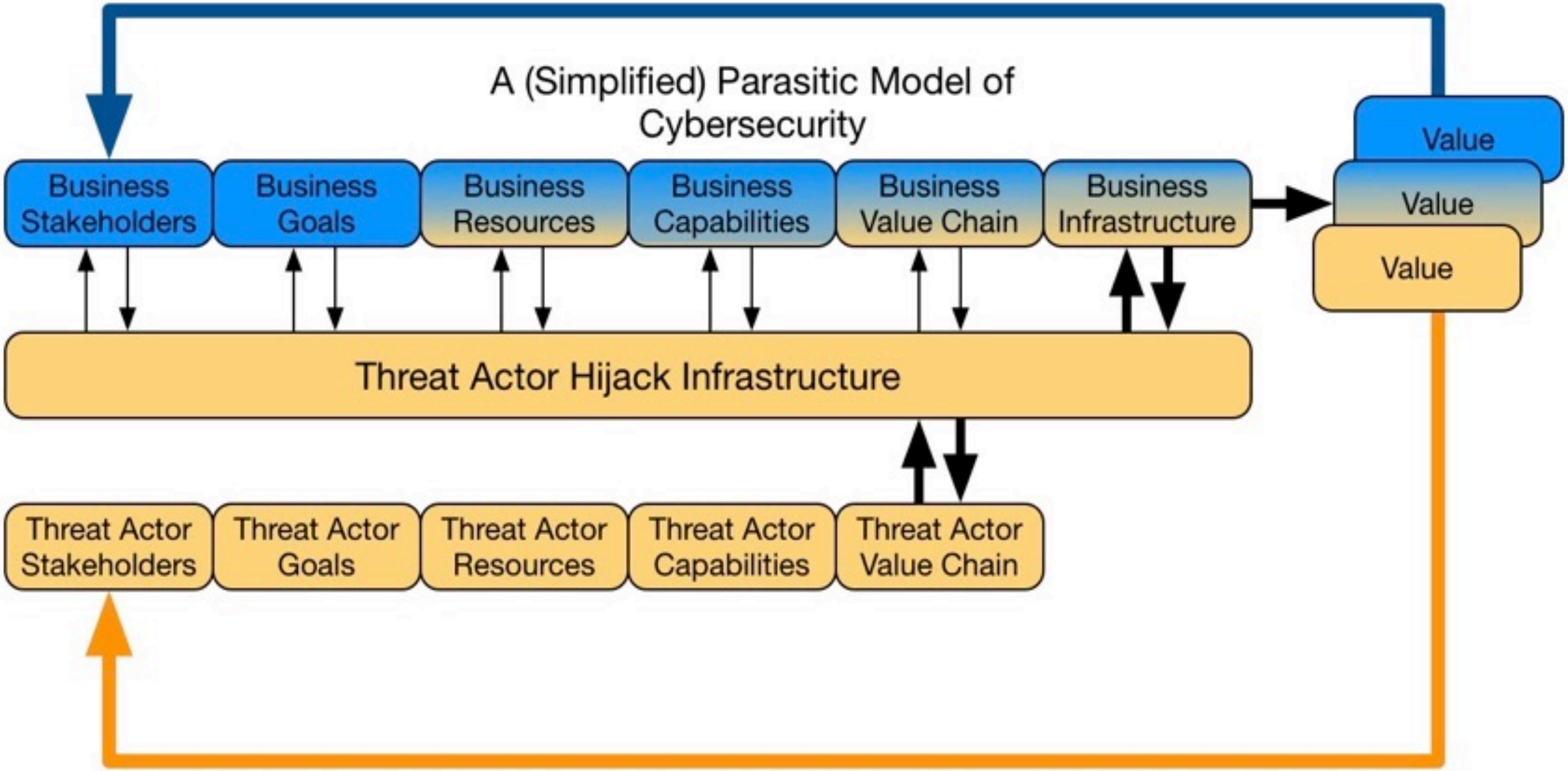
Why not the Whole System?

Sufficiency?

- Application Threat Modeling Process Leaves out massive components of systems
  - Systems Don't Stop with Applications
  - Systems Don't Stop with Technology
  - Technology is simply a part of our larger business processes, value chains, etc.
- If we want to understand our *real* threat, cannot exclude parts of the system
  - Gives false, incomplete, and misleading threat perspectives
- Limited definitions point to misaligned solutions
- Need to better understand what actual threat landscape looks like and what the security model is actually protecting against than what is possible by limiting threat modeling to applications

