# Risk Management and Threat Modeling

Cybersecurity

GRC Day 2

# Class Objectives

By the end of today's class, you will be able to:

Identify threat agents, possible attacks, and exploitable vulnerabilities relevant to a given asset.

Prioritize risks based on likelihood and impact potential.

Choose and justify controls for a given risk.

Today’s class will introduce risk management and threat modeling as methods for identifying, anticipating, budgeting, and planning for when risks occur.

These tools will allow us to:

| Enumerate | Identify | Evaluate | Develop |
| --- | --- | --- | --- |
| possible risks, threats, and vulnerabilities to a company. | the most likely and most serious risks. | the impact that the occurrence of a serious risk may have. | strategies for monitoring or mitigating. |

# Threat Modeling and Risk Management


What’s the difference
between a vulnerability,
a threat, and a risk?

A **vulnerability** is an aspect of a business that can be exploited to compromise a system’s CIA.

A **threat** is an actor that might exploit a vulnerability.

A **risk** is the possibility of losing something valuable.

# Risk Management And Threat Modeling

| | |
|---|---|
| **Risk analysis** | Understanding what risks face an organization, which are most severe, and which are most likely. |
| **Risk management** | Using the results of risk analysis to create a plan for preventing likely risks. |
| **Threat modeling** | Determining which attacks an organization is most likely to experience, who is most likely to launch them, and what actions can be done to prevent them. |

# Risk Management And Threat Modeling

## What is a business's primary objective? **Profit!**

- Risk analysis, risk management, and threat modeling directly contribute to business profit.
- Risk analysis helps business understand how much they'll need to spend if a given security break happens.
- When possible, risks are measured quantitatively in financial figures, which businesses use to prioritize threats.
- Threat modeling results are shared upwards to the executives who make the major business decisions.

# Risk Management And Threat Modeling

These practices directly relate to a business's pursuit of profit:

## Risk analysis

is important because it quantifies how much a business needs to spend if a given security break happens.

**Therefore, businesses can plan for setbacks before they occur.**

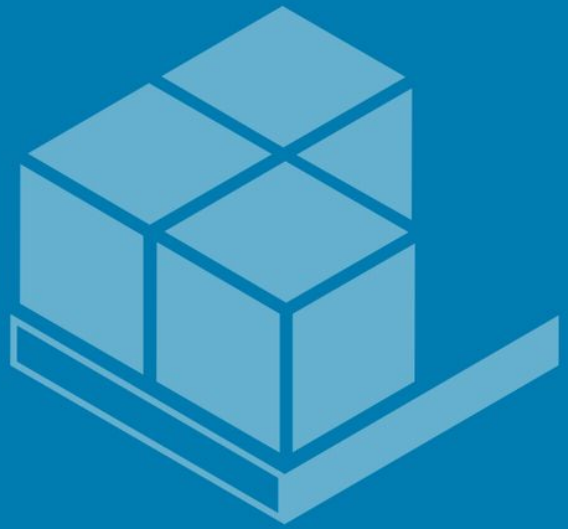
## Threat modeling

is a key step to risk management because a risk is essentially a price the business pays if the threat happens.

**Therefore, they can prioritize the most expensive risks.**

# Threat Modeling Methodology: PASTA

## **PASTA**: **P**rocess for **A**ttack **S**imulation & **T**hreat **A**nalysis



PASTA focuses on aligning considerations of **business objectives** with **technical requirements**.

# Threat Modeling Methodology: STRIDE

**STRIDE**: **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**oS (Denial of Service), **E**levation of Privilege

STRIDE focuses on identifying **what can fail** in the system being modeled.

# Threat Modeling Methodology: OWASP

Today we'll focus on OWASP:

**O**pen **W**eb **A**pplication **S**ecurity **P**roject

OWASP focuses on **identifying possible threats**, **prioritizing risks**, and **planning mitigation strategies**. It is mainly used with web and desktop applications.

# OWASP

The **OWASP Threat Modeling process** consists of six steps.

1. Determine assessment scope.
2. Identify threat agents.
3. Identify potential attacks.
4. Identify exploitable vulnerabilities.
5. Prioritize identified risks.
6. Mitigate risks.

Step 1
**Determine Scope**

## List the assets under consideration, determine their value, and define objectives for your threat modeling assessment.

- Businesses can't effectively evaluate everything at once, so they adjust their scope to focus on a specific category of risk.

  **Example:** Performing a risk analysis to assess the weakness of a network infrastructure. Within this scope, we are not concerned with application security.

- Scoping begins with **asset inventory**, the process of identifying and assigning asset value to all of an organization's assets.

  **Example:** The asset value of a web application could be measured by the revenue or profit it generates.

Step 2
**Identify Threat Agents**

## Determine which attackers would be interested in the relevant assets.

**Threat agents** include a person or group that can produce a threat, whether or not that person or group is malicious.

Threat agents include:

- APTs (Advanced Persistent Threats)
- Script kiddies
- Employees opening phishing emails
- Incompetent users breaking configurations on company computers

Today, we'll focus on *malicious* threat agents.

Previously, we've addressed *unwitting* threat agents, like employees opening phishing emails.

Step 3
**Identify Potential Attacks**

## Identify the attacks each agent is likely to perform.

- Different attackers use different modes of attacks. Different attacks mean different risks and different considerations.

  **Example:** Script kiddies will have different goals than disgruntled employees.

- We can identify a potential attack by considering the threat agent's:
  - Motivation
  - Skill level
  - Amount of funding

  **Example:** If a client's web application is taken offline by a DoS attack, the severity of the risk depends on which threat agent is responsible.
  - Script kiddies might DoS a server simply to cause trouble.
  - An APT might DoS a server as a smoke screen to steal valuable data.

Step 4

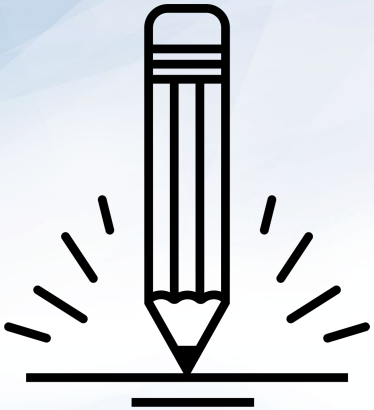
# Identify Exploitable Vulnerabilities

**Identify the most vulnerable points in a system, how the agent will deliver the attack, and where an attack is most likely to occur.**

- Once we determine who might attack and what methods they might use, we determine where exactly in the system they will likely direct their attacks, and what the risk will be if they do.

