Risk and Risk Analysis

the foundation of IS governance

Dr. Hale
University of Nebraska at Omaha
Information Security and Policy– Lecture 2

“Know your enemy and know yourself, find naught in fear for 100 battles. Know yourself but not your enemy, find level of loss and victory. Know thy enemy but not yourself, wallow in defeat every time.”

– Sun Tzu, The Art of War

Today's topics:

What is risk?

- Definition
- Examples

Risk analysis

- Assets and Loss
- Threats and scopes
- Definitions
- Risk Management Lifecycle

Risk prioritization and strategic spending (or lack thereof)

- Annualized threat loss expectancy
- Examples

At its core:
Risk is the potential for loss

Ex. Financial Risk

Invest $100

Option 1: make Guaranteed 3% - leave with $103

Option 2: Flip a coin. Heads $200, tails $0

Option 3: Flip a coin. Heads $150, tails $60

Minimize risk? Or Maximize Profit potential?

What is Risk

Ex. Financial Risk

Invest $100

Option 1: make Guaranteed 3% - leave with $103

Option 2: Flip a coin. Heads $200, tails $0 => EV = 100

Option 3: Flip a coin. Heads $150, tails $60 => EV =105

Expected values

Ex. Financial Risk

Invest $100

Option 1: make Guaranteed 3% - leave with $103

Option 2: Flip a coin. Heads $200, tails $0 => EV = 100

Option 3: Flip a coin. Heads $150, tails $60 => EV =105

Will talk more about this next time

Ex. Software Development Risk

Pick a framework

Option 1: PHP (team knows languages)

Option 2: Node/Express.js + Angular/Ember.js (team doesn't know javascript)

Risks related to language power, amount of work, and getting team up to speed

Better to choose more powerful or more familiar languages?

Definition

Security Risk is the potential that an asset will be compromised and thereby cause harm to an organization.

Ex. Security Risks

Laptops can be stolen

Systems can be hacked

Staff can be socially engineered

Ex. Security Risks

Laptops can be stolen

Systems can be hacked

Staff can be socially engineered

Ex. Security Risk Choices

Allocate $10,000 to Info. Sec.

Option 1: Encrypt laptops

Option 2: Buy a firewall

Option 3: Train staff against phishing

What is the best choice? How do you decide?
(We'll return to this)

Quantitative Definition

Risk = Likelihood of incident occurring x *Impact of an Incident*

$$R = L \times I$$

$$EnterPrise\ Risk = \sum_{i=1}^{n} L_i \times I_i$$

What is Risk

Looking back at Sun Tzu's quote
…know thyself and thine enemy

Know thyself
= understand business assets (and vulnerabilities)

Know thine enemy
= understand threats

Definition

An *asset* is anything of value to an organization

Definition

A *threat* is an action that could harm an asset

Types of assets

- Physical entities
  - IT Hardware (Laptops, desktops, servers, networks)
  - Infrastructure (Power, water, cooling, etc)
  - Supplies (brooms, toilet paper)
- Logical entities
  - Information (SSNs, address list, product specs)
  - Systems (POS, web apps, email, ftp, VPN, phone)
  - Thoughts (intellectual property – possible overlap with info.)
- Humans (developers, IT admins, other staff, users)

Types of threats

- Physical
  - Natural Disaster (earthquake, tornado, etc)
  - Loss of Services (water, power, cooling)
  - Theft (Laptops, hard drives, papers, trash)
- Logical
  - Disclosure of sensitive info.
  - Unauthorized modification
  - Malware, Spyware, etc
  - Network exploitation (DoS, etc)
  - Many others
- Human
  - Malicious Insiders
  - Social Engineering
  - Phishing

Definition

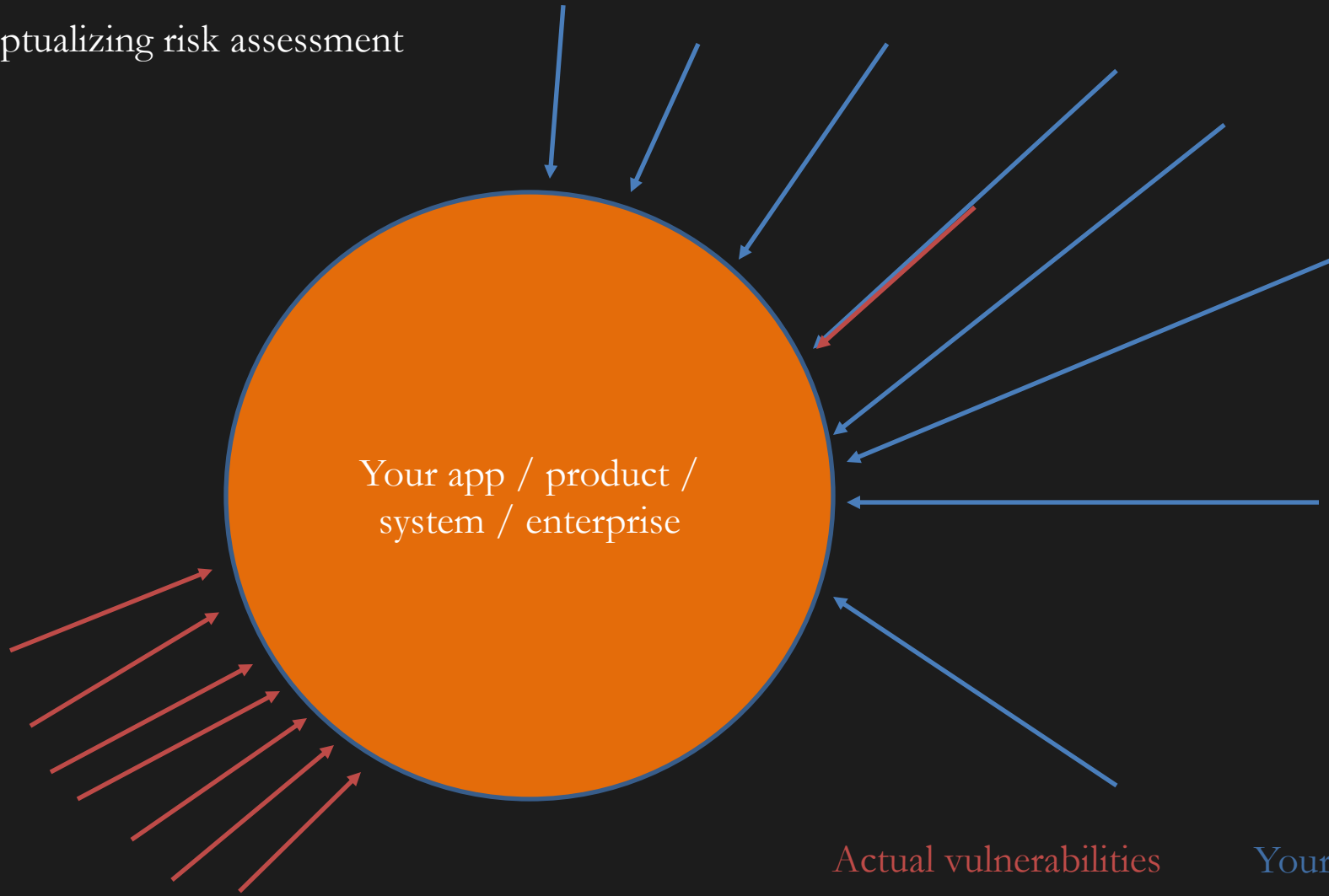
Security Risk Analysis is the process of identifying assets, identifying and assessing vulnerabilities, and determining threats

