FRSecure CISSP Mentor Program

2023

Class #10 – Domain 7 part 2

Security Operations

Ron Woerner

Forrester, Sr Consultant
Cyber-AAA, Founder & CEO & vCISO
Bellevue University, CyberSecurity Studies Professor

CISSP® MENTOR PROGRAM – SESSION FOUR

WHOAMI

Ron Woerner, CISSP, CISM

Chief Security Officer, Cyber-AAA

Sr Consultant, Forrester

ISC2 North American Advisory Council

https://linktr.ee/cyberron

https://www.linkedin.com/in/ronwoerner/

@ronw123

Hackers Wanted

TEDx Omaha

Please...Don't Shoot the....
PIANO PLAYER
He's Doing The Best He Can!

CISSP® MENTOR PROGRAM – SESSION TEN

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.
- **DO NOT share or post copywritten materials. (pdf of book)**

GETTING GOING…

Managing Risk!

Study Tips:

- Study in small amounts frequently (20-30 min)
- Flash card and practice test apps help
- Take naps after heavy topics (aka Security Models)
- Write things down, say them out loud
- Use the Slack Channels
- Exercise or get fresh air in between study sessions

Let's get going!

CISSP® MENTOR PROGRAM – SESSION TEN

GETTING GOING…

Great job last week! We’re almost through Domain 7 (Security Operations)

- Shout Out to Chris for a great class!
- Ready for more?
  - We are close to the finish
  - USE the Discord channel to connect with others
  - Ask questions in #questions in slack
- Check-in.
- How many have read Domain 7?

Let’s get going!

CISSP® MENTOR PROGRAM – SESSION TEN

DAD JOKE

Before we get too deep into this.

How about a dum

It's inappropriat
joke“ if you're n

HAHAHAHA

Moving on…

DOMAIN 7
SECURITY OPERATIONS

Review

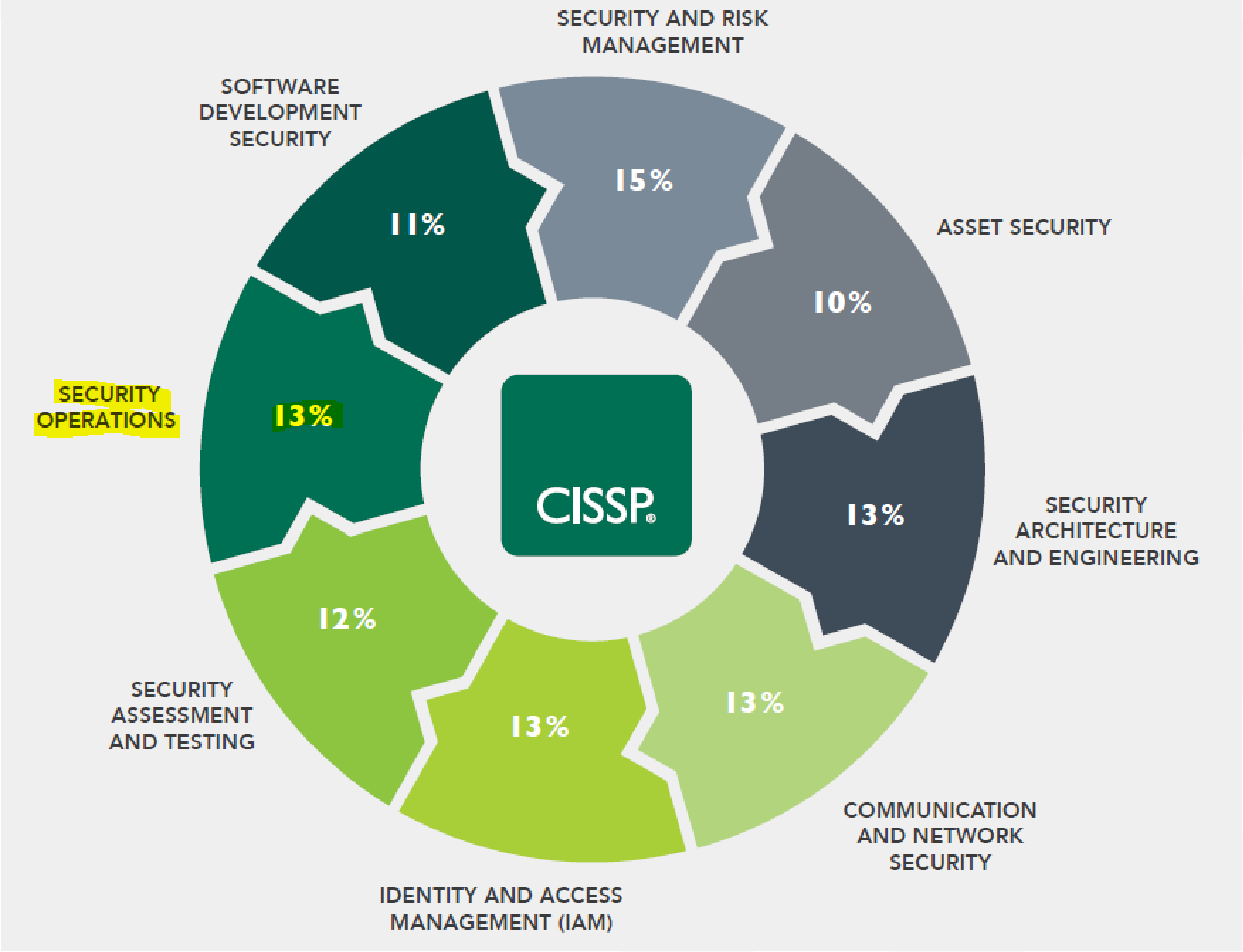
The Security Architecture and Engineering domain covers topics relevant to implementing and managing security controls across a variety of systems. Secure design principles are introduced that are used to build a security program, such as secure defaults, zero trust, and privacy by design. Common security models are also covered in this domain, which provide an abstract way of viewing a system or environment and allow for identification of security requirements related to the CIANA+PS principles. Specific system types are discussed in detail to highlight the application of security controls in a variety of architectures, including client- and server-based systems, industrial control systems (ICSs), Internet of Things (IoT), and emerging system types like microservices and containerized applications.

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7: SECURITY OPERATIONS

CISSP **Exam Overview**

Caution!
Concepts overlap between domains.



https://www.isc2.org/-/media/ISC2/Certifications/Ultimate-Guides/UltimateGuideCISSP-Web.ashx

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7: SECURITY OPERATIONS – OVERVIEW

Part 1 – Session 9

- Understand and comply with investigations
- Conduct logging and monitoring activities
- Perform Configuration Management (CM) (e.g., provisioning, baselining, automation
- Apply foundational security operations concepts
- Apply resource protection
- Conduct incident management
- Operate and maintain detective and preventative measures

Part 2 – Session 10

- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

https://www.isc2.org/Certifications/cissp/Certification-Exam-Outline

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT INCIDENT MANAGEMENT

Quick Review

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT INCIDENT MANAGEMENT

Quick Review

First, you MUST define what an “incident” is.

An **event** is something that happened.

An **incident** is ~~something that happened~~ an event with a negative consequence.

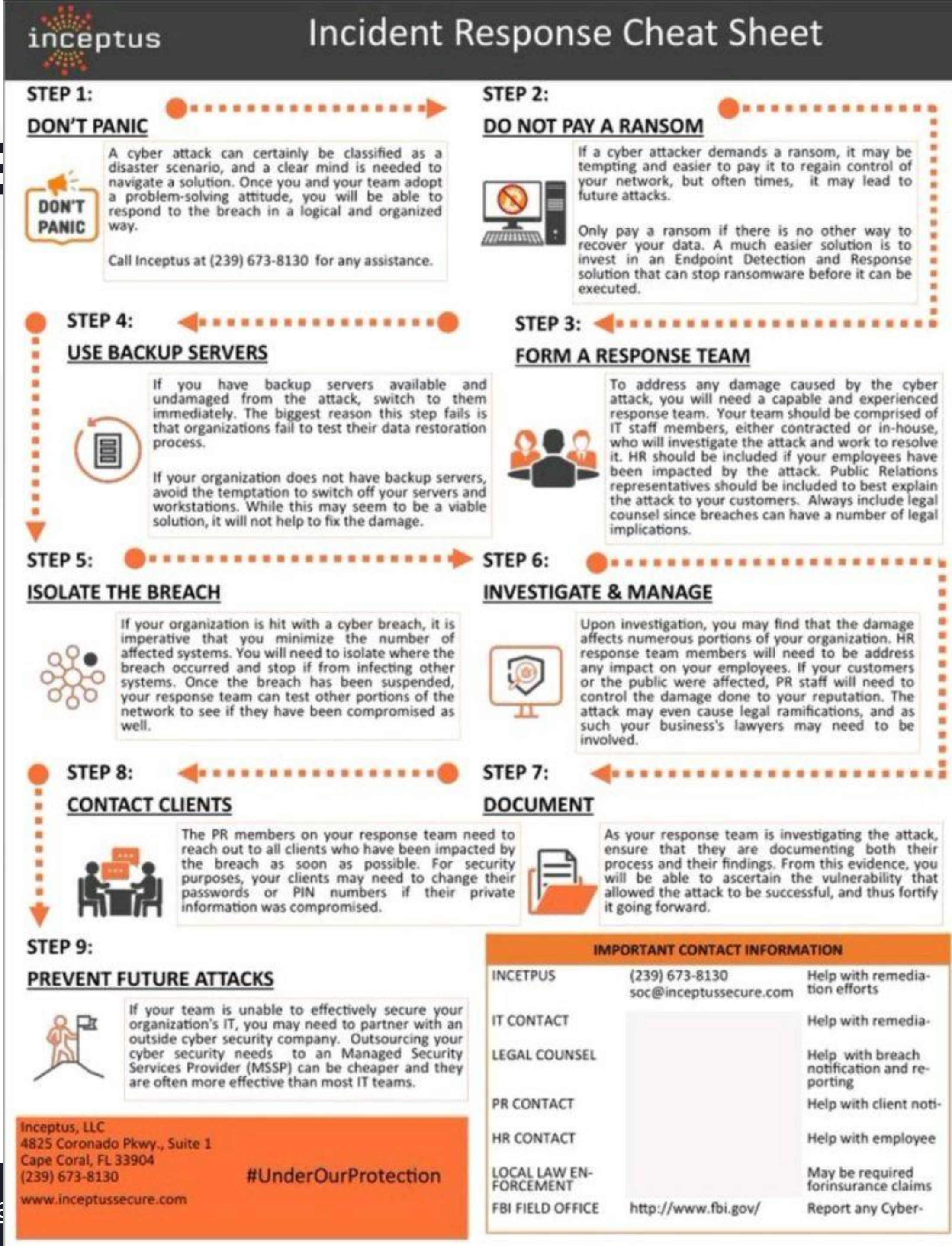
See “official” definitions at https://csrc.nist.gov/glossary

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPE

CONDUCT INCIDENT MANAGEMENT

https://www.linkedin.com/posts/brcyrr_cybersecurity-infosec-blueteam-activity-7064527718859571201-Ds2j



inceptus

Incident Response Cheat Sheet

STEP 1:

DON'T PANIC

A cyber attack can certainly be classified as a disaster scenario, and a clear mind is needed to navigate a solution. Once you and your team adopt a problem-solving attitude, you will be able to respond to the breach in a logical and organized way.

