IS4231
Information Security Management

Lecture 10

Planning for Contingencies

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Reading: Chapter 10

Learning Objectives

- Describe the major components of incident response, disaster recovery, business continuity and crisis management
- Discuss how the organization would prepare and execute a test of contingency plans

Topics

- Business Impact Analysis
- Incident Response Planning
- Disaster Recovery Planning
- Business Continuity Planning
- Crisis Management
- Timing & Sequence of CP Elements
- Testing Contingency Plans

Introduction to Contingency Planning

What is Contingency Planning?

- Contingency Planning (CP)
  - The overall process of preparing for *unexpected adverse events*
  - Main goal
    - Restore normal modes of operation with minimal cost asap
  - Involves IT and InfoSec managers, supported by all other communities of interest or stakeholders

due to limited resources, usually it is not possible to react to adverse event in the most ideal way
- typically, there is a need to balance and compromise

Four Major Components

- Business Impact Analysis (BIA)
  - Help the organization identify which business functions and information systems are the most critical to the success of the organization
- Incident Response Plan (IRP)
  - Focus on the immediate responses to unexpected adverse event
- Disaster Recovery Plan (DRP)
  - Focuses on restoring operations at the primary site after disasters occur
- Business Continuity Plan (BCP)
  - Facilitates establishment of operations at an alternate site

Components of Contingency Planning

- CP major components:
  - BIA, IR plan, DR plan, BC plan, CR plan

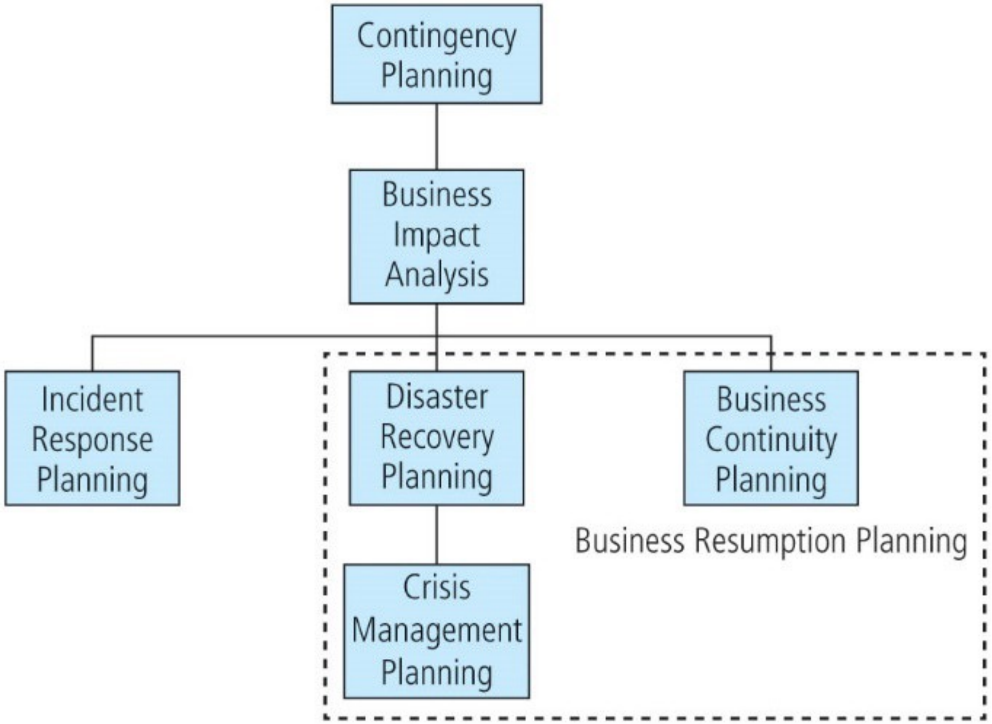

Contingency Planning
Business Impact Analysis
Incident Response Planning
Disaster Recovery Planning
Business Continuity Planning
Business Resumption Planning
Crisis Management Planning

Figure 10-1 Contingency planning hierarchies

Fundamentals of Contingency Planning (cont.)

- Contingency planning management team (CPMT)
  - CIO, system administrators, CISO, key IT and business managers should be actively involved
- Developing a CP document
  - Develops the CP policy statement
  - Conducts the BIA
  - Identifies preventative controls
  - Creates contingency strategies
  - Develops a contingency plan
  - Ensures plan testing, training, and exercises
  - Ensures plan maintenance

Fundamentals of Contingency Planning (cont.)

- Individuals and teams involved in CP
  - CPMT should include:
    - Champion
    - Project Manager
    - Team Members
      - □ Business managers
      - □ Information technology managers
      - □ Information security managers
- Incident response team - manages and executes the IR plan
- Disaster recovery team - manages and executes the DR plan
- Business continuity team - manages and executes the BC plan

Since the ITSec team is usually very small, it is very normal for overlapping to occur between the different teams

Business Impact Analysis

What is Business Impact Analysis?

- BIA investigates and assesses the impact that identified adverse events can have on the organization
  - By assuming that attack succeeded, the worst has happened, then assessing how that adversity will impact the organization.
- The CPMT conducts the BIA in three stages:
  1. Determine mission/business processes and recovery criticality
  2. Identify resource requirements
  3. Identify recovery priorities for system resources

1. Determine Mission/Business Processes and Recovery Criticality

- A BIA questionnaire is an instrument used to collect relevant business impact information for analysis, It can allow functional managers to enter:
  - Information about their functions
  - Impacts the functions have on the business
  - Dependencies that exist for the functions from specific resources and outside service providers
- Then a weighted table analysis (WTA) could be used to decide which business processes and functions are most critical

by default, CISO/CIO should already know about the **crown jewels** of the business

1. Determine Mission/Business Processes and Recovery Criticality (cont.)

however most of the time there has to be hard requirements set which will come from external forces- these will come from external organisations (compliance agency)

- Key recovery measures affecting B.I.A
  - **Maximum Tolerable Downtime (MTD)** - "the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations
  - **Recovery time objective (RTO)** - maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and processes
  - **Recovery point objective (RPO)** - the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered from backups after an outage

1. Determine Mission/Business Processes and Recovery Criticality (cont.)

- Key recovery measures affecting B.I.A
  - **Work Recovery Time (WRT)** - the amount of effort (expressed as elapsed time) that is necessary to get the business function operational AFTER the technology element is recovered (as identified with RTO).
    - It typically involves the addition of nontechnical tasks required for the organization to make the particular information asset usable for its intended business function again