Conceptualizing risk assessment

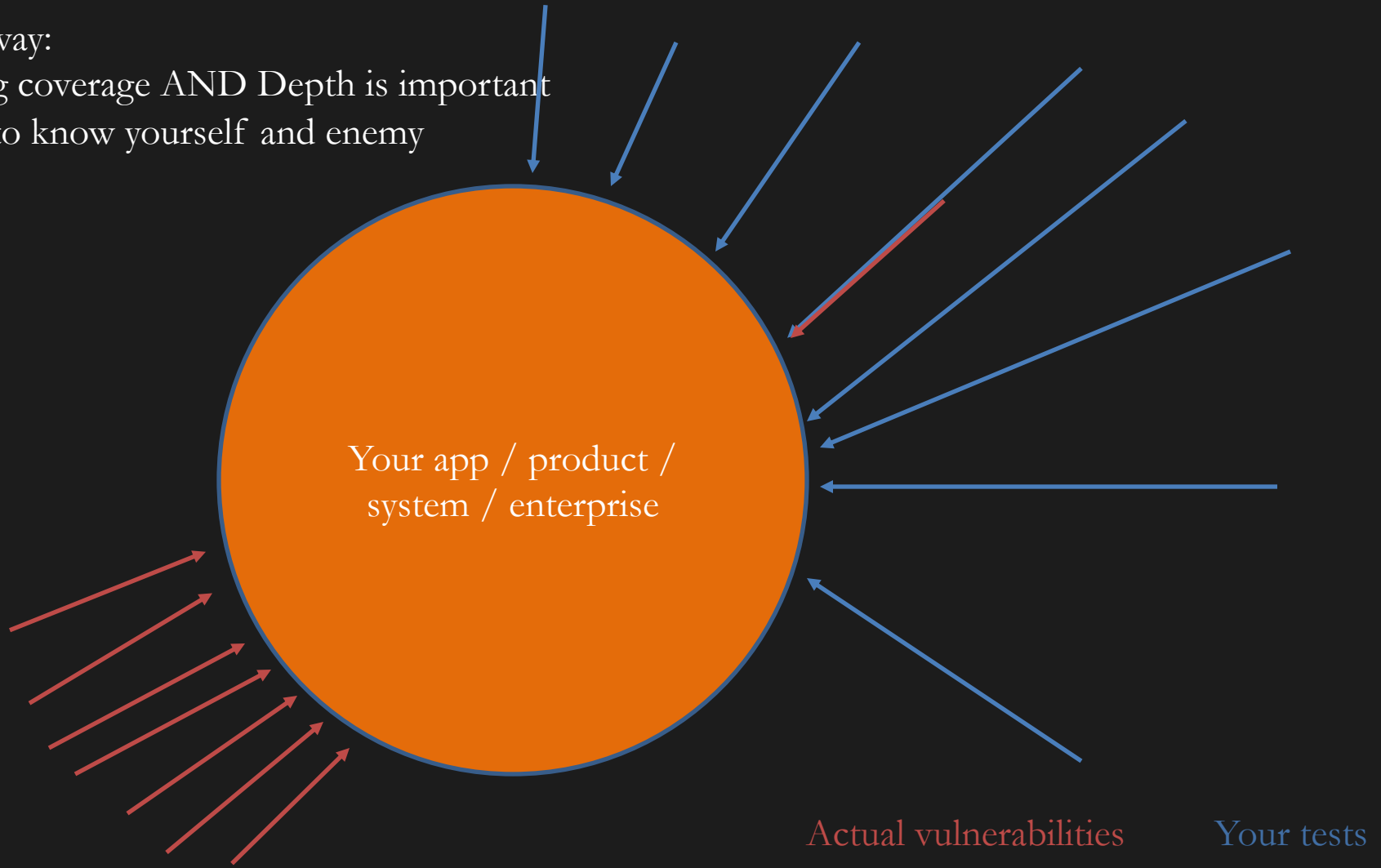
Actual vulnerabilities

Your tests

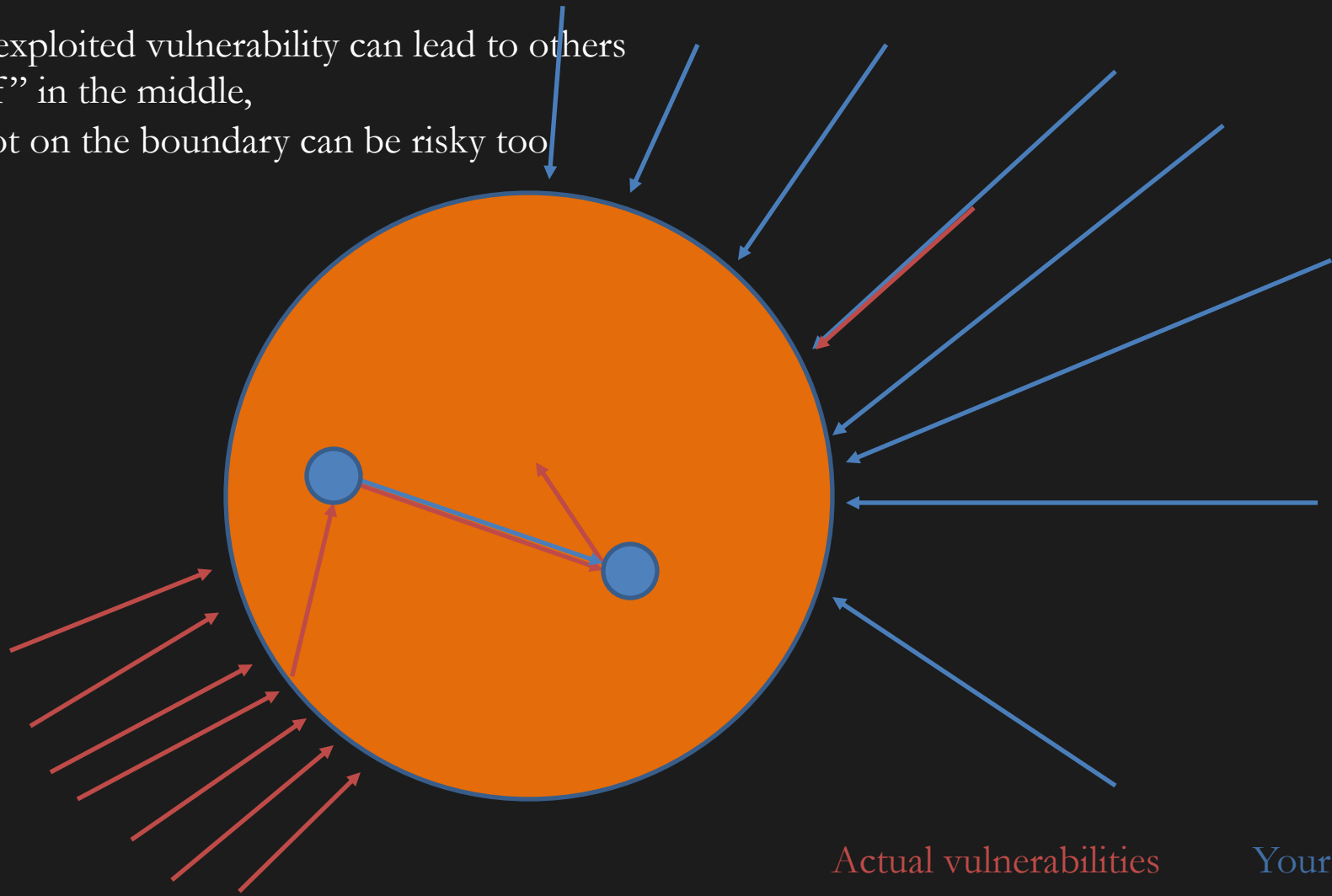
Conceptualizing risk assessment



