Introduction to Incident Response (Unit-1)

Cyber Incident Statistics:

COVID-19 Statistics

- Following the onset of COVID-19, 85% of CISOs overlooked cybersecurity to quickly enable remote working.
- The cybersecurity market is expected to grow 6.2% per year until 2023 because of the COVID-19 pandemic.
- 445 million cyber-attacks were reported during the first three months of the pandemic — a 20% increase as compared to the previous quarter.
- By March 2020, there was over a 650% increase in COVID-19-themed spear-phishing emails.
- Between January and May 2020, the FTC recorded a loss of $24.44 million as a result of COVID-19-themed online scams.

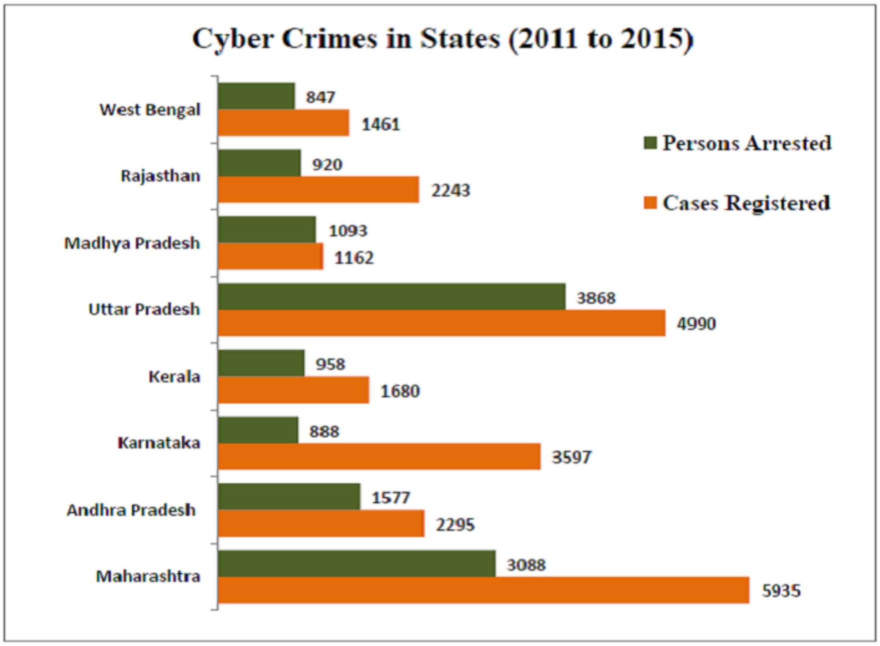
Managed Service Provider Cyber Attack Statistics

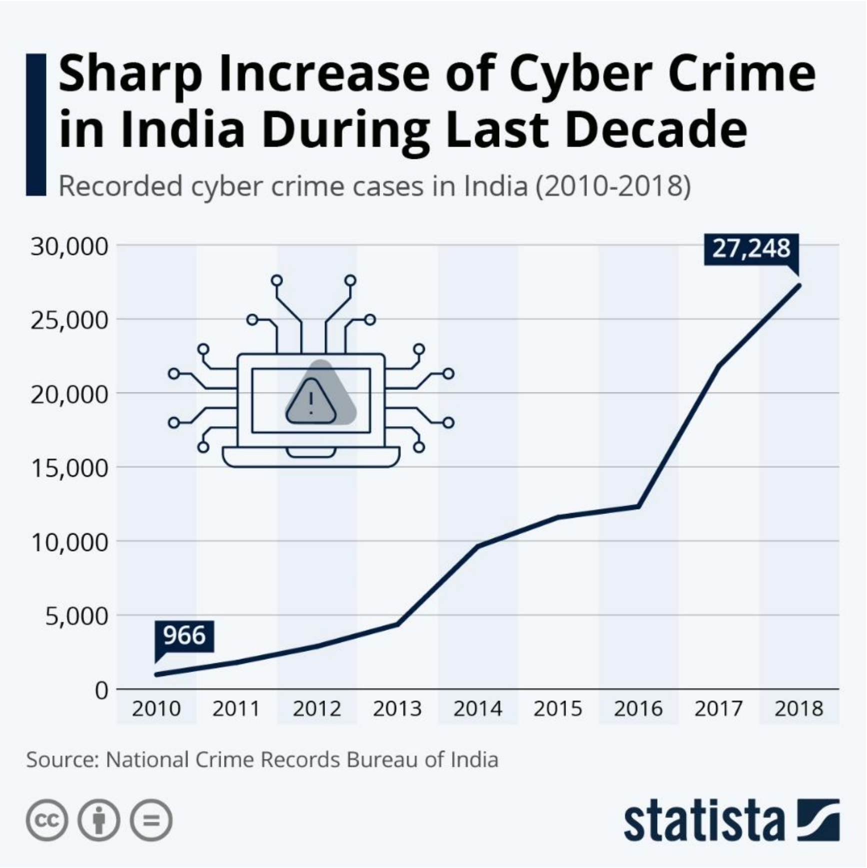
- 4 in 5 managed service providers (MSPs) have experienced an increase in ransomware attacks.
- The average amount of ransom for MSPs went up from $10,000 to more than $100,000 during the last couple of years.
- 25% of MSPs plan to offer security management software and tools and 22% plan to offer intrusion monitoring services in the next year.
- 43% of MSPs offer managed security services in partnership with an MSSP because of the complexity surrounding cybersecurity.

Small Business Statistics

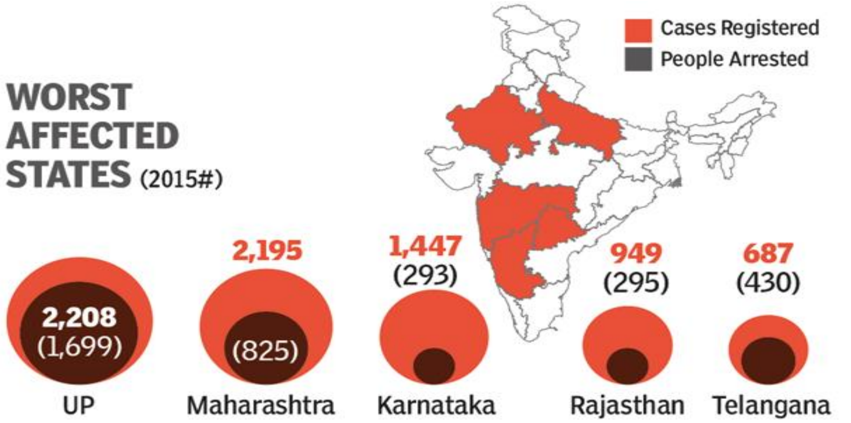
- The average data breach cost for small organizations (less than 500 employees) fell to $2.35 million in 2020, compared to $2.74 million in 2019.
- One in every five small businesses does not have any endpoint security in place, while one in three relies only on free cybersecurity solutions.
- 28% of all data breaches involve small businesses.
- 30% of small businesses consider phishing attacks to be their top cybersecurity concern.

