JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Welcome

## RISK MANAGEMENT FOR MANAGERS

# What does this class cover?

- What is risk?
- What happens when risk management fails?
- What can you do with risk?
- How do you calculate risk?

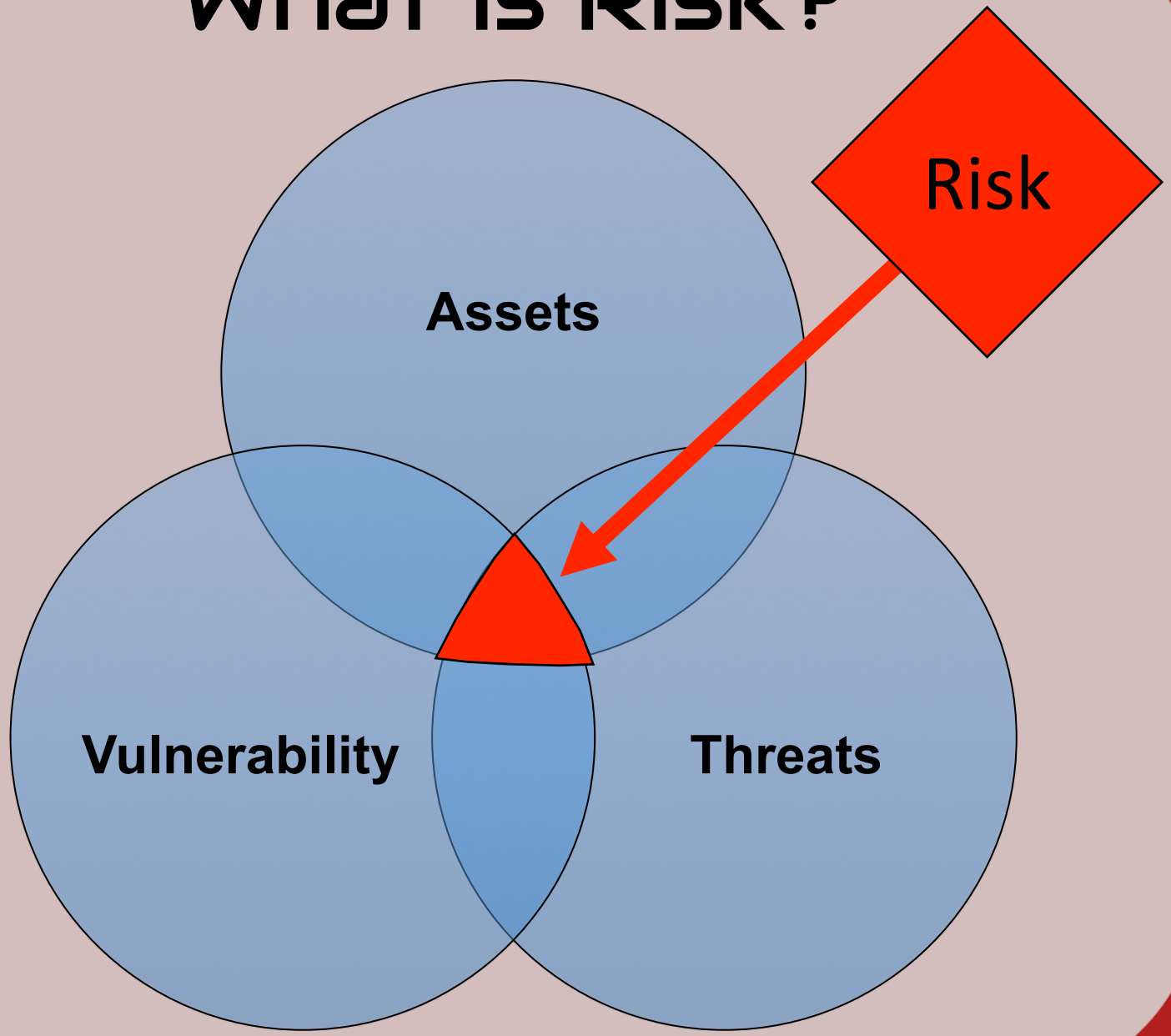
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# What is Risk?