Takeaway:
Having coverage AND Depth is important
Need to know yourself and enemy

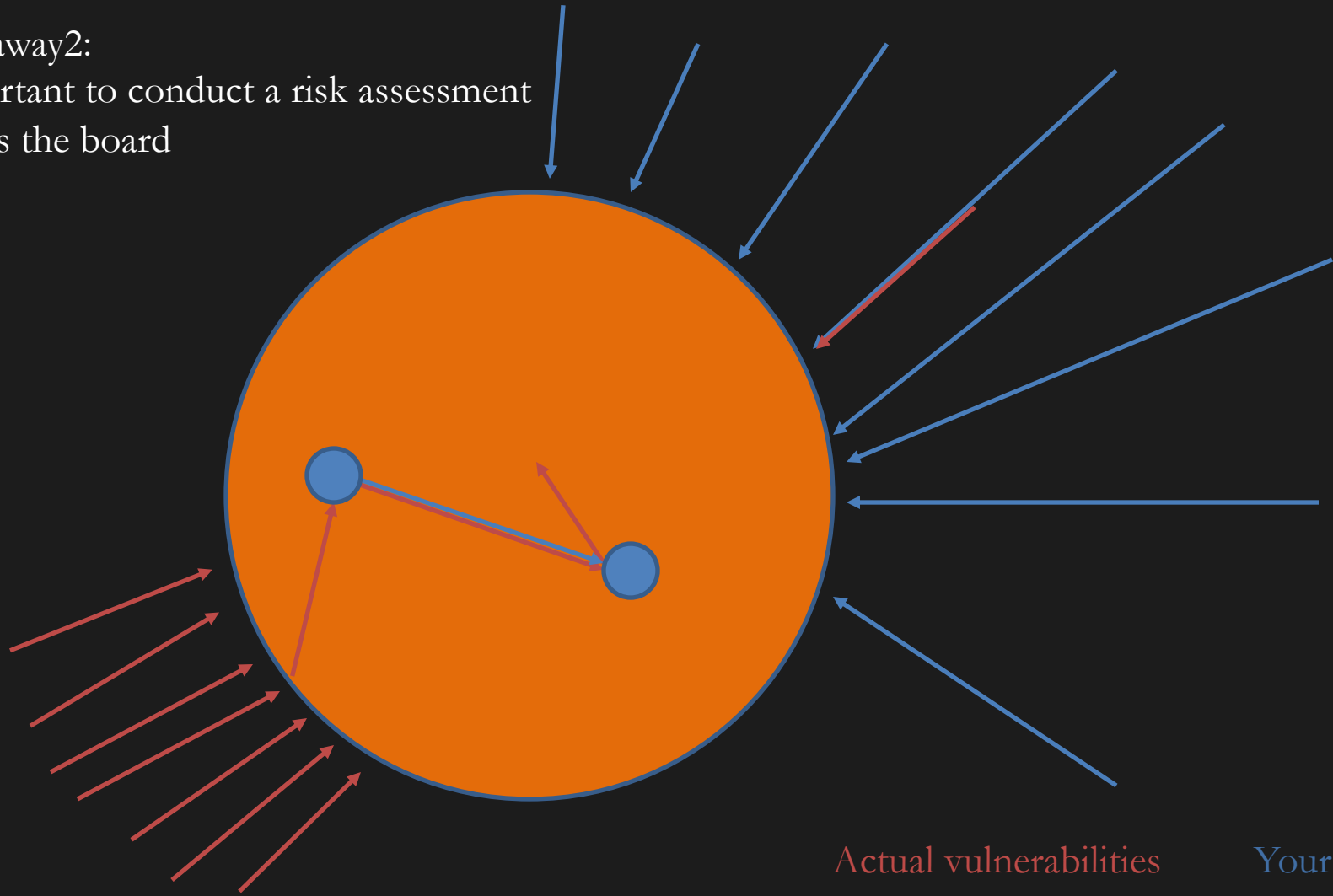


One exploited vulnerability can lead to others
"stuff" in the middle,