Piecemeal Modeling

A good “Whole System” Model: Parasites

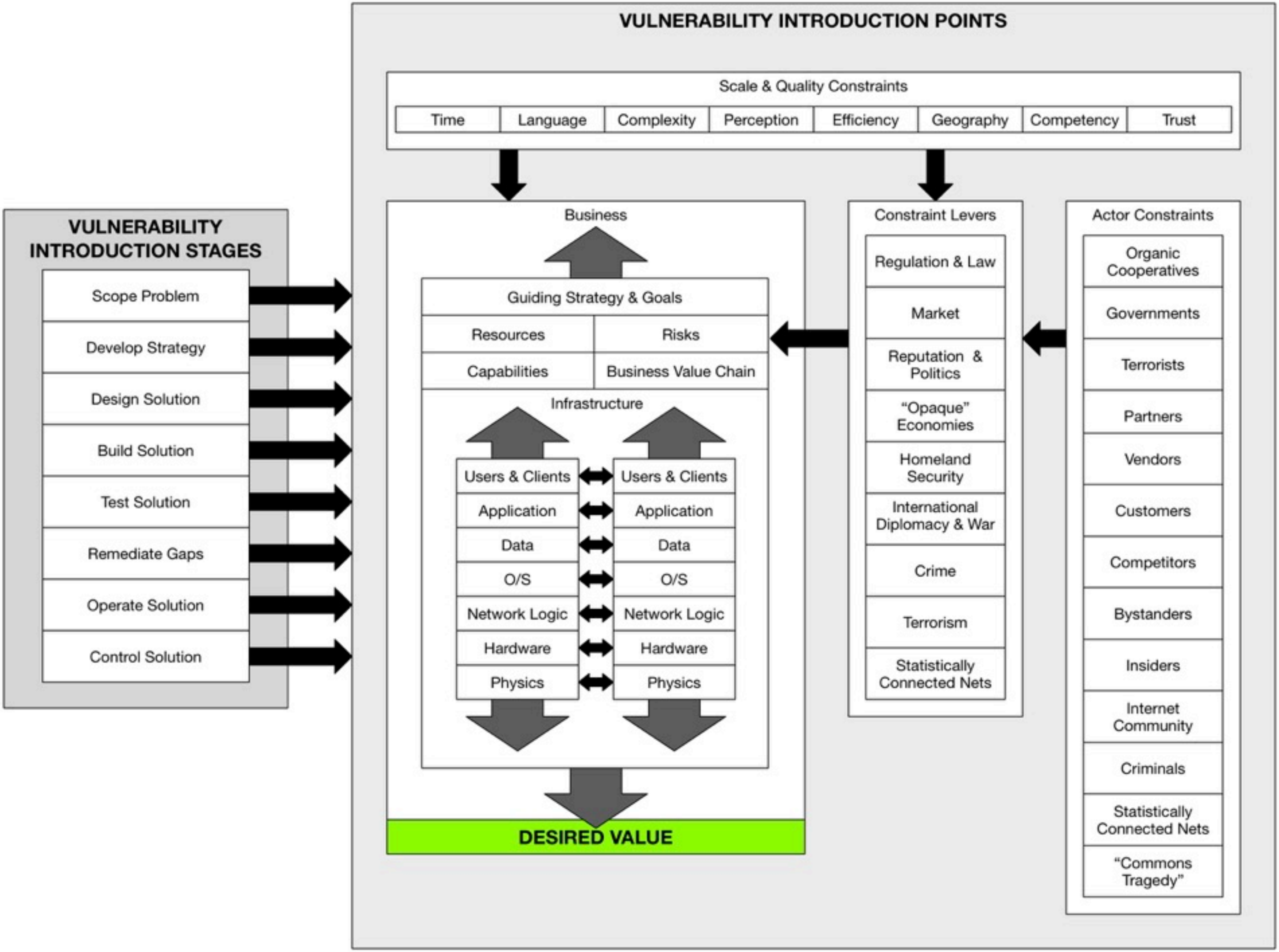


Parasites

- Two Sides, One side is comprised of your peers
  - Opposing Pressure
  - But…not…inside/out
  - Instead, competing with you to…
- Hijack value
  - Value is what we want to produce
  - They want to Stop, Alter, Inject value
  - Use Cyber systems to influence value chain or value chain to access cyber systems
  - Once you connect infrastructure to the internet, it's not yours
  - **All infrastructure is connected to the internet; data passes**
- Parasites not a typical natural situation
  - Hurricanes, Floods, Earthquakes do not take advantage of gaps intentionally
  - Actors using ICT/Cyber systems will
  - Thinking, reacting, adaptable: Solving for solution
  - Huge difference between old automated threats and today's (leads to exposure)

Why can Parasites Attach?

- Humans Fill Roles
- In Roles, they Fulfill Goals
- Within Constraints (Positive/Negative Resources)
- By Coming to Decisions
- And Taking Action
- These Actions May Create System States that
  - Create vulnerable system states that can be immediately exploited
  - Contribute to a vulnerable system state that, in concert with other actions, lead to a state that can be exploited
  - Limit other future actions of the system that will likely lead to an exploitable system state


VULNERABILITY INTRODUCTION STAGES
Scope Problem
Develop Strategy
Design Solution
Build Solution
Test Solution
Remediate Gaps
Operate Solution
Control Solution
VULNERABILITY INTRODUCTION POINTS
Scale & Quality Constraints
Time
Language
Complexity
Perception
Efficiency
Geography
Competency
Trust
Business
Guiding Strategy & Goals
Resources
Risks
Capabilities
Business Value Chain
Infrastructure
Users & Clients
Application
Data
O/S
Network Logic
Hardware
Physics
Users & Clients
Application
Data
O/S
Network Logic
Hardware
Physics
DESIRED VALUE
Constraint Levers
Regulation & Law
Market
Reputation & Politics
"Opaque" Economies
Homeland Security
International Diplomacy & War
Crime
Terrorism
Statistically Connected Nets
Actor Constraints
Organic Cooperatives
Governments
Terrorists
Partners
Vendors
Customers
Competitors
Bystanders
Insiders
Internet Community
Criminals
Statistically Connected Nets
"Commons Tragedy"

So What is “Security”?

