Module-3

Security Standards Organization

ISO

- ISO (International Organization for Standardization) is the world's **largest developer** and publisher of **International Standards**.
- ISO is a **network** of the national standards institutes of **160 countries**, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.
- ISO is a **non-governmental organization** that forms a bridge between the public and private sectors.
- Many of its member institutes are part of the governmental structure of their countries, or are mandated by their government.
- Other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations.
- ISO enables a **consensus** to be reached on solutions that meet both the requirements of business and **the broader needs of society.**

ISO 27x

- ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization.
- National bodies, members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity.
- ISO and IEC technical committees collaborate in fields of mutual interest.
- Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, **ISO/IEC JTC 1.**
- International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.
- The main task of the joint technical committee is to prepare International Standards.
- Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

JTC-1

- ISO 27000 Series is developed by JTC1-SC27
- Certification is given for ISO 27001 Only
- There are a number of supporting standards and best practices

JTC-1

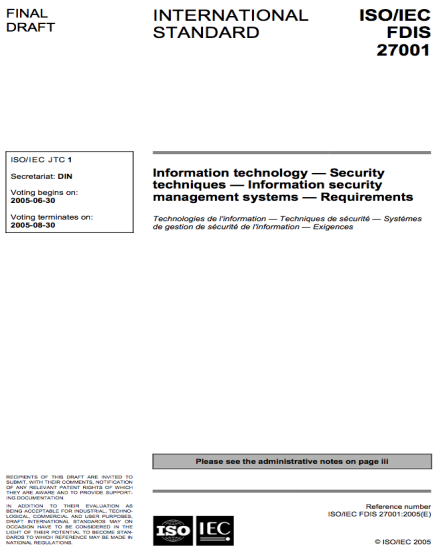
ISO 27001

- It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – the aim of which is to help organizations make the information assets they hold more secure.
- A European update of the standard was published in 2017.
- Organizations that meet the standard's requirements can choose to be certified by an accredited certification body following successful completion of an audit.
- The effectiveness of the ISO/IEC 27001 certification process and the overall standard has been addressed in a recent large-scale study.

ISO 27001

- **ISO/IEC 27000**, *Information security management systems — Overview and vocabulary*
- **ISO/IEC 27001:2005**, *Information security management systems Requirements*
- **ISO/IEC 27002:2005**, *Code of practice for information security management*
- **ISO/IEC 27003**, *Information security management system implementation guidance*
- **ISO/IEC 27004**, *Information security management — Measurement*
- **ISO/IEC 27005:2008**, *Information security risk management*
- **ISO/IEC 27006:2007**, *Requirements for bodies providing audit and certification of information security management systems*
- **ISO/IEC 27007**, *Guidelines for information security management systems auditing*
- **ISO/IEC 27011**, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

ISO 27001


FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 27001

ISO/IEC JTC 1

Secretariat: DIN

Voting begins on: 2005-06-30

Voting terminates on: 2005-08-30

Information technology — Security techniques — Information security management systems — Requirements

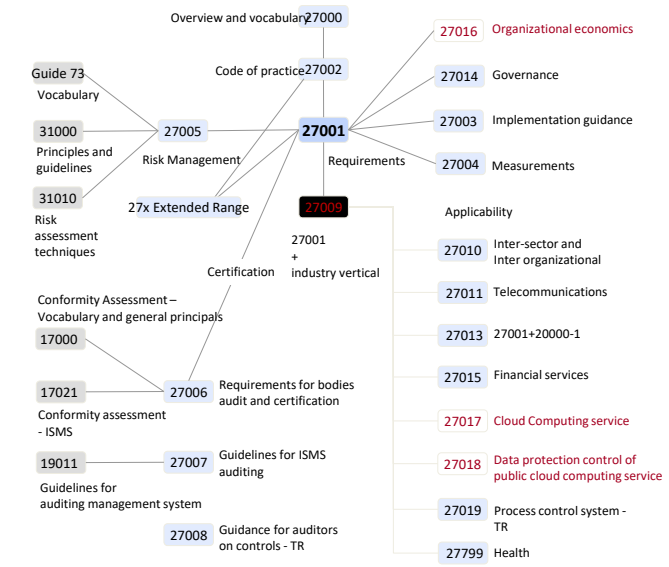
Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Please see the administrative notes on page iii

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC FDIS 27001:2005(E)



ISO 27002:2005

- 12 areas covered in ISO 27002:2005
  1. Information security management
  2. Risk assessment and treatment
  3. Security policy
  4. Organization of information security
  5. Asset management
  6. HR Security
  7. Physical security
  8. Communication and Operations Management
  9. Access control
  10. IS acquisition, development and maintenance
  11. IS incident management
  12. Business continuity

Consultative Committee For Telephone and Telegraphy (CCITT)

- The CCITT, now known as the ITU-T (for Telecommunication Standardization Sector of the International Telecommunications Union), is the primary international body for fostering cooperative standards for telecommunications equipment and systems. It is located in Geneva, Switzerland.

American National Standards Institute (ANSI)

- American National Standards Institute (ANSI) oversees the creation, promulgation and use of thousands of norms and guidelines that directly impact businesses in America in nearly every sector: from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more.
- ANSI is also actively engaged in accreditation - assessing the competence of organizations determining conformance to standards.

Institute Of Electronics and Electrical Engineers (IEEE)

- IEEE is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity.
- IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities.
- IEEE, pronounced "Eye-triple-E," stands for the Institute of Electrical and Electronics Engineers.

Electronic Industries Association

- The Electronic Industries Association (EIA) comprises individual organizations that together have agreed on certain data transmission standards such as EIA/TIA-232 (formerly known as RS-232).
- The Electronics Industries Alliance (EIA) is an alliance of trade organizations that lobby in the interest of companies engaged in the manufacture of electronics-related products.

National Institute of Standards and Technology (NIST)

- National Institute of Standards and Technology's web site.
- Founded in 1901 and now part of the U.S. Department of Commerce, NIST is one of the nation's oldest physical science laboratories.
- US Congress established the agency to remove a major handicap to U.S. industrial competitiveness at the time.
- The National Centre for Standards and Certification Information (NCSCI) provides research services on standards, technical regulations and conformity assessment procedures for non- agricultural products.

National Center for Standards and Certification Information (NCSCI) Policy

- The U.S. Department of Commerce (DOC), National Institute of Standards and Technology (NIST), National Center for Standards and Certification Information (NCSCI) does not provide analyses or comparisons of documentary standards, nor does it establish equivalence among documentary standards or technical regulations.
- Documentary standards include:
  - Product standards and specifications to establish qualities or requirements for a product
  - Process standards to specify requirements to be met by a process (example: assembly line operation)
  - Performance standards to describe desired functions
  - Design standards to define product specifications
  - National standards developed and promulgated through a National Standards Body (example: ANSI)
  - International standards developed by international organizations (examples: ISO, IEC)

World Wide Web Consortium (W3C)

- The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards.
- Led by Web inventor Tim Berners-Lee and CEO Jeffrey Jaffe, W3C's mission is to lead the Web to its full potential.

Internet Corporation for Assigned Names and Numbers (ICANN)

- ICANN's role is to oversee the huge and complex interconnected network of unique identifiers that allow computers on the Internet to find one another.
- To reach another person on the Internet you have to type an address into your computer - a name or a number.
- That address has to be unique so computers know where to find each other.
- ICANN coordinates these unique identifiers across the world.
- Without that coordination we wouldn't have one global Internet.

Backups of security devices, Performance Analysis

Backup
Why Backup?

"If you are not backing up your files regularly, you deserve to lose them."

Average user experiences loss once a year

Backup
What Can Cause Data Loss?

- Incorrect software use
- Input data incorrectly
- Software may harm data
- Hard disk malfunctions
- Accidentally delete files
- Virus infection

Backup

Methods	Media
Full backup Differential backup Incremental backup	Diskette Tape Zip disk CD-R / CR-RW DVD-RAM Mirrored hard drive

Best Practices for storing and securing your data

The goal of data storage is to ensure that your research data are in a safe and secure environment which is accessible, secure, and redundant.

Hardware and Software

- Desktops and laptops – not for storage of original or only copies of data!
- Removable media – not for storage of master copies. Check it yearly and migrate to new media every 3-5 years
- Cloud storage
  - store additional copies of data
  - no sensitive data, esp. highly sensitive data
  - Read terms and conditions

Hardware and Software

- Desktops and laptops – Computer equipment can be damaged, lost, stolen.
- Removable media – Media degrades over time. Software programs to read the media change and can become obsolete. Hardware changes over time, and is not always backward compatible.
- Cloud storage
  - Cloud providers go out of business
  - Data formats change (what you upload may not be useable when you download it)
  - Accidents happen. Data is corrupted, or stolen.

Servers and Network Drives

- Storage, backup and recovery available
- Who is responsible?
- Practical backup and recovery

File Formats

- Think about the ability to use and re-use data in the future. Both for you, and for others.
- Accessibility of future data because of technology changes - proactively plan for hardware and software obsolescence.
- Think about who needs access to your data. Are you collaborating with someone within the University, or outside of it?
- Conducting funded research - be aware of any data storage and data sharing requirements.
- Think about data security.

Best Practices for File Formats

Formats most likely to be accessible in the future are:

- non-proprietary
- open
- documented standard commonly used by a discipline-specific research community
- standard representation (ASCII, Unicode)
- unencrypted and uncompressed

Remember that comprehensive documentation (metadata) is essential to accurate use, and reuse, of all data.

Data Security and Access Control

- **Network security**
  - Keep confidential or highly sensitive data off computers or servers connected to the internet
- **Physical security**
  - Access to buildings and rooms
- **Computer systems & files**
  - Use strong passwords on files and systems
  - Virus protection (updated continuously and running!)
  - Encryption

Data Backups

- Reduces the risk of damage or loss
- Use multiple locations (here-near-far or 3-2-1)
- Create a backup schedule and put someone dependable in charge
- Use reliable backup medium
- Test your backup system (test file recovery, data consistency, data accuracy)

Module-3

Information Security Laws, Regulations & Guidelines

Information Security Laws, Regulations & Guidelines

- Information Security Law is the body of legal rules, codes, and standards that require you to protect that information and the information systems that process it, from unauthorized access.
- The legal risks are potentially significant if you don't take a pragmatic approach.
- Indian ministry of Communication and Information Technology has implemented IT-rules, 2011(Privacy rules).

Information Security Laws, Regulations & Guidelines

- India enabling legislation India Information Act 2000.
- While India continues to adhere to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Rules) enacted in 2011, the Centre for Internet and Society presented a new Privacy (Protection) Bill, 2013 (Bill), on September 30, 2013.

Information Security Laws, Regulations & Guidelines

- The Bill seeks to further refine provisions of the Rules, with a focus on protection of personal data through limitations on use and requirements for notice.
- The collection of personal data would be prohibited unless "necessary for the achievement of a purpose of the person seeking its collection," and, subject to sections 6 and 7 of the Bill, "no personal data may be collected under this Act prior to the data subject being given notice, in such form and manner as may be prescribed, of the collection."

Information Security Laws, Regulations & Guidelines

- The Bill acknowledges the collection of data with and without consent;
- The regulation of personal data storage, processing, transfer, and security; and discusses the different types of disclosure.

Information Security Laws, Regulations & Guidelines

- **Data protection authority and registration requirement**
  - No specific data protection authority exists the privacy rule states that, in case of breach as defined under Act, must answer to "the agency mandated under the Law"
  - No registration is required to collect the data.
  - Data security Council of India (DSCI) has been providing "DSCI Privacy Certified" for data collection.

Information Security Laws, Regulations & Guidelines

- **Protected personal data**
  - Personal data is information that relates to an identified or identifiable individual.
  - What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.

Information Security Laws, Regulations & Guidelines

- **Protected personal data**
  - If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.
  - If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable.
  - You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.

Information Security Laws, Regulations & Guidelines

- **Data Collection and Processing**
  - The Privacy Rules requires a Body Corporate that collects, receives, possesses, stores, deals, or handles sensitive or personal data to provide a privacy policy for handling of such data and ensure that the policies are available for view by the data subjects who have provided the information under contract.

Information Security Laws, Regulations & Guidelines

- **Data Collection and Processing**
  - The policy shall provide:
    - clear and easily accessible statements of its practices and policies;
    - the type of personal or sensitive personal data or information collected;
    - the purpose of collection and usage of such information;
    - the disclosure of information including sensitive personal data or information; and
    - reasonable security practices and procedures.

Information Security Laws, Regulations & Guidelines

- **Data Collection and Processing**
  - Data may be collected and processed when all of the following conditions are met:
    - the data subject has provided written consent and is aware at the time of collection that the information is being collected, the purpose of collection, the intended recipients of the information; and the name and address of the agency that is collecting and will retain the information;
    - the data subject has been provided with the option not to provide its sensitive personal data or information;
    - the data subject is permitted to withdraw his/her consent, in writing, at any time;
    - the information may be collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
    - the collection of the sensitive personal data or information is considered necessary for that lawful purpose.

Information Security Laws, Regulations & Guidelines

- **Data Transfer**
  - Disclosure of data to a third party requires prior permission of the data subject, whether the information is provided under contract or otherwise, except in the following situations:
    - Disclosure has already been agreed to in a contract;
    - Disclosure is necessary for compliance with a legal obligation;
    - Disclosure is pursuant to an order under the law.
    - Data is shared with government agencies with the authority to obtain the data for the purpose of verification of identity, or for the prevention, detection, investigation, prosecution, and punishment of offenses, including cyber incidents;

Information Security Laws, Regulations & Guidelines

- **Data Transfer**
  - Data may be transferred domestically or internationally to any person or Body Corporate that ensures the same level of data protection that is adhered to by the Body corporate, but the transfer is allowed only if:
    - the data subject consents; or
    - the transfer is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and the data subject.