i.e. not on the boundary can be risky too



Actual vulnerabilities Your tests

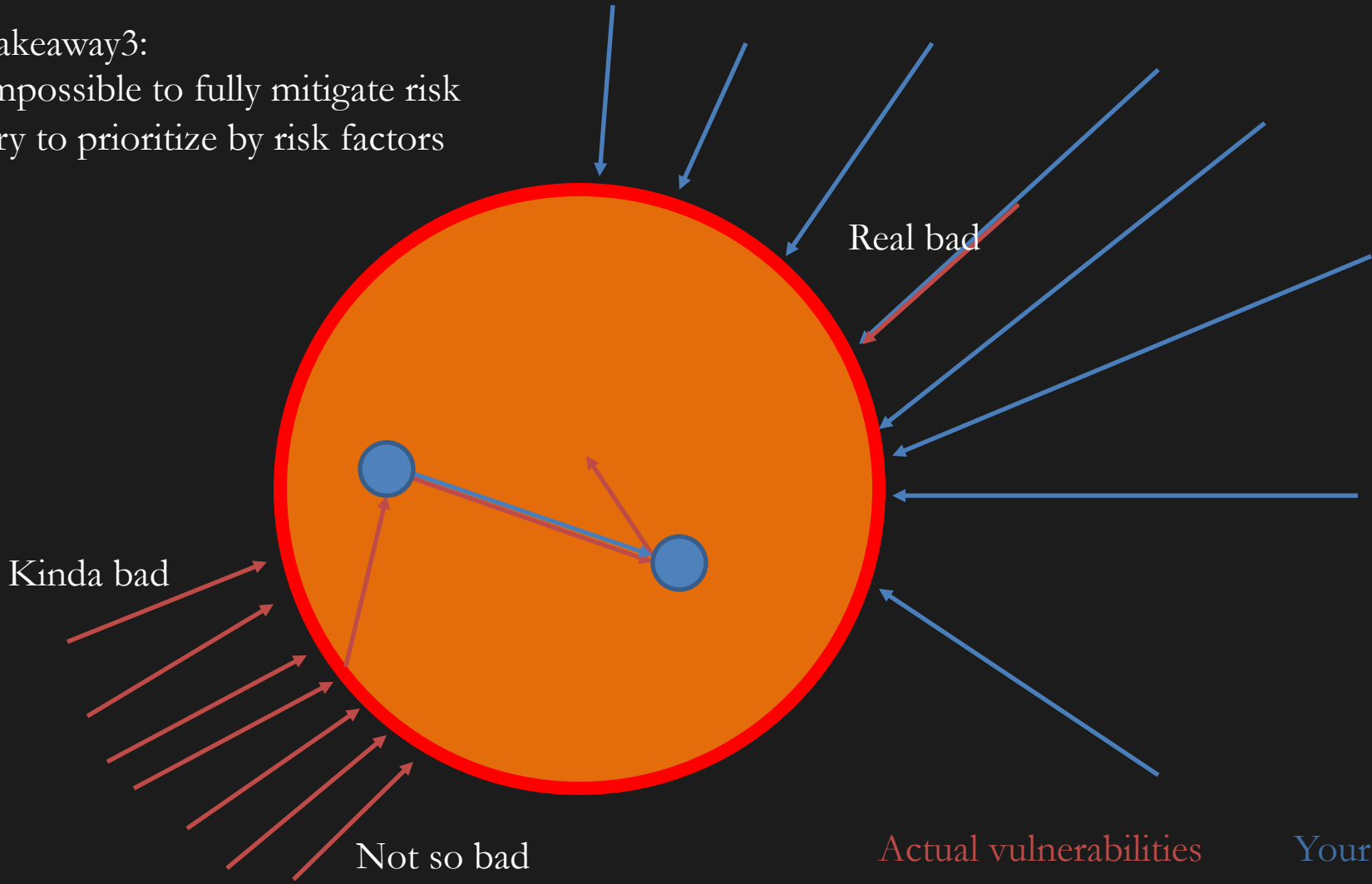
Takeaway2:
Important to conduct a risk assessment across the board