## RISK MANAGEMENT FOR MANAGERS

# What is Risk?




JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

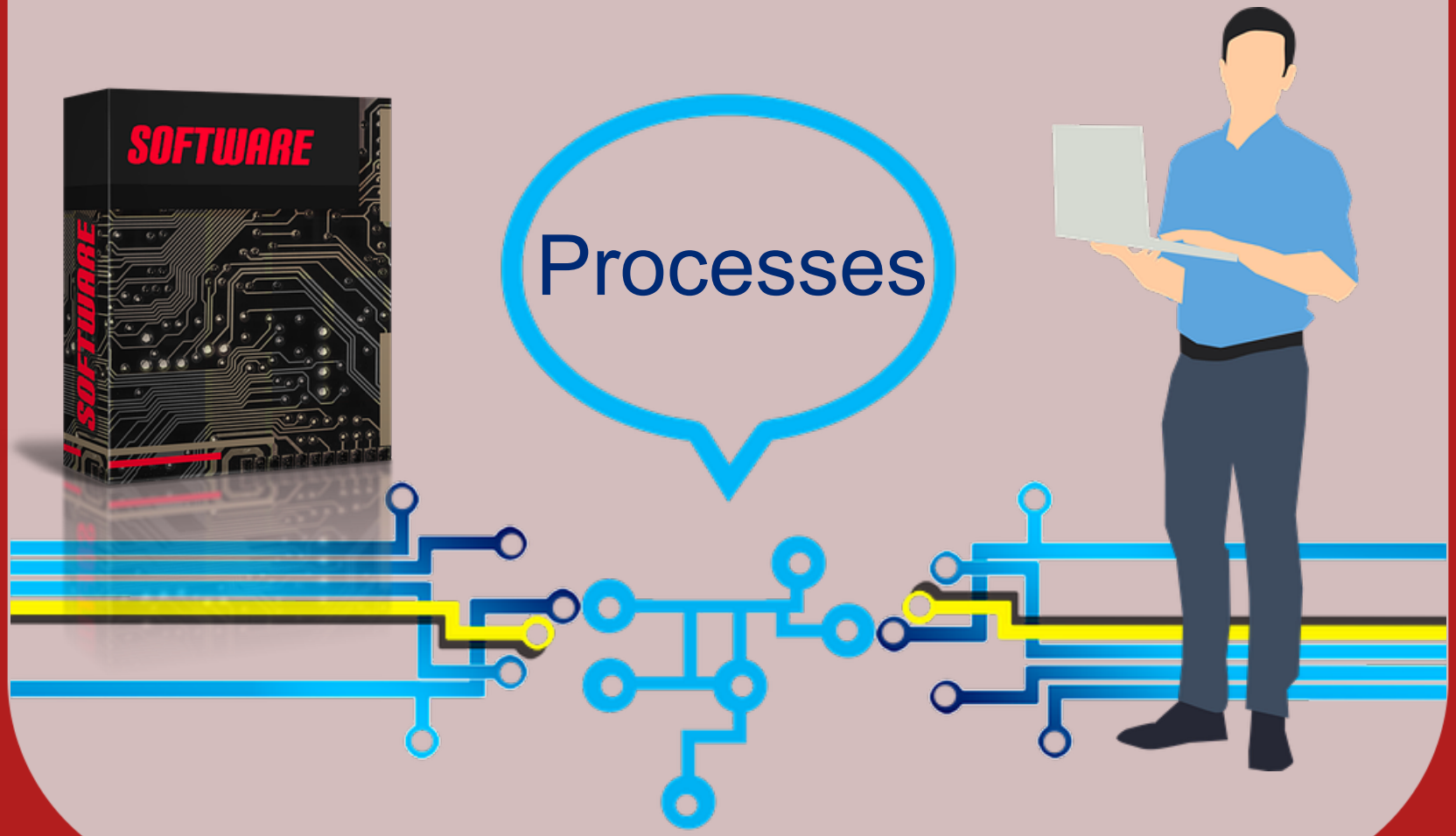
# Assets

Any item that has a value to organization


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Assets

Any item that has a value to organization






# Vulnerabilities

Any weakness in the system design, implementation, software code, or lack of preventative mechanisms

