International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org
Vol. 8 Issue 1, January-2018,
ISSN (O): 2249-3905, ISSN(P): 2349-6525 | Impact Factor: 7.196 |

ANALYSIS ON CYBER SECURITY IN INFORMATION TECHNOLOGY ORGANIZATIONS

Jeevan Prasad Adhikari[1], Dr. Arvind Kumar Sharma[2]

Department of Computer Science and Engineering

[1,2]OPJS University, Churu (Rajasthan) - India

ABSTRACT

Cyber-attacks can significantly hurt an organization's IT environment, leading to serious operational disruptions, from simply damaging the first layers of IT security up to identity theft, data leakage and breaking down networks. Moreover, the dangers through which current cybercrimes practices affect organizations present a tendency of developing more rapidly that decision makers can assess them and find countermeasures. Because cyber threats are somewhat new thus a critical source of risks, within the context of the constantly changing IT environments (e.g. cloud services integration) organizations may not effectively implement and manage cyber threat risk assessment processes. This paper highlights the importance of designing effective security strategies and proactively addressing cybercrime issues as key elements within the organizational risk management approaches.

1. INTRODUCTION

The Information Technology, as we probably are aware it today, vastly affects putting away information on each possible subject important to humanity which has changed the communication system as an entirety. Advances in information technology and telecommunication networks have drastically expanded the measure of information and data that can be put away, recovered, accessed and ordered quickly. In a real sense, the headways in Information Technology have been exceptionally unequivocal; however, in the meantime, these have negative and decimating impact likewise covering an extensive variety of issues of social concern. In Indian point of view Information Technology' related difficulties is never again a deception however it demonstrates the forthcoming impact of the Information Communication Technology as the new outskirts of developments in criminal activities covering the global viewpoint through the network of the worldwide web (www) andother complex and enhanced techniques for technology [1].

Malware rises constantly in impact and complexity and has surpassed the traditional security model. One of the main ideas of the study is to present the main areas of risks related to cyber security to which an organization is subject to and provide a baseline of an analysis model that would adequately evaluate input data,

rank priorities and represent the results and solutions to decrease these risks. Since Cyber security is a major test in current Indian point of view, subsequently we require a decent, lawful framework in the zone of cyber law, cyber security to ensure e-transactions and the basic interests of overall population on the loose. In the present Indian lawful setting, the Information Technology Act, 2000 is a piece make enactment that is frail on the fronts of Cyber security and different zones of cyber criminality and therefore influencing the privacy privileges of Indian subjects and different components of e-administration. The advancements in communication technology and other route patterns of improvement in Information Technology have gone into making the captivating developments.

2. TRENDS AND SECURITY CHALLENGES

Subsequently, business data, organizational assets are progressively debilitated, and conventional IT security approaches are putting forth just the premise of arrangements. As a general characteristic, the present IT condition can be considered as reactive, with no time designated for risks evaluations; cybercriminals know about every one of these exposures and exploit them using end users (social building, robbery of accreditations), phishing attacks, through a wide range of unique double dealings, entrance and encryption methods to make their follow inaccessible [2]. As said beforehand, security occasions are constantly expanding, in recurrence and additionally in impact. Be that as it may, in a similar time quantitative information identified with these occasions are both hard to get and additionally difficult to put into a significant framework. On a general level, organizations should change from a for the most part security based way to deal with a more risk evaluation approach, consequently tending to vulnerabilities inside the risk management planning and techniques.

2.1 Workings of cyber crimes

Cybercrime has turned into a calling and the demography of the cybercriminal is changing quickly with the kind of composed criminals who are all the more customarily connected with drug-trafficking, coercion and tax evasion. The subject of how to get credit card/bank account data can be replied by a choice of strategies each including their own relative combinations of risk, cost and expertise. The plausible commercial centre for this transaction is a concealed IRC (Internet Relay Chat) talk room. Picking up control of a bank account is progressively refined through phishing. The majority of the accompanying phishing apparatuses can be gained inexpensively. The cyber criminals works in the accompanying ways:

2.2 Coders

They are the similar veterans of the hacking community. With a couple of years' involvement with the craftsmanship and a rundown of set up contacts, 'coders' deliver prepared to-utilize devices

(Trojans, mailers, custom bots) or services, (for example, making a twofold code imperceptible to AV motors) to the cybercrime work drive – the 'children'. Coders can influence a couple of hundred dollars for each criminal activity they to take part in [3].