- Electronic Data Liability Insurance average premiums range from $619 to $3,297 with the highest premiums going up to $55,500



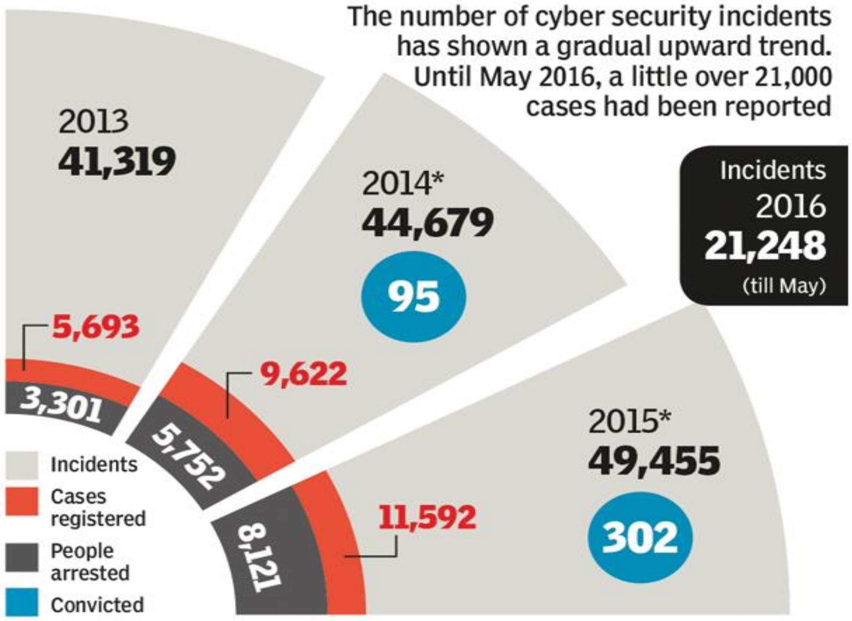


WORST AFFECTED STATES (2015#)



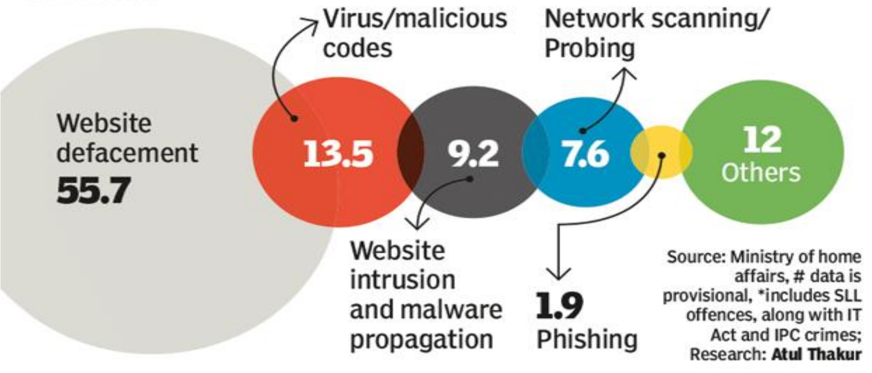
CONVICTION ONLY IN 0.03% OF REGISTERED CASES

The number of cyber security incidents has shown a gradual upward trend. Until May 2016, a little over 21,000 cases had been reported



ATTACK TYPE AND % OF TOTAL INCIDENTS/ ATTACKS

An analysis of various security incidents (2013 to 2015) shows that more than half were linked to website defacement, followed by virus and malware propagation



Source: Ministry of home affairs, # data is provisional, *includes SLL offences, along with IT Act and IPC crimes; Research: **Atul Thakur**

Computer Security Incident:

What is an incident?

An incident, in the context of information technology, is an event that is not part of normal operations that disrupts operational processes. An incident may involve the failure of a feature or service that should have been delivered or some other type of operation failure. Security incidents are events that indicate that an organization's systems or data may have been compromised.

What Is a Security Incident?

A security incident is any event related to compromised data resulting from non-existent or failed protective security measures. In the cybersecurity realm, an information security incident or a cybersecurity incident is a security incident that involves the unauthorized access, use, disclosure, breach, modification, or destruction of data.

What Are the Most Common Types of Security Incidents?

Nowadays, the most common types of security incidents are almost entirely relegated to the cyber domain. Using technology to their advantage, cybercriminals will do everything and anything possible for financial gain. Here are some of the most common types of security incidents executed by malicious actors against businesses and organizations:

- **Unauthorized Access Attacks**

This type of security incident involves any unauthorized attempts by a threat actor to access systems or data using an authorized user’s account. How a cybercriminal gains access to user accounts oftentimes remains a mystery, even long after an attack-but there are a few things your organization can do to prevent this type of security incident from occurring.

If you don’t already do so, require multi-factor authentication-or at least two-factor authentication-for all of your users. This will require users to provide an additional piece of identifying information after they enter a correct username and password. In many cases, multi-factor authentication alone is enough to deter a potential security incident from occurring-cybercriminals often go after the lowest hanging fruit, so any additional barriers you put in place between them and your data make you less likely to be targeted in the first place.

You should also consider encrypting your sensitive corporate data both at rest and in transit using suitable software or hardware technology. This way, attackers won't be able to access your confidential data even if an attack is successful.

- **Privilege Escalation Attacks**

This type of security incident occurs when an attacker attempts to gain unauthorized access to an organization's network and then also tries to obtain more privileges using a privilege escalation exploit. A successful privilege escalation exploits grants threat actors privileges that normal users don't have, and usually, this type of attack takes place only after a hacker has already compromised an organization's network by gaining unauthorized access to a lower-level user account.

With privileged access to your most sensitive information, there's no telling what a cybercriminal might do. However, there are some ways in which you can prevent this type of security incident from occurring.