**Example**: If a network has only one database that stores everything, the entire company will lose access to all data if it is compromised.

An attacker seeking to DoS the company's network can exploit this database to achieve their goal.



# **Activity:** Threat Modeling: Steps 1-4

In this activity, you'll learn more about GeldCorp's business operations and assets before applying steps 1-4 of the OWASP process.

**Suggested Time:**
25 Minutes

# **Time’s Up!** Let’s Review.

# Risk Analysis

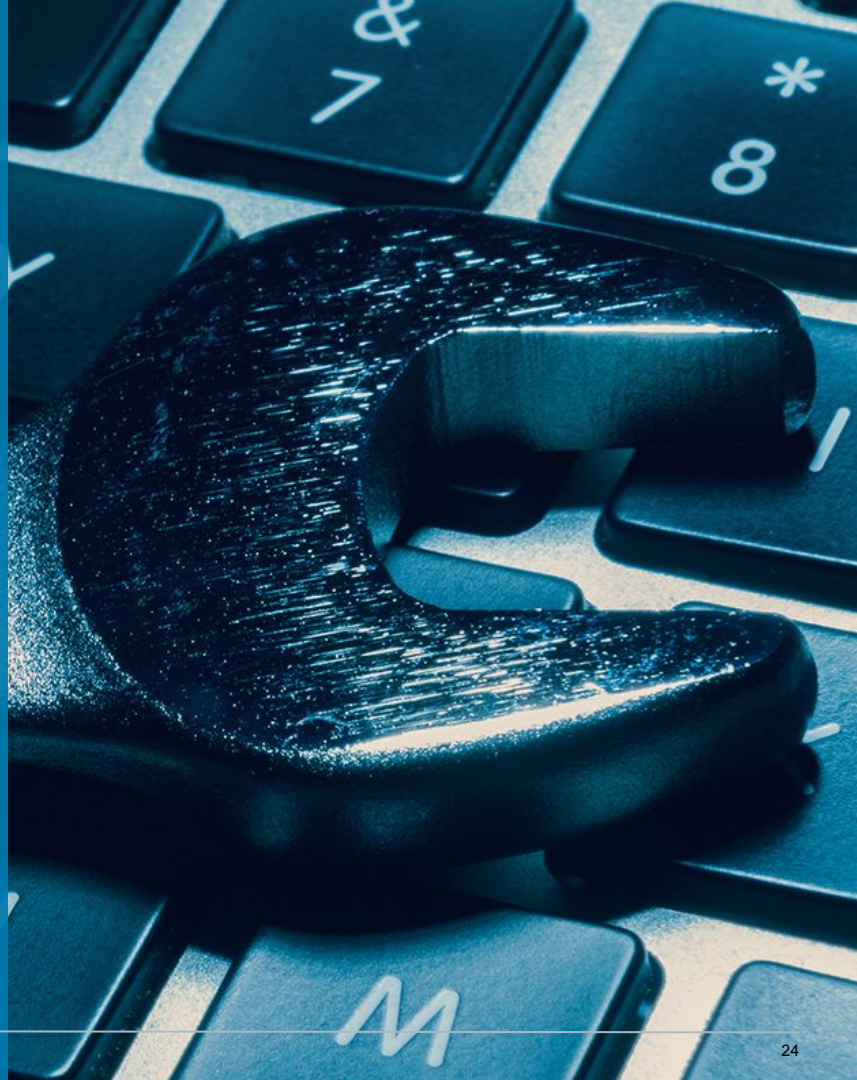
In this section, we will focus on risk analysis and walk through the process of prioritizing **possibilities of attack**.

# Risk Analysis

**Risk analysis** is the process of prioritizing threats identified in Steps 1-4 based on their potential impact and likelihood.

Some threats are more likely than others:

- **Script kiddies** are likely to be responsible for most of the attacks an organization experiences, simply because there are so many of them.
- For most organizations, organized **cyber criminals** aren't a major threat actor. They are more relevant to financial organizations, branches of government, and military targets.



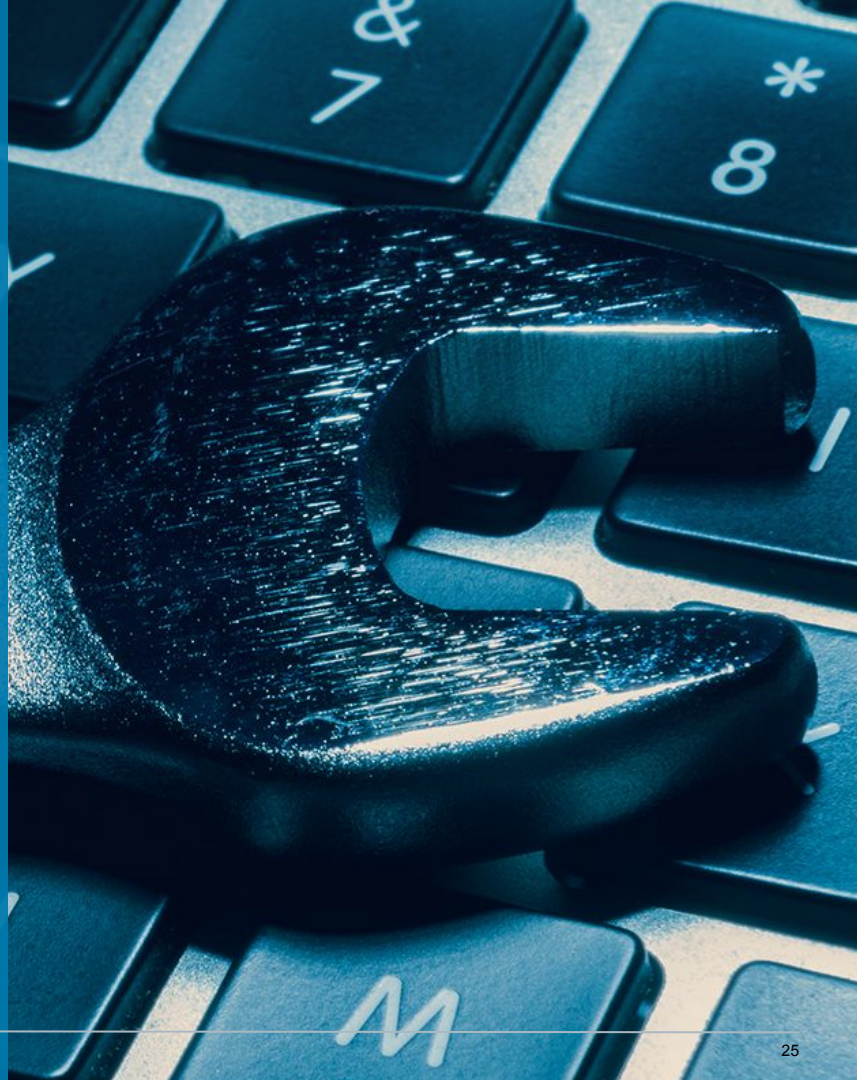
# Risk Analysis

## Scenario

You've identified more than 10 potential attacks that GeldCorp should consider. All can be mitigated, but each fix costs around $2.5k. GeldCorp's Security department only has $10k budgeted for the project. You must advise on which four fixes should be prioritized.

