GRC: Security Within an Organization

Cybersecurity

GRC Day 1

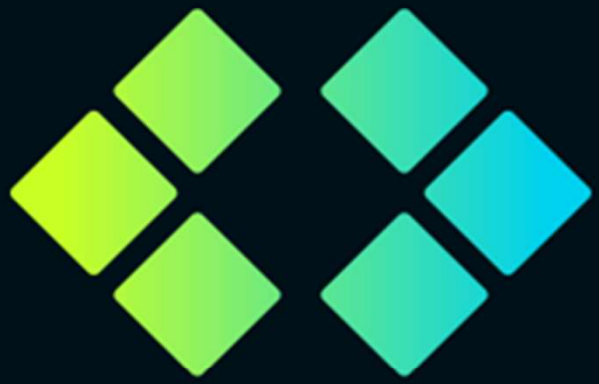
Class Objectives

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.

Let’s briefly look at some of this bootcamp’s modules and their corresponding professional roles.

Modules: **Linux and Windows**

These units introduce the fundamentals of systems administration.

What We'll Learn

How to manage users, control file permissions, schedule tasks with cron, manage installed software with apt, and configure system services.

Job Context

These are all common tasks for systems administrators.

Module: **Networking**

These units introduce the fundamentals of networking and network security.

What We'll Learn

How to configure firewalls, port-scan remote hosts, use Wireshark to capture live traffic, and analyze network protocols found in traffic captures.

Job Context

These are common tasks for network administrators. Traffic analysis is required in SOC analysis, network forensics, and threat hunting roles.

Module: **Web and Web Vulnerabilities**

These units introduce the network structure and protocols used on the modern web, and familiarize us with the most common vulnerabilities found on live web servers.

What We'll Learn

How to use Burp Suite to hunt for vulnerabilities in web applications.

Job Context

These are important skills for penetration testers and SOC analysts, as well as network administrators who maintain web servers.

Module: **Offensive Security**

These units introduce the basics of assessing a network's security with penetration testing.

Job Context

These skills are relevant to penetration testers, but knowledge of attack methodologies is also useful for SOC analysts and network forensics roles.

Module: **Defensive Security**

These units introduce Splunk, incident response procedures, and forensics.

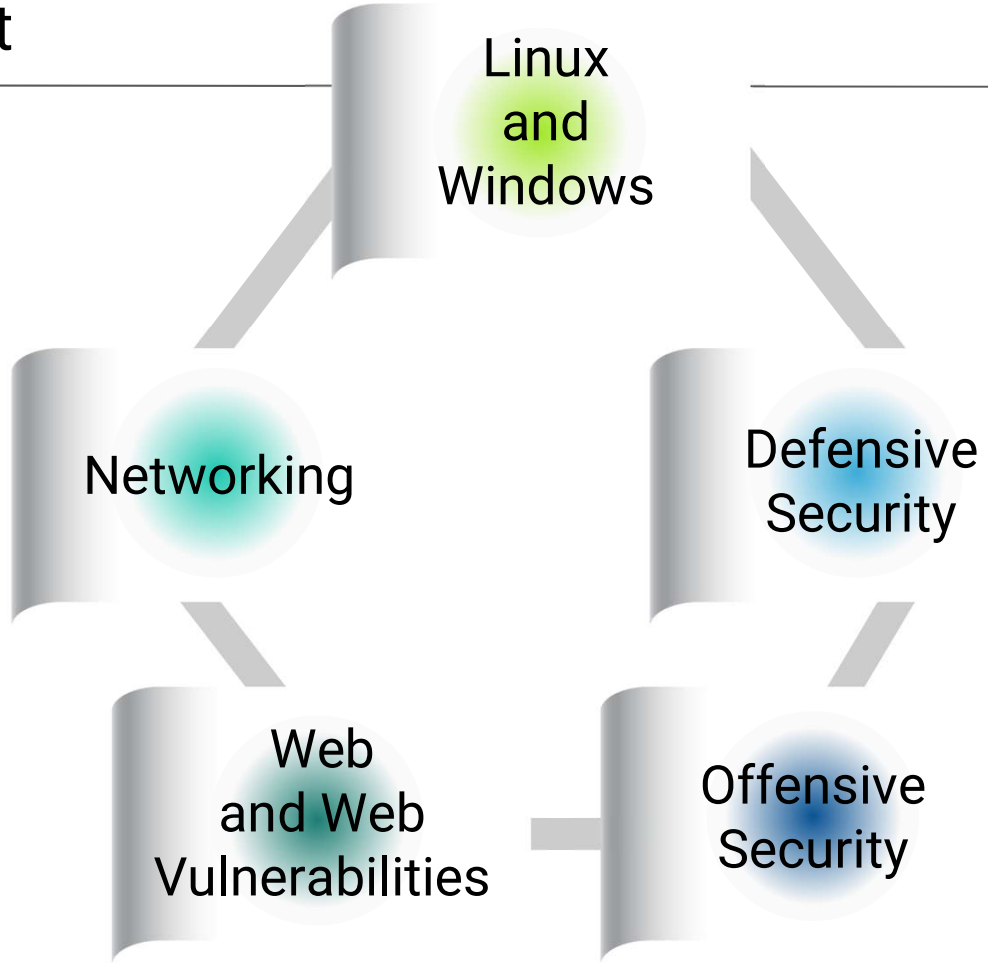
Job Context

These skills are most relevant to SOC analysts and network forensics roles.

Security Team Alignment

Multiple security teams work together to protect the larger organization.

Example: An organization's Incident Response team needs to work closely with its IT and Networking department to report breaches and recommend how to better secure systems.



