Introduction to Security Within the Organization

Cybersecurity

GRC Day 1

Class Objectives

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

Identify at least three concrete benefits of a healthy security culture.

Articulate the responsibilities of common C-Suite officers, including the CISO.

Explain the responsibilities of a Security department.

Identify appropriate security controls for a given resource and situation.

Security Aligning with an Organization

Throughout this course, you will be equipped with the tools needed to perform in common technical roles.

Today, we will see how these roles interact with each other and within the larger organization.

GRC Framework

GRC is a framework for answering the questions: *What assets are most important?* and *What is adequate protection?*

- **Governance**: Creating management processes for implementing security practices across the organization.
- **Compliance**: Making sure the business follows internal security policies and adheres to relevant security laws.
- **Risk management:** Identifying an organization's most important assets and determining how they might be compromised.

We define "important" by asking: *How would a security compromise of this asset affect the profits of the business?*

The more significant the loss, the more important the asset.

GRC Framework

We will study how GRC frameworks are considered and implemented into a business by first examining the following:

The Executive Management team

is ultimately responsible for the adherence and enforcement of laws, regulations, and security practices.

The Security team

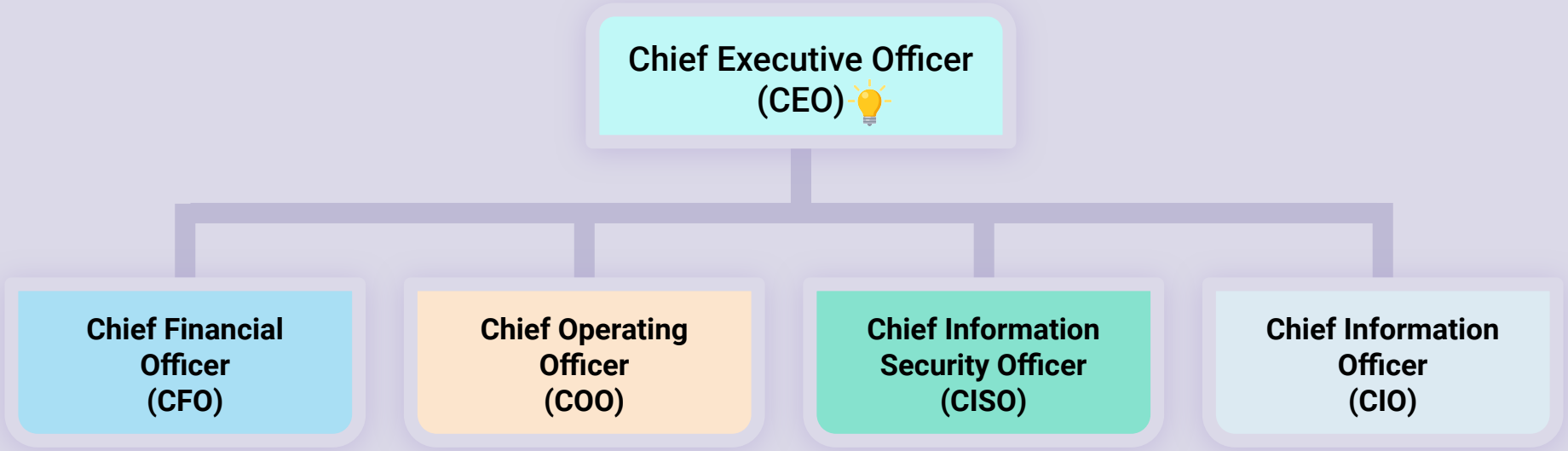
and the role it plays within the larger organization.

Security Roles and Responsibilities

In the next section, we'll cover the following:

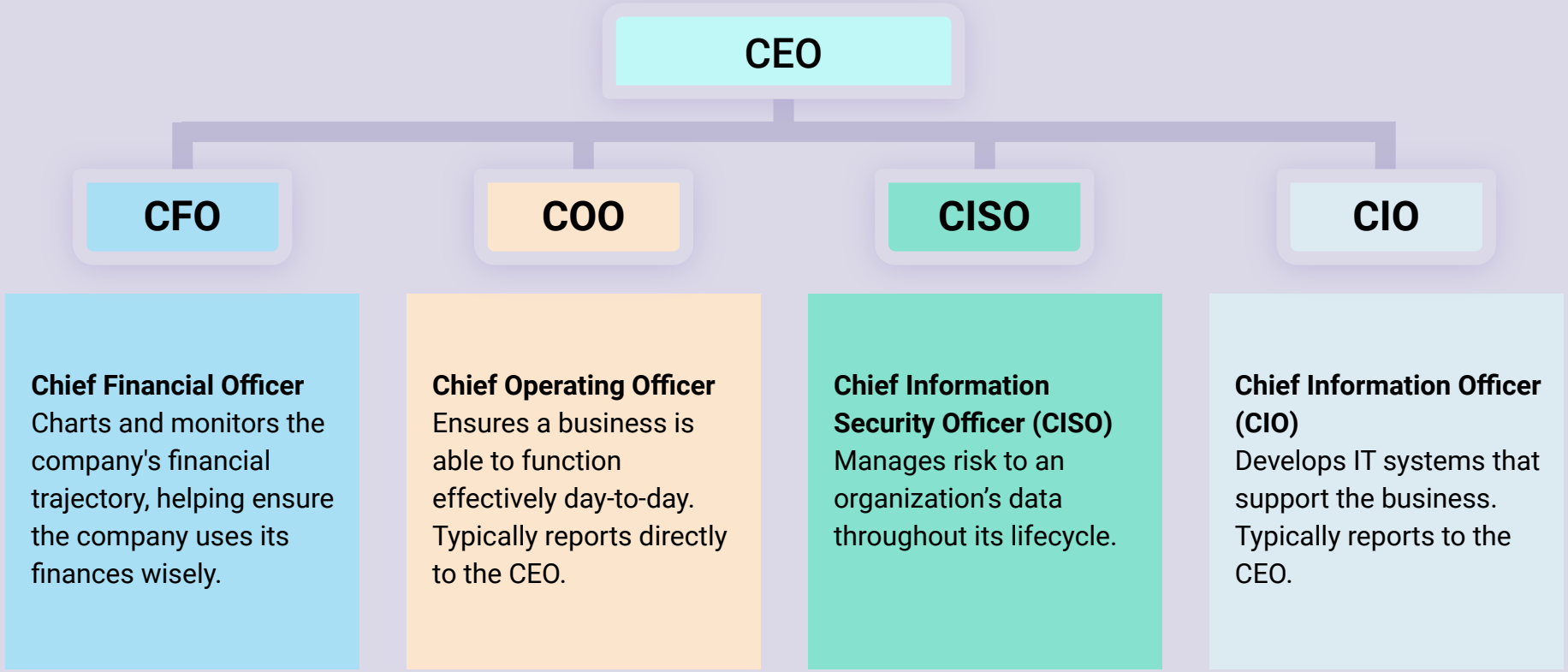
- Executive roles existing in most companies.
- Executive roles relevant to Security departments.
- The responsibilities of Security departments.
- The structure of the security organization.

Executive Roles: The Core Leadership Team



The **Chief Executive Officer (CEO)** is responsible for plotting the overall direction of the company. The CEO reports to the **board of directors**. This group is elected by shareholders and holds the CEO accountable for meeting their demands.

Executive Roles: The Core Leadership Teams



The Responsibilities of the Security Department

CISO is responsible for protecting the company's data, often overseeing the following teams, among others:

Network Security	Incident Response	Application Security
Director of networking or **director of network security** is in charge of networks.	**IR manager** or **SOC manager** manages and Incident Response unit.	**Security architect** is in charge of application security.
A director of networking often has **system administrators**, **network administrators**, and **physical network technicians** on staff. They may also manage a help desk.	An SOC manager employs **SOC analysts,** also known as **security analysts** or **incident handlers**.	A security architect typically manages **security engineers** and **software engineers.**

Security and the Larger Organization

Security operations will interact with other non-security teams within the organization.

For example: An organization's Marketing and Communications teams use the networks and accounts that IT and Networking manage.

What other examples can you think of?

Security Concerns vs. Business Concerns

The most profitable decision isn't always the most secure. Security objectives may be at odds with those of the business.

Security Team's Main Goal:
Protect the business's data.

Business's Main Goal:
Maximize profit and improve efficiency.

What Should the Security Team Do?

An organization's Engineering team proposes an innovative but insecure new feature for their flagship product.

Security Team:
Would probably advise against the new feature due to its poor security.

Business-At-Large:
Might decide to develop it anyway, believing the potential profit is worth the risk.

What Should the Security Team Do?

The Security team must adapt its operations to accomModate a product they *know* is insecure.

Potential Solutions:

Put in place more aggressive monitoring on data servers likely to be exposed by the new feature.

Advise IT and Networking to put in place more sophisticated access controls on important servers and proxies.

100% security is not the *business's* goal.

To limit spending and increase profit, businesses often provide only ***adequate protection*** for their most ***important assets***.