Before completing this activity, we'll learn about:

- Qualitative vs. quantitative risk analysis
- Likelihood, impact, and loss expectancies
- Risk factor and heat maps




- Evaluating risk based on intangible, unmeasurable factors.
- Used when decisions do not require cost-benefit analysis.

- Evaluating each risk based on its measured likelihood and impact.
  - **Likelihood**: The probability an event will take place.
  - **Impact**: The measure of damage done if a risk takes place.

# Qualitative Risk Analysis


**In some situations, likelihood and impact cannot be accurately measured.**

- **Example 1:** It's impossible to calculate the precise probability that some hacker, somewhere in the world, will attack your servers within the next year.
- **Example 2:** It's impossible to know the precise impact of a breach. The cost of an attack will depend on its length, which is impossible to determine ahead of time.

# Qualitative Risk Analysis

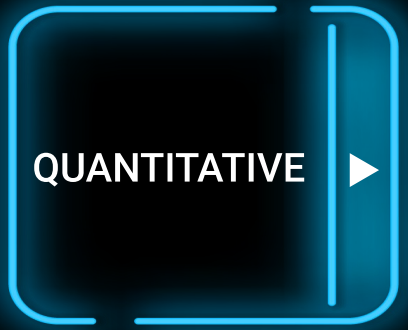
- **Used when a complex evaluation of cost vs. benefit is unnecessary.**

  **Example**: When a company is deciding between an inexpensive VPN service that logs traffic on its servers for internal use, and a more expensive service that does not keep any logs.


A **bakery** can use qualitative analysis to decide on an inexpensive VPN, since it shouldn't matter much if they're logging non-confidential information.


A **government defense** or **financial organization** can use qualitative analysis to decide on a more expensive service, since it knows it needs to keep its data confidential.

# Quantitative Risk Analysis: Example 1

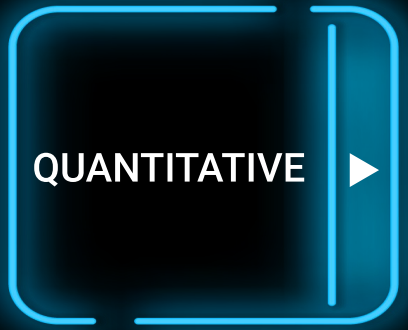



**However, there are circumstances where intuitive analysis is insufficient.**

- **Example:** The Security department wants to invest in protecting the organization's infrastructure.

  To secure the money from the Finance department, they must justify their ask. They will present a quantitative risk analysis to demonstrate that the cost of not investing is much greater than the budget they're requesting.

