

# Fireside Fridays

---

Evaluating risk  
Week 4

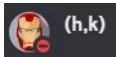
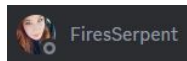
# Thanks to our sponsors!

**ACTIVE** | COUNTERMEASURES



Antisyphon Training

# Special Thanks to...

- Hermon  (h,k)
- Emily  FiresSerpent
- Both gave up many late nights to help with QA and development of this content
- Very much appreciate their efforts!
- Please give them a warm "thanks" the next time you see them online

# Lab requirements for this section

- No labs
- This section will be all lecture

# Your role with risk

- As a security architect, you are expected to:
  - Identify critical business assets
  - Identify potential vulnerabilities
  - Identify potential threat vectors
  - Identify how to best handle each of these risks
- Stick to a systematic approach
- Don't get overwhelmed!

# What is risk?

- Situation that exposes asset(s) to compromise
- Intersection of three components:
  - **Asset** - Something of value to the organization
  - **Threat** - Entity with the capacity to harm the asset
  - **Vulnerability** - Vector where by the threat could potentially compromise the integrity of the asset
- Will focus mostly on cyber risks

# Risk is a bit like the game of Clue

- Colonel Mustard in the library with the candlestick
- Untrained employee in production with poor procedures
- Criminals in the customer database vulnerable to SQL injection attacks
- Nation state actors in the file share with confidential blueprints via credential stuffing the VPN

# What are assets?

- Anything that provides value towards the goals of the organization
- The more critical to the business model, the greater the value of the asset
- What would it take to recover if the integrity of the asset is compromised?
  - Access lost?
  - Exposed to the public?



# Asset value can be tricky to calculate

- Also need to look at the value to the adversary
- Example: a network printer
  - Could be argued the value to the org is pretty low
  - Especially if there are multiple printers
  - What's the value to an adversary?
  - A printer could be a foothold to monitoring and accessing all other internal systems
- Adversary value should act as a modifier to overall value

# Adversarial threats

- **Insiders**
  - A good culture can go a long way towards mitigation
  - Both in caring and reporting without fear of retribution to false positives
- **Competitors**
  - Others in your business vertical
  - Nation states
- **Crime organizations**
  - If compromising the asset can be monetized
- **Generic jerks - Because they can**

# Non-hostile threats

- **Accidental/inadvertent**
  - Blameless postmortems are key
  - Poor planning or expertise
- **Structural**
  - Poor/wrong software
  - Bugs, lack of patching or upgrading (hardware or software)
- **Environmental (not really cyber)**
  - Natural disaster
  - Man made disaster

# Types of risk

- Operational risks
  - Human mistakes
  - Incorrect or incomplete processes
  - Software or hardware failures
- Strategic risks
  - Ability to implement business plan
  - Ability to execute at a specified time
  - Shifts in consumer preferences
  - Failure to reach target market

# Types of risk (cont)

- **Financial risks**
  - Wasteful spending
  - Allocate finances to the wrong resources
  - Inability to generate new revenue
- **Compliance risk**
  - Fines/penalties due to lack of compliance
  - PCI is a good example
- **Reputational risk**
  - Loss of community standing

# What can be done with risk?

- Avoid
- Mitigate
- Transfer
- Accept
- A combo of two or more of the above

# Risk avoidance

- Take steps to entirely eliminate the risk
- Examples:
  - Upgrade operating system - Move past old bugs
  - Patches - But typically only eliminates one vector
  - Secure configuration - Default configs tend to be open
  - Change platforms - But this may introduce new vectors
  - Re-evaluation of architecture based on current requirements and technologies

# Risk mitigation

- Mitigation reduces risk, but not eliminate it
- Option when risk cannot be avoided
- Examples:
  - Removing the network eliminates all network threats
  - But systems cannot exchange information
  - So we mitigate by using firewalls, 2-factor, EDR and various other cyber protection
  - Remaining risk is then "accepted"



# Risk transfer

- Move the risk to another entity
- Examples:
  - Buying (cyber) insurance
  - Extended warranty (when applicable)
  - Service moved to a third party
- Is outsourcing risk transference?
  - Risk typically resides with entity hosting the data
    - Consultants or MSPs versus fully hosted environments

# Risk acceptance

- Accept the potential impact the risk may have against the business
- Examples:
  - Replacement value exceeds the cost of avoidance
  - Mitigations are in place reducing risk to acceptable levels
  - Ignoring the risk
  - Ignorance of the risk
- You are accountable for the risks you accept
  - Intentionally or through ignorance