Call Inceptus at (239) 673-8130 for any assistance.

STEP 2:

DO NOT PAY A RANSOM

If a cyber attacker demands a ransom, it may be tempting and easier to pay it to regain control of your network, but often times, it may lead to future attacks.

Only pay a ransom if there is no other way to recover your data. A much easier solution is to invest in an Endpoint Detection and Response solution that can stop ransomware before it can be executed.

STEP 3:

FORM A RESPONSE TEAM

To address any damage caused by the cyber attack, you will need a capable and experienced response team. Your team should be comprised of IT staff members, either contracted or in-house, who will investigate the attack and work to resolve it. HR should be included if your employees have been impacted by the attack. Public Relations representatives should be included to best explain the attack to your customers. Always include legal counsel since breaches can have a number of legal implications.

STEP 4:

USE BACKUP SERVERS

If you have backup servers available and undamaged from the attack, switch to them immediately. The biggest reason this step fails is that organizations fail to test their data restoration process.

If your organization does not have backup servers, avoid the temptation to switch off your servers and workstations. While this may seem to be a viable solution, it will not help to fix the damage.

STEP 5:

ISOLATE THE BREACH

If your organization is hit with a cyber breach, it is imperative that you minimize the number of affected systems. You will need to isolate where the breach occurred and stop if from infecting other systems. Once the breach has been suspended, your response team can test other portions of the network to see if they have been compromised as well.

STEP 6:

INVESTIGATE & MANAGE

Upon investigation, you may find that the damage affects numerous portions of your organization. HR response team members will need to be address any impact on your employees. If your customers or the public were affected, PR staff will need to control the damage done to your reputation. The attack may even cause legal ramifications, and as such your business's lawyers may need to be involved.

STEP 7:

DOCUMENT

As your response team is investigating the attack, ensure that they are documenting both their process and their findings. From this evidence, you will be able to ascertain the vulnerability that allowed the attack to be successful, and thus fortify it going forward.

STEP 8:

CONTACT CLIENTS

The PR members on your response team need to reach out to all clients who have been impacted by the breach as soon as possible. For security purposes, your clients may need to change their passwords or PIN numbers if their private information was compromised.

STEP 9:

PREVENT FUTURE ATTACKS

If your team is unable to effectively secure your organization's IT, you may need to partner with an outside cyber security company. Outsourcing your cyber security needs to an Managed Security Services Provider (MSSP) can be cheaper and they are often more effective than most IT teams.

IMPORTANT CONTACT INFORMATION		
INCETPUS	(239) 673-8130 soc@inceptussecure.com	Help with remediation efforts
IT CONTACT		Help with remedia-
LEGAL COUNSEL		Help with breach notification and reporting
PR CONTACT		Help with client noti-
HR CONTACT		Help with employee
LOCAL LAW ENFORCEMENT		May be required forinsurance claims
FBI FIELD OFFICE	http://www.fbi.gov/	Report any Cyber-

Inceptus, LLC
4825 Coronado Pkwy., Suite 1
Cape Coral, FL 33904
(239) 673-8130
www.inceptussecure.com

#UnderOurProtection

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT INCIDENT MANAGEMENT

Quick Review

https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/

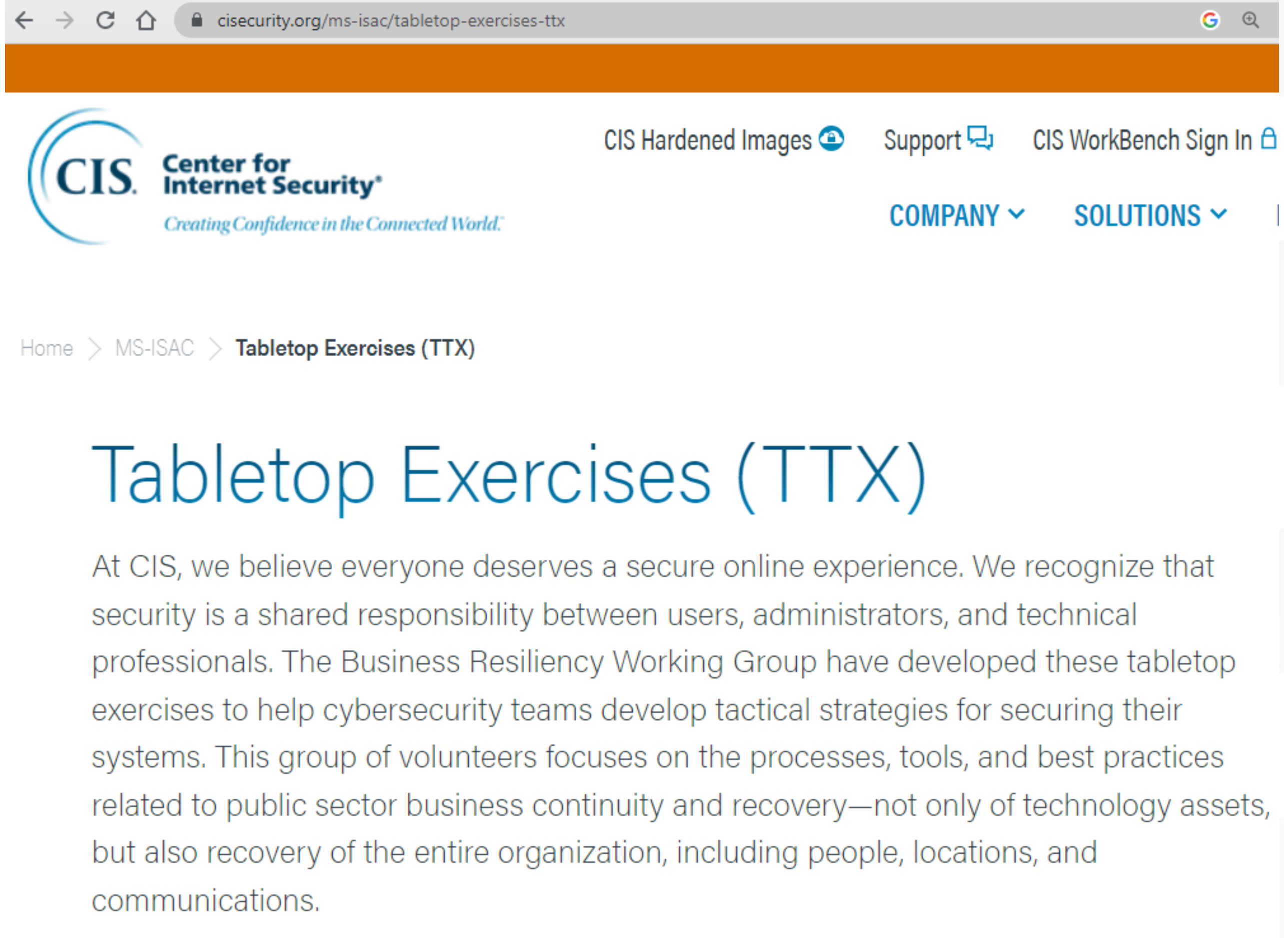
CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT INCIDENT MANAGEMENT

Quick Review

https://www.cisecurity.org/ms-isac/tabletop-exercises-ttx


cisecurity.org/ms-isac/tabletop-exercises-ttx
CIS Center for Internet Security®
Creating Confidence in the Connected World.
CIS Hardened Images
Support
CIS WorkBench Sign In
COMPANY
SOLUTIONS
Home
MS-ISAC
Tabletop Exercises (TTX)

Tabletop Exercises (TTX)

At CIS, we believe everyone deserves a secure online experience. We recognize that security is a shared responsibility between users, administrators, and technical professionals. The Business Resiliency Working Group have developed these tabletop exercises to help cybersecurity teams develop tactical strategies for securing their systems. This group of volunteers focuses on the processes, tools, and best practices related to public sector business continuity and recovery—not only of technology assets, but also recovery of the entire organization, including people, locations, and communications.

DOMAIN 7 – SECURITY OPERATIONS

IMPLEMENT AND SUPPORT PATCH AND VULNERABILITY MANAGEMENT

Patch Management

A generic security patch process incorporating all stakeholders must include the following:

Vulnerability detection – Scanning, researcher, user reporting a bug, etc.

Patch publication - By the vendor or development team, once the vulnerability is verified and relevant code is written to address it.

Evaluation - Patch applicability by each organization's administrative personnel to determine if the patch is needed in each environment.

Testing - Ensure the patch won’t introduce problems.

Apply and Track - Ensure the patch doesn’t have a negative impact on functionality.

Rollback - If issues are encountered.

Documentation - Of the system including the patch, which becomes the

DOMAIN 7 – SECURITY OPERATIONS

IMPLEMENT AND SUPPORT PATCH AND VULNERABILITY MANAGEMENT

Vulnerability Management

Vulnerabilities are one-half of risk, and a significant part of a security practitioner's responsibilities

Threat hunting – Practice of looking for threats that evade the organization's existing security solutions.

Vulnerability scanning - Detect known vulnerabilities like insecure configurations or unpatched software, a key detective control.

Red teaming - Targeted form of testing for vulnerabilities.

Penetration testing – Human-run tests, usually broader in scope then red teaming.

Bug bounties- rules of the engagement may require that the tester only document, but not exploit, any vulnerabilities they find.

DOMAIN 7 – SECURITY OPERATIONS

Understand and Participate in Change Management Processes

Change Management

Change management is concerned with keeping the organization operating effectively and moving from one secure state to another.

Standard changes – Low risk and are considered unlikely to have a negative impact, so they are preapproved to reduce operational overhead.

Normal changes - Changes require the full change management process of request and review before implementing.

Emergency changes - Change is made as needed to deal with the incident or emergency, and all details are documented for later review.

DOMAIN 7 – SECURITY OPERATIONS

Implement Recovery Strategies

All recovery metrics should be driven by business decisions of criticality and cost.

Recovery is measured by several key metrics, such as the following:

Recovery time objective (RTO) – The amount of time after an incident or disaster that passes before the system or process is recovered using contingency procedures

Recovery point objective (RPO) - The amount of data loss tolerable when a disaster occurs, usually expressed as a number of transactions or data points. RPO can also be expressed using time, like an RPO of no more than one day of data.

Maximum tolerable or allowable downtime (MTD or MAD) - The amount of time the organization can survive without an asset or process, after which the organization may no longer be viable. RTO should always be less than the MTD; otherwise, recovery is a moot point as the organization will cease to function before it occurs.

DOMAIN 7 – SECURITY OPERATIONS

Implement Recovery Strategies

Backup Storage Strategies

Full backups – Take the longest to run and use the most space.