RTO, RPO, MTD and WRT

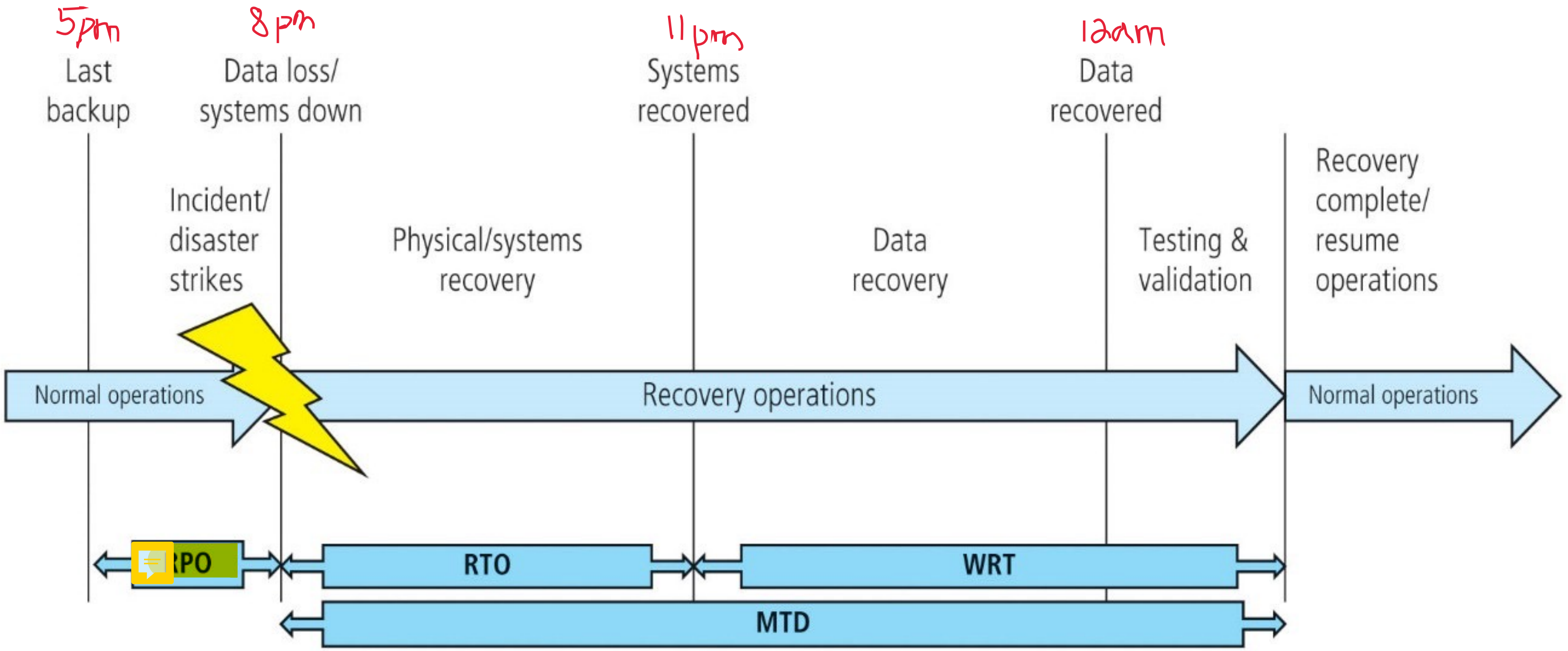


Figure 10-4 RTO, RPO, MTD, and WRT

Source: http://networksandservers.blogspot.com/2011/02/high-availability-terminology-ii.html.

MTD = 4h
RPO = 3h
RTO = 3h
WRT = 1h

1. Determine Mission/Business Processes and Recovery Criticality (cont.)

- Must balance the cost of system inoperability against the cost of recovery

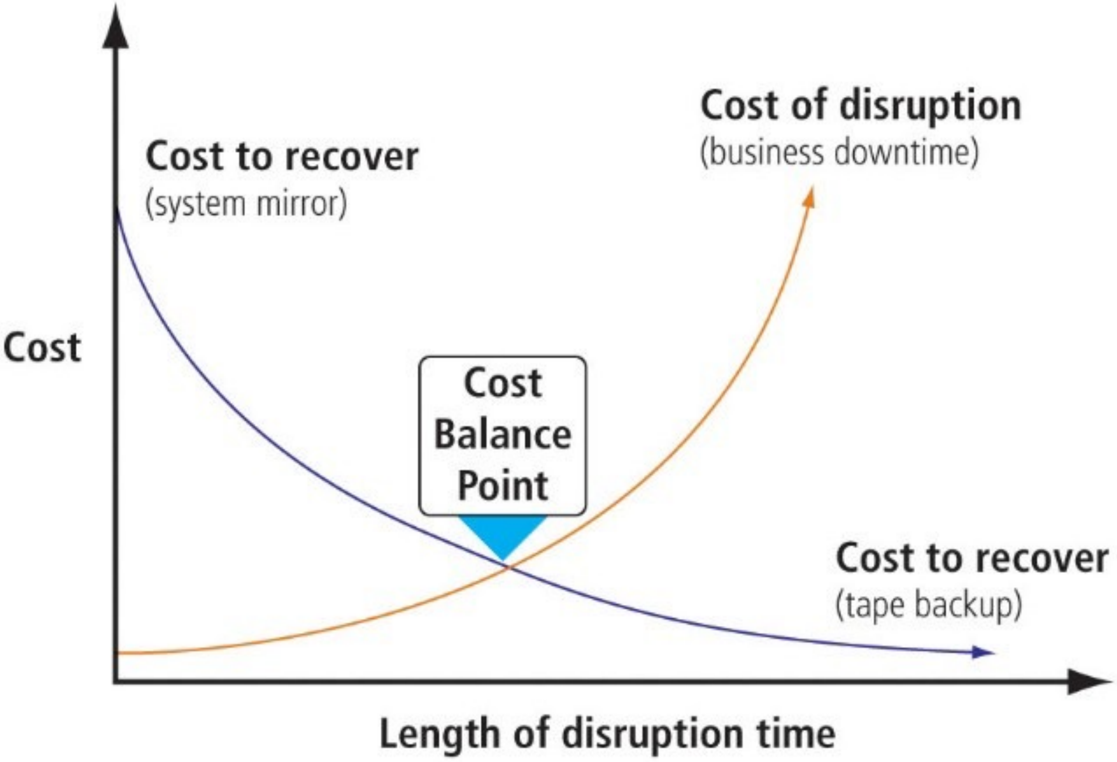
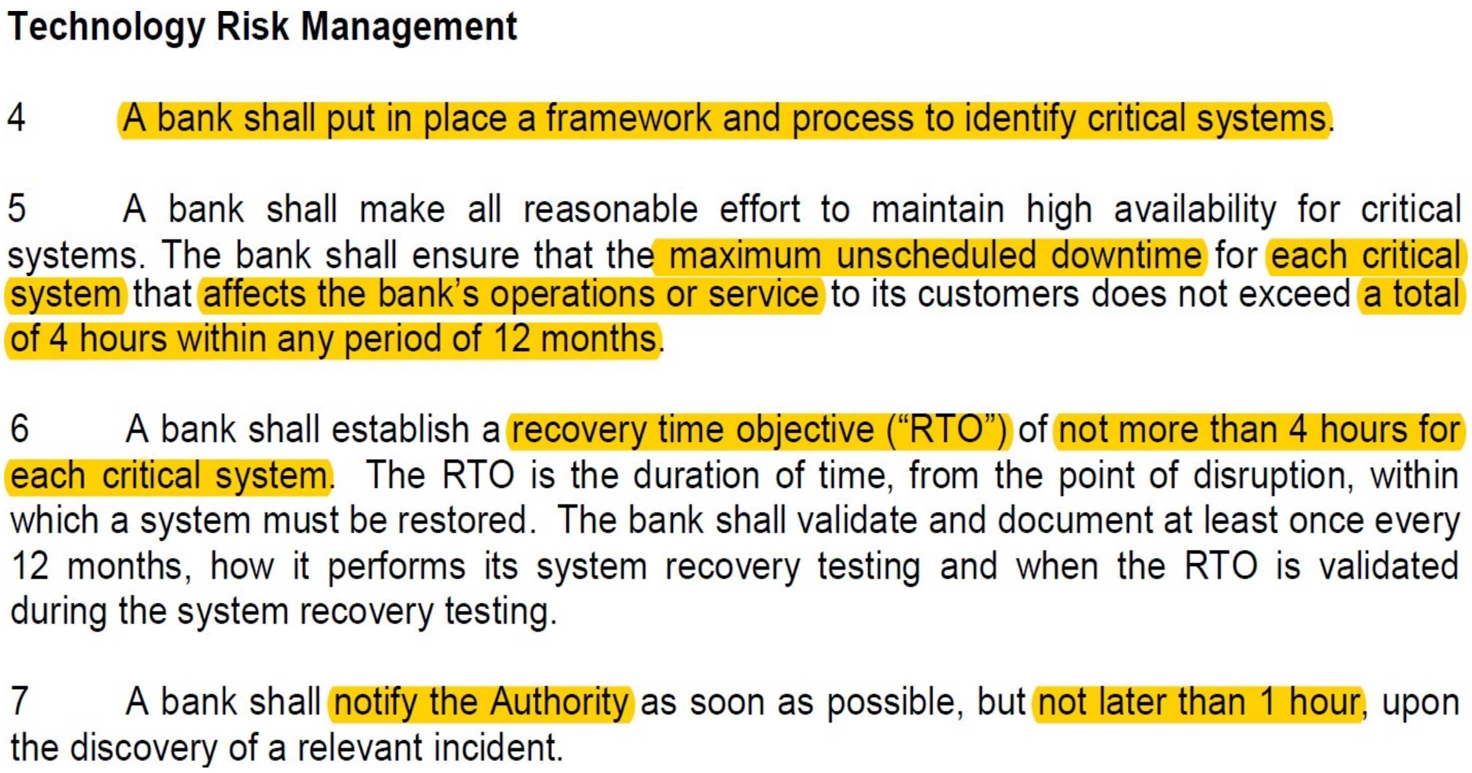