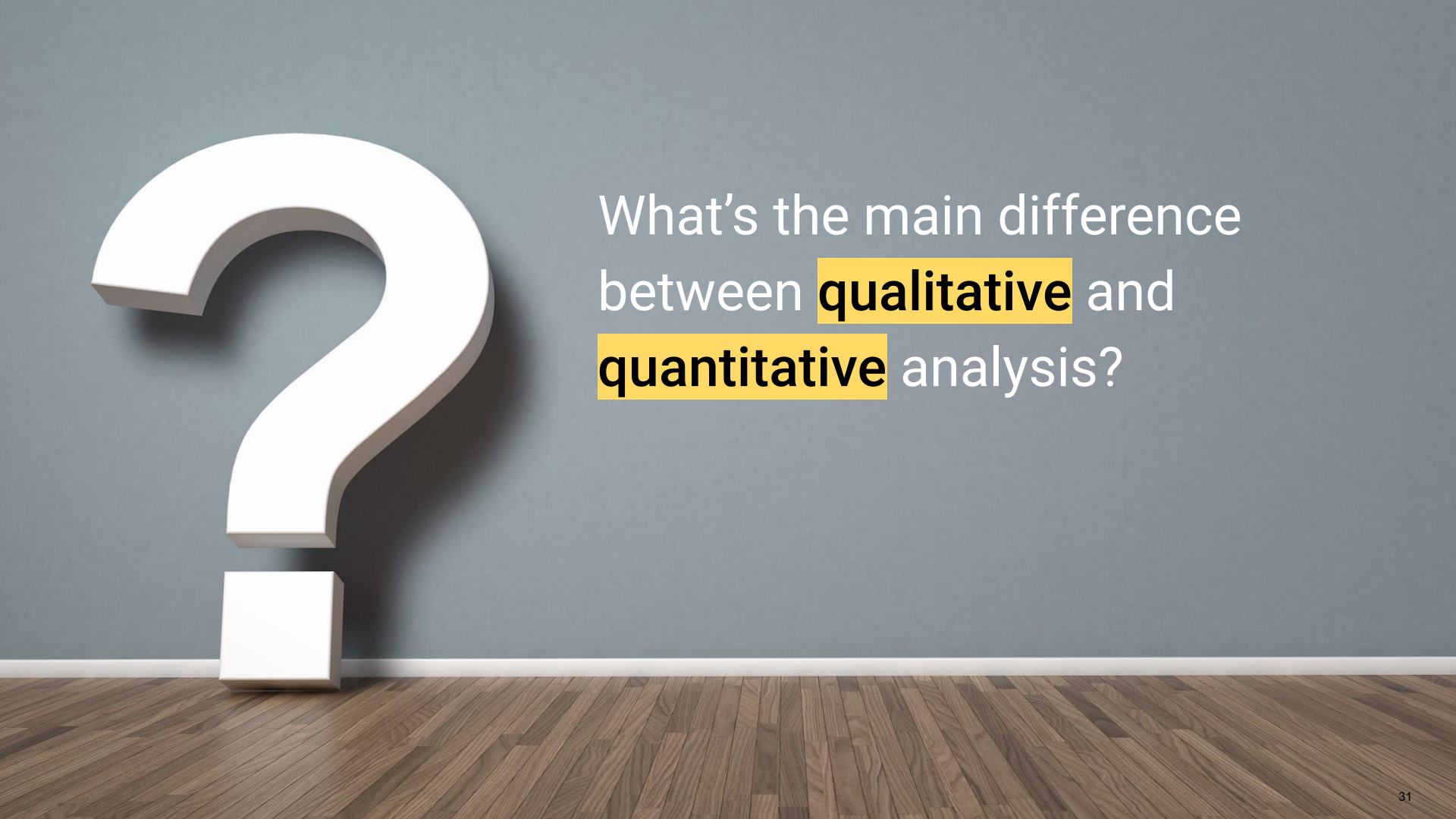
# Quantitative Risk Analysis: Example 2

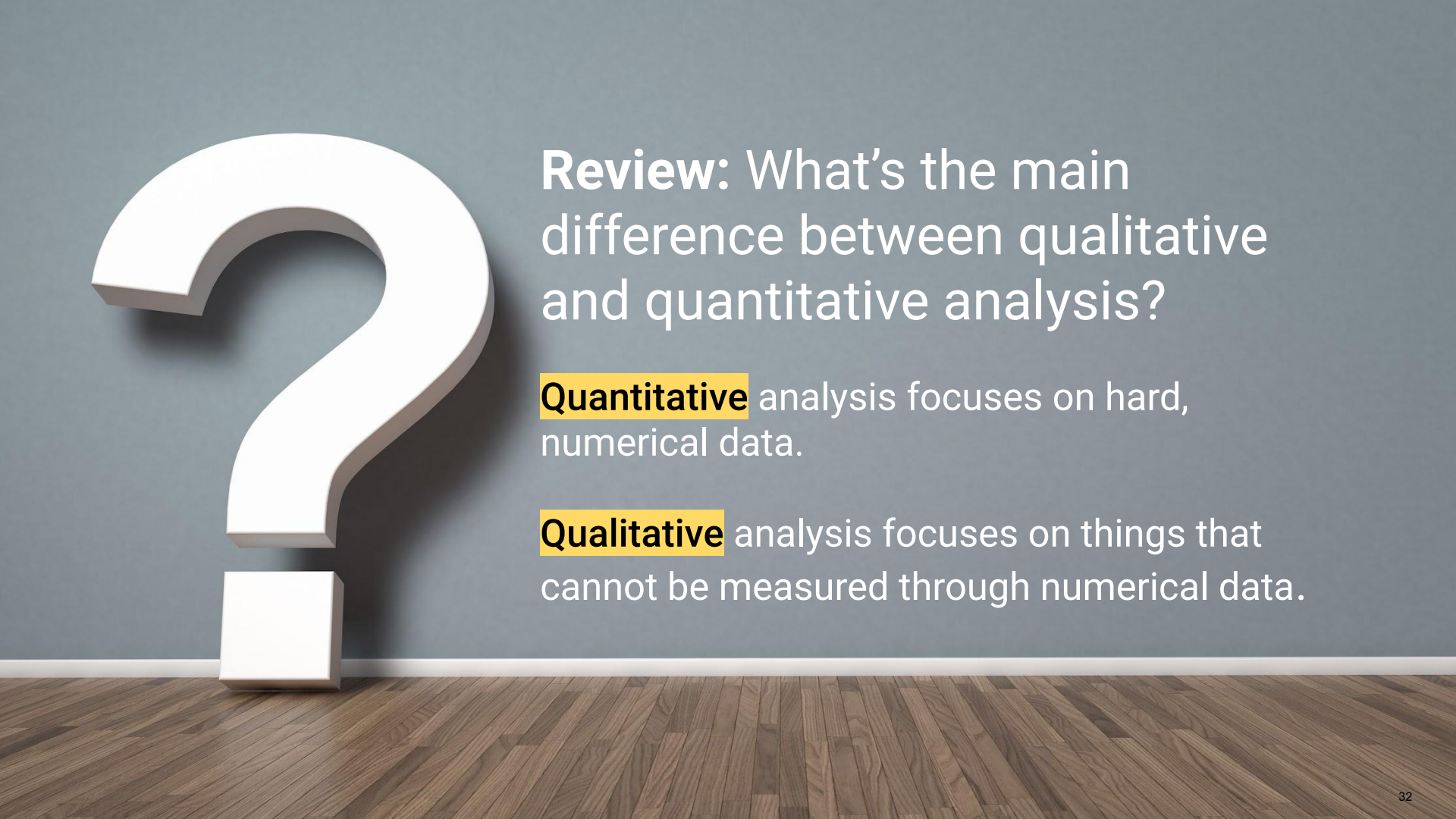



**However, there are circumstances where intuitive analysis is insufficient.**

- **Example:** The Executive team must decide whether to migrate to a new cloud provider as part of negotiations with a potential partner.

  This transition has major financial implications. To make the decision, they need an accurate assessment of potential losses due to downtime, retraining, risk of data corruption during migration, and other issues.


What’s the main difference between qualitative and quantitative analysis?



**Review:** What's the main difference between qualitative and quantitative analysis?

**Quantitative** analysis focuses on hard, numerical data.

**Qualitative** analysis focuses on things that cannot be measured through numerical data.

# Asset Value and Exposure Factor

To perform quantitative risk analysis, analysts start by calculating how much it will cost if an asset is breached.

- Analysts first quantify **asset value** and **exposure factor**.
- **Asset value** is how much money an asset is worth in currency.
- **Exposure factor** is how much of an asset will be affected in a breach.
- In other words, whether an attack will result in **partial and temporary** or **complete and permanent** destruction of an asset.

