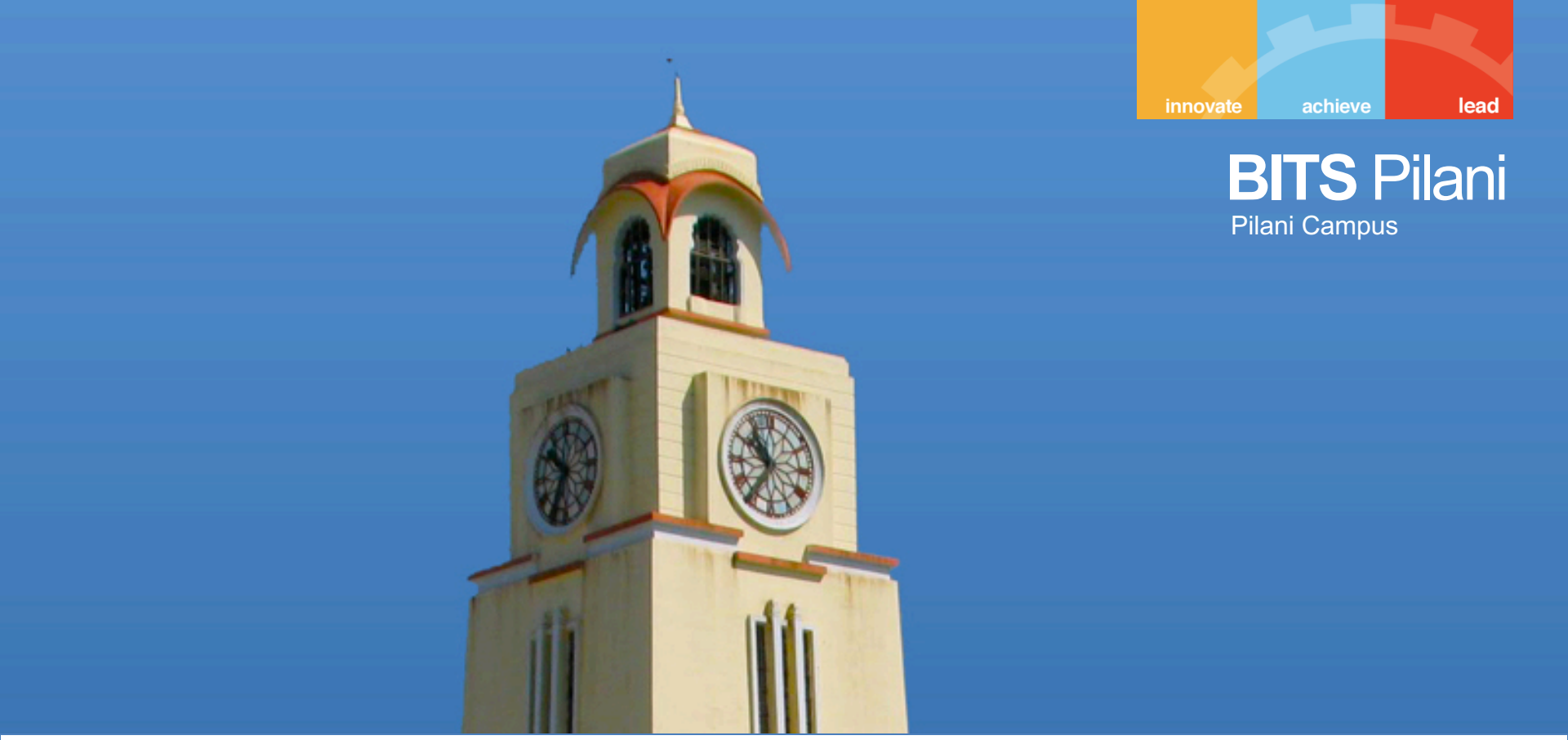
BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP



innovate achieve lead

BITS Pilani
Pilani Campus

SSZG681: Cyber Security
Lecture No: 07

Management and Incidents

Agenda

- Event, Incident and Incident Management
- Incident Management phases
- Preparation phase
  - Security response plan
  - Security committee
  - Business Continuity Plan
- Detection phase
- Containment, Mitigation and Recovery phase
- Post-review
- Communication phase
- Computer Emergency Response Team (CERT)