Information Security Laws, Regulations & Guidelines

- **Data Security**
  - A Body Corporate is required to implement reasonable security practices and procedures.
  - The Privacy Rules indicate that reasonable practice methodologies include IS/ISO/EIC 27001 or other measures that have been pre-approved by the central government and are subject to annual audits by a central government approved auditor.

Information Security Laws, Regulations & Guidelines

- **Breach Notification**
  - There is no mandatory requirement to report data security breach incidents under the Privacy Rules.

Information Security Laws, Regulations & Guidelines

- **Other Considerations**
  - Data retention rules state that information should not be retained longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law.
  - Accordingly, outsourcing service providers in India should be exempted from obtaining consent from the individuals whose data they process.

Information Security Laws, Regulations & Guidelines

- **Enforcement & Penalties**
  - A corporate entity may be liable for up to Rs.5,00,00,000 for the negligent failure to implement and maintain reasonable practices and procedures, causing wrongful loss or gain.

Information Security Laws, Regulations & Guidelines

- **International Directory of laws:**
  - This directory includes laws, regulations and industry guidelines with significant security and privacy impact and requirements.
  - This is largely USA focused but used by International agencies as a reference point.

Information Security Laws, Regulations & Guidelines

Broad laws:

- Sarbanes-Oxley Act (SOX);
- Payment Card Industry Data Security Standard (PCI DSS);
- Gramm-Leach-Bliley Act (GLB) Act;
- Electronic Fund Transfer Act, Regulation E (EFTA);
- Customs-Trade Partnership Against Terrorism (C-TPAT);
- Free and Secure Trade Program (FAST);
- Children's Online Privacy Protection Act (COPPA);
- Fair and Accurate Credit Transaction Act (FACTA), including Red Flags Rule; Federal Rules of Civil Procedure (FRCP)

Information Security Laws, Regulations & Guidelines

Industry specific laws:

- Federal Information Security Management Act (FISMA);
- North American Electric Reliability Corp. (NERC) standards;
- Title 21 of the Code of Federal Regulations (21 CFR Part 11) Electronic Records;
- Health Insurance Portability and Accountability Act (HIPAA);
- The Health Information Technology for Economic and Clinical Health Act (HITECH);
- Patient Safety and Quality Improvement Act (PSQIA, Patient Safety Rule);
- H.R. 2868: The Chemical Facility Anti-Terrorism Standards Regulation

Data Backup

WHAT IS BACKUP?

- **Backup** is an additional copy of data that can be used for restore and recovery purposes

- This Backup copy can be created by:
  - Simply coping data (there can be one or more copies)
  - Mirroring data (the copy is always updated with whatever is written to the primary

WHY BACKUP?

- Disaster Recovery

Restores production data to an operational state after disaster

- Operational

Restore data in the event of data loss or logical corruptions that may occur during routine processing

- Archival

Preserve transaction records, email, and other business work products for regulatory compliance

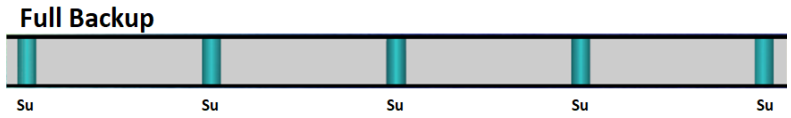
TYPES OF BACKUPS

Three basic types of backups:

- Full Backups
- Differential Backups
- Incremental Backups

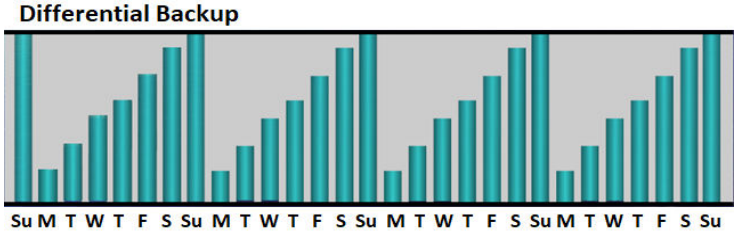
FULL BACKUP

- Full and complete backup of entire system:

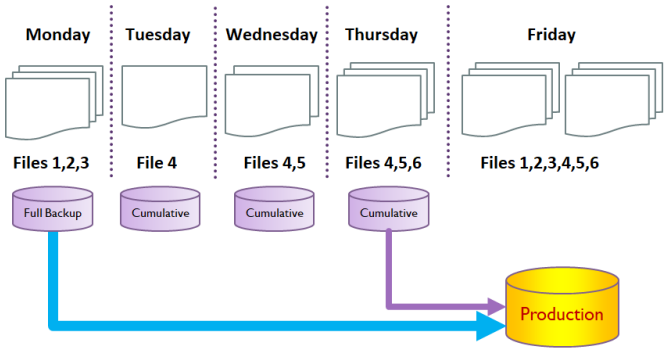


DIFFERENTIAL BACKUP

- Storage of all files that have changed or been added since last full backup:



RESTORING FROM DIFFERENTIAL BACKUP

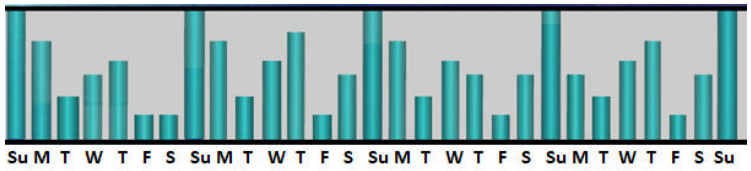


KEY FEATURES OF DIFFERENTIAL BACKUP

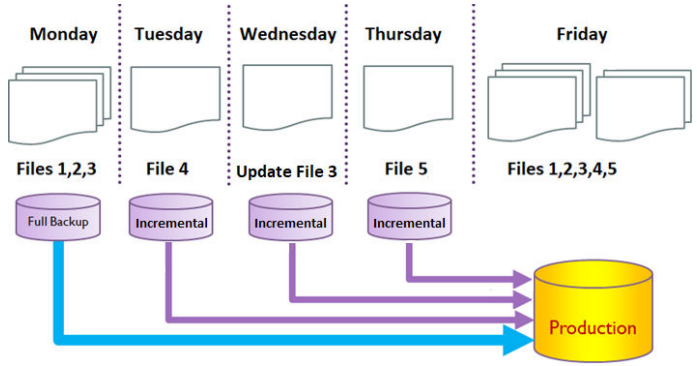
- More files to be backed up therefore it takes more time to backup and uses more storage space
- Much faster restore because only the last full and the last cumulative backup must be applied

INCREMENTAL BACKUPS

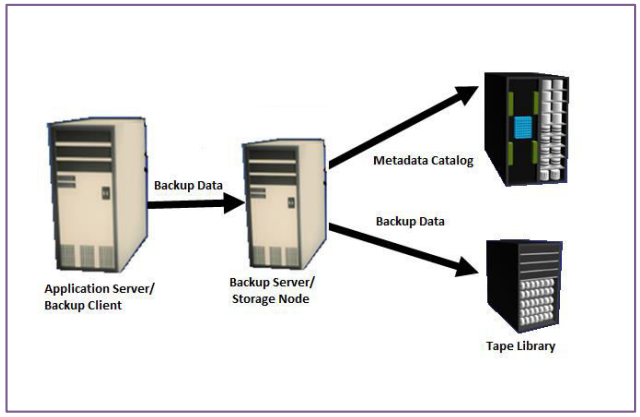
- Only archives data that have been modified that day.



INCREMENTAL BACKUPS

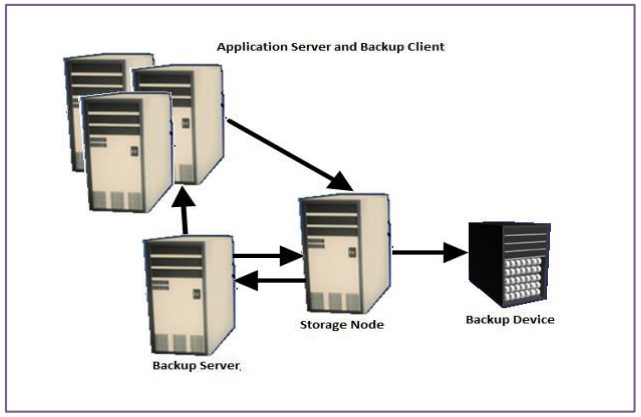


BACKUP ARCHITECTURE AND PROCESS

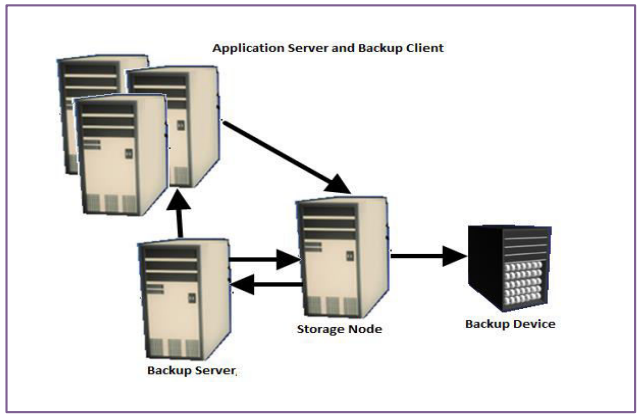


https://www.ques10.com/p/2626/explain-backup-and-restore-process-in-detail/

BACKUP OPERATION



RESTORE OPERATION



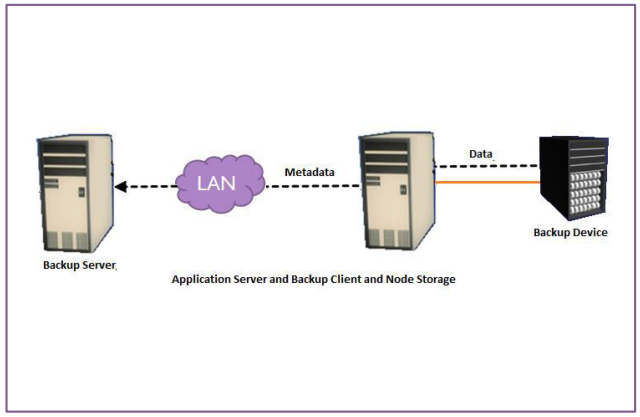
https://www.druva.com/blog/understanding-rpo-and-rto/

BACKUP TOPOLOGIES

There are three basic backup topologies

- Direct Attached Base Backup
- LAN Based Backup
- SAN Based Backup

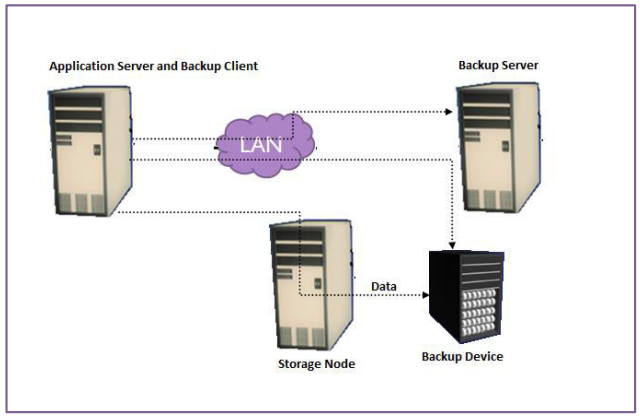
DIRECT ATTACHED BACKUP



DIRECT ATTACHED BACKUP

- **In a *direct-attached backup***, a backup device is attached directly to the client.
- Only the metadata is sent to the backup server through the LAN.
- This configuration frees the LAN from backup traffic.
- In the example shown in Figure depicts use of a backup device that is not shared.
- As the environment grows, however, there will be a need for central management of all backup devices and to share the resources to optimize costs.

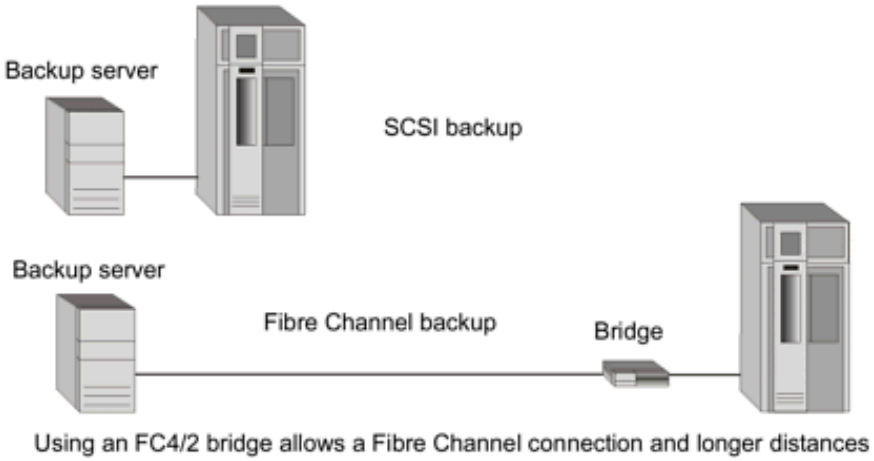
LAN BASED BACKUP



LAN BASED BACKUP

- **In *LAN-based backup***, all servers are connected to the LAN and all storage devices are directly attached to the storage node.
- The data to be backed up is transferred from the backup client (source), to the backup device (destination) over the LAN, which may affect network performance.
- Streaming across the LAN also affects network performance of all systems connected to the same segment as the backup server.
- Network resources are severely constrained when multiple clients access and share the same tape library unit (TLU).

