A Game Theoretic Approach to Minimizing Cybersecurity Risk

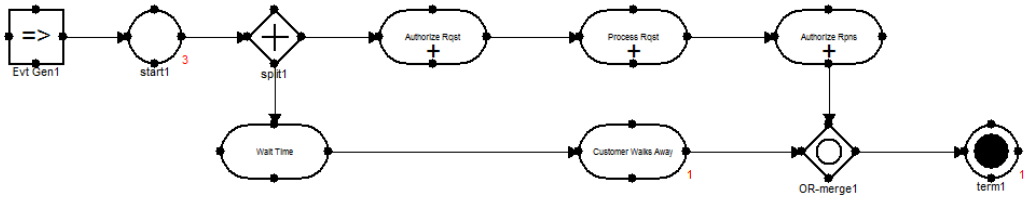
Presenter:

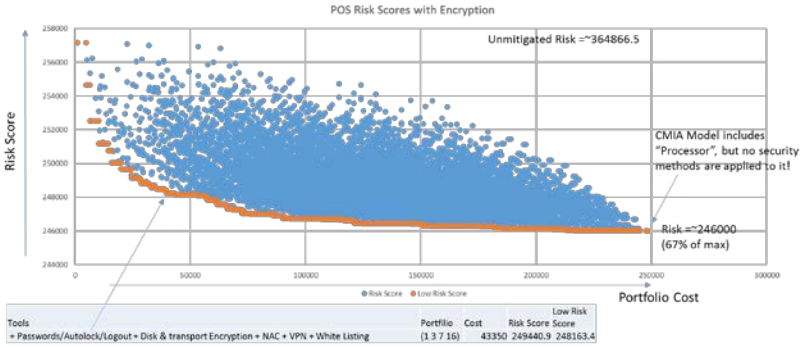
Scott Musman

smusman@mitre.org

Andrew Turner

ajturner@mitre.org





April 2017

MBE Summit

Approved for Public Release: Cases # 16-3240 and 16-3460

MITRE

Why Model-based Cybersecurity Engineering?

- **How do you build security in, rather than bolt it on?**
- **Common techniques like heat maps over-focus on compliance, the reliance on "best practice", or qualitative assessments**
- **Improving security and resilience costs money, so how do you justify that expense and maximize your ROI?**
- **Today's cybersecurity risk assessments have not provided the information they need to make well-informed cybersecurity decisions.**
- **Your ultimate goal should be to help your organization succeed**
- **Here we will describe a risk assessment/mitigation method that computes cybersecurity risks/mitigations using models of your system**

Question: What is Your Single Biggest Risk in Cybersecurity?

Answer: How You Measure Cybersecurity Risk and Your Ability to Reduce it

Source: Doug Hubbard – How to measure anything in Cybersecurity

  - The method implements a consistent, coherent approach for estimating risk
  - It formalizes the information gathering activities into computable artifacts
  - The models provide traceable artifacts representing your knowledge mission, system and assumptions that contribute to your risk assessments

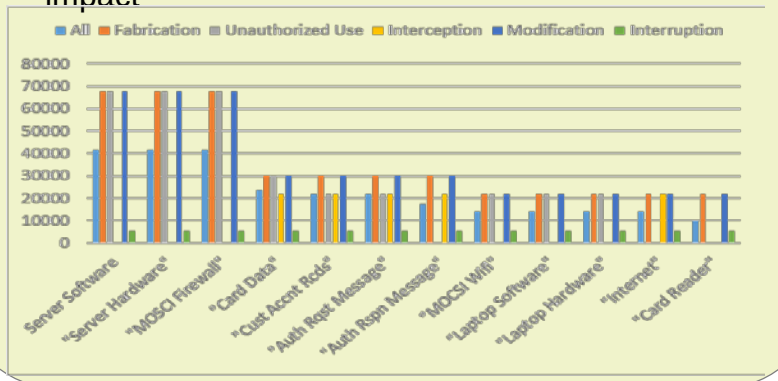
BLUF: Cyber Mission Impact Assessment (CMIA) and Cyber Security Game (CSG)

Cyber Mission Impact Assessment (CMIA) and Cyber Security Game (CSG) makes it possible to:

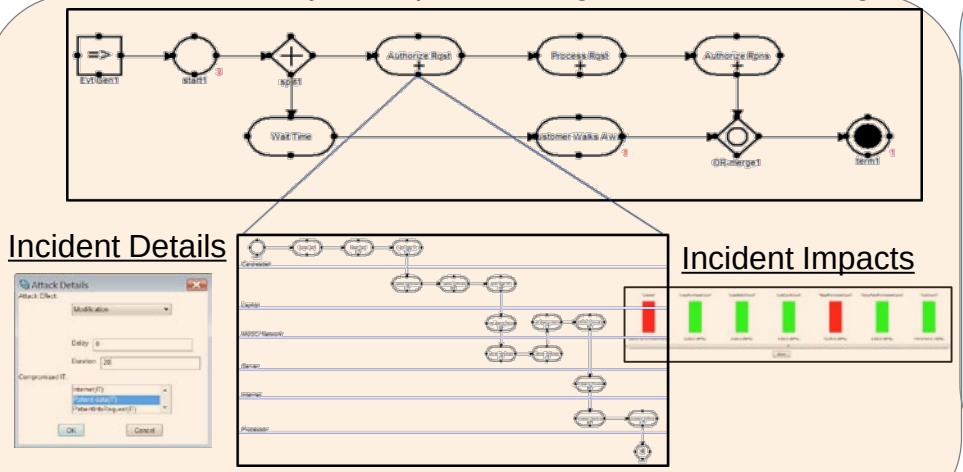
- Represent a System and its cyber dependencies
- Assess the operational impact of cyber incidents
- Produce a quantitative Cyber Crown Jewels analysis
- Assess Cyber Risk
- Guide mitigation engineering by identifying which incident types must be prevented, and where they should be prevented
- Use a game formulation for course of action (CoA) decision making, targeted improvements and to optimize cyber security investment decisions

CMIA Analysis Enables:

- An estimate of Cyber Incident Impacts
- Quantitative identification of Cyber Crown Jewels
- Identification of which incidents, when, where, cause impact

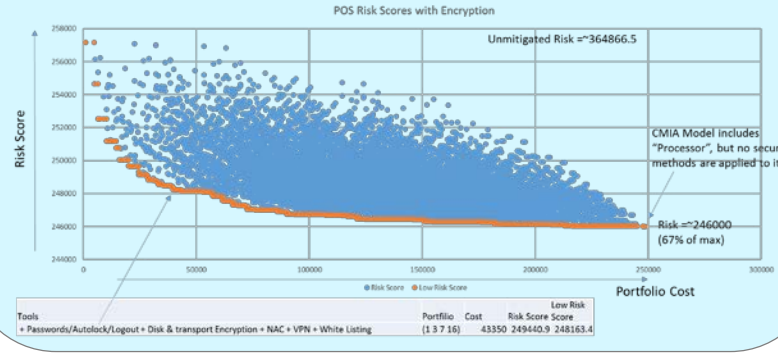


CMIA Models Cyber Impacts through Process Modeling



CSG Analysis Enables:

- An estimate of the systems cyber risk
- An assessment of how security tools reduce risk
- Optimization of security portfolio investments



MITRE

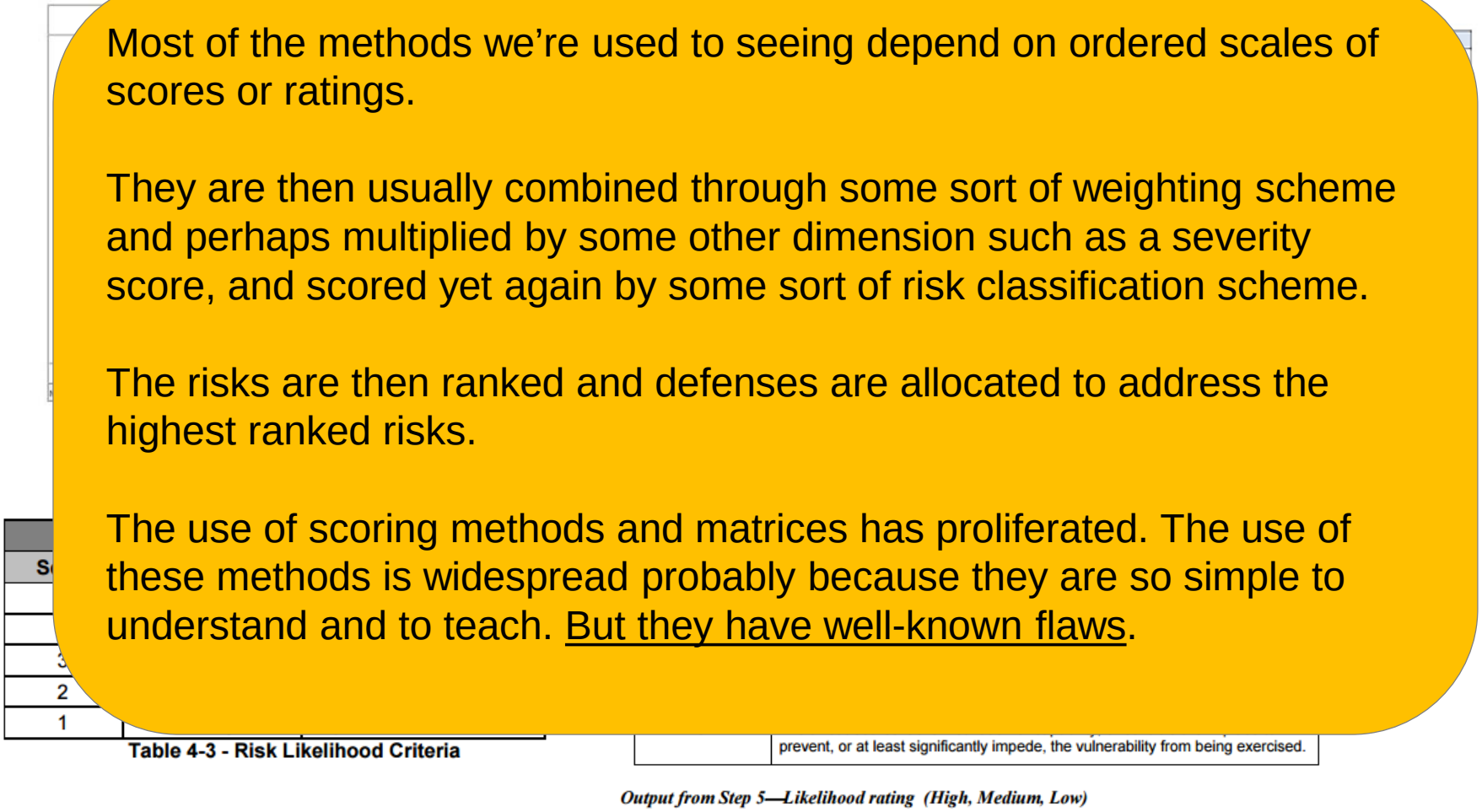
Cybersecurity Risk Management as You Currently See It Applied

Most of the methods we're used to seeing depend on ordered scales of scores or ratings.