Figure 10-5 Cost balancing

Example: MAS requirements

- MAS Notice PSN05
  - Notice to operators and settlement situations of designated payment systems, 5 Dec 2019
  - Notice on technology risk management



Technology Risk Management

4 A bank shall put in place a framework and process to identify critical systems.

5 A bank shall make all reasonable effort to maintain high availability for critical systems. The bank shall ensure that the maximum unscheduled downtime for each critical system that affects the bank's operations or service to its customers does not exceed a total of 4 hours within any period of 12 months.

6 A bank shall establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. The RTO is the duration of time, from the point of disruption, within which a system must be restored. The bank shall validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing.

7 A bank shall notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

Incident Contingency Planning

Incident

- Adverse event: An event with negative consequences that could threaten the organization's information assets or operations. Sometimes referred to as an incident candidate

- Incident: An adverse event that could result in a loss of information assets, but *does not threaten the viability of the entire organization* severity of situation is manageable/controlled = then will be called an incident

- It is important to understand that IR is a *reactive measure, not a preventative one*

Getting Started

- An early task for the CPMT is to form a computer security incident response team (IRT)
  - An IR team composed of technical IT, managerial IT, and InfoSec professionals who are prepared to detect, react to, and recover from an incident
- Key members of the IRT become the IR planning committee and begin work by
  - Developing policy to define the operations of the team,
  - Articulating the organizational response to various types of incidents
  - Advising end users on how to contribute to the effective response of the organization

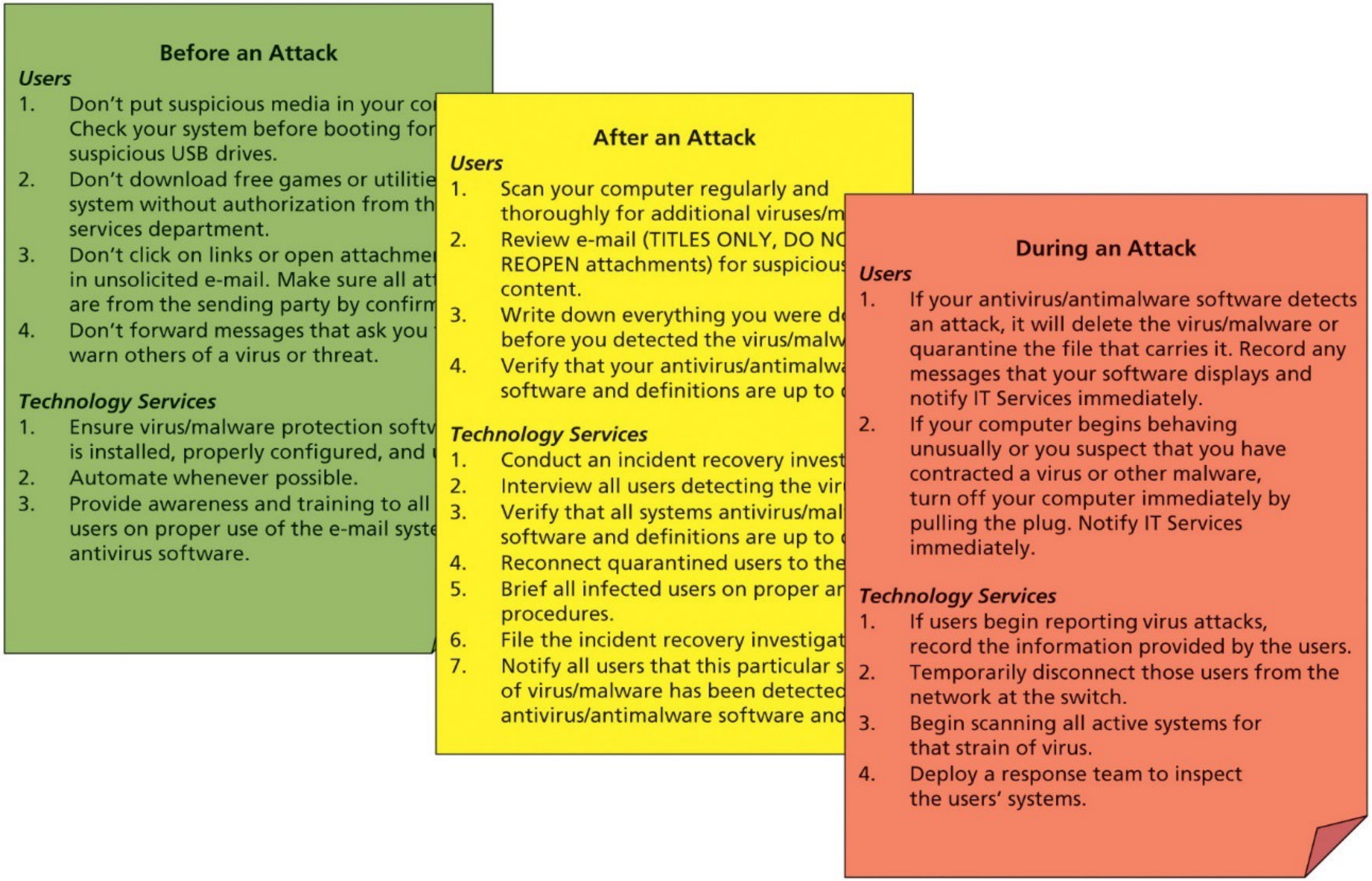
Incident Response Policy

- The policy statement that guides the development and implementation of IR plans and the formulation and performance of IR teams
- Key Components
  - Statement of management commitment
  - Purpose and objectives of the policy
  - Scope of the policy
  - Definition of InfoSec incidents and related terms
  - Organizational structure and definition of rules, responsibilities, and levels of authority
  - Prioritization or severity ratings of incidents
  - Performance measures
  - Reporting and contact forms

Incident Response Planning

- For every incident scenario, the CP team creates three sets of incident-handling procedures:
  - Before the incident
    - Details of data backup schedules
    - Disaster recovery preparation
    - Training schedules
    - Testing plans
    - Copies of service agreements
- During the incident
- After the incident

Example of IRP Incident-handling procedures



Before an Attack

Users

1. Don't put suspicious media in your co
   Check your system before booting for
   suspicious USB drives.
2. Don't download free games or utilitie
   system without authorization from th
   services department.
3. Don't click on links or open attachme
   in unsolicited e-mail. Make sure all att
   are from the sending party by confirm
4. Don't forward messages that ask you
   warn others of a virus or threat.

Technology Services

1. Ensure virus/malware protection softv
   is installed, properly configured, and
2. Automate whenever possible.
3. Provide awareness and training to all
   users on proper use of the e-mail syste
   antivirus software.

After an Attack

Users

1. Scan your computer regularly and
   thoroughly for additional viruses/m
2. Review e-mail (TITLES ONLY, DO NO
   REOPEN attachments) for suspicious
   content.
3. Write down everything you were d
   before you detected the virus/malw
4. Verify that your antivirus/antimalwa
   software and definitions are up to

Technology Services

1. Conduct an incident recovery invest
2. Interview all users detecting the vir
3. Verify that all systems antivirus/mal
   software and definitions are up to
4. Reconnect quarantined users to the
5. Brief all infected users on proper ar
   procedures.
6. File the incident recovery investigat
7. Notify all users that this particular s
   of virus/malware has been detected
   antivirus/antimalware software and

During an Attack

Users

1. If your antivirus/antimalware software detects an attack, it will delete the virus/malware or quarantine the file that carries it. Record any messages that your software displays and notify IT Services immediately.
2. If your computer begins behaving unusually or you suspect that you have contracted a virus or other malware, turn off your computer immediately by pulling the plug. Notify IT Services immediately.