First, you should start by looking for and remediating any security vulnerabilities – weak spots – in your IT environment. Ideally, this is something your organization should do regularly by conducting vulnerability assessments and vulnerability scans as part of your overall risk management program. During the risk management process, your organization should take cyber risks into serious consideration by evaluating the risks to your sensitive data and taking the necessary steps to secure that data with a risk analysis and a well-documented risk management plan.

- **Insider Threat Attacks**

No organization wants to admit that their employees are capable of acting maliciously, but unfortunately, it's a harsh reality that requires some serious attention. Insider threats are malicious (intentional) or accidental (unintentional) threats to your organization's security data. Typically, this type of security incident is attributed to employees, former employees, or third parties including contractors, temporary workers, or customers.

While it can be difficult to prevent insider threats from affecting your business, there are some things you can do to deter the possibility of a successful security incident. First and foremost, you should implement spyware scanning programs, antivirus programs, firewalls, and a rigorous data backup and archiving routine.

You should also train your employees and any contractors on security awareness before allowing them access to your corporate network. A robust security awareness training program should also include routine training sessions to avoid any unintentional security incidents resulting from user error.

To deter insider threats, you can also implement employee monitoring software to reduce your risk of a data breach or the theft of intellectual property by identifying careless, disgruntled, or malicious insiders. Additionally, a comprehensive whistleblower program that protects any employees who come forward about malicious activity can help your organization to gain intel about potential security incidents.

A data loss prevention policy will also let insiders know what’s expected of them when it comes to handling company data and that they’re being monitored for unwanted behaviors. Sometimes, this alone is enough to prevent internal actors from acting carelessly or maliciously.

- **Phishing Attacks**

In this type of social engineering attack, the attacker assumes the identity of a reputable entity or person via email to distribute malicious links or attachments that can perform a variety of functions, including extracting login credentials or account information from victims. More targeted types of phishing attacks are known as spear phishing attacks, wherein the attacker invests more time researching the victim to pull off an even more sophisticated attack.

On a technical level, a gateway email filter will help you trap a large number of mass-targeted phishing emails and reduce the overall number of emails that reach your users' inboxes. However, you probably won't be able to prevent every single phishing attempt from entering every single inbox, but there are some things you can do to reduce the likelihood that one of your employees will fall victim to a phishing attack.

Start by educating your users so that they're better able to identify phishing attempts on their own. In some organizations, incentive programs encourage employees to identify and report phishing emails in exchange for a reward. These types of programs have shown success in preventing phishing attacks from leading to more serious types of security incidents, like malware attacks.

- **Malware Attacks**

Malware is a broad term for a variety of different types of malicious software, including Trojans, worms, ransomware, adware, spyware, and other types of viruses. Malware can either be inadvertently installed when a user clicks on an advertisement, visits an infected website, or installs freeware or other infected software; or, it can be installed intentionally by insider threat actors or malicious actors with unauthorized access.

The signs of a malware attack include unusual system activity, sudden loss of disk space, unusually slow speeds, repeated crashes or freezes, an increase in unwanted internet activity, and pop-up advertisements.

To protect your organization against this type of security incident, you should install an antivirus tool to detect and remove any malware. Whether you decide on real-time protection or routine system scans to detect and remove malware, whichever tool you choose should protect your organization against any existing malware in addition to any future malware attacks.

- **Distributed Denial-of-Service (DDoS) Attacks**

This type of security incident takes place when a threat actor floods the target with traffic or sends it some information that triggers an attack to shut down an individual machine or an entire network so that it's unable to respond to service requests. Typically, these types of attacks can be dealt with by simply rebooting the system.

To block any future unwanted traffic, you can also reconfigure your firewalls, routers, and servers. Keep your firewalls updated with the latest security patches as part of your overall patch management program to keep your systems, software, and applications at their most secure. If you so choose, you can also integrate front-end hardware into your network to help analyze and screen data packets to classify them as they enter the system.

- **Man-in-the-Middle (MitM) Attacks**

This type of security incident occurs when an attacker secretly intercepts and alters messages between two parties who believe they are communicating directly with each other. In a man-in-the-middle attack, the attacker manipulates both victims to gain access to their data. This can take place via session hijacking, email hijacking, and wi-fi eavesdropping.

Although this type of attack is difficult to detect, there are some ways you can prevent it from happening. You should first consider implementing an encryption protocol that provides authentication, privacy, and data integrity between communicating computer applications such as Transport Layer Security (TLS). Or, perhaps a network protocol that gives users, particularly systems administrators, a secure way to access a computer over an unsecured network such as a Secure Shell Protocol (SSH).

You should also educate your employees on the dangers of using open public wi-fi networks because it's much easier for hackers to exploit these connections. For the most network protection, use a virtual private network (VPN) to help ensure more secure connections.

- **Password Attacks**

A password attack is a type of security incident in which the attack is aimed specifically at obtaining a user's password or an account's password. To do so, hackers use a variety of methods, such as password-cracking programs, dictionary attacks, password sniffers, or simply guessing passwords via brute force trial and error.

A password cracker is an application or program that’s used to identify an unknown or forgotten password to a computer or network’s resources. When in the hands of a hacker, a password cracker can be used to gain unauthorized access to company resources.

A dictionary attack is a method of breaking into a password-protected computer system or server by systematically entering every word in the dictionary as a password until the attacker guesses correctly. While this method might not be the most efficient, if a hacker does guess a correct password, they may try to log in to multiple accounts using the same hacked password.

A brute force attack is one in which a hacker or bot attempts to log in using a series of generated passwords over and over again until they are successful. This type of trial and error attack can also cause websites to crash and is yet another reason why multi-factor authentication is so important.

These types of security incidents can be difficult to prevent completely, but there are some things you can do to defend yourself against them in the future. As mentioned above, multi-factor authentication is the best way to prevent unauthorized logins. Even if a cybercriminal guesses the correct password, it won’t be enough information to get them into your system.

- **Web Application Attacks**

This type of security incident occurs when a web application is used as the vector of an attack. Web application attacks include exploits of code-level vulnerabilities in the application as well as attacks that thwart authentication mechanisms.

For example, a cross-site scripting attack is a type of web application attack called an injection security attack and occurs when an attacker injects data (such as a malicious script) into content from otherwise trusted websites.

To avoid this type of attack, your organization should review code early in the development phase to detect any vulnerabilities automatically by using static and dynamic code scanners. You should also implement **bot detection functionality** to prevent bots from accessing your application data. Finally, a web application firewall will help you monitor your network and block potential attacks.