Security Incident Management: Key Definitions

- **Cyber Security Event:** A cyber security change that may have an impact on organisational operations (including mission, capabilities, or reputation).
- **Cyber Security Incident:** A single or a series of unwanted or unexpected cyber security events that are likely to compromise organisational operations.
- **Cyber Security Incident Management:** Processes for preparing, for detecting, reporting, assessing, responding to, dealing with and learning from cyber security incidents.

Basic Principles

- There is no simple one-size-fits-all solution
- Top management's commitment is paramount: active involvement with budget
- Involve every member of the organization
- Keep an off-line copy of documents required during an incident
- Don't link backups to rest of the system
- Importance of logging and keeping security logs for a certain period (upto 6 months)
- Keep cyber security response plan and related information/ documents regularly updated
- Ensure compliance to all legal aspects while managing a cyber security incident
- Document every step of a cyber security incident

Security Incident Management Phases

1. **Preparation phase:** Plan how to handle a security incident
   - Create a cyber security incident response plan and keep it up to date
   - Content of a cyber security incident response plan
   - Assigning responsibilities and creating a cyber security incident response team
   - Call upon external experts
   - Equip your organisation to address a cyber security incident
   - Prepare your communication strategy
   - Cyber insurance
2. **Detection phase:** Identify potential security incidents
   - Categories of incidents
   - Methods to detect incidents

Security Incident Management Phases

3. **Containment, Mitigation & Recovery phase:** Handling an actual security incident
   - Convene your cyber security incident response team
   - Situational awareness
   - Containing a cyber security incident
   - Eradication and clean-up
   - Recovery
4. **Prepare for Future:** Follow-up, closure and learnings for future
   - Evaluation of lessons learned and future actions: organise a post-incident review
   - Incident tracking and reporting
5. **Communication:** During and post security incident
   - Tools
   - Incident specific communication plan

Preparation Phase

Preparation Phase

- Plan how to handle a security incident
  - Create a cyber security incident response plan and keep it up to date
  - Content of a cyber security incident response plan
  - Assigning responsibilities and creating a cyber security incident response team
  - Call upon external experts
  - Equip your organisation to address a cyber security incident
  - Prepare your communication strategy
  - Cyber insurance

Security Response Plan

- A security plan is an official record of current security practices plus a blueprint for orderly plan to improve those practices
- Security plan identifies and organizes the security activities of critical computer assets
- Create a formal document for cyber security incident response plan and keep it up to date
- Review cyber security response plan at regular interval and incorporate changes as required
- Define a number of standard operating procedures for common incidents that are likely to occur in the organization

Security Response Plan: Key Elements

- What to protect
- What is a security incident
- who has the ultimate responsibility in case of a security incident
- Potential incident categories
- Composition and roles of incident response team
- How to address technical protection and end-point protection
- When will external experts be involved
- Internal and external communication in case of security incident
- Identify vital assets and potential threats
- When will external experts be involved
- Internal and external communication in case of security incident

Contents of Security Plan

1. **Security Policy:** Goals for security and willing ness of people to work to achieve those goals
2. **Current State Assessment:** Assessment of current status security
3. **Security Requirements:** Recommendation to meet the security goals
4. **Recommended Controls:** Mapping controls to the vulnerability identified in the policy and requirements
5. **Accountability:** Who is responsible for each security activity
6. **Timetable:** When different security activities are to be done
7. **Plan Maintenance:** Specifying a process for periodic updation of security plan