# Risk controls

- Administrative
  - Mitigate risk via policies and attestations
- Operational
  - Mitigate risk via processes and audits
- Technical
  - Mitigate risks via the implementation of security tools
  - Usually requires capital expenditure
  - But the first two may require additional personnel

# Qualitative risk analysis

- Based on probability, not exact science
- Subjective, based on feelings and expertise
  - Hard to perform when you are new to the field
- Informed decision based on what you know
  - Increase accuracy via proper risk assessment
- Useful when insufficient data for full quantitative eval
  - But quantitative has its own problems
  - (Discussed later)

# Probability/Impact matrix

Impact

Probability

	Trivial	Minor	Moderate	Major	Extreme
Rare	Insignifigant	Low	Low	Medium	Medium
Unlikely	Low	Low	Medium	Medium	Medium
Moderate	Low	Medium	Medium	Medium	High
Likely	Medium	Medium	Medium	High	High
Very Likely	Medium	Medium	High	High	Critical

## Vulnerability risk rating

# Determining vulnerability probability

- Probability components:
  - Age - How long has the vector existed?
  - Complexity - How easy is it to perform the attack?
  - Accessibility - Are tools available to automate the attack?
  - Fix - Is a patch available eliminating vector?
- A combo of the above will produce probability
- Not an exact science

# Determining vulnerability impact

- Common Vulnerability Scoring System (CVSS)
- Open standard for rating vulnerabilities 0 - 10
- Synced with NIST vulnerability database
- Provides impact assessment for known vulnerabilities
- Environment probability may modify scores

<https://nvd.nist.gov/>

# CVSS example

- ConnectWise 2024 ScreenConnect (CVE-2024-1709)
- Age - All versions are vulnerable
- Complexity - Exploitable with a web browser
- Accessibility - Known URL searchable on Shodan
- Impact - Provides remote Admin to key systems
- CVSS score - Perfect 10
  - We see about 40+ of these per year
  - 2,300+ scored at 9.8 or above



# Qualitative limitations

- Does not identify how much budget/resources should be allocated to a specific risk
- Not really an option when you are new
  - You don't know what you don't know
  - Easy to get blindsided
- With the above said, it's frequently the best option

# Quantitative risk analysis

- Quantitative is based on Probabilistic Risk Assessment (PRA)
- Identify Single Loss Expectancy (SLE)
- Identify Annual Rate of Occurrence (ARO)
- Calculate Annual Loss Expectancy (ALE)
  - $SLE \times ARO = ALE$
  - May need to modify SLE based on additional attributes such as reputation loss

# Single Loss Expectancy (SLE)

- Product of two attributes:
  - The Asset Value (AV)
  - The Exposure Factor (EF) of the asset
  - EF is percentage of AV lost during event
- So our PRA formula becomes:
  - $(AV \times EF) \times ARO = ALE$

# Data breach example - asset value

- SLE calculation of data breach of PII data
- Asset value (AV) includes:
  - Cost to remove adversaries from the system
  - Cost to investigate and close the vulnerability
  - Consulting and legal services
  - Notification and possible ID theft services
  - Lost sales due to reputation hit
  - Fines/lawsuits due to data compromise

# Data breach example - SLE calculation

- Exposure factor (EF) of asset
  - Database is still functional
  - Everybody gets compromised - no longer big news
- The above may lower the SLE calculation
- For the sake of argument, let's assume SLE of \$4.45M\*  
which is the global average

\* Research into this value was funded by multiple organizations that profit from helping companies prevent data breaches.

# Quantitative example - ARO calculations

- Need to factor in Annual Rate of Occurrence (ARO)
- How frequently do companies get breached?
- Anecdotal data at best in this space
- Estimates are major breach every 5 to 8 years
- Let's split the difference and call it 6.5 years