Another type of web application attack is called an **advanced persistent threat (APT**), which is a prolonged and targeted cyberattack that's typically executed by cyber criminals or nation states to gain access to a network and remain undetected for some time. Ultimately, the goal of this type of security incident is to monitor the target's network activity and steal data rather than cause damage to the network or organization.

To avoid this type of attack, your organization should monitor both incoming and outgoing traffic to prevent hackers from installing backdoors and extracting sensitive data. Again, web application firewalls at the edge of your network perimeter will help to filter any traffic coming into your web application servers. A firewall can also help filter out application layer attacks such as SQL injection attacks which are often used during the APT infiltration phase.

How to Prevent & Mitigate Security Incidents?

For each of the common security incidents described above, we included several things you can do to prevent or at least reduce the chances of an incident occurring. To make things easier, we've compiled those suggestions into a singular and actionable list so that you can get started preventing and mitigating security incidents for your organization.

- ***Security Incident Detection***

The first step to preventing security incidents from occurring is to put the right tools and processes in place to detect security incidents before they occur. Security incident detection is not only important for detecting and responding to incidents before they do damage, but also so that you can track and trace the origins of the security incident and put the appropriate security controls in place to prevent it from happening again.

- ***Monitor User Account Behavior***

Start by implementing behavior analytics tools to monitor user account behavior. Before you start looking for any anomalous behavior, you need to set the baseline for what "normal" behavior looks like. Once you've established that pattern, you can start looking for anomalies in behavior patterns- and especially so for privileged users. Any unusual behaviour could be an indication that a security incident is taking place.

You should also monitor for any unauthorized users attempting to access servers and data or requesting access to data that isn't critical to their job function. This type of behavior is indicative of two scenarios: an inside threat actor attempting to gain unauthorized access to sensitive information for malicious purposes; or, a malicious actor has successfully gained access to a user account and is using that account to attempt to gain access to more privileged data.

As a general rule, you should always use the principle of least privilege when it comes to your data. This means only granting access to data to those employees who need access to perform their duties. However, to implement this principle, you'll need to start by categorizing your data by sensitivity so that you know which data your employees should have the least access to.

- ***Monitor Network Traffic***

Your organization's network is the gateway into your systems and datthe a-keeping it secures is the best way to prevent attackers from gaining unauthorized access to your organization's sensitive information. However, when it comes to network traffic, it's important to monitor not just the traffic coming into your network, but also the traffic leaving your network perimeter.

This might include insiders uploading large files to personal cloud applications, sending large numbers of email messages containing attachments to addresses outside the company, or downloading large files to external storage devices such as USBs. You should also monitor for any traffic sent to or from unknown locations-especially if your company only operates in one country.

In general, your administrators should investigate any unknown or suspicious network traffic to ensure its legitimacy. Even if there isn't anything malicious occurring, in this case, it's better to be safe than sorry.

- ***Monitor Suspicious Activity***

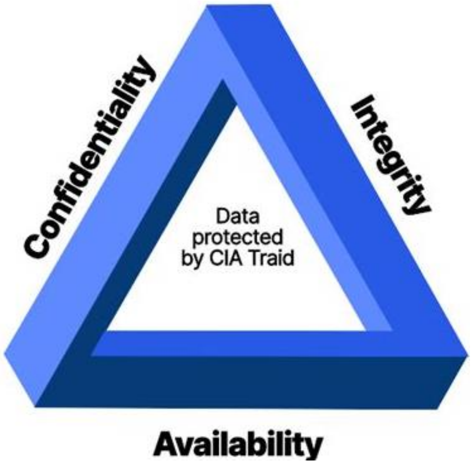
Monitoring user account behaviour and network traffic are just two of how you can deter potential security incidents from occurring. Some of the other suspicious activity you should monitor include:

- Excessive consumption or an increase in the performance of server memory or hard drives could mean an attacker is accessing them.
- Changes in a configuration that haven't been approved, such as reconfiguration of services, installation of startup programs, or firewall changes are often a sign of possible malicious activity.
- Hidden files that might be considered suspicious due to file names, sizes, or locations and could indicate a data leak.
- Unexpected changes such as user account lockouts, password changes, or sudden changes in group memberships.
- Abnormal browsing behavior like unexpected redirects, changes in browser configuration, or repeated pop-ups.
- Suspicious registry entries, which are usually a result of a malware infection.

Information Warfare: Information warfare can be a combination of lies, manipulated truths, manufactured media, or in some cases exploiting human nature to sow confusion. OR it is a concept involving the battlespace use and management of information and communication technology (ICT) in pursuit of a competitive advantage over an opponent.

Key Concepts of Information Security:

The ultimate goal of information security is to maintain the CIA triad within an organization. The elements of the CIA triad are shown below:



Confidentiality: This means ensuring that only authorized users have access to information. Whenever a company suffers from a data breach or data leak and individuals' information is accessed by criminals, the public or employee's that don't have the proper authorization, confidentiality has been compromised. Some of the key security controls that you can use to maintain confidentiality are:

- Encryption: Encrypting information ensures that even if an unauthorized user can get access to the information, without the decryption key the information will be in an unreadable format and therefore confidentiality will be maintained.
- Strong Passwords: By having strong passwords reduces the chances of someone being able to access accounts or resources by guessing the password.
- Two-factor authentication: 2FA supplements traditional login information (username and password) by requiring an additional code before granting someone access to a resource.
- Identity and Access Management (IAM): IAM is the practice of ensuring that only the correct individuals are given access to resources. It follows something called the "least privilege model", this means that users should only be given access to the resources needed to do their job and nothing more. This helps to enforce the confidentiality of information.
- Proper Technical Controls: Technical controls include things like firewalls and security groups. These controls prevent people from accessing the company's network and prevent them from obtaining company information without authorization.

- Physical Locks and Doors: Physical security measures like cabinet locks, vaults, biometric scanners, and door locks prevent people from physically sneaking into the company and taking company documents.