Security and the Larger Organization

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

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

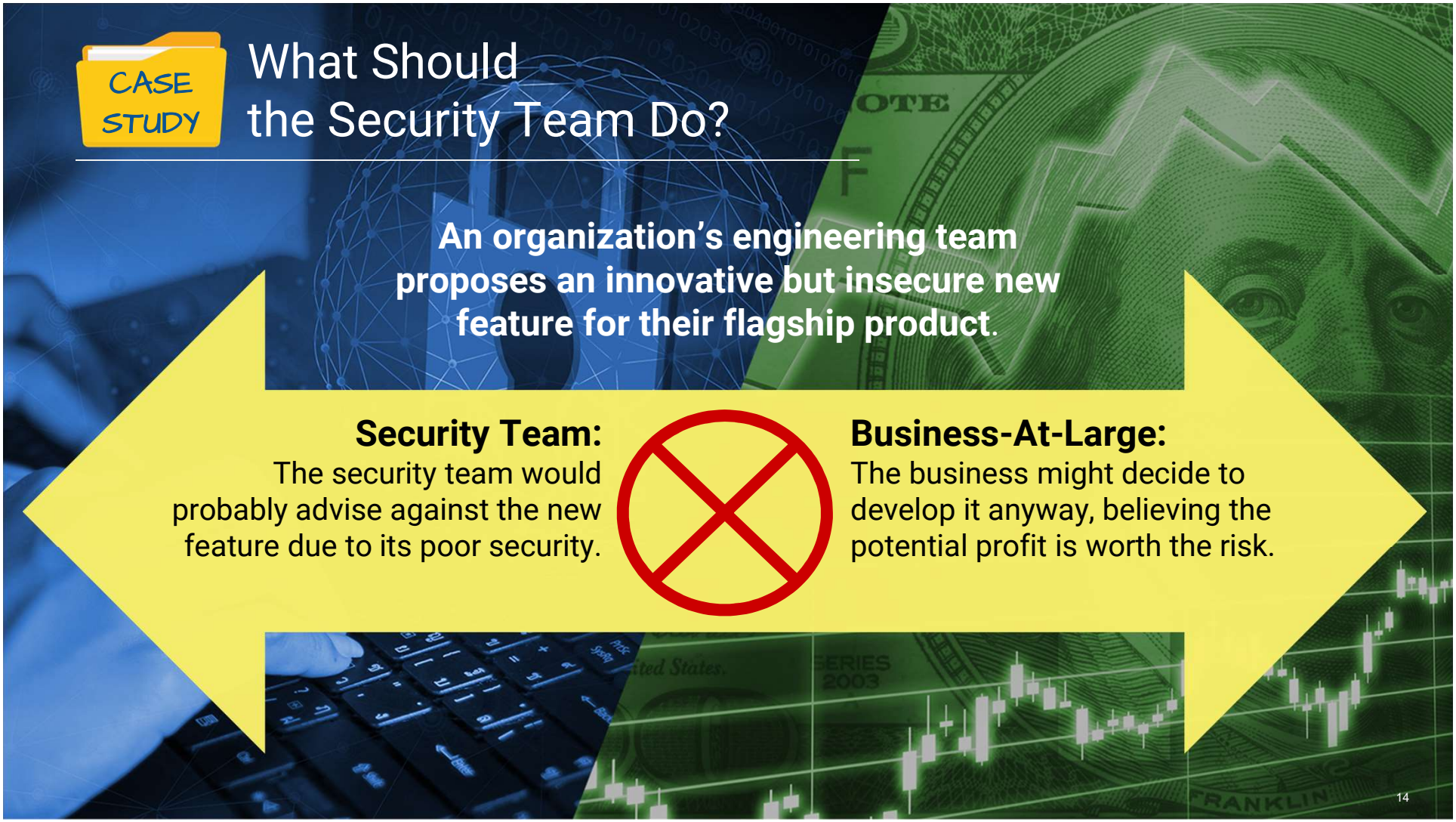
What other examples can you think of?