Differential backups- Capture all data changed since the last full backup, meaning they run faster and require less storage.

Incremental backups- Capture all data that has changed since the last full or incremental backup, meaning they capture the smallest amount of data and run the fastest.

When restoring, incremental backups will typically take the longest to restore from, as they require the last full backup and all incremental backups made since, while differential backups require only the last full and differential backup.

Implement Recovery Strategies

Backup Storage Strategies

- We must always balance the cost and speed desired for backup and recovery.
- Length of data retention requirements.

3-2-1 Backup Strategy

- A common rule for a robust backup strategy is the 3-2-1 rule. This states that at least three copies of data should be kept: two stored locally or onsite, including the main copy of the data, and one copy stored offsite. In this way, simple data issues or hardware failures can be easily solved with the local backup, and more drastic issues like the destruction of a facility can be addressed by restoring from the offsite backup.

Implement Recovery Strategies

Integrity and Confidentiality of Backups

- The integrity of the data backed up is also of crucial concern
- Some dedicated backup systems offer the capability to perform integrity checks of data after it is written to backup media like hard disks or tape drives.
- Performing test restorations to verify the data is also a best practice to both double-check the integrity and ensure the correct data has been backed up.

Implement Recovery Strategies

Integrity and Confidentiality of Backups

- It is important to treat backup media with at least the same level of security controls.
- In many cases, alternative or additional controls will be required.
- Access requirements for data on backup media may also differ.
- Backup media and the data it contains should be tracked in the asset inventory, with full consideration during risk assessment and mitigation

Implement Recovery Strategies

RAID (Redundant Array of Inexpensive Disk)

- Pooling multiple disks, which may be **cheaper** than a single disk of equivalent size, to provide benefits of **increased space**, **increased read/write speeds, data fault tolerance**, or some combination of all three.

- A **Raid Controller** is used to handle data operations.

- **Striping** breaks incoming data into smaller pieces that are written across multiple drives to increase read/write speed.
- **Mirroring** makes copies of data and writes them across multiple drives, while parity calculations use a mathematical model to allow striped data to be reconstructed even if some stripes are lost.

DOMAIN 7 – SECURITY OPERATIONS

Implement Recovery Strategies

RAID (Redundant Array of Inexpensive Disk)

RAID 0 – Striped disk array with no fault tolerance; the primary benefit is increased read/write performance.

RAID 1 - Mirrored array that provides fault tolerance, but no read/write performance benefit.

RAID 5 - Striping with a parity array, which increases read/write performance and provides fault tolerance.

RAID 0+1 and 1+0 - Nested RAIDs that implement both functions of RAID 0 and 1 in different orders. 0+1 is a striped array of mirrors, while 1+0 is a mirrored array of stripes. Both combine fault tolerance with increased performance.

DOMAIN 7 – SECURITY OPERATIONS

Implement Recovery Strategies

Cloud

- Cloud services like software as a service (SaaS) are often configured for high availability, automatic data replication, and data durability, which is the proactive management of data to preserve integrity and availability.
- Can also be used solely for backup purposes, due to its availability and relatively low costs
- Storage solutions like infrastructure as a service (IaaS) or platform as a service (PaaS) may be appropriate
- PaaS may be utilized to create an environment similar to the organization's production environment, like a database, that can be easily switched over in the event of a disruption.
- Loss of physical control over data needs to be evaluated against cost savings.

Implement Recovery Strategies

Recovery Site Strategies

- Site configuration and location should be driven by the cost-benefit analysis of the speed of recovery it can support and its proximity to the primary location.
- The further away a recovery site is, the longer it will take key personnel to reach it in the event that operations must be moved.
- Organizations with very short RTO and MTD windows, dividing staff, resources, and processes permanently between multiple sites is an acceptable, but costly, solution known as a mirror site

Implement Recovery Strategies

Recovery Site Strategies

- **Cold site -** is an empty facility that must be provisioned with equipment and utilities before being useful, which takes time and does not support a short RTO, but it also does not incur the high costs of duplicate infrastructure before an incident.
- **Warm sites -** have some equipment but also require some buildout.
- **Hot site -** has the same infrastructure and data as the primary site, which is costly but useful for meeting a short RTO or RPO.
- **Mobile site -,** which is a data processing facility that can be deployed quickly wherever needed.
- **Cloud bursting -** is a relatively new recovery strategy that utilizes cloud services temporarily in the event of a disaster.

Implement Recovery Strategies

Multiple Processing Sites

- Safeguard against impacts of a disaster by proactively designing **processes or functions that span multiple processing sites**, which should be geographically distributed to prevent multiple sites being impacted by the same disaster.

- Benefit to multiple processing sites is the **redundancy built in**. The same redundancy has the drawback of higher costs for rent, personnel, and equipment.

- Technical **challenges of replicating and synchronizing data** among multiple processing sites, for which solutions like disk or database mirroring may be useful.

- Any migration to a cloud or outsourced service provider, there are **increased risks** related to losing control over data.

Implement Recovery Strategies

System Resilience, High Availability, Quality of Service, and Fault Tolerance

Resilience - describes the ability of a system or process to resist failure, relies on robust design that accounts for failure and builds in corrective actions. Can detect stuck or hung processes and automatically restart them by terminating and retrying the process.

High availability (HA) - configurations are one option—through the use of technologies like load balancers or clusters, a system provides redundancy and dynamic rerouting of requests if one component fails.

Quality of service (QoS) - is frequently implemented for networking technologies, to allow for prioritization of highly important traffic in the face of limited bandwidth.

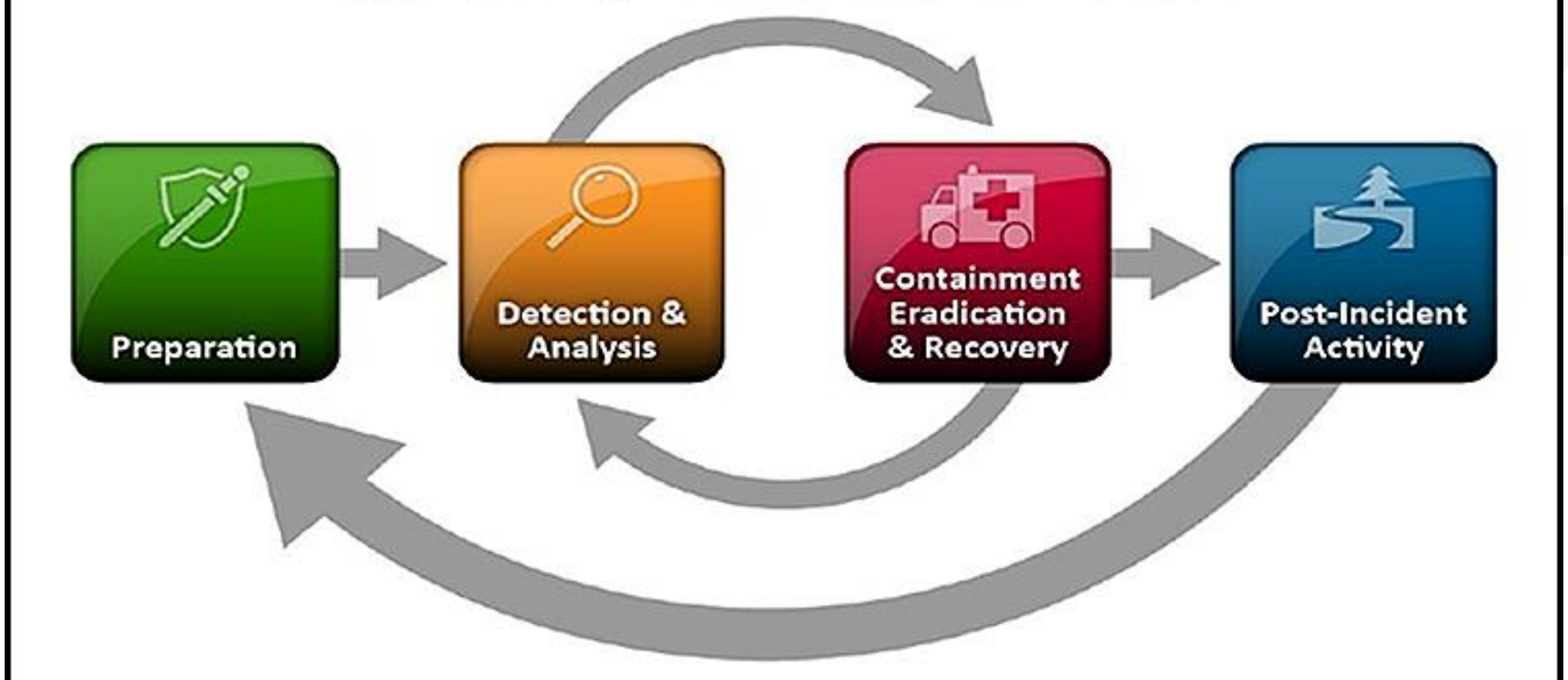
Fault-tolerant systems - can, as the name implies, tolerate a fault of hardware, software, or data handling and continue to function.

CISSP® MENTOR PROGRAM – SESSION TEN

CYBERSECURITY INCIDENT RESPONSE LIFE CYCLE

NIST SP 800-61 rev2

Cyber Security Incident Response Life Cycle



Source: U.S. Dept. of Commerce; National Institute of Standards & Technology (NIST)

CISSP® MENTOR PROGRAM – SESSION TEN

CYBERSECURITY INCIDENT RESPONSE LIFE CYCLE - RESPONSE

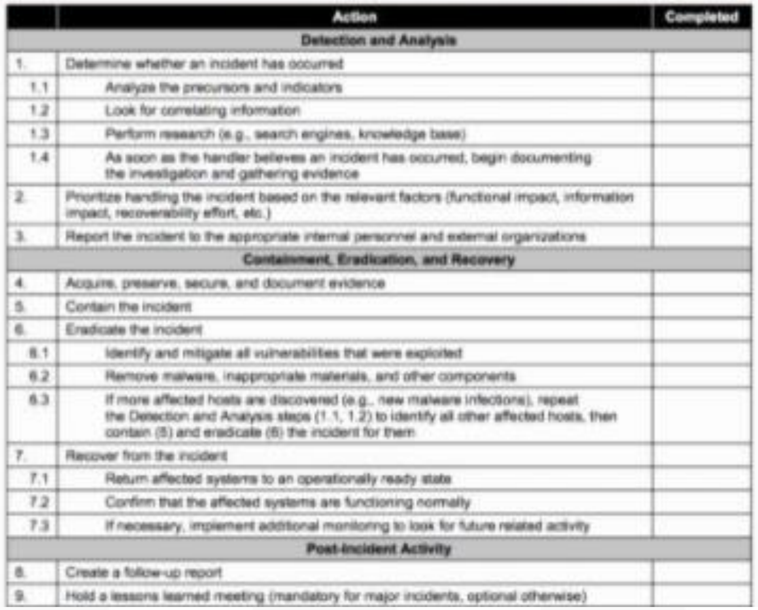
Set your Response Strategy & Plan

Checklists, checklists, checklists

Document, document, document

- https://us-cert.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pdf
- https://www.cisecurity.org/white-papers/cyber-incident-checklist/

Incident Checklist – Sample from NIST



	Action	Completed
Detection and Analysis		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Implement Disaster Recovery Process

Intro

BIA – Business Impact Analysis

BC – Business Continuity is focused on the continuity of the organization's business operations, which rely on systems and data that are handled in the DR plan

DR - is a subset of BC and is focused on restoring IT services and functions when a disaster occurs.