SAN BASED BACKUP (LAN FREE)



Using an FC4/2 bridge allows a Fibre Channel connection and longer distances

SAN BASED BACKUP

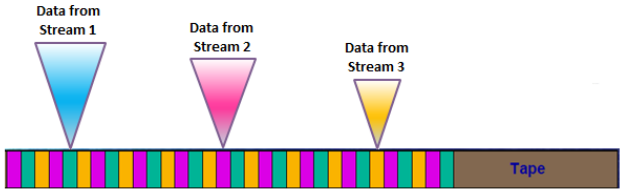
- **The *SAN-based backup*** is also known as the *LAN-free backup*.
- The SAN-based backup topology is the most appropriate solution when a backup device needs to be shared among the clients.
- In this case the backup device and clients are attached to the SAN.
- In this example, clients read the data from the mail servers in the SAN and write to the SAN attached backup device.
- The backup data traffic is restricted to the SAN, and backup metadata is transported over the LAN.
- However, the volume of metadata is insignificant when compared to production data.
- LAN performance is not degraded in this configuration.

https://flylib.com/books/en/3.316.1.62/1/

Mixed topology

- **The *mixed topology*** uses both the LAN-based and SAN-based topologies.
- This topology might be implemented for several reasons, including cost, server location, reduction in administrative overhead, and performance considerations.

BACKUP TO TAPE



TAPE LIMITATIONS

- Reliability
- Sequential Access
- Cannot be accessed by multiple hosts simultaneously
- Control environment for tape storage
- Wear and tear of tape

BACKUP TO DISK

- Ease of Implementation
- Fast access
- More reliable
- Random access
- Multiple host access
- Enhanced overall back and recovery performance

RAID - The challenge

- Disk transfer rates are improving, but much less fast than CPU performance
- We can use multiple disks to improve performance
  - by *striping* files across multiple disks (placing parts of each file on a different disk), we can use parallel I/O to improve access time
- Striping reduces reliability
  - 100 disks have 1/100th the MTBF (mean time between failures) of one disk
- So, we need striping for performance, but we need something to help with reliability / availability
- To improve reliability, we can add redundant data to the disks, in addition to striping

RAID

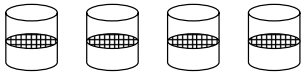
- A RAID is a Redundant Array of Inexpensive Disks
- Disks are small (physically) and cheap, so it's easy to put lots of disks (10s to 100s) in one box for increased storage, performance, and availability
- Data plus some redundant information is striped across the disks in some way
- How striping is done is key to performance and reliability

Some RAID tradeoffs

- Granularity
  - fine-grained: stripe each file over all disks
    - high throughput for the file
    - limits transfer to 1 file at a time
  - coarse-grained: stripe each file over only a few disks
    - limits throughput for 1 file
    - allows concurrent access to multiple files
- Redundancy
  - uniformly distribute redundancy information on disks
    - avoids load-balancing problems
  - concentrate redundancy information on a small number of disks
    - partition the disks into data disks and redundancy disks

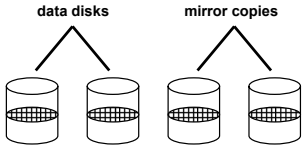
RAID Level 0

- RAID Level 0 is a non-redundant disk array
- Files are striped across disks, no redundant info
- High read throughput
- Best write throughput (no redundant info to write)
- Any disk failure results in data loss; sometimes a file, sometimes the entire *volume*



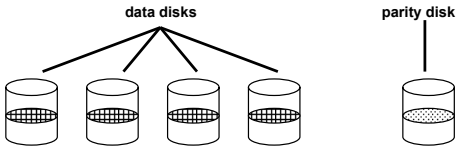
RAID Level 1

- RAID Level 1 is mirrored disks
- Files are striped across (half) the disks
- Data is written to multiple (two) places – data disks and mirror disks
- On failure, just use the surviving disk(s)
- Factor of N (2x) space expansion



RAID Levels 2, 3, and 4

- RAID levels 2, 3, and 4 use ECC (error correcting code) or parity disks
  - E.g., each byte on the parity disk is a parity function of the corresponding bytes on all the other disks
- A read accesses all the data disks
- A write accesses all the data disks plus the parity disk
- On disk failure, read the remaining disks plus the parity disk to compute the missing data



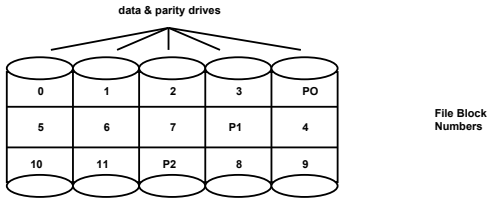
Refresher: What's parity?

1	0	1	1	0	1	1	0	1

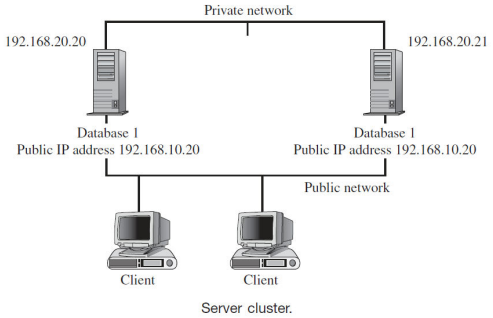
- To each byte, add a bit set so that the total number of 1's is even
- Any single missing bit can be reconstructed
- (Why does memory parity not work quite this way?)

RAID Level 5

- RAID Level 5 uses block interleaved distributed parity
- Like parity scheme, but distribute the parity info (as well as data) over all disks
  - for each block, one disk holds the parity, and the other disks hold the data
- Significantly better performance
  - parity disk is not a hot spot



Designing a Failover Solution



- Implement **clustering** to configure **failover** between two or more servers that perform the same role.
- Clustering is a process by which multiple servers share the same role, host name, and IP address on a network
- DNS/DHCP???
- A server cluster can consist of two types of nodes: active nodes and passive nodes. An **active node** is one that participates in handling service requests.
- A **passive node** is one that is inactive until a server configured as an active node fails.
- The number of nodes supported and the configuration supported depend on the operating system.
- For example, Windows Server 2003 supports up to eight nodes.
- A server cluster can use direct-attached storage or can connect to storage through a SAN.

Module-4

Incident Management

https://www.kennasecurity.com/blog/risk-vs-threat-vs-vulnerability/

Risk Assessment & Configuration Review

- Risk Assessment
  - Risk Overview
  - Risk Identification
  - Risk Analysis
  - Risk Treatment
  - Risk Management Feedback Loops
  - Risk Monitoring
- Security incident management
- Third party security management
- Incident Components, Roles

Risk Overview

- **Risk:**
  - A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action.

Risk Overview

- **Risk assessments:**
  - whether they pertain to information security or other types of risk, are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk.

Risk Overview

- **Risk assessments:**
  - All risk assessments generally include the following elements.
    - Identifying threats that could harm and, thus, adversely affect critical operations and assets.
    - Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.

Risk Overview

- **Risk assessments Steps:**
  - **Step** 1: Identify the hazards.
  - **Step** 2: Decide who might be harmed and how.
  - **Step** 3: Evaluate the **risks** and decide on precautions.
  - **Step** 4: Record your findings and implement them.
  - **Step 5**: Review your **assessment** and update if necessary.

Risk Overview

- **Risk assessments:**
  - Estimating, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materializes, including recovery costs.
  - Identifying cost-effective actions to mitigate or reduce the risk.
  - These actions can include implementing new organizational policies and procedures as well as technical or physical controls.

Risk Overview

- **Risk assessments:**
  - Documenting the results and developing an action plan.
  - There are various models and methods for assessing risk, and the extent of an analysis and the resources expended can vary depending on the scope of the assessment and the availability of reliable data on risk factors.
  - In addition, the availability of data can affect the extent to which risk assessment results can be reliably quantified.

Risk Overview

- **Risk assessments:**
  - A quantitative approach generally estimates the monetary cost of risk and risk reduction techniques based on
    1. the likelihood that a damaging event will occur,
    2. the costs of potential losses, and
    3. the costs of mitigating actions that could be taken.

Risk Identification

- It is the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives.
- It includes documenting and communicating the concern.
- The objective of risk identification is the early and continuous identification of events that, if they occur, will have negative impacts on the project's ability to achieve performance or capability outcome goals.
- They may come from within the project or from external sources.

Risk Identification

- There are multiple types of risk assessments, including program risk assessments, risk assessments to support an investment decision, analysis of alternatives, and assessments of operational or cost uncertainty.
- Risk identification needs to match the type of assessment required to support risk- informed decision making.

Risk Identification

- There are multiple sources of risk.
- For risk identification, the project team should review the program scope, cost estimates, schedule (to include evaluation of the critical path), technical maturity, key performance parameters, performance challenges, stakeholder expectations vs. current plan, external and internal dependencies, implementation challenges, integration, interoperability, supportability, supply-chain vulnerabilities, ability to handle threats, cost deviations, test event expectations, safety, security, and more.
- In addition, historical data from similar projects, stakeholder interviews, and risk lists provide valuable insight into areas for consideration of risk.

Risk Identification

- Risk identification is an iterative process.
- As the program progresses, more information will be gained about the program (e.g., specific design), and the risk statement will be adjusted to reflect the current understanding.
- New risks will be identified as the project progresses through the life cycle.

Risk Analysis

- Risk Analysis
  - Requires an entity to, conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected information held by the entity.
  - A tool for risk management, is a method of identifying vulnerabilities and threats, and assessing the possible damage to determine where to implement security safeguards.

Risk Analysis

- **Risk Analysis steps:**
  1. Identify the scope of the analysis.
  2. Gather data.
  3. Identify and document potential threats and vulnerabilities.
  4. Assess current security measures.
  5. Determine the likelihood of threat occurrence.
  6. Determine the potential impact of threat occurrence.
  7. Determine the level of risk.
  8. Identify security measures and finalize documentation.

Risk Analysis

- **A risk analysis has four main goals:**
  1. Identify assets and their values
  2. Identify vulnerabilities and threats
  3. Quantify the probability and business impact of these potential threats
  4. Provide an economic balance between the impact of the threat and the cost of the countermeasure

Risk Analysis

- **Risk Evaluation**
  - The risk evaluation process receives as input the output of risk analysis process.
  - It compares each risk level against the risk acceptance criteria and prioritize the risk list with risk treatment indications.

Module-4

Incident Management

Risk Treatment

- Risk treatment efforts should be undertaken to mitigate identified risks, using appropriate administrative, technical and physical controls.
- Control includes:
  - applying appropriate controls to avoid, eliminate or reduce risks;
  - transferring some risks to third parties as appropriate (e.g., by insurance);
  - knowingly and objectively accepting some risks; and
  - documenting the risk treatment choices made, and the reasons for them.

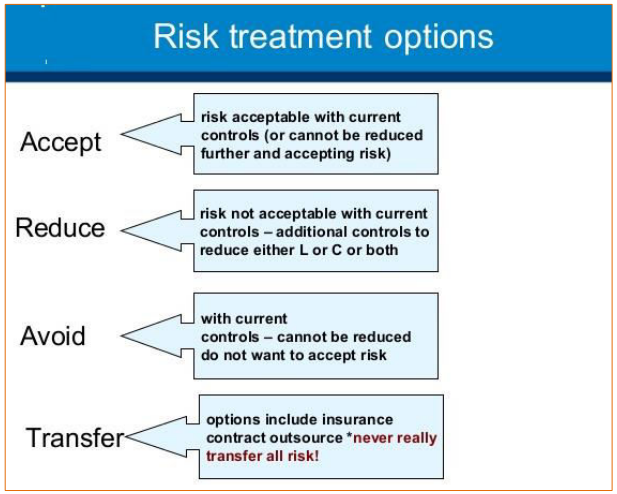
Risk Treatment

- Risk treatment procedure should consider:
  - legal-regulatory and private certificatory requirements;
  - organizational objectives, operational requirements and constraints; and
  - costs of implementation and operation relative to risks being reduced.

Risk Treatment

- Risk treatment strategies:
  1. Risk reduction
  2. Risk sharing/ transference
  3. Risk avoidance
  4. Risk acceptance

Risk Treatment



Risk Treatment

- Risk reduction
  - Taking the mitigation steps necessary to reduce the overall risk to an asset will include selecting countermeasures that will either reduce the likelihood of occurrence or reduce the severity of loss, or achieve both objectives at the same time.
  - For example, the risk of computer viruses can be mitigated by acquiring and implementing antivirus software. When evaluating the strength of a control, consideration should be given to whether the controls are preventative or detective.
  - The remaining level of risk after the controls/countermeasures have been applied is often referred to as “residual risk.”
  - An organization may choose to undergo a further cycle of risk treatment to address this.

Risk Treatment

- Risk sharing/transference
  - The organization shares its risk with third parties through insurance and/or service providers.
  - Insurance is a post-event compensatory mechanism used to reduce the burden of loss if the event were to occur.
  - Transference is the shifting of risk from one party to another.
  - For example, when hard-copy documents are moved offsite for storage at a secure-storage vendor location, the responsibility and costs associated with protecting the data transfers to the service provider.
  - The cost of storage may include compensation (insurance) if documents are damaged, lost, or stolen.

Risk Treatment

- Risk avoidance
  - The practice of eliminating the risk by withdrawing from or not becoming involved in the activity that allows the risk to be realized.
  - For example, an organization decides to discontinue a business process in order to avoid a situation that exposes the organization to risk.
- Risk acceptance
  - An organization decides to accept a particular risk because it falls within its risk-tolerance parameters and therefore agrees to accept the cost when it occurs.
  - Risk acceptance is a viable strategy where the cost of insuring against the risk would be greater over time than the total losses sustained.
  - All risks that are not avoided or transferred are accepted by default

Risk Management Feedback Loops

- Risk management is a comprehensive process that requires organizations to:
  1. frame risk
     - (i.e., establish the context for risk-based decisions);
  2. assess risk;
  3. respond to risk once determined;
  4. monitor the risk

Risk Management Feedback Loops

1. Risk Frame
   - Establishing a realistic and credible risk frame requires that organizations identify:
     - risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time);
     - risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration);

Risk Management Feedback Loops

1. Risk Frame
   - Establishing a realistic and credible risk frame requires that organizations identify:
     - risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and
     - priorities and trade-offs (e.g., the relative importance of missions/business functions, trade- offs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses).