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Vulnerabilities

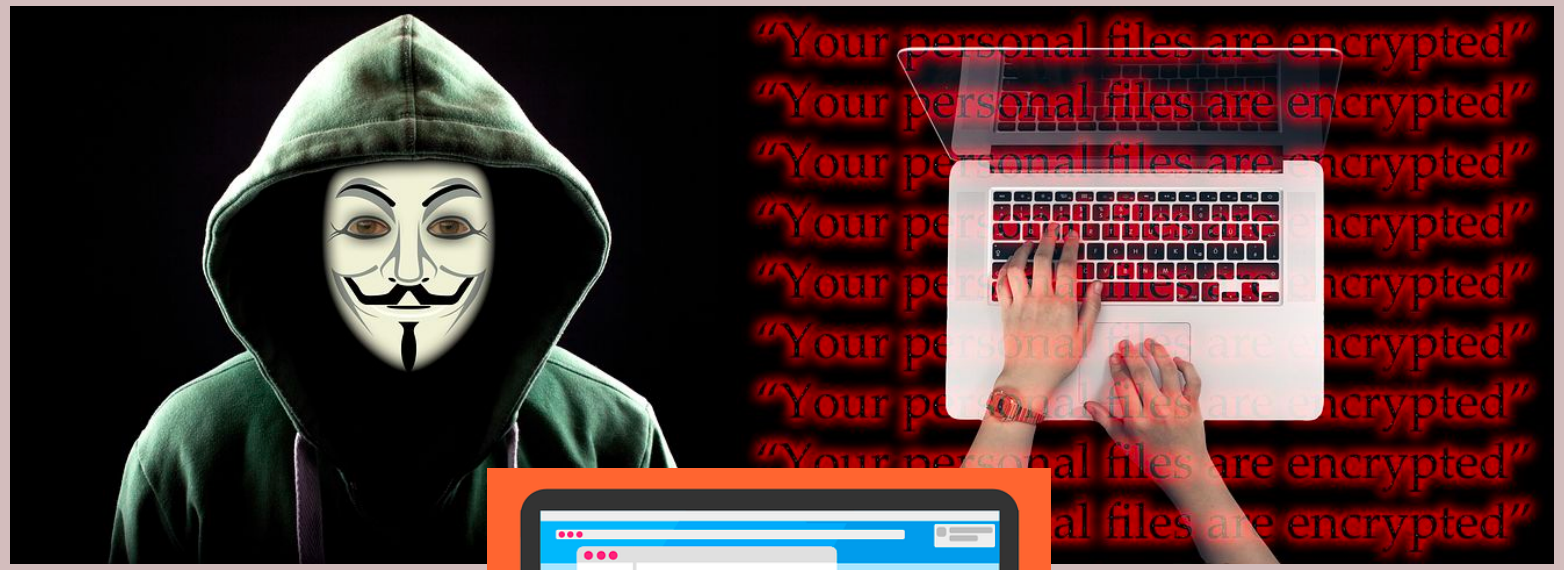
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Cybersecurity and IT professionals are in control of vulnerabilities in their platforms

Vulnerabilities are internal factors

# Threats

Any condition that could causes harm, loss, damage, or compromise of an asset

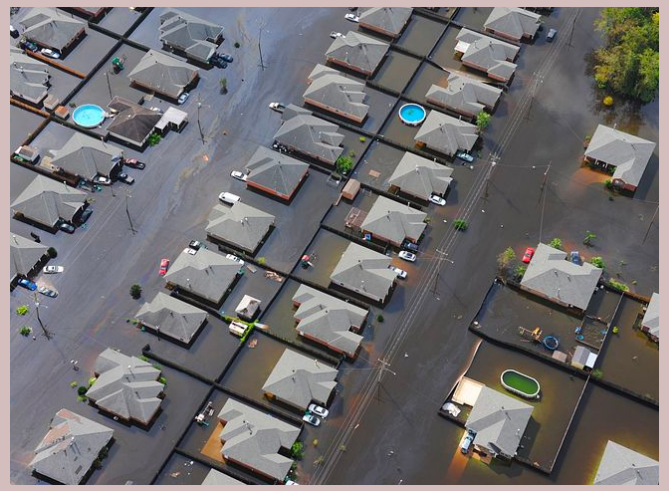




JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Threats

Any condition that could causes harm, loss, damage, or compromise of an asset




# Threats

- Cybersecurity and IT professionals cannot control threats in their platforms
- Can only manage and mitigate them
- Threats are external factors