They are then usually combined through some sort of weighting scheme and perhaps multiplied by some other dimension such as a severity score, and scored yet again by some sort of risk classification scheme.

The risks are then ranked and defenses are allocated to address the highest ranked risks.

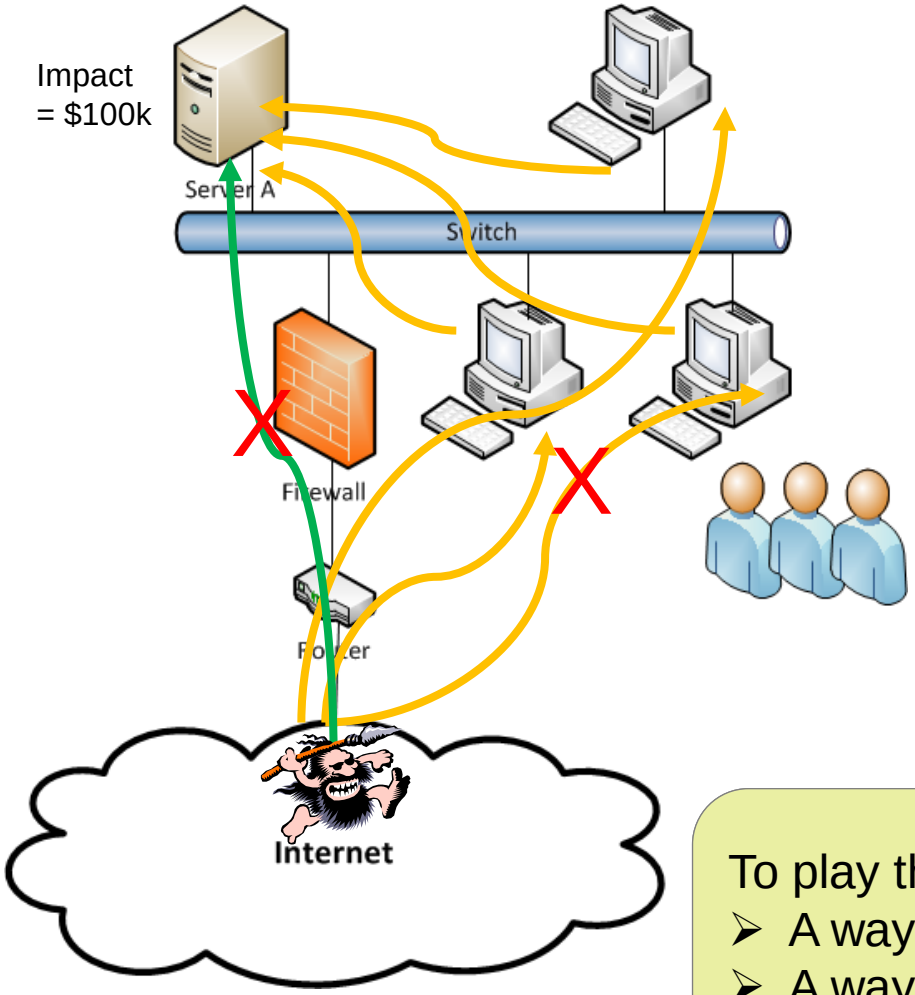
The use of scoring methods and matrices has proliferated. The use of these methods is widespread probably because they are so simple to understand and to teach. But they have well-known flaws.

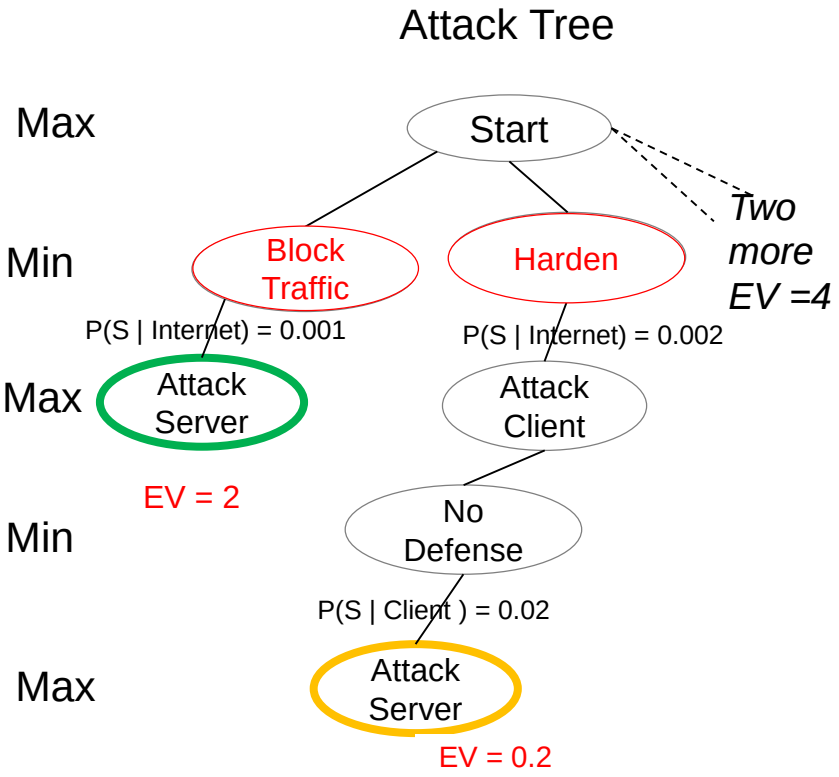


Known limitations of current practice

- **The use qualitative labels rather than quantitative numbers**
  - Even rigorously defined scoring scales cannot be applied predictably and consistently
  - Qualitative methods cannot provide prescriptive advice
- **Factors tend to be scored and treated as independent variables, ignoring the well-known problem of correlation**
  - One cannot even produce a reasonable rough estimate if correlation and interaction assumptions are incorrect
- **Risk Matrices introduce systemic errors that lead to misranking**
  - Iso-risk contours are convex curves, not straight
  - According to Tony Cox: "…they can be 'worse than useless,' leading to worse-than-random decisions."
- **Commonly accepted security properties like "privilege restriction", "diversity" and protection of non-critical resources are not captured**
  - Knowledge of component type, and network topology is not explicitly represented
- **Allocating risk management resources based on risk priority rankings is ineffective**
  - Greedy allocation schemes are known to be sub-optimal
  - Ranking omits information essential for optimization: How will an adaptive attacker respond?

Cybersecurity and the Adversary



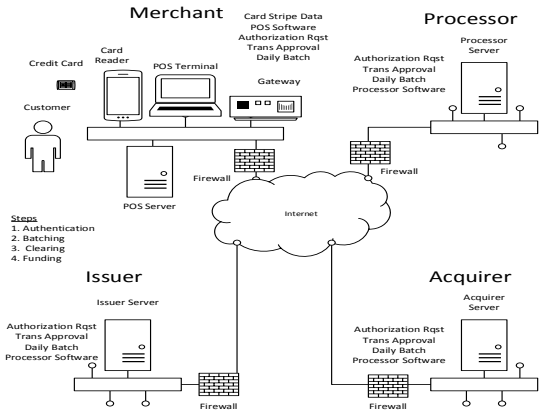


To play this game you need:

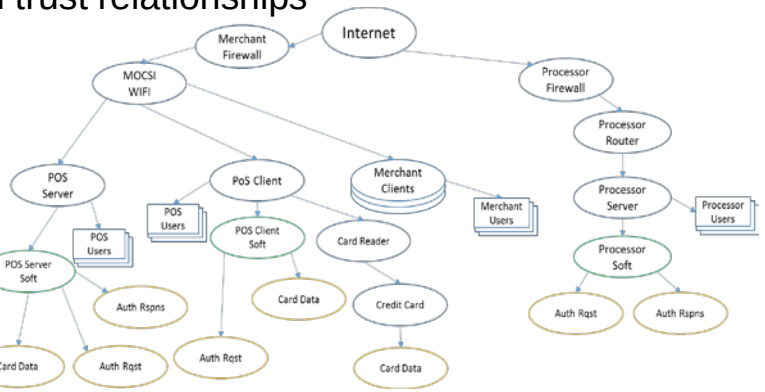
- A way to compute impacts
- A way to compute attacker paths
- A way to represent defense methods

Representing a System in the Cyber Security Game

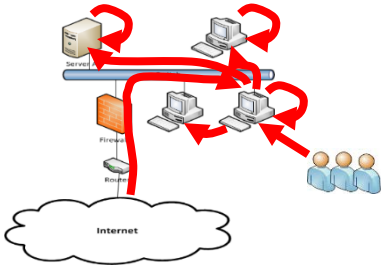
System



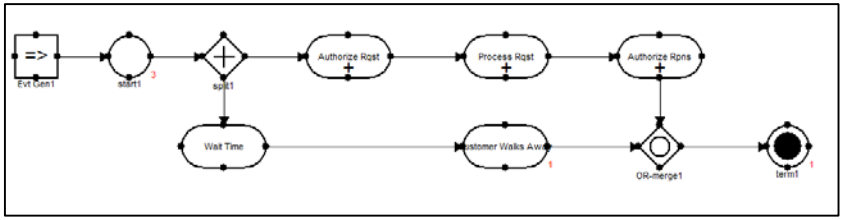
System Topology Model: Describes how cyber components are interconnected, their type, access and trust relationships



Attacker Move Model: Describes how the attacker moves across the topology



CMIA Process Model: Describes what you do with the system, and computes incident impacts



Defender Move Model: Describes the defense methods the defender can deploy

Category	Method	Applies-to Tool	Purpose	Install Cost	Maintenan	Operationa	Total Cost	Interruptio	Modificati	Fabricatior	Unauthoris	Interceptio
Terminal Access Control	Passwords/Token	POS Server	Access Cor	To Limit ur	10000	500	2000	12500	0	40	40	50	50
Terminal Access Control	Passwords/Autolock/Logout	POS Server	Built-in + n	To Limit ur	750	50	3000	3800	0	20	20	40	40
Terminal Access Control	Passwords/Token/Autolock/Logout	POS Server	Access Cor	To Limit ur	10500	550	5000	16050	0	40	40	60	60
Encryption	Disk & transport Encryption	Cust Accnt	LUKS & TL	Protect da	1000	0	50	1050	0	40	40	40	60
Server Configuration Management	Harden Server	POS Server	Puppet	to harden	2000	2000	100	4100	20	20	20	20	20
POS terminal Configuration Management	Harden POS Term	Laptop PO	MaaS360	to harden	55000	5000	1000	61000	20	60	20	40	20
Network Access Control	NAC	MOCSI Wif	Cisco ISE	Stop unaut	30000	3000	1000	34000	0	20	20	60	20
Network Access Control	NAC + VPN	MOCSI Wif	Cisco ISE +	Stop unaut	35000	3000	-5000	33000	0	20	20	60	20
Network Intrusion Detection	NIDS	POS Server	Security O	reduce the	5000	500	0	5500	20	20	20	20	20
Network Intrusion Detection	NIDS + Applications Monitoring	POS Server	ModSecuri	reduce the	10000	0	0	10000	20	20	20	20	40
Server Intrusion Detection	File Integrity	POS Server	Tripwire	reduce the	15000	1500	1000	17500	0	40	20	20	20
Tokenize	Tokenize Transactions	Cust Accnt	First Data	Ensures th	30000	1000	0	31000	0	0	0	90	90
Host Intrusion Detection	Virus detection/HIPS	Laptop PO	Semantec	Detect and	5000	500	1000	6500	20	20	20	20	20
EMV	CHIP n Sig	Card Data;	PCI	Authentica	20000	1000	500	21500	0	0	60	0	0
EMV	CHIP n PIN	Card Data;	PCI	Authentica	20000	1000	10000	31000	0	0	85	60	0
Reimage POS Systems	periodic POS terminal re-image	Laptop POS Software;		Laptop Ha	25000	1000	5000	31000	20	60	20	50	20
Whitelist processes	White Listing	POS Server	Bit9 Parity	run only al	5000	0	500	5500	40	60	20	60	25