Actual vulnerabilities

Your tests

Takeaway3:
Impossible to fully mitigate risk
Try to prioritize by risk factors



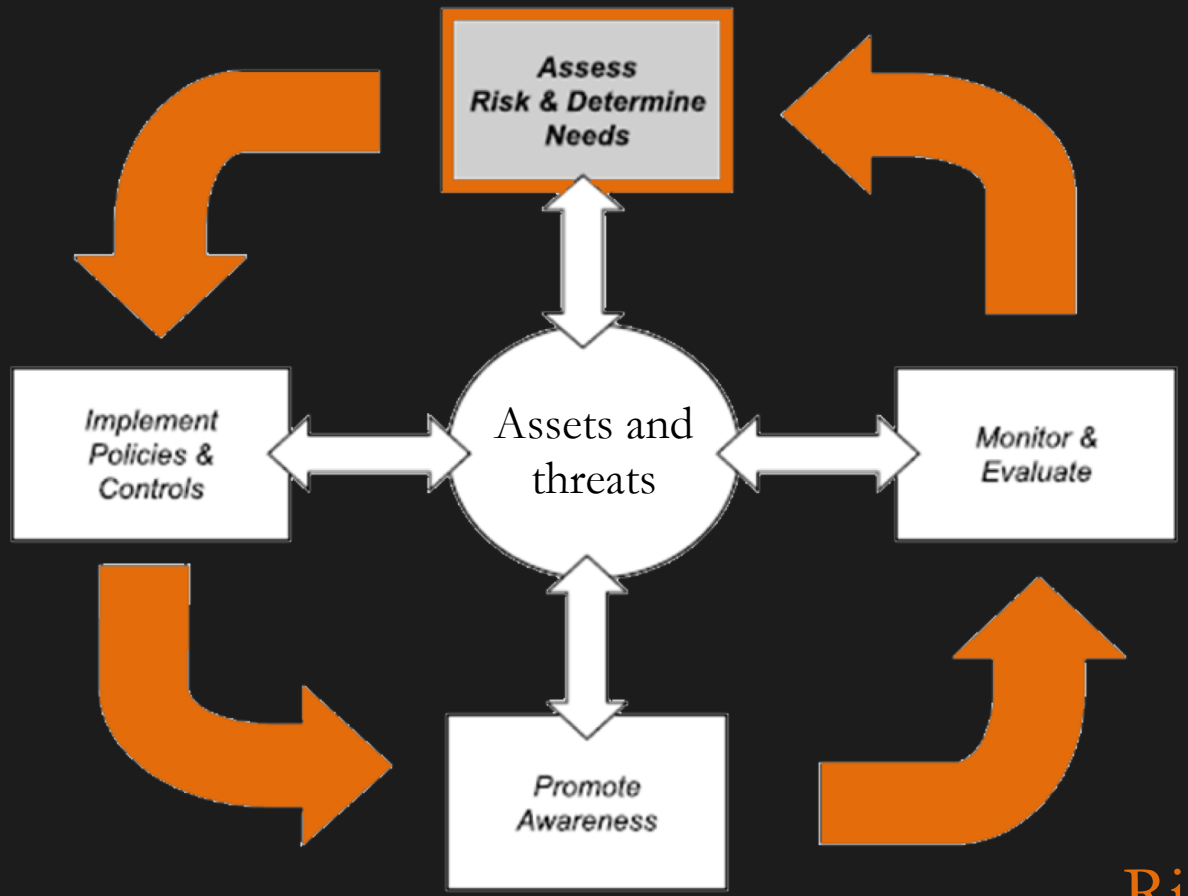
Value of Risk Analysis

- Increased understanding of strategic goals
- Direct mitigation efforts
- Prioritize and focus expenditures on biggest holes
- Minimize vulnerability surface
- Means for communicating to management
- Bottom line: Optimize allocation of limited security resources

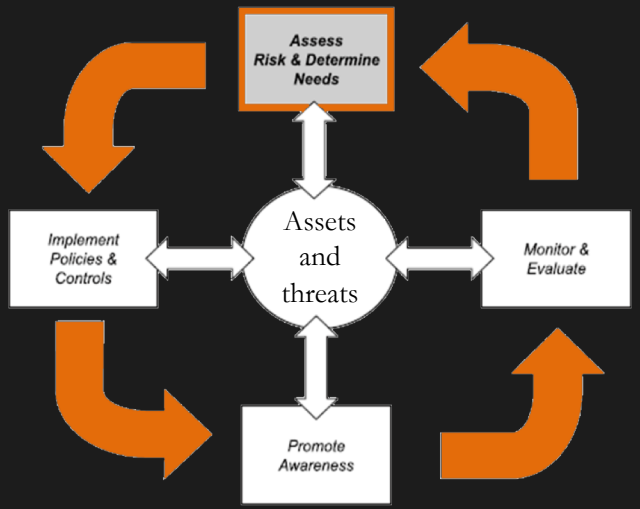
Who should be involved in Risk Analysis?

- Security Experts (you)
- Domain Experts (your customers or others at your company)
  - Know how things work
- Managers
  - Responsible for implementing strategy

Risk Management Lifecycle

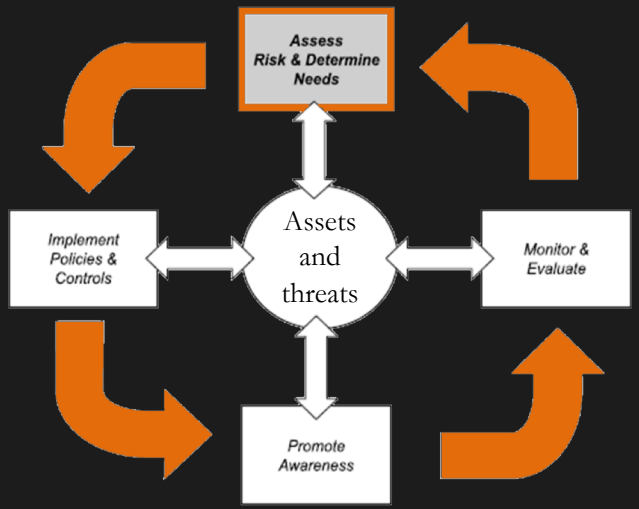


Risk Analysis



Components of Risk Mgmt. Lifecycle

- Risk analysis (assessment) [experts]
- Policy development [experts and mgrs.]
- Awareness and training [experts and staff]
- Monitoring [automated, IT staff, experts]



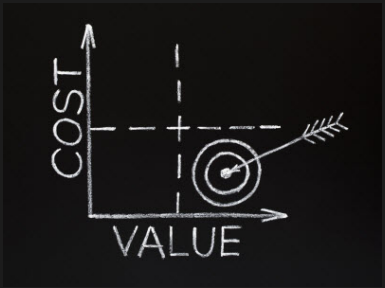
Risk Mgmt. by Domain

- Different process with third parties
  - Cloud implications
  - Web services
  - Outsourced business processes
    - e.g. payroll
- Domain affects policy decisions
  - Can result in contracts or service level agreements

Risk Assessment requires stakeholders to evaluate resources, calculate value, and determine threats.

