Cyber Security: Disaster Recovery Plan

**Introduction**

Cyber security attack is a kind of attack where companies are being attacked by black hat hackers who have malicious intentions, which mostly have a devastating negative impact on companies. The key focus of these hackers encompass stealing data, blackmailing, or knowing the financial status of companies (Miranda 2018).

**Type of cyber-attack that companies face**

They are two types of cyber security attacks that a company can face; internal attack or external attack. Internal attack, this is a kind of attack where companies are being attacked by their own employees. In this kind of attack, the attackers have a reason as to why they are attacking the company this may include; seeking revenge, spying for another company, and many more. External attack this is a kind of attack that is being facilitated by people from outside the company. In this kind of attack, this attacker have also some reasons to attack; this may include: to know the financial status of the company being attacked, blackmailing, stealing of data from companies.

**Type of Malware that can be used to Attack a given Company**

Malicious software is a kind of program or files that are made to corrupt other computers' data and how it functions. This kind of malware can be in various forms, including worms, viruses, trojans, and other computer harmful programs. If an organization falls under tack of this malware program, the organization should take these measures to recover from the disaster and prevent a future attack. For example, if a trojans virus attacks the organization, the organization should consider the following recovery plan from the attack (Agrafiotis, Nurse, Goldsmith, M., Creese, & Upton, 2018). Trojans' virus is a kind of virus coded with the drive to know someone or an organization's financial statistics and captivating over the system possessions. Some of the ways recovering from the attack include;

**Measures on how to Recover from External Attacks**

First, the organization should determine what was lost when the attack happened. It will help the company know which kind of information was stolen from them, and also, it will assist them in understanding the second step they will take to recover from the attack. For instant, think of those police spider diagrams they use to investigate a certain crime. A company should also form a spider diagram by starting with what was stolen and then relate the acquaintances. Then, it will help the company determine the next step to follow down to where the attackers got a chance to hack the company systems. The second way the company should consider a recovery plan from a cyber-attack is to replace the old technology with the new technology. The company should also add tools to form a more complex defensive way to prevent future attacks by malicious viruses or hackers.

The company should also consider the following step from recovering from an attack; the company should stop at nothing from finding which virus, worm, or Trojan viruses were used to attack and damage the company data. This step will help the company to determine the degree to take to recover from the attack. Also, it will help the people involved in the physical recovery of the company systems to which kind of defensive ways to use to recover the data and prevent future attacks.

The company should also consider investing in proper software. These is because it is very hard for the employees in the company not to make mistakes, which may lead from the attack; good software will help in detecting any attack that is about to occur, or that has already happened this by it will give a warning to the company before the damage spread to become a complex issue (Watkins, 2014).

Another way the company will consider in recovery plan from a cybersecurity attack is to consider the following steps; the company should make back up their data and files in an external device. It will help the company to have a simple way of restoring the stolen data or the data that has been damaged from the attack. Also, it will help the company to get their sensitive file and document to a safer place to prevent future episodes.

Another way a company should consider when faced with a cybersecurity attack is keeping the virus from spreading this is by disconnecting all the company systems from the internet; this help in securing the company information and data because if the attack is external, the hacker will use the internet to break in the company systems. So, when the system is being disconnected, no threat can further attack the company.

A secure password is another recovery measure from a cybersecurity attack. Passwords help the company to secure customer data and information from attacks from hackers. This password must be a complex password that will not be easy for a hacker to access and compromise the company data and files. The company should also use the last pass as a way of securing the internal password. Another method for a company to recover from a cybersecurity attack includes the following. If the company has lost data and files, the company should consider the following ways to recover from the given problem.

The company must make sure that the company system is up to date. It will help the company prevent future attacks because the software will detect the threat and block it from accessing the company systems if it is up to date. Also, updating the system does not give any hacker room to penetrate the system because the system will not have any weakness.

The company should also ensure endpoint protection. For example, making sure the laptop and phone and other devices that use internet connection are connected to a secure network within the organization to prevent any attack from the link. The company should also install a firewall in its system. The firewall will prevent and lump any instinctual aggression made to your system or before the virus damages your system. The company should also control the access to its system this because nowadays cybersecurity attack can happen physically. For example, a person can access data using a USB cable, which might lead him or her to steal sensitive data of a company, leading to company downfall.

The company should also block the employee from downloading some of the applications or accessing some data because it may lead to the company being faced with a cybersecurity attack or installing some viruses that might distort the data and file from the company. The company should also consider an insurance plan as a kind of recovery plan from the attack of their system. This insurance policy will cater for the IT Infrastructure in the company. Also, it will help the company benefit from working with professional in regards to cyber-attacks on the company and seek outside advice regarding the security breach.

The company should also create contact. This contact is by knowing who to call if there is an attack. It will help the company gather support, and it will have confidence when opera rating in global technology. The company should also employ staff who are well trained and who can act in case of the attack and those who know, ensuring that the company system is not in harm of any cybersecurity attack. The company should also train its employees to see when the system is affected by any attack. It includes teaching them behaviors the attacked system displays; this may include; hanging when doing some work, loss of data in the computer, the system can also switch off, the system can open application which the user did not open, the system can lock itself, and the system can crush itself.

The company should also purchase more advanced antiviruses, which will prevent the system from future attacks by malware. This kind of antiviruses includes the following. Kaspersky, AVG Antivirus, panda security, Avast, widow defender, Bull guard internet security, Norton 360, comodo internet security, F- secure Antivirus, and Webroot anywhere Antivirus among many others which are found in the market. This kind of Antiviruses helps to detect any foreign application or a virus trying to penetrate the system. It also warns when you interact with some bad sites containing viruses that can affect the company system or when an employee is downloading some document or application from a harmful site.

The company should also put in place policies to ensure the workers are proactively working to protect the company data and files. The company should also screen new workers to verify they are not there to still the company's data or affect the company systems with some malware that can erase data or enable them to change some of the company data. The company also should consider the following measures as a recovery plan. First, the company should perform a cybersecurity valuation; this assessment will help the company know the cybersecurity risks that the company may face and the way to avoid them, and areas that need to be upgraded. The company should also write a cyber incident plan. The plan will help the ICT staff know how to handle any attack that may arise because this will have led to how to solve some issues. The company should also review the storage and identify the weak point where the hacker could penetrate the company system. Then after knowing the weak point areas, rectify the weakness and monitor the procedure to prevent the future attack. The company should also consider the following for the recovery process from attack in the future.

The company should generate a robust internal control. This robust control will help the company avoid attack because it enables the system to update once the workers have left the workplace. Hence it will reduce the cybersecurity attack on the company systems. The company should also consider third-party security. It will help any person accessing the company system be aware of risks and ensure high security. In addition, this will help the company to know the risks and the threats to their system; hence it stays secured.

The company should also consider restricting the network admin rights. The company should limit the network admin right to some limit to avoid a network breach. The company should entrust trustworthy workers with these confident rights and passwords and a highly trained person. The company should also consider discouraging password sharing among the workers in the company. This could lead to a system breach of the company, so the company workers should always be encouraged to keep the passwords of their located secret from any foreign member who is not a worker of the company. The company may also consider educating the workers on the dangers of using an unsecured network because it may allow hackers to penetrate the system. It should also teach them how to know if the network they are using is secure or not secure. It will help them to avoid using networks that are venerable to being hacked by hackers.

**Measures to Recover from an Internal Attack**

In other cases, if the attack was internal, the company should consider these measures to recover from the attack and prevent future attacks. These measures include the following; the company should first document policies and always pressure workers to follow the guidelines. Then, if the workers follow the laid down procedures, it may prevent any future attack. Another measure company can take to recover from the attack is to make sure it screens and tale any unusual behavior starting with the employment procedure. It comprises dealing with the most abused policy blasphemy, increasing and affecting private and specialized stress signals.