- **Secure system:** One that does no more or less than we want it to for the amount of effort and resources we’re willing to invest in it.

- **Cybersecurity:** The enablement of **an environment in which business objectives are sustainably achievable by Information Security, Control Systems Security, and Other Related Security Activities** in the face of continuous risk resulting from the use of cyber systems.

- **Cyber Risk:** the possibility that actors will use our systems as a means of repurposing our value chains to alter the value produced, inhibit the value produced, or produce new value in support of their own value chains.

How attacks work: Exploitation Opportunities

Goal + Exposure + Timing

– The longer the time window, the higher the complexity of the environment, the more likely there will be the right combination of errors/ exposures and timing to create an exploitation opportunity

– Exploitation Opportunities are chained together to achieve goals

Threat Modeling Redefined

Organizational Threat Modeling

- Threat Modeling is a procedure for optimizing **ORGANIZATIONAL security** by identifying **BUSINESS objectives** and **VULNERABILITY INTRODUCTION POINTS STEMMING FROM OR AFFECTING THE USE OF CONNECTED TECHNOLOGY**, and then defining **BUSINESS LEVERS** to **prevent**, or mitigate the effects of threats to the **PRODUCTION OF VALUE FOR STAKEHOLDERS**.

Organizational Threat Modeling

- Addresses two distinct, but related, topics in computer security:
  - a description of the security issues and resources **STAKEHOLDERS** care about. This is often represented as a **????** that shows the potential **VULNERABILITY INTRODUCTION POINTS CREATED BY THE SYSTEM**.
  - Threat modeling the development of attack trees, which are descriptions of a set of **computer security aspects**. That is, when looking at a **BUSINESS**, one can define a threat model by defining a set of **possible attacks** to consider.
- Each model defines a narrow set of possible attacks to focus on.
- Can help to assess the probability, the potential harm, the priority etc., of attacks to help **THE BUSINESS CHANGE THE BEHAVIOR THAT INTRODUCES THE EXPOSURE TO SUCH ATTACKS**
- Based on the notion that any system or organization has assets of value worth protecting, vulnerabilities, exploitation opportunities, and controls

Organizational Threat Modeling

- **Attacker-centric**
  - Attacker-centric threat modeling starts with an attacker, and evaluates their goals, and how they might achieve them. Attacker's motivations are often considered, for example, "The NSA wants to read this email," or "Jon wants to copy this DVD and share it with his friends." This approach usually starts from either **BUSINESS OR TECHNICAL entry points.**
- **TECHNICAL SYSTEM-centric**
  - Software-centric threat modeling (also called 'system-centric,' 'design-centric,' or 'architecture-centric') starts from the design of the system, and attempts to step through a model of the system, looking for types of attacks against each element of the model
- **Asset-centric**
  - Asset-centric threat modeling involves starting from assets entrusted to a system, such as a collection of sensitive personal information.
- **DEFENDER-CENTRIC**
  - **Starts with existing Information Security Capabilities and extrapolates out to Business, Asset, Attacker, and Technical System protections. Could also be called “Control-Centric”**
- **BUSINESS ARCHITECTURE CENTRIC**
  - **Looks at how the way a business creates value – its capabilities, business units, value chains, supply meshes, etc. - introduces exposure or can be exploited through connected technology**

How do we begin?

Multiple Starting Points

- Goal: Develop Converged Model of Threats
- Multiple Entry Points Possible:
  - Business Architecture-Centric
  - Attacker-Centric
  - Asset-Centric
  - Technical System-Centric
- Where you start depends on where you have
  - The most information
  - The greatest span of influence
- Business Architecture-Centric should still always be the top level model, if not the first developed
  - It is "The Point" of it all

Business Architecture-Centric

We have to know how our Business generates exposure and how it is exploited from a “Value Hijacking” perspective.