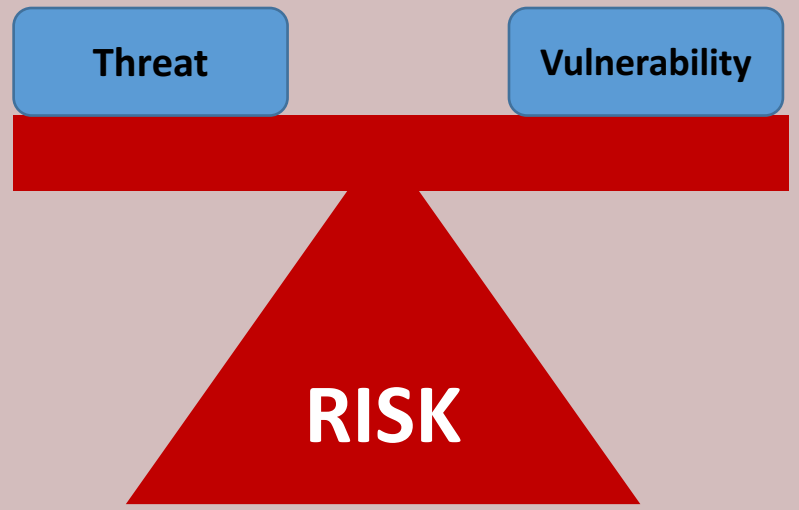
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# What is RISK?

Probability of the realization of a threat

There is no risk if a vulnerability AND a threat do not exist

**RISK = Vulnerability X Threat**




JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

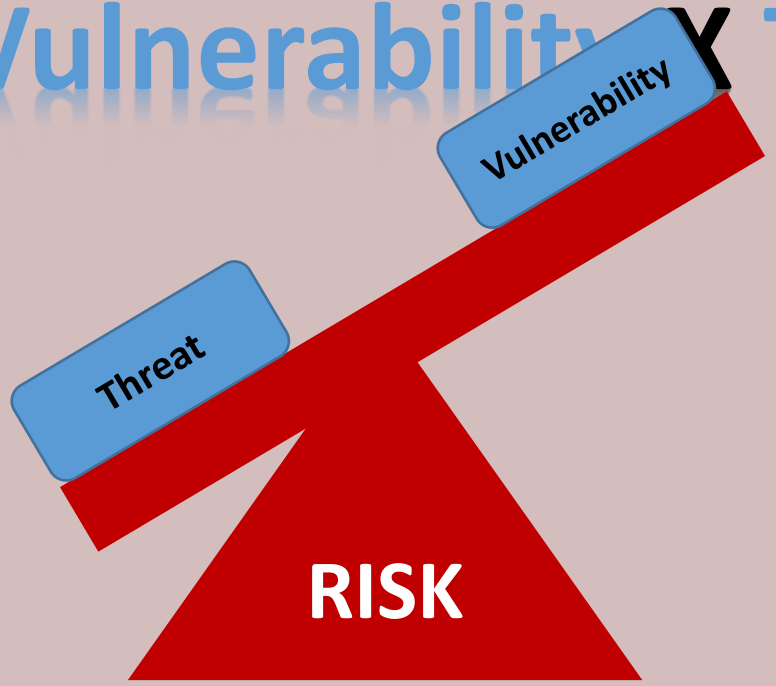
# What is RISK?

Probability of the realization of a threat

x

There is no risk if a vulnerability AND a threat do not exist

**RISK = Vulnerability X Threat**




JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# What is RISK?

Probability of the realization of a threat

There is no risk if a vulnerability AND a threat do not exist

**RISK = Vulnerability X Threat**


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# What is Risk?