Risk Management Feedback Loops

2. Risk Assessment
   - The purpose of the risk assessment component is to identify:
     - threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation;
     - vulnerabilities internal and external to organizations;
     - the harm (i.e., consequences/impact) to organizations that may occur given the potential for threats exploiting vulnerabilities; and
     - the likelihood that harm will occur. The end result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring).

Risk Management Feedback Loops

2. Risk Assessment
   - To support the risk assessment component, organizations identify:
     - the tools, techniques, and methodologies that are used to assess risk;
     - the assumptions related to risk assessments;
     - the constraints that may affect risk assessments;
     - roles and responsibilities;
     - how risk assessment information is collected, processed, and communicated throughout organizations;
     - how risk assessments are conducted within organizations;
     - the frequency of risk assessments; and
     - how threat information is obtained (i.e., sources and methods).

Risk Management Feedback Loops

3. Risk Response
   - The purpose of the risk response component is to provide a consistent, organization-wide, response to risk in accordance with the organizational risk frame by:
     - developing alternative courses of action for responding to risk;
     - evaluating the alternative courses of action;
     - determining appropriate courses of action consistent with organizational risk tolerance; and
     - implementing risk responses based on selected courses of action.

Risk Management Feedback Loops

4. Risk Monitoring
   - Purpose of the risk monitoring component:
     - To verify that planned risk response measures are implemented and information security requirements derived from/traceable to organizational mission/business functions, federal legislation, directives, regulations, policies, and standards, and guidelines, are satisfied;
     - To determine the ongoing effectiveness of risk response measures following implementation; and
     - To identify risk-impacting changes to organizational information systems and the environments in which the systems operate.

Risk Management Feedback Loops

4. Risk Monitoring
   - Analyzing monitoring results gives organizations the capability to maintain awareness of the risk being incurred, highlight the need to revisit other steps in the risk management process, and initiate process improvement activities as needed.

Risk Management Feedback Loops

4. Risk Monitoring
   - Organizations employ risk monitoring tools, techniques, and procedures to increase risk awareness, helping senior leaders/ executives develop a better understanding of the ongoing risk to organizational operations and assets, individuals, other organizations, and the Nation.
   - Organizations can implement risk monitoring at any of the risk management tiers with different objectives and utility of information produced.

Risk Management Feedback Loops

4. Risk Monitoring
   - For example, Tier 1 monitoring activities might include ongoing threat assessments and how changes in the threat space may affect Tier 2 and Tier 3 activities, including enterprise architectures (with embedded information security architectures) and organizational information systems.

Risk Management Feedback Loops

4. Risk Monitoring
   - Tier 2 monitoring activities might include, for example, analyses of new or current technologies either in use or considered for future use by organizations to identify exploitable weaknesses and/or deficiencies in those technologies that may affect mission/business success.

Risk Management Feedback Loops

4. Risk Monitoring
   - Tier 3 monitoring activities focus on information systems and might include, for example, automated monitoring of standard configuration settings for information technology products, vulnerability scanning, and ongoing assessments of security controls.

UNIT 6

Incident Response –Roles, and Responsibilities

MODULE-5

- Incident Response - Handling Different Types of Information Security Incidents - Preparation for Incident Response and Handling. Incident Response Team - Incident Response Team Dependencies - Incident Response Process

Incident Response

Incident Response Process

- Step 1: identification
- Step 2: incident recording
- Step 3: initial response
- Step 4: communicating the incident
- Step 5: containment
- Step 6: formulating a response strategy
- Step 7:incident classification
- Step 8: incident investigation
- Step 9: data collection
- Step 10: forensic analysis
- Step 11: evidence protection
- Step 12: notify external agencies
- Step 13: eradication
- Step 14: systems recovery
- Step 15: incident documentation
  - audio and video documentation strategies

Obtaining and validating information related to information security issues

- In incident handling, detection may be the most difficult task. Incident response teams in an organization are equipped to handle security incidents using well-defined response strategies beginning with information gathering.
- Preparing a list most common attack vectors such as **external/removable media, web, email, impersonation, improper use by authorized users etc.** can narrow down to the most competent incident handling procedure.
- Therefore, it is important to validate each incident using defined standard procedures and document each step taken accurately.

Common issues and incidents of information security that may require action and whom to report

- An indicator may not always translate into a security incident given the possibility of technical faults due to human error in cases such as server crash or modification of critical files.
- Determining whether a particular event is actually an incident is sometimes a matter of judgment.
- It may be necessary to collaborate with other technical and information security personnel to make a decision.
- Therefore, incident handlers need to report the matter to highly experienced and proficient staff members who can analyse the precursors and indicators effectively and take appropriate actions.

Issues…

Mentioned below are some of the means to conduct initial analysis for validation

- **Profiling networks and systems** in order to measure the characteristics of expected activity so that changes to it can be more easily identified and used one of the several detection and analysis techniques.
- **Studying networks, systems and applications** to understand what their normal behavior is so that abnormal behavior can be recognized more easily.
- **Creating and implementing a log retention** policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks.

Issues…

- **Correlating events using evidence of an incident** captured in several logs such wherein each may contain different types of data — a firewall log may have the source IP address that was used, whereas an application log may contain a username.
- **Synchronizing hosts clock using protocols** such as the network time protocol (NTP) to record time of attack.
- **Maintain and use a knowledge base of information** that handlers need for referencing quickly during incident analysis.
- **Use internet search engines for research** to help analysts find information on unusual activity.
- **Run packet sniffers to collect additional data** to record traffic that matches specified criteria should keep the volume of data manageable and minimize the inadvertent capture of other Information.
- **Filter the data to segregate** categories of indicators that tend to be insignificant.

Step 2: Incident recording

- Any occurrences of incident must be recorded and the incident response team should update the status of incidents along with other pertinent information.
- Observations and facts of the incident may be stored in any of the following sources such as logbook, laptops, audio recorders and digital cameras etc.

Incident record samples and template

- Documenting system events, conversations and observed changes in files can lead to a more efficient, more systematic and error-free handling of the problem.
- Using an application or a database, such as an issue tracking system helps ensure that incidents are handled and resolved in a timely manner.

Step 2: Incident recording

The following useful information are to be included in an incident record template:

- Current status of the incident as new, in progress, forwarded for investigation, resolved etc.
- Summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, if applicable
- Impact assessments related to the incident
- Contact information for other involved parties (system owners, system administrators etc.)
- List of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken (rebuild the host, upgrade an application etc.)

Step 3: Initial response

- Commence initial response to an incident based on the type of incident, the criticality of the resources and data that are affected, the severity of the incident, existing service level agreements (SLA) for affected resources, the time and day of the week, and other incidents that the team is handling.
- Generally, the highest priority is handling incidents that are likely to cause the most damage to the organization or to other organizations.

Step 4: Communicating the incident

- The incident should be communicated in appropriate procedures through the organization's points of contact (POC) for reporting incidents internally.
- Therefore, it is important for an organization to structure their incident response capability so that all incidents are reported directly to the incident response team, whereas others will use existing support.

Step 4: Communicating the incident

- **Assigning and escalating information on information security incidents**
- Organizations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time.
- This can happen for many reasons. For example, cell phones may fail or people may have personal emergencies.
- The escalation process should state how long a person should wait for a response and what to do if no response occurs.
- On failure to respond within a stipulated time, then the incident should be escalated again to a higher level of management. This process should be repeated until the incident is successfully handled.

Step 5: Containment

Containment and quarantine

- Containment is important before an incident overwhelms resources or increases damage.
- Most incidents require containment so that is an important consideration early in the course of handling each incident.
- Containment provides time for developing a tailored remediation strategy.
- An essential part of containment is decision-making where the situation may demand immediate action such as shut down a system, disconnect it from a network and disable certain functions.

Containment

Various containment strategies may be considered in the following ways:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (network connectivity, services provided to external parties etc.)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (partial containment, full containment etc.)
- Duration of the solution (emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution etc.)

Quarantine

- Handling an incident may necessitate the use of strategies to contain the existing predicament and one such method being redirecting the attacker to a sandbox (a form of containment) so that they can monitor the attacker's activity, usually to gather additional evidence.
- Hence, once a system has been compromised and if allowed with the compromise to continue, it may help the attacker to use the compromised system to attack other systems.

Understand network damage

- On the other hand, containment may give rise to another potential issue and that is some attacks may cause additional damage when they are contained.
- Hence the incident handler attempts to contain the incident by disconnecting the compromised host from the network, the subsequent pings will fail.
- As a result of the failure, the malicious process may overwrite or encrypt all the data on the host's hard drive.

Identify and isolate the trust model

- Network information systems are vulnerable to threats and benign nodes often compromised because of unknown, incomplete or distorted information while interacting with external sources.
- In this case, malicious nodes need to be identified and isolated from the environment. The solution to insecure can be found in the establishment of trust.
- Trust model can be formed based on the characteristics, information sources to compute, most relevant and reliable information source, experience of other members of community etc.

Step 6: Formulating a response strategy

- An analysis of the recoverability from an incident determines the possible responses that the team may take when handling the incident.
- An incident with a high functional impact and low effort to recover from is an ideal candidate for immediate action from the team.
- In situations involving high end data infiltration and exposure of sensitive information the incident response team may formulate response by transferring the case to strategic level team. Each response strategy should be formulated

Step 6: Formulating a response strategy

- Based on business impact caused by the incident and the estimated efforts required to recover from the incident.
- Incident response policies should include provisions concerning incident reporting at a minimum, what must be reported to whom and at what times.
- Important information to be included are CIO, head of information security, local information security officer, other incident response teams within the organization, external incident response teams (if appropriate), system owner, human resources (for cases involving employees, such as harassment through email), public affairs etc.

Step 7: Incident classification

Classifying and prioritizing information security incidents

- An incident may be broadly classified based on common attack vectors such as
  - External/ removable media;
  - Attrition;
  - Web;
  - Email;
  - Improper usage;
  - Loss or theft of equipment;
  - Miscellaneous.

Incident prioritization

- **Functional impact of the incident** on the existing functionality of the affected systems and future functional impact of the incident if it is not immediately contained.
- **Information impact of the incident** that may amount to information exfiltration and impact on organization's overall mission and impact of exfiltration of sensitive information on other organizations if any of the data pertain to a partner organization.
- **Recoverability from the incident** and how to determine the amount of time and resources that must be spent on recovering from that incident. Necessity to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.

Incident classification guidelines and templates

- Organizations should document their guidelines and templates to handle any incident but should focus on being prepared to handle incidents that use common attack vectors.
- Capturing the attack pattern formally with required information may help understand specific parts of an attack, how it is designed and executed, providing the adversary's perspective on the problem and the solution, and gives guidance on ways to mitigate the attack's effectiveness.

Incident classification guidelines and templates

- **Requirements** – identification of relevant security requirements, misuse and abuse cases.
- **Architecture and design** – provide context for architectural risk analysis and guidance for security architecture.
- **Implementation and development** – prioritize and guide review activities.
- **Testing and quality assurance** – provide context for appropriate risk-based and penetration testing.
- **System operation** – leverage lessons learned from security incidents into preventative guidance.
- **Policy and standard generation** – guide the identification of appropriate prescriptive organizational policies and standards

Incident prioritization guidelines and templates

- Creating written guidelines for prioritizing incidents serve as a good practice and help achieve effective information sharing within an organization.
- The step may also help in identifying situations that are of greater severity and demand immediate attention.
- An ideal template for incident prioritization should be formulated based on relevant factors such as the functional impact of the incident (e.g. Current and likely future negative impact to business functions), the information impact of the incident (e.g. Effect on the confidentiality, integrity and availability of the organization's information) and the recoverability from the incident (e.g. The time and types of resources that must be spent on recovering from the incident).

Step 8: Incident investigation

- One of the key tasks of an incident response team is to receive information on possible incidents, investigate them, and take action to ensure that the damage caused by the incidents is minimized.
- **Following up an incident investigation**
- In the course of the work, the team must adhere to the following procedures deemed
- Receive initial investigation and data gathering from IT help desk members and escalate to high strategic level specialist if situation demands.
- Use appropriate materials that may be needed during an investigation.

Step 8: Incident investigation

- Should become acquainted with various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them.
- Maintain record of chain of custody forms should detail the transfer and include each party's signature while transferring evidence from person to person.
- Should be careful to give out only appropriate information — the affected parties may request details about internal investigations that should not be revealed publicly.
- Ensure law enforcement are available to investigate incidents wherever necessary.
- Collect required list of evidence gathered during the incident investigation.
- Should collect evidence in accordance with procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court.

Step 8: Incident investigation

Lessons learnt from security incident

- Handling and rectifying security incident work best in a "learning and improving" model. Therefore, incident handling teams must evolve to reflect on new threats, improved technology and lessons learned. Each lesson's learned brief must include the following agenda:
- What exactly happened and during times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?

Step 8: Incident investigation

- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze and mitigate future incidents?

Process change for the future

- The changing nature of information technology and changes in personnel requires the incident response team to review all related documentation and procedures for handling incidents at designated intervals. A study of incident characteristics (data collected of previous incidents) may indicate systemic security weaknesses and threats as well as changes in incident trends.
- Incident data can also be collected to determine if a change to incident response capabilities causes a corresponding change in the team's performance (improvements in efficiency, reductions in costs etc).

Incident record keeping

- Incident record keeping or collecting data that are actionable, rather than collecting data simply because they are available will be useful in several capacities to the organization.
- It may help in deriving at the following information:
  - Systemic security weaknesses and threats, as well as changes in incident trends.
  - Selection and implementation of additional controls.
  - Measure the success of the incident response team.
  - Expected return on investment from the data.