From there we can model our exposure and use what we know about our exposure – and theirs – to maintain control of the value we produce

Attacker-Centric: Cyber Kill Chain

1. Recon
2. Weaponize
3. Deliver
4. Exploit
5. Install
6. Create persistence
7. Control
8. Move laterally
9. Escalate privilege
10. Action on Objectives
11. Re-Use or Re-Sell Access

Looks Like a Business Value Chain

Asset-Centric: Hard or Soft Assets

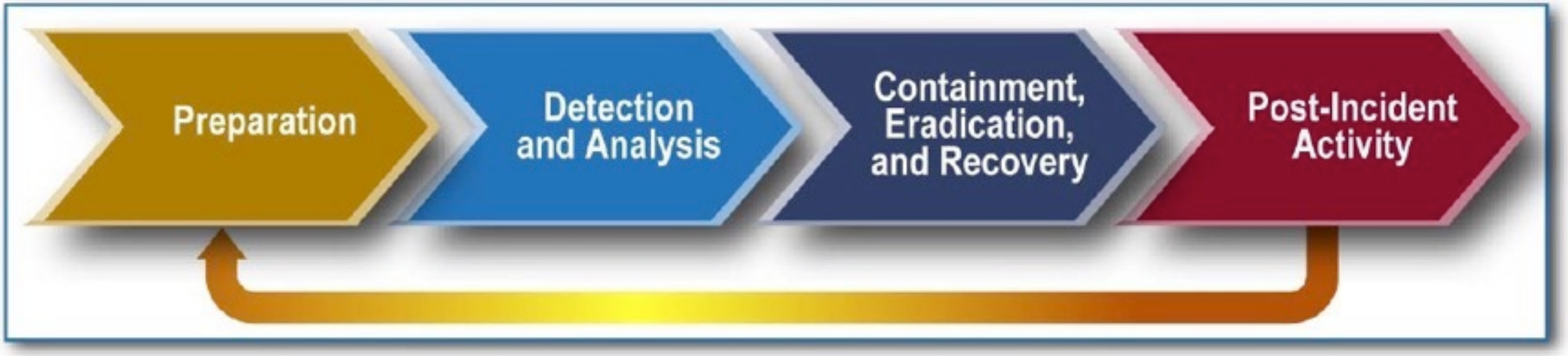
- Asset definition often mistakenly limited to “pieces of hardware”
- Instead, are discrete “Goals” to be protected
- Can be
  - Data
  - System Functionality
  - Executive Goals
  - Hardware
  - Value Production
- Protecting Assets is NOT the same as Limiting Attacker Objectives, Protecting Technical Systems, or Executing Defender Capabilities Effectively
- The point is to list things that need to be achieved and work back through the other threat modeling perspectives to assure these assets are protected in a coordinated way

Technical System-Centric

- Often, the Threat Modeling process is started when a technical system is being designed, built, or changed
- At this point, the goal is not to protect the technical system, but to identify ways the technical system can achieve goals and ways it can be misused to negatively impact goals
- Use other threat modeling perspective to then bridge that gap

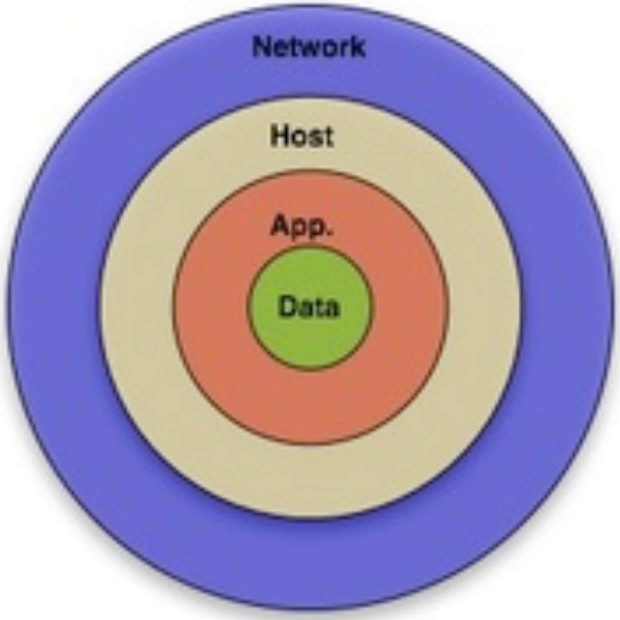
Defender-Centric:
Information Security Common Practices

- Sometimes our span of influence exists only in the realm of classic information security controls
- Starting from a defenders point of view should involve listing capabilities, controls AND their limitations
- Use capability/control architecture to identify uncontrolled risks
  - Helps inform Business Architecture, Asset, and Technical System Threat Models