The company should also uphold this measure as a recovery plan from internal attacks. It should forestall and handle negative workplace issues: the company should work from pre-employment to termination in case of violation of any policy by any worker. The workers should be fortified to debate office problems deprived of any anxiety of being ended because many attacks happen after the end of a worker. The company should trail and protect the carnal atmosphere: The access to fleshly and computer-generated areas should be limited to those who need it. Any bid of heresy should be checked. The company should also implement parting of obligations and small freedoms. The sleeper workers should ensure that the work is shared across workers so when there is an attack, the command is given to each worker to access what they are needed to take out (Agrafiotis, Nurse, Goldsmith, Creese, & Upton, 2018).

Some of the internal attacks occur during the system repairs. Therefore, the company should limit the admission to gridlock systems because a hacker can pretend to be a repair person. Still, she or he compromises the system by planting some viruses or stealing some data from the company. The company should use additional attentiveness with system managers to use their mechanical familiarity to take vengeance for professed wrongs. Some policies like the parting of labor can use the decree of two-person decree for the serious system manager. The company should also gadget system modification control because unlawful change is vital for an insider to compromise, so the company management should strappingly modify switch apparatuses and alarms. The company should also keep an eye on and do some inspections on the worker's online activities. It will help the company to spot apprehensive commotion such as the copying of private documents. This mechanism will benefit the company to know any imminent threat and be ready to act. The company should also consider using the incrusted protection to counter distant occurrence; the workers are more poised when they are not inspected by colleagues, so counterattack entree to labor- built appliance except peripheral entree is needed which situation display watches closely.

The company should also ensure that they have applied safe backup and repossession procedures: Safeguard backup and repossession measures are in place, solitary ideas of catastrophe are eradicated, the trial procedure frequently, etc. The company must also come up with an external occurrence rejoinder strategy. A rejoinder is needed to rheostat the impairment. Would an occurrence happen it is very wise that robust suggestion is correctly assembled and not tainted and that teachings are cultured? The company should also use sandboxing as a recovery plan: Sandbox is a sanctuary device for keeping apart consecutively apparatuses of a given system. It was designated in 1996, but it is used more largely nowadays. It is good to say that some of the application has this sandboxing, for example, HTML5 is secondhand with iframes. The function of this sandbox is to perform untrusted programs that come from campus turf, or even proved, bases. It gives avoidance of operation, reverse -engineering, and reprogramming of scheme and mechanisms and is typically a morally program-founded shield. The sandbox is like a virtual machine, which has been set to rival a whole host processor, on which a predictable operating system may wader and lane as real hardware. In other events, the combination of more than one sandbox can replace numerous parts of a scheme embattled by innumerable threats. This kind of program can help the company recover from disasters and prevent future attacks from happening in the company.

Other measures that a company can take recover from a disaster include the following: the company faced by the disaster should chase and sue the culprits: doing this may help stop cybersecurity attacks because those who carry out the attacks will have to do it because they know when they will be caught will be jailed. It also might change the mind of those who do it also because they will be brought before justice. They may serve a long sentence in jail of about 30 to 40 years in prison with heavy punishment, reducing the companies' rate of cybersecurity attacks. The company should also develop the best security practices: These practices will help the company create policies that may lead to zero disasters. Also, this rule should cover all the aspects of any crime in the field of cybersecurity. Also, the company can adapt to the international regulations laid down by the nation to fight cybersecurity threats.

The company should also deploy vital security applications: this kind of application includes antiviruses, strong passwords, firewalls, and intrusion detection systems. It will help the company recover from future disasters because the company will be provided utmost protection. The company may also encourage research and development: this will help the company know how to protect their data and file from future attacks. Also, it will help the company to come up with new development to fight against cybersecurity breaches in the company (Watkins, 2014). The company should also develop a system with protection; for example, it can develop software for their system with a virus that will affect the computer of that hacker trying to penetrate inside the system (Watkins, 2014). It will protect the company data and file this because no threat can enter into the system. The company should discourage the workers from inserting hard drives inside the system, this because they may contain viruses or application which will affect the machine. This can make the company systems be affected by viruses that may distort data. In addition, they may open a door for hackers to hack the company's sensitive information.