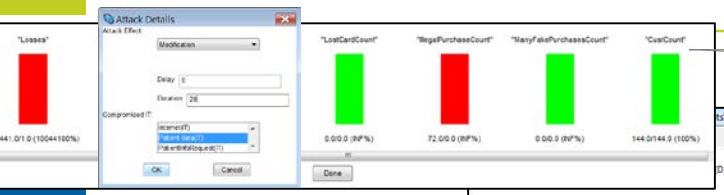
Cyber Mission Impact Assessment (CMIA)

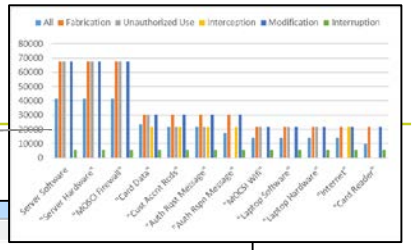
- **It is fundamentally necessary to understand the value proposition of one's cyber infrastructure, and how incidents affect that value**
- **Business Process Modeling (BPM) has been used successfully by many organizations to describe mission processes and relate the capability of mission resources to performance outcomes**
- **Our contribution to BPM is to include cyber resource and cyber activities in the process model so we can map the impacts of what happens when a cyber incident occurs**

Cyber Mission Impact Assessment (CMIA) Tool

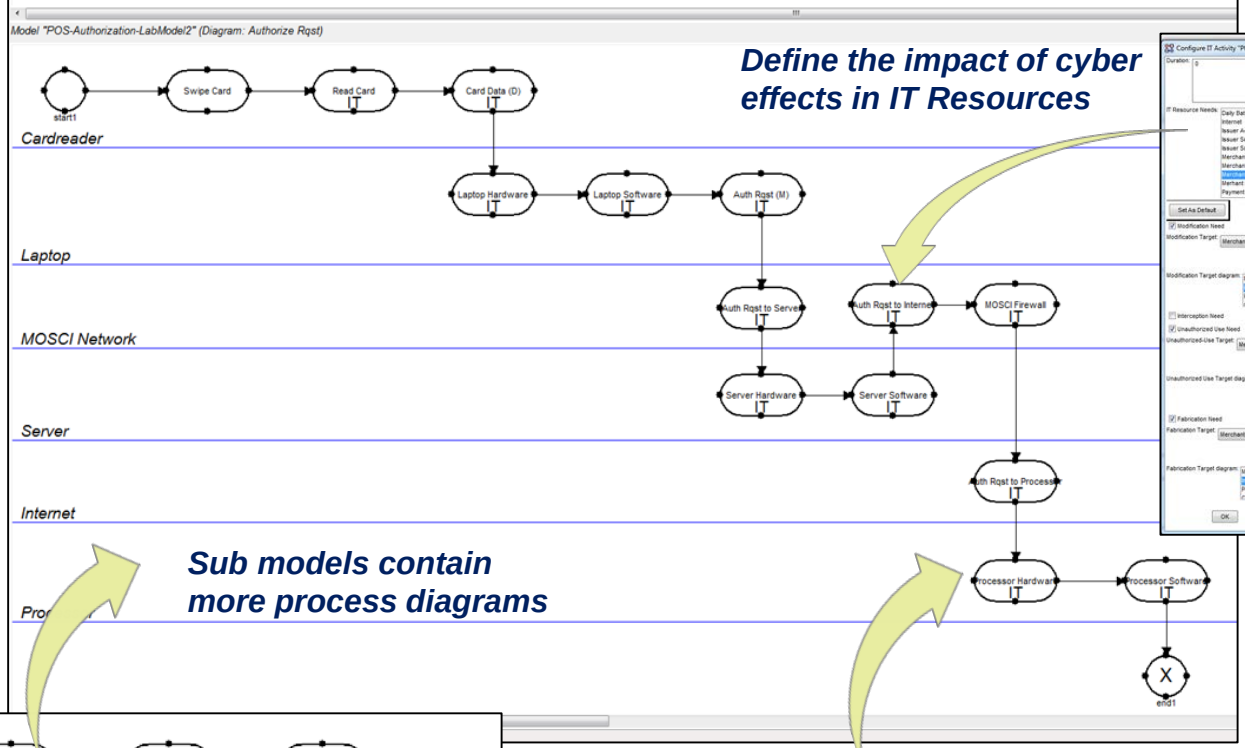
Computes the impact of a cyber incident (can be called by CSG)

Compute cyber impacts from all cyber effects against all IT resources for CJA and model validation

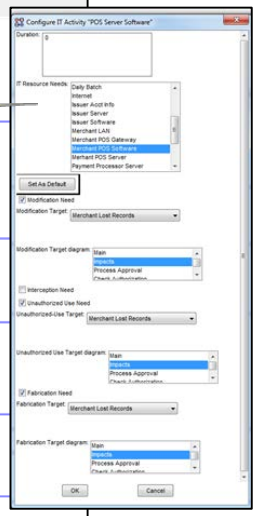




The process model is linked to a discrete event simulation engine that simulates the mission thread

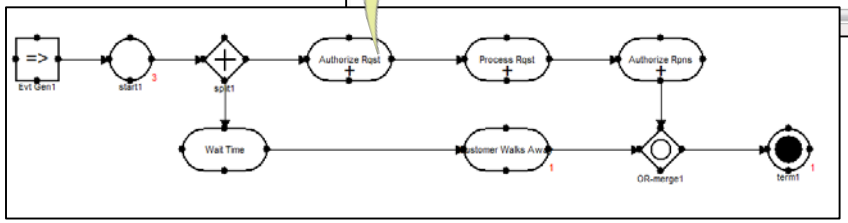


Define the impact of cyber effects in IT Resources



Swim lanes help identify the systems and actors

Sub models contain more process diagrams

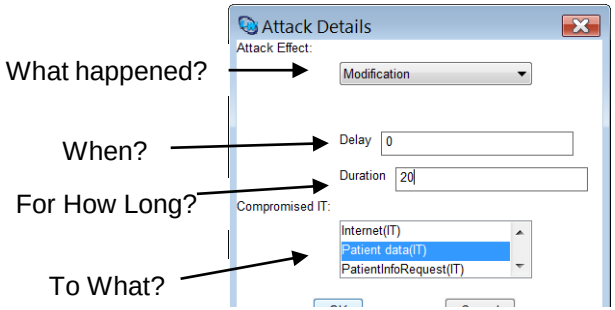


During simulation activities can execute code to set simulation variables or alter process flow

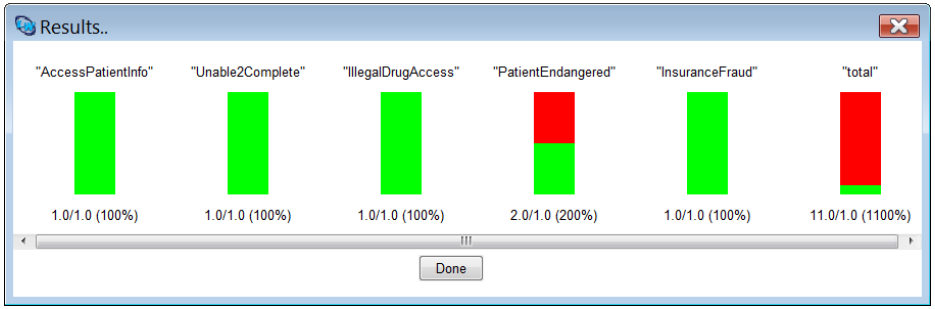
See: "A Cyber Mission Impact Assessment Tool", IEEE Homeland Security Technologies Conference, 2015

MITRE

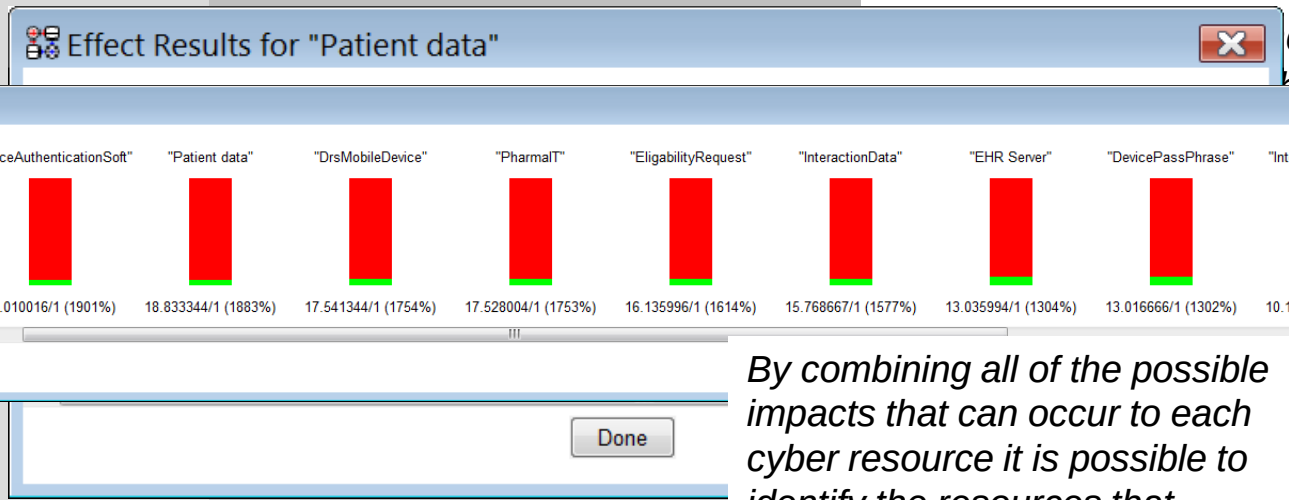
How the Estimation of Cyber Mission Impact Allows us to Identify the Cyber Crown Jewels



Modification of Patient Data



EFFECT	COMPONENT	DURATION	DELAY	AccessPatientInfo	Unable2Complete	IllegalDrugAccess	PatientEndangered	InsuranceFraud	total
Interception	Patient Data	280	0	2	2	2	2	2	32.1
Interception	Patient Data								
Interruption	Patient Data								
Interruption	Patient Data								
Interruption	Patient Data	60	10	1	1	1	1		
Interruption	Patient Data	80	0	1	2	1	1		