Evaluating resources means enumerating *what you have*.

Calculating value means answering the question: how does what you have translates to $$$? This process needs to include reputation, customer satisfaction, and other non-tangibles as well as other assets.



Risk Analysis

Determining threats means understanding how what you have can be harmed (vulnerability), how likely it is to be harmed (likelihood), and how harming it reduces value (impact).

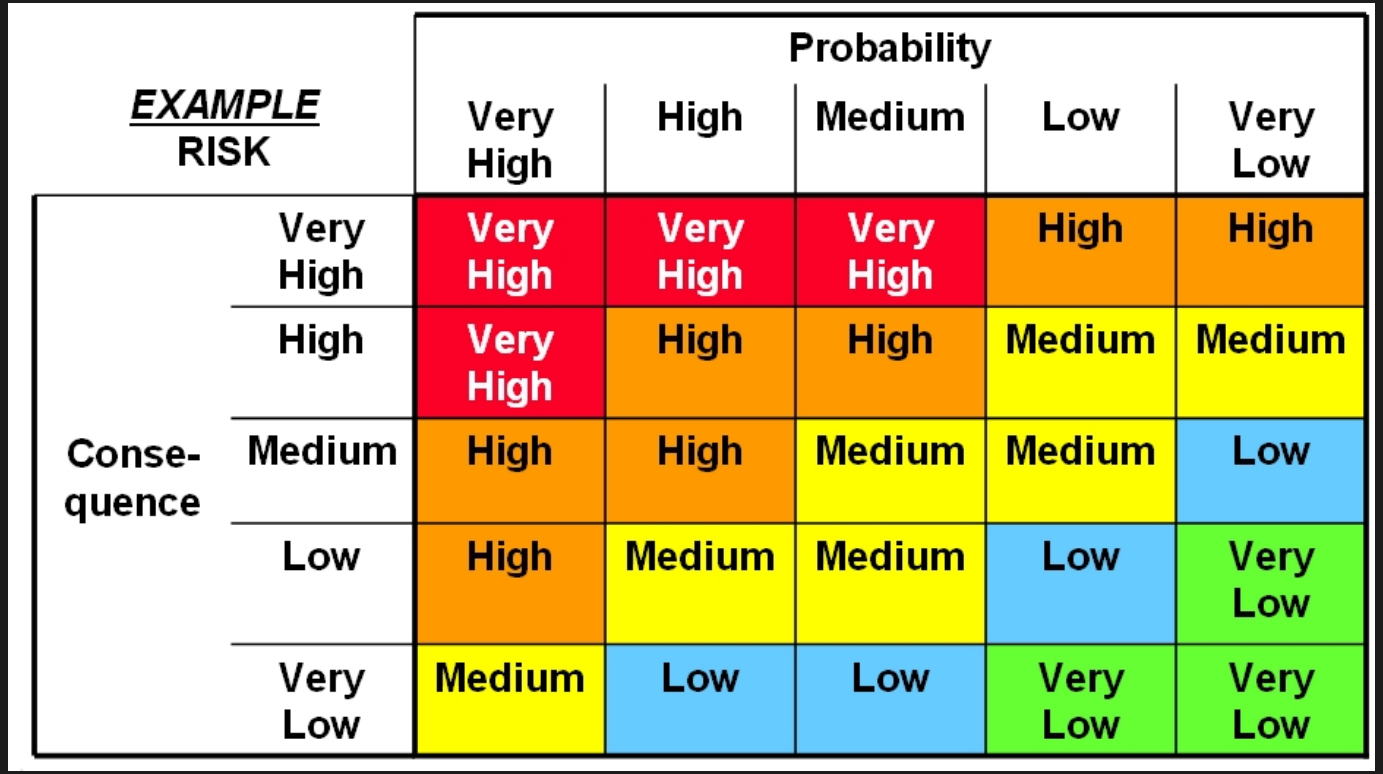
Risk Analysis

These components inform policy makers (a role you may find yourself in as a security expert or manager).

The other steps (after assessment) in the lifecycle will be major topics discussed later in this course.

The last step of risk assessment before policy making is perhaps the most important: Prioritizing risks

The obvious chart



EXAMPLE RISK		Probability				
		Very High	High	Medium	Low	Very Low
Conse-quence	Very High	Very High	Very High	Very High	High	High
	High	Very High	High	High	Medium	Medium
	Medium	High	High	Medium	Medium	Low
	Low	High	Medium	Medium	Low	Very Low
	Very Low	Medium	Low	Low	Very Low	Very Low

Risk prioritization

This assumes your predictions of likelihood and impact are accurate.

To nail down accuracy – you can look at an organization's loss metrics.

Definition

Annual Threat Loss Expectancy (ATLE) is the cost per year due to loss (partial or whole) of a collection of assets as a result of a threat.

Quantitative Definition

$$ATLE_{threat} = L_{rate} \times L_{cost}$$

Risk prioritization

L_{rate} is the frequency of a threat realization
L_{cost} is best formulated in terms of *single loss expectancies* and *expected threat impacts*

Definition

Single Loss Expectancy (SLE) is the cost incurred by a successfully executed threat on an asset.

Quantitative Definition

$$SLE_{threat,\ asset} = \text{Asset Value (AV)} \times \text{Percentage Lost (PL)}$$

Asset Value is determined during risk analysis.
Percentage lost is based on how much a threat affects an asset's value. It ranges from 0 (no affect) to 1(total loss).