Security vs. Business: Is the Feature Worth the Risk?

An organization's Engineering team proposes an innovative but insecure new feature for their flagship product.

The organization performs a **risk assessment** and concludes that the feature could lead to a 25% increase in quarterly profits. The feature would also risk exposing an isolated data server containing customer names, usernames, and email addresses, but no other PII (personally identifiable information).

Security vs. Business: Is the Feature Worth the Risk?

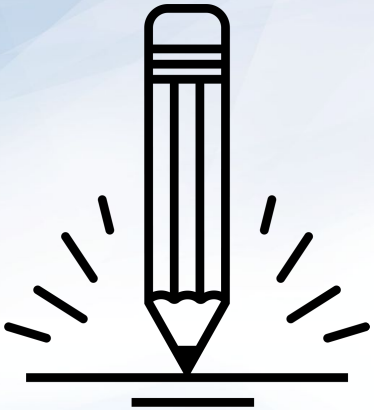
In this case, the *business objective* of achieving profit targets overrides the *risk* of the strategy.

Business Wins

The Security team objects to the feature due to its insecurity. But the business decides that the cost of the potential breach—of an isolated server with no sensitive PII—would be less than the potential profit of the feature.

After making a decision, the business updates its security practices to account for the risk they've undertaken, and regularly confirms everyone is following the rules.

This is **governance** and **compliance**.



Activity: Weighing Security and Business Objectives

In this activity, you'll play the role of a security consultant hired to help a business determine how risky its plans are.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

Security Culture Framework

Security Culture

Strong organizational security begins with making sure employees both *consider security important* and *understand the security implications of their decisions*.

Security culture is the way members of an organization think about and approach security issues. A healthy security culture has employees who are invested in the organization's security and "behave securely."

The health of an organization's security culture is determined by:

- How important employees consider security.
- How aware employees are of common security risks.
- Whether employees know how to avoid insecure behavior.

A healthy security culture requires **motivating employees** to value security, and training them on how to **avoid insecure behavior**.

Security Culture Framework Steps

The **security culture framework** identifies problems in an organization's security culture and develops plans to solve them.

01 Measure and Set Goals

02 Involve the Right People

03 Create an Action Plan

04 Execute the Plan

05 Measure Change

Applying the Framework: Security Scenario

Employees are receiving emails to their work accounts from external sources.

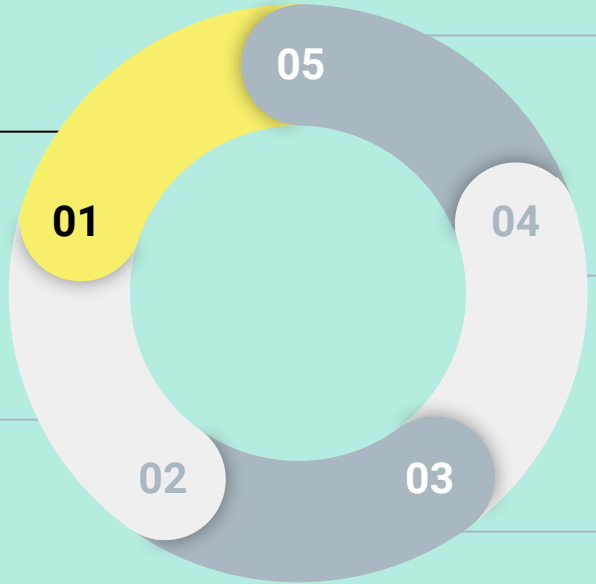
- Employees are clicking on links and downloading attachments in these emails.
- The organization's Security team determined that many of the links and attachments contain malware.

Step 1: Measure and Set Goals

Hire a pentester to run a phishing campaign against your organization. They will send malicious files to everyone in the organization and keep track of who downloads them.

Measure and Set Goals
Set a click rate goal of 5%. Measure this data to determine (1) what percentage of employees download the files and (2) which employees download them.

Involve the Right People



Measure Changes

Execute the Plan

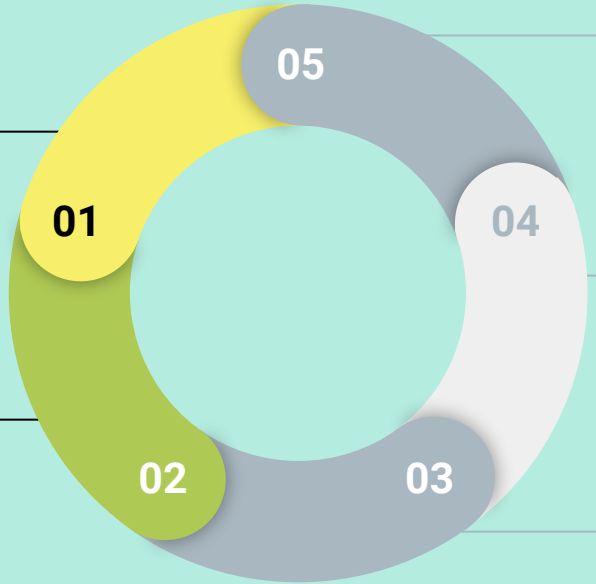
Create an Action Plan

Step 2: Involve the Right People

Since this training will affect all members of the organization, inform the Executive team about the problem and your decision to implement training.