BCDR - The combined process areas and associated plan documents are sometimes referred to as BCDR.

RTOs and RPOs must be defined

Recovering cross-functional organization processes requires the participation of a cross-functional team

Implement Disaster Recovery Process

DOMAIN 7 – SECURITY OPERATIONS

Implement Disaster Recovery Process

Response

#1 Life, health, and safety - of personnel, which is always the primary concern.

Coordinated response - actions with direction and oversight of a designated disaster or crisis coordinator are crucial to provide focus.

Clear and consistent communications - must be made to various stakeholders including employees, executive management, and possibly members of the public or law enforcement.

Document - everything done to support post-disaster reviews, as well as to support any evidence needed for insurance or legal action.

DOMAIN 7 – SECURITY OPERATIONS

Implement Disaster Recovery Process

Personnel

Novel risks to personnel - such as new personnel performing equipment installation in an unfamiliar environment.

Security practitioner must account for these - when planning and ensure BC or DR plans include measures to minimize the risks

BCDR plans must also document roles and responsibilities - for personnel needed to continue the organization's critical processes.

Named personnel and contact details should be documented - in the plan for vital functions, like disaster declaration or crisis communications, to ensure clear assignment of duties

Personnel practices like job rotation and cross-training - can support contingency operations, as personnel capable of performing multiple roles can be critical in an emergency.

Implement Disaster Recovery Process

Food and Other Needs

Plans should include arrangements for dealing with **basic needs like housing and food** for not only personnel but family members as well.

Transportation to the alternate site should be considered.

Tempers may be short, hygiene supplies may be limited, and **people do need to eat**.

Break time diversions like video games or a nap room can be vital for employees under stress.

Costs like catering or entertainment associated with disaster operations may even be **covered by cyber insurance** as part of recovery costs!

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

Implement Disaster Recovery Process

Food and Other Needs

Plans should include arrangements for de **ood** for not only personnel but family members as

Transportation to the alternate site shoul

Tempers may be short, hygiene supplies r

Break time diversions like video games o nder stress.

Costs like catering or entertainment asso be **covered by cyber insurance** as part of rec

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

Implement Disaster Recovery Process

Communications

DOMAIN 7 – SECURITY OPERATIONS

Implement Disaster Recovery Process

Communications

Crisis communications **are difficult** due to limited or rapidly evolving information and the need to provide timely notifications to a wide variety of internal and external stakeholders.

Crisis communications plan that accounts for the **dynamic environment** and provides clear information is essential.

“**one voice**” principle is essential to crisis communications and dictates that the organization should have a unified voice when communicating, especially with outside stakeholders like press or the public.

This principle should be **documented** and included as **part of training**—any personnel who receive requests from media or other outsiders must refrain from making a statement and instead refer to the appropriate communications contact.

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

Implement Disaster Recovery Process

Communications

Internal stakeholders - include employees and management, who need not only information about the incident but also instructions on how to participate in the response, should include security-relevant information.

Methods and paths for communicating with internal stakeholders can include active methods like a phone tree, which requires a response from each person called, or passive, like a message posted on a website that employees can access.

The method chosen should account for the criticality of the personnel receiving it and the information being conveyed.

Implement Disaster Recovery Process

Communications

External stakeholders - can include customers or users, members of the public, and business partners or vendors who are likely to be impacted by the organization's contingency operations.

Law enforcement and response providers like DFIR firms are also key external stakeholders who will need information and access to perform their jobs related to the response operations.

Methods and paths of communication to external stakeholders may be determined by legal or contractual obligations, such as privacy notifications in the event of a breach. Active and passive methods should be used depending on the situation, such as actively mailing or calling customers to notify them or issuing a press releases for general consumption.

Implement Disaster Recovery Process

Assessment

- Similar to risk assessment—the primary goal is to **ascertain the impact** and prioritize steps needed to address it.
- Identifying the **nature and source of the disaster**, such as man-made or natural, and determining the priority of recovery actions.
- May be ongoing as **incidents are dynamic**
- The results of a disaster assessment must be conveyed to **management and decision-makers** for determination of the correct course of action.
- **Prioritize life, health, and safety**, and should also consider any impacts to customers, regulatory obligations, and both direct and indirect costs like loss of revenue and reputation.
- **Post-recovery** to determine the total impact of the disaster or incident

Implement Disaster Recovery Process

Restoration

- Once the minimum level of contingency is reached, the focus of the DR team shifts to **restoring the original site** or facilities impacted by the disaster.
- The term **primary site** may be used to avoid confusion between the old and new facilities.
- Goal of **recovery** is a **resumption of critical business functions**
- Goal of **restoration** is the **return to normal** service levels at the primary site.

- Many variables in restoration that are outside the purview of the security team, but **security practitioners are still critical stakeholders.**
- The security function may have **critical roles** assigned in the DR plan and may need to be consulted regarding decisions like **safeguarding data during relocation** to the primary site.

Implement Disaster Recovery Process

Training and Awareness

- All personnel should be trained on **basic life, health, and safety plans**, including how to spot and respond to emergencies like a fire or extreme weather preparedness specific to the region the organization operates in.

- The purpose of these trainings is twofold: **personnel acquire a trained response** that speeds up reaction times during an emergency, and the exercise provides an opportunity to **identify incorrect weaknesses in the plan**.

- More **advanced training is required for personnel with specific duties** identified in the BC and DR plans (like sys admins).
- Training and awareness opportunities should be provided on a **routine basis** to ensure the knowledge remains current.

DOMAIN 7 – SECURITY OPERAT

Implement Disaster Recovery Process

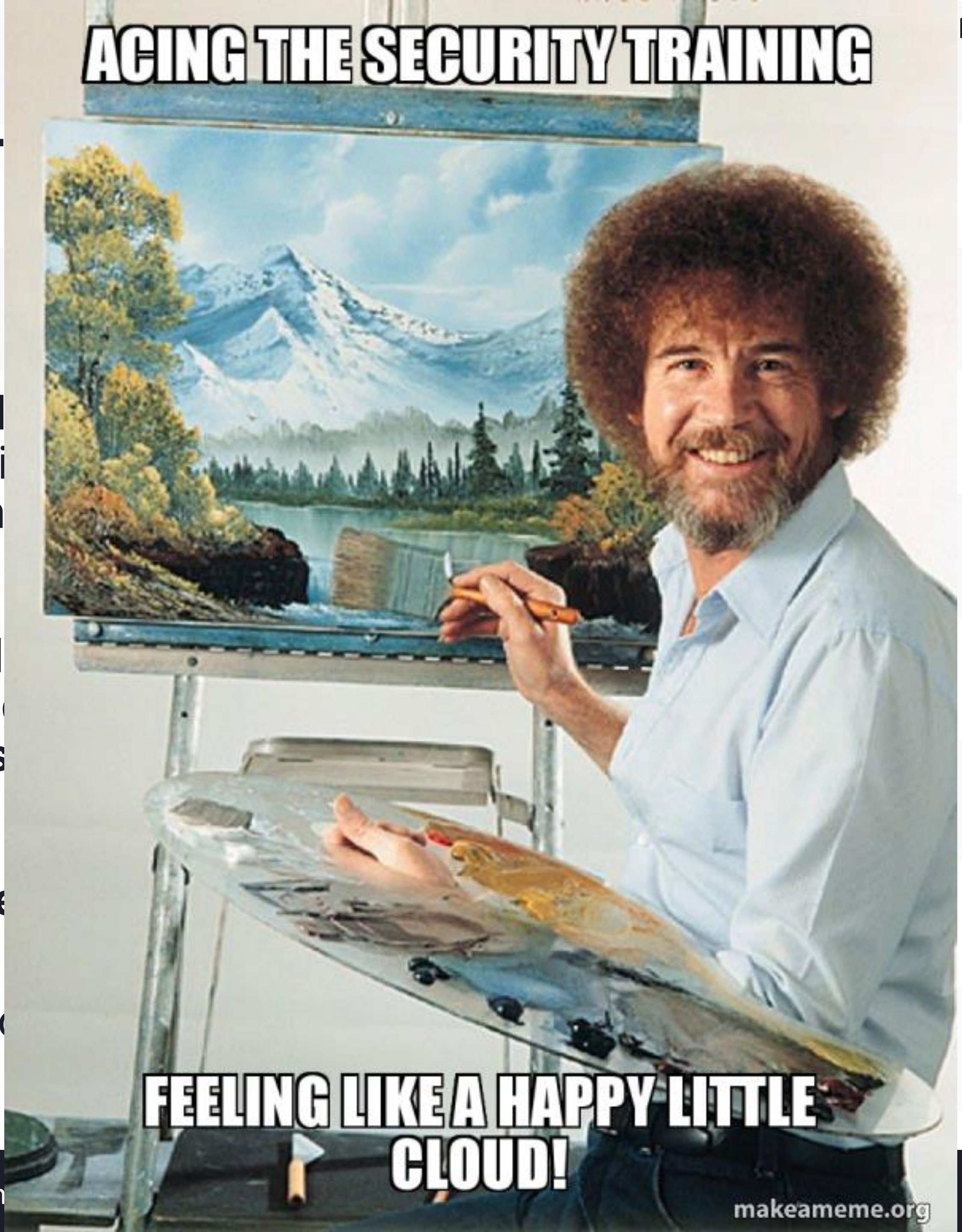
Training and Awareness

- All personnel should be trained on **basic I**
  spot and respond to emergencies like a fi
  to the region the organization operates in

- The purpose of these trainings is twofold
  speeds up reaction times during an emer
  opportunity to **identify incorrect weaknes**

- More **advanced training is required for pe**
  BC and DR plans.

- Training and awareness opportunities sh
  the knowledge remains current.


ACING THE SECURITY TRAINING
FEELING LIKE A HAPPY LITTLE CLOUD!
makeameme.org

Money

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

Implement Disaster Recovery Process

Training and Awareness

- All personnel sho s, including how to spot and respond paredness specific to the region the

- The purpose of th **ed response** that speeds up reacti ovides an opportunity to **ide**

- More **advanced t es** identified in the BC and DR plans.

- Training and awa **ne basis** to ensure the knowledge re

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

Implement Disaster Recovery Process

Training and Awareness

- All personnel sho , including how to spot and respond aredness specific to the region the
- The purpose of th d **response** that speeds up reactio ides an opportunity to **ide**
- More **advanced t** s identified in the BC and DR plans.
- Training and awa e **basis** to ensure the knowledge re

DOMAIN 7 – SECURITY OPERATIONS

Implement Disaster Recovery Process

Lessons Learned

Continuous improvement

Formal review should be conducted after restoration is complete.