Risk prioritization

Definition

Expected threat impact is the expected total cost to all assets incurred by the realization of a threat.
i.e. the sum of SLE for all assets related to the threat

Quantitative Definition

$$ETI_{threat} = \sum_{i=1}^{n} SLE_{threat,i}$$

Simple example
Threat: Someone steals from a jewelry story

Expected Window damage:

AV = \$5000 , PL = .1 => $SLE_{breakin,\ windows}$ = \$500

Expected jewelry theft:

AV = \$1000, PL = 1 => $SLE_{breakin,\ jewelery}$ = \$1000

$ETI_{breakin}$ = \$1500

Risk prioritization

Simple example

Someone steals from a jewelry store

Assuming jewelry theft happens twice a year.

Then

$$L_{rate} = 2 \text{ and } L_{cost} = ETI_{breakin} = \$1500.$$

Hence,

$$ATLE_{breakin} = \$3{,}000$$

Returning to the Ex. of Security Risk Choices

Allocate $10,000 to Info. Sec.

Option 1: Encrypt laptops

Option 2: Buy a firewall

Option 3: Train staff against phishing

Risk prioritization

To determine how to allocate Information Security Dollars you can calculate the ATLE for all threats then determine how much an investment lowers ATLEs.

Risk prioritization

Full Example

A business tells you:

They deal with laptop theft. Avg. laptop cost is 1000 dollars and average information on the laptop is worth 10k. They lose or have laptops stolen about 10 times per year. They also are subjected to denial of service attacks about 20 times per year. The company does an average of $5000/hr in sales. DOS attacks typically occur for an hour. They also get hacked about once every 5 years. Past hacks on web servers have cost about $50,000 to fix, while past workstation hacks cost about $1000. The last few times they were hacked, information reached the public and they hired an advertising firm to redeem their brand identity and rebuild their reputation. Over the advertising campaign, the paid about $100,000 to the agency. Lastly, their employees also routinely get phished (about 100 incidents per year). It costs the company an average of $500 for identity protection services per incident and an additional $100 for a technician to check and remove any malware on affected machines.

Risk prioritization

Full Example

Identify and quantify threats:

Laptop theft: Loss of a device and all company data on them

$ETI_{theft} = SLE_{theft,\ device} + SLE_{theft,\ companydata}$

Denial of Service: Loss of available of point of sale systems

$ETI_{dos} = SLE_{dos,\ pos}$

Hack: Network hacks exposing information on webservers or workstations

$ETI_{hacks} = SLE_{hacks,\ webservers} + SLE_{hacks,\ workstations} + SLE_{hacks,\ reputation}$

Phishing: Loss of personnel data or installation of malware on workstations

$ETI_{phishing} = SLE_{phishing,\ personneldata} + SLE_{phishing,\ workstations}$

Risk prioritization

Full Example (with numbers)

Threats:

Laptop theft: Loss of a device and all company data on them

$ETI_{theft} = SLE_{theft, device} + SLE_{theft, companydata}$

Avg. device cost is 1000 dollars, average information on the laptop is worth 10k

$SLE_{theft, device} = 1x \$1,000 = 1,000$, $SLE_{theft, companydata} = 1x \$10,000 = \$10,000$

$ETI_{theft} = \$11,000$

Risk prioritization

Full Example (with numbers)

Threats:

Denial of Service: Loss of availability of point of sale systems

$ETI_{dos} = SLE_{dos, pos}$

The average sales per hour using the POS system is $5000 and an average DOS attack occurs for an hour.

$SLE_{dos, pos} = 1x\$5000 = \$5,000$

$ETI_{dos} = \$5000$

Risk prioritization

Full Example (with numbers)

Threats:

Hack: Network hacks exposing information on webservers or workstations

$ETI_{hacks} = SLE_{hacks,\ webservers} + SLE_{hacks,\ workstations} + SLE_{hacks,\ reputation}$

The average hack on a web server incurs a cost of $50,000 while a workstation hack results in a cost of $1000.

$SLE_{hacks,\ webservers} = \$50{,}000$, $SLE_{hacks,\ workstations} = \$1000$

A successful hack on a web server also results in lost reputation in the public worth $100,000

$SLE_{hacks,\ reputation} = \$100{,}000$

$ETI_{hacks} = \$151{,}000$

Risk prioritization

Full Example (with numbers)

Threats:

Phishing: Loss of personnel data or installation of malware on workstations

$ETI_{phishing} = SLE_{phishing,\ personneldata} + SLE_{phishing,\ workstations}$

Personnel data costs the company an average of $500 for each item.

$SLE_{phishing,\ personneldata} = \$500$

On average some malware is installed as well which costs IT an additional $100 to remove.

$SLE_{phishing,\ workstations} = \$100$

$ETI_{phishing} = \$600$

Risk prioritization

Full Example Summary

Threats:

ETI_{theft} = $SLE_{theft,\ device}$ + $SLE_{theft,\ companydata}$
= $1000 + $10,000 = $11,000

(occurs 10 times a year) => $ATLE_{theft}$ = 10 x $11,000 = $110,000/year

ETI_{dos} = $SLE_{dos,\ pos}$
= $5000

(occurs 20 times a year) => $ATLE_{dos}$ = 20 x $5,000 = $100,000/year

ETI_{hacks} = $SLE_{hacks,\ webservers}$ + $SLE_{hacks,\ workstations}$ + $SLE_{hacks,\ reputation}$
= $50000 + $1000 + $100,000 = $151,000

(occurs once every 5 years [.2 times/year]) => $ATLE_{hacks}$ = .2 x $151,000 = $30,200/year

$ETI_{phishing}$ = $SLE_{phishing,\ personneldata}$ + $SLE_{phishing,\ workstations}$
= $500 + $100 = $600

(occurs 100 times a year) => $ATLE_{phishing}$ = 100 x $600 = $60,000/year

Risk prioritization

Full Example (Decision time)
Allocate $10,000 to Info. Sec.