Measure and Set Goals
Measure how employees interact with the campaign, determining the percentage of employees who download the files and who they are. Set goals based on this data.

Involve the Right People
Inform at least the CEO and/or CIO, director of HR, and the person in charge of internal training and communication.



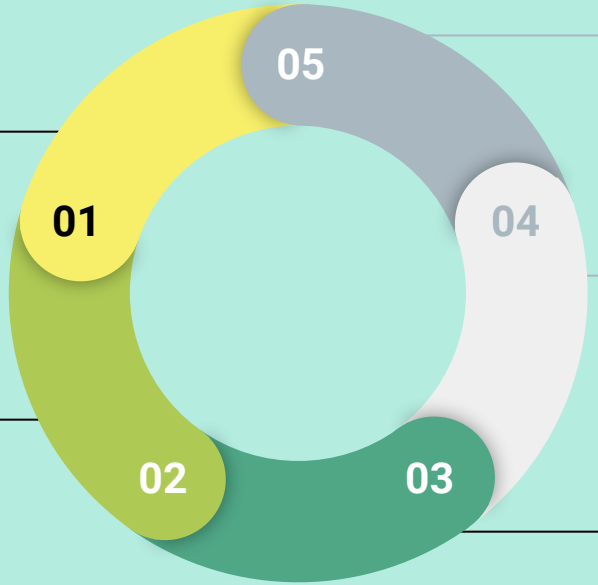
Measure Changes

Execute the Plan

Create an Action Plan

Step 3: Create an Action Plan

After getting clearance to run the training, plan to deliver an annual Cybersecurity Awareness Training event.



Measure and Set Goals
Measure how employees interact with the campaign, determining the percentage of employees who download the files and who they are. Set goals based on this data.

Involve the Right People
Inform at least the CEO and/or CIO, director of HR, and the person in charge of internal training and communication.

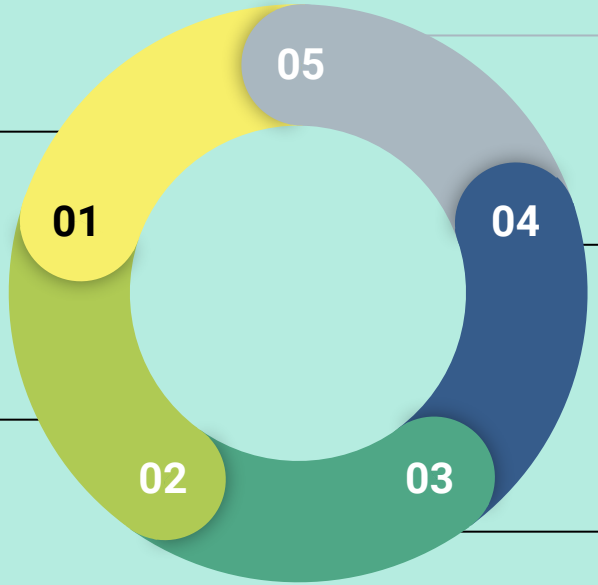
Measure Changes

Execute the Plan

Create an Action Plan
Develop training to cover dangers of malware and how malware can spread through phishing and vishing.

Step 4: Execute the Plan

After developing the training, run it with the goal of training 25% of employees every quarter.



Measure and Set Goals
Measure how employees interact with the campaign, determining the percentage of employees who download the files and who they are. Set goals based on this data.