- Actions or processes that went well.
- Actions or process that did not go well.
- Staff and personnel actions that either contributed to or hindered recovery and restoration. Note that this should not be designed to place blame or point fingers, but to identify opportunities to improve. As such, a facilitator can be useful to avoid issues like individuals feeling persecuted.

- May be called a **postmortem, after action report, retrospective, or lessons learned**.
- **Root-cause analysis** of the disaster may also be valuable to identify proactive measures that reduce the likelihood or impact of a future incident.

DOMAIN 7 – SECURITY OPERATIONS

Test Disaster Recovery Plans

TESTING

- Testing the DRP is an essential, proactive risk mitigation and serves two main purposes.
- Can identify incorrect assumptions or out of date information in the plan that, if not corrected, limits the plan's effectiveness.
- Provides vital training opportunities for staff. A rehearsed response, like a fire drill, creates a trained response capability for staff and increases the effectiveness of actions during a real disaster or emergency, as personnel will execute familiar procedures.
- Visible BCDR planning, testing, and exercises provide assurance to employees, customers, and other stakeholders that the organization is taking security seriously.

DOMAIN 7 – SECURITY OPERATIONS

Test Disaster Recovery Plans

TESTING

- **Start simple**, due to the cost and potential disruption inherent in a test and the need to build the testing capability.
- Staff who are unfamiliar with procedures should be given the opportunity to **build knowledge over time.**
- **Less burdensome** types of tests like a read-through may also be **conducted more frequently.**

- Output of DR plan testing should be **lessons learned** and plan updates, which the CISSP may be responsible for incorporating into the plan.
- Plans should be in a **format that is resistant to disaster**. For example, paper copies of the plan may be distributed, and employees instructed to store them at home, in case a disruption renders information systems or organization facilities unusable.

DOMAIN 7 – SECURITY OPERATIONS

Test Disaster Recovery Plans

Read-through/Tabletop

- Usually performed with a **small group** including managers or representatives from all stakeholder groups.
- Includes verifying information and procedures needed for communications during a disaster, and the goal is to **spot missing or outdated details**, as well as any assumptions that are incorrect.
- Each participant talks through not only the information presented in the plan, but also talks through the **steps they would perform to execute** the procedures, information they require in the scenario, and issues they foresee.
- **Least expensive method** of testing, both in terms of time and cost, as well as the potential for disrupting normal operations.

DOMAIN 7 – SECURITY OPERATIONS

Test Disaster Recovery Plans

Walkthrough

- Extends the tabletop exercise but **simulates responding** in the actual locations described in the DRP.
- The response team not only talks through the elements of the plan, but **physically walks or moves through the appropriate plan steps**, as dictated by an exercise scenario such as a fire rendering a data center unusable.
- Personnel **actually drive to the facility**. Physically walking through response steps builds some familiarity for the key participants and helps uncover details like missing or relocated equipment needed in the response.
- Physically exercising the response is twofold. It can **challenge assumptions made**, such as “staff relocate to the alternate facility within one hour of a disaster declaration.” If the facility is too far away to reach in an hour, the RTO will obviously not be met.
- Second, it offers the **opportunity for staff to familiarize themselves with the procedures** or facilities, enabling them to respond more quickly in the event of an actual disaster.

Test Disaster Recovery Plans

Simulation

- DR team can be called together and given a scenario that requires activating an alternate facility, recalling data from offsite storage, and loading it.

- This can be done to validate that the system can be restored according to defined RTO and RPO metrics and that the backup data integrity is intact.

DOMAIN 7 – SECURITY OPERATIONS

Test Disaster Recovery Plans

Parallel

- Systems impacted by a disaster scenario are tested side by side with their alternates to ensure the alternate systems are capable of handling a realistic operational load.
- Parallel tests **reduce the impact on primary systems** while providing relatively full coverage for testing recovery capabilities.
- They do **incur significant costs and may have operational impacts** like slightly delaying processing or reducing staff productivity as resources are split between daily operational tasks and the parallel test tasks.
- Due to the breadth of testing, a parallel exercise **can find issues that other testing might miss**, such as incorrectly configured alternate sites or incomplete data backup

Test Disaster Recovery Plans

Full Interruption

- In a full interruption test, the organization's DR capability is **tested as if a real disaster had occurred**, which involves high costs and the potential for disrupting normal operations if the test is not successful.
- **Interrupts normal processing** and switches the organization to contingency procedures and alternate sites, with the goal of identifying all possible issues with BCDR plans and procedures.
- May be performed on a **subset of systems** to minimize the impact or costs involved.

Test Disaster Recovery Plans

Participate in Business Continuity Planning and Exercises

- CISSPs are key stakeholders in planning and executing critical continuity tasks, but they are often not the owners of the BC process.
- Key tasks include providing input on how security requirements change during contingency operations and implementing or managing the responses needed to meet these new requirements.
- Guiding the process of identifying changes that need to be reflected in the BC or DR plans.
- New copy of the plan should be made available for all relevant stakeholders, including offline copies in case information systems are not accessible. Old copies must also be recovered and destroyed to ensure no outdated or incorrect information is utilized during an actual emergency.

Test Disaster Recovery Plans

Participate in Business Continuity Planning and Exercises

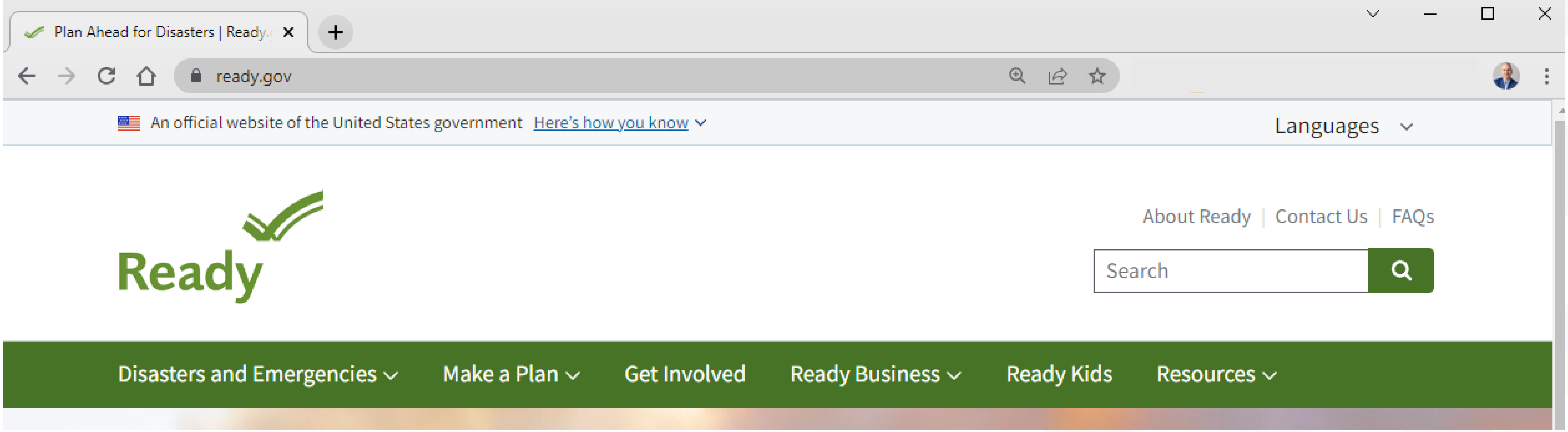
- Because security incidents can lead to declaration of a disaster, the security function may be critical in designing the scenarios used to test and exercise BC plans. For example, a ransomware attack would normally be handled by IR procedures, but if it is sufficiently widespread, it may require declaration of a disaster and activation of alternate facilities and procedures.

- A security practitioner is ideally suited to not only craft this exercise scenario, but also to act as a moderator as they likely have knowledge needed to answer questions during the simulation.

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

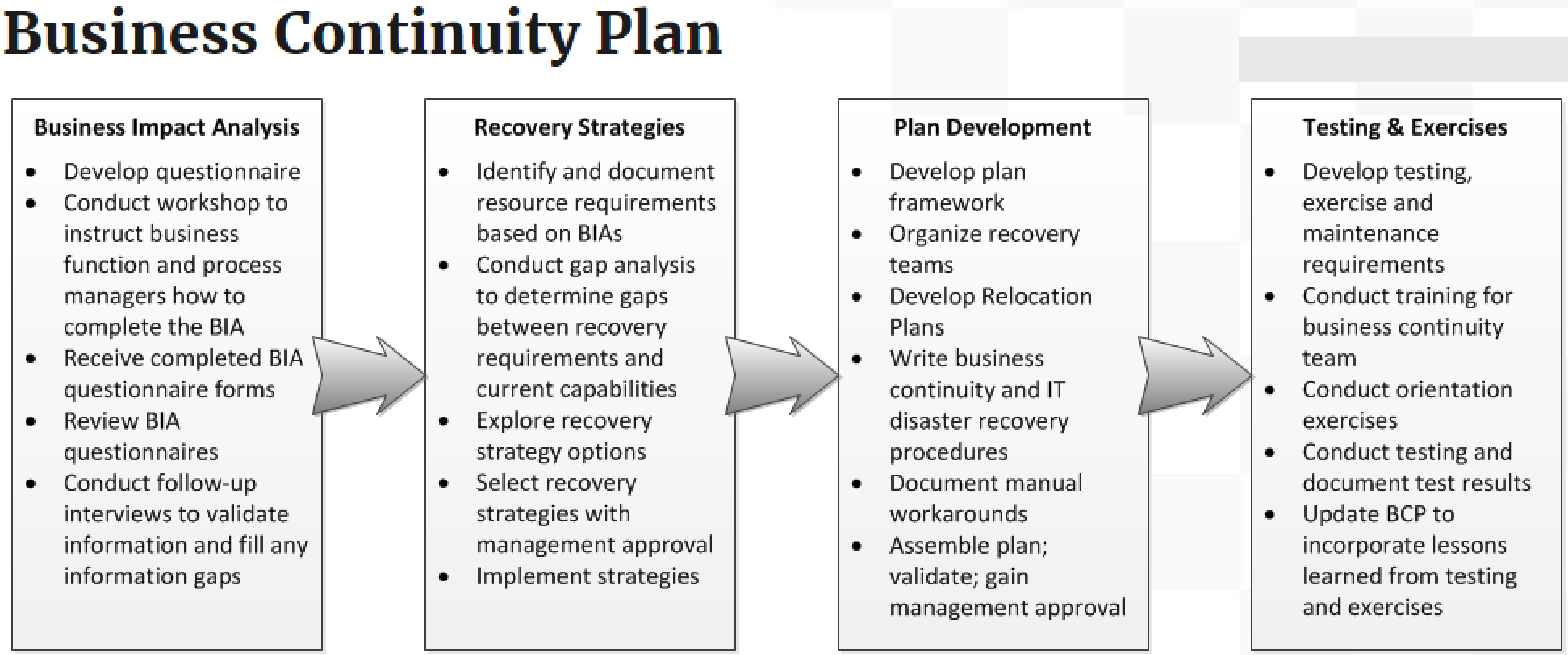
Real World Resource – Ready.gov


Plan Ahead for Disasters | Ready.
ready.gov
An official website of the United States government
Here's how you know
Languages
Ready
About Ready | Contact Us | FAQs
Search
Disasters and Emergencies
Make a Plan
Get Involved
Ready Business
Ready Kids
Resources