Step 9: Data collection

Chain of Custody

- Evidences collected should be accounted for at all times whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature.
- A detailed log should be kept for all evidence, including the following:
  - Identifying information (e.g. The location, serial number, model number, hostname, media access control (MAC) addresses and IP addresses of a computer).
  - Name, title, and phone number of each individual who collected or handled the evidence during the investigation.
  - Time and date (including time zone) of each occurrence of evidence handling.
  - Locations where the evidence was stored.

Step 10: Forensic analysis

- Incident handling requires some team members to be specialized in particular technical areas, such as network intrusion detection, malware analysis or forensics. Many incidents cause a dynamic chain of events to occur, an initial system snapshot may do more good in identifying the problem and its source than most other actions that can be taken at this stage.
- Therefore, it is appropriate to obtain snapshots through full forensic disk images, not file system backups. Disk images should be made to sanitized write-protectable or write-once media.
- This process is superior to a file system backup for investigatory and evidentiary purposes. Imaging is also valuable in that it is much safer to analyze an image than it is to perform analysis on the original system because the analysis may inadvertently alter the original.
- Some of the useful resources in forensic aspects of incident analysis may include digital forensic workstations and/ or backup devices to create disk images, preserve log files, and save other relevant incident data

Step 11: Evidence protection

Importance of keeping evidence relating to information security incidents

- Collecting evidence from computing resources presents some challenges.
- It is generally desirable to acquire evidence from a system of interest as soon as one suspects that an incident may have occurred.
- Users and system administrators should be made aware of the steps that they should take to preserve evidence.
- In addition, evidence should be accounted for at all times whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature and a registry or log be maintained location of the stored evidence.

Step 12: Notify external agencies

- An organization's incident response team should plan its incident coordination with those parties before incidents occur to ensure that all parties know their roles and that effective line of communication are established.
- Some of the organizations' external agencies may include other or external incident response teams, law enforcement agencies, internet service providers and constituents, law enforcements/ legal departments and customers or system owner etc.

Step 13: Eradication

- Eliminating components of the incident such as deleting malware and disabling breached user accounts as well as identifying and mitigating all vulnerabilities that were exploited follow next to successful containment and quarantine.
- During the process, it is important to identify all affected hosts within the organization so that they can be remediated.
- In some cases, eradication is either not necessary or is performed during recovery.

Step 13: Eradication

Identify data backup holes

- Verify data back-up and restore procedures. Incident response should be aware of the location of back-up date storage, maintenance, user access and security procedures for data restoration and system recovery.
- Following are the suggested data back-up sources:
  - Spare workstations, servers, networking equipment or virtualized equivalents, which may be used for many purposes, such as restoring back-ups and trying out malware.
  - Other important materials include back-up devices, blank media, basic networking equipment and cables.

Step 13: Eradication

Operating system updates and patch management

- All hosts patched appropriately using standard configurations be configured to follow the principle of least privilege — granting users only the privileges necessary for performing their authorized tasks.
- Hosts should have auditing enabled and should log significant security-related events, security of hosts and their configurations should be continuously monitored.
- In some organizations, the use of security content automation protocol (SCAP) expressed operating system and application configuration checklists to assist in securing hosts consistently and effectively.

Step 13: Eradication

Infrastructure and security policy improvement

- Security cannot be achieved by merely implementing various security systems, tools or products. However, security failures are less likely through the implementation of security policy, process, procedure and product(s).
- Multiple layers of defense need to be applied to design a fail-safe security system.
- The organization should also report all changes and updates made to its IT infrastructure, network configuration and systems.
- Organization should also focus on longer-term changes (e.g. Infrastructure changes) and ongoing work to keep the enterprise as secure as possible.

Step 14: Systems recovery

- In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.
- Recovery may involve such actions as restoring systems from clean back-ups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords and tightening network perimeter security (e.g. Firewall rulesets, boundary router access control lists etc.).
- Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again or other resources within the organization are attacked in a similar manner.

Step 15: Incident documentation

- A logbook is an effective and simple medium for recording all facts regarding incidents. Documenting system events, conversations and observed changes in files can lead to a more efficient, more systematic and less error prone handling of the problem.
- Every step taken from the time the incident was detected to its final resolution should be documented and time-stamped.
- Every document regarding the incident should be dated and signed by the incident handler as such information can also be used as evidence in a court of law if legal prosecution is pursued.

Importance of keeping records and evidence relating to information security incidents

- The incident response team should maintain records about the status of incidents along with other pertinent information.
- Using an application or a database, such as an issue tracking system, helps ensure that incidents are handled and resolved in a timely manner.

Audio and video documentation strategies

- Recording details of evidence gathering accessories including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms etc. is one of the common strategies used to track incidents and security.
- In addition, laptops, audio recorders, and digital cameras can also serve the purpose beside system events, conversations, and observed changes in files can lead to a more efficient, more systematic and less error prone handling of the problem.

Update the status of information security incidents

- Incident handling team may need to provide status updates to certain parties even in some cases the entire organization.
- The team should plan and prepare several communication methods, including out-of-band methods (in person or on paper), and select the methods that are appropriate for a particular incident.

Possible communication methods include:

- Email
- Website (internal, external or portal)
- Telephone calls
- In person (daily briefings)
- Voice mailbox greeting (set up a separate voice mailbox for incident updates and update the greeting message to reflect the current incident status and use the help desk's voice mail greeting)
- Paper (post notices on bulletin boards and doors, hand out notices at all entrance points etc.)

Incident status template

- An incident status should carry statement of the current status of the incident so that communications with the media are consistent and up-to-date.
- Template may include the following details:
- Current status of the incident Summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, if applicable
- Impact assessments related to the incident
- Contact information for other involved parties (e.g. System owners, system administrators)
- List of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken (e.g. Rebuild the host, upgrade an application)

Preparing reports on information security incidents

- This estimate may become the basis for subsequent prosecution activity by law enforcement entities.
- Follow-up reports should be kept for a period of time as specified in record retention policies
- Another important post-incident activity is creating a follow-up report for each incident, which can be quite valuable for future use.
- The report provides a reference that can be used to assist in handling similar incidents.

INCIDENT REPORT TEMPLATES

- Creating a formal chronology of events in the incident report template for criteria including time- stamped information such as log data from systems (important for legal reasons) and monetary estimate of the amount of damage the incident caused.

Additionally, the following information may also be a part of the report:

- Number of incidents handled
- Time per incident
- Objective assessment of each incident
- Subjective assessment of each incident

- Organizations should specify which incidents must be reported, when they must be reported and to whom.
- The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the organization and system owners.

Step 16: Incident damage and cost assessment

- After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents.
- The incident data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the incident response team.
- Cost of storing evidence and the cost of retaining functional computers that can use the stored hardware and media can be substantial.
- Cost is a major factor, especially if employees are required to be onsite 24/7.
- Organizations may fail to include incident response-specific costs in budgets, such as sufficient funding for training and maintaining skills.

SUBMITTING INFORMATION SECURITY REPORTS

- Security follow-up reports are usually kept for a period of time as specified in record retention policies.
- Most organizations have data retention policies that state how long certain types of data may be kept.
- For example, an organization may state that email messages should be retained for only 180 days.
- If a disk image contains thousands of emails, the organization may not want the image to be kept for more than 180 days unless it is absolutely necessary.

Step 17: Review and update the response policies

- The organization must review and update response policies, related activities, gather information from the handlers, provide incident updates to other groups, and ensure that the team's needs are met.
- The gambit of the work may also include periodically reviewing and updating threat update information through briefings, web postings, and mailing lists published by authorized agencies or public bodies

Step 18: Training and awareness

Organizations must create, provision, and operate a formal incident response capability.

Security awareness and training checklist

- Establishing an incident response training and awareness should include the following actions:
- Creating an incident response training and awareness policy and plan.
- Developing procedures for performing incident handling and reporting.
- Setting guidelines for communicating with outside parties regarding incidents.
- Training it staff on complying with the organization's security standards and making users aware of policies and procedures regarding appropriate use of networks, systems and applications.

Step 18: Training and awareness

- Training should be provided for sop (delineation of the specific technical processes, techniques, checklists and forms) users.
- Staffing and training the incident response team.
- Providing a solid training program for new employees.
- Training to maintain networks, systems and applications in accordance with the organization's
- Security standards.
- Creating awareness of policies and procedures regarding appropriate use of networks, systems, and applications.

Incident response knowledge base

- The knowledge base is the consolidated incident data collected onto common incident database. Organizations can create their own knowledge base or refer to those established by several groups and organizations.
- Although it is possible to build a knowledge base with a complex structure, a simple approach can be effective.
- Text documents, spreadsheets and relatively simple databases provide effective, flexible and searchable mechanisms for sharing data among team members.
- The knowledge base should also contain a variety of information, including explanations of the significance and validity of precursors and indicators, such as IDPS alerts, operating system log entries and application error codes.

Incident response knowledge base

Accessing and updating knowledge base

- An incident handler may access knowledge databases information quickly during incident analysis, a centralized knowledge base provides a consistent and maintainable source of information.
- The knowledge base should include general information such as data on precursors and indicators of previous incidents.

Importance of tracking progress

- Several groups collect and consolidate incident data from various organizations into incident databases.
- This information sharing may take place in many forms such as trackers and real-time blacklists.
- The organization can also check its own knowledge base or issue tracking system for related activity.

Incident response knowledge base

Corrective and preventative actions for information security incidents

- In the absence of security controls higher volumes of incidents may occur overwhelming the incident response team.
- An incident response team may be able to identify problems that the organization is otherwise not aware of.
- The team can play a key role in risk assessment and training by identifying gaps.

Incident response knowledge base

The following text, however, provides a brief overview of some of the main recommended practices for securing networks, systems and applications:

- Periodic risk assessments of systems and applications to determine what risks posed by combinations of threats and vulnerabilities.
- Hardened hosts appropriately using standard configurations while keeping each host properly patched, hosts should be configured to follow the principle of least privilege — granting users only the privileges necessary for performing their authorized tasks.
- The network perimeter should be configured to deny all activity that is not expressly permitted.
- Software to detect and stop malware should be deployed throughout the organization.
- Users should be made aware of policies and procedures regarding appropriate use of networks, systems and applications

Preparation for Incident Response and Handling

Incident Handling Preparation

- Preparation is the first step to handling an incident response and it accounts for establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks and applications are sufficiently secure.
- Incident handling procedures include the following requirements:
- Contact information for team members and others within and outside the organization (primary and back-up contacts) such as law enforcement and other incident response teams etc.
- On-call information for other teams within the organization including escalation information.

Incident Handling Preparation

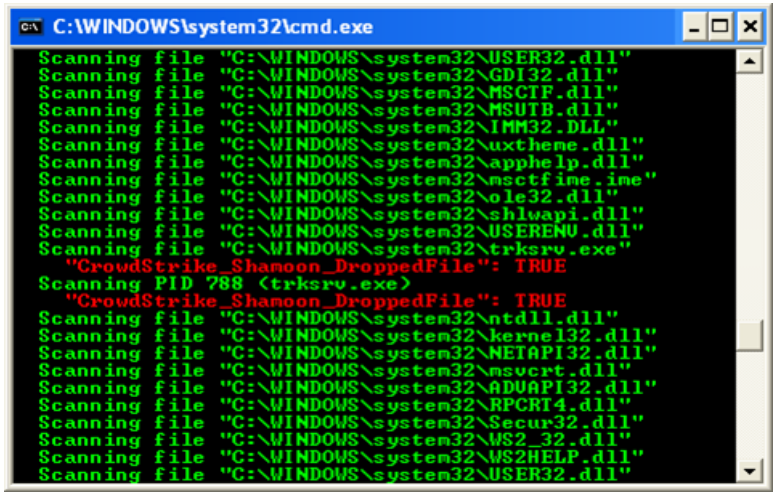
- Incident reporting mechanisms, such as phone numbers; email addresses; online forms; and secure instant messaging systems that users can use to report suspected incidents.
- Issue tracking system for tracking incident information, status etc.
- Encryption software to be used for communication among team members, within the organization and with external parties and federal agencies, software must use a flips-validated encryption algorithm.
- Digital forensic workstations and/ or backup devices to create disk images, preserve log files, and save other relevant incident data.
- Laptops for activities such as analyzing data, sniffing packets and writing reports.

- Portable printer to print copies of log files and other evidence from non-networked systems.
- Packet sniffers and protocol analyzers to capture and analyze network traffic.
- Port lists, including commonly used ports and Trojan horse ports.
- Documentation for oss, applications, protocols, and intrusion detection and antivirus products.
- Network diagrams and lists of critical assets, such as database servers.
- Current baselines of expected network, system and application activity.
- Cryptographic hashes of critical files to speed incident analysis, verification and eradication.
- Access to images of clean of and application installations for restoration and recovery purposes.

For malicious code incidents, the following preparation steps can be taken:

- **Step 1. Make users aware of malicious code issues –** this information should include a basic review of the methods that malicious code uses to propagate and the symptoms of infections. Holding regular user education sessions helps to ensure that users are aware of the risks that malicious code poses.
- **Step 2. Read antivirus vendor bulletins –** sign up for mailing lists from antivirus vendors that provide timely information on new malicious code threats.
- **Step 3. Deploy host-based intrusion detection systems to critical hosts –** host-based IDS software can detect signs of malicious code incidents such as configuration changes and system executable modifications. File integrity checkers are useful in identifying the affected components of a system.

- Some organizations configure their network perimeters to block connections to specific common Trojan horse ports, with the goal of preventing Trojan horse client and server component communications.
- However, this approach is generally ineffective. Known Trojan horses use hundreds of different port numbers, and many Trojan horses can be configured to use any port number.
- Also, some Trojan horses use the same port numbers that legitimate services use so their communication cannot be blocked by port number. Some organizations also implement port blocking incorrectly so legitimate connections are sometimes blocked.
- Implementing filtering rules for each Trojan horse port will also increase the demands placed on the filtering device. Generally, a Trojan horse port should be blocked only if the organization has a serious Trojan horse infestation.