## RISK MANAGEMENT FOR MANAGERS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

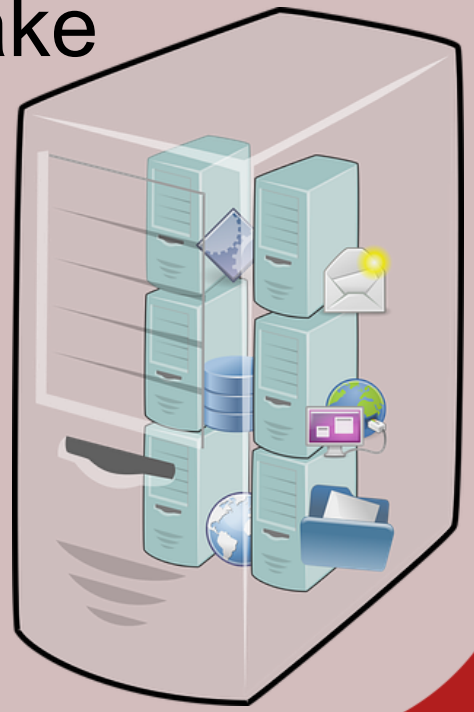
# Types of Risk

## RISK MANAGEMENT FOR MANAGERS

# Strategic Risk

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Resulting directly from operating within a specific industry at a specific time
- Shifts in consumer preference or new technologies can make your product lines obsolete
- Counteract by putting mitigations in place to detect change early



# Compliance Risk

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Legislative laws and bureaucratic regulations are another form of risk for our organizations

- Compliance is required with laws, but also introduces risks to the organization

# Financial Risk

- How does your organization handle money?
- How do you allow your customers to pay you?
- Do you extend credit to them?
- Also takes into account interest rates and foreign exchange rates




# Operational Risks

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Results from internal failures from internal processes, people, or systems

- Can result from unforeseen external events like power outage or cyber attack

# Reputational Risk

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Loss of a company's reputation or community standing from product failures, lawsuits, or negative publicity

- Reputations take a long time to build, only a day to lose…

MOTOR HARLEY-DAVIDSON COMPANY

TARGET

# Other Risks

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Much more difficult to categorize

- Environmental
  - Natural Disasters

- Employee Management
  - Maintaining a trained staff with up-to-date skills

- Political Instability
  - Change in laws and regulations

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Types of Threats

## RISK MANAGEMENT FOR MANAGERS

# Adversarial Threats

- Consider their capability, intent, and likelihood

- Examples:
  - Trusted insiders
  - Competitors
  - Suppliers
  - Customers
  - Business partners
  - Nation states



# Accidental Threats

- Occurs when someone makes a mistake that hurts the security of the system

- Example:
  - System administrator accidently takes servers offline causing loss of availability



# Structural Threats

- Occurs when equipment, software, or environmental controls fail

- Example:
  - IT server fails due to hard drive failure
  - Servers fail due to overheating (HVAC fail)
  - Software failure (OS bug or crash)



# Environmental Threats

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Occurs when natural or man-made disasters occur

- Example:
  - Fires
  - Flooding
  - Severe storms
  - Loss of power from the city power grid
  - Fiber or telecommunication lines cut

# Always Remember…

- Threats come from both external and internal sources, but most risk assessors think of internal sources first…
- We aren't just worried about hackers, but also the trusted insider…
- As you design security controls, don't forget to think about disgruntled employees, inept administrators, or the insider threat!



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Types of Threats

## RISK MANAGEMENT FOR MANAGERS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# When Risk Management Fails?

## RISK MANAGEMENT FOR MANAGERS

# When Risk Management Fails...

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

AMAZON | CLOUD COMPUTING

## Amazon's massive AWS outage was caused by human error

One incorrect command and the whole internet suffers.

By Jason Del Rey | @DelRey | Mar 2, 2017, 2:20pm EST

TWEET SHARE LINKEDIN


Sean Gallup / Getty

# When Risk Management Fails…

- Amazon Web Services (Feb 28, 2017)
- 100s of websites were taken offline
- Technician utilized a SOP to take a small number of servers offline, but input the command incorrectly
- It took down the entire US-EAST-1 region!