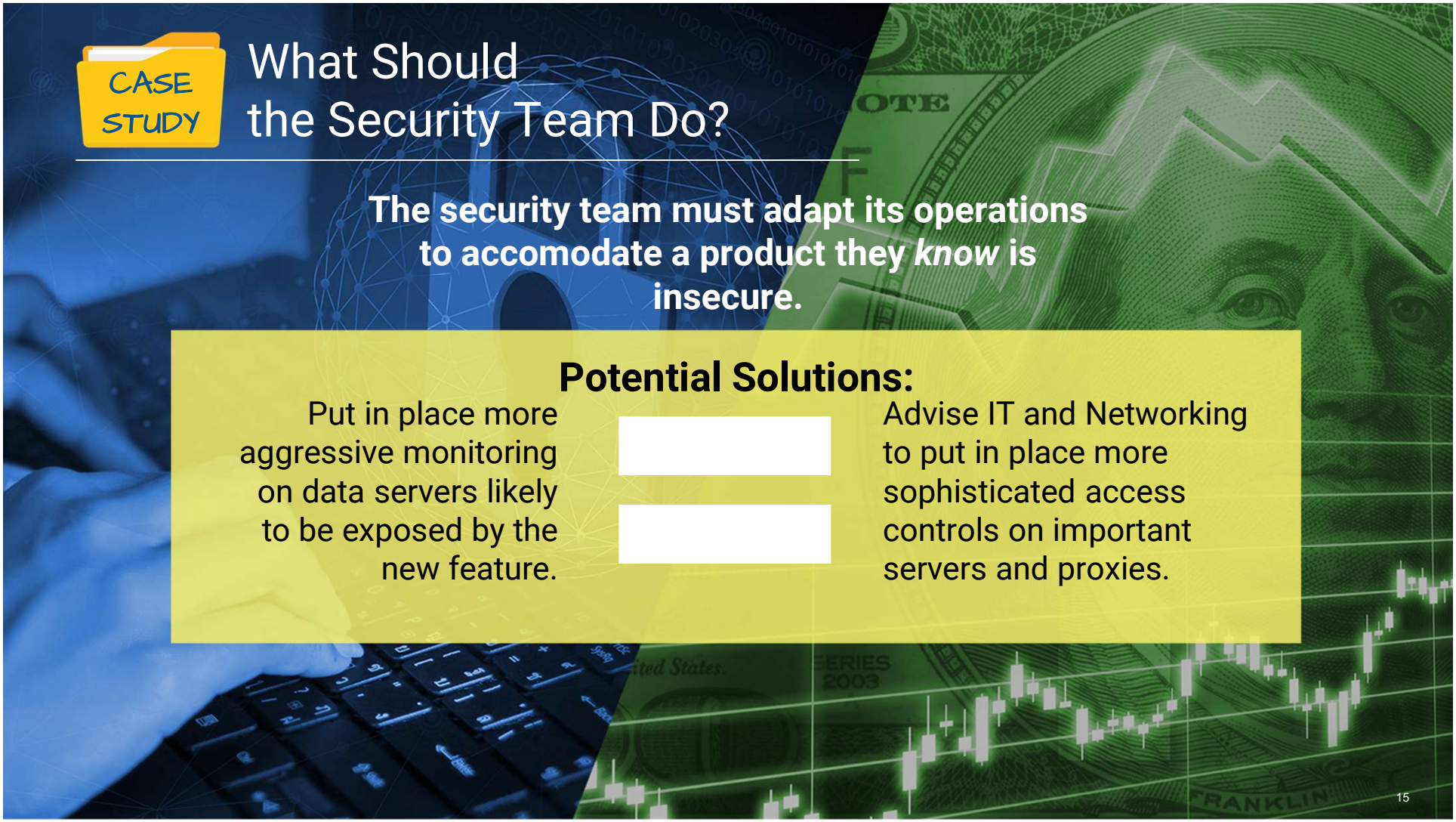
Security Concerns vs. Business Concerns

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-At-Large's Main Goal:
Maximize profit
and improve efficiency


CASE STUDY
What Should the Security Team Do?
An organization's engineering team proposes an innovative but insecure new feature for their flagship product.
Security Team:
The security team would probably advise against the new feature due to its poor security.
Business-At-Large:
The business 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 accomodate 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*.

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.

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).

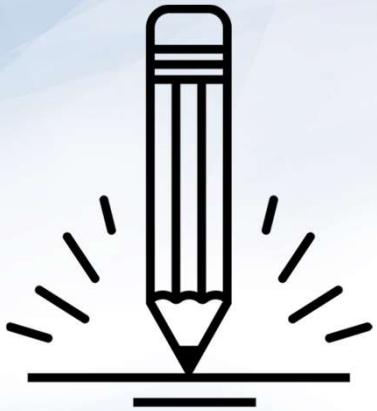
Security vs. Business: Is the Feature Worth the Risk?

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 on the grounds of 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

Times Up! Let’s Review.

Weighing Security and Business Objectives

Activity Review: Weighing Security and Business Objectives

Business Plans

1. The director of Engineering suggested giving all developers access to all data.

2. The director of IT suggested exposing administration servers to the public internet.

3. An SOC analyst recommended merging all of the company's mail servers into a single server, in order to cut costs and improve efficiency.

Activity Review: Weighing Security and Business Objectives

Business Plans

1. The director of Engineering suggested giving all developers access to all data.
   Benefits: Makes development easier.
   Detractors: Allows *any* developer to access *any* user data, including sensitive PII that has nothing to do with their jobs.
   Recommendation: Reject on grounds of privacy.
2. The director of IT suggested exposing administration servers to the public internet.
3. An SOC analyst recommended merging all of the company's mail servers into a single server, in order to cut costs and improve efficiency.

Activity Review: Weighing Security and Business Objectives

Business Plans

1. The director of Engineering suggested giving all developers access to all data.
   Benefits: Makes development easier.
   Detractors: Allows *any* developer to access *any* user data, including sensitive PII that has nothing to do with their jobs.
   Recommendation: Reject on grounds of privacy.
2. The director of IT suggested exposing administration servers to the public internet.
   Benefits: Administrators can work from any computer they choose.
   Detractors: The servers would be publicly accessible, which is unacceptable for a private network.
   Recommendation: Reject this request. A VPN would be a better solution to this problem.
3. An SOC analyst recommended merging all of the company's mail servers into a single server, in order to cut costs and improve efficiency.

Activity Review: Weighing Security and Business Objectives

Business Plans

1. The director of Engineering suggested giving all developers access to all data.

   Benefits: Makes development easier.

   Detractors: Allows *any* developer to access *any* user data, including sensitive PII that has nothing to do with their jobs.

   Recommendation: Reject on grounds of privacy.

2. The director of IT suggested exposing administration servers to the public internet.

   Benefits: Administrators can work from any computer they choose.

   Detractors: The servers would be publicly accessible, which is unacceptable for a private network.

   Recommendation: Reject this request. A VPN would be a better solution to this problem.

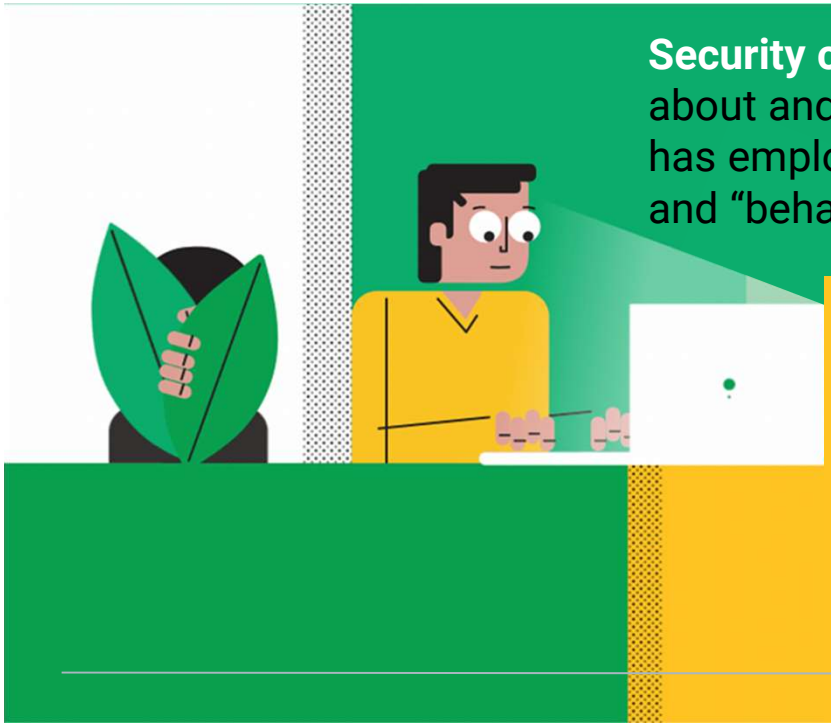
3. An SOC analyst recommended merging all of the company's mail servers into a single server, in order to cut costs and improve efficiency.