The impact depends on the resource(s) cident

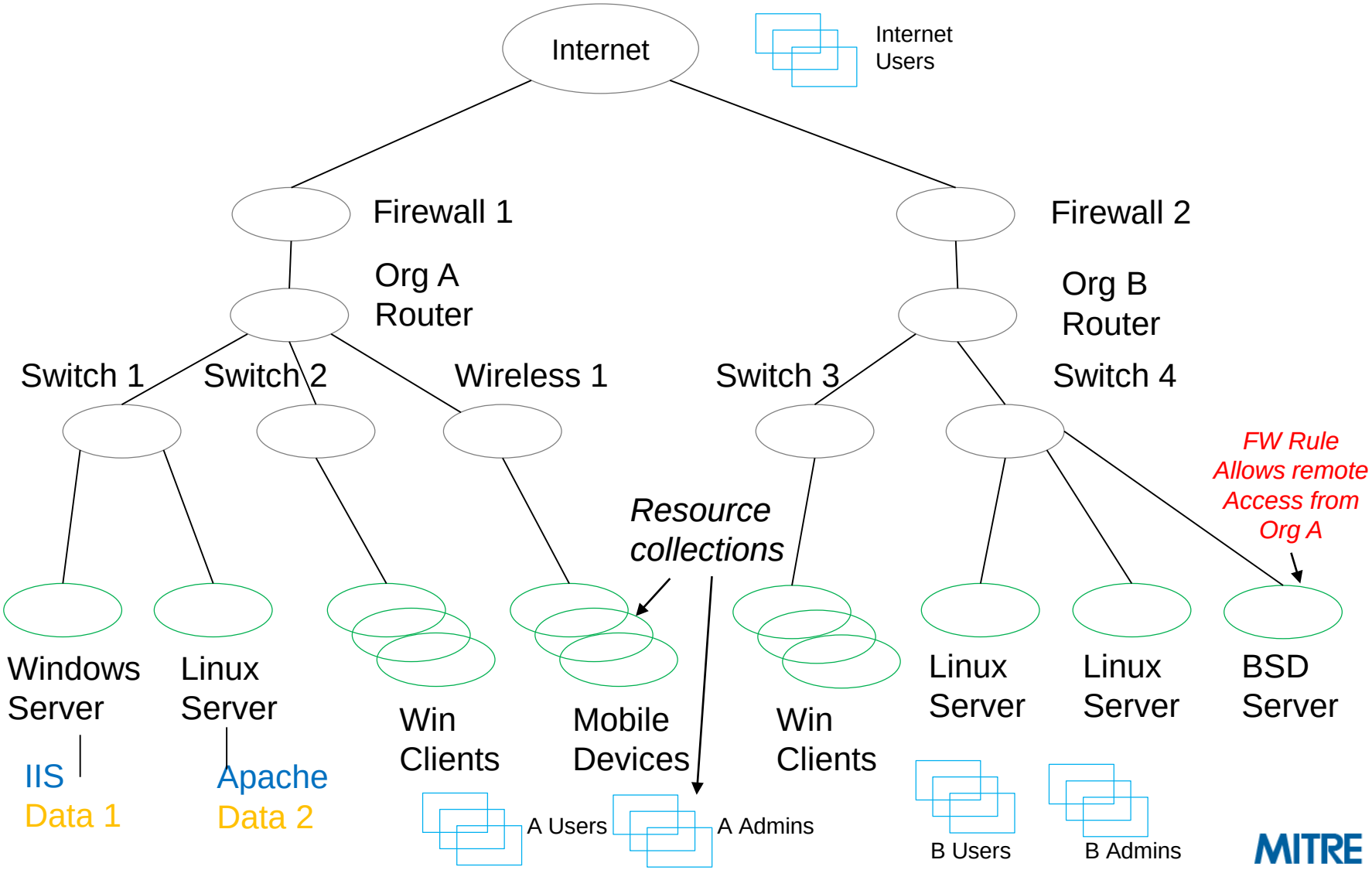
By combining all of the possible impacts that can occur to each cyber resource it is possible to identify the resources that create the largest impacts, and hence are most critical

MITRE

Overview of The Cyber Security Game (CSG)

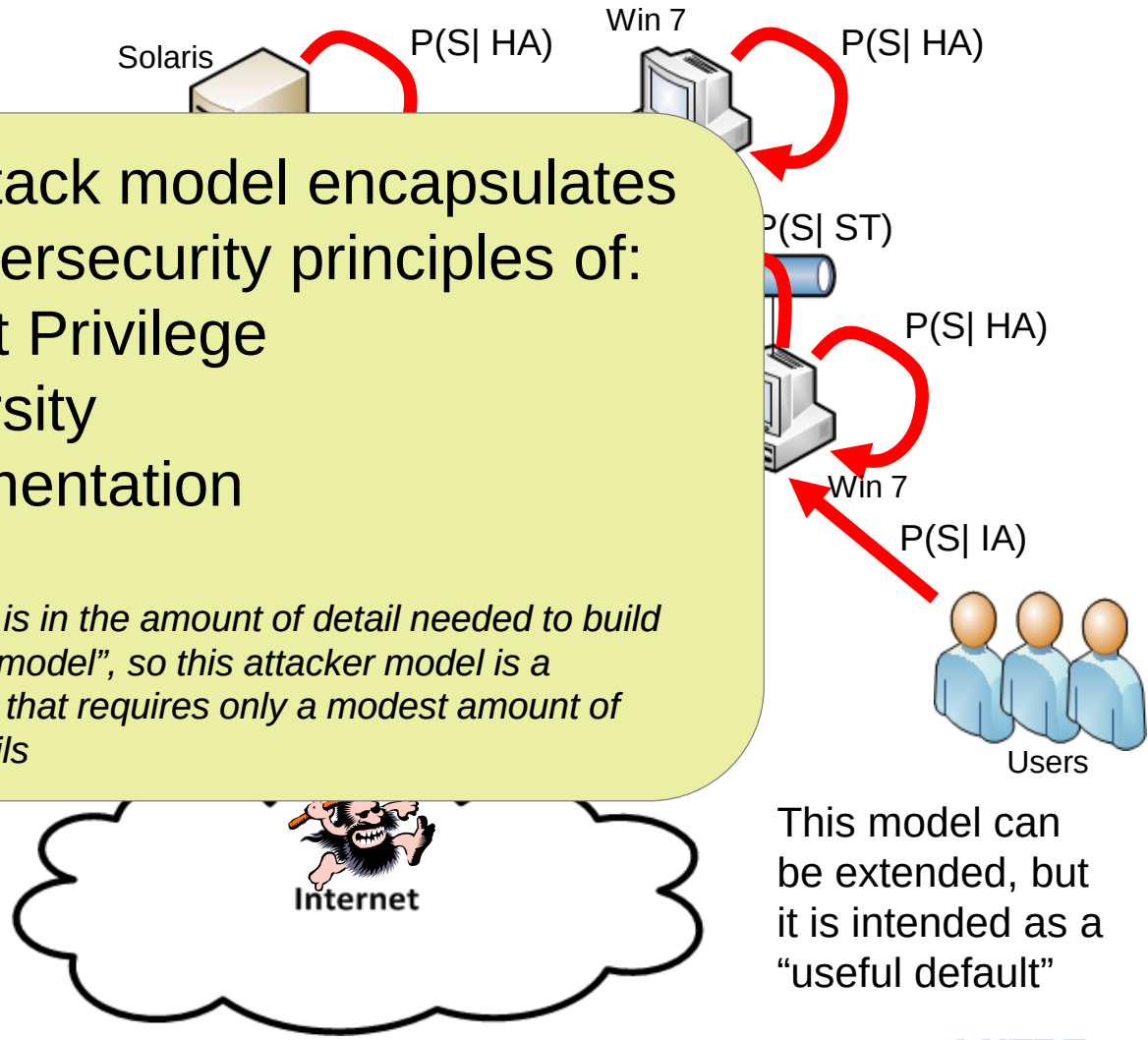
- **To go beyond impact and criticality it is necessary to be able to predict how likely the incidents are to occur**
- **Your network architecture will constrain how an attacker can access the cyber resources to compromise them**
- **The employment of cyber security and resilience mechanisms can either reduce the chance that incidents occur, or reduce the impacts that they cause when they do occur**
  - Hardening can reduce the number of attack instances that succeed
  - Redundancy can reduce impact if a component fails
- **Cost/benefit tradeoffs are required to determine how best to invest in cyber security and resilience**

A "Computable" System Topology Model Captures the Connectivity and Trust Relationships Between Mission Cyber Resources



Attacker Model Can be Used to Estimate how the Architecture Affects the Likelihood that Attacker Incidents Succeed

- **P(S| IA)**
  - Malicious Insider
- **P(S | OI, Srvr)**
  - Outsider tryin
- **P(S | HA)**
  - Compromisin components
- **P(S | ST, Srvr)**
  - Compromisin the same type
- **P(S | DT, Srvr)**
  - Compromisin host/compone different type
- **Magnitude of thr**
  - P(S| IA) < P(S|OI) < P(S| DT, F) < P(S | DT, T) < P(S| ST, F) < P(S | ST, T) < P(S| HA)
- **This model is composable over multiple networks**



This attack model encapsulates the cybersecurity principles of:

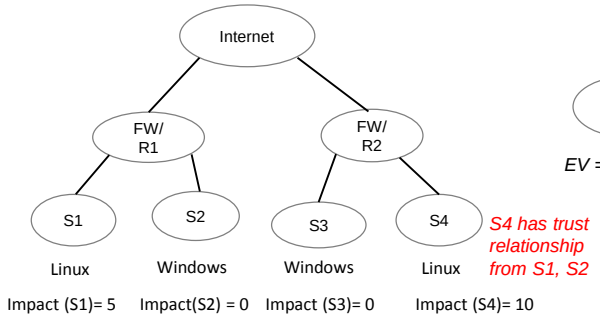
- Least Privilege
- Diversity
- Segmentation

The tradeoff is in the amount of detail needed to build the "system model", so this attacker model is a compromise that requires only a modest amount of system details

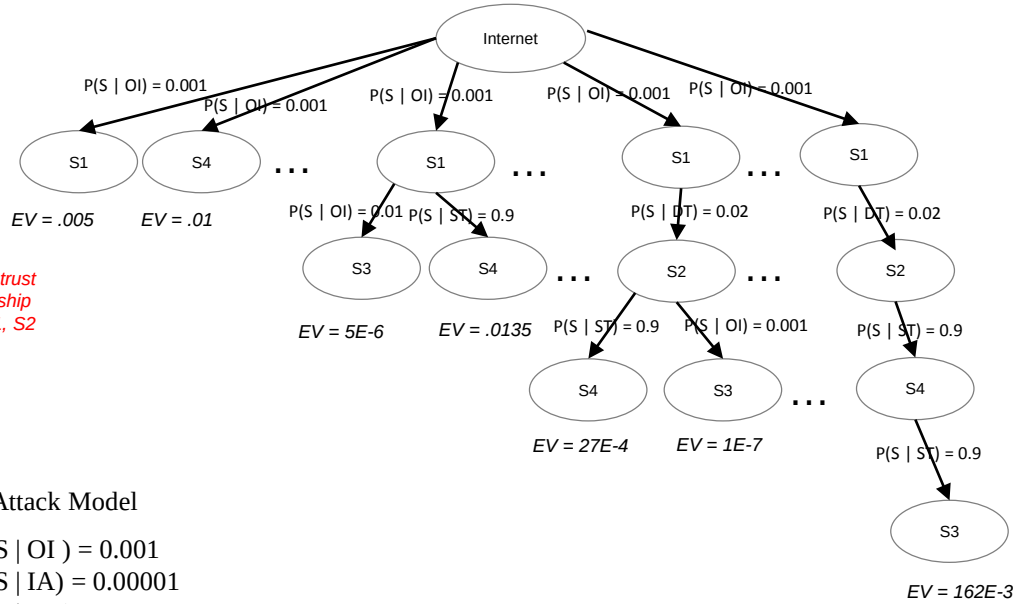
This model can be extended, but it is intended as a "useful default"

Computing Mission Risk

System Topology



Attack Tree



Mission Impacts (from CMIA)

Impact(S1,S2) = 5
Impact(S1,S3) = 5
Impact(S1,S4) = 15
Impact(S2,S3) = 0
Impact(S2, S4) = 10

Independent additive impacts

.....