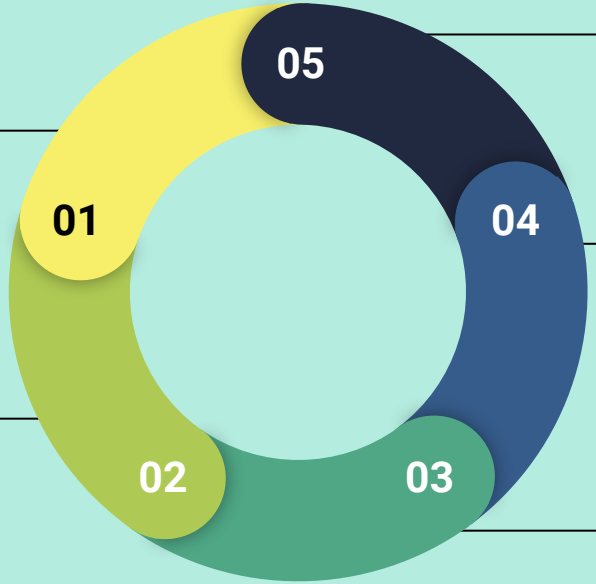
Involve the Right People
Inform at least the CEO and/or CIO, director of HR, and the person in charge of internal training and communication.

Execute the Plan
Run training with a goal of training 25% of employees each quarter.

Create an Action Plan
Develop training to cover dangers of malware and how malware can spread through phishing and vishing.

Step 5: Measure Change

After training the entire company, have the pentesters rerun the original phishing campaign.



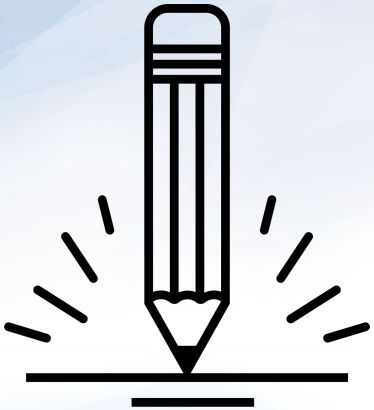
Measure and Set Goals
Measure how employees interact with the campaign, determining the percentage of employees who download the files and who they are. Set goals based on this data.

Involve the Right People
Inform at least the CEO and/or CIO, director of HR, and the person in charge of internal training and communication.

Measure Changes
Determine success or failure based on goals set in Step 1.

Execute the Plan
Run training with a goal of training 25% of employees each quarter.

Create an Action Plan
Develop training to cover dangers of malware and how malware can spread through phishing and vishing.



Activity: Applying the Security Culture Framework: Part 1

You'll play the role of a security consultant contracted by a local bank to develop a plan for strengthening physical security.

Suggested Time:
15 minutes

Time’s Up! Let’s Review.


4:46
Break

Security Culture Framework: Action Plan

Back to Our Security Scenario...

Employees are receiving emails to their work accounts from external sources.

- Employees are clicking on links and downloading attachments in these emails.
- The organization's Security team determined that many of the links and attachments contain malware.

Let's walk through the steps again, with the added context of coordinating with other team members.

Security Culture Framework Steps

Step 1: The Security Culture Framework (SCF) team meets to assess the impact of the phishing incident and the risk posed by future campaigns. This discussion includes:

- An assessment of the damage done by the previous phishing incident.
- Using a pentesting phishing attack to show how many employees download malicious files. This assessment might find a 10% click-through rate, meaning that 10% of employees downloaded malicious email attachments.
- Setting a target click-through rate. The team might decide that a 5% click-through rate is acceptable.

Security Culture Framework Steps

Step 2: The SCF team manager (in this case, the IR manager) meets with the CISO to explain that the previous phishing attack was successful because 10% of employees downloaded files from unknown email addresses.They request a budget to carry out a plan that will bring this number down to 5%, and explain how it will profit the business.

Security Culture Framework Steps

Step 3: The SCF team develops a training plan to educate employees.

In addition, the SCF team develops a Supplemental Security Awareness training plan. This plan will only be delivered to employees who continue to click malicious links after training.

Security Culture Framework Steps

Step 4: After developing the training, the SCF team decides on incentives and disincentives. These will be awarded based on how employees behave during penetration tests and security audits.

Since employees won't know exactly when the assessments are being conducted, the team expects more people to follow the new download guidelines.

Incentives for not clicking:	Disincentives for clicking:
A $40 gift card, free or discounted security conference attendance, and additional vacation time.	Supplemental security awareness training and additional random device audits for one quarter.

Security Culture Framework Steps

Step 5: The SCF team collaborates with HR to determine the best dates to run trainings.

During these meetings, the HR team explains that the most reliable way to ensure 100% attendance over the next fiscal year is to have quarterly training sessions, training 25% of employees each time.

SCF and HR coordinate the specific dates and location of the training.

Security Culture Framework Steps

Step 6: The SCF team collaborates with Communications to develop and distribute information about the training.