   If the company has so many emails that it *needs* to maintain multiple servers, this suggestion is not possible. Otherwise, hosting all of the data on a single server makes sense.

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.

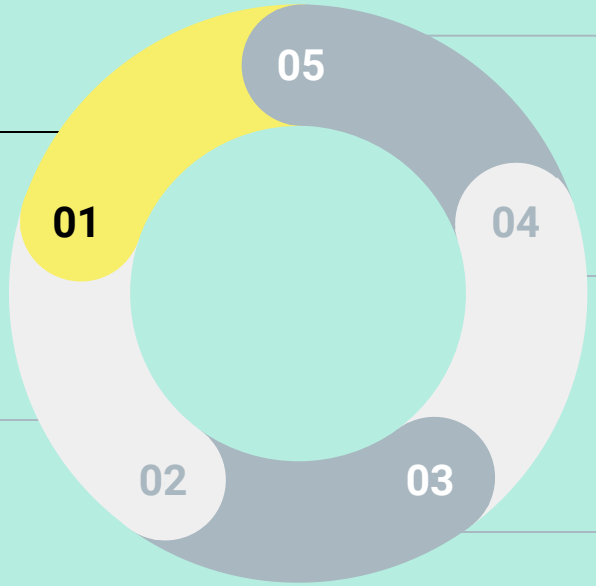
- Employees are clicking on links and downloading attachments in these emails.
- The organization's security team determined that many of the links and attachments contain malware.

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

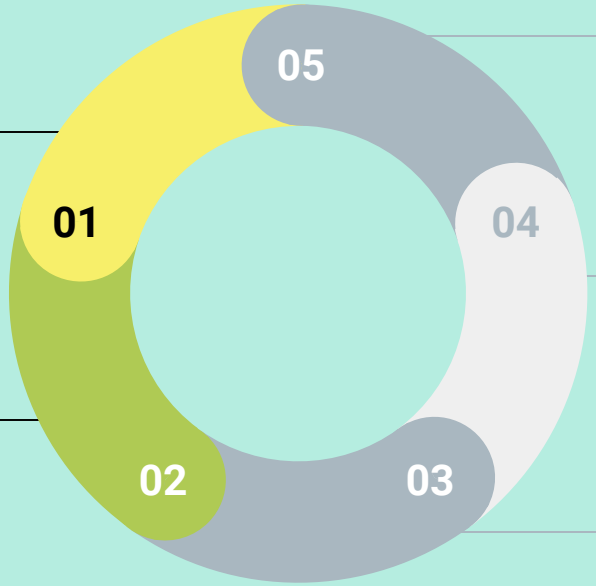
Create an Action Plan

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.



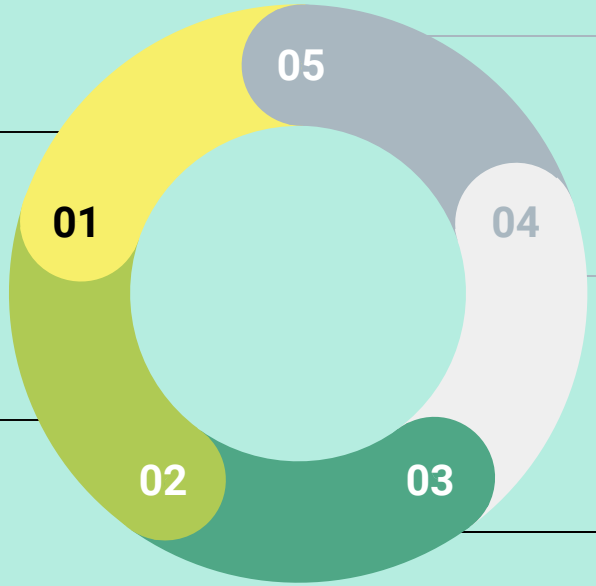
Measure Changes

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.

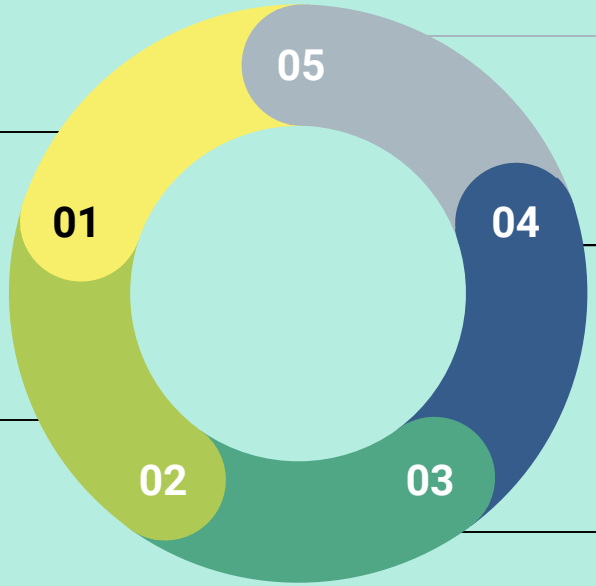
Measure Changes

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.

Measure Changes

Step 5: Measure Change

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

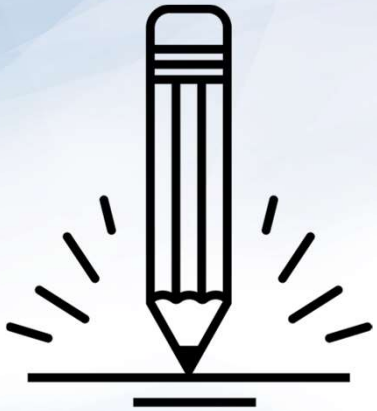
Measure and Set Goals
Measure how employees interact with the campaign, determining the percentage of employees who download the files and who they are. Set goals based on this data.

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.

Instructions shared on Slack.

Suggested Time:
15 minutes

Times Up! Let’s Review.