# When Risk Management Fails...

- Employees were debugging an issue with the billing system and accidentally took more servers offline than intended

- The error started a domino effect that took down two other server subsystems



# Accidental Threats

- Removing a significant portion of the capacity caused each of these systems to require a full restart

- While the subsystems were restarted, S3 was unable to service requests

- Other AWS services in the US-EAST-1 Region that rely on S3 for storage, including the S3 console, EC2, EBS, and Lambda were impacted



# What Concepts Are Illustrated?

- Accidental threat
  - Someone made a mistake hurting the system
- Employee Risk Management
  - Maintaining a trained staff with up-to-date skills
- Operational Risk
  - Internal failure from internal processes and people



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# When Risk Management Fails?

## RISK MANAGEMENT FOR MANAGERS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# What Can You Do With Risk?

## RISK MANAGEMENT FOR MANAGERS

# Management's Responsibility

Cybersecurity and IT managers minimize risk to the organization by choosing the appropriate controls


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# What Can You Do With Risk?

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Risk Mitigation

Risk Transference

Risk Avoidance

Risk Acceptance

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# What Can You Do With Risk?

## RISK MANAGEMENT FOR MANAGERS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Risk Mitigation

## RISK MANAGEMENT FOR MANAGERS

# Risk Mitigation

- Main goal of security is to minimize risk to an acceptable level
- Our goal is not necessarily to eliminate all risks…
- By adding risk controls, we can mitigate the risk down to an acceptable level



# Risk Mitigation

Main goal of security is to minimize risk to an acceptable level

# Risk Mitigation

Our goal is not necessarily to eliminate all risks…



# Risk Mitigation

By adding risk controls, we can mitigate the risk to an acceptable level



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Risk Mitigation

## RISK MANAGEMENT FOR MANAGERS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Risk Transference

## RISK MANAGEMENT FOR MANAGERS

# Risk Transference

- If the organization cannot afford to accept, avoid, or mitigate the risk, they can transfer the risk to another business

Example:

- If the organization is concerned that it would be too costly to recover from a flood, they can purchase flood insurance



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Risk Transference

## RISK MANAGEMENT FOR MANAGERS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Risk Avoidance

## RISK MANAGEMENT FOR MANAGERS

# Risk Avoidance

- Risk is too high to accept, so the system configuration or design is changed to avoid the risk associated with a specific vulnerability

Example:

- Utilizing Windows XP is too dangerous, so we install Windows 10 instead to avoid the risk of an unsupported operating system



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Risk Avoidance

## RISK MANAGEMENT FOR MANAGERS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Risk Acceptance

## RISK MANAGEMENT FOR MANAGERS

# Risk Acceptance

- Organization accepts the risk associated with a system's vulnerabilities and their associated risks

- Risk acceptance is common when the risk is low enough to not apply countermeasures, or adequate countermeasures have already been applied



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Risk Acceptance

## RISK MANAGEMENT FOR MANAGERS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Risk Controls

## RISK MANAGEMENT FOR MANAGERS

# Risk Controls

- Technical controls
- Operational controls



# Technical Controls

- Systems, devices, software, and settings used to enforce CIA requirements

- Examples
  - Using firewalls, IDS, and IPS
  - Installing antivirus and endpoint security



# Operational Controls

- Practices and procedures to increase security

- Examples
  - Conducting penetration tests
  - Utilizing standard operating procedures



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Risk Controls

## RISK MANAGEMENT FOR MANAGERS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Calculating Risk

## RISK MANAGEMENT FOR MANAGERS

# Calculating Risk

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Senior executives are always looking to compare on risk against another in order to make the best resourcing decisions
- Should I fix this vulnerability or those multiple vulnerabilities?
- We need to have a way to compare…

# Apples & Oranges

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

# Measuring Risk

Qualitative is subjective

Quantitative is countable

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Calculating Risk

## RISK MANAGEMENT FOR MANAGERS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Qualitative Risk Measurement

## RISK MANAGEMENT FOR MANAGERS

# Qualitative Risk

- Used when there isn't any precise values
- Measures the probability of occurrence and the impact if it occurred
- Subjective in nature
- Most commonly used with a risk matrix



# Qualitative Example

| PROBABILITY \ IMPACT | Low | Medium | High |
|---|---|---|---|
| High | Medium | High | High |
| Medium | Low | Medium | High |
| Low | Low | Low | Medium |



# Qualitative Risk Example

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Considering allowing a BYOD policy
- You will save $$$ on buying devices
- But, inherit the risk of employee devices
- What is the risk associated with a cyber attack caused by your BYOD policy?