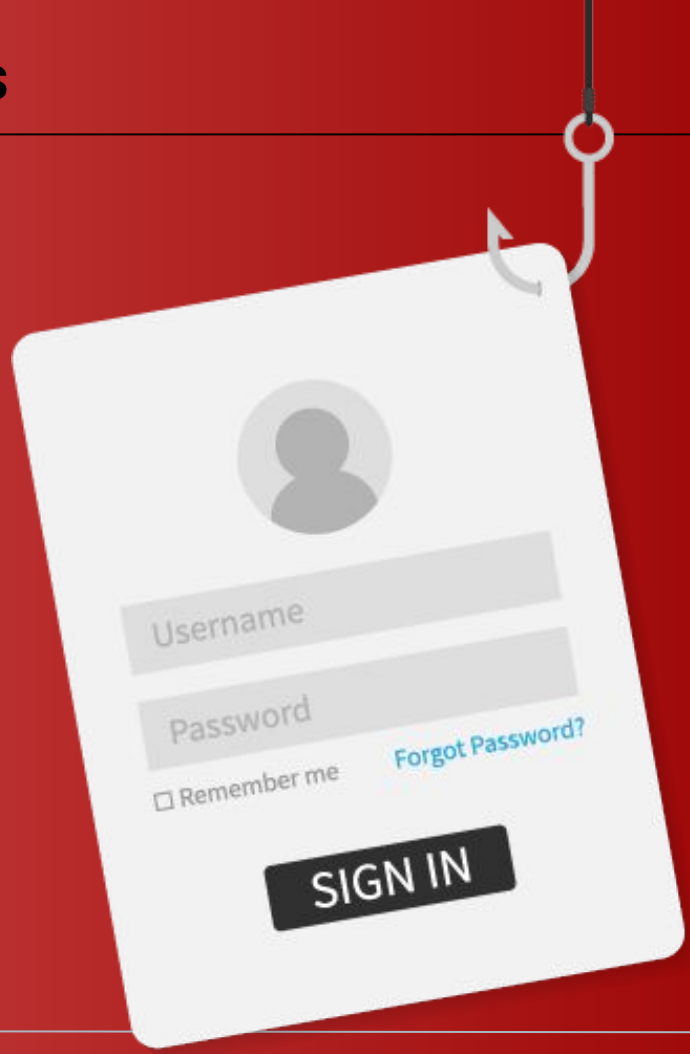
Step 7: The SCF team sets up and runs the training as scheduled.

Security Culture Framework Steps

Step 8: Every quarter, the SCF team contracts the same pentesting firm to run the phishing campaign against all employees who have already been trained.

Step 9: After every test, the SCF team identifies employees who still clicked malicious links, and requires them to go through Supplemental Security Awareness training.

In addition, they verify whether the click-through rate drops closer to 5%.



Security Culture Framework Steps

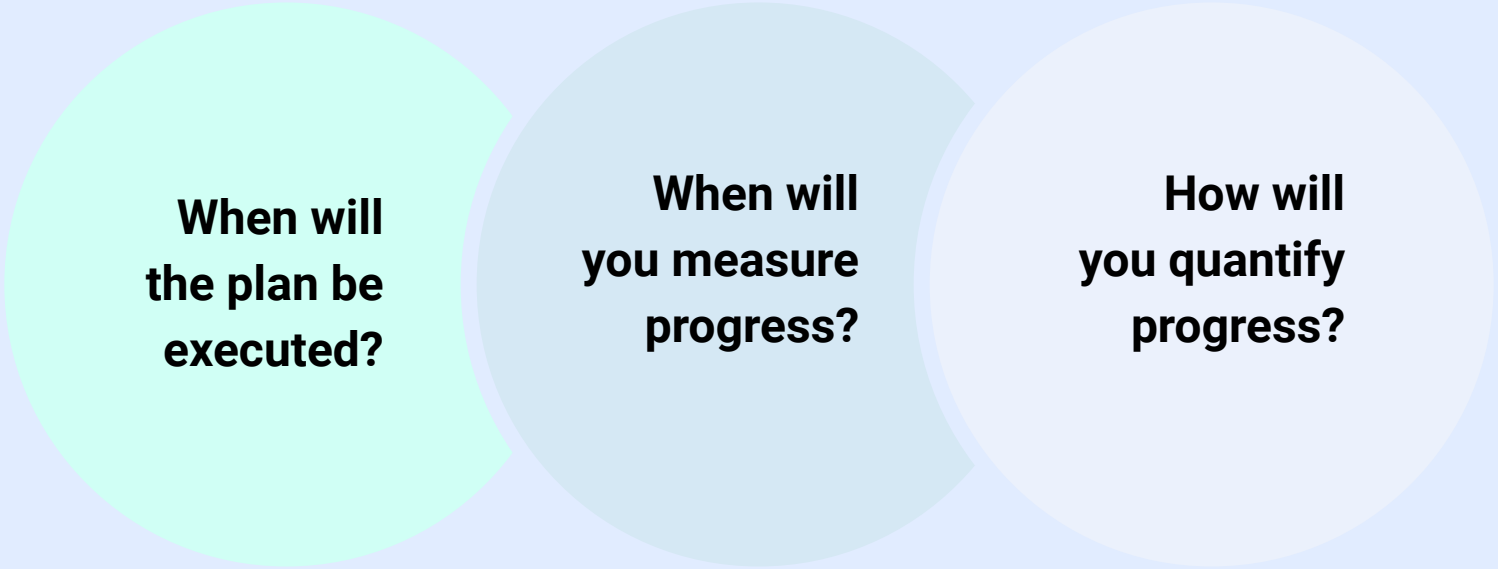
Step 10: After training the entire company, the SCF team runs a final phishing campaign to evaluate the overall effectiveness of the training.