Applying the Security Culture Framework: Part 1

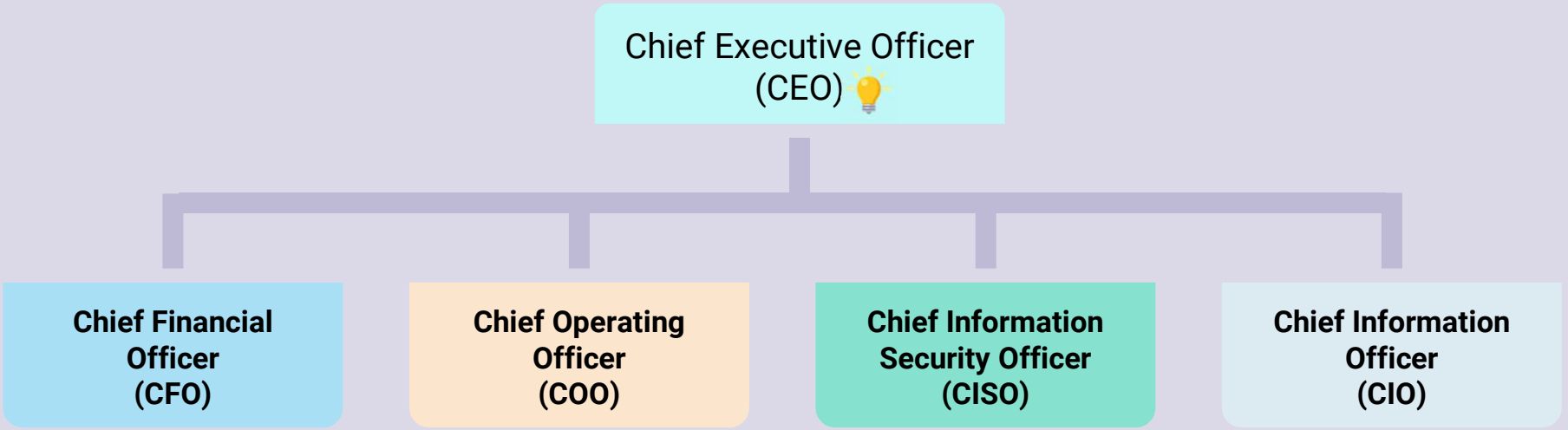
Security Roles and Responsibilities

Security Roles and Responsibilities

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

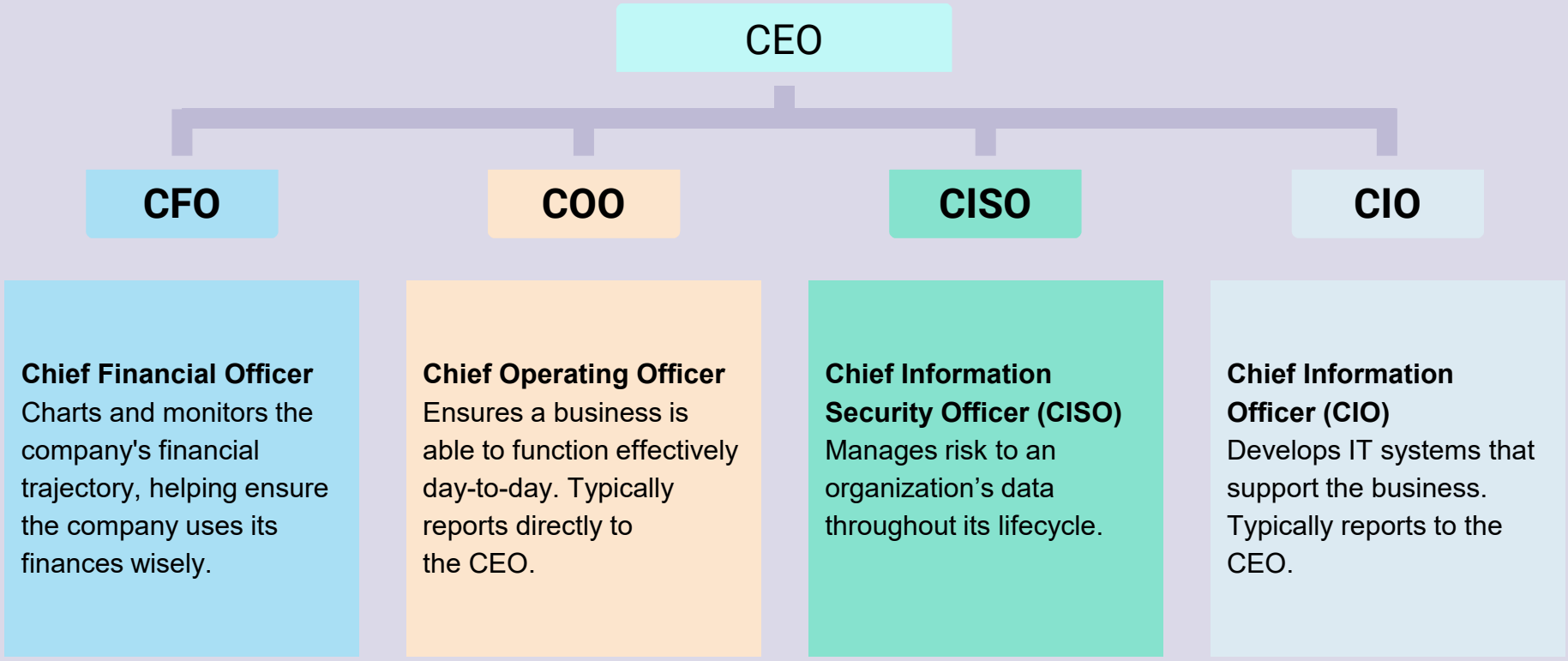
- Executive roles existing in most companies
- Executive roles relevant to security departments
- The responsibilities of the security department
- The structure of the security organization