# Qualitative Example

| PROBABILITY \ IMPACT | Low | Medium | High |
|---|---|---|---|
| High | Medium | High | High |
| Medium | Low | Medium | High |
| Low | Low | Low | Medium |



# Qualitative Risk Example

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- You purchased data breach insurance
- Insurance transfers risk of loss
- But, can't transfer the negative affects to your reputation if a breach occurs…
- What is the risk to your reputation if a data breach occurred?

# Qualitative Example

| PROBABILITY | Low | Medium | High |
|---|---|---|---|
| High | Medium | High | High |
| Medium | Low | Medium | High |
| Low | Low | Low | Medium |

IMPACT



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Quantitative Risk Measurement

## RISK MANAGEMENT FOR MANAGERS

# Quantitative

- Seeks to numerically assess the risk
- Known as Probabilistic Risk Analysis
- Measures the probability of occurrence and the impact if it occurred
- Describes the consequences in dollars, time, lives lost, or other metrics



# Single Loss Expectancy

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

**SLE =**
**Asset Value X Exposure Factor**

- Exposure Factor (EF) is the percentage of an asset lost during an event
- EF is 1.0 is the asset loses all value

# Annual Loss Expectancy

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Common calculation to determine the cost associated with a particular risk

- Used by executives in determining when to mitigate, transfer, avoid, or accept the risk

**ALE = Cost X Occurrences**

**If a risk would be actualized 3 times a year, then Occurrences equals 3.0.**
**If a risk would be actualized once ever 3 years, then Occurrences equals 0.33.**

# Quantitative Example

- Assume that an organization will suffer one (1) data breach every three (3) years
- Chief Security Officer suggests budgeting $524k annual to provides data security protections
- Each breach is estimated to cost your organization $103k
- Should you authorize the budget?



# Annual Loss Expectancy

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

## ALE = SLE X Occurrences

**Assuming a data breach occurs once every three years and costs the company $103k each time…**

**...Does it make sense to spend $524k to mitigate this risk?**

# Annual Loss Expectancy

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

**ALE = SLE X Occurrences**

**ALE = $103k X 0.33**

**Assuming a data breach occurs once every three years and costs the company $103k each time…**

**...Does it make sense to spend $524k to mitigate this risk?**

# Annual Loss Expectancy

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

**ALE = SLE X Occurrences**

**ALE = $103k X 0.33**

**ALE = $34k**

**Assuming a data breach occurs once every three years and costs the company $103k each time…**

**...Does it make sense to spend $524k to mitigate this risk?**

# Annual Loss Expectancy

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

**ALE = SLE X Occurrences**

**ALE = $103k X 0.33**

**ALE = $34k**

15+ Years @ $34k to equal $524k

**Assuming a data breach occurs once every three years and costs the company $103k each time…**

**...Does it make sense to spend $524k to mitigate this risk?**

# Quantitative Example

- Assume that an organization will suffer three (3) data breach every year
- Chief Security Officer suggests budgeting $214k annual to provides data security protections
- Each breach is estimated to cost your organization $103k
- Should you authorize the budget?



# Annual Loss Expectancy

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

**ALE = SLE X Occurrences**

**Assuming a data breach occurs three times every year and costs the company $103k each time…**

**...Does it make sense to spend $214k to mitigate this risk?**

# Annual Loss Expectancy

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

**ALE = SLE X Occurrences**

**ALE = $103k X 3.0**

**Assuming a data breach occurs three times every year and costs the company $103k each time…**

**...Does it make sense to spend $214k to mitigate this risk?**

# Annual Loss Expectancy

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

**ALE = SLE X Occurrences**

**ALE = $103k X 3.0**

**ALE = $309k**

**Assuming a data breach occurs three times every year and costs the company $103k each time…**

**...Does it make sense to spend $214k to mitigate this risk?**

# Annual Loss Expectancy

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

**ALE = SLE X Occurrences**

**ALE = $103k X 3.0**

**ALE = $309k**

8+ months @ $103k to equal $214k

**Assuming a data breach occurs three times every year and costs the company $103k each time…**

**...Does it make sense to spend $214k to mitigate this risk?**

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Case Study (Equifax)

