Computer Incident Response Team Plan

Name

Institution

Introduction

In the current modern world, communications infrastructure has converged with information technology (IT) to create a cyberspace that is being used in almost every part of the world. There are more activities that are conducted using computers and thus the importance of the Computer Incident Response Team (CIRT) in the IT programs. An incident response program is a complex task and hence proper planning and resources have to be availed to ensure a successful program.

**1**. **Objectives and elements of a CIRT Plan**

A CIRT has the responsibility of providing a company with an incident management experience. The entity has to be part of the company. It acts as the starting point of a response that is in charge of coordination and support. It is cheaper to prevent the cyber-attacks than responding to them after they have occurred (Maxwell, Anton & Swire, 2012). Thus the CIRT plan must have prevention measures that must include high-security control measures to reduce the probability of incidents. Sufficient security measures reduce pressure on the CIRT plan whenever there is attack and the CIRT will only focus on recovery and mitigation measures (Gibson, 2010).

Thus, the purpose of a CIRT plan is to aid a company to get ready for any computer incident that can occur. The plan does this by creating a plan with the organization to think of any potential problems that could occur and offer possible solutions to the problems. It receives, reviews and responds to any computer incident reports. The company has to avail adequate resources to the incident response to warrant the security of the networks, applications, and systems (Borodkin, 2001). A CIRT plan helps in complementing the security channels available in the organization as it ensures that the department in charge of incident recovery has all the resources that they will need. The resources include adequate training of the IT staff and creating awareness to the security policies that are available. These simple security resources will help in preventing a number of security threats (Borodkin, 2001).

Similarly, a CIRT plan is created to help in minimizing the impacts of a computer incidence. The impacts can be on the partners of the organization, customers or the normal operations of the organization. It helps in ensuring that in the case of an attack, the response is immediate and that takes minimal time and resources. A CIRT also helps in determining the motive of an attack, what caused it and how to prevent future attacks. This helps in updating the risk management procedures for future attacks.

Finally, another objective of the CIRT plan is to assess the financial loss that has resulted from the computer incident. The financial loss will be in terms of the cost of liabilities and fines to be paid. Losses can also result from disruption of business operations. Finally, there is a financial cost to put the system back to normal.

There are a number of CIRT elements that should be contained in a CIRT plan. However, the elements depend on the organization’s objectives, plans, and goals. The basic features of a CIRT plan are the members, policies and responsibilities and incidence policy strategy. The CIRT members have the rules that govern each member. An important person in this element is the security analyst (Maxwell, Anton & Swire, 2012). A security analyst has expertise in cyber-security and can help in proving ways of containing and incidence. Another member should be the IT staff who understands the technology infrastructure of the company. The CIRT policies contain the guidelines to be followed in case of an incident. Similarly, each individual’s responsibility after an occurrence is clearly stated in this element. The final element of responsibilities and incidence policy strategy has the rules and procedures that are to be followed during an incident occurrence. After every incidence, this element is often modified to cater for new incidents.

**2**. **How the CIRT supports risk management plans**

A clear and knowledgeable understanding of the incidences of an attack helps a company to handle the anticipated threats. Thus, the CIRT plan will help a company in understanding and planning for the incidents. A knowledge of any of the incidences likely to occur will put the team in an enhanced position in effectively and efficiently dealing with the problems. The topmost level management has to be involved in the risk analysis to ensure an effective CIRT plan. This is because the top management can make decisions without further consultation with other staff that helps in reducing the incidence report time (Maxwell, Anton & Swire, 2012). The management of the CIRT team must actively help others in understanding all the procedures and processes involved in creating, upholding and executing the CIRT plan. However, the work of the management is to support and participate in the plan’s development and execution. It is only when the management is committed to implementing the CIRT plan that the other employees will be motivated to inform the team of any incident that might occur.

**3.** The main function of a CIRT plan is to prepare the management for incidents by providing a framework on how to handle the situation when it occurs. Thus, the rules and rights have to be provided for an effective response. The steps to be followed are outlined and it answers the question of who, what, when, where, and why of the response. “Who” indicates the people who will be responsible for various activities when the incident happens. “What” indicates the type of incident that has occurred while “when” identifies when the company will be effective after the incidence. “Where” determines the part of the organization that the incident will affect and finally “why” determines the reason for the attack (Rajnovic, 2010).

An example would be when ex-workers from one of the companies decides to send scam emails to the users of the same company. In the email, the users would be informed of some lottery won that they have to pay a service fee to get the lottery. In such an event, the conditions would be to open a new account and give out personal information to get the lottery. The fraudster would then use this information to get money from the users will at the same time getting the users’ personal information. In this scenario, the “who” is the company’s ex-workers and users. “What” is a fraud attack targeting the company’s workers while the “why” is getting money fraudulently from the workers as they pay for the service fee and surrendering their bank account details through the false accounts. Where is the financial account of the users in terms of their bank's accounts. This shows that the CIRT had not considered such a threat or otherwise the company’s workers would not have entered such a trap. An analysis would have helped in detecting the scam and finding mitigation measures.

The second example is the team viewer. Team Viewer is a software used globally by large companies and they use it a remote control. This is a system that allows its users to send log files to a support center in a different location for data analysis. The users then provide information collected from the organization. Team viewer has already been exposed to a number of incidences such as unauthorized access, service interruptions, and reduced privacy. It has information that can be used by a hacker to gain authorized access to any involved company. The data is stored on the server and the data can be obtained by sending an application to the server. The log file contains the answer to what, when, where and what are consequences of what happened. There is a continuous analysis that is done on the software to determine any new incidences that are likely to occur.