Executive Roles: The Core Leadership Teams

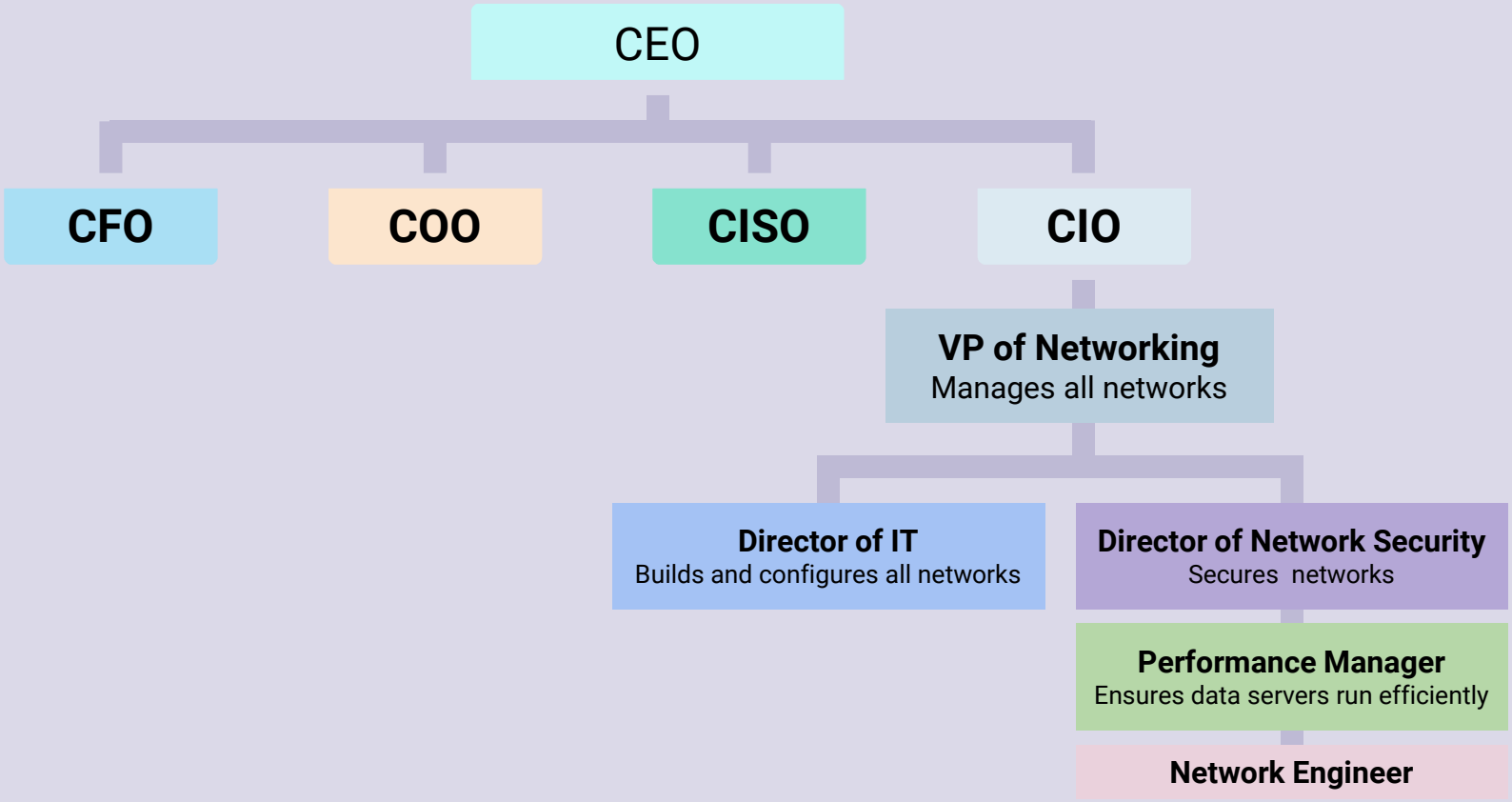


The **Chief Executive Officer (CEO)** is responsible for plotting the overall direction of the company. The CEO reports to the **Board of Directors**. This group is elected by shareholders and holds the CEO accountable for meeting their demands.

Executive Roles: The Core Leadership Teams



Organizational Structure



Sample Reporting Structure

Reports their progress to the Performance Manager.

Receives reports from several Network Engineers, each working on different tasks.

Uses these reports to inform the Director of IT if the organization is meeting network performance targets.

Receives reports from several managers, each in charge of a different aspect of the network.

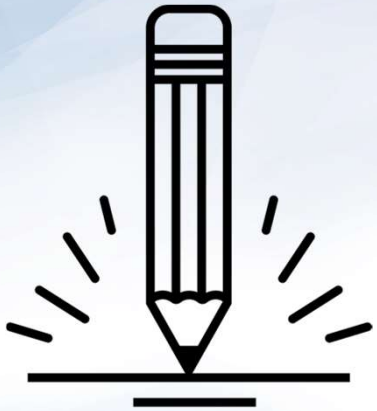
Uses these reports to tell the VP of Networking which functions of the IT department are going well.

Receives reports from all of Directors and uses these to determine the overall health of the company's networking teams and infrastructure, and how they're helping the organization achieve its goals.

The Responsibilities of the Security Department

CISO is responsible for protecting the company's data, often over seeing the following teams, roles and responsibilities:

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.**



Activity: Designing a Security Org Chart

In the next activity, you will create an organizational chart based on a description of the client company.

Instructions shared on Slack.

Suggested Time:
20 Minutes

Times Up! Let’s Review.

Designing a Security Org Chart


Break
4:46

Security Culture Framework: Action Plan

Back to Our Security Scenario...