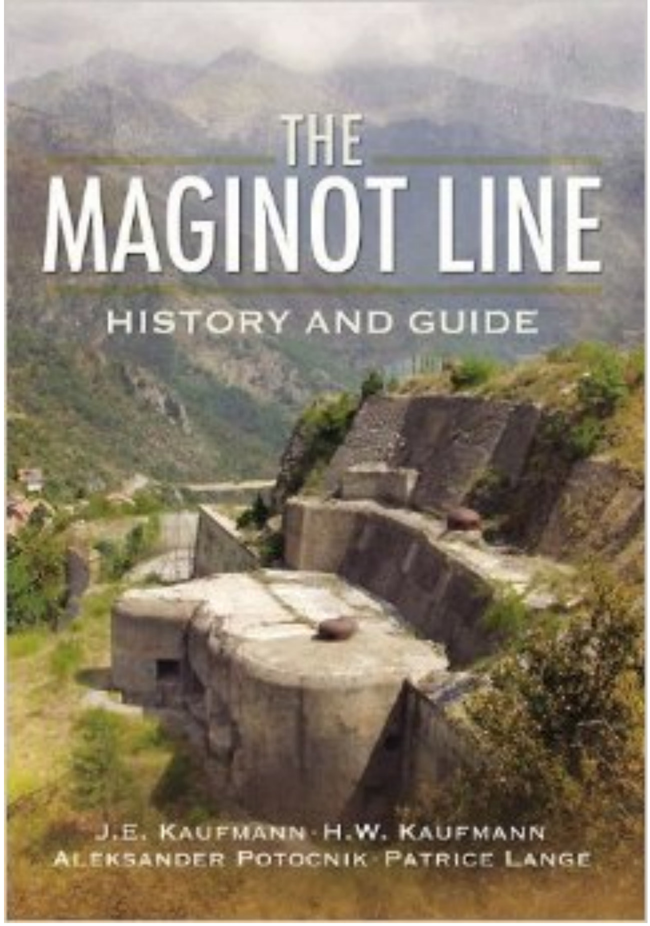
Beyond Threat Modeling (What to do with it)

Inform Defense In Depth



~~Defense In Depth~~

~~Defense In Depth~~


THE
MAGINOT LINE
HISTORY AND GUIDE
J.E. KAUFMANN · H.W. KAUFMANN
ALEKSANDER POTOCNIK · PATRICE LANGE

So What Is Defense In Depth?

- Operating Effectively in a Conflict Zone:
  - Managing a ~~city~~ system under siege
  - Where everyone is a potential threat
  - While providing sufficient service in the middle of the conflict indefinitely
  - **By Limiting problem space and improving ability to take effective, timely action**
  - **Through effective Analysis and Decision Making**

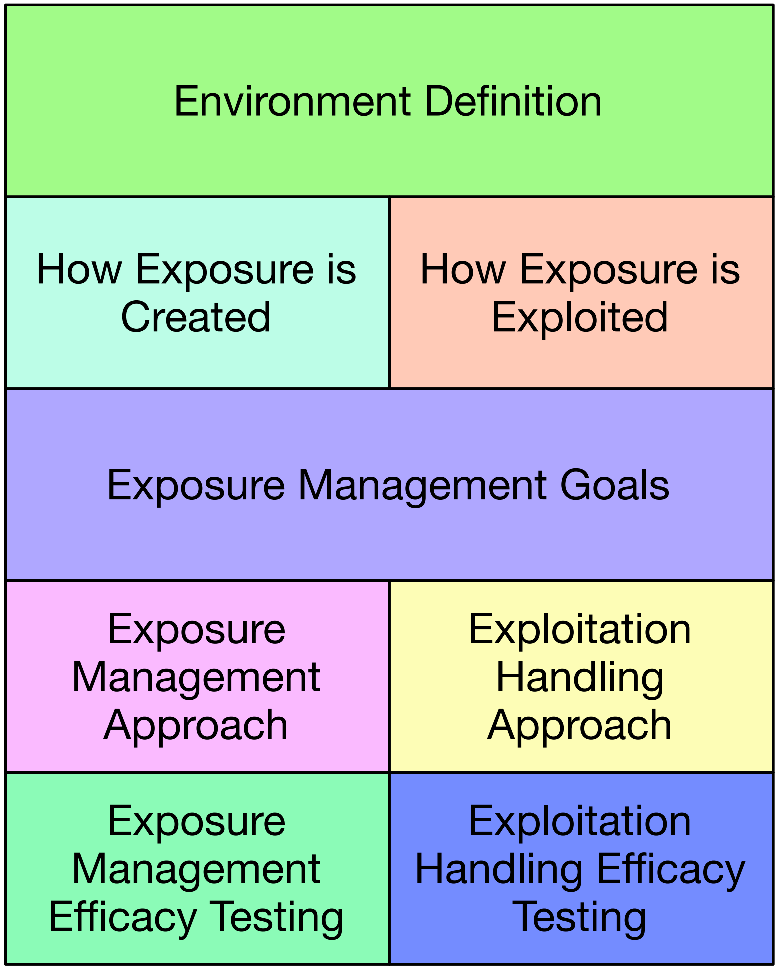
Defense In Depth

- Quality Defense in Depth Decision Making
  - Demands efficiency
    - Limit exposure area and utilize kill zones
  - Is agile
    - Can arrive at good enough quality answers in enough time to navigate thoughtful enemies with objectives
  - Relies on
    - Sufficient Supporting information
    - Involvement of Whole System
    - Effective tools
    - Actionable, defined, limited, specific non-security goals

Beyond Threat Modeling: Creating a Kill Zone

- We have Mixed/competing priorities and Limited Resources
  - In real life, it might not be possible to protect against everything for given $$, so what and how to decide?
  - Threat modeling first, consolidation, then prioritization
  - Prioritization based on most effect for least cost and most sustainable effort
  - Look at VIP Chains
  - Create Kill Zone
- This might not be a typical definition of “Kill Zone” ☺