Impact(S3,S4) = 50
Impact(S1,S2,S3,S4) = 1000

Dependent impacts

Attack Model

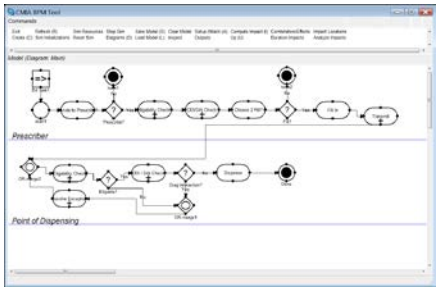
$P(S \mid OI) = 0.001$
$P(S \mid IA) = 0.00001$
$P(S \mid ST) = 0.9$
$P(S \mid DT) = 0.02$

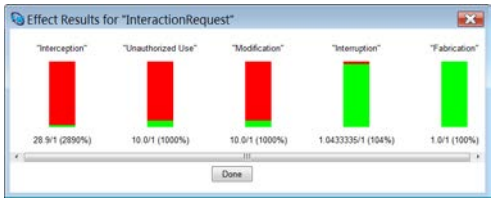
CSG looks multiple attack steps ahead to identify attacker pathways that can cause impacts AND to identify impacts that stem from compromising multiple components

MITRE

Evaluating The Cyber Security Game State

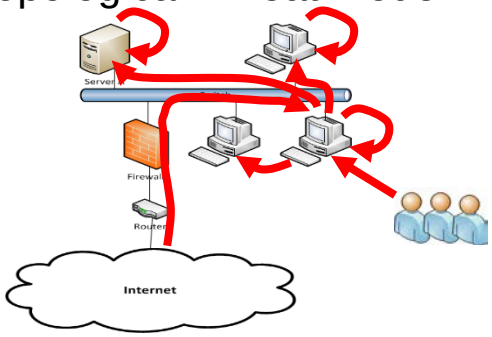
CMIA Process Model





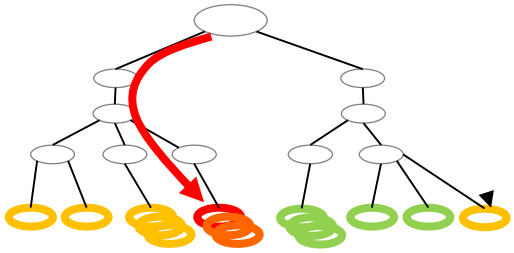
CMIA can Estimate the Impact of Attacks

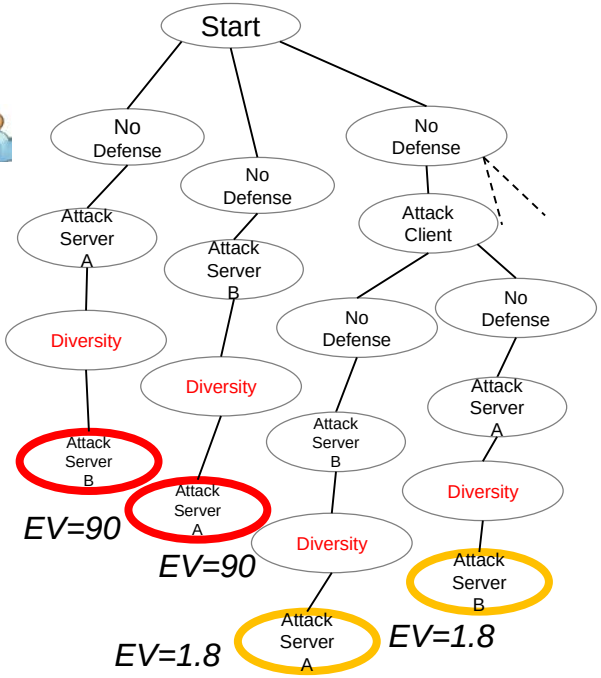
Topological Threat Model



X

=





Combining the Topology and Attack Model can Estimate how Likely Attacks are to succeed

Mission Risk =

Expected Value lost to Attacker

MITRE

Running CSG Requires the Defender to Describe the Set of Defensive Actions they can Perform

Methods that Reduce the Chance of Attack Success

Category	Method	Applies-to	Tool Name	Install Cost	Maintenance Cost	Operational Cost	Total Cost	Interruption	Modification	Fabrication	Unauthorized-Use	Interception
Encryption	Encrypt Disk & transport Layer	Mobile Dvc	LUKS & TLS	$1000	$0	$50	$1050	0	40	40	40	60
Server Configuration Management	Harden	EHR Server	Puppet	$2000	$2000	$100	$4100	20	20	20	20	20

Tool category

Method it employs

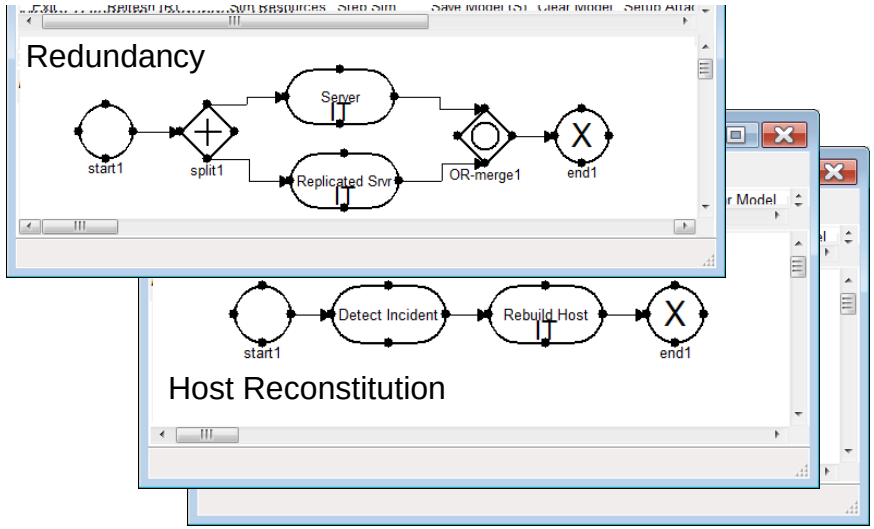
What system resources it applies too

Cost to employ and operate tool

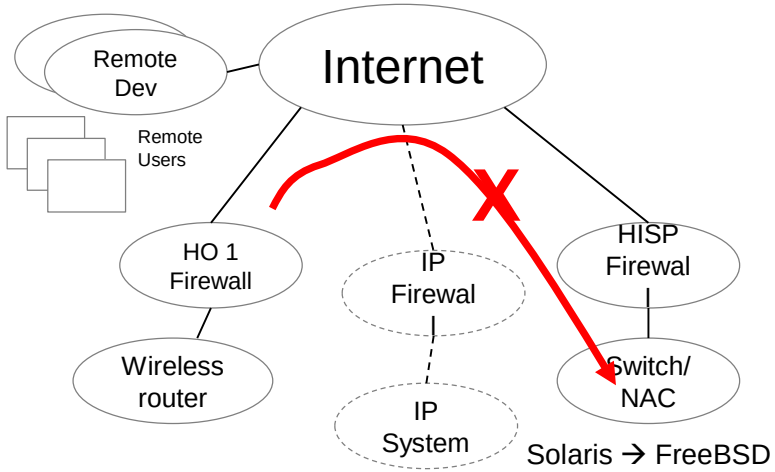
40 implies it will stop 40% of the attacks