**4. How a CIRT Plan helps management in developing a more proactive approach**

Cyber-security was not an important aspect in many companies. However, this is changing as many attacks are taking place. Companies who do not have any risk management plan are vulnerable to failure. Thus, currently, no company wants to be the target of cyber-attacks. Building a successful CIRT plan requires a number of components. It is dependent on the expertise, resources, and timeframes.

Currently, it is important to have a proactive approach when risk management is involved. As much as it is difficult to eliminate all the computer incidents, an effective CIRT plan will help in reducing the impacts of these incidents. Identifying a risk before it attacks, helps the company to develop a coping mechanism as they build a defense against the identified threats. Thus a number of recommendations should be considered.

Continual improvement of a CIRT plan requires an input of all the stakeholders. The stakeholders must comprehensively understand the CIRT plan and know what they are to expect from the plan. The vision of the plan will have to be communicated to everybody to ensure that everybody participates in the awareness program.

Similarly, it is important to create a cyber-risk governance. The governance structure of any organization is important in developing any successful risk management plan. This involves determining the individuals who will be part of the response team. Equally, it involves developing the structure of the report with guidelines for operating the process (Maxwell, Anton & Swire, 2012).

Thirdly a CIRT plan should be adaptable to create boundaries. Any cyber vulnerability should extend to any location that stores data and can be accessed by staff. This vulnerability is then communicated to the customers and trusted stakeholders. This will help improve the communication channel for report such computer incidents.

**5.** **How IT threats have evolved over the past decade**.

Threats have been evolving over the last decade. These threats are being created and sent to people and organizations. The motive of these threats is to gain a competitive advantage. However, others are just sent for personal gains. Thus, hackers are advancing their skills and looking for new technologies to gain access. As much as companies are also finding new updates and improving their systems to cater for these challenges, hackers also are working to improve their skills and gain access.

Cyber-security has become a nightmare for many organizations as may believe that it, not a matter of “if” but a matter of “when”. The threats that are currently affecting cooperate networks are SQL injections, login attacks, cross-site scripting and registration spamming. Thus, a CIRT plan is important in helping a company in prioritizing on cyber threats and being prepared for the outcomes (Maxwell, Anton & Swire, 2012).

Advancement in technology has enhanced information gathering. This information can be used by companies to improve their cyber-security. Each company has to conduct training and create awareness for its users to always alert the company whenever there is a security threat. Similarly, the company should also give the users easy reporting mechanisms that could help it handle any breaches that occur before it causes serious damages.

Likewise, it is important for every company to ensure that the IT department certification is up-to-date. There should be continuous training to help workers update their skills. Thus, this will enable users to detect any security threats. They will also be able to correct minor issues (Gibson, 2010).

The changes in technology and cyber-security advancement require companies to have a flexible compliance program that can be adjusted to effectively manage the current threats. The modifications in the compliance program enable the organization to manage its infrastructure to help curb new threats while ensuring business continuity. Some notable regulatory changes include changing from 3G to 4G wireless technology. Their improved internet speeds reduce the time it takes to transfer information. Similarly, there is the advancement from Internet protocol version 4 to version 6 that has changed how companies handle requests online (Rajnovic, 2010).

**6. Regulatory requirements that mandate risk management processes and plans.**

There number of threats and attacks have improved over the decades. Thus, the regulatory requirements needs to advance as well. The regulatory requirements involved in risk management will have to be intense. The overall objective of the plan is to identify all the potential risks and create a response plan through the recommendations given. The recommendations will always be changing to cater for new cyber-security risk. Companies will need to adhere to the new regulations that will be put in place. Thus, is the risk management plan needs to be flexible to respond to any new updates and changes.

The U.S. Federal Sentencing Guidelines for Organizations mandates compliance to risk management. The mandate has evolved in that any company not complying with these rules faces certain fines and penalties. The risk compliance is to ensure that every company has a risk management plan. The current world is that of regulatory convergence and it is becoming more complex. Thus, new regulatory requirements do emerge every day to cater for the increased risks.

Risk management is a continuous process and that is why the companies will need to be flexible enough to change and update the process regulations. This will help many of them prevent most of the computer incidences. New attack methods require new programs, equipment, plans and process to help in fighting and mitigating the attacks (Rajnovic, 2010).

**Conclusion**

Every business has risks and each company must have a risk management plan. However, it is critical to select the right way of managing these risks. This ensures that the response team can successfully control the situation that has occurred. There are a number of ways to control incidences that can affect a company. One method is using the CIRT plan and requires the involvement of the management team to ensure its successful implementation. The elements of a CIRT plan are often aligned to the company’s policies. Thus, with sufficient training and planning, the plan can be used mitigate computer incidents. It helps the organization in responding quickly to an incident and ensure business continuity.

References

Borodkin, M. (2001). Computer Incident Response Team. SANS Institute InfoSec Reading Room: Swansea, UK.

Gibson, D. (2010). Managing Risk in Information Systems. Jones & Bartlett Learning: Burlington, Massachusetts.

Maxwell1, J. C., Anton, A. I. & Swire, P. (2012).Managing Changing Compliance Requirements by Predicting Regulatory Evolution: An Adaptability Framework. *IEEE*.

Rajnovic, D. (2010). Computer Incident Response and Product Security. Pearson Education: London, UK.