1: Security Policy

- Documentation of an organization's security needs and priorities
- High level statement of purpose and intent
- What are the most precious assets for an organization to protect:
  - **Pharmaceutical:** research on new drugs, marketing strategy
  - **Hospital:** Confidentiality of its patients
  - **TV Studio:** Archives of previous broadcasts
  - **On-line Merchant:** Availability of on-line presence
- Trade-off between level of security and cost, inconvenience, time factors

1: Security Policy…

- Policy document must answer:
  - Who should be allowed access?
  - To what systems and organizational resources should the access be allowed?
  - What type of access should each user be allowed for each resource?
- Policy document should also specify:
  - **Organizations goals on security:** protect data leakage, data loss, data integrity, loss of business due to system failure etc. what is higher priority – serving customers or securing data?
  - **Where does the responsibility of security lie:** should it be with security team, each employee or respective managers?
  - **Organizations commitment to security:** where does security fit into organization structure (a team in some department or an executive level position), who provides security support to employees?

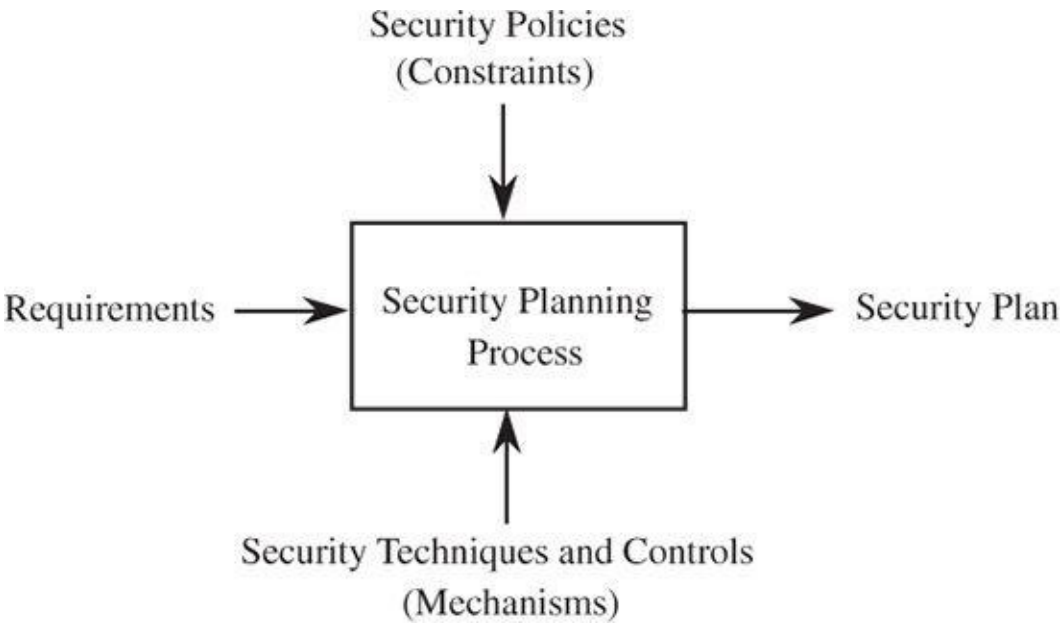
2: Current Status Assessment

- What are current vulnerabilities – perform risk analysis
- A systematic analysis of systems, IT environment and where things could go wrong
- Listing of current assets, controls in place to protect the assets and security threats to the assets
- Limits of responsibility for security
  - **Who is responsible:** in joint ventures may have one organization providing security support
  - **Boundaries of responsibility:** who provides security for routers, leased lines, internal systems, cloud data storage etc?
- Vulnerabilities to the system
  - Due to use of system in an unanticipated manner
  - Due to new scenarios or requirements

3: Security Requirements

- Identify assets and potential threats
  - Identify businesses and resources that need to be protected
  - Determine 'Vital' assets and resources
  - Assign business priority for recovery
  - Document how these business systems work: Network schema, equipment and services inventory, account and access list etc
- Document internal and external security demands
- Document functional and performance requirements for desired level of security
- Determine compliance to regulatory or commercial standards
- Confidentiality, integrity and availability needs
- Strength and quality level of security required