How effective is it at stopping attack effects

Methods that Change Process



Methods that Change Access



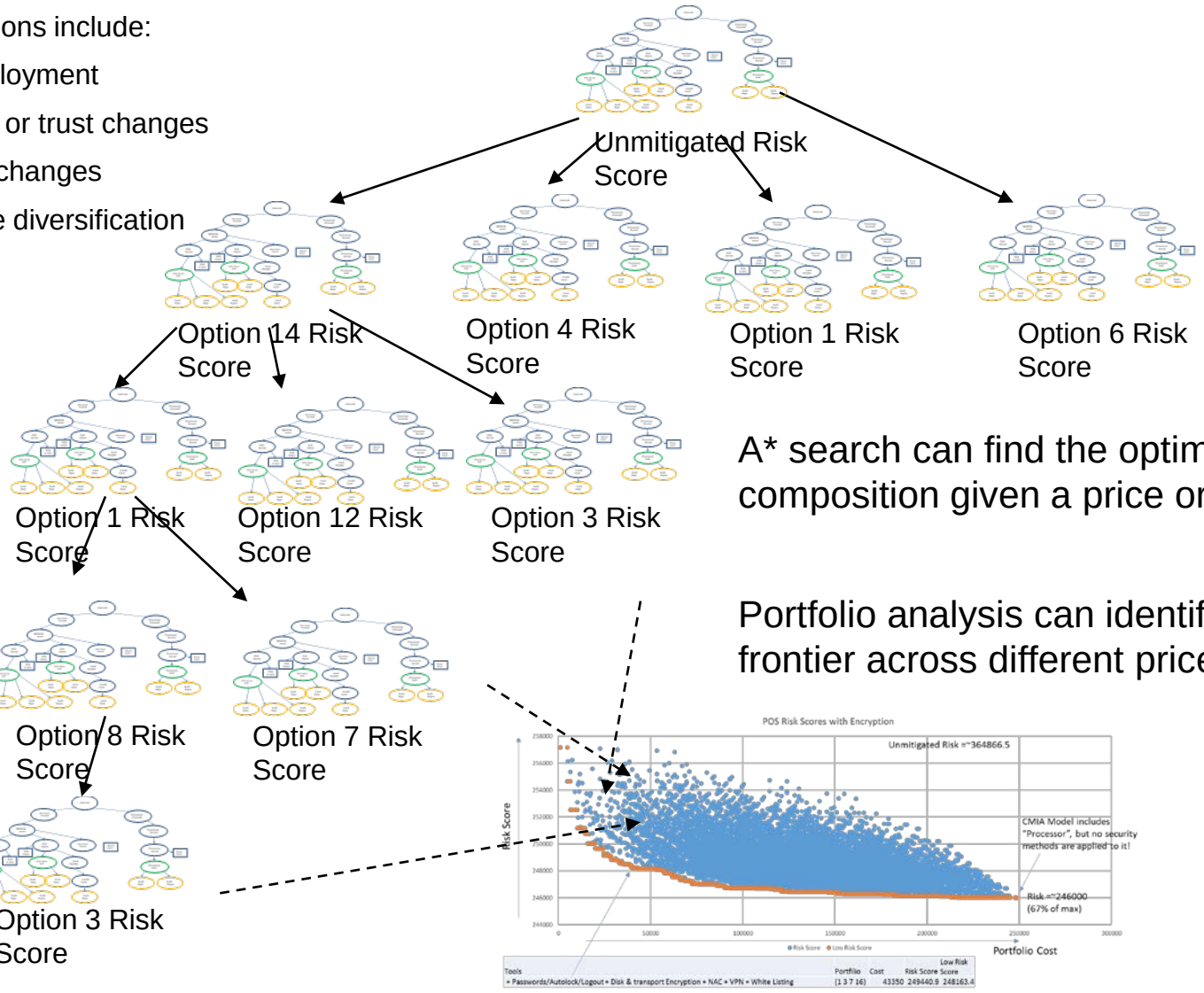
Methods that Change Type

MITRE

CSG Provides the Ability to Compose Defenses and Assess Defender Choices

Defender options include:

- Tool employment
- Topology or trust changes
- Process changes
- Resource diversification



A* search can find the optimum composition given a price or risk target

Portfolio analysis can identify the Pareto frontier across different price points

MITRE

Example of Defensive Methods (for a Point of Sale System)

Category	Method	Applies-to	Tool	Purpose	Install Cost	Maintenan	Operationa	Total Cost	Interruptic	Modificati	Fabricatior	Unauthori:	Interceptic
Terminal Access Control	Passwords/Token	POS Server	Access Car	To Limit ur	10000	500	2000	12500	0	40	40	50	50
Terminal Access Control	Passwords/Autolock/Logout	POS Server	Built-in + n	To Limit ur	750	50	3000	3800	0	20	20	40	40
Terminal Access Control	Passwords/Token/Autolock/Logout	POS Server	Access Car	To Limit ur	10500	550	5000	16050	0	40	40	60	60
Encryption	Disk & transport Encryption	Cust Accnt	LUKS & TL	Protect da	1000	0	50	1050	0	40	40	40	60
Server Configuration Management	Harden Server	POS Server	Puppet	to harden	2000	2000	100	4100	20	20	20	20	20
POS terminal Configuration Management	Harden POS Term	Laptop PO	MaaS360	to harden	55000	5000	1000	61000	20	60	20	40	20
Network Access Control	NAC	MOCSI Wil	Cisco ISE	Stop unaut	30000	3000	1000	34000	0	20	20	60	20
Network Access Control	NAC + VPN	MOCSI Wil	Cisco ISE +	Stop unaut	35000	3000	-5000	33000	0	20	20	60	20
Network Intrusion Detection	NIDS	POS Server	Security O	reduce the	5000	500	0	5500	20	20	20	20	20
Network Intrusion Detection	NIDS + Applications Monitoring	POS Server	ModSecuri	reduce the	10000	0	0	10000	20	20	20	20	40
Server Intrusion Detection	File Integrity	POS Server	Tripwire	reduce the	15000	1500	1000	17500	0	40	20	20	20
Tokenize	Tokenize Transactions	Cust Accnt	First Data	Ensures th	30000	1000	0	31000	0	0	0	90	90
Host Intrusion Detection	Virus detection/HIPS	Laptop PO	Semantec	Detect anc	5000	500	1000	6500	20	20	20	20	20
EMV	CHIP n Sig	Card Data;	PCI	Authentica	20000	1000	500	21500	0	0	60	0	0
EMV	CHIP n PIN	Card Data;	PCI	Authentica	20000	1000	10000	31000	0	0	85	60	0
Reimage POS Systems	periodic POS terminal re-image	Laptop POS	Software;	Laptop Ha	25000	1000	5000	31000	20	60	20	50	20
Whitelist processes	White Listing	POS Server	Bit9 Parity	run only al	5000	0	500	5500	40	60	20	60	25

Host Intrusion Detection/Prevention on POS Terminals

Disk and Transport Layer Encryption

Network Intrusion Detection

Access Controls

Process Whitelisting

Network Access Controls

POS Terminal Hardening

POS Server Hardening & Configuration Management

File Integrity Checking

Periodic Reimaging of POS Terminals

Tokenization

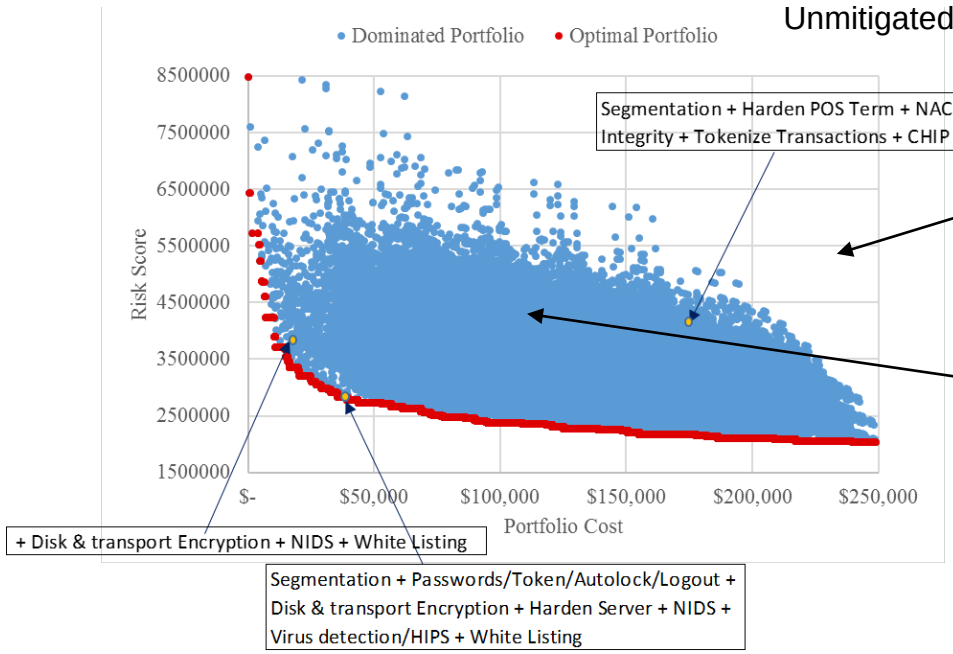
EMV Chip n Signature

Merchant Network Segmentation (Topology Model Option)

EMV Chip n Pin

MITRE

CSG Point Of Sale Portfolio Analysis



The best POS risk reduction can be achieved used all of the tools, at a cost of ~$250,000, but 89% of the best risk reduction is achieved spending only 16% of the max cost

Cost Rank	Portfolio Defenses	Cost	Risk
1[P]	Segment	500	6,441,843
3[P]	Disk & transport Encryption + Segment	1,050	7,613,147
10[P]	Passwords/Autolock/Logout + Disk & transport Encryption	4,850	5,238,869
38[P]	Passwords/Autolock/Logout + Disk & transport Encryption + White Listing	10,350	3,892,103
570	Segmentation + Passwords/Token + NIDS + Applications Monitoring + Virus detection/HIPS + White Listing	35,000	3,418,609
581	Harden Server + CHIP n PIN	35,100	7,114,348
55295[P]	Segmentation + Passwords/Token/Autolock/Logout + Disk & transport Encryption + Harden Server + Harden POS Term + NAC + NIDS + Applications Monitoring + File Integrity + Tokenize Transactions + Virus detection/HIPS + CHIP n PIN + periodic POS terminal re-image + White Listing	249,200	2,038,408

Summary

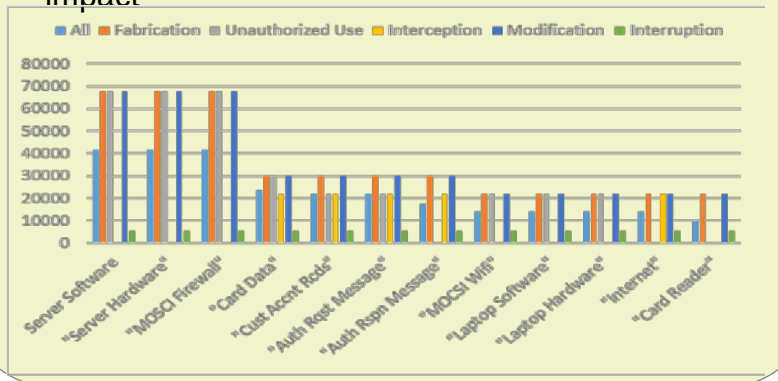
- **Our game theoretic approach codifies several expert level capabilities into a tool that avoids "users" from having to perform them manually**
- **Our method forces "users" to focus is on describing their mission system and how it fulfills operational functionality in the face of cyber incidents**
  - CSG requires a CMIA model, a Topology and a Defender model
  - Useful defaults for a threat model are provided, but it can be extended if you are willing to provide additional system details
- **Can be applied to "As is", or "As might be" versions of a system**
- **Performs an analysis that is much more comprehensive than can be achieved manually**
- **Makes it possible to quantitatively assess cybersecurity risk and a return on investment assessment of mitigations to that risk**

Summary: Cyber Mission Impact Assessment (CMIA) and Cyber Security Game (CSG)

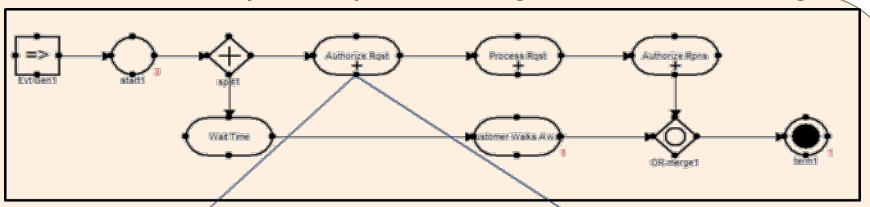
- **Cyber Mission Impact Assessment (CMIA) and Cyber Security Game (CSG) makes it possible to:**
  - Represent a System and its cyber dependencies
  - Assess the operational impact of cyber incidents
  - Produce a quantitative Cyber Crown Jewels analysis
  - Assess Cyber Risk
  - Guide mitigation engineering by identifying which incident types must be prevented, and where they should be prevented
  - Use a game formulation for course of action (CoA) decision making, targeted improvements and to optimize cyber security investment decisions

CMIA Analysis Enables:

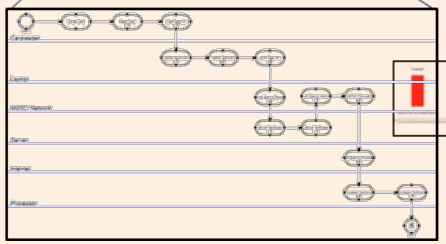
- An estimate of Cyber Incident Impacts
- Quantitative identification of Cyber Crown Jewels
- Identification of which incidents, when, where, cause impact



CMIA Models Cyber Impacts through Process Modeling



Incident Details



Incident Impacts

CSG Analysis Enables:

- An estimate of the systems cyber risk
- An assessment of how security tools reduce risk
- Optimization of security portfolio investments

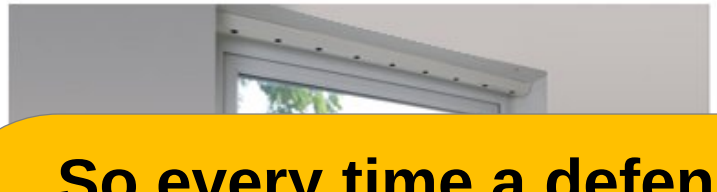
MITRE

Backup

Some Core Terms

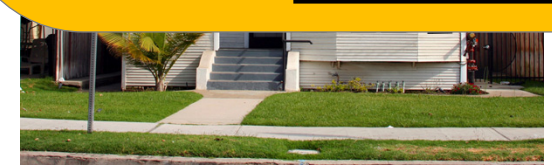
- **Mission Impact**
  - A change in one or more performance outcomes as a result of an incident occurring
- **Criticality**
  - Resources and incidents that cause the greatest impacts
- **Risk**
  - The impacts conditioned on how likely the incidents that cause them are to occur

Defending Against a Determined Attacker is not like Defending Against Natural Hazards



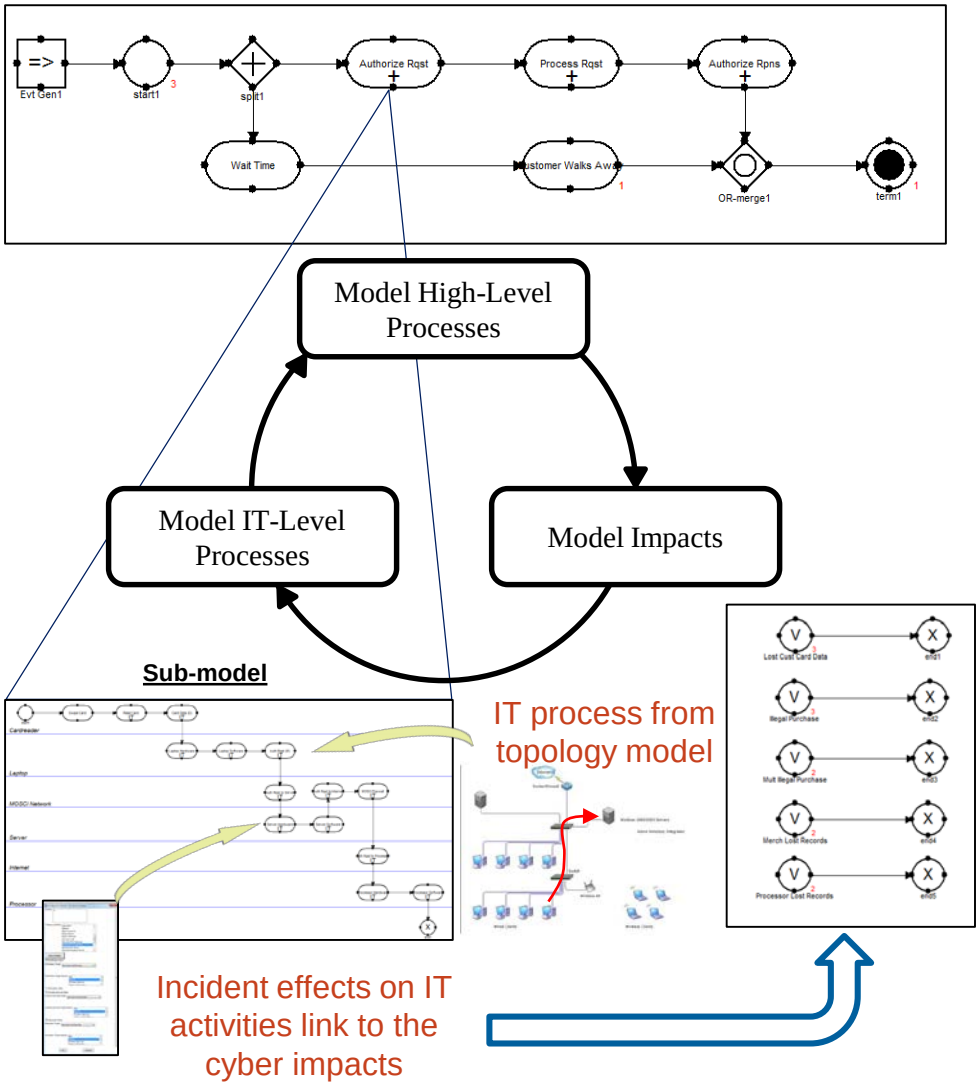
So every time a defender makes an attempt to protect a portion of the system, the attacker will consider their other options to circumvent the defenses, or to choose another "next best" option.

<u>Defender strategies that fail to consider the adversary are doomed to failure</u>



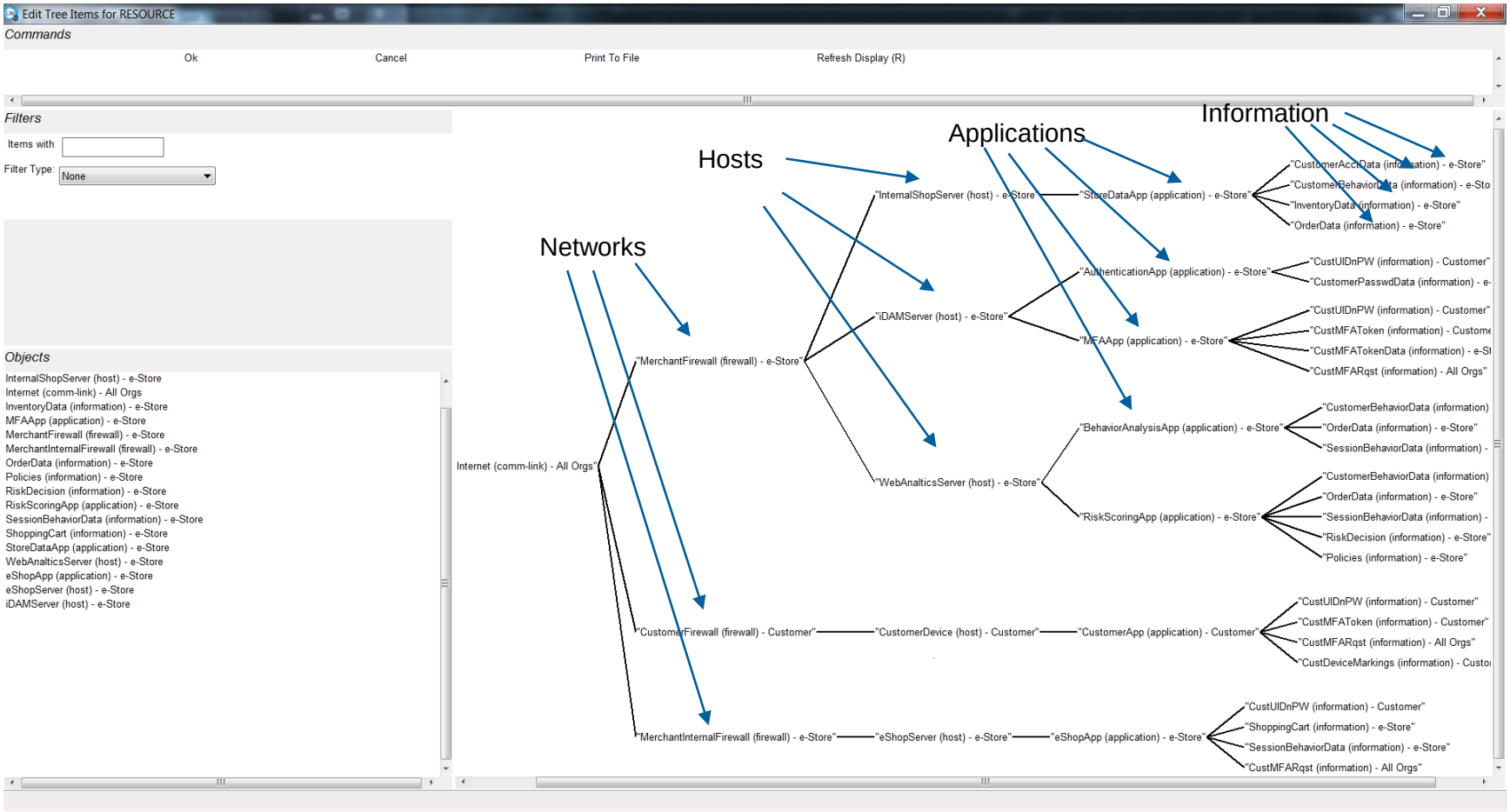
But if you only put bars on windows in the front of the house, then a determined burglar will check the back, and break in there..

The CMIA Methodology



1. Model High-Level Processes
   a. Build process flow of High-Level activities
   b. Create and link required sub-models
   c. Create required simulation variables and write supporting code
2. Model Impact Diagram
   a. Define the set of impact events and consider temporal impacts
   b. Build process flow of impacts with catches
   c. Create required simulation variables with supporting code to calculate impact
3. Model IT-Level Processes
   a. Build process flow of IT-Level activities
   b. Create and link required sub-models
   c. Create required simulation variables and write supporting code
   d. Create required IT resources
   e. Assign resources to IT activities
   f. Assign cyber effects and link them to Impacts

A "Computable" System Topology Model Captures the Connectivity, Access and Trust Relationships between Mission Cyber Resources



Not shown, but included in the topology model are user access and component trust relationships (i.e. firewall rules)

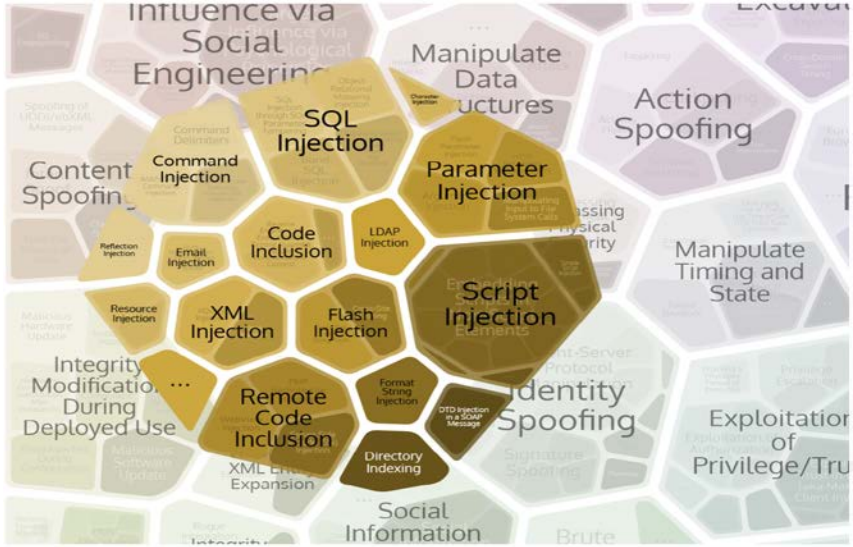
MITRE

To Avoid Having to Think About Every Attack Instance we Consider the Attack Effects