If they find that the click-through rate (CTR) is 5% or lower, it is considered a success.

Otherwise, they might decide to run the training for an additional year, or take a different approach to solving the problem.

What’s the (Action) Plan?

Some important considerations when developing a plan:



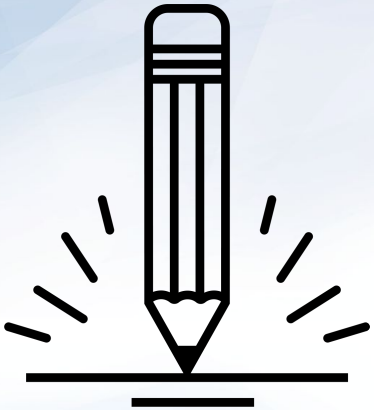
What's the (Action) Plan?

Questions you should ask when developing a plan:

- **When will the plan be executed?**
  The SCF and HR teams will run the training once every quarter, training 25% of employees each time. This ensures 100% of employees will be trained by the end of the year.

- **When will you measure progress?**
  The SCF team will run a phishing campaign each quarter, targeting only the most recently trained cohort. After all cohorts have been trained, a final campaign will test how well everyone follows the new guidelines over time.

- **How will you quantify progress?**
  The SCF team decides to quantify the click-through rate, which is the percentage of employees who download malicious links from emails. Their goal is to decrease this number from 10% to 5%.



Activity: Security Culture Framework: Part 2

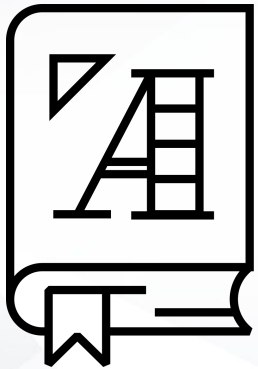
In this activity, you will complete the plan you began drafting in Part 1 earlier today.

Suggested Time:
20 Minutes

Time’s Up! Let’s Review.

Security Controls

In addition to improving security culture over the *long term*, the security team should enforce **security controls** that manage issues in the *short term*.



A **security control** is any system, process, or technology that protects the confidentiality, integrity, and accessibility of a resource.

Security Controls and Control Types

Security controls can be administrative, technical, or physical in nature.

Administrative

Example

Requiring employees to follow training guidelines.

Technical

Example

Requiring developers to authenticate using SSH keys rather than passwords.

Physical

Example

Protecting a building by requiring keycard access.

Security controls can have different goals.

01 **Preventative** controls *prevent* access with physical or technical barriers. (For example: Keycard access)

02 **Deterrent** controls *discourage* attackers from attempting to access a resource.

03 **Detective** controls *identify and alert* attempts to access a resource.

04 **Corrective** controls attempt to *fix* an incident, and possibly stop it from happening again.

05 **Compensating** controls *restore* the function of compromised systems.

We'll see more security controls in future units.

Regardless of their type, all security controls seek to restrain or respond to access of a resource. The following *access controls* determine who can access specific resources:

Linux

Example

File permissions act as access controls by preventing users from modifying files they don't own.

Networks

Example

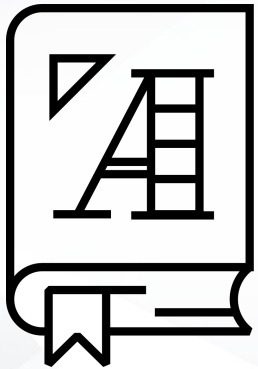
Firewalls control access to networks.