Integrity: To protect information from being modified by unauthorized people and ensures that the information is trustworthy and accurate. Anytime information is modified by someone that isn't authorized to do so, whether it was someone inside the company or outside, it is a violation of the information's integrity. An example would be if the CFO sends a document to be examined or reviewed by the director of finance. The director of finance may try to manipulate the information without the CFO knowing to make his/her department look better, launder money, etc. You need to have a means of knowing whether or not a document has been modified without your knowledge so that you can trust that document's integrity. Also, in the event data is lost, you need to be able to recover all of that data or at least most of it from a trusted source. Some controls you can use to maintain integrity are:

- Hashes: A hash is the output of a hashing algorithm such as MD5 or SHA. A hash algorithm takes a message of any size and creates a fixed-sized value called a hash (eg 12 characters long). If any character in the original message is changed, it will result in a different hash being generated. By creating a hash of a message when you first receive it, you can later test to see if that message has been altered in any way.
- For example, say I have a word document on March 10th, 2020, I use a hash algorithm to generate the hash 123456789. Then on March 15th, I want to check if anyone has modified that file, I can use the hash algorithm again and if the hash created is not the same, I know someone changed the contents of that file.
- Secure Backups: By creating secure backups if you ever have doubts about the integrity of the data on a system you can reboot that system using the information you have in your backups. Hashes can be used with your backups to ensure that they have not been altered in any way. This way you can be confident that the information you are using to reboot your systems is accurate. A good example of when you will need this is if your company ever suffers a ransomware attack and is unable to recover your data.

- User access controls: By controlling what information users have edit access to, you limit the potential for users to edit information without permission.

Availability: To ensure that the information is accessible to authorized people whenever it is needed. An example of this would be a website like Netflix. Most companies want the availability of at least 99.99%, which means that 99.99% of the time you go to Netflix you should be able to access the services that you want. To do this there are several practices you can implement to ensure that your company will have a high uptime:

- Off-site backups: Having off-site backups ensures that if something happens you have a copy of data to restart your systems and keep your business going.
- Disaster Recovery & Business Continuity Planning: These plans outline how your company should respond to certain types of situations such as earthquakes, floods, fires, hurricanes, etc
- Redundancy: This is when you make multiple instances of network devices and lines of communication so that if one device or line fails it doesn’t cause a loss of availability.
- Failover: This is a backup node (system) that automatically switches into production if the primary system fails.
- Virtualization: This is the process of creating a software (virtual) version of something that physically exists. Usually, this takes one piece of hardware and enables it to run multiple operating systems in virtual machines (VMs), this way you can have redundancy even though you only have 1 physical machine.
- Proper Monitoring of the environment: You want to have proper monitoring through tools like a SIEM. This way you will know as soon as there is a problem in your environment and you can address the issue asap.

In addition to these three principles, there is a fourth principle that is very popular. **Non-Repudiation:** This means that users cannot deny that they have performed a particular action and it enables you to hold people accountable for their actions. It’s important that people can be held accountable for their actions and that people know they will be held accountable so that it deters negative behaviour. Also, if someone does something against company policy or the law they can be punished, and corrective action is taken. Here are some tools that will allow you to enforce non-repudiation:

- **Account logging and Monitoring:** It's important to log the activities of users on different accounts so that you know who did what and can trace that back to an individual. Typically, each user should also have an account so that no one can deny that they acted.
- **Digital Signatures:** Digital signatures function similarly to written signatures, they verify an individual's identity. Usually used to sign messages or contracts.
- **Read Receipts:** When you send an email, text, or notification most platforms allow you to request some type of reading receipt. This confirms that the person received the message and records the time.

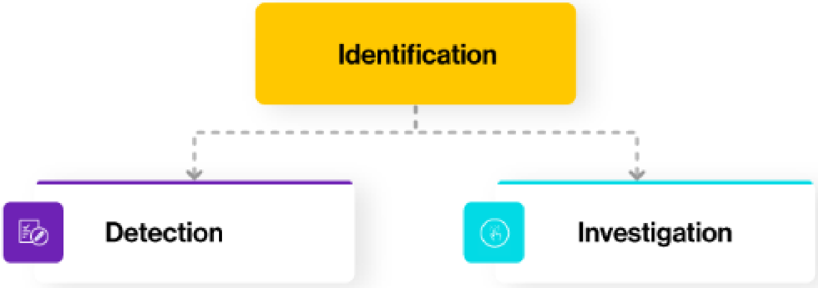
Types & examples of Computer Security Incidents:

Name of an Incident	Brief Detail	Preventive Measures
Unauthorized Access Attacks	access systems or data using an authorized user's account	multi-factor authentication-or at least two-factor authentication-for all of your users
Privilege Escalation Attacks	an attacker attempts to gain unauthorized access to an organization's network and then also tries to obtain more privileges using a privilege escalation exploit.	conducting vulnerability assessments and vulnerability scans as part of your overall risk management program. Also, consider security monitoring tools to help you collect and analyze potential security threats so you can respond appropriately.

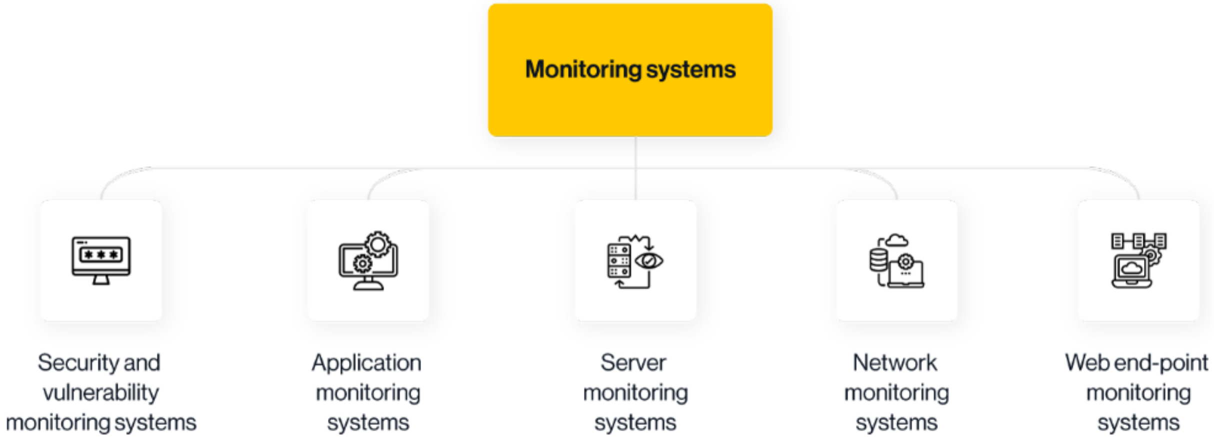
Insider Threat Attacks	No organization wants to admit that their employees are capable of acting maliciously, but unfortunately, it’s a harsh reality that requires some serious attention.	implement spyware scanning programs, antivirus programs, firewalls, and a rigorous data backup and archiving routine. Also, train your employees and any contractors on security awareness before allowing them access to your corporate network.
Phishing Attacks	the attacker assumes the identity of a reputable entity or person via email to distribute malicious links or attachments that can perform a variety of functions, including extracting login credentials or account information from victims.	Use the gateway email filter. Start by educating your users so that they’re better able to identify phishing attempts on their own.
Malware Attacks	Malware is a broad term for a variety of different types of malicious software, including Trojans, worms, ransomware, adware, spyware, and other types of viruses. The signs of a malware attack include unusual system activity, sudden loss of disk space, unusually slow speeds, repeated crashes or freezes, an increase in unwanted internet activity, and pop-up advertisements.	install an antivirus tool to detect and remove any malware. Whether you decide on real-time protection or routine system scans to detect and remove malware.
Distributed Denial-of-Service (DDoS) Attacks	a threat actor floods the target with traffic or sends it some information that triggers an attack to shut down an individual machine or an entire network	reconfigure your firewalls, routers, and servers. Keep your firewalls updated with the latest security patches as part of your overall patch management program to keep your systems, software, and applications at their most secure.