Option 1: Encrypt laptops

Will prevent loss of data on laptops

Option 2: Buy a firewall

Expected to reduce rate of hack success by 50% and dos by 50%[e.g. ddos still works]

Option 3: Train staff against phishing

Expected to reduce rate of phishing attack success by 40%

Full Example (Decision time)
Allocate $10,000 to Info. Sec.

Option 1: Encrypt laptops

(reduces $SLE_{theft,\ companydata}$ to 0) => $ATLE_{theft}$ reduced by $100,000

Option 2: Buy a firewall

(reduces rate of hack success by 50% and dos by 50%[e.g. ddos still works])
=> DoS L_{rate} drops to 10 (from 20) and $ATLE_{dos}$ reduced by $50,000
=> hack L_{rate} drops to .1 (from .2) and $ATLE_{hacks}$ reduced by $15100
for a total of $65,100

Option 3: Train staff against phishing

(reduces rate of phishing attack success by 40%)
=> reduces Phishing L_{rate} to 60 (from 100) and $ATLE_{phishing}$ reduced by $24000

Definition

Return on Investment (ROI) is the ratio of profit to cost. In security risk explorations – `profit` can be formulated in terms of *savings* through reduction of risk

Quantitative Definition

$$ROI_{investment} = \frac{profit}{cost}$$

Full Example (Decision time)
Return on investment

Option 1:
ROI_1= \$100,000/\$10,000 = 10

Option 2: Buy a firewall
ROI_2 = \$65,100/\$10,000 = 6.51

Option 3:
ROI_3 \$24000/\$10,000 = 2.4

Full Example (Decision time)

Allocate $1000 to Info. Sec.

Clearly the best solution

Option 1:

Encrypt laptops (reduces $SLE_{theft,\ companydata}$ to 0) => $ATLE_{theft}$ reduced by $100,000

Option 2: Buy a firewall

(reduces rate of hack by 50% and dos by 50%[ddos still works])

=> DoS L_{rate} drops to 10 (from 20) and $ATLE_{dos}$ reduced by $50,000

=> hack L_{rate} drops to .1 (from .2) and $ATLE_{hacks}$ reduced by $15100

for a total of $65,100

Option 3:

Train staff against phishing (reduces rate of phishing attacks by 40%)

=> reduces Phishing L_{rate} to 60 (from 100) and $ATLE_{phishing}$ reduced by $24000

Questions:

What do these ROIs indicate strategically to the company?
What conclusions can we draw about spending?
What should you advocate for as a security analyst?
What assumptions were made here?

This assumes you have good average assessments of what your assets are worth and how much threats cost you.

It also assumes you can identify how countermeasures (info sec spending) will mitigate losses.

Sadly organizations don’t always have a full or complete understanding of these costs.

Next Time

More about Risks:
zero day risk prioritization
risk probability theory
countermeasures and mitigation analysis

…and more

Reading

Read Ch. 2 in Brotby

Homework

Homework 1: ATLE/ETI/SLE exercise

https://mlhale.github.io/CYBR3600/homework/iasc3600-homework1.pdf

Next Time

Quiz on Thursday (Aug 31st) on Governance and Risk

Questions?

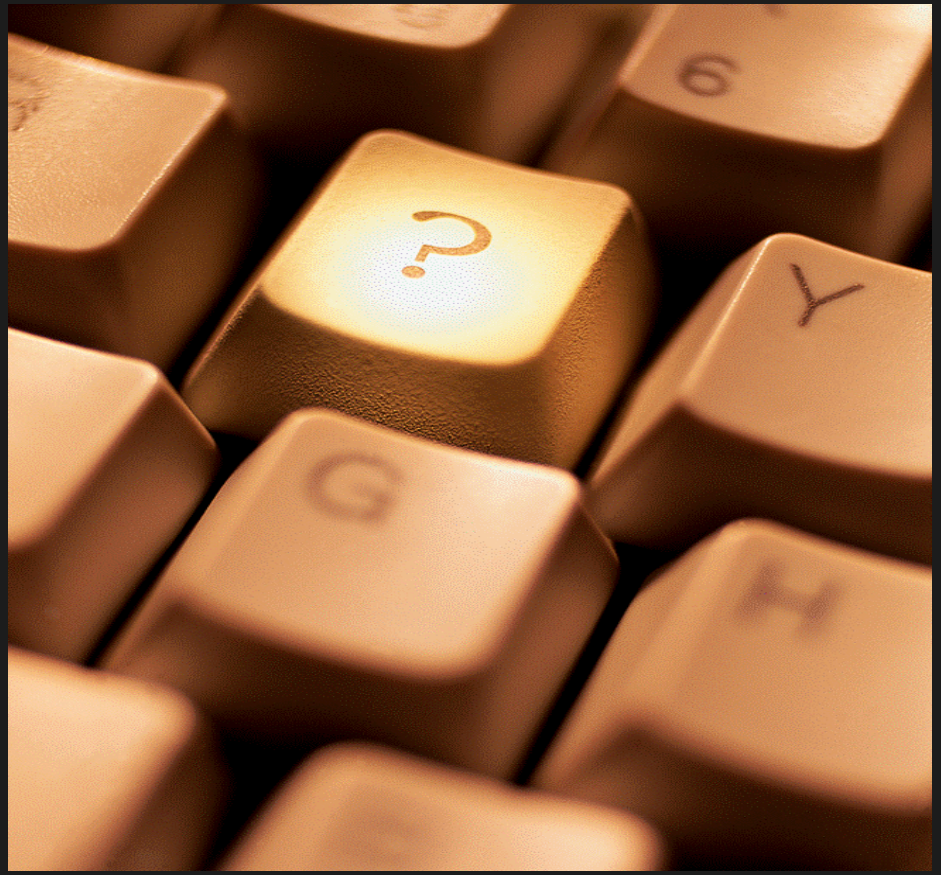
Matt Hale, PhD

University of Nebraska at Omaha

Interdisciplinary Informatics

mlhale@unomaha.edu

Twitter: @mlhale_



© 2014-2018 Matthew L. Hale