Incident Response

Example

Monitoring systems act as detective control.

Layering security controls is a fundamental aspect of the security design framework known as **defense in depth.**



Defense in depth is the practice of using multiple defenses to secure a resource.

Defense in Depth

For example, a secure network may protect an SSH server in three ways.

01 **Technical control:** Hiding the server behind a firewall that only forwards connections from the corporate VPN.

02 **Technical control:** Forcing users to authenticate with SSH keys *and* passwords.

03 **Procedural control:** Requiring users to generate new keys, with new strong passwords, every quarter.

Control Diversity and Redundancy

A system with multiple layers of protection is said to have **control diversity**, because it is protected in multiple ways.

01

Protecting the SSH server with a firewall prevents unwanted connections from unintentional attackers.

02

If an attacker bypasses the VPN, it is still hard to compromise the server. Users must authenticate with SSH keys *and* passwords, so attackers can't easily brute-force the login.

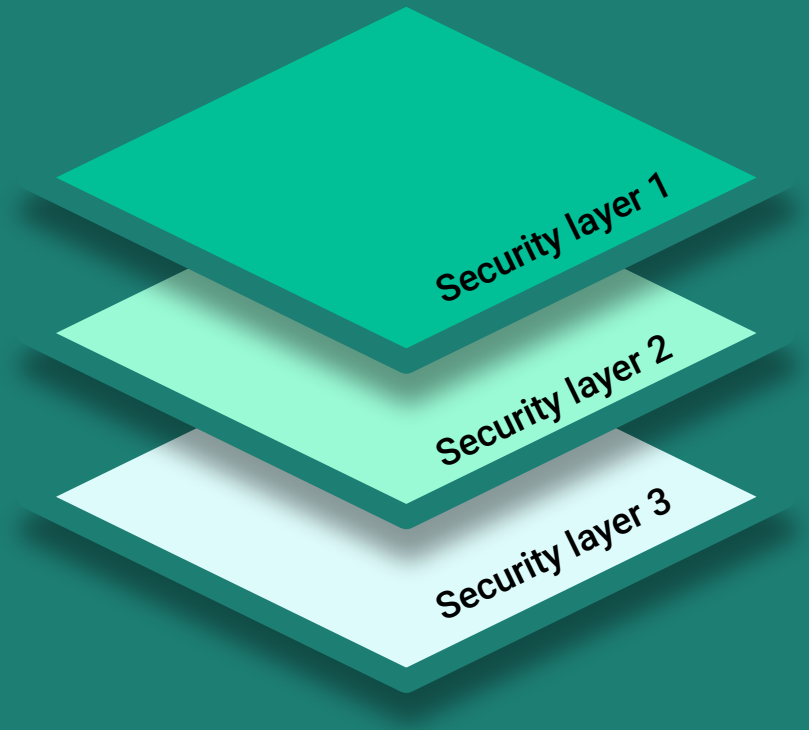
03

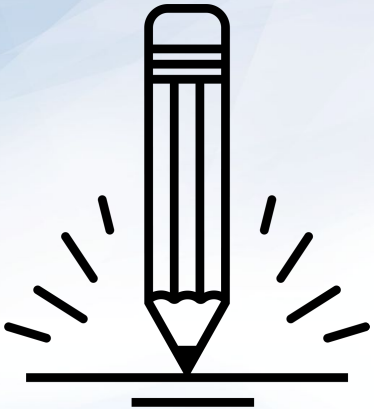
If an attacker does steal both a valid SSH key *and* its password, they will only be able to compromise the server for a limited time, since the stolen key will expire after, at most, three months.

Redundancy and Single Points of Failure

Defending the system with multiple methods ensures that it remains protected *even if one of them fails*. This concept is known as **redundancy**.

- If the system only has a single control, that control is its **single point of failure**. An attacker can compromise the system by breaking just a single control.
- Creating redundancy eliminates the inherent risk of single points of failure.





Activity: Implementing Security Controls

In this activity, you will draft the final piece of security recommendations for GeldCorp.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

What We've Covered

Today's activities put you in the role of a security consultant hired to help a financial technology firm respond to a major security breach. You had to:

- Identify the source of the breach.
- Develop a plan to improve security and security culture.
- Define metrics to measure if the plan was successful.
- Propose controls, in addition to training, that can mitigate risk.

Looking Forward...

What we learned today will prepare us to learn about **governance later in the week**.

Governance is the portion of the GRC framework used to enforce security standards, policies, and procedures.

Now that we have a good understanding of how organizations develop best practices for security, we can learn how it uses governance methods to codify and enforce them.

Any Questions?


The End