Man-in-the-Middle (MitM) Attacks	the attacker manipulates both victims to gain access to their data. This can take place via session hijacking, email hijacking, and wi-fi eavesdropping.	implementing an encryption protocol that provides authentication, privacy, and data integrity between communicating computers. educate your employees on the dangers of using open public wi-fi networks because it's much easier for hackers to exploit these connections.

How to Identify an Incident?



To detect an incident, monitor the system


Monitoring systems
Security and vulnerability monitoring systems
Application monitoring systems
Server monitoring systems
Network monitoring systems
Web end-point monitoring systems

To investigate:

- Logging the incident

Here, the agent captures important information like the incident source, services that have been affected, and the date and time at which the incident was reported.

- Categorization

Agents understand the nature of the incident, its effects, the source, the impact, and other relevant information, and categories the incident to ensure the right stakeholders are brought in to resolve the incident at the earliest.

- Prioritization

Depending on whether the incident is a minor one or a major one, different levels of priority are assigned. An action priority matrix would help you classify the incident by severity.

EXAMPLE: DETECTION OF CYBER SECURITY INCIDENT

There are several methods to detect security incidents. They are:

- **The Privileged User Accounts Unusual Behavior:** If there is an abnormality in the behavior of a privileged user account, this indicates that someone is using the privileged user account to gain unauthorized access to the network.
- **The Servers and Data Accessed by Unauthorized Insiders:** The systems and data that can be accessed by the insiders will be tested by them. If unauthorized users are trying to access servers and data, trying to access the data that is not related to their jobs, abnormal times logging in from unusual locations, or trying to log in from multiple locations in a short period are all warning signs.
- **Outbound Network Traffic Abnormality:** Organizations should not only worry about the traffic that is coming into the network, but they should also worry about monitoring the

traffic exiting their perimeters. Traffic exiting their perimeters include large files uploaded by the insiders to personal cloud applications, large files downloaded to external storage devices like USB flash drives, or a large number of email messages sent with attachments outside the company.

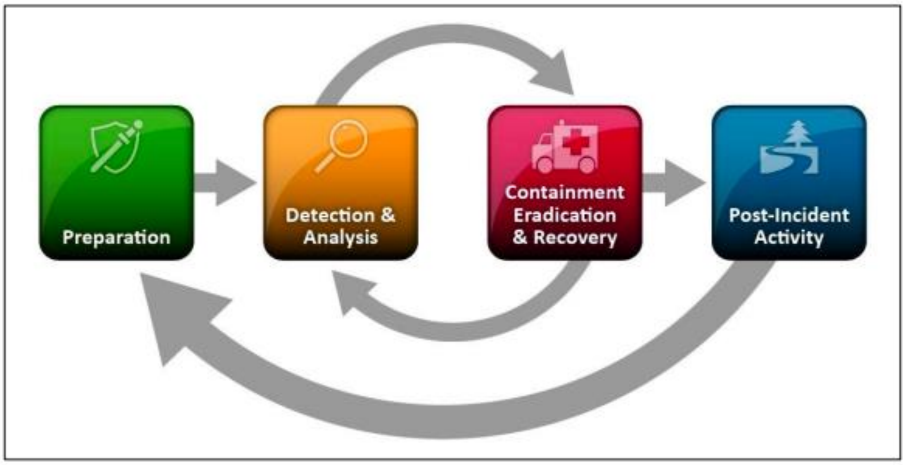
- **Traffic Sent to Unknown Locations or Traffic Sent from Unknown Locations:** Suppose an organization is operating in only one country, the traffic sent to other countries indicates malicious activity. Investigation of traffic to any unknown network must be done by the administrators to make sure the traffic is legitimate.
- **Too Much Consumption:** Performance improvement of server memory or hard drives means that the attacker is accessing the server memory or hard drives illegally.
- **Configuration Changes:** Changes like a reconfiguration of services, startup programs installation, or changes in the firewall that are not approved are an indication of possible malicious activity. The same holds for the added scheduled tasks.
- **Files that Are Hidden:** Hidden files are considered suspicious because their filenames, sizes, or locations indicate the data or logs can be leaked.
- **Unexpected Changes:** Unexpected changes are lockouts of a user account, changes in password, or group membership changes.
- **Abnormal Browsing Behavior:** Abnormal browsing behavior includes unnecessary redirects, browser configuration changes, or pop-ups that keep repeating.
- **Registry Entries that Are Suspicious:** When the windows system is infected by malware, suspicious registry entry happens, and it is one of the main ways for the malware to make sure that it remains in the infected system.

Need for Incident Response (plan):

An incident response plan is a prepared strategy how to respond to an IT security breach. Any incident response plan aims to contain, eradicate, and recover from the attack as quickly as possible with the least amount of risk or damage.

An incident response plan is a written document that outlines the steps to be taken in an emergency. It typically covers how to identify and respond to cybersecurity incidents, what roles should be notified, and who has responsibility for different aspects of managing an incident.

What Are the Steps of Incident Response in Order?



1. Preparation

The preparation consists of two parts: external preparation and internal preparation. External preparation means setting up your perimeter firewall, ensuring that all ports are closed that are not needed for business operation, having port scanning alerts set up for all critical servers, intrusion prevention system (IPS), etc.

Internal preparation means that you should have a contact person who will respond to security alerts like suspicious activity reporting software (SARs) or IDS/IPS alerts on network devices. In this way, if any malicious traffic crosses the internal network, they can immediately tell the relevant people to respond only by knowing the source and destination.

2. Detection and Analysis

Detection and analysis are vital parts of identifying security events within any organization's networked systems through manual (e.g., reviewing logs) and automated means. In general, detection is the process of recognizing that an event has occurred. The analysis is the investigation to determine whether it's a security incident, and if so, what type.

Only after preparation can you apply detection where you set up (IDS/IPS) alerts on your network devices to help detect any unusual activity, which might indicate compromise or malware traffic.

- An example of automated detection is an intrusion detection system (IDS). This simple tool runs in the background, looking for patterns of activity that could be a sign of a security incident.
- Manual detection and review mean deploying human staff to closely monitor network activity, look out for specific events or anomalies, and investigate them further when necessary,

You should know how to decipher these alerts so that the response team can immediately act. Then you must decide what kind of action should be handled, like taking down the infected system, quarantining it, disconnecting the system, etc. These steps will depend upon discovering if unauthorized software runs on your system or whether it is a malware attack or worm infection.

3. Containment, Eradication, and Recovery

The containment and eradication process is to prevent further damage. This means blocking access to the infected machines or computers. It would be best to stop the processes on those machines that allow them to communicate with other computers on the network. If many compromised computers and servers start corresponding, more systems will be compromised, which can quickly turn into a snowball effect.

This leads to a disaster scenario where 99% of all affected machines have been compromised after only one hour. To ensure this doesn’t happen, you must stop communication from your infected hosts before they get out of control.

After an incident has been contained, we may need to take away the parts of it. You will delete malware and disable user accounts hacked and identify and fix any problems with the computers and machines.

Eradication is important. It would be best if you found out who was affected and which means are infected. It might not always be necessary, but you should do it if it’s needed.

In recovery, administrators fix computer problems. They make sure the computers work properly and if there is a problem they fix them. It can include restoring systems from backup files, rebuilding systems from scratch, replacing harmful files with good ones, installing patches, changing passwords, and making your network safer.

4. Post-Event Activity

Learning about new threats and improving your team's response is non-negotiable when it comes to securing your network and computers. You should also learn from the mistakes that you made in the past. This is why post-incident activity should involve anyone who experienced the breach.

Holding meetings where people talk about what has happened and how to make it better can help fix security issues, how it was fixed, and whether or not the solution worked. This meeting should be held within a few days of when the incident occurred.

Goals and Purpose of Incident Response:

- Detect incident quickly
- Diagnose incident accurately
- Manage incident properly
- Contain and minimize damage
- Restore affected services
- Determine root causes
- Implement improvements to prevent further causes.

Signs of a computer Incident: (suggest preventive measures)

Sr. No	Sign of computer incident	Probable Cause'/s
1	Loss of performance	Malware attack
2	Loss of bandwidth	Botnet attack
3	Exposure to other dangerous software	Malware attack
4	Loss of information	Virus attack
5	Breach of privacy	Virus attack

6	Unexpected pop-up windows	Virus attack
7	Slow operation	Bad sector, virus, defragmentation
8	Random connections to unknown websites	Malware attack
9	Inability to download antivirus software	Virus
10	Sudden lack of HDD space	Malware, virus
11	Modified or deleted files	Virus
12	Program running without your consent	
13	Your default search engine has been changed	
14	Hardware malfunction	
15	System shows error on boot	
16	Unfamiliar program running in task manager	
17	Asking for ransom amount	
18	Files turned into shortcuts	

Incident Categories (by type of incident):

What is incident classification?

Incident classification is a standardized way of organizing incidents with established categories. Incidents can include outages caused by errors in code, hardware failures, resource deficits anything that disrupts normal operations. Each new incident should fit into a category dependent on the areas of the service affected, and in a ranking of the severity of the incident. Each of these classifications should have an established response procedure associated with it.

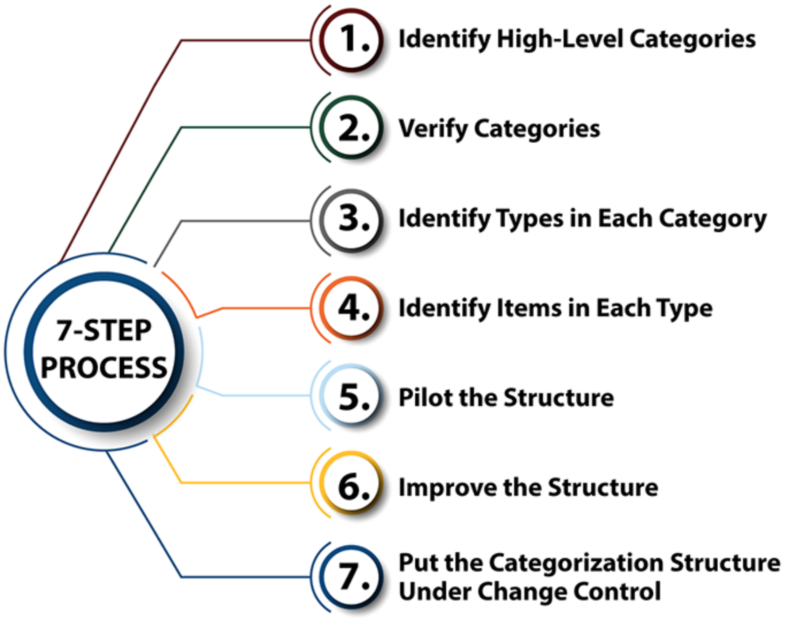
Why classify incidents?

Having a robust classification system is beneficial for many reasons:

- Improves triage by ensuring you respond to the most critical incidents first
- Determines who should be alerted and what roles they should play in resolution

- Helps with consistent responses, saving time and toil, and reducing confusion about how other people will proceed
- Measures the expected impact of incidents by type for longer term planning
- Identifies patterns in incident occurrences to prioritize preemptive fixes

Steps to categories incident:


7-STEP PROCESS
1. Identify High-Level Categories
2. Verify Categories
3. Identify Types in Each Category
4. Identify Items in Each Type
5. Pilot the Structure
6. Improve the Structure
7. Put the Categorization Structure Under Change Control

Incident Categories	**Incident Types**
Compromised Asset	Data breach or other data compromise Fraud Compromised system
External Internet	Denial of Service (DoS) or Distributed DoS (DDoS) Network probing / logical attack E-mail spamming / phishing / social engineering Threat intelligence
Malware	Malware including Trojans, worms, viruses, et al.

Equipment Loss	Loss of equipment or phone Loss of credential
Internal / Personnel	Improper e-mail usage Improper internet usage System or network misuse
Information Security Services	Other incidents not categorized above HR support for HR related issues Other services as required

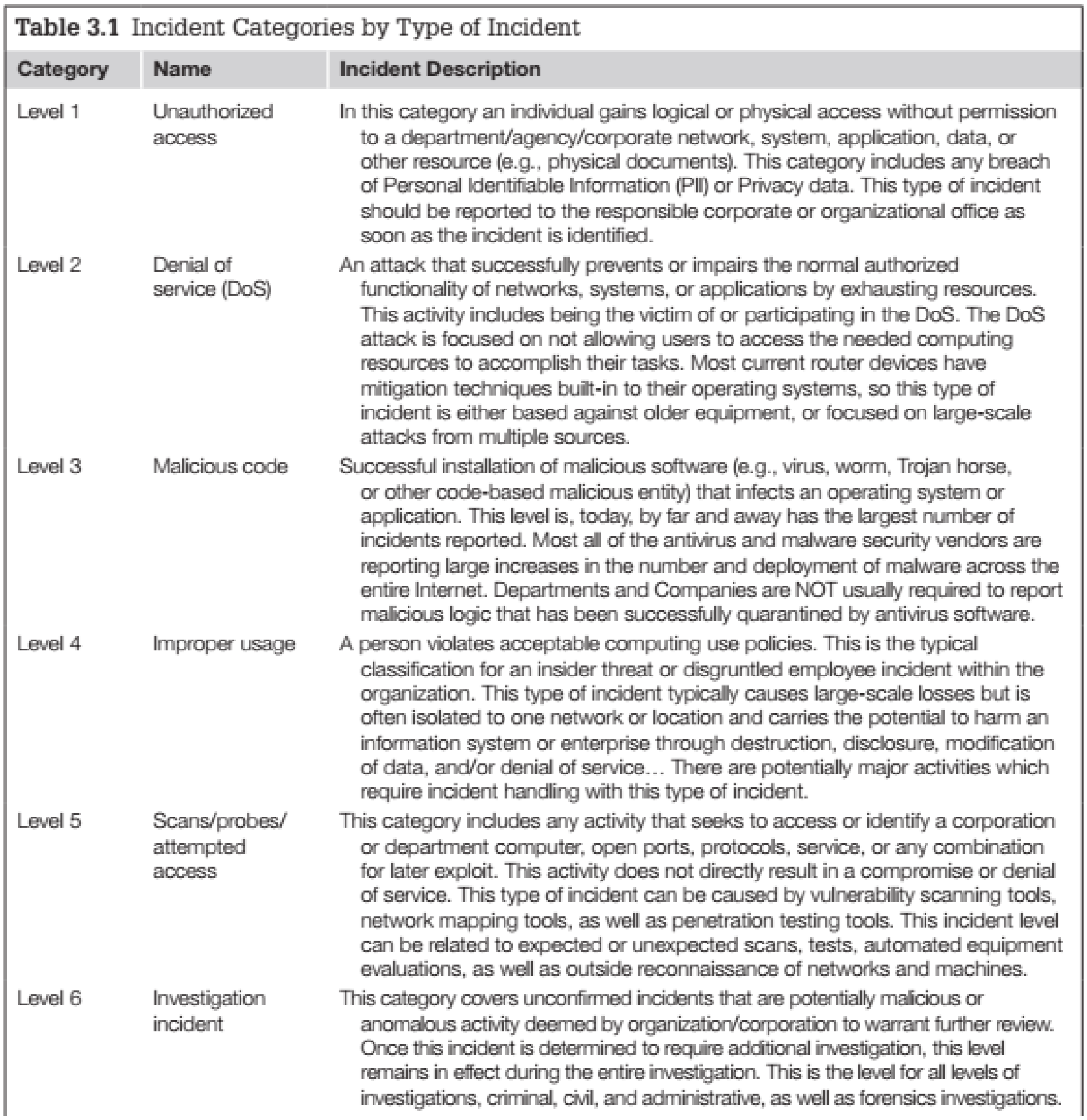


Table 3.1 Incident Categories by Type of Incident

Category	Name	Incident Description
Level 1	Unauthorized access	In this category an individual gains logical or physical access without permission to a department/agency/corporate network, system, application, data, or other resource (e.g., physical documents). This category includes any breach of Personal Identifiable Information (PII) or Privacy data. This type of incident should be reported to the responsible corporate or organizational office as soon as the incident is identified.
Level 2	Denial of service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of or participating in the DoS. The DoS attack is focused on not allowing users to access the needed computing resources to accomplish their tasks. Most current router devices have mitigation techniques built-in to their operating systems, so this type of incident is either based against older equipment, or focused on large-scale attacks from multiple sources.
Level 3	Malicious code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. This level is, today, by far and away has the largest number of incidents reported. Most all of the antivirus and malware security vendors are reporting large increases in the number and deployment of malware across the entire Internet. Departments and Companies are NOT usually required to report malicious logic that has been successfully quarantined by antivirus software.
Level 4	Improper usage	A person violates acceptable computing use policies. This is the typical classification for an insider threat or disgruntled employee incident within the organization. This type of incident typically causes large-scale losses but is often isolated to one network or location and carries the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service… There are potentially major activities which require incident handling with this type of incident.
Level 5	Scans/probes/attempted access	This category includes any activity that seeks to access or identify a corporation or department computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. This type of incident can be caused by vulnerability scanning tools, network mapping tools, as well as penetration testing tools. This incident level can be related to expected or unexpected scans, tests, automated equipment evaluations, as well as outside reconnaissance of networks and machines.
Level 6	Investigation incident	This category covers unconfirmed incidents that are potentially malicious or anomalous activity deemed by organization/corporation to warrant further review. Once this incident is determined to require additional investigation, this level remains in effect during the entire investigation. This is the level for all levels of investigations, criminal, civil, and administrative, as well as forensics investigations.