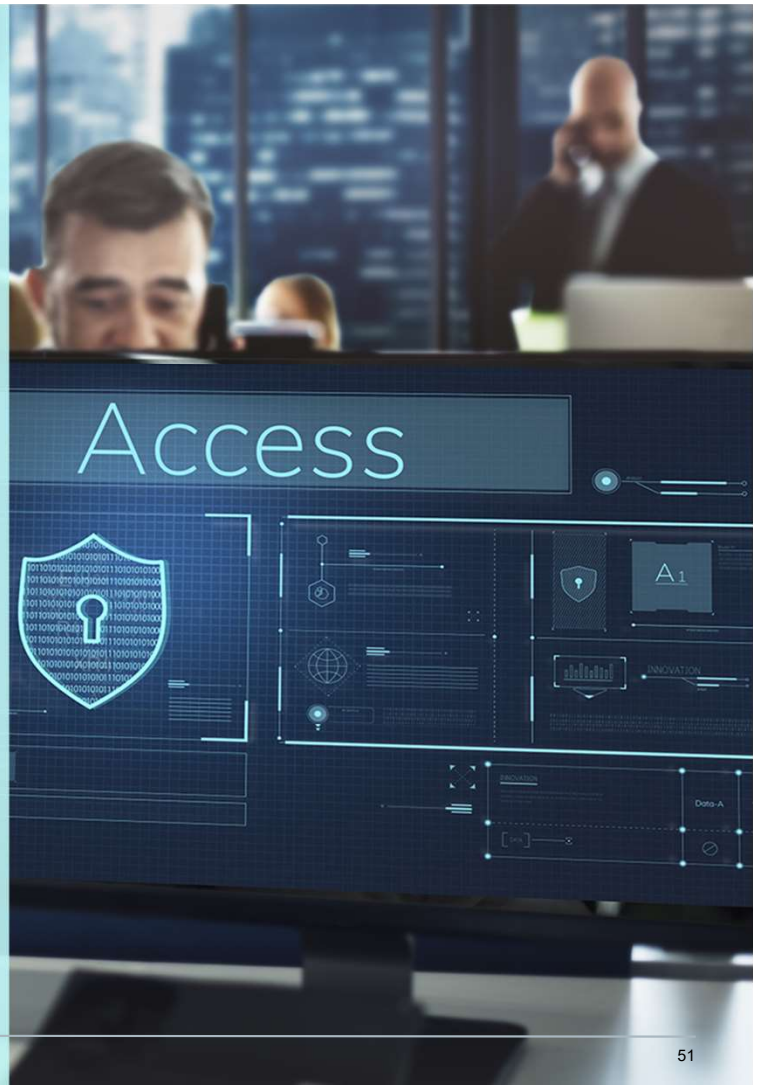
Employees are receiving emails to their work accounts from external sources.

- 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.

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.



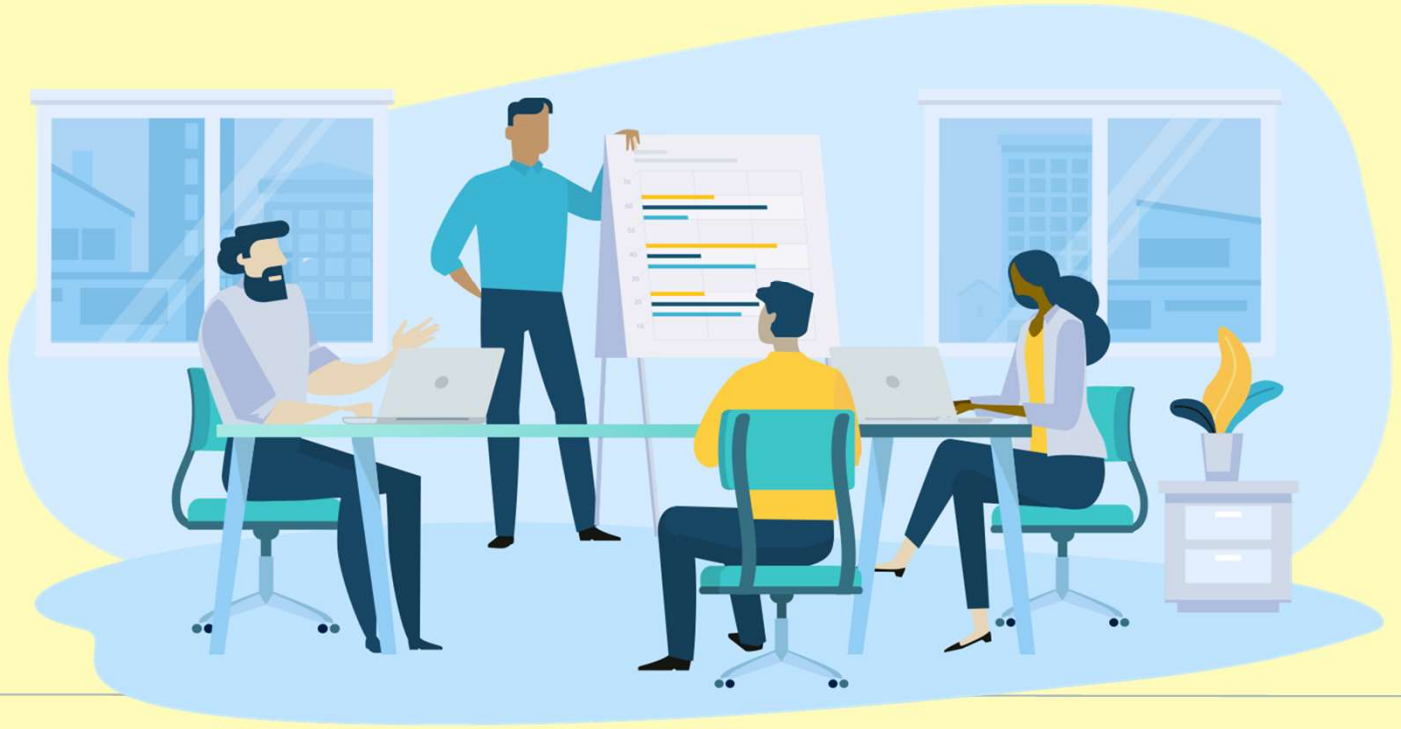
Security Culture Framework Steps

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.



What’s the (Action) Plan?

Some important considerations when developing a plan:

When will the plan be executed?

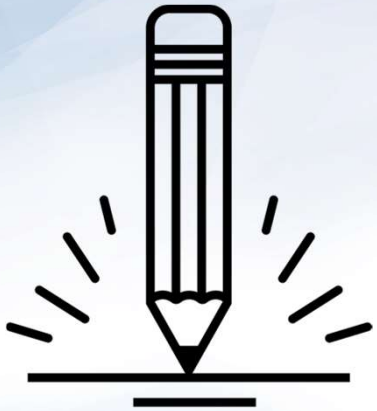
When will you measure progress?

How will you quantify progress?

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.

Instructions shared on Slack.

Suggested Time:
20 Minutes

Times Up! Let’s Review.

Security Culture Framework: Part 2

Review: Security Culture Framework: Part 2 - Sample Solution

Involve the Right People: The planning team involves **HR**, **Security**, **Finance**, and **Communications**.