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

Real World Resource – Ready.gov



Business Continuity Plan

Business Impact Analysis

- Develop questionnaire
- Conduct workshop to instruct business function and process managers how to complete the BIA
- Receive completed BIA questionnaire forms
- Review BIA questionnaires
- Conduct follow-up interviews to validate information and fill any information gaps

Recovery Strategies

- Identify and document resource requirements based on BIAs
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities
- Explore recovery strategy options
- Select recovery strategies with management approval
- Implement strategies

Plan Development

- Develop plan framework
- Organize recovery teams
- Develop Relocation Plans
- Write business continuity and IT disaster recovery procedures
- Document manual workarounds
- Assemble plan; validate; gain management approval

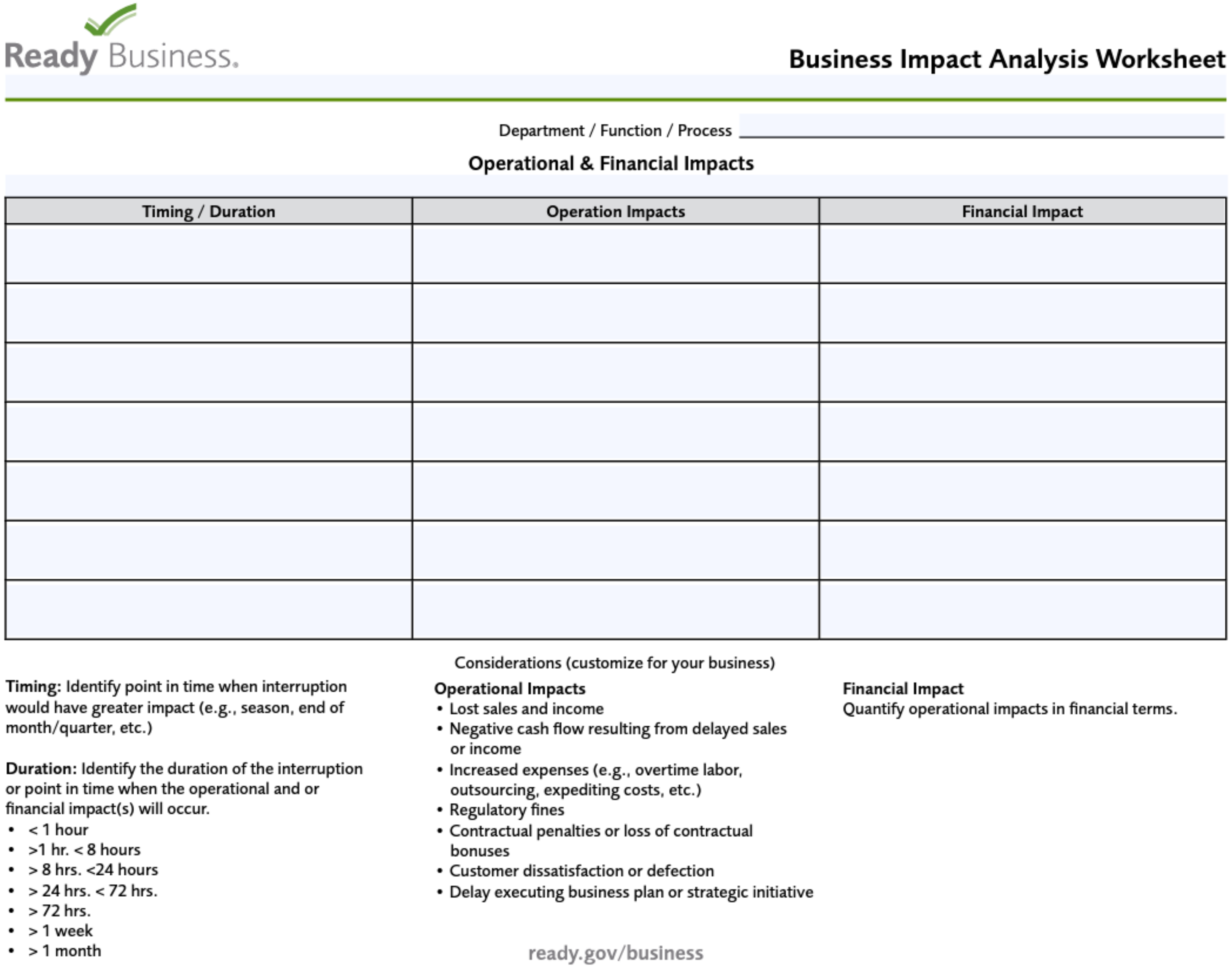
Testing & Exercises

- Develop testing, exercise and maintenance requirements
- Conduct training for business continuity team
- Conduct orientation exercises
- Conduct testing and document test results
- Update BCP to incorporate lessons learned from testing and exercises

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

https://www.ready.gov/sites/default/files/2020-07/business-impact-analysis-worksheet.pdf



Ready Business.

Business Impact Analysis Worksheet

Department / Function / Process ____________________

Operational & Financial Impacts

Timing / Duration	Operation Impacts	Financial Impact

Considerations (customize for your business)

Timing: Identify point in time when interruption would have greater impact (e.g., season, end of month/quarter, etc.)

Duration: Identify the duration of the interruption or point in time when the operational and or financial impact(s) will occur.

- < 1 hour
- >1 hr. < 8 hours
- > 8 hrs. <24 hours
- > 24 hrs. < 72 hrs.
- > 72 hrs.
- > 1 week
- > 1 month

Operational Impacts

- Lost sales and income
- Negative cash flow resulting from delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay executing business plan or strategic initiative

Financial Impact

Quantify operational impacts in financial terms.

ready.gov/business

CISSP® MENTOR PROGRAM – SESSION TEN

TIME FOR A … DAD JOKE

Please play along

Knock knock.

Nobel

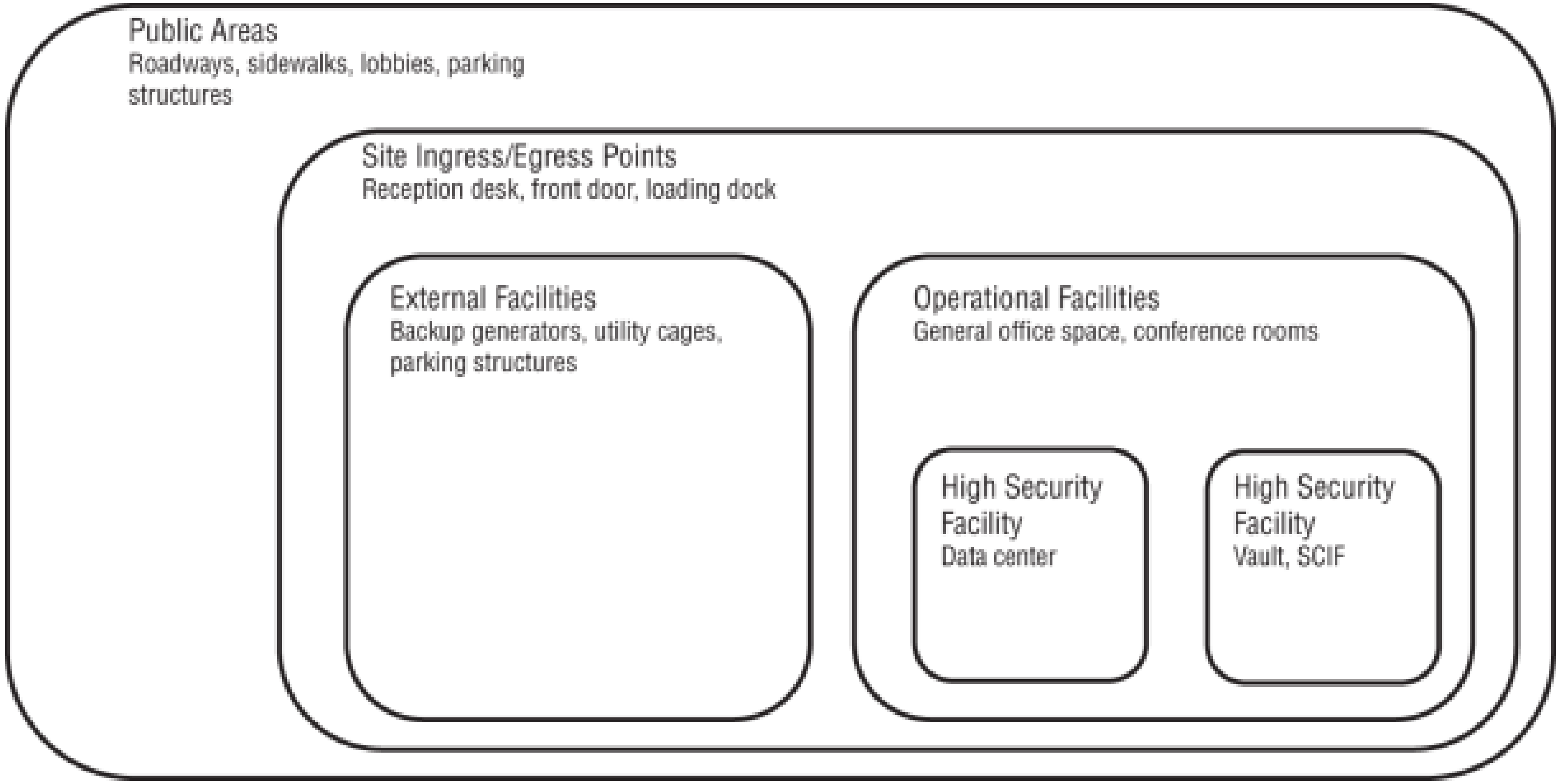
No bell.
It's just another
Dad joke

HAHAHAHA 😂

Moving on…

Implement and Manage Physical Security

Physical


Public Areas
Roadways, sidewalks, lobbies, parking structures
Site Ingress/Egress Points
Reception desk, front door, loading dock
External Facilities
Backup generators, utility cages, parking structures
Operational Facilities
General office space, conference rooms
High Security Facility
Data center
High Security Facility
Vault, SCIF

DOMAIN 7 – SECURITY OPERATIONS

Implement and Manage Physical Security

Physical

- Should be chosen from multiple control categories like preventive, deterrent, detective, compensating, recovery, directive, and corrective.
- Should also be implemented with a combination of physical (barriers, fences), technical (badge readers), and administrative controls (policies and procedures).
- Using a layered model, with multiple layers and chokepoints between the outside world and rooms or offices where high-value assets are stored or handled.
- Selection of physical access controls at each layer should be guided by the cost of the control and the value of the assets protected.