## RISK MANAGEMENT FOR MANAGERS

# Equifax Data Breach

- 145 million Equifax customers affected
- Data breach occurred in July 2017
- Attackers used a vulnerability in Apache Struts

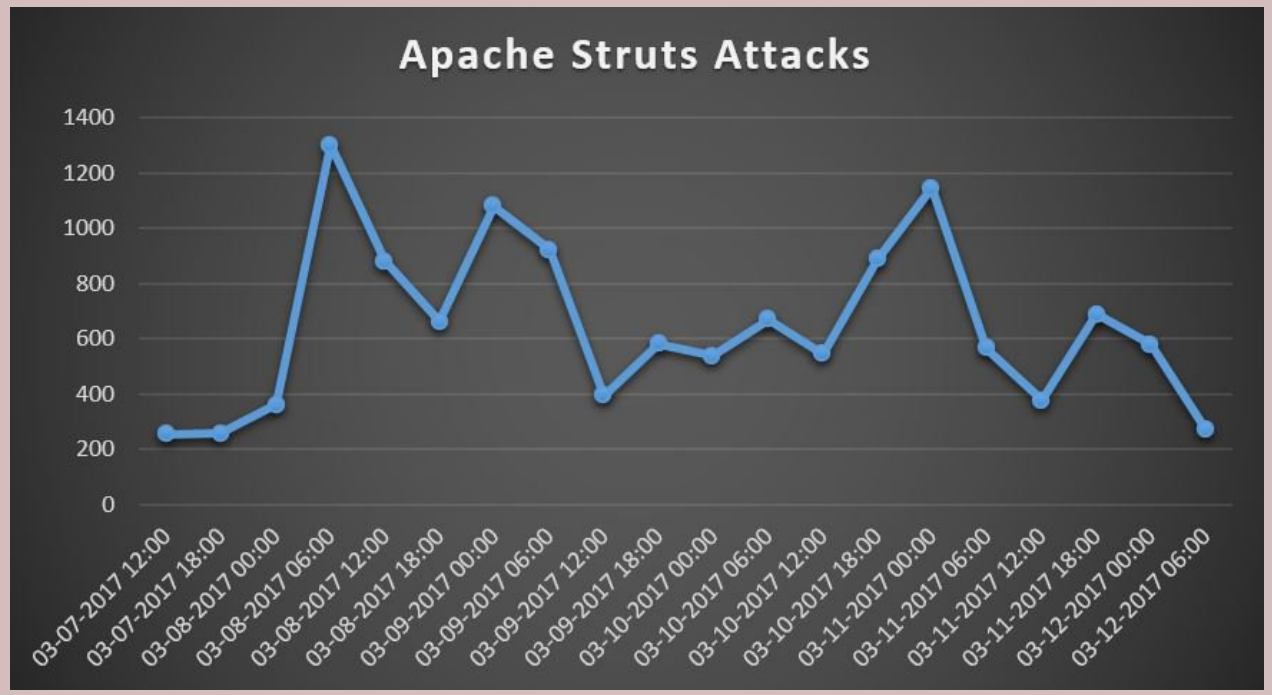
Struts

# CVE-2017-5638 (Release 3/6/17)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Apache Struts 2 framework vulnerability

- Over the first 6 days of the vulnerability being discovered, thousands of attacks



# How to Mitigate Vulnerability?

- Upgrade Apache Struts to either version 2.3.32 or 2.5.10.1, or a different multipart parser

- Requires rewriting, retesting, and redeploying their code

- Assumed cost:
  $3.5 million (man-hours & downtime)



# What's At Risk?

- Social Security Numbers
- Date of Birth
- Names
- Addresses

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# How Much Is Security Worth?


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# In FY17-Q3, Equifax spent...

- Security Products ($55.5 million)
- Consulting Fee ($17.1 million)
- Consumer Support ($14.9 million)
- Estimate additional costs still coming ($56 million to $110 million)



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

# Conclusion

## RISK MANAGEMENT FOR MANAGERS

# What did this class cover?

- What is risk?
- What happens when risk management fails?
- What can you do with risk?
- How do you calculate risk?

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE