Cyber Security: A Guide for Small Businesses

Author Name

Table of Contents

1. What is Cyber Security?

Ever since the preliminary times of public usage of internet almost three decades back, protection mechanisms for information assets and the practice of cyber security have evolved enormously. Cyber-attacks are increasing in number and sophistication, while our dependence on the internet and other networks is growing simultaneously. As much as the digital world is interconnected with a chain of cloud computing, smartphones, intelligent transport systems, e-governance, e-banking, etc., it is making it impossible to avoid threats in the cyber space.

Despite the global nature of today's computer systems and networks, there is no one universally accepted definition of Cyber Security. This has led to a hampering in protection efforts at national and international level, and security incidents are treated according to the existing and often outdated national penal codes. However, the digitization of businesses has led to an increased awareness of Cyber Security and its importance in the past decade. This is why large and small businesses are now focusing on integrating their businesses with security best practices for long term profitability, customer satisfaction and security of financial and information assets.

1.1. Cyber Security Defined

According to Tech Target, a technology media company, Cyber Security is defined as:

"*Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access."*

Techopedia defines Cyber Security as the "*preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code."*

Cyber security is also often referred to as IT security. In the context of computing, the term security denotes Cyber Security. It includes all methods that prevent and protect critical information from being compromised and stolen.

1.2. Why is Cyber Security Important?

Enterprises, governments, financial institutions, hospitals, etc. gather, store and process huge amounts of confidential data on their computers and transmit critical information across their networks. The growing numbers of sophisticated cyber-attacks have made these entities realize that malware is now a readily available commodity which can allow anyone to try their hands at cyber-attacks. Companies that offer basic security solutions do little to provide a solid defense mechanism against such attacks. Security of critical personal, business, and government level information requires ongoing attention and security-focused system.

Realizing this trend, global spending on cyber security has been continually growing in the past years. In the year 2014 it was 71.1 billion (7.9 percent more than that in 2013), which rose to 75 billion in 2015 (4.7 percent increase than the previous year). By the year 2018 it is expected to reach approximately 101 billion.

1.3. Elements of Cyber Security

Security experts need to have a deep understanding of what makes up a complete Cyber Security framework. Before moving further with the threats we face in the cyber world, we need to understand what elements Cyber Security is composed of, so that security loopholes can be countered likewise.

1.3.1. Application Security

Application Security is the use of hardware, software and procedural methods to safeguard applications from external threats.

Security approach to deal with threats to applications involves knowledge of potential threats, enhanced security of the application, host or network; and implementing security in the software development lifecycle. This way, a rigorous application security routine can minimize the likelihood of unauthorized code manipulating applications to access, steal, amend or erase sensitive data.

Application security can be optimally achieved by the process of threat modelling which includes; defining organizational assets, identifying the role of each application in relation to the assets, developing security profile for every application, classifying and ranking potential threats in order of priority, recording adverse events, and documenting the actions taken in case of such events. In the context of Cyber Security, a threat is a real or potential adverse event that can result in compromising organizational assets. We shall be defining threats and their types in section _____ of the book.

1.3.2. Information Security

Information Security ensures the safety of sensitive information from being illegitimately accessed, used, revealed, disrupted, altered, read, inspected, damaged or recorded. It also ensures that no data is lost in adverse circumstances like theft, system malfunctioning or a natural disaster, etc.

Information Security is defined by three attributes, i.e. Confidentiality, Integrity and Availability.

Confidentiality – Ensures safe transmission of data through the communication channel without it being leaked to an unintended receiver.

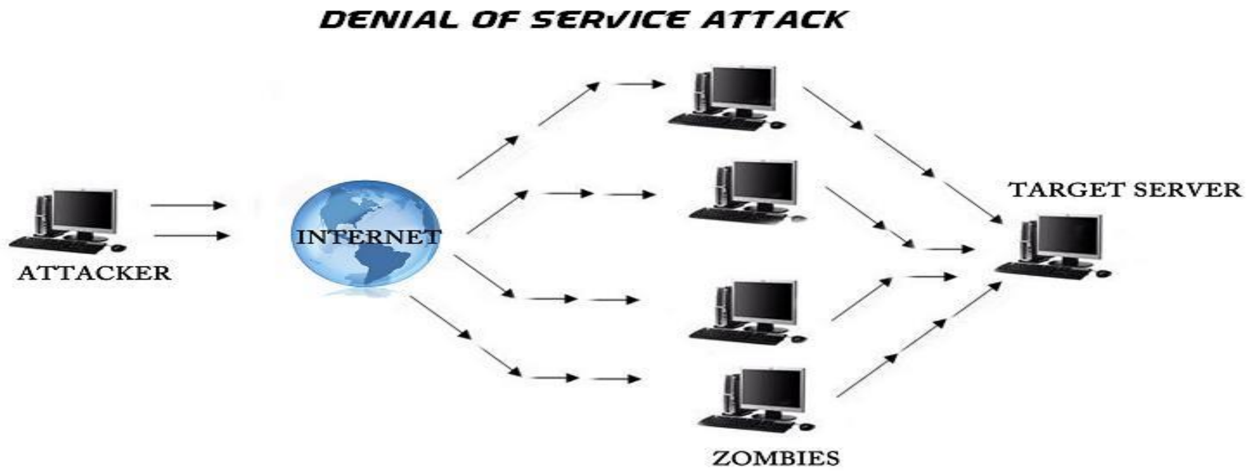
Integrity – Refers to the accuracy and reliability of classified data during the course of its lifetime. This means protecting the data from being modified during storage or transit without authorization.

Availability – This implies to the data being available to authorized parties when needed. Data needs to be classified according to the authority level and be made available to the concerned parties accordingly.

1.3.3. Network Security

It involves all-inclusive security policies and procedures adopted proactively by a network administrator, who monitors and prevents unauthorized access, misuse, denial of service attacks, etc. for computer host and other network resources. It also maintains access control by keeping a check on user activity according to the privilege granted to them.

Network security procedure begins with user authentication, which can be one (only password), two (password along with security card, dongle or mobile phone), or three-factor authentication (biometric scan along with the first two). Upon authentication, a network firewall manages the user access according to the authority and required usage. Intrusion-detection systems and antiviruses help monitor suspicious user activity along the network.

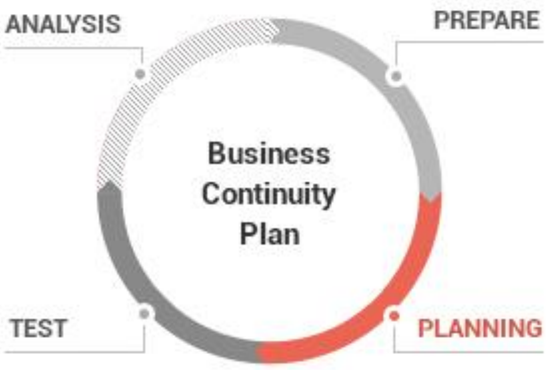


Network attacks can be passive (idle scan, wiretapping, port scanner, etc.) or active (DDoS attack, ARP poisoning, spoofing, buffer overflow, SQL injection, format string, etc.)

1.3.4. Business Continuity Planning / Disaster Recovery Planning

Business Continuity is the process of carrying out planned actions and procedures during the course of a planned or unplanned disruption in routine business operations, enabling the organization to continue with the functioning of its critical business units.

In cases where a company has already incurred loss to its information systems due to a cyber-attack, it is the business continuity plan that plays a key role in helping the business sustain and survive.



A good business continuity plan has to cover all aspects of disaster recovery. Which areas should the business prioritize for recovery? What should be the acceptable time frame within which recovery of critical information units should be started off, without bearing enough loss to the business? What would be required infrastructure and resources? These, and many other questions need to be catered for when devising a comprehensive business continuity plan.

A Business Continuity Plan or Disaster Recovery Plan should be tested at least once a year to determine the effectiveness of the plan against the desired results.

1.3.5. User Training and Awareness

Perhaps, the most important factor of Cyber Security is the human factor, which can be the weakest link in any security setup of an organization. No matter how strict the security controls, it all comes down to how information is handled by the employees and workforce of an organization. This is why it is important for organizations to adequately train their workforce in order to make critical information less vulnerable. Detailed security policies and procedures need to be conveyed and made understood by users at each level. Rather than conducting a uniform security awareness session for all employees, it is more effective to conduct custom-made trainings at each employee level and according to their job roles and responsibilities.

Regular trainings and awareness sessions are imperative to convey security flaws and system vulnerabilities and remind them of the already-known-but-forgotten security practices that are mandatory to be followed within the organization.

User awareness is also necessary to cater to the threat of social engineering, wherein cyber criminals try to seek inside information by using deceiving tactics with the employees, such as a phishing scam.

2. Why Small Businesses are at Risk?

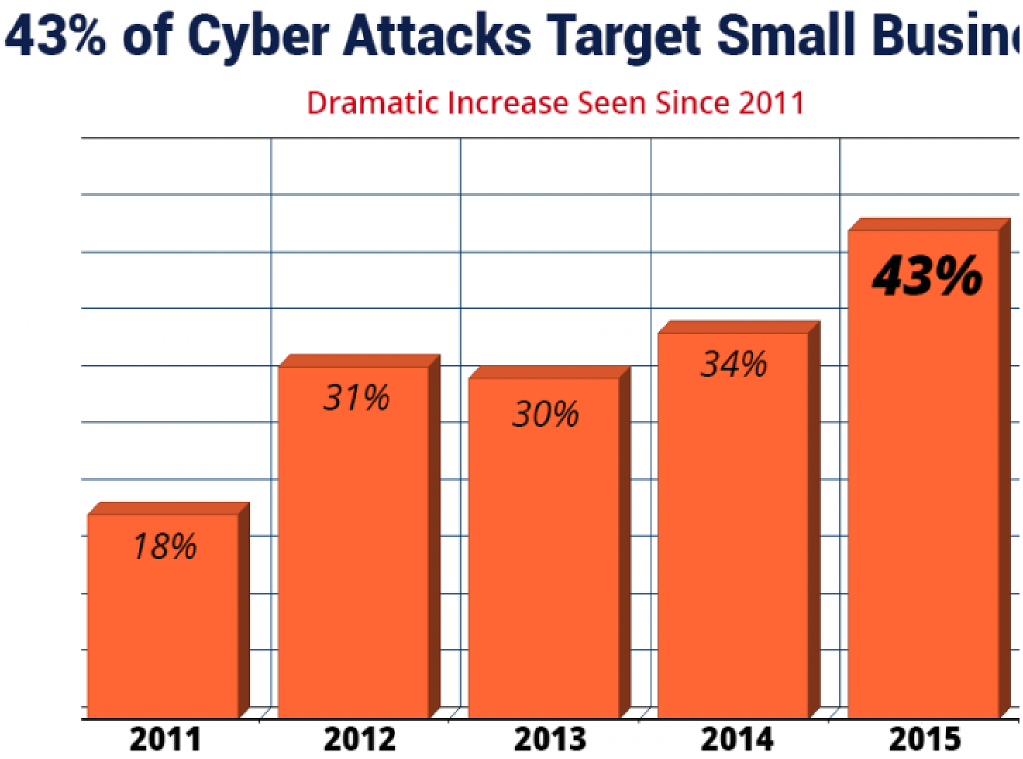
Small and medium businesses are now more at risk at the hands of cyber criminals as compared to large enterprises. This is because big corporations are now investing and implementing strict security measures as part of their compulsory fulfillment of business requirements. Small businesses on the other hand have still not realized the importance of security and potential consequences of information theft. They do not have the resources and finances to invest in a comprehensive security solution. On the attackers end, automation has made it much easier for them to attack thousands of small businesses at one time, most of which are easy and vulnerable targets. In other words, small businesses have more digital assets than an individual, and less security than a corporation; hence, they are more attractive to cyber criminals to target.

A number of security experts have cited various reasons why small business attract criminals.

- Lack the expertise and budget for providing thorough security defense
- Don’t have dedicated cyber security specialists on their payroll
- Employees lack security awareness

- Security defenses may be implemented but are not always kept up to date
- Lack of risk awareness and risk management policy and procedure
- Failure in securing endpoints

According to Internet Security Threat Report 2016 by Symantec, number of cyber-attacks targeting small business have been on the rise since 2011. Phishing attacks last year targeted small business 43 percent of the time out of total phishing attacks, which showed an increase of 9 percent from its previous year 2014.



In addition to the aforementioned reasons, cyber criminals also find small businesses as easy targets because they are now interconnected. In the past, their online presence was only limited to a website and email account. But now, their data is generated on mobile, cloud and interactions with partners and customers.

Another reason of SME's attractiveness to attackers is that they are considered as the "stepping stones" for gaining access to larger networks – the ultimate target of attackers. Small businesses that serve as vendors, business partners or contractors of large enterprises now need to interact with their internal departments such as logistics, procurement, human resources, maintenance, etc. These interactions allow small vendors to get access to the larger organization.

Realizing the risks small businesses face, regulators are now also focusing on enforcing strict security standards for SMEs. The Payment Card Industry Data Security Standard (PCI DSS), for example, has put strict requirements for contractors and third-party vendors – since these have been the weakest link in data breach incidents of large enterprises like Target.

Though it is not practical to expect small business to have the same high level of controls and monitoring as the large enterprise, but they must have basic security controls in place.

3. Understanding the Risks to Your Business

3.1. What is at Risk?

Your money and financial assets are at risk, which you may lose as a result of loss due to breach. A data breach also puts your organization's reputation at risk, which can cause you to lose your existing and potential customers. Moreover, your information is at the highest risk of being lost at the hands of criminals, and which may cause your organization to suffer long term irrecoverable losses. Information can take many forms such as customer database, list of clients, finance details of your organization, financial details of customers, your products and manufacturing processes, pricing information, etc.

IT services and information assets are at risk wherever stored, whether on your personally owned devices or third party hosts i.e. cloud.

3.2. Who can Pose a Threat?

Your current or former employees, or your clients, can pose greater threat to securing your information. They may compromise your information by accident, negligence, or deliberate malicious intention.

Cyber criminals, on the other hand, intend to harm you in all aspects. They either want to gain personal advantage by accessing your information or sell it off to another party.

If you are doing well in your business, your competitor may want to know your secrets and try to gain economic advantage over you. This is why competitors can also pose threat to your information assets. They usually try to access information with the help of expert cyber criminals or through employees.

3.3. What could be the Impact?

Impact to your business can vary in intensity, but your business will suffer in one way or the other.

- Financial loss due to information theft
- Financial loss due to disruption in business and trade, especially in online businesses
- Costs incurred on data recovery and system recovery in case of infected systems
- Cost of imposed fine in case of loss of personal data
- Costs incurred as a result of reputational damage and subsequent low customer turnover
- Damage incurred to your third party suppliers and contractors

4. Identifying Types of Cyber Threats

In almost every case, the motive behind a cyber-attack is stealing and exploiting sensitive information such as personal credentials, credit card information, or business secrets; which can be misused as the victim's online identity or used for personal gain by the attacker, such as a competitor in case of small businesses. Though individuals and businesses have found ways to prevent cyber-attacks for the most part, it by no means indicates that they are totally safe from the risks they pose.

Since adopting security measures cannot ensure total protection of a business against cyber threats, businesses need to stay vigilant towards online threats at all times. Let us examine some of the most common cyber threats that individuals and small businesses face and how they can be avoided.

4.1. Phishing Scams

A phishing scam is perhaps the most common cyber threat faced by individuals and businesses today. In a phishing scam the perpetrator tries to collect sensitive information such as usernames, passwords, credit card information, etc. through a fraudulent email which appears to be sent by trustworthy websites or reputable organizations. The email either directly asks you for your personal information or asks you to click a given link which takes you to a forged website, asking for your credentials.

4.1.1. Types of Phishing

Phishing can take many forms and each type is directed for specific gains. Here we will have a look at some of the most common types of phishing attacks.

i. **Deceptive Phishing**

This is the simplest version of phishing, wherein an attacker sends an email to users with a message and asks users to reply with their information or click on a link.

ii. **Spear Phishing**

A type of phishing attack in which the sender of the email appears to be an individual or an organization you know. It is a socially engineered email in which the attacker has already gained information of you and your peers. The contents of the email draw reference to a particular true event or thing that make it look like an authentic email. The attacker sends a personalized email to the receiver, such as from your boss or your business client, to make it look like a real message.

iii. **Spy Phishing**

It involves installing spyware or Trojan on the user's system by manipulating them to click on an infected email attachment, or installing a downloadable file from a website. Small and medium businesses are particularly prone to this threat if they do not have their software updated. This type of phishing is mostly used for gathering business and proprietary information and can be used in industrial espionage.

iv. **Keyloggers and Screenloggers**

These are variants of malware that record input from keyboard and screen display and send relevant information to the hacker by internet. These are embedded into the user's browser as utility programs and run automatically when the browser starts. They can also be found as screen monitors or device drivers in system files.

v. **Session Hijacking**

In a session hijacking attack, the attacker is already tracking the victim's activity by hacking into their system, and waits till the victim logs in to a bank account or for a credit card transaction. At that time the attacker "hijacks" the system from the user and takes control of the activity by taking unauthorized actions, such as funds transfer, etc.

vi. **System Reconfiguration Attack**

In this type of phishing attack, system settings of a user's computer are modified with malicious intentions. For example, browser bookmarks saved by the user may have their URL changed to forged lookalike website to get username or password, such as a bank URL.

vii. **Search Engine Phishing**

This type of phishing attack aims at credit card information of users. Phishers create professional ecommerce websites and index them legitimately with search engines. Users who search for specific products and services land on these websites through search engine and give up their information without even knowing the illegitimacy of the website.

4.1.2. Phishing Techniques

Whichever type of phishing attack is used, it is done through some technique. Below are some of the most common techniques that are used to carry out successful phishing attacks.

i. **Link Manipulation**

A technique by which an attacker maliciously manipulates a user to click a link that leads to a fake website. Users are now generally aware of the risks associated with clicking links in emails. This is why hackers are now using other means of manipulation such as URL shorteners, use of subdomains, hidden URLs, or misspelled URLs.

ii. **Website Forgery**

A phishing technique in which a malicious website impersonates an authentic one, thus making the users share their personal information like password or account details. Website forgery is carried out either through Cross-site Scripting or Website Spoofing.

In **Cross-Site Scripting**, also called XSS, a hacker executes malicious payload or script into a real website or web application. When a victim visits the website, the malicious script delivers to their browser. To avoid an XSS attack, it is recommended to use browsers with built-in XSS protection.

In **Website Spoofing**, the attacker creates a fake similar-looking website to a real website. A visitor who is in a hurry may not notice that the website is fake because a spoofed website looks almost the same as the real one. If you get a link to a website in an email, always hover your cursor over the link to find out its real URL and ensure that the intended page is the legitimate one.

iii. **Popups**

These messages make a very easy technique for conducting successful phishing scams. The hacker sends a popup message to the user to fill in their particulars on an online form, or to lead them to forged websites through link manipulation.

How to Prevent Phishing Attacks?

For small businesses, the risk of phishing attacks can be decreased mainly with the help of end user training and awareness. Because most phishing attacks make use of social engineering to be successful, it is very important for small businesses to regularly educate their employees about how they can fall prey to a phishing scam and give away important business secrets. Employees should know never to give any sensitive information over email without verifying the authenticity of the sender. In case information is required by a client or vendor, call them and confirm before passing on the required information.

Businesses also need to ensure that all computer systems are using approved anti-phishing tools and the browser holds anti-phishing capability. Browsers highlighting the "domain name" of a URL should preferably be used, to prevent the risk of landing on a malicious domain.

4.2. Insider Attacks

Insider attacks are hard to avoid as they can be initiated by someone who holds administrative privileges and misuses that privilege to gain access to private business data on purpose. This can be done by disgruntled employees or former employees who left the company at bad terms, but may not have had their privilege removed yet.

To **prevent** insider attacks, small businesses are recommended to record log activity and cancel all official accounts of the employees as soon as they leave the company.

4.3. Advanced Persistent Threats

APTs are long-term threats targeted to infect and steal user's data. Instead of immediate attack, it breaks into a network in a number of stages so that it cannot be detected easily.

Here we will have a brief look at the five stages of an APT attack.

i. **Reconnaissance** – the attacker gathers information from difference sources to study and understand their target
ii. **Incursion** – the attacker uses social engineering to break into the target's system and injects malware to vulnerable areas

iii. **Discovery** – the attackers keep a low profile and quietly observe the organization's defenses against threats. They then prepare a high strength attack with many kill chains to ensure its success.

iv. **Capture** – the attackers capture information from unprotected systems and install malware to acquire data in secret

v. **Exfiltration** – the attackers send the captured information for analysis to the attack center

How to Prevent APTs?

It is very important to understand the "kill chain" in order to be able to prevent or at least minimize the threat of APTs. The earlier in the chain a threat is detected, the easier it is to combat. A good understanding of the five stage of APT can help to implement required security controls at each step.

Perhaps a better way is to regularly test your network against vulnerabilities. Carrying out regular penetration tests will identify security loopholes and possible threats looming over your network.

4.4. Denial of Service Attacks

A Denial of Service attack, commonly known as DoS attack, occurs when attackers disrupt services to a network by sending large volumes of data or traffic through the network. This results in the network or website being overloaded and unable to function any longer.

DoS attacks can be carried out in different ways but the most common form of a DoS attack is a Distributed Denial of Service (DDoS) attack. This attack is launched by using a number of computers that send data or traffic to a server to overload it. Users whose computers are being used for DDoS attack may not even be aware that they are contributing to the attack.

DDoS attacks on small businesses were reported to be significantly high in the last quarter of the year 2015. A study by Akamai in the same year indicated that DDoS attacks on small businesses increase by 180% every year and attackers mostly target WordPress plugins.

A company can be under a DDoS if:

- Page-loading times are slow
- Transactions fail
- Internet service is completely disrupted
- Spam is in large volume
- Customer inputs are significantly increased as compared to routine days

How can small businesses prevent DDoS attacks?

- Install hardware and software that can counter DDoS attack attempt by analyzing the traffic
- Develop a plan for moving your website to another host in case of an attack
- Keep your IT infrastructure operation area away from the reach of customer access so that it is not affected if there is an attack.

- Keep regular backups
- Monitor your data flow to identify any threats right in the start before the problem gets worse

4.5. Password Attacks

Password Attacks can be carried out in three ways i.e. Brute-force attack, dictionary attack and keylogging.

A brute-force attack is when the hacker keeps on guessing possible passwords until they succeed and enter. In a dictionary attack the attacker tries different combinations of dictionary words with the help of a program. Both these methods are based upon guessing passwords through different techniques. In a third type of password attack, called keylogging, a hacker tracks keystrokes entered by a user and uses the information collected to break into an account.

Password Attacks can be prevented by keeping strong passwords which include upper case and lowercase letters, numbers and symbols. Also, a strong password must be of eight or more characters. It is also recommended to change passwords regularly. Dictionary words should be avoided to be kept as passwords since they make the job of password attacker easier.

4.6. Malware

Malware is a short form of “malicious software”, and refers to any program that is installed into a system with the intention of causing harm or gaining unauthorized access to the system. Many people confuse the term malware with virus, but the fact remains that virus is only a type of malware. Malware exists in many forms, the most common of which are explained below.

4.6.1. Virus

A virus makes copies of itself by spreading infection from file to file. Running a virus on a system will infect programs on it. When those files are run on another computer via email or USB port, the virus infects programs on that computer. A virus can steal passwords, display unwanted ads, or even crash a computer system.

4.6.2. Worm

A worm performs similar functions as a virus, but it is different because of the way it spreads. Worm does not need to attach itself to a file but rather replicates itself by spreading through computer networks.

4.6.3. Trojan Horse

Trojan horse, commonly known as Trojan, is another malware type that presents itself as a genuine file. Once downloaded and run, it runs in the background and lets third parties access your computer.

Trojan files can monitor your activity, join your system to a botnet or even download other malware on your computer.

4.6.4. Spyware

Spyware can be any malware that quietly spies upon your activities and collects data from your system. Different malware types can work as spyware e.g. a Trojan with spyware that monitors and records keystrokes and screen logs to gather financial data.

Some spyware programs are intended to monitor online activity and then sell it to advertising servers.

4.6.5. Adware

Adware often comes along combined with spyware. Based upon your online activity monitored by spyware, adware runs advertisements on your computer. All adware programs cannot be termed malicious. However, when an adware program displays ads as popups or appears on your screen when you are not doing any online activity, it is intended as malware. Malicious adware may also inject other web pages viewed by you with more advertisements.

4.6.6. Botnet

Botnet is a network of computers under the control of one person. Each computer is infected with specific malware and works as a "bot". A Bot is created when a computer is infected by bot software which connects it to a control server and waits for the hacker's instructions. Botnets are mostly used to launch DDoS attacks.

4.6.7. Rootkit

Rootkit digs deep into your computer system and hides itself completely from all security programs. It is capable of disappearing itself from the windows task manager. It then allows privileged user or administrative-level access to an unauthorized user.

4.6.8. Ransomware

This type of malware is a relatively new concept. It takes your files or computer into custody and demands ransom payment in exchange of getting the files back. Some ransomware can be removed with antimalware software but others like CryptoLocker encrypts your data so that you cannot access them unless you make a payment. These can be harmful if you do not have data backup.

Preventing Malware Attacks

Malware can best be prevented by:

- Installing anti-malware software with strong protection against malware and keeping it updated
- Avoiding downloading unknown attachments and clicking links sent by unknown senders.
- Deploying robust firewalls
- Turning on automatic updates of your operating system to make sure that it has up-to-date security system installed.

4.6.9. Man in the Middle (MITM)

Man in the Middle attacks are carried out by intervening an ongoing communication between two parties. It impersonates as the sender to the receiver and vice versa. For instance, in an ongoing online banking session, man in the middle will communicate with you by impersonating as the bank, and communicate with bank by impersonating itself as you. Both end users, unaware of the existence of a man in the middle, will exchange vital information which will go directly to the perpetrator.

MiTM attacks are mostly successful in case of unencrypted WiFi devices where the information transferred between two parties can be easily intercepted.

How to Prevent MiTM Attacks?

Small businesses can prevent MiTM attacks by:

- Communicating online through encrypted WiFi only that uses WPA or WPA 2 security
- Giving details of sensitive data on a website that uses a secure connection (HTTPS)
- Investing in a Virtual Private Network or VPN for increased security

4.6.10. Drive-By Downloads

These are the type of malicious programs that are automatically downloaded onto a user's system when they visit a legitimate website injected with malware. It does not require the user to click or download any link and rather downloads itself once you "drive by" an infected web page.

A drive-by download works by exploiting an app, browser, or operating system that is outdated and has a security vulnerability. Initial code downloaded on the system is a small snippet and goes unnoticed. It then gets in touch with another computer to get the remaining code on your computer or smartphone.

How to Prevent Drive-By Downloads?

Best way to avoid the risk of drive-by downloads is to avoid visiting unfamiliar websites, especially those with suspected malicious content such as file-sharing website or adult sites. Some other measures that small businesses need to implement in their systems are as below:

- Always keep your browser and operating system updated
- Use a security software that provides comprehensive protection from all potential threats. Make sure the approved software is installed on every running system of the organization
- Implement the policy of using safe search tool across the workspace. This warns the user when they visit a malicious website
- Avoid using unnecessary browser add-ons. These increase security risks

4.6.11. Malvertising

Malvertising or Malicious Advertising is the act of using online advertisements to spread malware.

Cyber criminals upload infected advertisements to various websites by using ad networks. These ads then spread to other websites that match search criteria and keywords. When a user clicks on such an ad, malware is downloaded into their system.

Malvertising can be prevented by avoiding clicking unnecessary ads and using common sense before falling prey to marketing tactics. Any ad that seems too good to be true, such a free vacations or 5 million lottery should rather not be clicked at all as it may hold malware. Updated operating system and security software are of course recommended as always for early detection.

4.6.12. Rogue Software

A very common cyber threat, rogue software is actually a malware that impersonates as a legitimate security software and promises to protect your system against security threats.

Rogue software works in the form of alerts and popup windows that advise users to immediately download their security software as their systems have been detected with threats. Some alerts ask users to update their current security software to protect against latest threats. Once the user agrees and clicks on the link, the rogue software gets downloaded on their system.

The best way to prevent rogue software is to install a security firewall and keep it up to date. Just like security software, small businesses need to implement firewalls across all their offices and employee computer systems to provide protection against such attacks.

5. Managing Risk as a Small Business

Risk management is itself a vast subject and requires thorough knowledge for better understanding. Small and medium businesses are always exposed to risks which can have a direct impact on their routine operations, increase their expenses and decline revenue. Since every business has the potential to suffer loss from risks that remain unplanned for, a risk management plan is considered successful only when it reduces the chances of all unfavorable events from taking place; or minimizing their impact in case they do take place. A comprehensive risk management can, among many others, provide the benefits of:

- Reduced chances of facing legal action
- Reduced financial loss
- Reduced loss of information theft
- Lower premiums on insurance
- Reduced business downtime

In this section we will briefly explain how small businesses can plan, implement and review their risk management strategies.

5.1. Planning your Cybersecurity

When planning cybersecurity, small businesses need to consider the following questions.

1. Which are the most valuable information assets of the business?
2. What are the potential risks the assets may be exposed to?
3. What are the legal and security compliance requirements of our business?
4. What will be our business continuity plan in case of adverse circumstances?
5. How can our business manage ongoing risks?

Keeping the aforementioned questions in mind, a cybersecurity risk management planning cater to the following:

- Calculate the probability of your business being a target of an attack. Study your suppliers, distributors, clients and competitors to discover the risk level your business may be exposed to
- Find out your merchant level and consider complying with security standards such as Payment Card Industry – Data Security Standard, ISO 27001, etc.
- Identify your business's critical information and financial assets and your IT services. Evaluate risk exposure of all your IT equipment. This can include information such as what data is stored on your assets, who can access them, how is data transferred, etc.
- Assess your password policy and check to see if it provides the required protection against your online services and equipment.
- Create a mechanism to assess the knowledge of your employees regarding safe information security practices and conduct regular security awareness trainings to develop a vigilant mindset in the workspace.
- Make a decision to implement required security controls for your business. This can be done best by taking help from security consultants.
- Develop a business continuity/disaster recovery plan to consider your plan of action in case of disruption in business due to undesirable circumstances

5.2. Implementing your Cybersecurity

Now that planning has been done, it is time to implement what was planned. But before implementing, small businesses need to ask themselves

1. Do we have the right security controls in place for protecting our information and financial assets, equipment and IT services?
2. Have we trained the staff to know about their responsibilities? Are they aware of security best practices?

Whether you have hired services of a security consultant or third-party managed IT services, always check your service level agreement and contract to make sure all security controls are in place.

- Install anti-malware solution on all systems and keep your operating system and web browsers updated. Make a policy of how and when to install security updates
- Use firewalls, access lists and proxies to protect your wired and wireless networks
- Develop secure configuration of your business IT equipment and change default passwords. Also maintain an inventory list of your equipment
- Develop an Access Management Policy to define privileged access and restricted access roles. Restrict access of defined roles to sensitive information, IT equipment and systems. Ensure the physical safety of your assets to avoid unauthorized access.
- Other that computer systems in office premises, ensure that employees transferring official information through their mobile devices or home laptops encrypt it before undergoing the transfer.
- Restrict usage of removable storage devices at your offices such as Flash disks, CDs, DVDs, external hard disk, etc. Protect and encrypt data on such devices
- Monitor activity logs and validate your proficiency to detect unauthorized malicious activities

5.3. Reviewing your Cybersecurity

A successful cyber security risk management procedure ensures that the steps planned out and implemented are effective in achieving desired goals. When reviewing whether your implemented security controls are operational and bringing aimed results, small businesses should consider the following questions.

1. Do you regularly review and test the effectiveness of your security controls?
2. Are you up to date with the latest threats?
3. Based upon the answers received in the first question, are you taking the required mitigation steps to monitor the security controls?

To review security and to respond to security flaws, small businesses can take help from the following tips:

- Test and monitor security controls regularly to identify change in risk levels and adjust the controls accordingly
- Do not keep software or obsolete equipment that is no longer in need. Before discarding, ensure that it has all the confidential business data removed
- Monitor user access and manage creation and deletion of accounts when a new employee joins or and old one leaves respectively
- In case of disruption in business, identify the cause and ensure its removal. E.g. a malware threat must be removed immediately when causing disturbance in business activities.

6. Cybersecurity Solutions

Apart from manual security procedures and best practices that small businesses need to adopt, the IT market also provides ready-made security software and solutions to businesses to help them achieve maximum protection. Let us look at these in detail.

6.1. Encryption Software

An encryption software helps protect sensitive information such as financial statement, client records, etc., from being stolen and read by encrypting the data file. This way, a perpetrator cannot recover original data during communication between two parties, or when the file is simply stored in a system.

Some useful and well known encryption software solutions are Folder Lock, Cypherix Secure IT, CertainSafe, Kruptos 2, etc.

6.2. Data Leakage Prevention

Data Leakage or Data loss prevention software solutions are used to detect and prevent the leakage of data during transmission or while at rest. Whether a small business deals with payment information of customers, intellectual property, Personal Health Information, etc., the data it holds needs serious protection from leakage as it can not only contribute to financial loss but also cause reputational damage. Data nowadays is on the move frequently, and new technologies like virtual data centers and cloud computing have made it difficult to trace the exact location of data. Hence, deploying data leakage prevention software is necessary for enterprises to protect their data and avoid unnecessary penalties from regulators.

According to Search Security, some of the best DLP solutions of 2016 are Intel Security by McAfee, TrueDLP by Code Green Networks, RSA DLP Suite by EMC, Symantec, etc.

6.3. Firewalls and Antivirus

A firewall is an enterprise's first line of defense against threats. Small businesses cannot afford to operate without a firewall as it lays the key foundation of network security. The purpose of a firewall is to inspect all traffic passing in and out of your network to make sure it's legitimate. A well configured firewall will allow authentic users to access your network resources and keep away malicious users or programs. Some of the best firewalls for small businesses are FireEye, McAfee Next Generation, FortiGate Platform, Juniper XRS, etc.

Just like firewall, antivirus is a mandatory requirement for ensuring data protection and computer system safety. Some of the reliable antivirus software solutions are Bitdefender, Kaspersky, Avast, AVG, Norton, BullGuard, Panda, ESET, F-Secure, and G Data.

6.4. Data Backup Solutions

Data Backup software creates a duplicate copy of data at some other location and later enables recovery in case the file gets lost, corrupted or infected with malware. Data can also be lost due to a natural disaster, human error, power outage, or any other adverse event.

For small and medium businesses, it is advised to maintain regular backup on a separate location. Though operating systems generally come with the capability to backup data without requiring any specialized backup software, data backup software with its inbuilt expertise can make this task much easier.

Data backup software for enterprises saves resources and time and makes the admin's job much easier. Enterprise backup solutions often come with centralized management, automatic backup scheduling, providing reports and monitoring. Some solutions also secure confidential data with encryption in addition to providing backup.

Some recommended data backup software packages for small businesses are Acronis True Image, StorageCraft ShadowProtect, Paragon Backup and Recovery, Genie Timeline Home and NTI Backup Now.

6.5. Two-Factor Authentication / Password Security Software

Two-Factor Authentication, also known as TFA or 2FA is an extra security layer that makes password cracking difficult by requiring two times verification before a user can log into an account. In addition to username and password, a user is made to verify their identity a second time with someone only that particular user is capable of providing. This can be a security code, a piece of information only the user knows, or a physical token.

With passwords prone to social engineering exploits and threats such as brute force, rainbow table and dictionary attacks, 2FA considerably helps to reduce the success of phishing scams, identity thefts, and all other forms of online fraud.

Some well-known offerings for 2FA and multi-factor solutions are RSA SecureID, Microsoft Phonefactor, Dell Defender and Google Authenticator.

7. Best Cybersecurity Practices for Small Businesses

Below we shall be explaining some fundamental best practices that can help small businesses in keeping their information secure and achieving overall cyber security in the business setup.

7.1. Passwords

Passwords have an important role in day to day business operations, especially internet usage and online transactions. Every computer system in an office premises needs to be password protected, email communication needs password protection, online financial transactions are also protected by passwords, etc. Hence, it is a good practice for small businesses to develop and follow a password policy and circulate it to all employees to aware them about what makes a good and strong password. The combinations that made strong password five years ago may not contribute to password strength the same way now as hackers have become more sophisticated with their password cracking techniques.

A good password must

- Be of at least 16 characters wherever allowed
- Must include at least one Uppercase and one lowercase letter, numbers and special characters such as!@#$%^
- Should not be based upon dictionary words; real words are much easier to crack
- Should not be based upon personal data such as date of births, name, roll number, etc.

Follow the Password Regime

- Never use the same password for all your accounts. Use different passwords with a little variation.
- Change your password as often as you can
- Do not allow any website to "remember" your password
- Do not save your passwords on any file on your personal computer
- If you want to write a password somewhere for remembrance, lock it in a drawer or encrypt the file if it is on a computer
- Never share your password with anyone

The more a password is a combination of jumbled up words, the harder it is to guess. With all the rules of a good password in mind, it might be harder to make a password that cannot be forgotten easily. Let us see some tips to make a number of "difficult to guess" passwords while still managing to remember all of them. You may consider keeping same letters or numbers for all your passwords while changing a few characters only, those also in a pattern only you can understand or guess such as the last 3 letters of the website you are using. You may also use a dictionary word that is easy to remember or holds relevance for you, but use only some of its letters in a pattern such as alternate letters, first 4 or last 4 letters, etc. This way you will end up with a password that will only be remembered by you as you will know the pattern on which the password was built.

7.2. Avoiding Phishing Scams

Phishing scams are everywhere, on emails, social media and even fake websites. It is hard to not come across them at one point or the other. These scams can, however, be avoided if employees are aware of the characteristics common to all online scams.

- **They pass a threat at you.** Any threat in an email or message indicates its inauthenticity. For example, "If you don't click you will hear bad news in 48 hours".
- **They have spelling or grammatical mistakes.** A legitimate and professional company sending out an email to mass audience will always proofread and edit its email for

mistakes before sending. An email with mistakes will indicate that it is not authentic and most probably sent by an individual who does not speak English as a native language.

- **They ask you to click on a Link.** Phishing scams are also used to spread malware in your system and collect your information. This is done by sending you an infected link and asking you in manipulative ways to click on it. Always hover your cursor over the link to check the actual URL where it is taking you to. Be suspicious of links that come with unsolicited or unexpected emails or messages. Many a times, a link can also take you to a spoofed website, which is a fake copy of a legitimate website. For example a fake website of your bank may ask you for your login credentials. Sometimes, only visiting a spoofed website can infect your system without you doing anything else. To avoid falling victim to this, pick up some key words from the link and google them. See if the website is fake or real. But never click directly on the link given.

To confirm the legitimacy of an email, get valid contact information from google or official website and call on their given numbers. Ask them if they have sent the email. In case a scammer is calling you, ask them their name and specific details. If they refuse to give the details or get confused, hang up.

It is a good practice by small businesses to develop Email policy for its employees to follow.

7.3. Employee Information Security Awareness Trainings

A large number of security breach incidents happen not because of outsiders, but because of lack of knowledge and carelessness on part of your own employees. To rectify this, it is vital to educate and train your new and old employees time and again about how they can protect their business's information assets.

Below we will focus on some key aspects of information security that must be made a part of your trainings. These are applicable to all employees that use computer systems, smartphones and mobile devices, or any other form of equipment.

- **Authentication:** Employees need to know what components constitute a strong password and how they are not supposed to ever tell their password to anyone. Even if one employee's laptop or mobile device is stolen, an attacker can enter your enterprise's entire network through it – if he knows the password or is able to crack it. For services like file sharing and email, all employees must use two-factor authentication to add an extra layer or security for authentication.
- **Network Connections:** Wireless connections such as Bluetooth and unsecured Wireless LAN have proved to be highly unsafe as they are very easy for attackers to infiltrate into. Protect office and home wireless networks with WPA2 encryption and complex password for router. A better practice would be to use a Virtual Private Network for all official communication.
- **Access Management:** An employee needs to be trained to never allow access to their system to another employee. Sometimes an employee may want to give their device to

kids or someone else for other purpose such as playing games, etc. In such a case, they must make a separate account that does not have administrator privileges.

- **Physical Security:** Physical security of your devices is as much important as network security. Mobile devices should never be left unattended anywhere and data on tangible sources such as paper must be shredded off after it is no longer required to perform job duties.
- **Data Encryption:** Even if employees are very careful otherwise, their device can get lost or stolen. That is where encryption is very important as it encodes sensitive data to make it unreadable to a third party.
- **Data Backup:** Train your employees to keep a backup of all important data. Once they lose data because of a security breach, loss or theft, and there is no hope of recovery, backed up data can save from a lot of trouble. A backup system such as cloud service is a good way to keep your data available at all times.
- **Software:** As an operational business that is conscious about security, you must provide a list of allowed software programs to your employees. Inform your employees that they must never install free or unapproved software programs from the internet, as they may be infected with malicious code. Even approved software needs security patches soon after they are released.
- **Basic Security Regime:** Employees also need to follow a security regime to adopt security practices in their routine such as installing anti-malware software, firewall, avoiding phishing scams, etc.

7.4. Network Security

Small business can have a variety of access controls across the network. Whether large or small, a network must have some basic security configured onto the system.

Let us look at some basic network security controls that must be implemented by all small businesses.

- **Disable Remote Admin Access to the Network** – Limiting admin rights to internal network stops attackers from accessing and attacking the network. Do not enable remote access to a network unless otherwise required
- **Deploy Alternate Domain Name Server Provider** – the ISP provided DNS normally do not provide increased security features like blacklisting or blocking of infected websites. To enhance your web security, use commercial or open-source DNS providers.
- **Protect your Wireless Network with WPA2** –Wired Equivalent Privacy (WEP) was used in older access points. Encryption done with this algorithm can be decrypted easily by a hacker who can also trace the entire traffic across a wireless network. Older devices may need hardware or software upgrade to support WiFi Protected Access 2. , use WiFi Protected Access 2

- **Apply Strong Passwords to Network Devices** – Strong passwords have already been explained before. Not only does the access point require strong password, it is also a basic security need to put password on all devices that are managed with a web interface, such as network printers.
- **Disable Universal Plug N Play (UPNP)** – By default, all network devices and wireless access points come have UPNP enabled. UPNP is used for automating connection with the network device. Once connection is complete, it is a good practice to turn it off so that no outsider can access the wireless network devices.
- **Dedicate separate subnetwork to critical devices** – all devices that handle confidential information should be separated out on a separate subnetwork to reduce the risk of security breach.
- **Enable MAC Address Filtering –** This will allow only authorized MAC or hardware address systems to access a wireless network.
- **Disable SSID Broadcasting** – this will hide the name of your wireless network from the wireless medium and prevents detection of the network. All client computer systems need to manually set up and access the network.

7.5. Secure Browsing

Most of the cyber-attacks take place through web browsers when a malicious site is visited by a user.

- **Choose the Best Browser for Yourself** – Small businesses must therefore consider it very important to choose the right browser. By far Google Chrome is the best option for secure browsing because of its quick response to fixing discovered vulnerabilities. It also uses sandboxing for every opened tab, thus making it difficult for hackers to exploit a vulnerability.
- **Never browse as an Administrator** – Always log in as a limited user as going online with administrator privileges makes the hacker's job much easier to control your system.
- **Use NotScript or NoScript –** Scripts are used by some websites for giving a better experience to the website visitor. However, malicious websites may have malicious scripts which aim to exploit vulnerabilities in your system. NotScripts and NoScript are Chrome and Firefox extensions respectively that stop scripts from running by default when you visit a website. It is up to the user to allow the scripts of selected websites to run.
- **Beware of Link Manipulation and Phishing Scams** – Phishing scams aim to direct a user to a malicious website by manipulating them with social engineering and other techniques to click on a link received in email. It is important to train all employees to refrain from clicking uninvited links and thoroughly ensure that the link they are about to click is safe. It is a good practice to hover cursor over a link and check the actual URL

where the link is directed. Some of the techniques used by scammers to manipulate users to malicious websites are URL cloaking, use of subdomains and URL shortners.

7.6. Securing Workstations and Servers

Workstations and servers form the basis of a small business's operational activities. Securing these devices properly is of integral importance as they store customer and financial records, transactional records and all other sorts of confidential information. For improved security of workstations and servers, below are some suggestions.

- Update your server to the latest operating system and 64-bit hardware platform. This will help overcome many of the security loopholes of the previous operating systems and 64 bit platform will help avoiding 16 bit and 32 bit malware from executing
- Always turn on automatic updates
- Install a complete host-based security software suite which provides the features of antivirus, secure browsing, phishing scam detection, Host based Intrusion Prevention System, firewall, etc.
- Limit administrator privileges to authorized accounts only
- Use PDF reader that supports sandboxing as it protects the system from being infected with a PDF file containing malicious code
- Use a browser that supports sandboxing
- Keep all your application software programs updated
- Always keep Autoplay or Auto run turned off on all mediums to prevent malicious software from running automatically
    - For Mac OS Laptops, File Vault should be implemented to encrypt user data in case of device loss or theft

7.7. Securing Mobile Devices

Keeping your mobile devices safe at workplace and out of work premises plays an equally important role in the security of small enterprises.

Below are some suggestions that must be adhered to in order to keep your mobile devices secure and protect business data from being compromised. These must also be made a part of employee security training sessions to remind them of using safe practices when handling mobile devices.

- When travelling, never connect your device to open hotspots. Instead, a better option is to utilize mobile Wi-Fi service provided by cellular networks, use a Virtual Private Network (VPN) or as a last resort use open hotspot with limited activity that does not involve entering personal information
- Enable full disk encryption if a mobile device is to be left unattended
- Always keep your mobile operating system up to date. New updates come with security fixes along with new features
- Keep Wireless and Bluetooth disabled when device is not in use

- Download mobile apps from Google Play for Android and App Store for iOS devices. Do not download from untrusted sources. Even when downloading from trusted sources, check the application reviews before proceeding to download
- Install trusted Antivirus mobile software as it acts as an added security layer. Encrypt your sensitive data with Data Encryption option available in both Android and iOS mobile devices
- Use an Encrypted Email Service, such as ProtonMail to send and receive emails securely.
- Backup all your important mobile data on a remote storage to prevent yourself from losing information in case of loss or theft of a device. Avoid storing sensitive information on the mobile device itself for longer periods of time and erase it from the device after backing up at a remote storage and when it is no longer needed on the device

7.8. Risk Management and Disaster Recovery Planning

Until now we have talked about preventative measures that can help us avoid incidents of security breach. However, it is a fact that no matter how strict the measures, there is always a possibility that a security incident actually takes place. It is therefore, very important to develop recovery plan in case an actual cyber-attack takes place. Risk management is an integral part of cyber security planning and having a disaster recovery plan in place can help minimize the losses.

Below are some important factors to keep in mind when developing a risk management and disaster recovery plan.

- To avoid complete loss of data in case of a natural disaster, theft or cyber-attack, always store critical business information such as customer records and financial information on a backup solution.
- Act fast and do not wait until it is too late to recover. Time means everything and every single minute counts. Small businesses must proactively identify key resources and data critical to business operations.
- Keep your employees well trained for bad times. Regular security awareness trainings play a key role in this regard. Small businesses, with their limited human resources, must train all employees how to follow best practices in the event of a disaster.
- Test your recovery plan regularly to assess weak areas. Make sure everything is in place according to the plan.
- Be prepared for the bad time, at all times.
  - Identify important functions that must need to go on under all situations
  - Organize these vital functions in the order of priority
  - Develop resource requirements
  - Identify activities required to support the functions
  - Create a plan for performing other functions if the situation allows
- And the most important of all, develop comprehensive Risk Management and Business Continuity Plans in accordance with ISO 31000 and ISO 22301 respectively.

7.9. Incident Response

Incident Response is a systematic approach to managing the consequences of a security breach (also called an incident). It is an integral part of information security management system of a business and aims to minimize the losses with quick planned response to an incident.

But it is more than just handling a simple security breach initiated by an outsider. It corresponds to all incidents that range from systems being infected with virus to major loss or theft of data caused at the hands of a malicious user. According to a survey by Nationwide in 2015, eight in 10 small and medium businesses i.e. 79% of SMEs do not have incident response plan to prepare themselves for adverse circumstances. The reason is that most of them believe their data to be useless for external parties or they believe that they are too small a business to be noticed by the outside world.

Let us look at how small businesses can stay prepared for incident response.

- **Preparation:** Keeping yourself well prepared is the first and foremost step to minimize downtime when an incident occurs and avoid hasty decisions made in panic. Conventionally, preparing for an incident response includes thorough work and understanding of developing incident response plan which includes team selection, communication strategy, emergency action plan, required software packages, etc.
- **Identification:** Now that the Incident Response Plan is in place, it can be used in times of actual occurrence of an incident. The incident team gathers and analyzes data and concludes if an incident has taken place.
- **Containment:** In this step, the Incident Response Team (IRT) aims to prevent further loss or damage by containing or confining the damage that has already incurred. Immediate actions taken would be changing DNS information or disconnecting power cables. After stopping the damage from spreading, a backup copy for analysis of the system has to be made.
- **Eradication:** In this step, the IRT has to actually eradicate all entities that participated in the incident such as malicious code, and also remove the loopholes that resulted in the security breach in the first place. After determining the cause, system is rebuilt from an earlier good backup or by reinstalling from scratch.
- **Recovery:** In this phase, system is fully recovered and ready for normal operations after passing through all the security checks.
- **Lessons Learned:** In this final stage of incident response, the incident is evaluated to avoid the same from happening in future. A report is developed which answers all questions related to the incident such as, what caused the incident. How the incident was carried out? Have all necessary steps been taken to prevent future attacks?