Implement and Manage Physical Security

Physical

- One methodology for designing a comprehensive physical security strategy is crime prevention through environmental design (CPTED)
- **Landscape design** can be used to provide physical security without designing the facility like a fortress. Water features, shrubs, and trees can all be used to restrict access without building walls or other barriers.
- **Lighting plays a major role** in deterring unwanted behavior. Well-lit spaces are less attractive to criminals due to the increased likelihood of getting caught.
- **Decisions about placement of and materials used for windows** should be made with respect to the security needs of the facility. For example, placing a window right next to a door could allow the window to be broken and the door opened from the inside, and windows may require additional reinforcement like metal screens or meshwork for high security applications.

CISSP® MENTOR PROGRAM – SESSION TEN

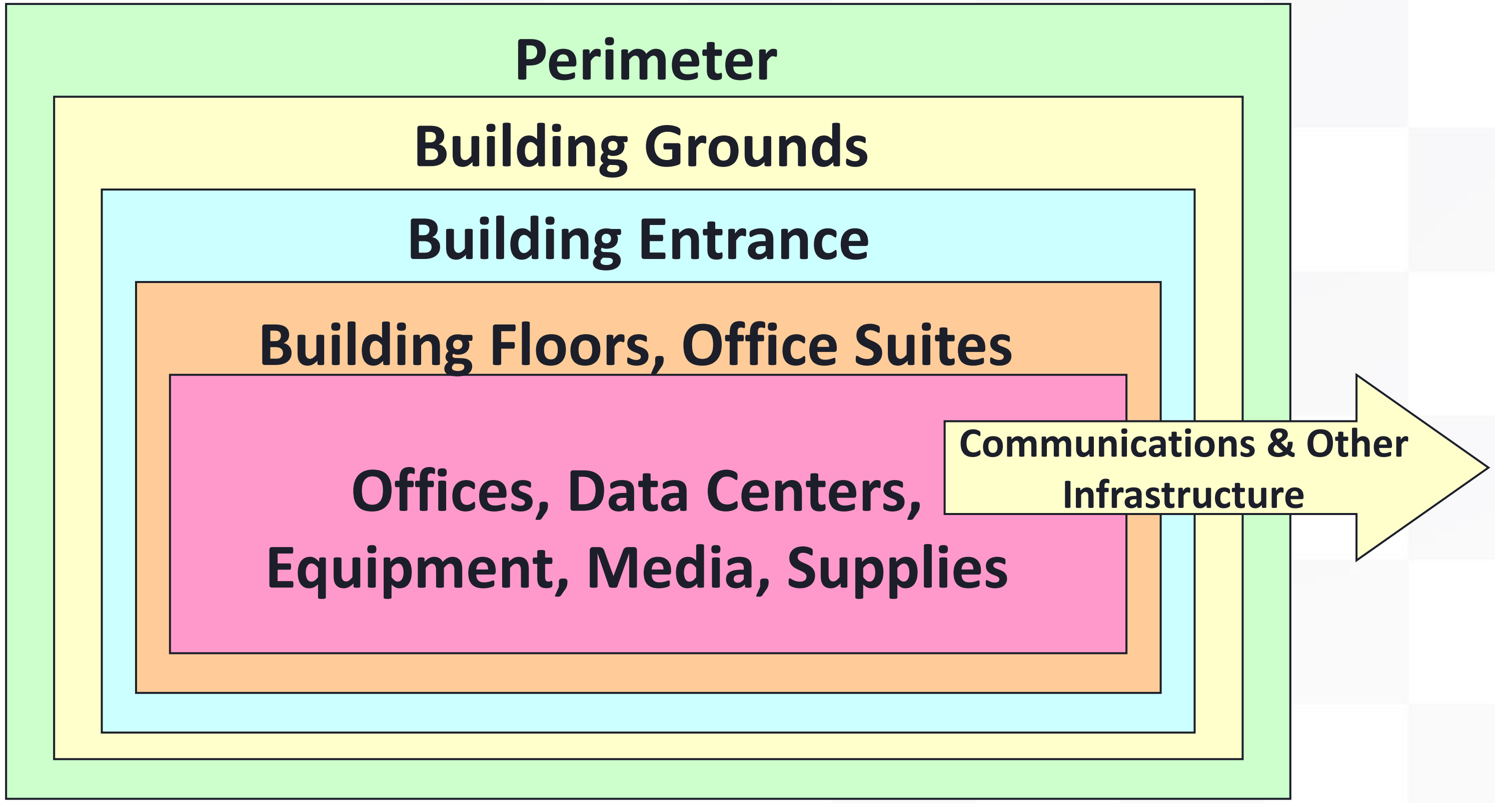
DOMAIN 7 – SECURITY OPERATIONS

Implement and Manage Physical Security

Physical

Layered defenses... countermeasures can be used at every layer to protect, detect, react

> Communications and other infrastructure may cross multiple boundaries and security zones... some of it is shared


Perimeter
Building Grounds
Building Entrance
Building Floors, Office Suites
Offices, Data Centers, Equipment, Media, Supplies
Communications & Other Infrastructure

Implement and Manage Physical Security

Perimeter Security Controls (Public Areas)

- For public approaches to a facility, such as roads or sidewalks, barriers designed to slow, direct, or impede traffic may be deployed and typically require coordination with authorities like landlords or zoning/planning commissions.
- Monitoring public areas is typically easy to achieve, as there are few restrictions on the use of monitoring tools in public areas. Clear line of sight and adequate lighting are necessary, and cameras capable of covering large areas might be needed, such as wide-angle or pan-tilt-zoom (PTZ).
- Monitoring for the safety of organization assets, cameras observing public areas may also need to be monitored for evidence of other criminal activity. Additionally, the presence of utilities like power, water, and sewer connections in public areas may require monitoring or hardening to prevent tampering, such as locked utility cages or dedicated camera coverage on utility hookups.

DOMAIN 7 – SECURITY OPERATIONS

Implement and Manage Physical Security

Perimeter Security Controls (Site Ingress and Egress Points)

Reception or guard staff - will implement access controls like ID verification, visitor registration, and inspections of material entering or exiting the facility.

Physical access controls - These include turnstiles, gates, doors, and mantraps for personnel, and bollards, delta barriers, and speed bumps for vehicular traffic. Administrative controls may also be used, like procedures for visitor inspection and escort or verification of deliveries against purchase orders for new IT assets entering the facility.

Sensors - can detect temperature or infrared light, motion, or pressure to identify the presence or movement of people. will typically be connected to an alarm or monitoring console, and function to detect unwanted activity that triggers a response like a guard investigating or summoning law enforcement. (Physical IDS)

Cameras - The presence of cameras can be a deterrent to malicious activity, and they can be a key detective control if the camera feed is monitored. Guards are often used to monitor camera feeds, but many cameras include AI-powered object detection that can recognize people, vehicles, and even animals.

Guards - Human guards can deter, prevent, detect, correct, and assist with recovery from malicious action.

Implement and Manage Physical Security

Perimeter Security Controls (External Facilities)

- External facilities may be under the organization's direct control, but often require sharing control due to the presence of equipment that does not belong to the organization.
- Controls in place for these external facilities will focus primarily on controlling physical access to prevent tampering. Life, health, and safety controls will also need to be considered due to dangerous elements like highly charged electrical equipment and dangerous chemicals like fuel. Safety equipment including gloves, fire suppression, and emergency shutoff tools are a good idea and may be required per local laws.
- Landscaping can be part of the organization's physical security plan, as well as a way to add to the aesthetics of a facility. Landscape features like terraced gardens or trees can act as a barrier to human or vehicular traffic, and landscaping maintenance like clearing dead leaves or branches from the perimeter of the facility is a vital fire prevention control.

Implement and Manage Physical Security

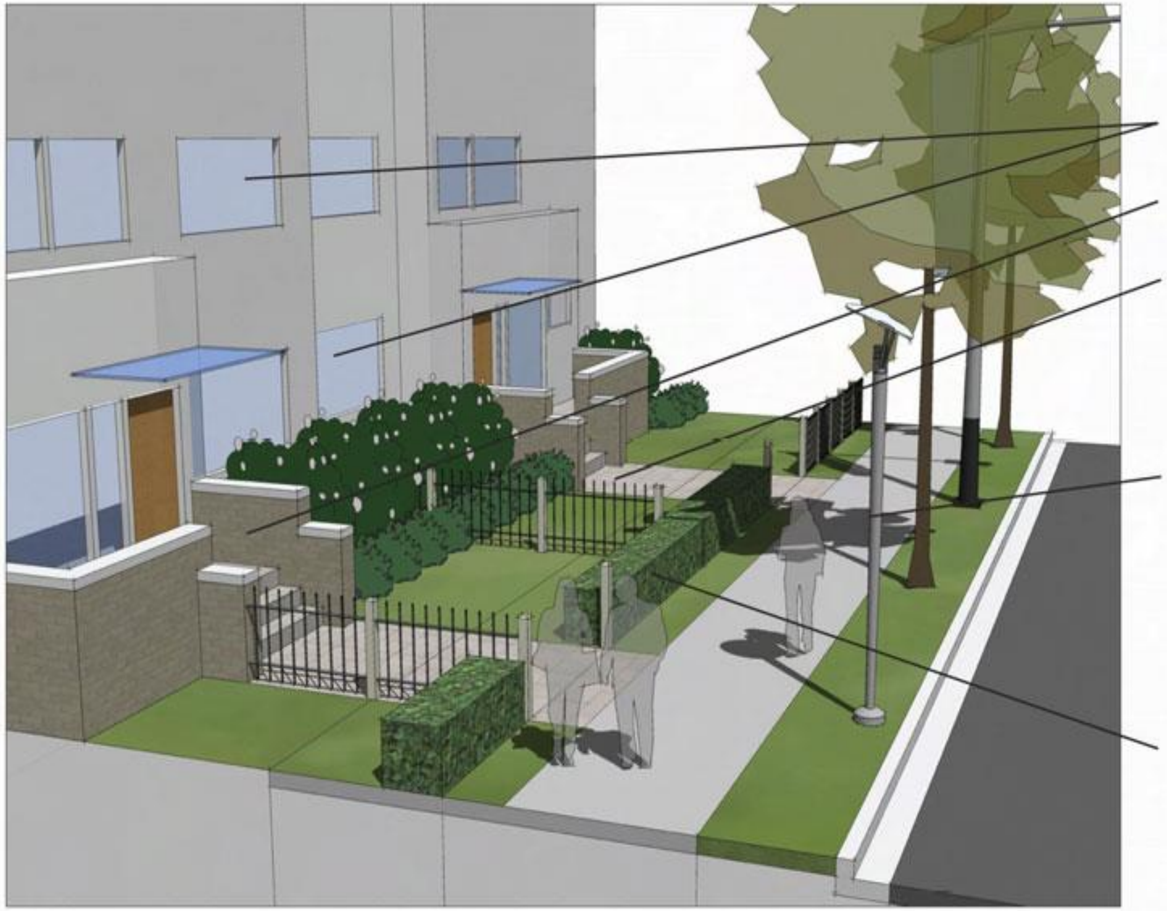
CPTED = Crime Prevention Through Environmental Design

- CPTED is psychological and sociological way of looking at physical security
- Strategies: Physical environment of building can be changed or managed to produce behavioral effects reducing the incidence or fear of crime.
  - Natural Access Control
  - Natural Surveillance
  - Natural Territorial Reinforcement
- Methods:
  - Use a combination of security hardware, psychology and site design to discourage crime
  - Reduce the opportunity for specific crimes or incidents
  - Make legitimate users feel safe while deterring illegal users
    - Example: Exterior lighting

DOMAIN 7 – SECURITY OPERATIONS

Implement and Manage Physical Security

CPTED = Crime Prevention Through Environmental Design



Large windows promote casual supervision of sidewalk.

