







GRC: Organizational Security

Cybersecurity
GRC Unit, Day 1



Class Objectives

By the end of class today, students 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 the security department
-  Identify appropriate security controls for a given resource and situation

Security Aligning with an Organization



*Let's begin with a brief
recap of some modules
we've covered so far in the
course.*

Modules Review: **Linux**

These units introduced you to the fundamentals of Linux systems administration

What You Learned

Managing users; controlling file permissions; scheduling tasks with cron; managing installed software with apt; and configuring system services.

Job Context

These are all common responsibilities of system administrators.

Modules Review: Networking

These units introduced you to the fundamentals of networks and network security.

What You Learned

Configuring firewalls; port-scanning remote hosts; using Wireshark to capture live traffic; and analyzing network protocols found in traffic captures.

Job Context

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

Modules Review: Web and Web Vulnerabilities

These units introduced you to the network structure and protocols used on the modern web, and introduced them to the most common vulnerabilities found on most live web servers.

What You Learned

Configuring a LAMP server from the command line; using 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.

Modules Review: Offensive Security

These units introduced you to 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 in network forensics roles.

Modules Review: Defensive Security

These units introduced you to Splunk, Incident Response procedures, and Forensics.

Job Context

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

Security Teams Aligning

While responsibilities and skills vary across teams, the multiple security teams work in conjunction with each other to protect the larger organization.

For example: An organization's Incident Response team will need to work closely with its IT & Networking department to alert them of breaches and provide recommendations as to how to better secure their systems.

What other examples can you think of?

These Teams Also Work with Other Organizational Functions

For example, an organization's Marketing and Communications teams use the networks and accounts that IT & Networking manage.

What other examples can you think of?

Business Concerns vs. Security Concerns

The most profitable decision is *not* always the most secure.

Security objectives may be at odds with the overall direction of the



Security Team's Main Goal:

Protect the business's data



Business-At-Large Main Goal:

Maximize profit and improve efficiency

Case Study: What Should the Security Team Do?

An organization's engineering team may propose an innovative but insecure new feature for their flagship product:



Security Team:

The security team would probably advise against developing the feature due to its poor security.

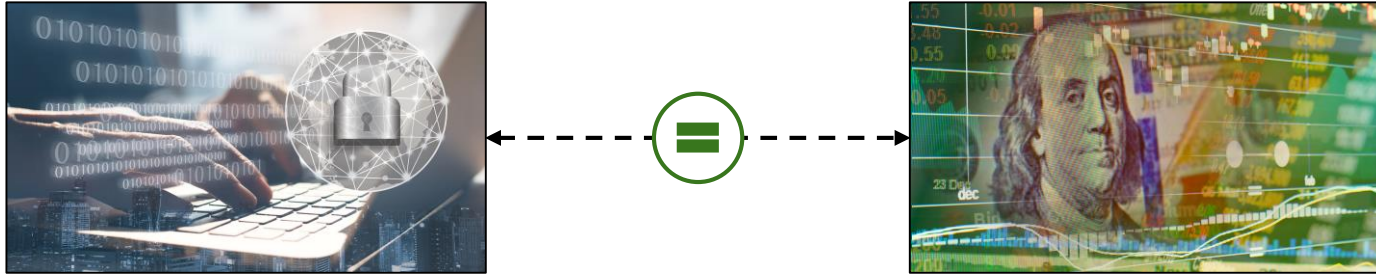


Business-At-Large:

However, the business might decide to develop it under the assumption that the feature profit potential is worth the insecurity.

Case Study: What Should the Security Team Do?

So, the security team must adapt its operations to accomodate a product they *know* is insecure.



Potential Solutions:

Implement more aggressive monitoring on data servers likely to be exposed by the new feature

Advise IT & Networking to implement more sophisticated access controls on important servers and proxies

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

Rather, in effort to turn the largest profit, business are only concerned about providing *adequate protection* for their most *important assets*.

Mark's Reminders:

*Security does not drive a business, it supports it.
Security is there to protect assets, not waste them.*

GRC Framework

The Goals of GRC provide a framework for answering the questions:
“What assets are most important?” and *“What is adequate protection?”*

Risk Management helps an organization identify which assets are most important and determine how they're most likely to be compromised.

Governance provides management frameworks for implementing these security practices in the organization.

Compliance is the field that focuses on ensuring internal security policies are being followed, as well as verifying that the business abides by any relevant security laws.



By important , we mean in a security-business sense:

How can a potential security compromise of this asset affect the profits of the business?

The more significant the loss, the more important the asset

Case Study, Revisited

An organization's software development team may propose 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, at the cost of exposing an isolated data server that contains customer names, usernames, and email addresses, but no other PII (personally identifiable information).

Case Study, Revisited

In this case, the **business objective** of meeting profit targets overrides the **risk** inherent in the strategy.



The security team objects to the feature on the grounds of insecurity. But the business decides that a breach of an isolated server with no truly confidential information would cost less to contain than they would gain by building the feature.

After making a decision, the business would update its security practices to manage the risk they've chosen to undertake, and periodically verify that everyone is following the rules. This is where **governance** and **compliance** kick in.



Activity: Weighing Security and Business Objectives

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

[Activities/Stu_Security_vs_Business/Readme.md](#)

Suggested Time:
10 Minutes



Review: Business vs. Security

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 SOC efficiency.

Review: Business vs. Security

Business Plans

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

Benefits: is that this makes development easier.

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

Recommended Decisions: The business should **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 SOC efficiency.

Review: Business vs. Security

Business Plans

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

Benefits: is that this makes development easier.

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

Recommended Decisions: The business should **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 obviously unacceptable for a private network.

Recommended Decisions: The organization should **reject** this request outright. 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 SOC efficiency.

Review: Business vs. Security

Business Plans

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

Benefits: is that this makes development easier.

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

Recommended Decisions: The business should **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 obviously unacceptable for a private network.

Recommended Decisions: The organization should **reject** this request outright. 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 SOC efficiency.

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

Security Culture Framework

Security Culture

Ensuring that developing a strong organizational security posture begins by ensuring 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. When employees are invested in the organization's security and they understand how to "behave securely", the company is said to have a healthy security culture.

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

- ☐ How important its employees consider security
- ☐ How aware employees are with common security risks
- ☐ Whether its employees know how to avoid insecure behavior



A healthy security culture (Security Hygiene) requires motivating employees to value security and training on how to avoid insecure behavior.

It is always a top down model!

Security Culture Framework Steps

A **Security Culture Framework** identifies problems in an organization's security culture and develops plans to solve them with the following steps:

01

Measure and Set Goals

02

Involve the Right People

03

Create an Action Plan

04

Execute the Plan

05

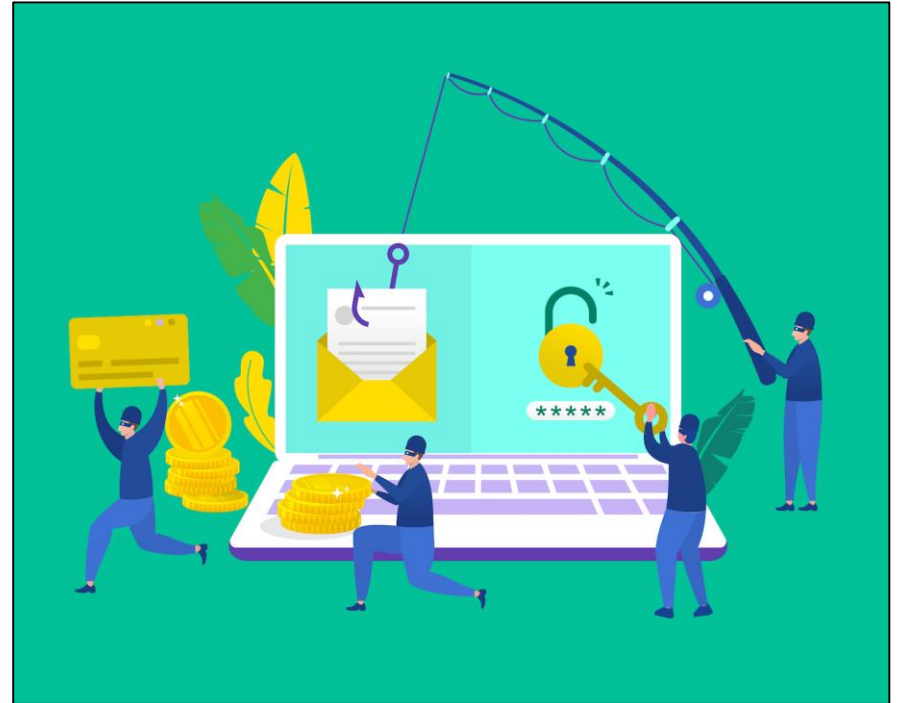
Measure Change

Applying the Framework: Security Scenario

Employees are receiving emails to their company email address from external sources.

The employees are then clicking on links and downloading attachments in these emails.

The security team at the organization has determined that the links/downloads in many of these emails have been determined to contain malware.



Step 1: Measure and Set Goals

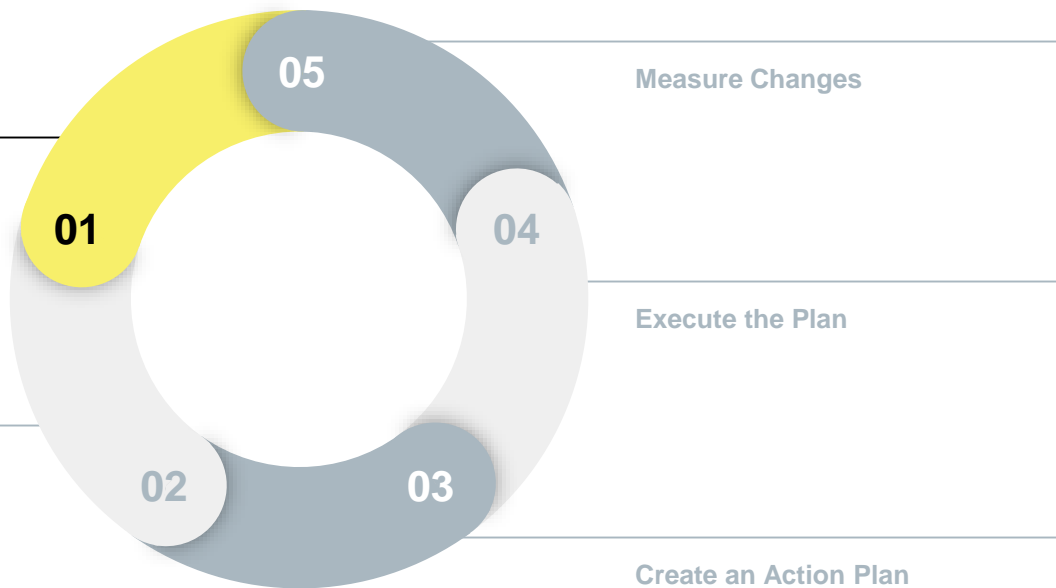
Begin by hiring a pentester to run a phishing campaign against your organization. They will send malicious files to everyone in the organization, and keep track of who downloads them.

Set a Goal of 5% click rate.

Measure and Set Goals:

Use this data to determine two things: What percentage of employees download the files and exactly who downloads them.

Involve the Right People



Step 2: Involve the Right People

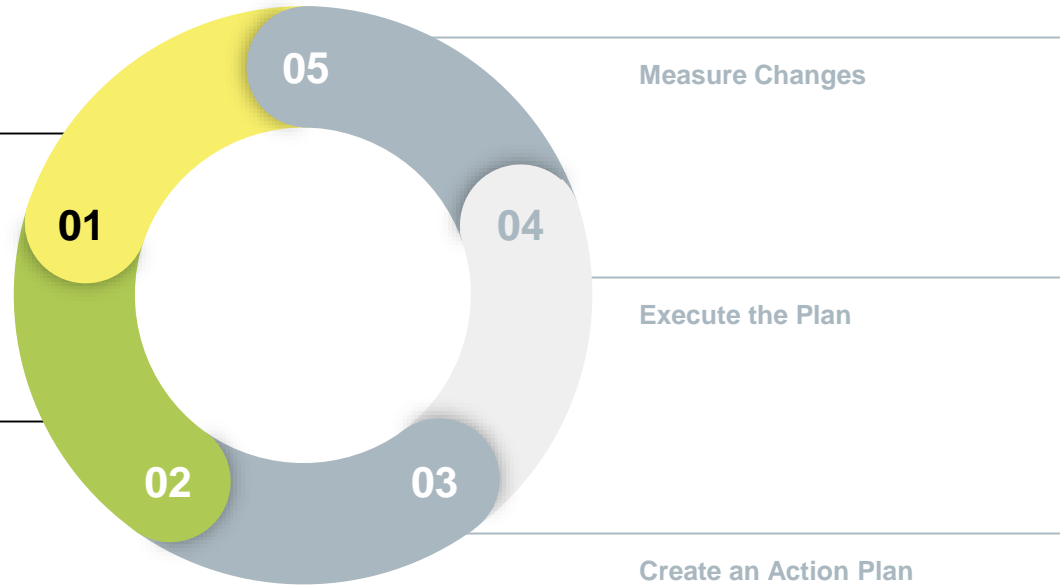
Since this training will affect all members of the organization, you decide to inform the executive team about the problem and your decision to implement training.

Measure and Set Goals:

Use this data to determine two things: What percentage of employees download the files and exactly who downloads them.

Involve the Right People:

Likely inform at least the **CEO and/or CIO, Head of HR**, plus whomever is in charge of internal training and communication.



Step 3: Create an Action Plan

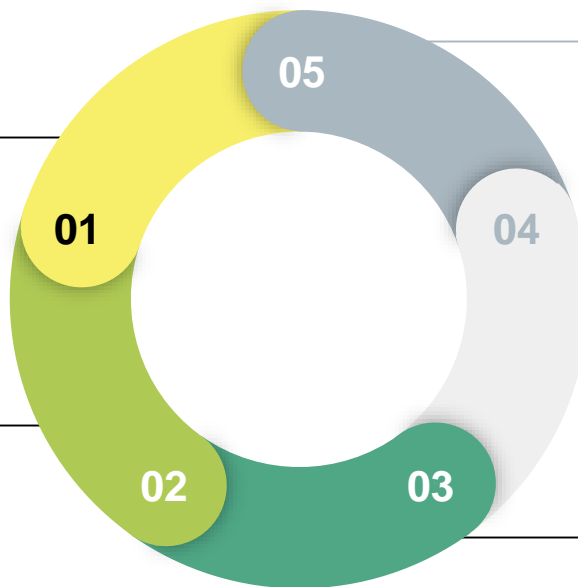
After getting clearance to run the training, plan to deliver an annual Cybersecurity Awareness Training event

Measure and Set Goals:

Use this data to determine two things: What percentage of employees download the files and exactly who downloads them.

Involve the Right People:

Likely inform at least the **CEO and/or CIO, Head of HR**, plus whomever is in charge of internal training and communication.



Measure Changes

Execute the Plan

Create an action Plan

Training will cover: Dangers of Malware + How Malware can spread through phishing and vishing

Step 4: Execute the Plan

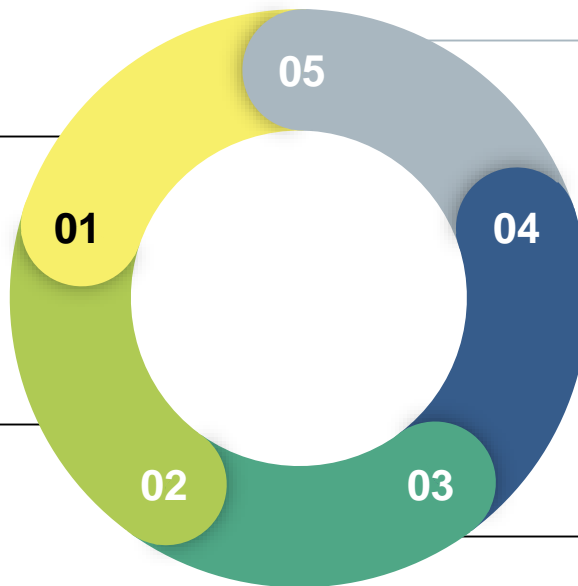
After developing the training, run it and aim to train 25% of employees every quarter in accordance with your original goal.

Measure and Set Goals:

Use this data to determine two things: What percentage of employees download the files and exactly who downloads them.

Involve the Right People:

Likely inform at least the **CEO and/or CIO, Head of HR**, plus whomever is in charge of internal training and communication.



Measure Changes

Execute the Plan:

After developing the training, run it and aim to train 25% of employees every quarter in accordance with your original goal.

Create an action Plan

Training will cover: Dangers of Malware + How Malware can spread through phishing and vishing

Step 5: Measure Change

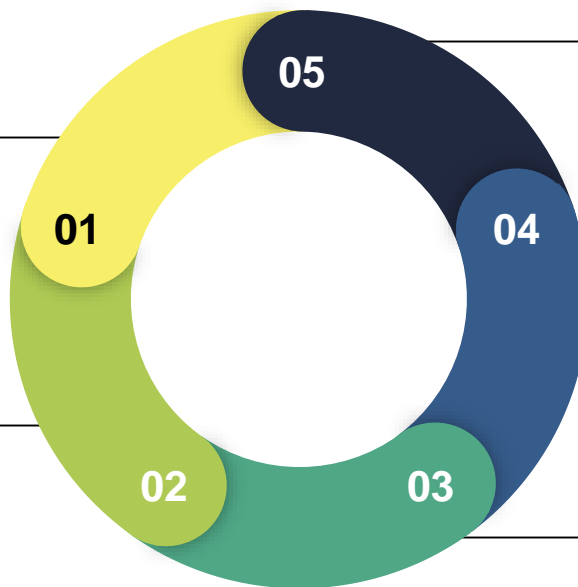
After training the entire company, have the pentesters run the same phishing campaign from before.

Measure and Set Goals:

Use this data to determine two things: What percentage of employees download the files and exactly who downloads them.

Involve the Right People:

Likely inform at least the **CEO and/or CIO, Head of HR**, plus whomever is in charge of internal training and communication.



Measure Changes:

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

Execute the Plan:

After developing the training, run it and aim to train 25% of employees every quarter in accordance with your original goal.

Create an action Plan

Training will cover: Dangers of Malware + How Malware can spread through phishing and vishing



Activity: Applying the Security Culture Framework

In this activity, you'll play the role of a security consultant who's been contracted to help a local bank develop a plan to address a physical security.

[Activities/Stu_Sec_Culture_Part1/Readme.md](#)

Suggested Time:
15 minutes



Security Roles and Responsibilities

Security Roles and Responsibilities

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

01

Which executive roles exist in most companies

02

Which executive roles are relevant to security departments

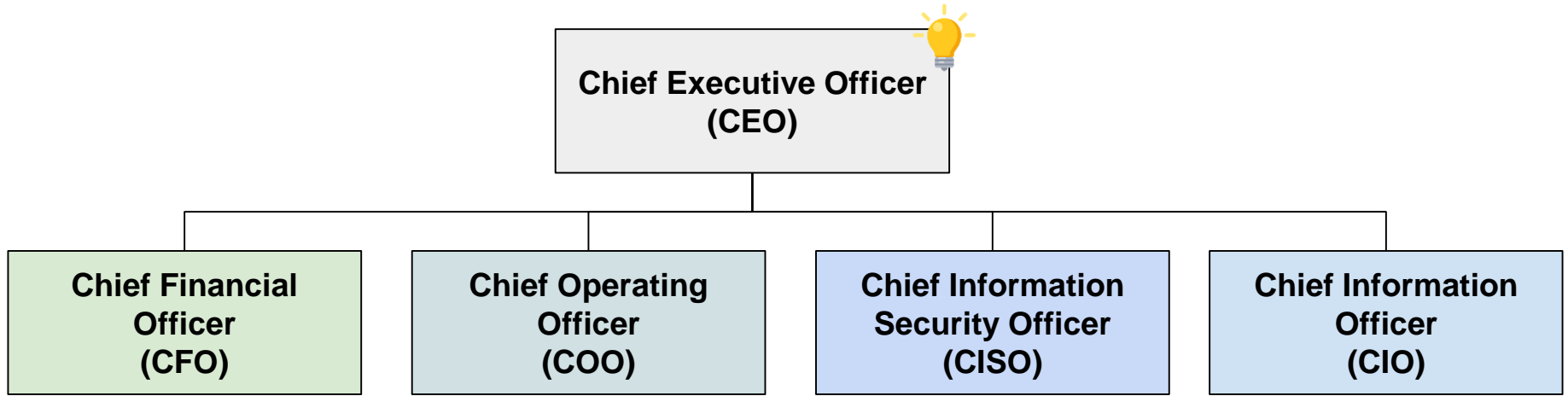
03

The responsibilities of the security department

04

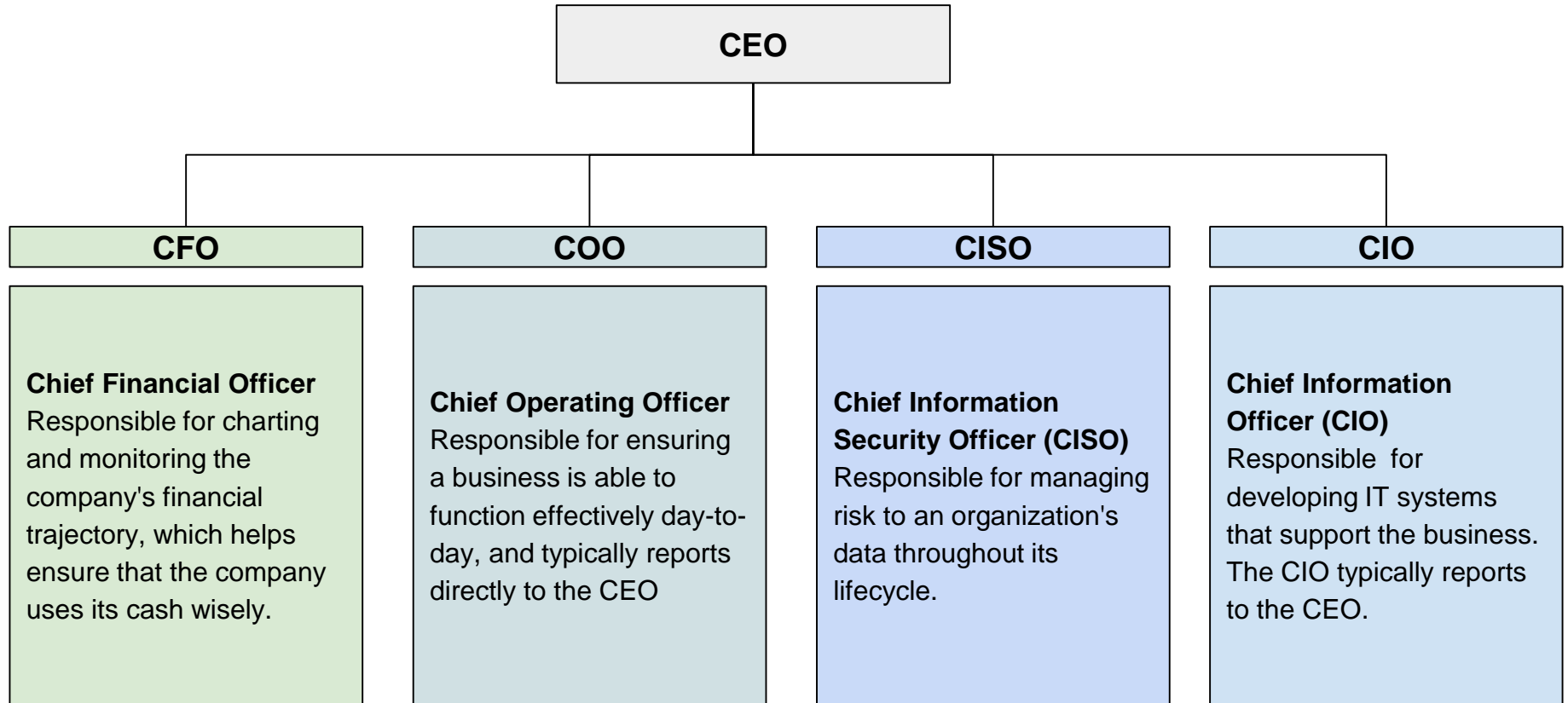
The structure of the security organization

Executive Roles: The Core Leadership Teams

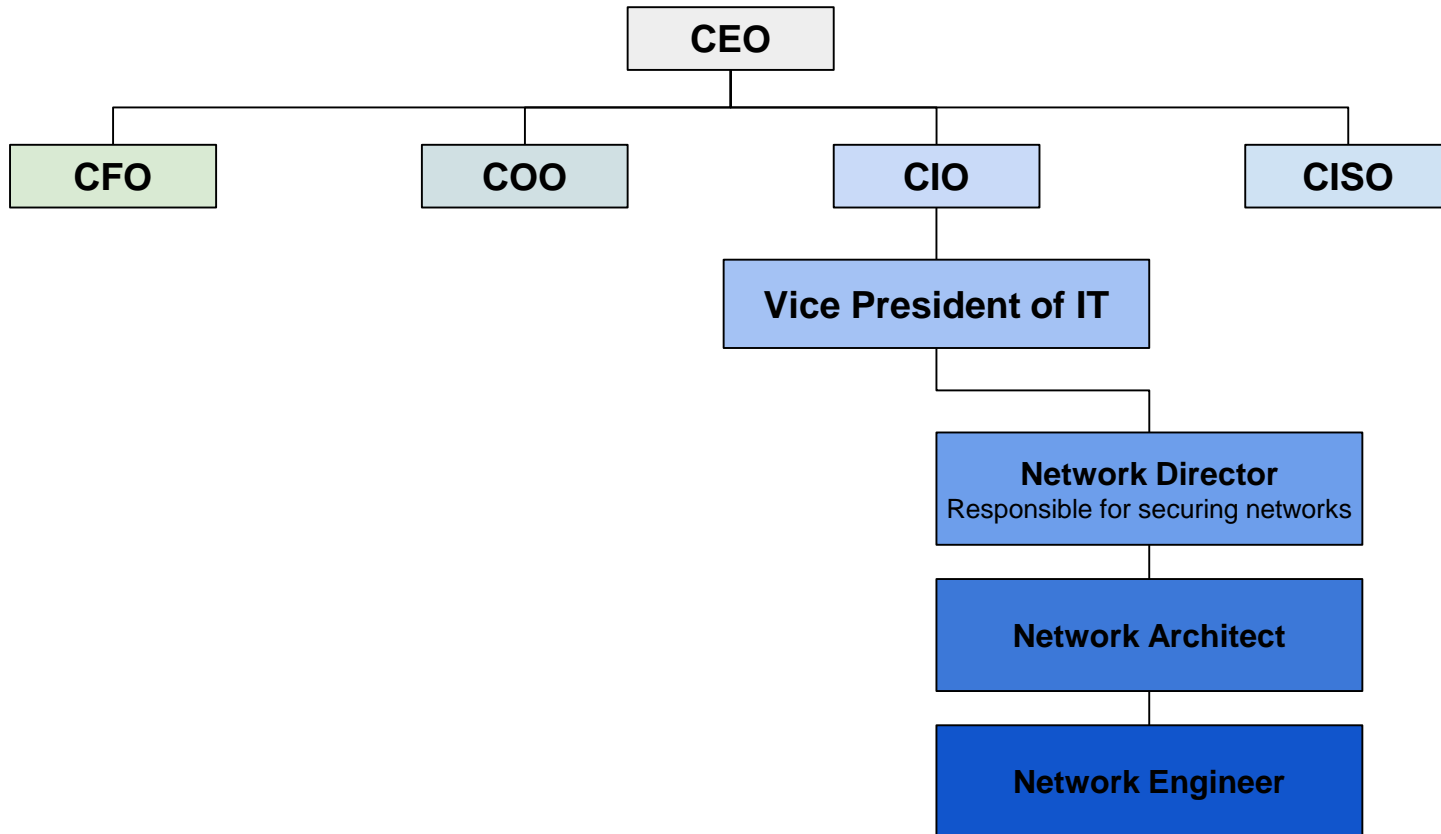


Chief Executive Officer (CEO) is responsible for plotting the overall direction of the company. Reports to the **Board of Directors**. This is a group of individuals, elected by shareholders, which holds the CEO accountable for meeting the demands of those shareholders.

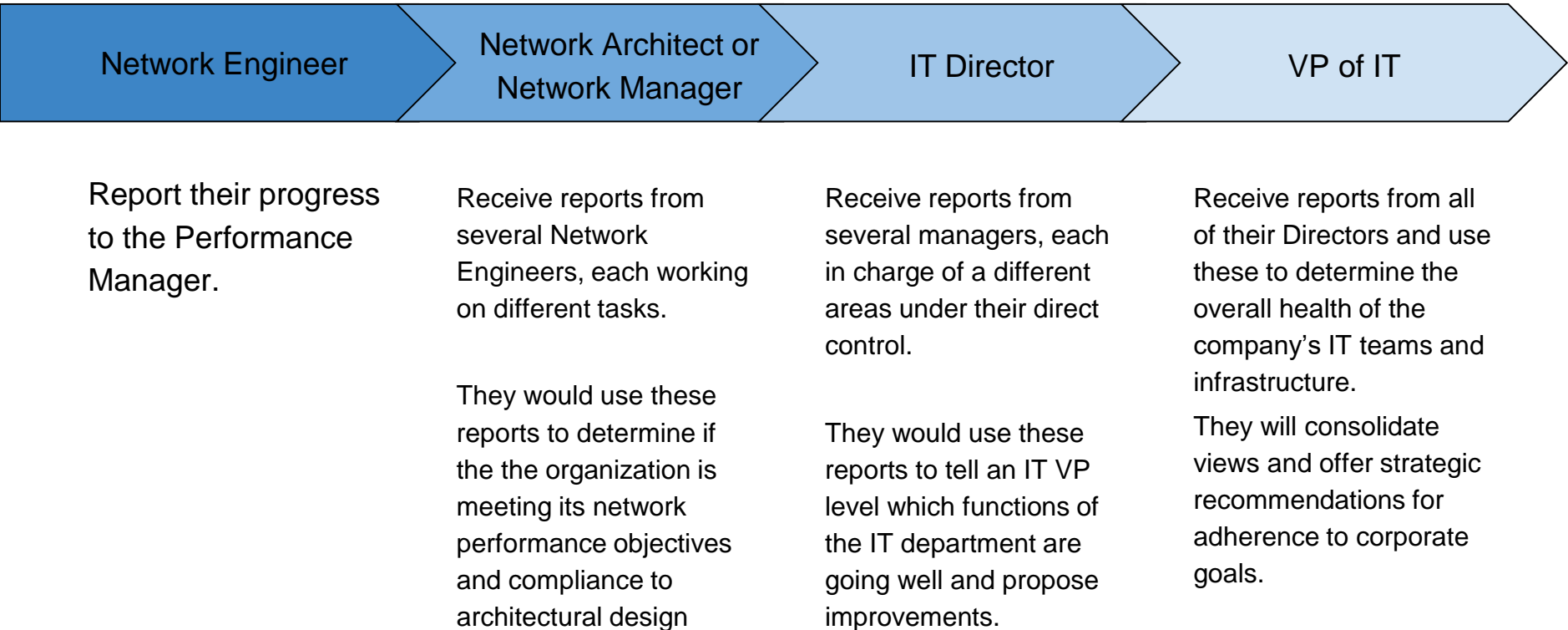
Executive Roles: The Core Leadership Teams



Organizational Structure



Sample Reporting Structure for Networking



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

A **Director of Networking** or **Director of Network Security** is often in charge of networks and network security devices.

A **Network Manager** often has **system administrators**, **network administrators**, and **physical network technicians** on staff.

Incident Response

An **IR Manager**, **NOC Manager**, or **SOC Manager** often manages an Incident Response unit

A **SOC/NOC/IR Manager** is responsible for **SOC Analysts**. Sometimes also the IT Helpdesk

Application Security

An **Application Security Architect** is typically in charge of application security.

An Application Security Architect typically reviews **Application Developers**



Activity: Designing a Security Org Chart

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

[Activities/Stu_Sec_Org_Chart/Readme.me](#)

Suggested Time:
20 Minutes



Take a Break!



Security Culture Framework: Action Plan

Back to Our Security Scenario...

Employees are receiving emails to their company email address from external sources.

The employees are then clicking on links and downloading attachments in these emails.

The security team at the organization has determined that the links/downloads in many of these emails have been determined to contain malware.



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?

Some important considerations when developing a plan:

- **When Will the Plan Be Executed?:**

The SCF and HR Teams agree to run the training once every quarter and train 25% of employees each time. They do this to ensure that they can train 100% of employees over the course of the year, and move people between sessions if necessary.

- **When Will You Measure Progress?:**

The SCF Team decides to run a phishing campaign every quarter. Each time, they'll run the campaign only against the most recently trained cohort. After all cohorts have been trained, they will run a final assessment to evaluate how well everyone adheres to the new guidelines over time.

- **How Will You Quantify Progress?:**

The SCF Team decided to quantify the *click-through rate*, which is the percentage of employees who download malicious links from emails. Their ultimate goal is to bring this number from 10% down to 5% after training.



Activity: Security Culture Framework Part 2

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

[Activities/Stu_Sec_Culture_Part2/Readme.md](#)

Suggested Time:
20 Minutes



Review: Security Culture Framework Part 2 Sample Solution

Involve the Right People: Training 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 decided that *quarterly* training made the most sense.

Metrics and KPIs: The security team wants 0% of employees to allow tailgating after the training has run.

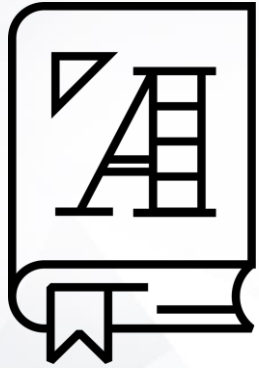
Measurements: One month after each quarter's training, security personnel will audit security cameras, and identify employees who allow others to tailgate. Those who have already been through training will be disciplined. Those who follow training guidelines will be rewarded. Those who have not yet been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



Security Controls



Apart from improving security culture over the *long term*, the security team will want to implement **security controls** in order to address the problem 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, and physical in nature.

Administrative

Example:

Requiring employees to adhere to training guidelines

Technical

Example:

Forcing developers to authenticate using SSH keys rather than passwords

Physical

Example:

Protecting a building by requiring key-card access

Security Controls

Security controls can be implemented to achieve **different goals**.



Preventative controls *prevent* access with physical or logical/technical barriers. Key-card access constitutes a preventive control



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



Detective controls do not protect access to a confidential resource, but instead identify and record attempts at access.



Corrective controls attempt to fix an incident, and possibly prevent reoccurrence.



Compensating controls do not prevent attacks, but restore the function of compromised systems.

We've seen security controls in previous units:

Regardless of type or goal, all controls seek to restrain or respond to **access** to a given resource. Access control is the practice of controlling who can access which resources.

Linux

- File permissions act as access controls by preventing users from modifying files they don't own.
- O/S Hardening

Networks

- Firewalls control access to networks.
- IDS/IPS
- Proxies
- UBA Controls
- Oversight of environment

Incident Response

- Monitoring systems act as detective control.
- Response to unauthorized activity
- Security Compliance reporting



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

Defense in Depth

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

01

Hiding it 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 them 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, they still can't easily compromise the server. Since it forces users to authenticate with SSH keys *and* passwords, they can't easily brute-force the login.

03

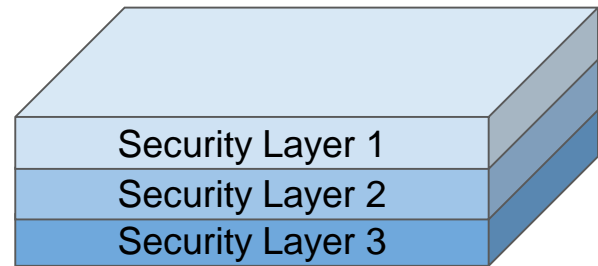
If an attacker *does* steal both a valid SSH key *and* its password, they would only be able to compromise the server for a limited amount of time, since the stolen key would be invalidated in at most three months.

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**.

Ensuring redundancy eliminates the inherent risk of **single points of failure**.

If the system only had a single control, that control would be its single point of failure. An attacker could compromise the system by breaking just a *single* control.





Activity: Implementing Security Controls

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

`Activities/Stu_Sec_Controls/Readme.md`

Suggested Time:
20 Minutes



Your Turn: Implementing Security Controls

Instructions:

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

The training plan you've already developed is a *personnel security* measure, and won't drastically reduce tailgating rates until at least next year. Consider *physical*, *technical*, or *procedural* controls that would result in immediate reductions in employee piggybacking.

Record *three* different controls. They can be of any type you'd like. Answer the following questions about each control:

- **How does this reduce piggybacking?**
- **What is the cost of implementation?**
- **What percentage reduction in piggybacking rates do you expect?**

Review: Implementing Security Controls

Sample Solution Controls:

Implement a Turnstile

- The organization could implement turnstiles in all of its data centers. These turnstiles would only allow one person through at a time, and require employees to scan an ID card to step through.
- This requires installing the system at all sites, and issuing key cards to all employees, both of which incur significant overhead. However, a financial organization might deem the added security of such *physical access controls* well worth it.

Encrypt Top-Secret Data

- The attacker wouldn't have been successful if they'd broken into the data facility and stolen *encrypted* financial records. The organization could choose to encrypt all of its top-secret data, and only allow it to be decrypted by a single server, verified by digital signature.
- As an advanced note, the company could then choose to allow access to that decrypted data via 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



Devise possible controls, in addition to training, that can mitigate risk

Looking Forward...





What we learned today will lead into **governance**...

Governance is the field of enforcing these standards, policies, and procedures, such that they are always obeyed.

Now that we have a good understanding of how organizations begin to develop best practices, we can begin to study how it codifies them into standards and applies ideas from governance to keep them enforced.

Class Objectives

By the end of class today, students 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 the security department
-  Identify appropriate security controls for a given resource and situation