3: Requirement, Constraints & Controls



Requirement Characteristics

- Correctness
- Consistency
- Completeness
- Realism
- Need
- Verifiability
- Traceability

4: Recommended Controls

- Mechanism to implement the security requirements
- Vulnerability mapping and methods to address the vulnerabilities
- How system will be designed and developed to implement the requirements

5: Accountability

Following questions need to be answered:

- Who is responsible for implementing controls when a new vulnerability is discovered?
- Who is the internal contact point for cyber security incidents? And how can he be contacted?
- What are the different incident response tasks? And who is responsible for doing what?
- Who is managing the incident from business/technical side? This should be someone within the company with decision-making authority, who will follow the incident from the beginning until the end.
- Who will liaise with senior management?
- Who can engage the external incident response partner?
- Who can file a complaint with law enforcement/inform the regulatory bodies?
- Who is entitled to communicate with the press and external parties?

5: Accountability…

Skill	Responsibilities	Roles
Incident Management	Manage the cyber security incident from the moment of its detection until its closure.	Cyber Security Incident Response Manager
Business Decision Capability	Assessing the business impact and act upon it. Engage the right resources. Take decisions on how to proceed e.g. decide if the internet connection of a compromised system can be shut down and when is the most appropriate time. Decide when to start clean- up activities. Decide whether to file a complaint or not	Management
Network Management Capability	Technical know-how on the organisation's network (firewall, proxies, IPS, routers, switches,...). Analyse, block or restrict the data flow in and out of your network. IT operations Information security and business continuity	ICT Technical Staff
Workstation and Server Administration Capability	Analyse and manage compromised workstations and servers	ICT Technical Staff
Legal Advice	Assess the contractual and judicial impact of an incident.Guarantee that incident response activities stay within legal, regulatory and the organisation's policy boundaries. Filing a complaint	Legal department/ Company Lawyer
Communication Skills	Communicate in an appropriate way to all concerned stakeholder groups. Answer customer, shareholders, press questions right away	Communication or Public Relation department
Forensic Skills	Gather and analyse evidence in an appropriate way i.e. in a way that the evidence is acceptable by a court of law	ICT Technical Staff
Physical Security	Handle the aspects of the incident that are linked to: a) the physical access to the premises, b) the physical protection of the cyber infrastructure	Security Officer
Crisis Management	Crisis Management	Crisis Manager

Smaller organization will need a minimum of Incident Response Manager and ICT Technical Staff

5: Accountability…

- Specific responsibilities
  - Users may be responsible for their own personal computers and devices
  - Project leaders may be responsible for project data and assets
  - Managers may be responsible to ensure that people they supervise implement security measures
  - DBAs may be responsible for access to and integrity of their databases
  - Information officers may be responsible for creation, use, retention and proper disposal of data
  - HR may be responsible for screening employees and training them in security measures
- Document the contact (phone, backup phone, email, residential address etc) details of security response team members and keep it in secure place

6: Timetable

- Timeline of how and when the elements of the plan will be executed
- Major milestone dates
- Expensive and complicated security measures should be implemented in gradual manner
- Order of control implementation and proper training plan for the same
- Extensible plan to ensure inclusion of new conditions and changes
- Plan should be reviewed periodically

7: Plan Maintenance

- Security plan must be revisited periodically to adapt it to changing conditions
- Review of security situation periodically to evaluate that the system is as secure as it is intended to be
- Change in users, data, equipment, and new exposures need to be addressed
- Current means of control may become obsolete or ineffective
- Inventory of assets and list of controls needs to be scrutinized and updated
- Security plan should define the timeline for these periodic reviews

Composition of Security Committee

- A security committee should be constituted representing all stakeholders (interested parties)
- Representation from different aspects of computer systems like operating system, networks, applications etc
- Committee size depends on size and complexity of security requirements of the organization
- Optimum size is between 5 – 9 members
- Sub-committees can be formed to address a particular section of the security plan (if required)

Commitment to Security Plan

- Plan must be accepted by organization leadership
- Commitment across all organization layers is required for implementation and execution of security functions
- Three groups of people are MUST for success:
  - Management, Operations and Users/Customers
  - Planning team must be sensitive to needs of each group affected by plan
  - Groups affected by security recommendations must understand what the plan means for the way they will use the system and perform business activities
  - Management must be committed to use and enforce the security measures
- Training and publicity is critical to understand security objectives
- Users to use the controls properly and effectively

Commitment to Security Plan…

- Security plan must articulate the potential losses v/s cost incurred in implementing security measures
- Security plan must present technical issues in a language which can be understood and appreciated by non-technical people
- Security plan should avoid technical jargon and should use business terminology
- Security plan should describe vulnerabilities and risks in terms of financial terms for management attention

Business Continuity Planning

- For a business: 'No computers - means no customers - means no sales - means no profit'
- For govt, educational, non-profit agencies: 'No computers means no effective services to customers hence adverse future impact'
- 80 percent of the organizations affected by security disasters close down in 18-24 months
- Business Continuity Plan (BCP) documents how business will function during or after a computer security incident
  - Normal security plan covers computer security during normal operations protecting against vulnerabilities
- BCP deals with situations having:
  - Catastrophic situations: all or major part of computing capacity is unavailable
  - Long duration: outage is expected to last so long that business will suffer

Business Continuity Planning…

innovate achieve lead

- BCP guides response to a crisis that threatens the business existence
  - Fire destroys complete network of the company
  - Seemingly permanent failure of a software renders computing system unusable
  - Abrupt failure of a supplier of electricity, network, telecom, or other critical service component
  - Natural disasters prevent support staff to reach operation centre
- Strategy to cope with such critical situations is to advance planning and preparation. The BCP steps are:
  - Assess the business impact of the crisis
  - Develop a strategy to control the impact
  - develop and implement a plan for the strategy

Business Continuity Plan Steps

1. Assess business impact
2. Develop strategy
3. Develop plan

1: Assess Business Impact

- What are the essential assets – things if lost will prevent doing business
  - Network, customer reservation system, traffic controllers etc
- What could disrupt availability of these assets – what are the vulnerabilities
  - A network could be unavailable due to failure, loss of power or corruption
- What is the minimum set of assets or activities required to keep business operational to some degree
  - Prepare manual system for such activities

2: Develop Strategy

innovate achieve lead

- Plan to safeguard critical assets
- Create backups, redundant hardware, manual process as alternatives
- Plan for operations at reduced capacity
- Pl for service from another center (in case of call centers)
- Identify function to preserve – half of A and half of B or full of A
- Define timeframe for restoration of business to normal
- Define strategy with multiple steps depending on how much & long the business will be disabled
- BCP forces a company to set base priorities
- Strategy must result in selection of best alternatives

3: Develop Plan

- A Plan specifies – who is in-charge when an incident occurs, what to do and who does it?
- Defines & justifies advance arrangements – redundant site, backup hardware, stockpiling supplies etc
- Advance training of people to respond to crisis
- Documented action procedures
- Person in-charge
  - Declares start and end of emergency
  - Decides to take actions best suited to the situation at give moment
- Focus of plan is
  - To keep critical assets and serious vulnerabilities to avoid business disruption for long
  - To keep the business going while someone else addresses the crisis
- BCP plan focuses on business needs

Detection Phase

How to identify Incidents?

- Identify warning signs: Normal operations throw exceptions which could be precursor to a larger failure
  - A pop-up for security patch application
  - A software upgrade
  - A network capacity utilization threshold break warning
  - An important configuration file missing
- Monitor and manage the warnings to avoid bigger catastrophe
- Develop incident handling capability to identify and respond to such incidents

How to identify Incidents?

- Categories of incidents
  - Define cyber security incident and related terms
  - Identify possible categories of cyber security incidents
- Methods to detect incidents
  - Employees are best positioned to detect an incident
  - Create awareness in employees about cyber security incidents and create a mechanism to reports such incidents
  - Technology and end point protection
  - Detection tools like IDS and IPS
  - Network and system logs
  - Anti-virus tools

Containment, Mitigation & Recovery Phase

Security Incident Management Phase

- Handling an actual security incident
  - Convene your cyber security incident response team
  - Situational awareness
  - Containing a cyber security incident
  - Eradication and clean-up
  - Recovery

Convene Security Response Plan

- When an actual incident is detected, inform security response manager
- Security response manager must convene a meeting of the cyber security incident response team
- Team must evaluate the risks fast in order to take the right measures.
- The cyber security incident manager and his team will report to the CEO, who will have to validate their decisions.

Situational Awareness

- Collect all available information on the activities around the incident's timeframe.
- Preserve integrity of the information and indexation.
- Verify if any data have been lost/stolen.
- Create full disk images, take (remote) memory dumps of a suspicious machine and protect these with write-blockers.
- Central storage of security information (images, logs, firewall logs etc) enables faster analysis and query resolution during investigation process.

Containing an Incident

innovate achieve lead

- Recover quickly or gather evidence:
  - Disconnect the systems immediately, recover fast and limit damage
  - Take the time to collect evidence against the cybercriminal who perpetrated the system
- Find a balanced approach
  - What could happen if the incident were not contained?
  - Is the attack or breach doing immediate severe damage?
  - Is there (potential) damage and/or theft of assets?
  - Is it necessary to preserve evidence? And if so, what sources of evidence should the organisation acquire? Where will the evidence be stored? How long should evidence be retained?
  - Is it necessary to avoid alerting the hacker?
  - Do you need to ensure service availability or is it OK to take the system offline? (for example, services provided to external parties)

Investigation: Gathering evidence

- To gather evidence, forensic investigation must be performed before you eradicate the incident
- Ask for external experts if required specifically in areas of digital forensics and legal. Some type of attacks (i.e. DDOS) also require specialized technical knowledge
- In order to admissible in court, evidence should be collected according to procedures that meet all applicable laws and regulations.
- Avoid compromising the evidence like:
  - Don’t immediately shutdown servers
  - Don’t immediately cut of the servers from internet
  - Don’t restore from backup if you are not sure about backup infection
  - Don’t re-install on same server without a forensic copy

Eradication and Cleanup

- Eradication must be started after investigation is complete and root cause of incident is known
- Eradication exercise must be fast, synchronized and thorough for all infected artifacts
- Potential list of actions:
  - Running a virus or spyware scanner to remove the offending files and services
  - Deleting malware and Updating signatures
  - Disabling or changing password of breached user accounts
  - Identifying and mitigating all vulnerabilities that were exploited
  - Identifying security gaps and fixing them
  - Informing employees about the threat and giving them instructions on what to avoid in the future
  - Informing external stakeholders such as the media and your customers
  - Informing top management about eradication and clean-up results

Eradication and Cleanup…

- Few action examples:
  - Individual files can be detected, quarantined or deleted from systems by the anti-virus solution. This solution should be open to accept specific virus definitions provided by you
  - Phishing e-mails can be blocked on the mail gateway by blocking based on the sender, the mail relay or parts of the content
  - IP and domain-based indicators can be blocked based on network traffic, by adding them to access lists, firewall policies or proxy policies. Therefore, it is important to have the necessary capability to implement these changes in an ad-hoc manner

Recovery

- Recovery refers to restoring of the system(s) in order to return to normal operation and (if applicable) remediate vulnerabilities to prevent similar incidents.
- There are multiple ways to restore following a cyber security incident with different impact on recovery time, cost limitations or data loss.
- Recovery depends on time and financial means at disposal
- It also depends on damage the incident may have caused to infrastructure
  - For example, it is possible that you don't have an uninfected backup. In that case the system must be reinstalled from scratch
- Before the system is put back online, it should be validated for both security and business functions.