Incident Prevention

- Incident prevention objectively works on minimizing larger negative business (e.g. More extensive damage, longer periods of service and data unavailability etc.) Impact and reduced number of incidents.
- Although incident response teams are generally not responsible for securing resources, they can be advocates of sound security practices.
- They can play a key role of identify problems that the organization is otherwise not aware of, the team can play a key role in risk assessment and training by identifying gaps.

- Some of the recommended practices for securing networks, systems and applications include:
- Periodic risk assessments of systems and applications.
- Hardening of hosts appropriately using standard configurations.
- Configuring network perimeters such as securing all connection points, such as virtual private networks (vpns) and dedicated connections to other organizations.
- Deploying malware protection at the host level (server and workstation operating systems), the
- Application server level (email server, web proxies etc.) And the application client level (email clients, instant messaging clients etc.)
- Applying the learning from previous incidents, and sharing with users so they can see how their actions could affect the organization.

- For preventing malicious code incidents, the following steps can be taken:
- **Step 1. Use antivirus software:** antivirus software is a necessity to combat the threat of malicious code and limit damage.
  - The software should be running on all hosts throughout the organization, and all copies should be kept current with the latest virus signatures so that the newest threats can be thwarted.
  - Antivirus software should also be used for applications used to transfer malicious code, such as e-mail, file transfer and instant messaging software.
  - The software should be configured to perform periodic scans of the system as well as real-time scans of each file as it is downloaded, opened or executed.
  - The antivirus software should also be configured to disinfect and quarantine infected files.
  - Some antivirus products not only look for viruses, worms and Trojan horses, but they also examine HTML, ActiveX, JavaScript and other types of mobile code for malicious content.

Step 2. Block suspicious files: configure email servers and clients to block attachments with file extensions that are associated with malicious code (e.g. .Pif, .Vbs) and suspicious file extension combinations (e.g. .Txt.Vbs, .Htm.Exe).

Step 3. Limit the use of nonessential programs with file transfer capabilities: examples include peer- to-peer file and music sharing programs, instant messaging software and IRC clients and servers. These programs are frequently used to spread malicious code among users.

Step 4. Educate users on the safe handling of email attachments: antivirus software should be configured to scan each attachment before opening it. Users should not open suspicious attachments or attachments from unknown sources. Users should also not assume that if the sender is known, the attachment is not infected. Senders may not know that their systems are infected with malicious code that can extract email addresses from files and send copies of the malicious code to those addresses. This activity creates the impression that the emails are coming from a trusted person even though the person is not aware that they have been sent. Users can also be educated on file types that they should never open (e.g. .Bat, .Com, .Exe, .Pif, .Vbs). Although user awareness of good practices should lessen the number and severity of malicious code incidents, organizations should assume that users will make mistakes and infect systems

Step 5. Eliminate open windows shares: many worms spread through unsecured shares on hosts running windows. If one host in the organization is infected with a worm, it could rapidly spread to hundreds or thousands of other hosts within the organization through their unsecured shares. Organizations should routinely check all hosts for open shares and direct the system owners to secure the shares properly. Also, the network perimeter should be configured to prevent traffic that uses NetBIOS ports from entering or leaving the organization's networks. This should not only prevent external hosts from directly infecting internal hosts through open shares but should also prevent internal worm infections from spreading to other organizations through open shares.

Step 6. Use web browser security to limit mobile code: all web browsers should have their security settings configured so as to prevent unsigned ActiveX and other mobile code vehicles from unknowingly being downloaded to and executed on local systems. Organizations should consider establishing an internet security policy that specifies which types of mobile code may be used from various sources (e.g. Internal servers, external servers).

Step 7. Configure email clients to act more securely: email clients throughout the organization should be configured to avoid actions that may inadvertently permit infections to occur. For example, email clients should not automatically execute attachments.

Detection of Malicious Code

- Detection of malicious code involves the preparation to handle incidents that use common attack vectors. Some of the key aspects useful in determining malicious code detection:
- Screening attack vectors such as removable media or other peripheral device.
- Keeping a tab on network flow information through routers and other networking devices that can be used to find anomalous network activity caused by malware, data exfiltration and other malicious acts.

- Monitoring alerts sent by most idps products that uses attack signatures to identify malicious activity. The signatures must be kept up to date so that the newest attacks can be detected.
- Observing antivirus software alerts for detecting various forms of malware, generates alerts and prevents the malware from infecting hosts.
- Maintaining and using a rich knowledge base replete with explanations of the significance and validity of precursors and indicators, such as idps alerts, operating system log entries and application error codes.

- Following appropriate containment procedures which require disconnection of host from the network, and cause further damage. Because malicious code incidents can take many forms, they may be detected via a number of precursors and indications. Some precursors and possible responses are listed below:
- **Precursor:** an alert warns of new malicious code that targets software that the organization uses.
- **Response:** research the new virus to determine whether it is real or a hoax. This can be done through antivirus vendor websites and virus hoax sites. If the malicious code is confirmed as authentic, ensure that antivirus software is updated with virus signatures for the new malicious code. If a virus signature is not yet available, and the threat is serious and imminent, the activity might be blocked through other means, such as configuring email servers or clients to block emails matching characteristics of the new malicious code. The team might also want to notify antivirus vendors of the new virus.

Precursor: antivirus software detects and successfully disinfects or quarantines a newly received infected file.

Response: determine how the malicious code entered the system and what vulnerability or weakness it was attempting to exploit. If the malicious code might pose a significant risk to other users and hosts, mitigate the weaknesses that the malicious code used to reach the system and would have used to infect the target host.

For example:

Similarly, there are certain indications that can highlight the onset of a malicious action.

For example:

Malicious action: a virus that spreads through email infects a host.

Indicators:

- ❖ Antivirus software alerts of infected files
- ❖ Sudden increase in the number of emails being sent and received
- ❖ Changes to templates for word processing documents, spreadsheets etc.
- ❖ Deleted, corrupted or inaccessible files
- ❖ Unusual items on the screen such as odd messages and graphics
- ❖ Programs start slowly, run slowly or do not run at all
- ❖ System instability and crashes

Malicious action: a worm that spreads through a vulnerable service infects a host.

Indicators:

- ❖ Antivirus software alerts of infected files
- ❖ Port scans and failed connection attempts targeted at the vulnerable service (e.G. Open windows shares, HTTP)
- ❖ Increased network usage
- ❖ Programs start slowly, run slowly or do not run at all
- ❖ System instability and crashes

Malicious action: malicious mobile code on a web site is used to infect a host with a virus, worm or Trojan horse.

- ❖ Indications listed above for the pertinent type of malicious code
- ❖ Unexpected dialog boxes, requesting permission to do something
- ❖ Unusual graphics such as overlapping or overlaid message boxes

Malicious action: a Trojan horse is installed and running on a host.

Indicators:

- ❖ Antivirus software alerts of Trojan horse versions of files
- ❖ Network intrusion detection alerts of Trojan horse client-server communication
- ❖ Firewall and router log entries for Trojan horse client-server communication
- ❖ Network connections between the host and unknown remote systems
- ❖ Unusual and unexpected ports open
- ❖ Unknown processes running
- ❖ High amounts of network traffic generated by the host, particularly if directed at external host(s)
- ❖ Programs start slowly, run slowly or do not run at all
- ❖ System instability and crashes

Containment Strategy

Containment strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based ddos attack. Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision making. Criteria for determining the appropriate strategy include:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g. Network connectivity or services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g. Partial containment or full containment)
- Duration of the solution (e.g. Emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks or permanent solution)

SENDING UNKNOWN MALICIOUS CODE TO ANTIVIRUS VENDORS:

- malicious code that cannot be definitively identified by antivirus software may occasionally enter the environment.
- Eradicating the malicious code from systems and preventing additional infections may be difficult or impossible without having updated antivirus signatures from the vendor.
- Incident handlers should be familiar with the procedures for submitting copies of unknown malicious code to the organization's antivirus vendors.

Containment Strategy

Identifying and isolating other infected hosts: antivirus alert messages are a good source of information, but not every infection will be detected by antivirus software.

- Incident handlers may need to search for indications of infection through other means such as:
  - Performing port scans to detect hosts listening on a known Trojan horse or backdoor port.
  - Using antivirus scanning and clean-up tools released to combat a specific instance of malicious Code.
  - Reviewing logs from email servers, firewalls and other systems that the malicious code may have passed through as well as individual host logs.
  - Configuring network and host intrusion detection software to identify activity associated with
  - Infections.
  - Auditing the processes running on systems to confirm that they are all legitimate.

Configuring email servers and clients to block emails:

- many email programs can be configured manually to block emails by particular subjects, attachment names or other criteria that correspond to the malicious code.
- This is neither a foolproof nor an efficient solution, but it may be the best option available if an imminent threat exists and antivirus signatures are not yet available.

Blocking outbound access:

- if the malicious code attempts to generate outbound emails or connections, handlers should consider blocking access to ip addresses or services to which the infected system may be attempting to connect.

Shutting down email servers:

- during the most severe malicious code incidents with hundreds or thousands of internal hosts infected, email servers may become completely overwhelmed by viruses trying to spread via email.
- It may be necessary to shut down an email server to halt the spread of email-borne viruses.

Isolating networks from the internet:

- networks may become overwhelmed with worm traffic when a severe worm infestation occurs. Occasionally a worm will generate so much traffic throughout the internet that network perimeters are completely overwhelmed.
- It may be better to disconnect the organization from the internet, particularly if the organization's internet access is essentially useless as a result of the volume of worm traffic.
- This protects the organization's systems from being attacked by external worms should the organization's systems already be infected. This prevents them from attacking other systems and adding to the traffic congestion.

Evidence Gathering and Handling

- The primary reason for gathering evidence during an incident is to resolve the incident however it may also be needed for legal proceedings. In the case of incident analysis, the procedure is implemented through the application of hardware and software and related accessories such as hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags and evidence tape and to preserve evidence for possible legal actions.
- With respect to legal proceedings, it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court. Thus, users and system administrators should be made aware of the steps that they should take to preserve evidence.

Eradication and Recovery

- After an incident has occurred, it is important to identify all affected hosts within the organization so that they can be remediated.
- For some incidents, eradication is either not necessary or is performed during recovery.
- In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally and (if applicable) remediate vulnerabilities to prevent similar incidents.

Eradication and Recovery

Eradication procedures may be performed in the following ways:

- ❖ Identify and mitigate all vulnerabilities that were exploited.
- ❖ Remove malware, inappropriate materials and other components.
- ❖ Repeat the detection and analysis steps to identify all other affected hosts, if more affected hosts are discovered (e.g. New malware infections.
- ❖ Contain and eradicate the incident in accordance with appropriate procedures.

Eradication and Recovery

- ➢ Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords and tightening network perimeter security (e.g. Firewall rulesets, boundary router access control lists).
- ➢ Some of the recommended practices in recovery procedures are:
  - ❖ Return affected systems to an operationally ready state
  - ❖ Confirm that the affected systems are functioning normally
  - ❖ Implement additional monitoring to look for future related activity, if necessary
- ➢ Eradication and recovery should be done in a phased approach so that remediation steps are prioritized.

Antivirus systems

- ➢ Antivirus software effectively identifies and removes malicious code infections however, some infected files cannot be disinfected. (Files can be deleted and replaced with clean backup copies.
- ➢ In case of an application, the affected application can be reinstalled.) If the malicious code provided attackers with root-level access, it may not be possible to determine what other actions the attackers may have performed.
- ➢ In such cases, the system should either be restored from a previous, uninfected backup or be rebuilt from scratch. Of course, the system should then be secured so that it will not be susceptible to another infection from the same malicious code.

Eradication and Recovery

- ➢ Antivirus software sends alerts when it detects that a host is infected with malware.
- ➢ It detects various forms of malware, generates alerts and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date.
- ➢ Anti-spam software is used to detect spam and prevent it from reaching users' mailboxes.
- ➢ Spam may contain malware, phishing attacks and other malicious content, so alerts from anti-spam software may indicate attack attempts.

CASE STUDY ON INCIDENT HANDLING PROCESS

The Challenge

- A large, multinational organization was alerted by US-CERT/FBI that it had been the source of a number of credit cards and details being leaked/sold on underground (carding) forums.
- After an initial investigation, the organization's security team discovered a compromised credit-card processing server but, having insufficient resources and skills in dealing with the incident, called in OSEC.

The Solution

- OSEC sent a team of analysts, including incident response, crisis management, and digital forensics personnel to the organization's head office and data centres to deal with the incident.
- Once there, the team initiated full incident response based on the information supplied by the organization itself as well as law enforcement/authorities.

Planning - After The Fact

- The first task was understanding what measures were in place to deal with the incident. Unfortunately, while the organization had an incident response plan, it had not undertaken the first step of incident response - preparation.
- Osec's incident response manager, along with the team, got to work coming up with a strategy: analysing the available information, using it to understand the extent of the compromise, and the incident, and working out how to contain and eradicate it.
- All the while, information to the rest of the organization and the world at large had to be controlled, due to the possible legal and regulatory implications.
- Now that you know the security challenge that had been faced by us-cert/fbi, you may now read the detection and eradication process that was adopted to handle the incident in a controlled manner:

Detection and Analysis

- Containment required understanding what data had been exfiltrated, and working back from there to the compromised resources, as well as examining the rest of the environment for other footholds that the attackers had.
- Quickly gaining an understanding of the network and segmentation, as well as rapidly implementing network behavioural analysis and performing content inspection between the payment processing infrastructure and external networks, OSEC detected connections back to command and control servers that were known to be operated by organized criminal elements ('carders').
- From there, we started performing analysis of the compromised systems using forensics techniques to determine how and what vulnerabilities had been exploited to gain access, correlating that with available logging information, all the while monitoring network flows to both ensure that no additional card information was being exfiltrated for the purposes of understanding what machines were under their control, all without alerting the bad guys.