- **Most people consider Confidentiality, Integrity and Availability**
- **We found that this was insufficient, and instead we chose DIMFUI:**
  - **Degradation**
    - An attacker causes a degradation in the performance of an information asset
  - **Interruption**
    - An attacker causes an information asset of the system to become unusable, unavailable, lost for some period of time
  - **Modification**
    - An attacker causes a modification of information, data, protocol , or software
  - **Fabrication**
    - An attacker causes information or components to be inserted into the system.
  - **Unauthorized Use**
    - An attacker uses the system resources for their own purposes.
  - **Interception**
    - An attacker causes or takes advantage of information leaked from the system
- **All cyber attacks will manifest themselves as one or more of the above effects applied to one or more IT assets**

Full CAPEC

2nd-Level Zoom

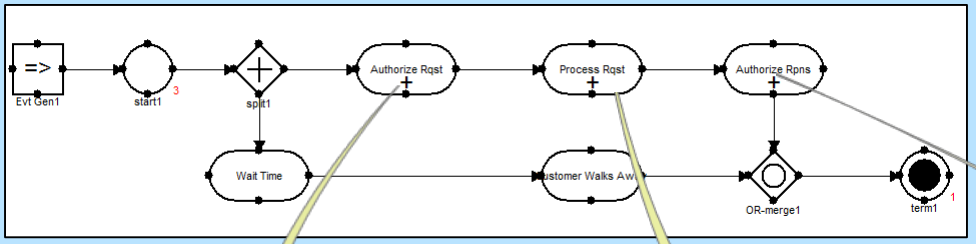


See "*A Language for Capturing Cyber Impact Effects*", MITRE Technical Report #100344, Sept 2010

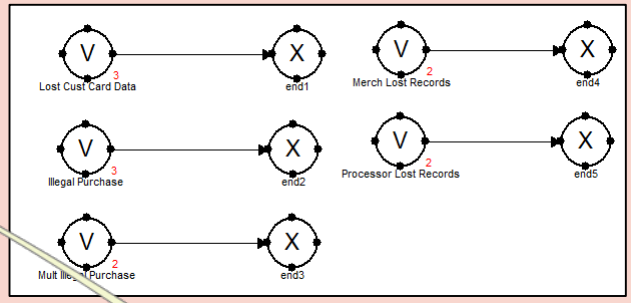
MITRE

The CMIA Model of PoS Authorization

Top Level Authorization Process



Cyber Impacts



Impacts:

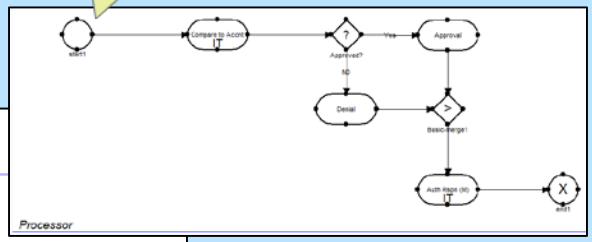
Lost Purchases

Lost Card Data

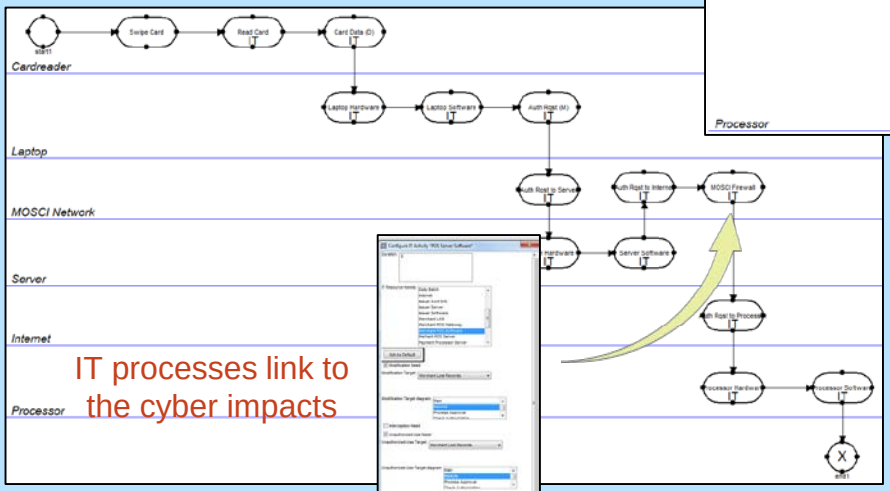
Illegal Purchases

Multiple Cards lost

Process Request

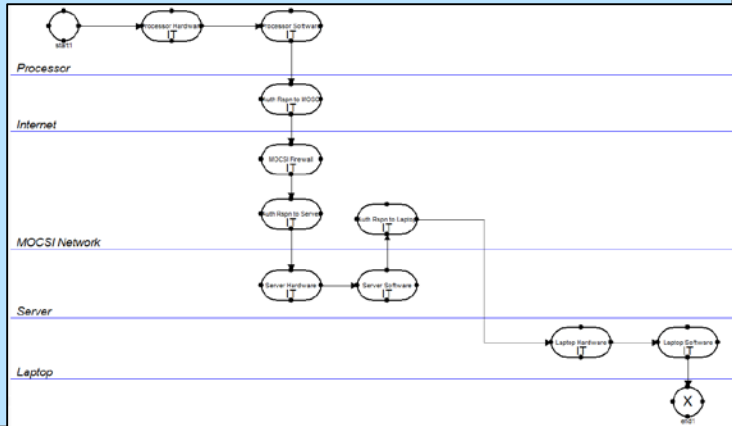


Authorization Request

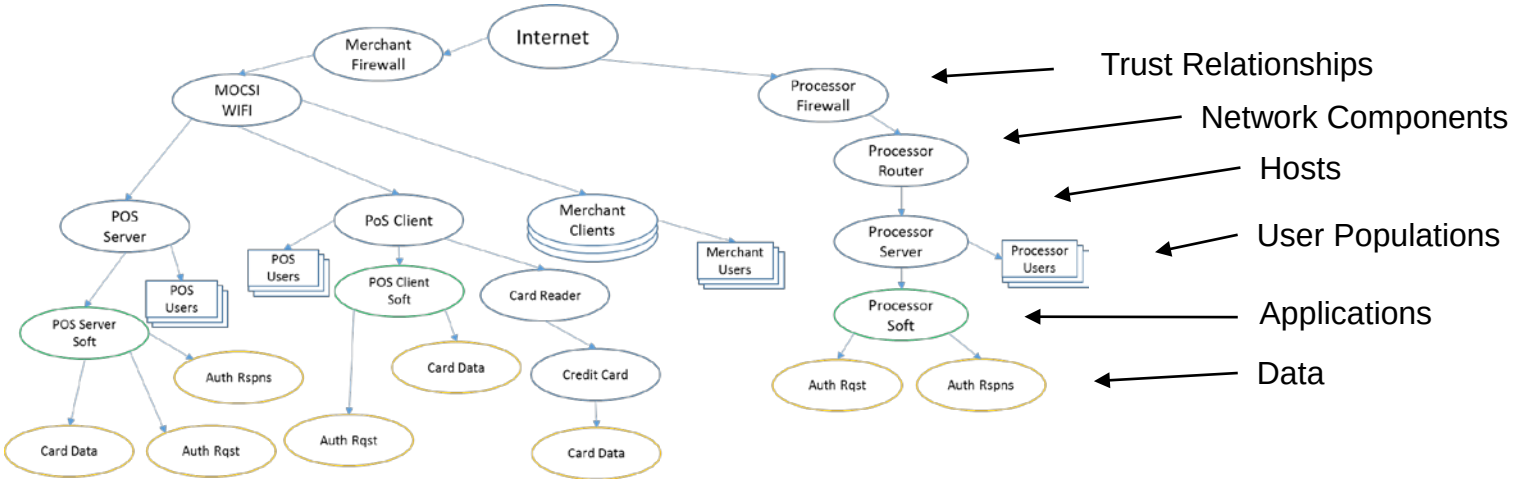


IT processes link to the cyber impacts

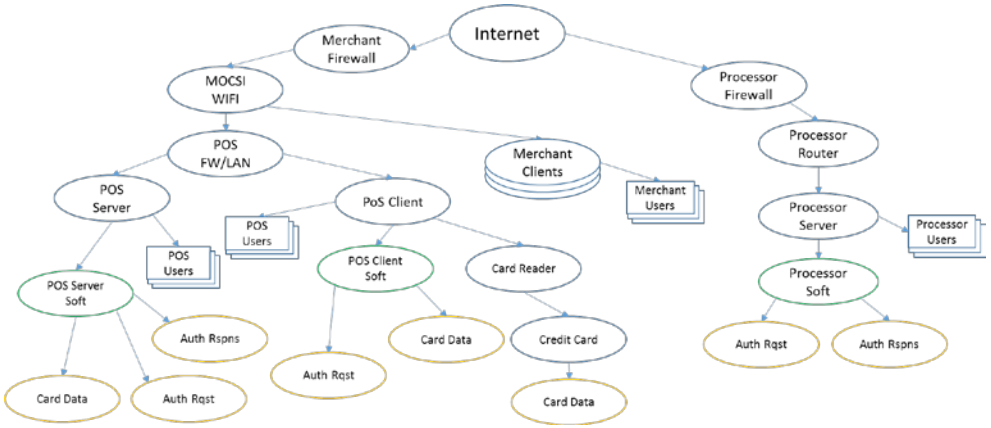
Authorization Response



CSG Models of POS Topology



Topology of Merchant and Processor



Topology Option Segmenting POS at Merchant

MITRE

Characteristics of CSG's Analysis

- **CSG analysis is quantitative**
  - Based on quantitative assessments of mission impact and attack paths
  - Based on an assessment of how defender methods mitigate cyber incidents
- **The analysis is holistic**
  - The generated attack trees explore the set of possible attacker/defender effects (based on the models)
  - Able to look multiple attacker steps ahead to identify compound impacts
- **The analysis is prescriptive**
  - Credits defenses that make it harder for the attacker to create the incident effects that cause impacts
- **Supports cybersecurity/resilience investment decision making**
  - Helps to avoid over investing in portions of the system at the expense of underinvesting in others
    - A resource is defended enough, when there are other resources that provide a better "payoff" for the attacker
  - Can answer questions like "how much diversity is enough"
- **Ensures a balanced defensive portfolio across the entire range of threats against the cyber assets**