Technology Services

1. If users begin reporting virus attacks, record the information provided by the users.
2. Temporarily disconnect those users from the network at the switch.
3. Begin scanning all active systems for that strain of virus.
4. Deploy a response team to inspect the users' systems.

Figure 10-8 Example of IRP incident-handling procedures

Incident Response Actions

- Incident response actions can be organized into three basic phases:
  1. Detection—Recognition that an incident is under way
  2. Reaction—Responding to the incident in a predetermined fashion to contain and mitigate its potential damage
  3. Recovery—Returning all systems and data to their state before the incident

1.Detecting Incidents

- Incident classification is the process of examining an adverse event or incident candidate and determining whether it constitutes an actual incident
- Three categories of incident indicators:
  - Possible indicators
    - *Presence of unfamiliar files*
    - *Presence or execution of unknown programs or processes*
    - *Unusual consumption of computing resources*
    - *Unusual system crashes*

1.Detecting Incidents (cont.)

- Three categories of incident indicators (cont.):
  - Probable indicators
    - *Activities at unexpected times*
    - *Presence of new accounts*
    - *Reported attacks*
    - *Notification from an Intrusion Detection and Prevention System (IPDS)*
  - Definite indicators
    - *Use of dormant accounts*
    - *Changes to logs*
    - *Presence of hacker tools*
    - *Notifications by partner or peer*
    - *Notification by hacker*

Indicators of Compromise (IOC)

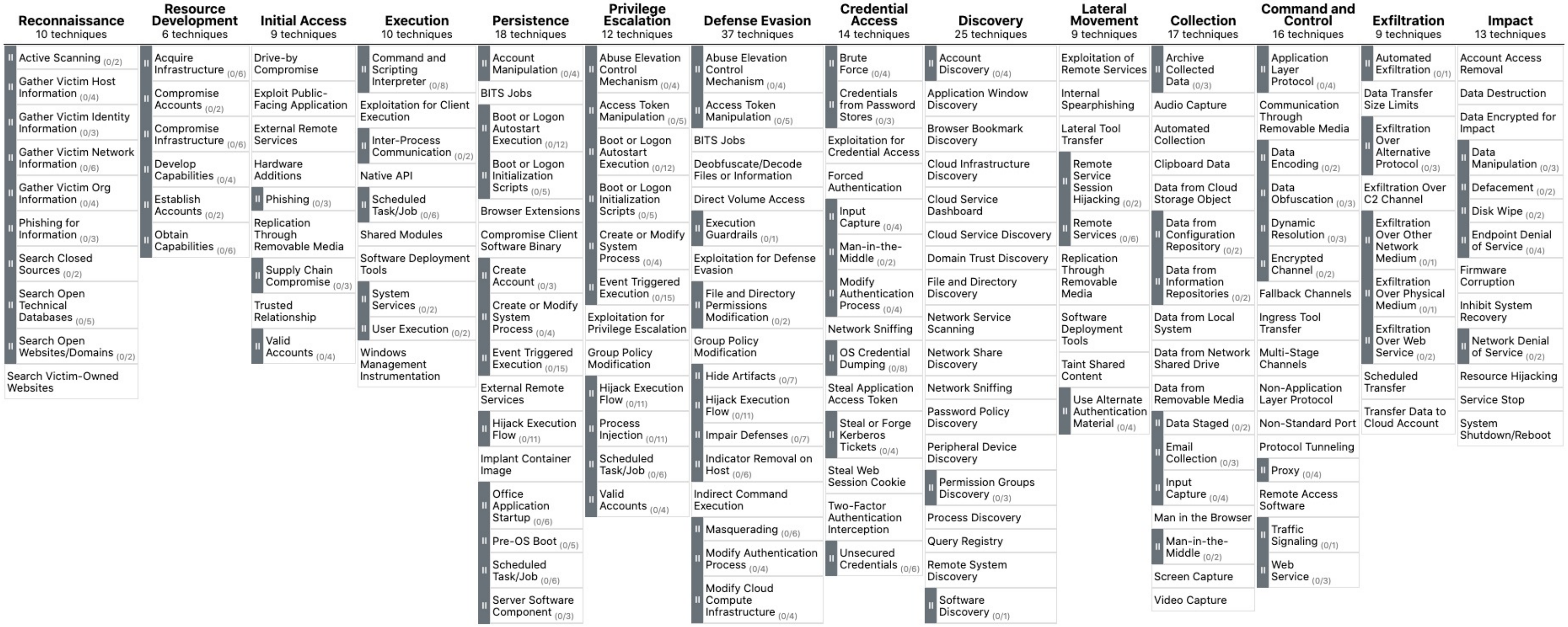
- Forensic artifacts that are used as signs that, with high confidence, indicates a computer intrusion.
  - Such as:
    - Unusual traffic going in and out of the network
    - Unknown files, applications, and processes in the system
    - Suspicious activity in administrator or privileged accounts
    - Irregular activities such as traffic in countries an organization doesn’t do business with
    - Dubious log-ins, access, and other network activities that indicate probing or brute force attacks
    - Anomalous spikes of requests and read volume in company files
    - Network traffic that traverses in unusually used ports
    - Tampered file, Domain Name Servers (DNS) and registry configurations as well as changes in system settings, including those in mobile devices
    - Large amounts of compressed files and data unexplainably found in locations where they shouldn’t be

MITRE ATT&CK Framework

- It contains a set of techniques used by adversaries to accomplish a specific objective.
  - **Reconnaissance**: gathering information to plan future adversary operations, i.e., information about the target organization
  - **Resource Development**: establishing resources to support operations, i.e., setting up command and control infrastructure
  - **Initial Access**: trying to get into your network, i.e., spear phishing
  - **Execution**: trying the run malicious code, i.e., running a remote access tool
  - **Persistence**: trying to maintain their foothold, i.e., changing configurations
  - **Privilege Escalation**: trying to gain higher-level permissions, i.e., leveraging a vulnerability to elevate access
  - **Defense Evasion**: trying to avoid being detected, i.e., using trusted processes to hide malware
  - **Credential Access**: stealing accounts names and passwords, i.e., keylogging
  - **Discovery**: trying to figure out your environment, i.e., exploring what they can control
  - **Lateral Movemen**t: moving through your environment, i.e., using legitimate credentials to pivot through multiple systems
  - **Collection**: gathering data of interest to the adversary goal, i.e., accessing data in cloud storage
  - **Command and Control:** communicating with compromised systems to control them, i.e., mimicking normal web traffic to communicate with a victim network
  - **Exfiltration**: stealing data, i.e., transfer data to cloud account
  - **Impact**: manipulate, interrupt, or destroy systems and data, i.e., encrypting data with ransomware

MITRE ATT&CK Framework (cont.)

- It contains a set of techniques used by adversaries to accomplish a specific objective.



Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
				Hijack Execution Flow (0/11)	Scheduled Task/Job (0/6)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data Staged (0/2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (0/4)	Impair Defenses (0/7)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (0/3)	Protocol Tunneling		Service Stop
				Office Application Startup (0/6)		Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (0/4)	Proxy (0/4)		System Shutdown/Reboot
				Pre-OS Boot (0/5)		Indirect Command Execution	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (0/6)		Masquerading (0/6)		Process Discovery		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
				Server Software Component (0/3)		Modify Authentication Process (0/4)		Query Registry		Screen Capture	Web Service (0/3)		
						Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery		Video Capture			
								Software Discovery (0/1)					

Source: https://attack.mitre.org/#

2. Reacting to Incidents

- Once an incident has been confirmed and properly classified
  - The IR plan moves from the detection phase to the reaction phase
- An effective IR plan includes the following steps:
  - Notification of key personnel
    - Alert roster, alert message
  - Documentation of the incident
    - It should record the who, what, when, where, why and how of each action taken while the incident is occurring
    - It serves as a case study after the fact
  - Assignment of tasks

2. Reacting to Incidents (cont.)

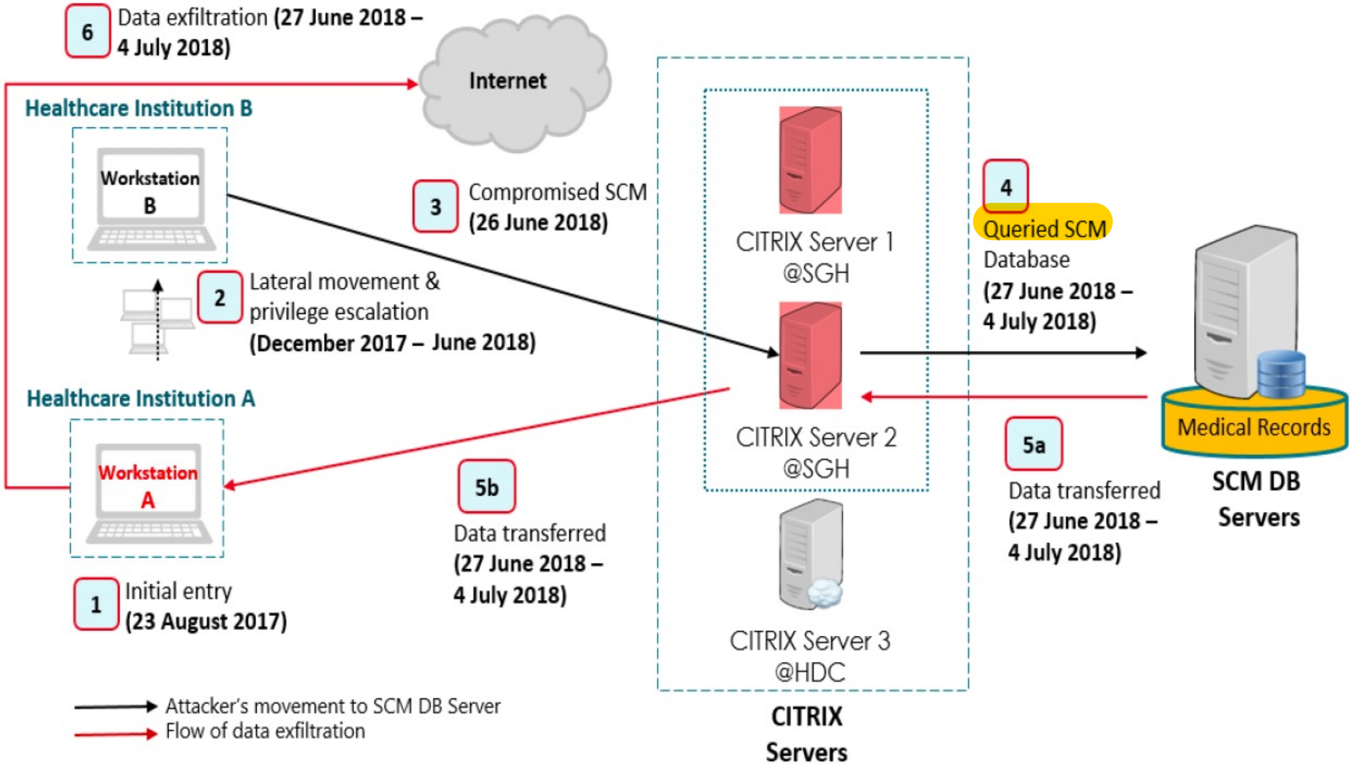
- Incident containment strategies:
  - Disabling compromised user accounts
  - Reconfiguring a firewall to block problem traffic
  - Temporarily disabling the compromised process or service
  - Taking down the conduit application or server
    - Example: e-mail server
  - Stopping all computers and network devices

- The nature of the attack and the organization's technical capabilities may dictate strategy

Case: SingHealth Breach

- *Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack*

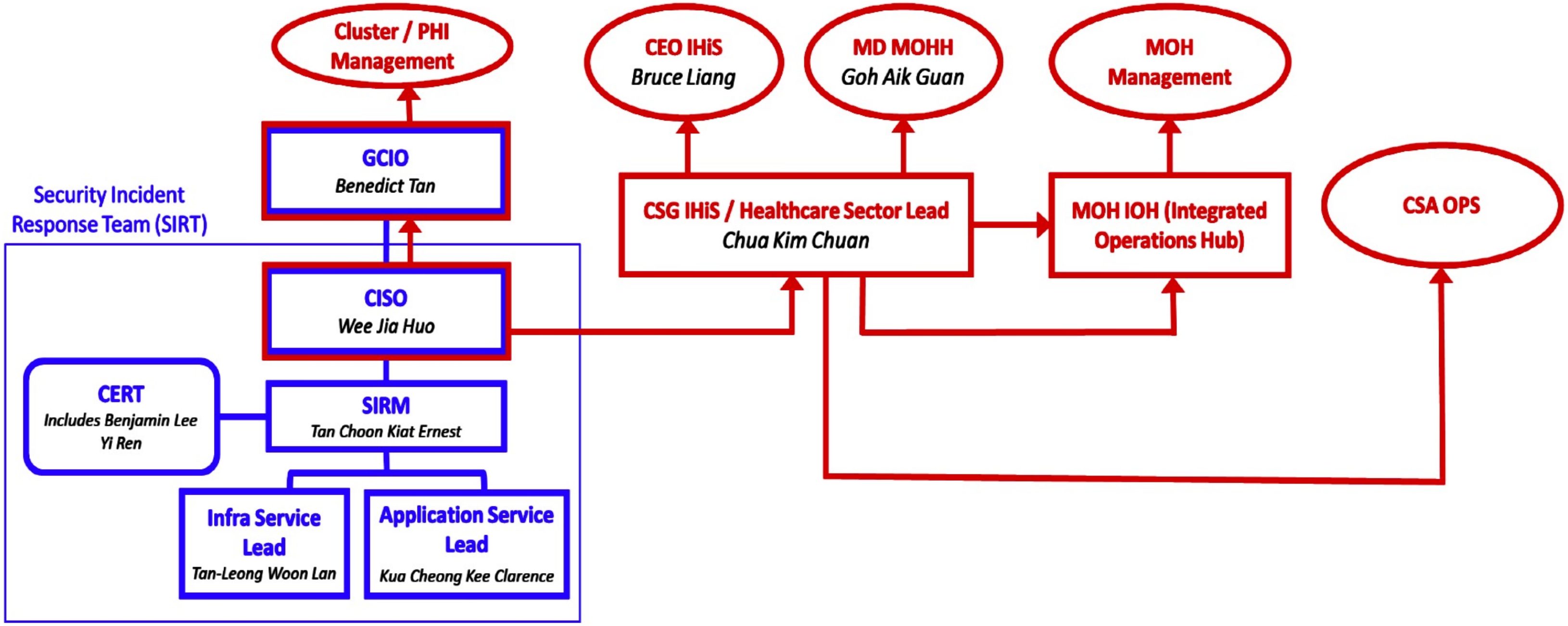
Figure 7: Key events of the Cyber Attack


6
Data exfiltration (27 June 2018 – 4 July 2018)
Internet
Healthcare Institution B
Workstation B
3
Compromised SCM (26 June 2018)
2
Lateral movement & privilege escalation (December 2017 – June 2018)
Healthcare Institution A
Workstation A
1
Initial entry (23 August 2017)
5b
Data transferred (27 June 2018 – 4 July 2018)
CITRIX Server 1 @SGH
CITRIX Server 2 @SGH
CITRIX Server 3 @HDC
CITRIX Servers
4
Queried SCM Database (27 June 2018 – 4 July 2018)
5a
Data transferred (27 June 2018 – 4 July 2018)
Medical Records
SCM DB Servers
Attacker's movement to SCM DB Server
Flow of data exfiltration

Case: SingHealth Breach (cont.)