# Determining Exposure Factor

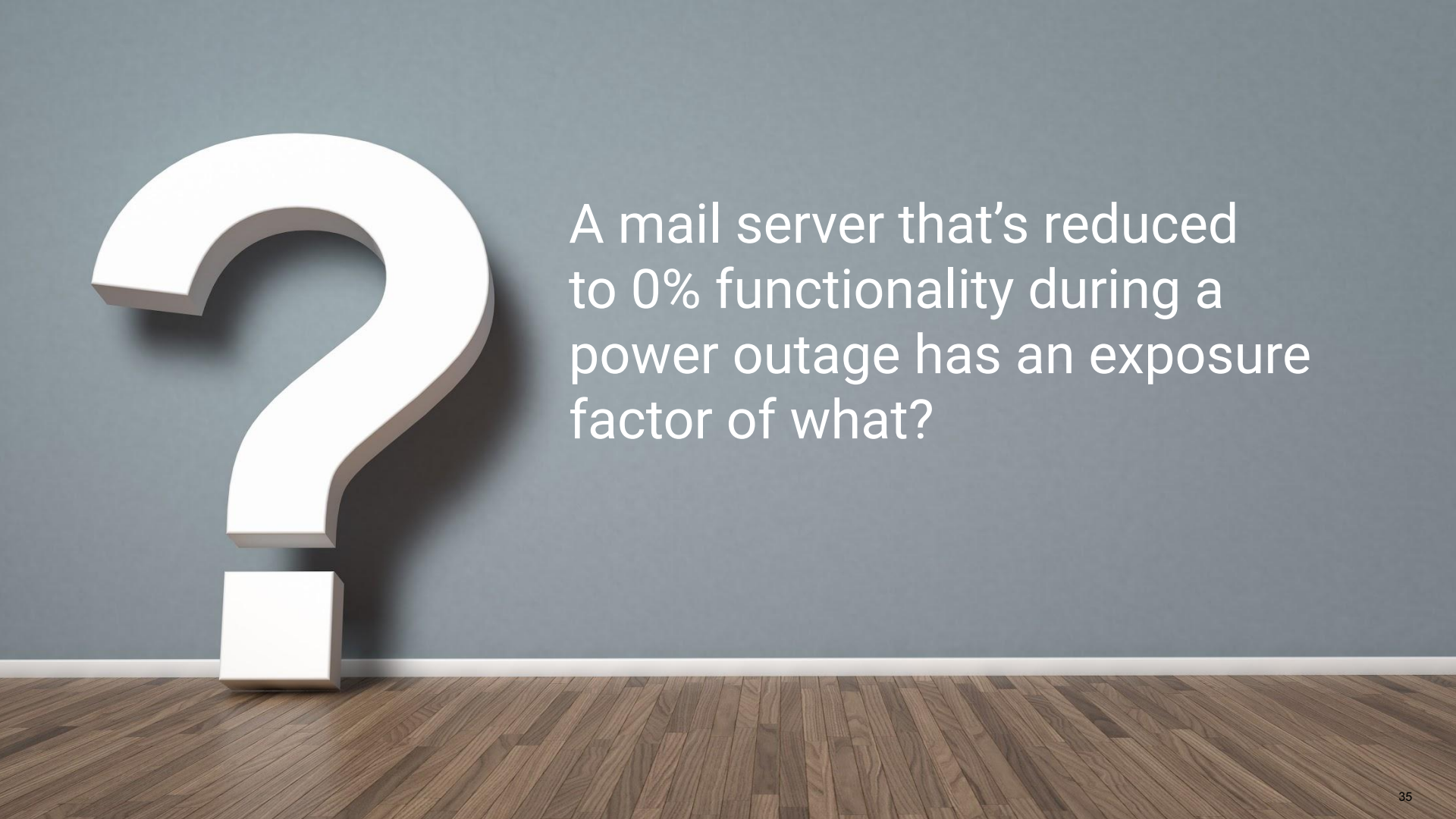
Exposure factor is always somewhat subjective. We apply a numerical value for the level of damage an exploited risk would produce.

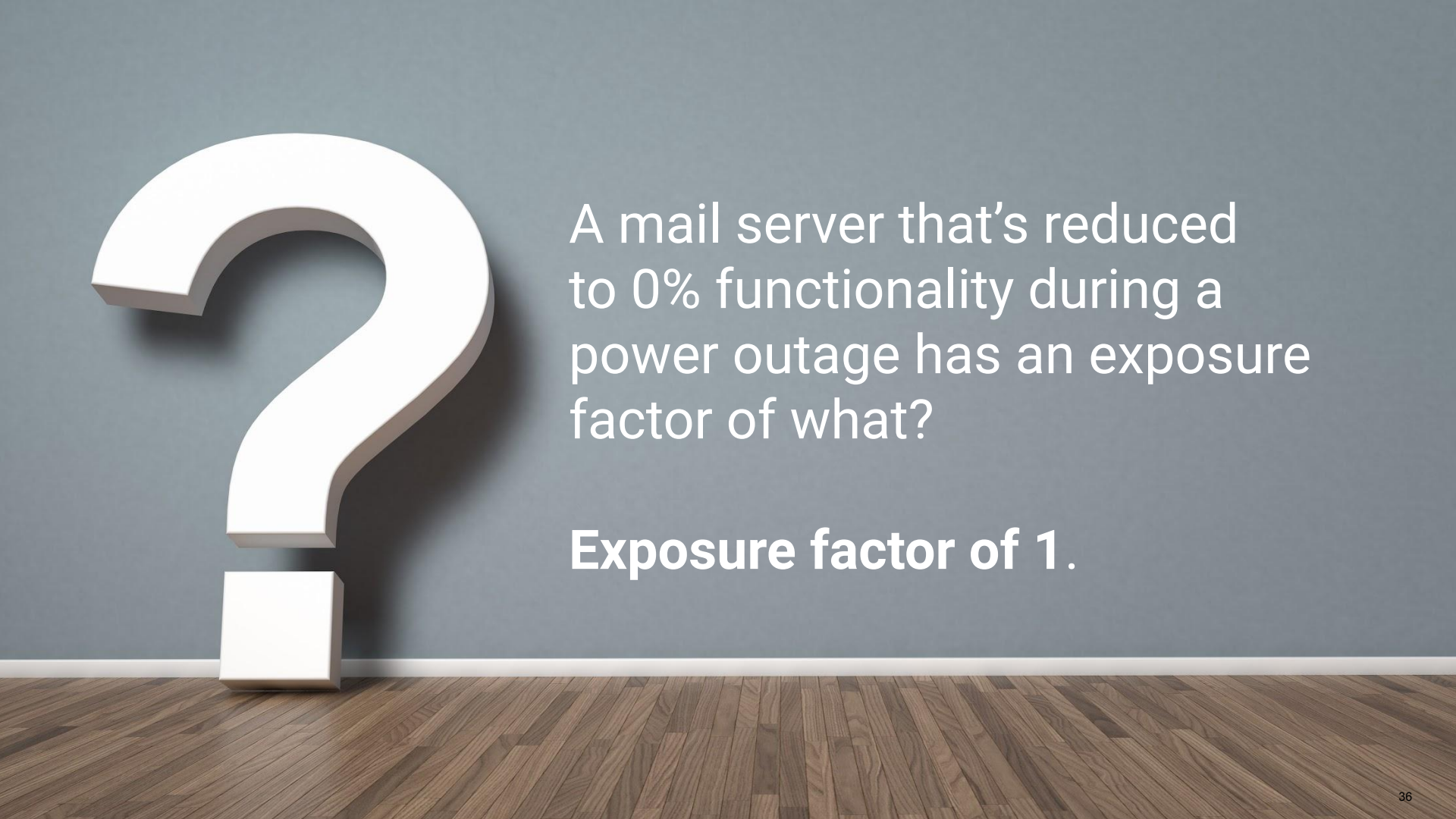

Attack would **completely eliminate** an asset.