The company should also try to make their software rather than buy the software because you never know who can hack the company. For instance, when they buy the software for their company, this software may contain malware that can affect the company system, making them lose data to hackers. The company should also employ some staffs who are well trained to deal with any threat that may emerge in the company.

**Recommendations**

After doing my research about how a company can recover from a disaster, I would like to recommend the following things that the company should consider when recovering from the disaster. First, I would like to recommend the company to be doing some investigation when hiring a worker to know if the worker is they to offer his or her services or he or she is there to compromise the company data and system. I would also like to acclaim that the company moves from the old technology to the new technology because this new technology has a more advanced tool to deal with any disaster inside the company. I would also like to acclaim that the company creates strong passwords for its system because when the company continues using some simple passwords, it will lead to another disaster.

I would also like to acclaim that the company offers education about the effect of cyber-attacks on its workers and show them how to know a system is being hacked. This will help them know of any threat, and also, they will be careful when downloading some of the files on the internet. I would also like to acclaim the company management to put in place a group of employees who have the skills to deal with any threat that the company may face. I would also like to acclaim that the company lay down policies that will help the company not fall into another disaster. I would also like to acclaim that the company considers having an insurance policy that will protect the IT system. I would also like to recommend the company consider the third-party relationship in the system to assist them in knowing the threats they are about to face (Arlitsch, & Edelman, 2014).

I would also like to recommend the company to upgrade their systems by putting in place software like Antivirus, a firewall that can assist in any other disaster. I would also like to recommend the company put some limitations on those who interact with the company systems. This limitation will help the company to avoid a future attack. I would also like to acclaim that the company supervises what workers do on the internet. The supervision will help the company to know if they are any employee who is planning something bad against the company. I would also like to recommend that the company take action against those caught going against the company policies. I would also like to recommend that the company encourage its workers to share any problem they face in the company. It will help the company to know how to deal with any disaster which may arise. I would also like to recommend that the company workers report anything that is not okay from the company system. It will help the company management to look at the problem and know how to solve the problem. I would also like to recommend the company make a copy of the backup because they can retrieve their data and important files in case of an attack (Luckey, 2009).

I would also like to recommend that the company employ qualified staff to assist in dealing with a disaster that emerges. I would also like to recommend the company to be scanning their system from time to time so that they can avoid any attack that may occur. I would also like to recommend that the company use robust software because it will help keep the system safe from any attack. I would also recommend the company encourage development and research to stay one mile ahead of hackers and protect their systems from being attacked. I would also recommend the company to keep on repairing their system from time to time because it will make the hacker lack a weakness and a place to penetrate inside the system. I would also recommend that the company keep in touch with people who can assist when the company systems are attacked. I would also like to recommend the company should also write a cybersecurity incidence plan that will help the workers to be able to know what to do in case of an attack of the system. I would also like to recommend the company to make sure they do an investigation and find who did it and sue him or her to the court to act as an example to others who think of doing the same thing. I would also like to recommend the company to investigate the damage that the attack has caused and identify what was stolen from them. This investigation will help them to move to the next step of discovering where the hacker got a chance to penetrate the company systems.

I would also like to recommend that the company restrict their workers from accessing some sites that may threaten the company. The restriction will help the company avoid future attacks. I would also like to recommend that the company formulate the best policy to protect the company resources from being hacked by hackers. I want to encourage the company to promote their workers not to disclose passwords to anybody. It will also lessen the probability of the company being attacked by any threat. Lastly, I would like to recommend that the company always look for the best way to avoid these attacks. The company management should invest in making the system better and eradicate this problem of being attacked.

**Conclusion**

In conclusion of the above-discussed point on how to recover from a disaster that has affected the company, we agree that if we can use those measures, the problem of being attacked by hackers and viruses would not happen at all.