# Crunching the quantitative numbers

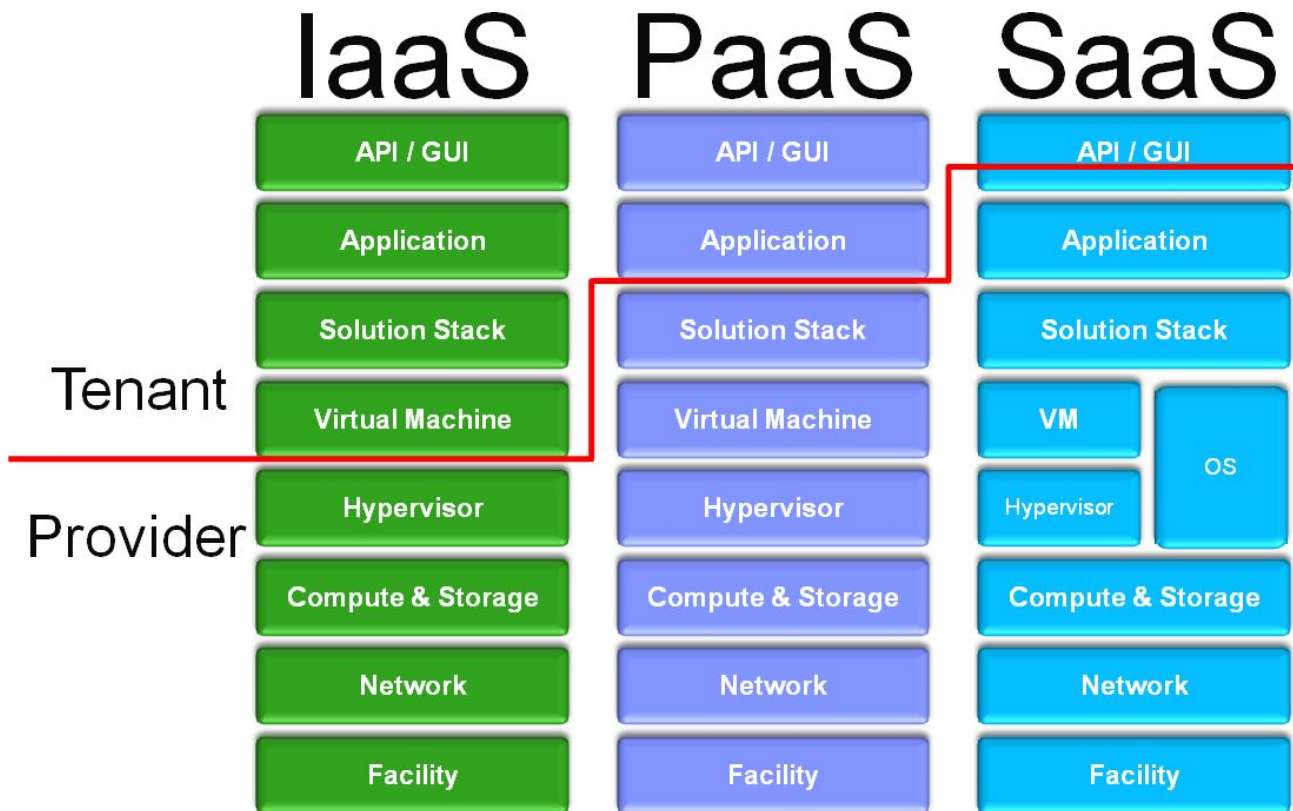
- SLE = \$4.45M
- ARO = .15 events per year
- Annual Loss Expectancy (ALE)
  - $4,450,000 \times .15 =$  loss of \$667,500 annual
- Annual budget should not exceed \$667K
  - That's all in
  - Hardware, software and staff
  - This is why you can't just be a cost center

# More on risk transference

- Does public cloud qualify as risk transference?
- We stated risk resides with the hosting entity
- This usually describes public cloud
- Extent depends on delineation of responsibility
- The higher the line is up the stack, the greater the amount of risk that can be shifted



# Provider's Cloud Deployment Model



# Firewalls - the fuzzy line

- Some attestations require the use of stateful firewalls
- Provider may accept responsibility for making a stateful firewall available
- They may leave responsibility for daily management up to you

# Impact on security attestations

- Security attestations are simply a collection of controls
  - Mentioned SOC II, PCI, etc.
  - Controls mitigate risk at different layers
- The higher the delineation line, the fewer controls you need to personally implement
- Providers attestation of compliance is essentially a "get out of jail" free card

# More on risk

- I cover this topic in more detail in my security leadership class
- Helps to ensure upper management makes good choices
- Also needed to drive funding

<https://www.antisiphontraining.com/live-courses-catalog/security-leadership-and-management-w-chris-brenton/>

# Next week on Fireside Fridays!!!

- Everything you ever wanted to learn about layer 2 comms
- But were afraid to ask
- And maybe even a bit more
- There will be some labs
- Need access to a Linux or Windows system

# Wrap up

- Thank you for attending!
- Certs & video usually go out in 24 hours
- If you have any lingering questions, the Discord channel will remain active
  - Also a good chance to socialize with others in the class
  - Have other tips and tricks? Please share with others!
  - Posting screenshots can be helpful :-)