Attack would **mostly eliminate** an asset.


Attack would **half eliminate** an asset.


Attack would **partially eliminate** an asset.


A mail server that’s reduced to 0% functionality during a power outage has an exposure factor of what?



A mail server that's reduced to 0% functionality during a power outage has an exposure factor of what?

**Exposure factor of 1**.

# Loss Expectancy

The measure of how much money an organization will lose in the event of a given breach.

**Single Loss Expectancy (SLE)**
Estimated cost of the risk occurring on a given asset.

**SLE = AVE × EF**

AV = Asset Value
EF = Exposure Factor

**Annual Rate of Occurrence (ARO)**
Estimated number of times the risk is likely to occur in a given year.

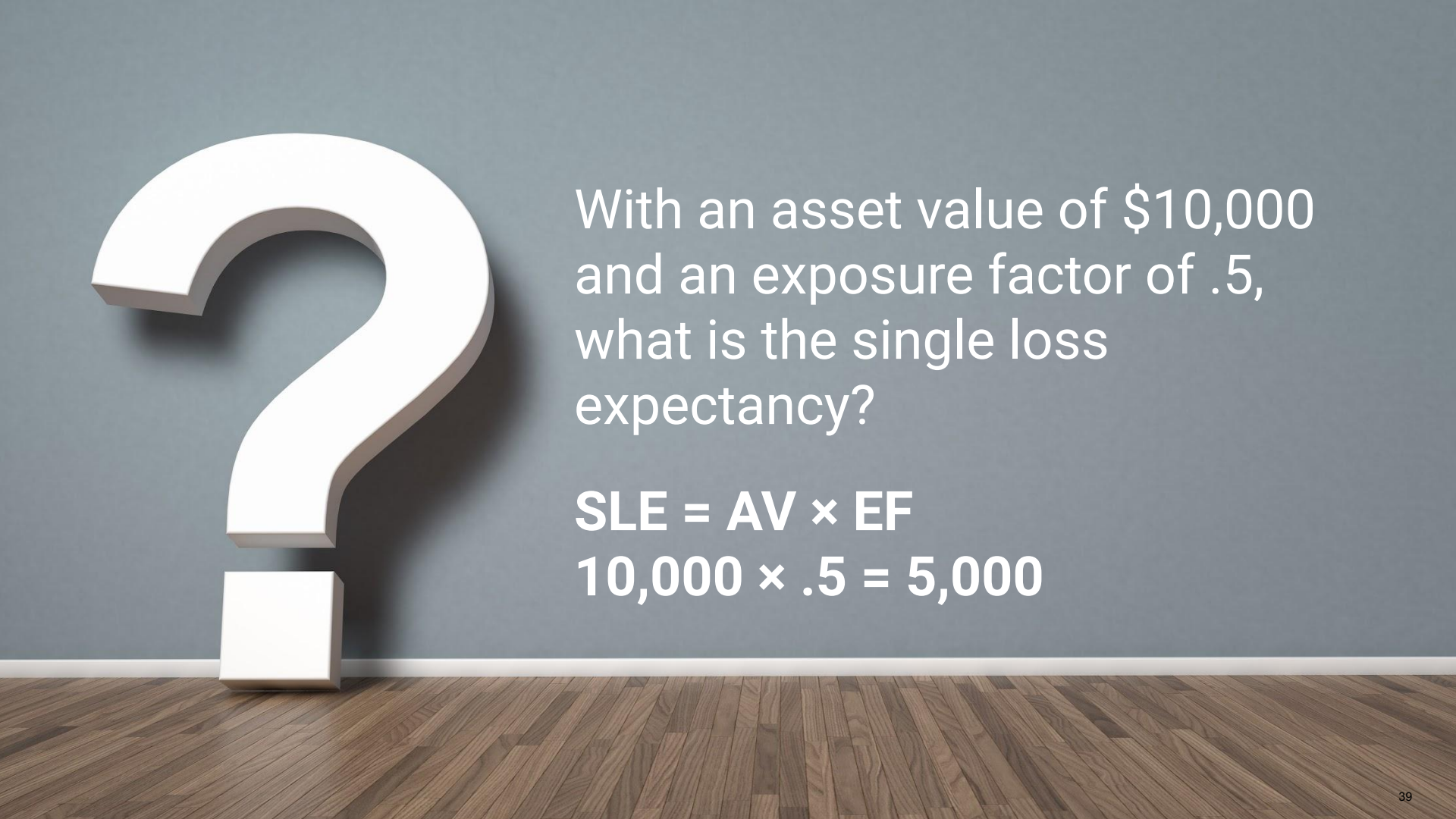
**ARO = X / years**

X = number of occurrences

**Annual Loss Expectancy (ALE)**
Estimated cost of a risk occurring in a given year.

**ALE = SLE × ARO**

With an asset value of $10,000 and an exposure factor of .5, what is the single loss expectancy?



With an asset value of $10,000 and an exposure factor of .5, what is the single loss expectancy?

**SLE = AV × EF**
**10,000 × .5 = 5,000**

# Loss Expectancy

Categories of loss expectancy refer to the degree of a breach's impact.

| Marginal | Notable | Severe | Catastrophic |
| --- | --- | --- | --- |
| The organization has the resources to respond to the breach immediately, without affecting day-to-day operations or revenue. | The organization has the resources to respond to the breach, but may not be able to do so immediately.<br><br>May experience interruptions to operations. | The organization experiences serious interruptions to operations, and doesn't have the monetary and/or personnel resources to respond effectively.<br><br>May have to defer revenue, delay project timelines, reassign employees, or hire consultants to fix the issue. | The organization suffers severe, lasting damage to its reputation and/or infrastructure.<br><br>The future of the business is threatened by reputational damage, bankruptcy, being found in contempt of federal regulations, or other issues. |

In the next demonstration, we'll see data presented in a spreadsheet and visual formats known as **risk matrices** and **heat maps**.