Action Plan:

- Schedule quarterly trainings
- Design and develop training
- Run quarterly training
- Evaluate impact after each training
- Evaluate overall impact after one year

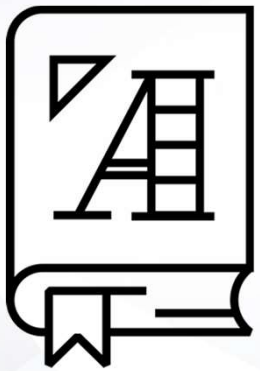
Schedule: The Security and HR Teams decide that *quarterly* training makes the most sense.

Metrics and KPIs: The Security team is aiming for 0% of employees to allow tailgating after training.

Measurements: One month after each quarter's training, security personnel will audit security cameras, and identify the employees allowing tailgating. Those who have already been through training will be disciplined. Those who follow training guidelines will be rewarded. Those who have not yet been trained will be notified that they should stop, but will *not* face disciplinary action.

Security Controls

In addition to improving security culture over the *long term*, the security team should enforce security controls that address 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 key-card access.

Security controls can have different goals.

01 **Preventative** controls *prevent* access with physical or technical barriers.
(Key-card access is an example of a preventive control.)

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

03 **Detective** controls *identify and record* attempts at access to 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* determining who can access specific resources:

Linux

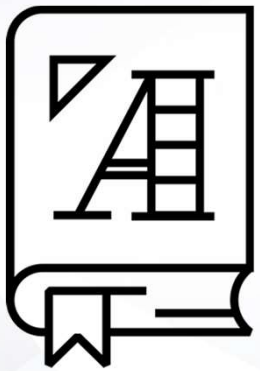
Example:
File permissions act as access controls by preventing users from modifying files they don't own.

Networks

Example:
Firewalls control access to networks.

Incident Response

Example:
Monitoring systems act as detective control.



Defense in Depth is a practice using multiple defenses to secure a resource.

Defense in Depth

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

01 Hiding the server behind a firewall that only forwards connections from the corporate VPN **(technical control)**

02 Forcing users to authenticate with SSH keys *and* passwords **(technical control)**

03 Requiring users to generate new keys, with new strong passwords, every quarter **(procedural control)**

Control Diversity

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 will still be difficult to compromise the server. Users must authenticate with SSH keys *and* passwords, so attackers can't easily brute-force the login.

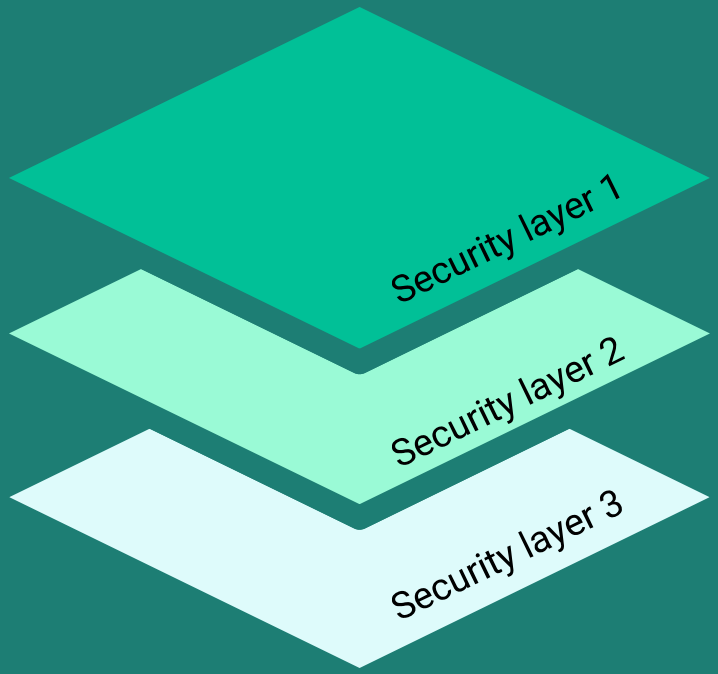
03

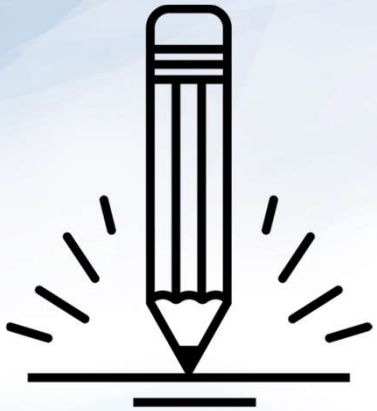
If an attacker does steal both a valid SSH key *and* its password, they will only be able to compromise the server for a limited time, since the stolen key will expire after, at most, three months.

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.
- Ensuring 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.

Instructions shared on Slack.

Suggested Time:
20 Minutes

Activity Instructions: Implementing Security Controls

In this activity, you'll draft the last piece of the recommendations you'll submit to GeldCorp.

The training plan you developed earlier is a personnel security measure, and won't drastically reduce tailgating rates until at least next year. Consider *physical*, *technical*, or *procedural* controls that will immediately reduce employee tailgating.

Record *three* different controls of any type. For each, answer the following questions:

- How does this reduce piggybacking?
- How much will this control cost to implement?
- What percentage reduction in piggybacking rates do you expect?

Suggested Time: 20 Minutes

Times Up! Let’s Review.

Implementing Security Controls

Review: Implementing Security Controls - Sample Solutions

Install a Turnstile

- Implement turnstiles at all of the organization's data centers. These turnstiles require employees to scan an ID card and allow one person into the building at a time.

- The system will need be installed at all sites, and key cards issued to all employees. These measures will be a significant expense. However, a financial organization might deem the added security of these *physical access controls* well worth the cost.

Encrypt Top-Secret Data

- Encrypt all top-secret data, and only allow it to be decrypted by a single server, verified by digital signature. (The attacker would not have been successful if they'd stolen *encrypted* financial records.)

- As an advanced measure, the organization can choose to only allow access to that decrypted data through API, and restrict access to this API to only trusted individuals. This is a *technical control*.

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 whether 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.

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.