- *Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack*

In blue – Security Incident Response Team reporting structure (IR-SOP)
In red – Security incident reporting flow (SIRF)



Case: SingHealth Breach (cont.)

- *Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack*
  - "The SIRM (Security Incident Response Manager) and the SingHealth CISO were both aware of the suspicion of attack since 13 June 2018 and the remediation efforts of 4 July 2018. They were both copied on emails and were members of a chatgroup created to investigate these incidents. The SingHealth CISO was apprised of the investigations but did not make further enquiries. Instead, he waited passively for updates. The SIRM was overseas until 18 June 2018 without nominating a covering officer. During this time, neither the SIRM nor the SingHealth CISO escalated the matter despite their knowledge of these circumstances through meetings and messages. Also, neither the SIRM nor the SingHealth CISO took any steps to activate the SIRT in accordance with the IR-SOP."

Source: https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx

Case: SingHealth Breach (cont.)

- *Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack*
  - Key findings:
    - "The Security Incident Response Manager ("SIRM") and Cluster Information Security Officer ("Cluster ISO") for SingHealth, who were responsible for incident response and reporting, held mistaken understandings of what constituted a 'security incident', and when a security incident should be reported.
    - The SIRM delayed reporting because he felt that additional pressure would be put on him and his team once the situation became known to management.
    - The evidence also suggests that the reluctance to escalate the matter may have come from a belief that it would not reflect well in the eyes of the organisation if the matter turned out to be a false alarm.
    - The Cluster ISO did not understand the significance of the information provided to him, and did not take any steps to better understand the information. Instead, he effectively abdicated to the SIRM the responsibility of deciding whether to escalate the incident."

Case: SingHealth Breach (cont.)

- *Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack*
  - 1) the Commissioner finds that it is insufficient for IHiS to have merely informed its non-security staff to alert the relevant personnel through emails, circulars, wallpapers and intranet banners.
  - 2) IHiS had admitted that while the SIRF and IT-SPS were made available via IHiS' intranet, it had not developed any written policy on IT security incident reporting for its non-security staff. Furthermore, regular training sessions and staff exercises should have been conducted to ensure that all IHiS staff are familiar with the IT security incident reporting and their role in recognising and reporting suspected IT security incidents.

non - security personnels should also be well aware of the SOP of participating in IR work

Source: https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx

3. Recovering from Incidents

- Once the incident has been contained and system control has been regained
  - Incident recovery can begin
- First task is to inform the appropriate human resources
- IRT must assess the full extent of the damage
  - To determine what must be done to restore the systems
- Incident damage assessment - determination of the scope of the breach of confidentiality, integrity, and availability of information assets

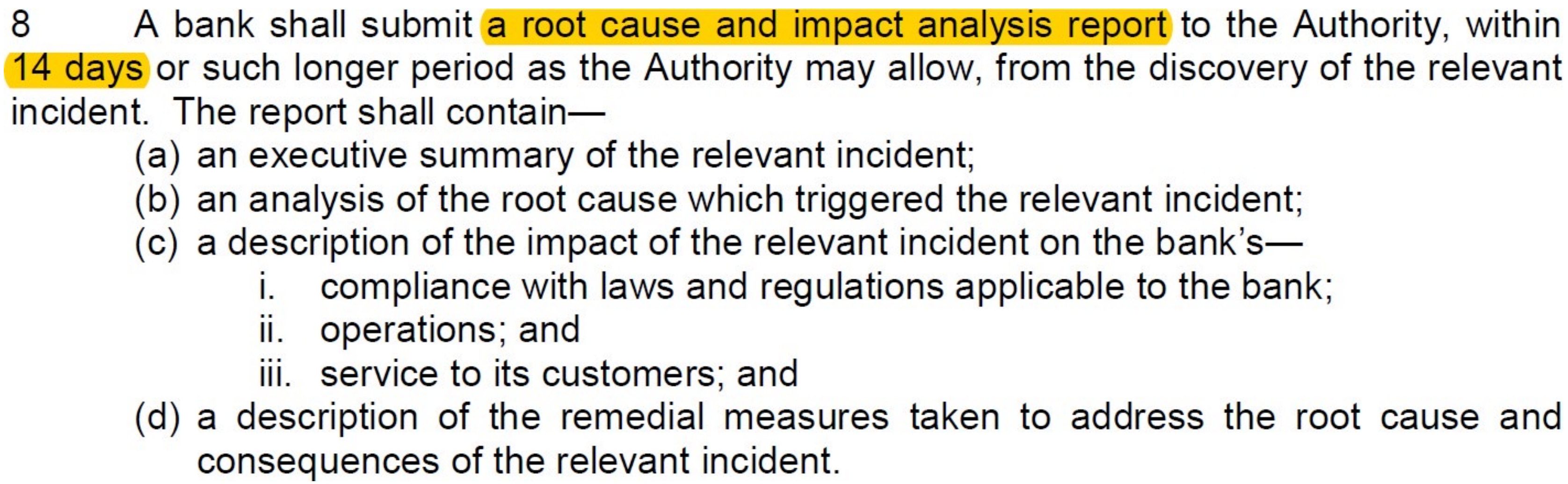
3. Recovering from Incidents (cont.)

- Recovery process steps:
  - Identify vulnerabilities that allowed incident to occur
  - Address safeguards that failed to stop or limit the incident
  - Restore data from backups
  - Restore the services and process in use
  - Continuously monitor the system
  - Restore the confidence of the members of the organization's communities of interest

- **After-action review (AAR):** detailed examination of the events that occurred

summarise the whole incident and identify the learning points for everyone

Example: MAS NOTICE 644



8 A bank shall submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report shall contain—

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the bank's—

i. compliance with laws and regulations applicable to the bank;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

Incident Response Planning

- NIST

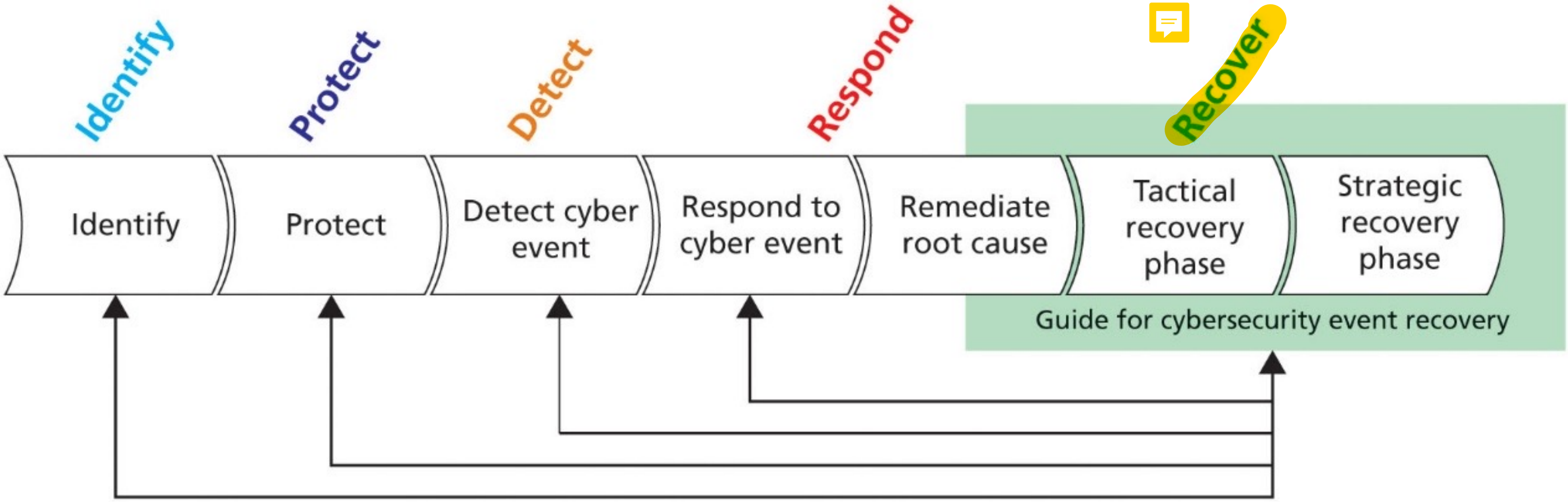


Figure 10-7 NIST Cybersecurity Framework

Disaster Response Planning

example is the Maserk ransomware attack

What is Disaster Recovery Planning?