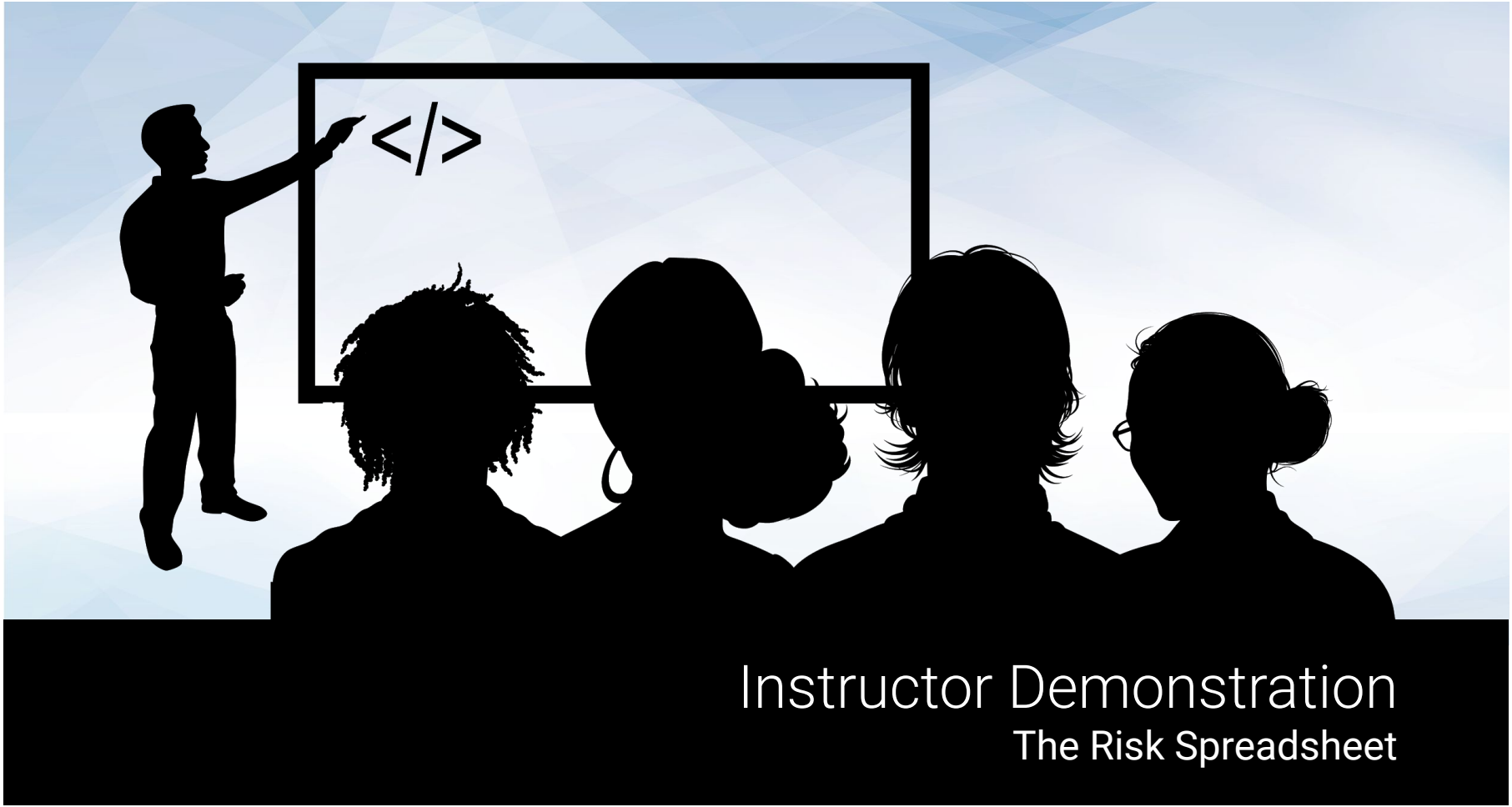
# Risk Matrices and Heat Maps

During a risk assessment, we visualize risks to get a holistic view of risks affecting an organization.

A **risk matrix** is used to compare how many of the risks facing an organization are mild and how many are severe.

A **heat map** is a visual representation of the probability and likelihood of risks. Organizations can use heat maps to make strategic decisions about how to protect the company.

| | | 10<br>Low | 20<br>Medium | 30<br>High | 40<br>Very High |
|---|---|---|---|---|---|
| 10 | Low | 1 | 0 | 0 | 0 |
| 20 | Medium | 2 | 0 | 0 | 0 |
| 30 | High | 2 | 1 | 0 | 1 |
| 40 | Very High | 1 | 0 | 0 | 1 |



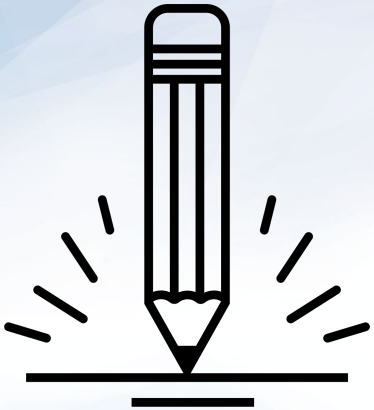

# Instructor Demonstration

## The Risk Spreadsheet


Countdown timer

15:00

(with alarm)



# **Activity:** Threat Modeling Step 5 - Risk Analysis

In this activity, you will complete a spreadsheet and generate a risk matrix and heat map for GeldCorp.

**Suggested Time:**
30 Minutes

# **Time’s Up!** Let’s Review.

# Mitigating Risks

Now that we’re able to determine which threats are worth our attention and resources, we can craft controls for mitigating risks.

# Deciding on Security Controls

Answer the following questions when determining an appropriate control.

**Required control type:** Should the control be physical, administrative, or technical?

**Required strength of control:** How strong does the control *really* need to be?

**Cost of implementation:** How much does the control cost compared to the benefit provided?

**Time of implementation:** How long will the control take to implement?

# Risk Mitigation: Example

**LifeNotes is a new medical records company that makes it easy for doctors from different hospitals to share medical records.**

When transferring a patient to another hospital or physician, they can use the application to share the patient's medical history, lab results, and medication schedules.

LifeNotes also ensures that doctors can only see records for their own patients.

However, a client recently reported that they were able to load records for patients they were not assigned to.

This violates regulatory standards protecting patient medical information, and must be resolved immediately.

# Risk Mitigation: Example

What security controls should we suggest to LifeNotes?

- Required control type?
- Required control strength?
- Control decisions?
- Cost of implementation?
- Time of implementation?

# Risk Mitigation: Example


Since this problem must be fixed immediately, LifeNotes must implement a corrective control.

They should also implement protective controls to prevent the issue from recurring. This can be accomplished with administrative or technical controls.