Recovery…

innovate achieve lead

	RECOVERY TIME	COST	DATA LOSS	REMARKS
Clean the malicious artefacts and replacing the compromised files with clean versions	Fast	Cost-effective		You might leave undiscovered artefacts behind
Restore from a backup	Medium	Cost-effective		This is only possible if you have a known good backup. In some cases, it is hard to determine the timestamp of the initial incident, or the incident might have been going on for a long time, with no backup from the period before the incident.
Rebuild the system(s) or environment from zero	Slow, not time-efficient	Very costly	Chances of data loss	This is, however, the only way to be 100% sure that you got rid of the perpetrator.

Communication Phase

Communication

- Communication strategy
  - Communicate TO WHOM
  - WHICH INFORMATION to Communicate
  - WHO will communicate
  - WHEN to communicate
- Communication types
  - Compliance related: Regulatory authorities & affected customers
  - Incident handling and resolution progress: Internal teams and third party response teams.
  - Reputation damage limiting: Customers, partners, media and internal staff
- Communication stakeholders
  - Internal stakeholders: Top management, impacted managers, employees
  - External stakeholders: media, customers, suppliers, other partners, etc.
  - Official stakeholders: Privacy Commission, Industry Regulator, CERT, Police

When to Communicate

innovate achieve lead

- Timing is important:
  - Some stakeholders will need information as soon as possible, because they can help in containing the cyber security incident (e.g. organisation's top management, employees)
  - Other stakeholders have to be contacted within a certain legally imposed timeframe (e.g. Privacy Commission, affected customers)
  - Others may contact you and in such a case you should have your answers ready (e.g. media)
- In order not to alert the attacker, it may be necessary to insert a **no-communication time** from the moment of the detection of the incident until the moment a full picture of the incident and an action plan is ready.
- Alerted attacker may re-treat and remove all his/her traces

Reporting to Authorities

- Reporting to authorities is a very specific and important for different reasons:
  - In some cases, reporting data leakage or other security incidents is **legally mandatory**
  - Certain authorities can **help** you. The cyber security incident you are faced with may not be an isolated incident. Authorities may have information that can help you contain your incident faster.
  - In case you want to file a complaint against the criminal behind the cyber security incident, you need to contact the law enforcement authorities.
  - Reporting to the authorities is a necessary step, allowing the **stocktaking and measuring of cybercrime** in the country.
  - Increased knowledge and understanding of the phenomenon and its prevalence will help to improve the overall security landscape, e.g. through the shaping of preventive measures and countermeasures.

Reporting to CERT

- Cyber security incidents should be reported to the central Cyber Emergency Response Team (CERT).
- CERT documents 'Indicators Of Compromise' (IOCs) observed on a network or an operating system that indicate that there has been an intrusion.
- CERT can determine whether the incident is isolated or not
- CERT will be able to provide some information and advice related to the incident that can help the victim to take effective countermeasures
- The information shared with CERT may help to prevent attacks on other computer systems.
- Information reported to CERT includes:
  - Your contact details , type of the incident, date of incident
  - Is the incident ongoing?
  - How did you notice this incident and What's the impact of the incident?
  - Have you already taken actions or measures? If so, which ones?
  - Do you have logs or other useful data?
  - Who have you already informed?

Notifying Individuals whose Personal Data were Compromised

- The notification to the persons involved needs to be clear and easy to understand.
- Following as a minimum needs to be informed:
  - Name of responsible for data processing
  - Contact information for further information
  - Short description of the incident during which the data breach occurred;
  - Probable date of the incident
  - Type and nature of personal data involved
  - Possible consequences of the breach for the persons involved
  - Circumstances in which the data breach occurred
  - Measures taken by the data processor to prevent the data breach
  - Measures which the person responsible recommends the involved persons to take to limit possible damages

Post-Incident Review Phase

Lessons Learned and Future Actions

- Is any security control action to be taken
  - Incident happened because patches were not updated
  - Access breached due to poor password
  - So, action required to ensure controls (patches to be applied in certain period, educate users for stronger passwords)
  - What can be done to avoid any control failures
- Did the incident response plan work
  - Did everyone knew who to inform?
  - Did the team have required resources to deal with incident?
  - Was the response quick?
  - What should eb done differently next time?