Porches and sidewalk encourage interaction between neighbors.

Paving and architectural treatments define public and private zones.

Good pedestrian-scaled lighting on street.

Low landscaping and fences define property lines without creating hiding places.

Implement and Manage Physical Security

Internal Security Controls (Operational Facilities)

Fire detection and suppression - primarily designed for human safety, fires can also damage valuable equipment. Fire and smoke detectors and corresponding suppression methods like sprinklers, gas-based suppression, and portable extinguishers can help minimize the impact of a fire

Access controls - Physical access controls should be implemented to segregate areas in the facility based on user authorization, with physical devices like badge readers or locks controlling access.

Policies and procedures - Personnel working in operational facilities should be trained on and expected to follow policies and security procedures like clean desk and clear screen. This includes procedures for evacuation and shelter-in-place, which may be coordinated with groups outside security including HR or facilities management.

Lighting and surveillance - Lighting should be sufficient to support safe human occupancy for facilities where personnel regularly work, and sufficient to enable monitoring by cameras in unoccupied areas. Camera coverage or routine inspection, such as a guard walkaround of the facility, should be implemented to ensure timely detection of issues or potential incidents.

Building materials - building materials sufficient to support security requirements are critical.

DOMAIN 7 – SECURITY OPERATIONS

Implement and Manage Physical Security

Internal Security Controls (High-Security Facilities)

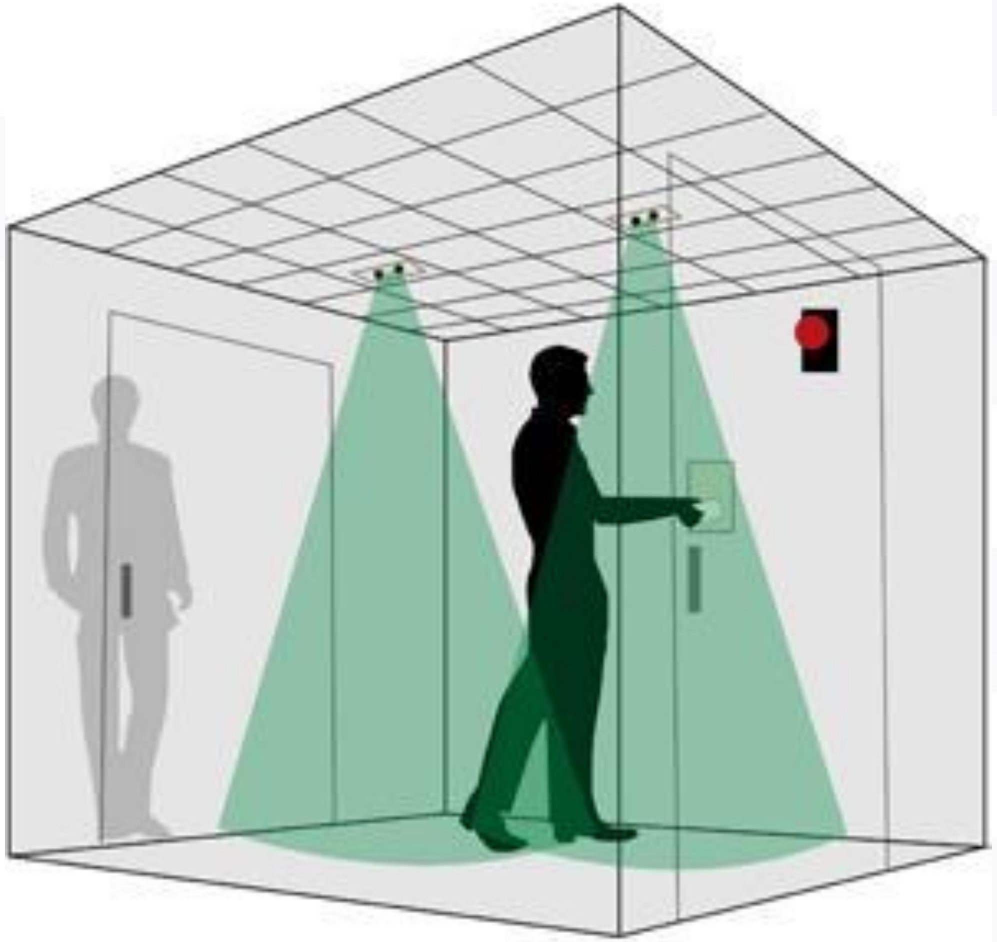
- **Specific areas** designated as high-security due to the value or sensitivity of assets they contain.
- Evidence storage rooms, secure compartmentalized information facilities (**SCIFs**), and server rooms or **data centers**.
- **Require additional types of security controls**, some of which may be quite burdensome to users, such as invasive searches of bags entering or leaving the facility, multiple layers of physical access controls with multifactor authentication, or restrictions against personal devices like smartphones.
- **Increased costs** such as special construction of walls designed to block electromagnetic fields (EMF), known as a Faraday cage, which are appropriate given the high value or sensitivity of assets store and handled in these areas.

DOMAIN 7 – SECURITY OPERATIONS

Implement and Manage Physical Security

ManTrap

- Double doors, where only one can be opened at a time
- Used to control personnel access
- Manually operated or automatic
- Only room for one person



DOMAIN 7 – SECURITY OPERATIONS

Implement and Manage Physical Security

Fences

- Effective preventive and deterrent control
- Keep unwanted persons from accessing specific areas
- Better when used with motion detectors, alarms, and/or surveillance cameras

Height	Effectiveness
3-4 ft	Deters casual trespassers
6-7 ft	Too difficult to climb easily
8 ft plus 3 strands of barbed or razor wire	Deters determined trespassers

Implement and Manage Physical Security

Fences

Perimeter Intrusion Detection and Assessment System (PIDAS):

- A type of fencing that has sensors on the wire mesh and base of the fence.
- A passive cable vibration sensor sets off an alarm if an intrusion is detected.

DOMAIN 7 – SECURITY OPERATIONS

Implement and Manage Physical Security

If you could pick one item for physical security, what would it be?

Address Personnel Safety and Security Concerns

Personnel

Human health and safety are always the most important considerations for any security program.

Choosing security controls should be done with respect to the life, health, and safety of personnel who use the organization's systems and data.

DOMAIN 7 – SECURITY OPERATIONS

Address Personnel Safety and Security Concerns

Travel

- Personnel may require **unique organization-provided services** such as additional insurance, medical coverage, and organization-defined emergency procedures.
- Personnel who are traveling should have **additional security and training on device security practices** for devices containing organization data. This includes organization owned as well as personal devices if a bring-your-own device (BYOD) program exists.
- Securing this data might include **encryption of all data at rest, provisioning secure network connectivity like a VPN**, and **additional controls** like issuing dedicated devices for use while traveling, which are then wiped and reimaged before being issued to another traveling user.
- Personnel should also be **trained on physical security measures** like securing laptops in use outside the office before they depart.

Address Personnel Safety and Security Concerns

Security Training and Awareness

Awareness - provide or reinforce basic information to a general audience, often through devices like posters, notes on a company intranet site, or email notices.

Training - designed to convey specific knowledge needed for performing the job function, such as system administrators only using privileged accounts for certain tasks to minimize phishing risks. Training is delivered by an authoritative source and takes many forms including computer-based and instructor-led training.

Education - is the most formal and is focused on explaining theories and their application. It often takes the form of academic classes, continuing education, or certifications like the CISSP. It demonstrates a deep level of knowledge for an individual and is suitable for specific roles in the organization like leading and managing the information security program.

Effectiveness should always be measured -. This may be difficult for general awareness but is relatively easy for training and education where tests or graded assignments can be used as metrics.

DOMAIN 7 – SECURITY OPERATIONS

Address Personnel Safety and Security Concerns

Emergency Management

Coordination with responders - First responders like medical, fire, or law enforcement can support the organization's response to some emergencies. Some organizations, like airports or large data center campuses, may coordinate emergency exercises or drills with these responders to ensure all relevant stakeholders are trained and able to identify weaknesses or issues with coordination among the different organizations involved.

Communications - emergency communications plans need to account for alternate means of getting critical information to required stakeholders. This includes details of BC or DR plans like alternate work arrangements and critical health and safety notices like shelter-in-place orders.

BCDR plan execution - Emergencies often necessitate the activation of BCDR plans and contingency procedures. **Crisis communications** must include **simple, easy-to-follow instructions** designed to eliminate confusion and ambiguity.

Security practitioners may not be directly involved in creating or delivering these messages, but as key stakeholders in the process, they must ensure vital security information is communicated effectively.

Address Personnel Safety and Security Concerns

Duress

Duress describes a condition where a person is forced to do something against their will. Blackmail and being held hostage are extreme examples.

- Security controls to detect duress should **focus on preserving the health and safety** of the individual—if an attacker knows that their victim has summoned help, they may take actions to harm the individual.
- **Subtle means of indicating duress**, such as entering a special code on an electronic lock or using a code word or phrase with a coworker, can allow for detection of duress without increasing the danger faced by the individual.
- Duress code words or phrases **should not be immediately recognizable by an outsider**. The phrase might sound ordinary, but not something an individual is likely to say in normal conversation with a colleague, like, "By the way, my aunt Sylvia says hi!"

CISSP® MENTOR PROGRAM – SESSION TEN

DAD JOKE

Before we get too deep into this.

How about a dumb dad joke before we go?

CISSP® MENTOR PROGRAM – SESSION TEN

SESSION 10 - FIN
YOU MADE IT!

Domain 7 is done WHOOT HECK YA!! YALL!

Next Session - Domain 8 – Software Development Security

Monday, 22 May 2023

- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in software development ecosystems
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure coding guidelines and standards

FRSecure CISSP Mentor Program

2023

Class #10 – Domain 7 part 2

Security Operations

Ron Woerner

Forrester, Sr Consultant
Cyber-AAA, Founder & CEO & vCISO
Bellevue University, CyberSecurity Studies Professor