- Preparation for and recovery from a disaster
  - Natural or caused by humans
- **Disaster recovery (DR) plan**: often activated when the IR plan no longer can handle the effective and efficient recovery from loss
- In general, an incident is a disaster when:
  - The organization is unable to contain or control the impact of an incident, or
  - The level of damage or destruction from an incident is so severe the organization is unable to quickly recover.
- The key role of a DR Plan is defining how to reestablish operations at the location where the organization is usually located (primary site)

Planning to Recover

- Key elements of the DR plan:
  - *Clear delegation of roles and responsibilities*
  - *Execution of the alert roster and notification of key personnel*
  - *Clear establishment of priorities*
  - *Procedures for documentation of the disaster*
  - *Action steps to mitigate the impact of the disaster on the operations of the organization*
  - *Alternative implementations for the various system components, should primary versions be unavailable*

Disaster Recovery Response Teams

- DR Management
- Communications
- Computer Recovery (Hardware) Team
- Systems Recovery (OS)
- Network Recovery Team
- Storage Recovery
- Applications Recovery
- Data Management
- Vendor Contact
- Damage Assessment and Salvage
- Business Interface
- Logistics
- Others as needed.

Responding to Disaster

- If physical facilities are intact
  - DR team should begin restoration of systems and data to work toward full operational capability
- If facilities are destroyed
  - Alternative actions must be taken until new facilities can be acquired
- When disaster threatens the viability of an organization at the primary site, the DR process becomes a business continuity process

Business Continuity Planning

can see how many companies might not have BCP already prepared since due to the pandemic there are many companies not ready to react with this rare but crucial plan

What is Business Continuity Planning?

- Disaster makes current business location unusable
  - **Business Continuity (BC) Plan** allows the business to continue at an alternate location
- Most properly managed by the CEO or COO
- Activated and executed concurrently with the DR plan when the disaster is major or long term

- While BCP reestablishes critical functions at alternate site, DRP focuses on reestablishment at the primary site

Continuity Strategies

- Several continuity strategies for business continuity, determining factor is usually
  - cost

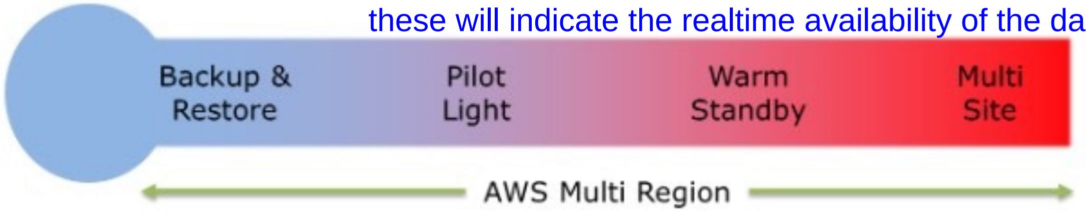
there are also non-exclusive

- Three exclusive-use options:
  - Hot sites
    - Fully configured computer facility, with all services, communication links, and plant operations
  - Warm sites
    - Provides many of the same services as a hot site, but typically software applications are not installed and configured
  - Cold sites
    - Provides only rudimentary services and facilities. No computer hardware or peripherals are provided.

only have the room and water/light - nothing else provided

Continuity Strategies

- AWS cloud:
  - With multiple regions and availability zones, recover from disaster using different DR approaches.
    - Backup & Restore
    - Pilot Light
      - □ Replicate part of your IT structure for a limited set of core services
    - Warm standby
      - □ A scaled-down version of a fully functional environment is always running in the cloud.
    - Multi-site



these will indicate the realtime availability of the data

Continuity Strategies (cont.)

- Three shared-use options:
  - Timeshare
    - Hot/warm/cold, but is leased in conjunction with a business partner
  - Service bureaus
    - Service agency that provides a service for a fee
  - Mutual agreements
    - A contract between two organizations in which each party agrees to assist the other in the event of a disaster

For NUS - the backup data center is in NUS High School
- they are also who we share mutual agreement with

Crisis Management

maybe something like the data breach of PII - such as the HIV data leak case

Crisis Management

- Focuses more on the effects that a disaster has on people than its effects on information assets
- According to Gartner Research, the crisis management team is responsible for managing the event from an enterprise perspective and performs the following roles:
  - Supporting personnel and their loved ones during the crisis
  - Keeping the public informed about the event and the actions being taken to ensure the recovery of personnel and the enterprise
  - Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties

Timing & Sequence of CP Elements

CP Implementation Timeline

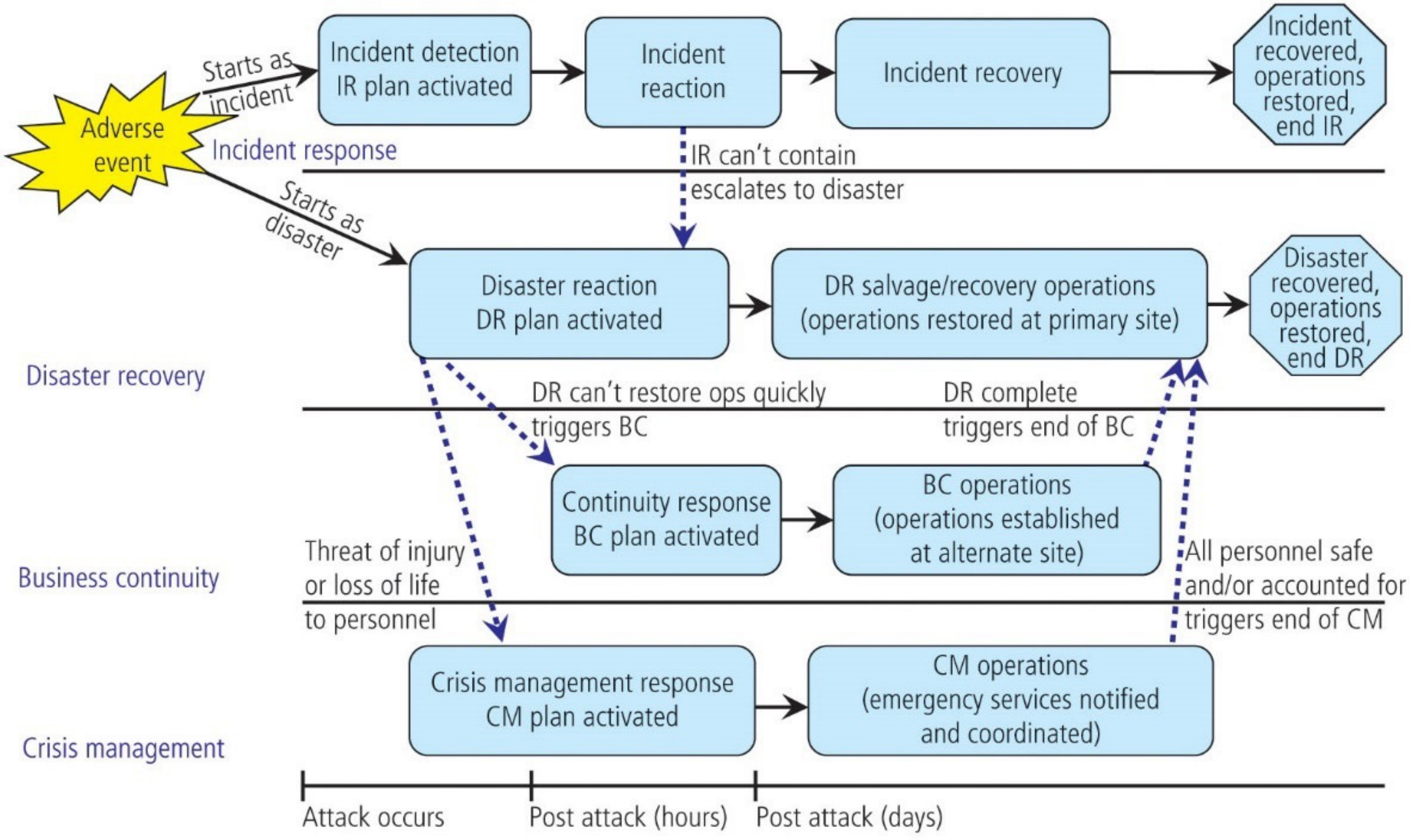
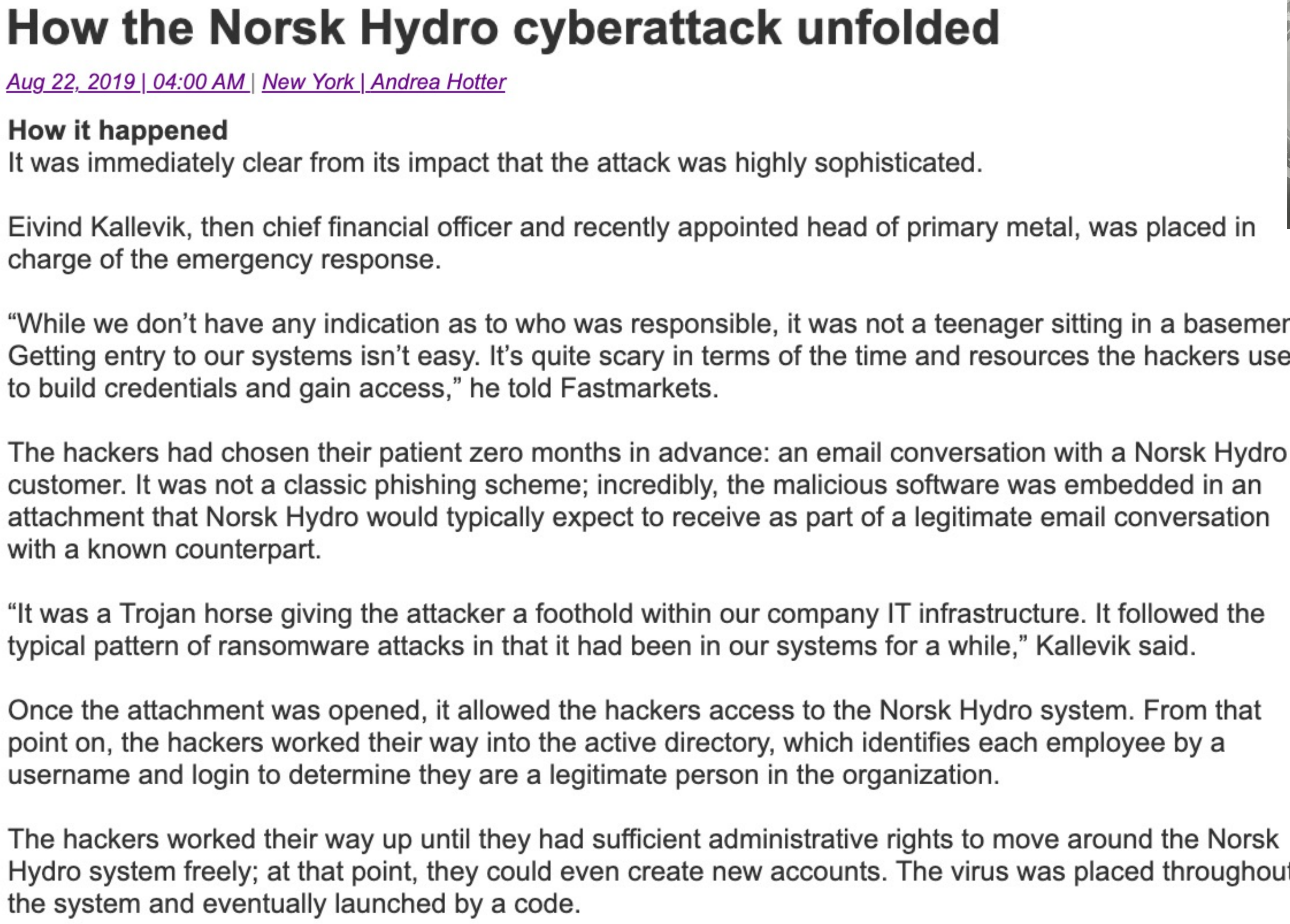

Adverse event
Starts as incident
Incident detection IR plan activated
Incident reaction
Incident recovery
Incident recovered, operations restored, end IR
Incident response
IR can't contain escalates to disaster
Starts as disaster
Disaster reaction DR plan activated
DR salvage/recovery operations (operations restored at primary site)
Disaster recovered, operations restored, end DR
Disaster recovery
DR can't restore ops quickly triggers BC
DR complete triggers end of BC
Continuity response BC plan activated
BC operations (operations established at alternate site)
Business continuity
Threat of injury or loss of life to personnel
All personnel safe and/or accounted for triggers end of CM
Crisis management response CM plan activated
CM operations (emergency services notified and coordinated)
Crisis management
Attack occurs
Post attack (hours)
Post attack (days)

Figure 10-14 Contingency planning implementation timeline

Norsk Hydro Cyber Attack



How the Norsk Hydro cyberattack unfolded

Aug 22, 2019 | 04:00 AM | New York | Andrea Hotter

How it happened
It was immediately clear from its impact that the attack was highly sophisticated.

Eivind Kallevik, then chief financial officer and recently appointed head of primary metal, was placed in charge of the emergency response.

“While we don’t have any indication as to who was responsible, it was not a teenager sitting in a basement. Getting entry to our systems isn’t easy. It’s quite scary in terms of the time and resources the hackers used to build credentials and gain access,” he told Fastmarkets.

The hackers had chosen their patient zero months in advance: an email conversation with a Norsk Hydro customer. It was not a classic phishing scheme; incredibly, the malicious software was embedded in an attachment that Norsk Hydro would typically expect to receive as part of a legitimate email conversation with a known counterpart.

“It was a Trojan horse giving the attacker a foothold within our company IT infrastructure. It followed the typical pattern of ransomware attacks in that it had been in our systems for a while,” Kallevik said.

Once the attachment was opened, it allowed the hackers access to the Norsk Hydro system. From that point on, the hackers worked their way into the active directory, which identifies each employee by a username and login to determine they are a legitimate person in the organization.

The hackers worked their way up until they had sufficient administrative rights to move around the Norsk Hydro system freely; at that point, they could even create new accounts. The virus was placed throughout the system and eventually launched by a code.

important to have backup for everything - including communication channels

Testing Contingency Plans

Testing Contingency Plans

- Contingency plans must be tested to identify vulnerabilities and faults
- Test strategies
  - **Desk check**
    - Distribute copies of the appropriate plans to all personnel with assigned incident roles
  - **Structured walk-through**
    - All involved personnel walk through the steps they would take during an event
  - **Simulation**
    - Each person works individually to simulate the performance of each task
  - **Full interruption**
    - Individuals follow each and every procedure, including interruption of service, restoration of data from backups, and notification of appropriate individuals

Next week – Reading week

- Course review and final exam briefing
    - Next Wed: 10-11am (attendance: optional)
    - Recorded.
- Online exam
    - Time:
        - □ Mon, 29 Nov 2021
        - □ 5-7pm
    - Channel
        - LumiNUS-Quiz
    - Format
        - Open book
        - All lecture, tutorial, guest talk content are examinable.
    - Invigilation
        - Zoom proctoring
        - Screen recording