- Within a short amount of time, OSEC determined that a third-party web application/site that was vulnerable to SQL injection had been initially compromised, and then used as a "base of operations" to penetrate further into the network, ultimately gaining access to the payment processing segments.
- By targeting administrators using social engineering attacks in combination with an internet explorer vulnerability, they had then stolen credentials that could be used to authenticate to payment processing servers, and utilized privilege escalation vulnerabilities on the servers themselves to harvest credit card numbers as they were being processed.
- In addition, they had installed customized malware that communicated with the command and control servers and exfiltrated data through encrypted tunnels, in bursts, to evade detection.

Containment and Eradication

- OSEC then went about stopping the spread of the malware and compromise, and expelling the attackers from the network. Once we had determined that the malware installed would not respond negatively to loss of connectivity to command and control servers, we quickly: ensured the initial point of compromise (SQL injection) was corrected scanned for similar common vulnerabilities in externally- visible systems, and ensured any identified issues were corrected reset all relevant authentication credentials blocked the attackers at the network perimeter.
- We then set about isolating and cleaning each of the compromised hosts as quickly as we could, in coordination with IT personnel, to ensure that the processing systems were impacted as little as possible.

- In most cases, we were able to wipe hosts and perform recovery to ensure all traces of malware were eradicated, but a number of systems required manual cleaning, which we undertook with the relevant organizational resources, and initiated extensive monitoring to ensure no undetected issues remained.
- Finally, once the full extent of the breach was understood - particularly what and how much data had been stolen, osec coordinated with pr and legal personnel to manage client and other regulatory- body notifications.

Post-Incident Activity

- Once the immediate incident had been dealt with, OSEC performed a post-mortem analysis of the incident, the organization's response, and compared it to osec's internally-developed IR processes, procedures, and frameworks to identify what needed to be done to ensure IR, vulnerability management, as well as overall information security management process and procedures were improved such that future incidents would be minimized we then sat down with the various stakeholders in the organization that had been involved and discussed the incident and response, explaining the relevant issues, identifying organizational problems that also needed to be corrected, as well as future strategies for avoiding incidents and dealing with them when they occurred, communicating our recommended incident response strategy and implementation to the organization's senior levels.

- Having reviewed osec's recommendations, the organization then asked us back to assist with implementing them.
- Over a 3 months' period, OSEC led a number of efforts, including implementing protection mechanisms at the host, application, and network layers; establishing a functioning vulnerability management within the overall information security management program, verifying processes, helping with staffing and training, and performing incident response drills to test the final product.

The Result

- Twelve months after implementing the recommendations, and achieving a practical incident response program, the organization has not suffered any subsequent breaches.
- In addition, it has gained the assurance, through incident response drills, that should a breach occur, response will be swift and effective.

Module-4

Incident Response –Roles, and Responsibilities

Incident Response –Roles, and Responsibilities

- Incident Response
- Handling Different Types of Information Security Incidents
- Preparation for Incident Response and Handling
- Incident Response Team
- Incident Response Team Dependencies
- Incident Response Process

https://www.cynet.com/incident-response/incident-response-plan

Incident Response

- Incident response (IR) is a structured methodology for handling security incidents, breaches, and cyber threats.
- A well-defined incident response plan allows you to effectively identify, minimize the damage, and reduce the cost of a cyber attack, while finding and fixing the cause to prevent future attacks.

Incident Response

- During a cyber security incident, security teams will face many unknowns and a frenzy of activity.
- In such a hectic environment, they may fail to follow proper incident response procedures to effectively limit the damage.
- This is important because a security incident can be a high-pressure situation, and your IR team must immediately focus on the critical tasks at hand.
- Clear thinking and swiftly taking pre-planned incident response steps during a security incident can prevent many unnecessary business impacts and reputational damage.

Incident Response

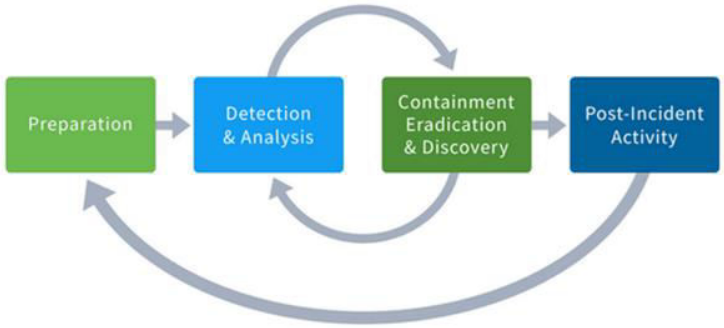
- Incident Response Team
  - A **Cyber** Security **Incident Response Team** (CSIRT) is a **group** of experts that assesses, documents and responds to a **cyber incident** so that a network can not only recover quickly, but also avoid future **incidents**.

Incident Response

- Incident Response Team Dependencies
  - **Employees**
    - the organization conducts all incident response-related activities by itself, without any guidance or intervention from external parties.
  - **Partially Outsourced**
    - the organization outsources certain elements of its incident response-related activities to external parties.
  - **Fully outsourced**
    - the organization outsources all elements of its incident response-related activities to external parties.

Incident Response

- Incident response phases



Incident Response

- The incident response phases are:
  1. Preparation
  2. Identification
  3. Containment
  4. Eradication
  5. Recovery
  6. Lessons Learned

Incident Response

1. Preparation

- This phase will be the work horse of your incident response planning, and in the end, the most crucial phase to protect your business.
- Part of this phase includes:
  - Ensure your employees are properly trained regarding their incident response roles and responsibilities in the event of data breach
  - Develop incident response drill scenarios and regularly conduct mock data breaches to evaluate your incident response plan.
- Ensure that all aspects of your incident response plan (training, execution, hardware and software resources, etc.) are approved and funded in advance

Incident Response

1. Preparation

- **Questions to address**
  - Has everyone been trained on security policies?
  - Have your security policies and incident response plan been approved by appropriate management?
  - Does the Incident Response Team know their roles and the required notifications to make?
  - Have all Incident Response Team members participated in mock drills?

Incident Response

2. Identification

- This is the process where you determine whether you've been breached. A breach, or incident, could originate from many different areas.
- **Questions to address**
  - When did the event happen?
  - How was it discovered?
  - Who discovered it?
  - Have any other areas been impacted?
  - What is the scope of the compromise?
  - Does it affect operations?
  - Has the source (point of entry) of the event been discovered?

Incident Response

3. Containment

- When a breach is first discovered, your initial instinct may be to securely delete everything so you can just get rid of it.
- However, that will likely hurt you in the long run since you'll be destroying valuable evidence that you need to determine where the breach started and devise a plan to prevent it from happening again..
- Instead, contain the breach so it doesn't spread and cause further damage to your business.
- If you can, disconnect affected devices from the Internet. Have short-term and long-term containment strategies ready.
- It's also good to have a redundant system back-up to help restore business operations.
- That way, any compromised data isn't lost forever.

Incident Response

3. Containment

- **Questions to address**
  - What's been done to contain the breach short term?
  - What's been done to contain the breach long term?
  - Has any discovered malware been quarantined from the rest of the environment?
  - What sort of backups are in place?
  - Does your remote access require true multi-factor authentication?
  - Have all access credentials been reviewed for legitimacy, hardened and changed?
  - Have you applied all recent security patches and updates?

Incident Response

4. Eradication

- Once you've contained the issue, you need to find and eliminate the root cause of the breach.
- This means all malware should be securely removed, systems should again be hardened and patched, and updates should be applied.
- Whether you do this yourself, or hire a third party to do it, you need to be thorough.
- If any trace of malware or security issues remain in your systems, you may still be losing valuable data, and your liability could increase.

Incident Response

4. Eradication

- **Questions to address**
  - Have artifacts/malware from the attacker been securely removed?
  - Has the system be hardened, patched, and updates applied?
  - Can the system be re-imaged?

Incident Response

5. Recovery

- This is the process of restoring and returning affected systems and devices back into your business environment.
- During this time, it's important to get your systems and business operations up and running again without the fear of another breach.

Incident Response

5. Recovery

- **Questions to address**
  - When can systems be returned to production?
  - Have systems been patched, hardened and tested?
  - Can the system be restored from a trusted back-up?
  - How long will the affected systems be monitored and what will you look for when monitoring?
  - What tools will ensure similar attacks will not reoccur? (File integrity monitoring, intrusion detection/protection, etc)

Incident Response

6. Lessons Learned

- Once the investigation is complete, hold an after-action meeting with all Incident Response Team members and discuss what you've learned from the data breach.
- This is where you will analyze and document everything about the breach.
- Determine what worked well in your response plan, and where there were some holes.
- Lessons learned from both mock and real events will help strengthen your systems against the future attacks.

Incident Response

6. Lessons Learned

- **Questions to address**
  - What changes need to be made to the security?
  - How should employee be trained differently?
  - What weakness did the breach exploit?
  - How will you ensure a similar breach doesn't happen again?

Incident Response

- Incident Response (IR) steps to take after a cyber security event occurs
  - The first priority is to prepare in advance by putting a concrete IR plan in place.
  - Your incident response methodology should be battle-tested before a significant attack or data breach occurs.
  - It should address the following response phases as defined by NIST *Computer Security Incident Handling Guide*

Incident Response

- Incident Response (IR) steps to take after a cyber security event occurs
  1. Assemble your team
  2. Detect and ascertain the source
  3. Contain and recover
  4. Assess the damage and severity
  5. Begin the notification process
  6. Start now to prevent the same type of incident in the future

Incident Response

1. Assemble your team

- It's critical to have the right people with the right skills, along with associated tribal knowledge.
- Appoint a team leader who will have overall responsibility for responding to the incident.
- This person should have a direct line of communication with management so that important decisions—such as taking key systems offline if necessary—can be made quickly.

Incident Response

2. Detect and ascertain the source

- The IR team you've assembled should first work to identify the cause of the breach, and then ensure that it's contained.

Incident Response

3. Contain and recover

- A security incident is analogous to a forest fire. Once you've detected an incident and its source, you need to contain the damage.
- This may involve disabling network access for computers known to be infected by viruses or other malware (so they can be quarantined) and installing security patches to resolve malware issues or network vulnerabilities.
- You may also need to reset passwords for users with accounts that were breached, or block accounts of insiders that may have caused the incident.

Incident Response

4. Assess the damage and severity

- Until the smoke clears it can be difficult to grasp the severity of an incident and the extent of damage it has caused.

Incident Response

5. Begin the notification process

– A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized person.

Incident Response

6. Start now to prevent the same type of incident in the future

- Once a security incident has been stabilized, examine lessons learned to prevent recurrences of similar incidents.
- This might include patching server vulnerabilities, training employees on how to avoid phishing scams, or rolling out technologies to better monitor insider threats.
- Fixing security flaws or vulnerabilities found during your post-incident activities is a given.

Module-7

Information Security Audit Preparation

Information Security Audit Preparation

- Nature and scope of information security audits
- Roles and responsibilities.
- Identify the procedures/guidelines/checklists
- Identify the requirements of information security Audits and prepare for audits in advance.

Information Security Audit Preparation

- **Security Audit Review**
  - Organize data/ information required for information security audits using standard templates and tools
  - Audit tasks, Reviews, Comply with the organization's policies, standards, procedures, guidelines and checklists
  - Disaster Recovery Plan

Security diagnostics

- Three main types of security diagnostics:
  - Information security audits
  - Vulnerability assessments
  - Penetration testing

Information System Audit vs Information Security Audit

- Information System Audit and Information Security Audit are two tools that are used to ensure safety and integrity of information and sensitive data.

Information System Audit vs Information Security Audit

- **Information Systems Audits**
  - Plan and conduct **information systems audits** to evaluate the control environment and internal controls regarding **information** technology governance structure, general and application controls, **system** development, backup and disaster recovery, data integrity, and **system** security.

Information System Audit vs Information Security Audit

- **Information security audit**
  - It is a systematic, measurable technical assessment of how the organization's **security** policy is employed.
  - It is part of the on-going process of defining and maintaining effective **security** policies.
  - **Security audits** provide a fair and measurable way to examine how secure a site really is.

Information Security Audit

- Computer security auditors work with the full knowledge and support of the organization, in order to carry out the audit.
- This usually includes receiving documentation and access by the organization representative.
- A security analyst may be assigned to support and facilitate the audit.

Information Security Audit

- Computer security auditors perform their work though personal interviews, reviewing policies, vulnerability scans, examination of operating system settings, analyses of network shares, and historical data and logs.

Scope of the Audit

- **The scope of the audit depends upon:**

Site business plan
Type of data assets to be protected
Value of importance of the data and relative priority
Previous security incidents
Time available
Auditors experience and expertise

Information Security Audit

- Purposes of audits:
  - Build awareness of current practices and risks
  - Reducing risk, by evaluating, planning and supplementing security efforts
  - Strengthening controls including both automated and human
  - Compliance with customer and regulatory requirements and expectations
  - Building awareness and interaction between technology and business teams
  - Improving overall IT governance in the organization

What should be covered in audits?

Access control	Accountability and audit	Application hosting	Application penetration
Application security	Application support	Application testing	Awareness and training
Business continuity	Certification, accreditation and security assessments	Computer assets, servers and storage networks	Configuration management
Content management	Contingency planning	Disaster recovery planning	Endpoints/edge devices
Identification, authentication and access management	Incident response	Infrastructure devices (e.g. routers, firewall services)	Intrusion detection/prevention

What should be covered in audits?