High Level Overview



Environment Definition

How Exposure is Created

How Exposure is Exploited

Exposure Management Goals

Exposure Management Approach

Exploitation Handling Approach

Exposure Management Efficacy Testing

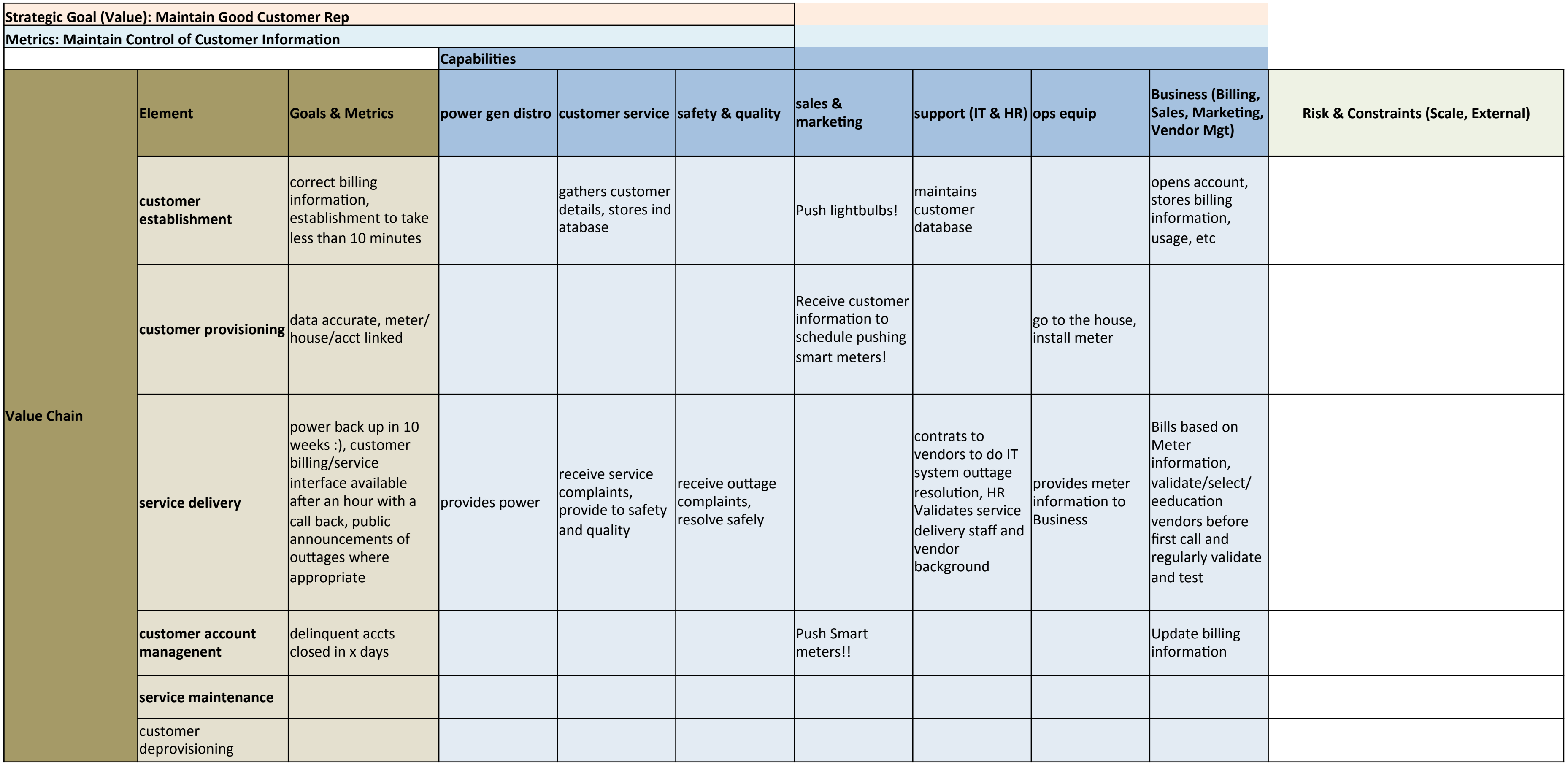
Exploitation Handling Efficacy Testing

Example Process

High Level Example Process

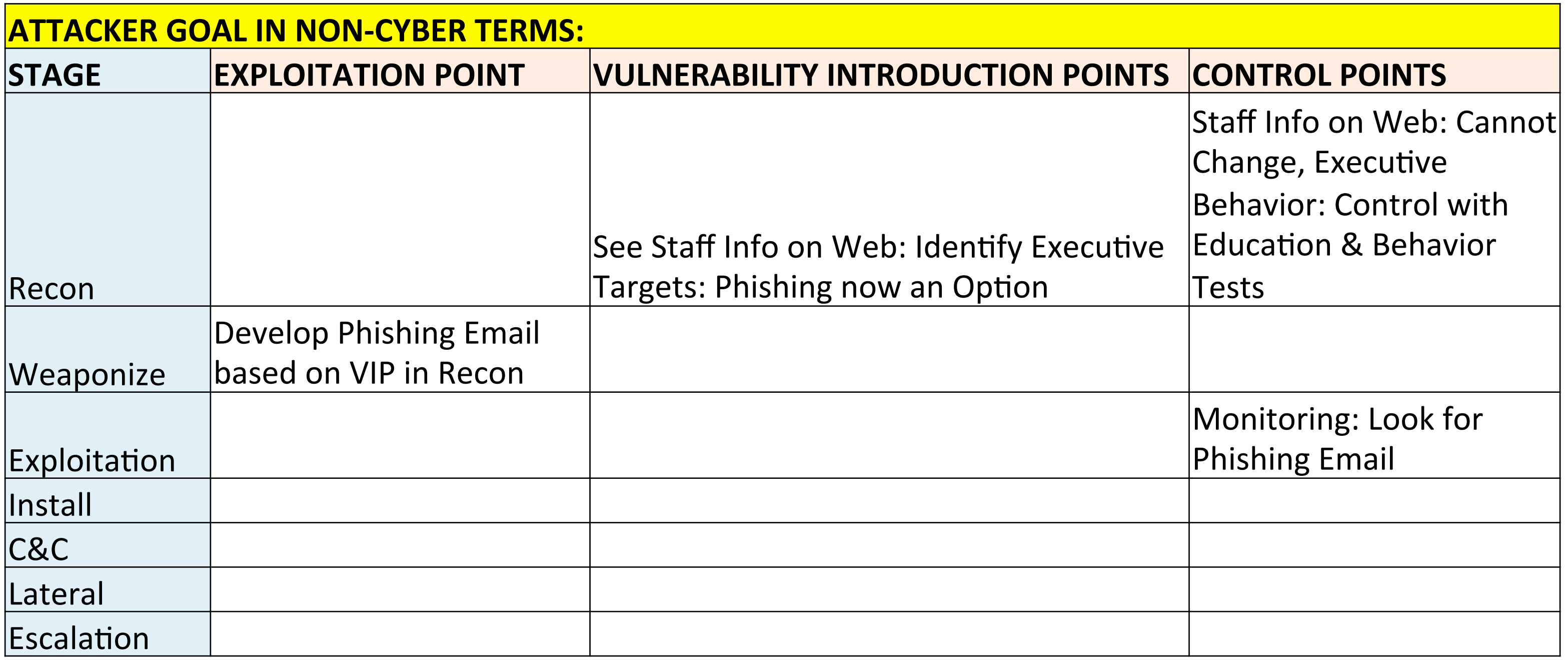
1. Document Business Architecture
2. Model Several Attacker Contexts with Kill Chains Against Business Architecture
3. Model Necessary Defender Capabilities and Limitations
4. Identify Business Capability Gaps, Prioritize, Determine Levers (ie, insert into Enterprise Risk Management Process)

Step 1: Business Architecture Documentation



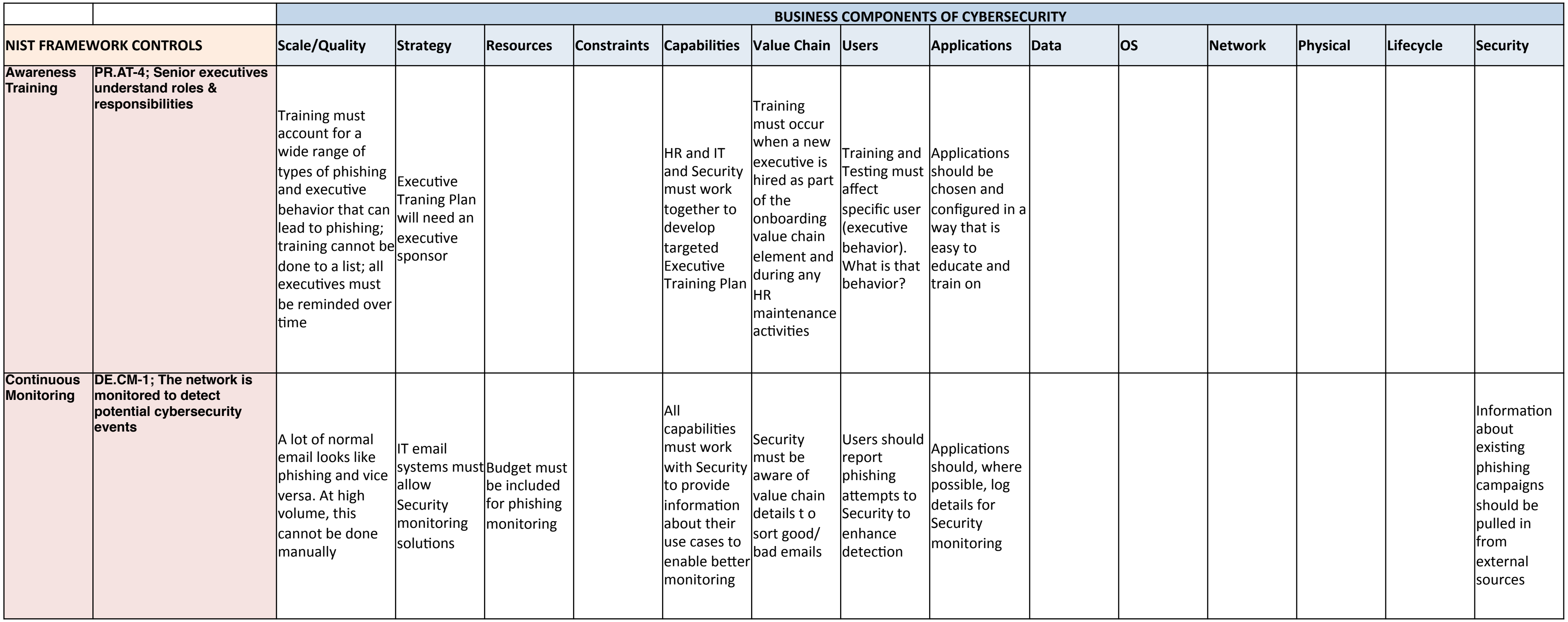
Strategic Goal (Value): Maintain Good Customer Rep										
Metrics: Maintain Control of Customer Information										
			Capabilities							
	Element	Goals & Metrics	power gen distro	customer service	safety & quality	sales & marketing	support (IT & HR)	ops equip	Business (Billing, Sales, Marketing, Vendor Mgt)	Risk & Constraints (Scale, External)
Value Chain	customer establishment	correct billing information, establishment to take less than 10 minutes		gathers customer details, stores ind atabase		Push lightbulbs!	maintains customer database		opens account, stores billing information, usage, etc	
	customer provisioning	data accurate, meter/ house/acct linked				Receive customer information to schedule pushing smart meters!		go to the house, install meter		
	service delivery	power back up in 10 weeks :), customer billing/service interface available after an hour with a call back, public announcements of outtages where appropriate	provides power	receive service complaints, provide to safety and quality	receive outtage complaints, resolve safely		contrats to vendors to do IT system outtage resolution, HR Validates service delivery staff and vendor background	provides meter information to Business	Bills based on Meter information, validate/select/ eeducation vendors before first call and regularly validate and test	
	customer account management	delinquent accts closed in x days				Push Smart meters!!			Update billing information	
	service maintenance									
	customer deprovisioning									