Post Incident Review

innovate achieve lead

- **Objective:** All cyber security incidents should be formally reviewed after the incident resolution to verify if security mechanisms or mitigating controls need to be put in place or adapted to prevent similar incidents in the future
- **Why:** Cyber security incidents can indicate important shortcomings in your security strategy or practice. Every important incident needs to be analysed to evaluate if lessons for future improvement can be learned.
- Checklist of questions that can help to evaluate:
  - Were the cyber security incident management plan and procedures followed? Were they adequate? Should the plan be adapted on certain points?
  - Was information available in time? If no, would it have been possible to have it sooner and how?
  - Were there any steps or actions you have taken that might have inhibited the recovery?
  - Could your information sharing with other organisations be improved?

Post Incident Review…

- What corrective actions could prevent similar incidents in the future?
- Are there precursors or indicators that should be monitored to detect similar incidents more easily in the future?
- What additional tools or resources are needed to detect, analyse, mitigate future cyber security incidents?
- Did the cyber security response team have the right organisational authority to respond to the incident? Should you recruit more people or place a consulting firm, lawyer,...on retainer in case of a future cyber security incident?

Incident Tracking and Reporting

- **Objective:**
  - **TRACKING:** All cyber security incidents and their resolution must be documented.
  - **REPORTING:** All cyber security incidents and their resolution must be reported to top management and, if this function exists within your organisation, to the Information Security Officer.
- **Why:**
  - **TRACKING:** Similar incidents might happen again and might require the same handling procedures, or a small incident might turn out to be a part of a bigger incident that you discover later.
  - **REPORTING:** Top management and/or the people within your organisation that analyse your organisation's risks (e.g. Operational Risk Committee or equivalent) need to be aware of cyber security incidents.
- A report based on post-review conclusions, must be written for all cyber security incidents and kept together with other cyber security incident reports.
- All major security incidents should be reported immediately to top management.
- At least once a year all cyber security incidents must be reported and explained to top management and the people that analyse organisation's risks.

Computer Emergency Response Team (CERT)

Incident Response Teams

innovate achieve lead

- Organizations maintain a team of people trained and authorized to handle security incidents
- Called ‘Computer Emergency Response Team’ (CERT) or ‘Computer Security Incident Response Team’ (CSIRT)
- These have dedicated people, and flexible on call specialists

CSIRT Types

- Full organizational response team to cover all incidents
- Coordination centers to coordinate incident response activity across organizations
- National CSIRT to coordinate within country and with national CSIRTs of other countries
- Sector CSIRTs to assist investigating incidents specific to a particular business sector
- Vendor CSIRTs to coordinate with manufacturer of an equipment/product
- Outsourced CSIRTs hired to perform incident response on contract basis to other companies

CSIRT Types…

- CSIRTs operate within organizations, nationally, internationally, by vendor or by sector
- Security Operation Centers (SOC) perform day to day monitoring of networks and are first to notice an unusual situation
- Information Sharing and Analysis Centers (ISAC) share threat and incident data across CSIRTs

CSIRT Activities

- Reporting
- Detection
- Triage
- Response
- Post-mortem
- Education
- Study current data to predict future attack trends (preventive measure)

CSIRT Team Skills

- Collect, analyze and preserve digital forensic evidence
- Analyze data to infer trends
- Analyze the source, impact and structure of malicious code
- Help manage installations and networks by developing defenses such as signatures
- Perform penetration testing and vulnerability analysis
- Understand current technologies used in attacks

Information Sharing

- Incident affecting one site may affect another site and analysis from one place may help another place
- No standards for automated information sharing between CSIRTs
- Sharing is also hindered due to fear of competition, regulations and negative publicity

Thank You