Maintenance	Media protection	Messaging	Networks (wired and wireless)
Personnel security	Physical and environmental protection	Risk assessment	Security incident management
Security of infrastructure	Security planning	Software	Storage devices
System and information integrity	System services and acquisition	Systems and communications protection	Third party security management
Web security			

Information Security Audit

- Key questions security audits attempt to answer:
  - Are passwords secure and difficult to crack?
  - Are access control lists (ACLs) in place on network devices to control who has access to shared data?
  - Are there audit logs to record to identify who accesses data?
  - Are the audit logs reviewed effectively and how are they reviewed?
  - Are the security settings for operating systems in accordance with accepted industry security practices?
  - How are unnecessary applications and computer services managed?
  - Are they eliminated in a timely and effective manner for each system?
  - Are these operating systems and commercial applications patched?
  - How and when did the patching take place?

Information Security Audit

- Key questions security audits attempt to answer:
  - How is backup media stored? What is the backup policy and is it followed?
  - Who has access to the backup media and is it up-to-date?
  - Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan? Does it have gaps in its construct?
  - Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?
  - What security considerations were used while writing custom-built applications, are these adequate and well documented?
  - How have these custom applications been tested for security flaws?
  - How are configuration and code changes documented at every level?
  - How are these records reviewed and who conducts the review?

Constraints of a security audit

- Time constraints
- Third party access constraints
- Business operations continuity constraints
- Scope of audit engagement
- Technology tools constraints

Types of Security Audits

- There are two types of Audit
  - Internal Audit
  - External Audit

Types of Security Audits

- External audits:
  - External audits are commonly conducted by independent, certified parties in an objective manner.
  - They are scoped in advance, finally limited to identifying and reporting any implementation and control gaps based on stated policies and standards such as the COBIT (Control Objectives for Information and related Technology).
  - At the end the objective is to lead the client to a source of accepted principles and sometimes correlated to current best practices

Types of Security Audits

- Internal audits:
  - Internal audits are usually conducted by experts linked to the organization, and it involves a feedback process where the auditor may not only audit the system but also potentially provide advice in a limited fashion.
  - They differ from the external audit in allowing the auditor to discuss mitigation strategies with the owner of the system that is being audited.

Phases of Information Security Audit

1. Pre-audit agreement stage
2. Initiation and Planning stage
3. Data collection and fieldwork (Test phase)
4. Analysis
5. Reporting
6. Follow-through

Phases of Information Security Audit

1. Pre-audit agreement stage
   - Agree on scope and objective of the audit.
   - Agree on the level of support that will be provided.
   - Agree on locations, duration and other parameters of the audit.
   - Agree on financial and other considerations.
   - Confidentiality agreements and contracting to be completed at this stage.
   - Developing/creating a formal agreement (e.g., statement of work, audit memorandum, or engagement memo) to state the audit objectives, scope, and audit protocol

Phases of Information Security Audit

2. Initiation and Planning stage
   - Conducting a preliminary review of the client's environment, mission, operations, polices, and practices.
   - Performing risk assessments of client environment, data, and technology resources.
   - Completing research of regulations, industry standards, practices, and issues.
   - Reviewing current policies, controls, operations, and practices.
   - Holding an Entrance Meeting to review the engagement memo, to request items from the client, schedule client resources, and to answer client questions.
   - This will also include laying out the time line and specific methods to be used for the various activities.

Phases of Information Security Audit

3. Data collection and fieldwork (Test phase)
   - This stage is to accumulate and verify sufficient, competent, relevant, and useful evidence to reach a conclusion related to the audit objectives and to support audit findings and recommendations.
   - During this phase, the auditor will conduct interviews, observe procedures and practices, perform automated and manual tests, and other tasks.
   - Fieldwork activities may be performed at the client's worksite(s) or at remote locations, depending on the nature of the audit.

Phases of Information Security Audit

4. Analysis
   - Analyses are performed after documentation of all evidence and data, to arrive at the audit findings and recommendations.
   - Any inconsistencies or open issues are addressed at this time.
   - The auditor may remain on-site during this phase to enable prompt resolution of questions and issues.
   - At the end of this phase, the auditor will hold an Exit Meeting with the client to discuss findings and recommendations, address client questions, discuss corrective actions, and resolve any outstanding issues.
   - A first draft of the findings and recommendations may be presented to the client during the exit meeting.

Phases of Information Security Audit

5. Reporting
   - Generally, the Information Security Audit Program will provide a draft audit report after completing fieldwork and analysis.
   - Based on client response if changes are required to the draft, the auditor may issue a second draft.
   - Once the client is satisfied that the terms of the audit are complied with the final report will be issued with the auditor's findings and recommendations.

Phases of Information Security Audit

6. Follow-through
   - Depending on expectations and agreements the auditor will evaluate the effectiveness of the corrective action taken by the client, and, if necessary, advise the client on alternatives that may be utilized to achieve desired improvements.
   - In larger, more complex audit situations, follow-up may be repeated several times as additional changes are initiated.
   - Additional audits may be performed to ensure adequate implementation of recommendations.
   - The level of risk and severity of the control weakness or vulnerability dictate the time allowed between the reporting phase and the follow-up phase.
   - The follow-up phase may require additional documentation for the audit client.

Role of an Auditor

- Auditors ask the questions, test the controls, and determine whether the security policies are followed in a manner that protects the assets the controls are intended to secure by measuring the organization's activities versus its security best practices.

Role of an Auditor

- The role of the auditor is to identify, measure, and report on risk.
- The auditor is not tasked to fix the problem, but to give a snapshot in time of the effectiveness of the security program.
- The objective of the auditor is to report on security weakness.

Role of an Auditor

- The auditor functions as an independent advisor and inspector.
- The auditor is responsible for planning and conducting audits in a manner that is fair and consistent to the people and processes that are examined.
- The auditing charter or engagement letter defines the conduct and responsibilities of an auditor.

Role of an Auditor

- Depending on how a company's auditing program is structured, ultimate accountability for the auditor is usually to senior management or the Board of Directors.
- Auditors are usually required to present a report to management about the findings of the audit and also make recommendations about how to reduce the risk identified.

Responsibilities of an Auditor

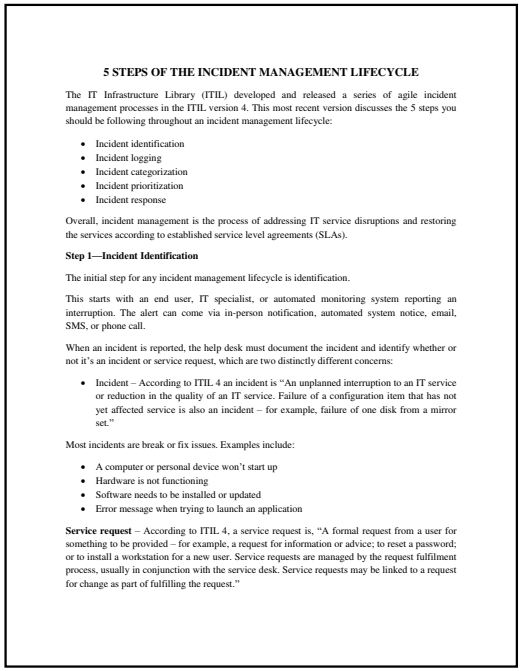
- Plan, execute and lead security audits across an organization.
- Inspect and evaluate financial and information systems, management procedures and security controls.
- Evaluate the efficiency, effectiveness and compliance of operation processes with corporate security policies and related government regulations.

Responsibilities of an Auditor

- Develop and administer risk-focused exams for IT systems.
- Review or interview personnel to establish security risks and complications.
- Execute and properly document the audit process on a variety of computing environments and computer applications.
- Assess the exposures resulting from ineffective or missing control practices.

Responsibilities of an Auditor

- Provide a written and verbal report of audit findings
- Develop rigorous "best practice" recommendations to improve security on all levels
- Work with management to ensure security recommendations comply with company procedure
- Collaborate with departments to improve security compliance, manage risk and bolstern effectiveness



5 STEPS OF THE INCIDENT MANAGEMENT LIFECYCLE

The IT Infrastructure Library (ITIL) developed and released a series of agile incident management processes in the ITIL version 4. This most recent version discusses the 5 steps you should be following throughout an incident management lifecycle:

- Incident identification
- Incident logging
- Incident categorization
- Incident prioritization
- Incident response

Overall, incident management is the process of addressing IT service disruptions and restoring the services according to established service level agreements (SLAs).

Step 1—Incident Identification

The initial step for any incident management lifecycle is identification.

This starts with an end user, IT specialist, or automated monitoring system reporting an interruption. The alert can come via in-person notification, automated system notice, email, SMS, or phone call.

When an incident is reported, the help desk must document the incident and identify whether or not it's an incident or service request, which are two distinctly different concerns:

- Incident – According to ITIL 4 an incident is "An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident – for example, failure of one disk from a mirror set."

Most incidents are break or fix issues. Examples include:

- A computer or personal device won't start up
- Hardware is not functioning
- Software needs to be installed or updated
- Error message when trying to launch an application

Service request – According to ITIL 4, a service request is, "A formal request from a user for something to be provided – for example, a request for information or advice; to reset a password; or to install a workstation for a new user. Service requests are managed by the request fulfilment process, usually in conjunction with the service desk. Service requests may be linked to a request for change as part of fulfilling the request."

Since these formal requests can be scheduled and follow predefined processes, they're not nearly as urgent as an incident. Examples include:

- Creating an account for a new employee/user
- Requesting upgraded hardware
- Needing to change a password

It's best if an incident can be identified early on through automatic monitoring. When that happens, the problem can be resolved before it has an impact on users. However, there will inevitably be times when the service desk is only made aware of the incident by the impacted user.

Once the incident has been identified, the service team can move to the next step in the incident lifecycle ITIL.

Step 2—Incident Logging

After the team has been notified about the incident, it's crucial that they record and document it.

Thorough reporting helps your organization notice incident trends that may morph into larger problems. It also gives your team better visibility over their workflow, allowing them to delegate their resources where they're needed most.

Every incident must be reported – big and small – and logged as a ticket. Tickets need to contain the following information:

- User name
- User contact information
- Date and time of the report
- Description of the incident

When it comes to incident logging, the more details you can include, the better. Rigorous data collection empowers your service team to find patterns and seek out the root causes for incidents that crop up repeatedly. Armed with this information, the team can either templatize responses for common issues or use automated programs to help streamline resolution processes.

Step 3—Incident Categorization

Incident categorization requires the service team to assign a category and at least one sub category to any incident. This is done for three critical reasons:

- It helps the service desk sort and model incidents according to their categories and subcategories.
- It makes it possible to automatically prioritize some of the issues.

- Provides accurate incident tracking.

By assigning appropriate categories, it becomes easier for the help desk to assign, escalate, and then monitor incident trends and frequencies. When done correctly, it streamlines incident logging, prevents redundancy, and quickens the entire resolution process.

Categorization utilizes a hierarchical structure with multiple levels of classification—usually with three to four levels of granularity. But since all organizations are unique, classification must be conducted internally, especially at lower levels. If you need help with yours, HCI recommends taking the following steps:

- Hold a brainstorming session among the relevant support groups
- Use this session to decide the 'best guess' top-level categories and include an 'other' category. Create relevant logging tools to use these new categories.
- Conduct a trial period that allows several hundreds incidents to fill up each category.
- Perform an analysis of incidents. The number of incidents logged per category will inform you as to whether or not they're worth having.
- Breakdown each incident within higher-level categories to decide if lower-level categories are necessary.
- Review the results and repeat the activities for a few more months to ensure that your results are accurate and repeatable.

By categorizing incidents you can extrapolate on which trends require training or problem management.

Step 4—Incident Prioritization

After incidents have been assigned their proper category, the next important task is to prioritize them according to urgency and impact on the users and the business. Urgency is how quickly a resolution needs to happen, whereas impact is the potential damage an incident could cause.

Incidents are typically designated one of three priority statuses:

- Low-priority incidents – Do not interrupt users or the business and can generally be worked around. Service to customers and users continues.
- Medium-priority incidents – Impact some employees and can moderately disrupt work. Customers may be slightly inconvenienced by the incident.
- High-priority incidents – Affect a significant number of users or customers, interrupt the business, and have a noticeable impact on service delivery. Such incidents will almost always cause a financial toll.

Since your help desk's resources and time is limited, the higher the assigned priority, the quicker the team must respond to the incident. The system ensures that IT teams aren't focusing on low-level incidents while much larger ones are wreaking havoc on your employees or customers.

Step 5—Incident Response

After an incident has been identified, logged, categorized, and prioritized, the service desk can get to work on resolution. Incident resolution has sub steps to follow, including:

- Initial diagnosis – User details the problem and undergoes troubleshooting with the service agent.
- Incident escalation – If the incident requires advanced support, it can be forwarded to certified support staff or on-site technicians. Most incidents should be able to be resolved by the initial service agent.
- Investigation and diagnosis – Once the initial incident hypothesis is confirmed, staff can then apply a solution or workaround.
- Resolution and recovery – The service desk confirms that the user's service has been restored to agreed upon SLA level.
- Incident closure – The incident is closed and no further work is required.

RSI Security: Incident Management Lifecycle Experts

From initial reporting to final resolution the incident management lifecycle entails 5 critical steps:

- Incident identification
- Incident logging
- Incident categorization
- Incident prioritization
- Incident response

At their best IT incidents can be a minor annoyance. But at their worst they can jeopardize your entire business. Should an incident occur, you'll require an expert partner to guide you through the expanded incident lifecycle.

Reference:

1. https://blog.rsisecurity.com/5-steps-of-the-incident-management-lifecycle/
2. https://digitalguardian.com/blog/five-steps-incident-response
3. https://www.manageengine.com/products/service-desk/itil-incident-management/what-is-itil-incident-management.html
4. https://www.alaska.edu/files/oit/ITSM_Program/Incident-Management-Process-Description-v1.pdf
5. https://www.bmc.com/blogs/itil-v3-incident-management/