Step 2: Model Several Attacker Contexts



ATTACKER GOAL IN NON-CYBER TERMS:			
STAGE	**EXPLOITATION POINT**	**VULNERABILITY INTRODUCTION POINTS**	**CONTROL POINTS**
Recon		See Staff Info on Web: Identify Executive Targets: Phishing now an Option	Staff Info on Web: Cannot Change, Executive Behavior: Control with Education & Behavior Tests
Weaponize	Develop Phishing Email based on VIP in Recon		
Exploitation			Monitoring: Look for Phishing Email
Install			
C&C			
Lateral			
Escalation			

Step 3: Model Defender Capabilities Against Business & Technical Architecture



		BUSINESS COMPONENTS OF CYBERSECURITY													
NIST FRAMEWORK CONTROLS		Scale/Quality	Strategy	Resources	Constraints	Capabilities	Value Chain	Users	Applications	Data	OS	Network	Physical	Lifecycle	Security
Awareness Training	**PR.AT-4; Senior executives understand roles & responsibilities**	Training must account for a wide range of types of phishing and executive behavior that can lead to phishing; training cannot be done to a list; all executives must be reminded over time	Executive Traning Plan will need an executive sponsor			HR and IT and Security must work together to develop targeted Executive Training Plan	Training must occur when a new executive is hired as part of the onboarding value chain element and during any HR maintenance activities	Training and Testing must affect specific user (executive behavior). What is that behavior?	Applications should be chosen and configured in a way that is easy to educate and train on						
Continuous Monitoring	**DE.CM-1; The network is monitored to detect potential cybersecurity events**	A lot of normal email looks like phishing and vice versa. At high volume, this cannot be done manually	IT email systems must allow Security monitoring solutions	Budget must be included for phishing monitoring		All capabilities must work with Security to provide information about their use cases to enable better monitoring	Security must be aware of value chain details t o sort good/ bad emails	Users should report phishing attempts to Security to enhance detection	Applications should, where possible, log details for Security monitoring						Information about existing phishing campaigns should be pulled in from external sources

Step : Insert into Risk Management Process

Business Goal Impacted	Business Goal Priority	Attacker Goal 1 NIST Control Points	Number of times in Attack Tree Control Point occurs	C2M2 Capability	C2M2 Capability Priority
Protect Reputation by Protecting Customer Info	5	PR.AT-4: Exec Eductation	1	Workforce Development	5 (5x1)
		DE.CM-1: Monitoring	1	Situational Awareness	5 (5x1)

Closing

Limitations

- Managing People isn't Binary
  - But yet we do it all of the time
- Systems are Large and Complex when defined this way
  - Need to set scope that matches with influence and account for out of scope components as risks
- We cannot account for all possibilities
  - Modeling several scenarios should be sufficient

Thank you!

Jack Whitsitt
jack@energysec.org | http://twitter.com/sintixerr