# Risk Mitigation: Example


The corrective control must completely resolve the issue, since the bug means LifeNotes is in violation of the law.

The protective control(s) must completely prevent this issue from recurring, for the same reason.

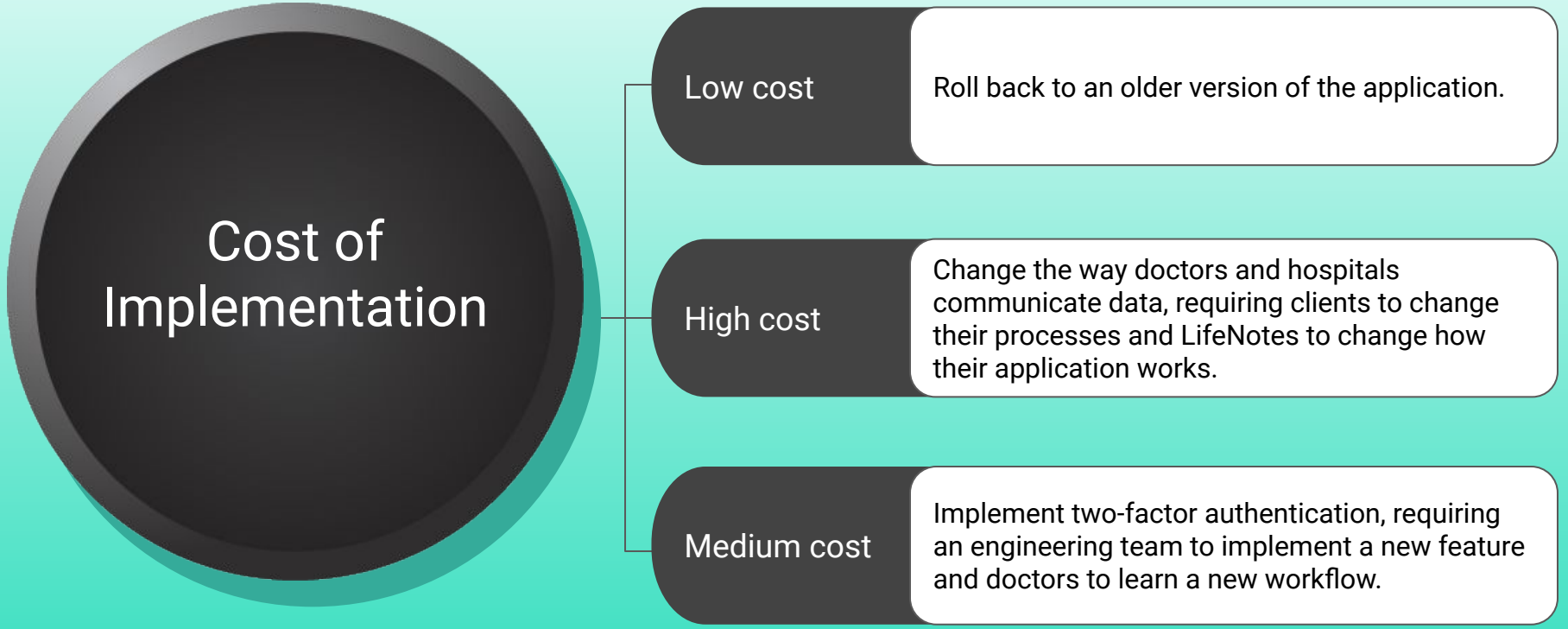
# Risk Mitigation: Example

LifeNotes can implement the following example controls:

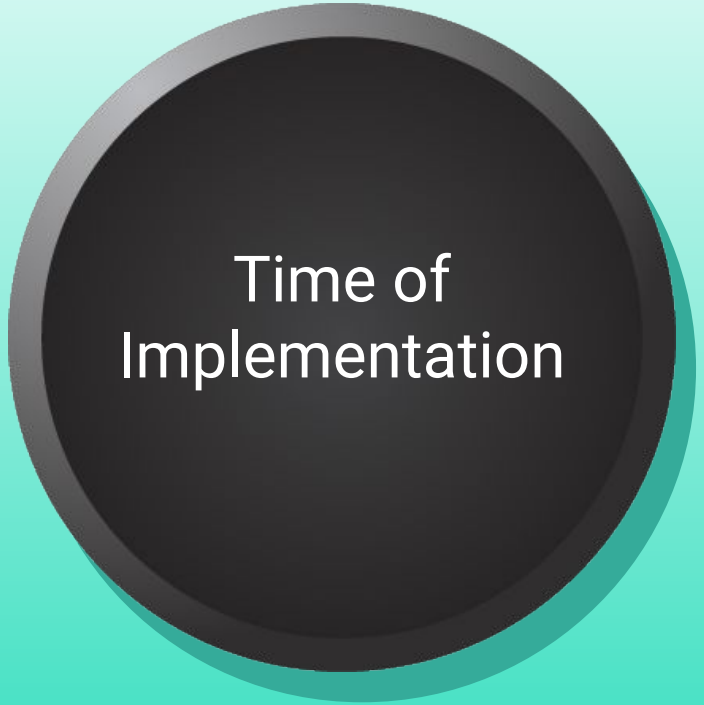

| | |
|---|---|
| Corrective control | Redeploy the older version of the application, which did not have this issue. |
| Administrative preventive control | Require doctors to transfer records to the target hospital, and then have the hospital pass those records to the specific doctor who needs them. |
| Technical preventive control | Require doctors to provide a password to log in, and provide their Employee ID to load specific patients' records (two-factor authentication). |

# Risk Mitigation: Example

LifeNotes can implement the following example controls:



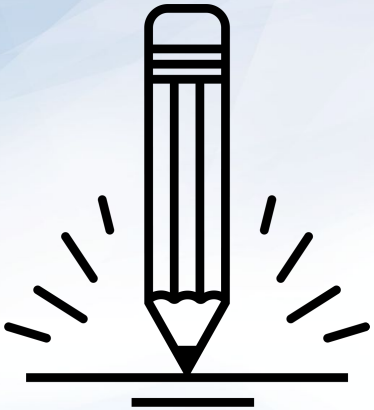
# Risk Mitigation: Example




Rolling back to an older version of the application should take less than a day.

Administrative controls would take months to implement.

Implementing two-factor authentication would likely take approximately one quarter (three months).



# **Activity:** Threat Modeling Step 6 – Risk Mitigation

You will conceptualize a risk mitigation plan.

**Suggested Time:**
15 Minutes

# **Time’s Up!** Let’s Review.

# Any Questions?


The End