2.3 Kids

It is called so on account of their youthful age, most are under 18. They purchase, exchange and exchange the basic building pieces of successful cyber-tricks, for example, spam records, PHP mailers, intermediaries, credit card numbers, hacked has, trick pages and so forth. 'Children' will make under $100 a month, to a great extent on account of the recurrence of being 'ripped off' by each other.

2.4 Drops

These individuals change over the 'virtual cash' acquired in Cybercrime into real cash. Generally situated in nations with remiss e-crime laws (Bolivia, Indonesia and Malaysia are currently exceptionally well known), they speak to 'safe' locations for goods purchased with stolen monetary points of interest to be sent, or else 'safe' legitimate bank accounts for cash to be exchanged illegally, and paid out of legitimately [4].

2.5 Mobs

These are professionally operating criminal organization which combines all of the above covered functions. Organized crime makes particularly good use of safe 'drops', as well as recruiting accomplished 'coders' onto their payrolls.

Privacy and security of the data will dependably be top security measures that any organization takes mind. We are directly experiencing a daily reality such that all the information is kept up in a digital or a cyber-shape. Social networking sites give a space where users feel sheltered as they interact with loved ones. On account of home users, cyber-criminals would keep on targeting social media sites to take individual data.

2.6 Web servers

The threat of attacks on web applications to extract data or to convey pernicious code continues. Cyber criminals disperse their malignant code by means of legitimate web servers they've traded off. In any case, data-taking attacks, a significant number of which get the consideration of media, are additionally a major threat.

2.7 APT's and targeted attacks

APT (Advanced Persistent Threat) is a whole new level of cybercrime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must

improve our security techniques in order to prevent more threats coming in the future.

2.8 Mobile networks

Today we can associate with anybody in any piece of the world. In any case, for these portable networks security is a major concern. Nowadays' firewalls and other security measures are getting to be permeable as individuals are utilizing devices, for example, tablets, telephones, PC's and so forth all of which again require additional securities separated from those present in the applications utilized [5].

3. CYBER-THREAT RISK ASSESSMENT PROCESS

Unless an organization is considerably developed related to cyber threat risk management practices, it cannot have the risk assessment infrastructure and governance elements designed to sustain an adequate security environment. For example, if the basic elements are not defined, such as specific risk definitions and business impact analysis, risk limits of acceptance or specific key performance indicators. If an enterprise cannot sustain at least the above mentioned elements, it is advisable as a starting point the evaluation of the following set of information security practices that significant for an appropriate cyber risk assessment process:

1. Existing security controls, implemented by the entity to identify and record known types of cyber-attacks that are characterized by stealth breaches.
2. Available methods of recording security breaches information from multiple sources (internal as well as external).
3. Exposure of employees to complex social engineering attacks that allows malware to be integrated in the administrative consoles or workstations..

3.1 Organizational process

Organizational business units are characterized by divided procedures, which are not continually conveying between them, certain manual information and execution of operational activities. Characterized forms must line up with big business-wide risk management framework previously mentioned and should be checked by IT workforce and official management at various levels; forms must achieve the level of being reliably integrated, robotized, and obviously archived identified with cyber threats risk appraisals. Organizations should formally gauge and screen process viability; mechanization must be seen as a target; cyber threat risk management might be sorted out at a larger amount as a self-standing unit and through which all procedures are tended to by constant change endeavors; the general goal is to achieve organized cyber threat risk management programs that are integrated with the effectively existing IT risk

management and undertaking risk management plans [6].

4. SECURITY TOOLS AND TECHNIQUES

Technology as of now introduced for security reasons must be empowered to log security occasions, to concentrate them and as a premise must send cautions if there should be an occurrence of episodes recorded or special cases; signature-based controls, for example, against infection and intrusion-detection software must be actualized. For an advanced organizational condition, legal devices might be utilized for reacting to excellent security occasions. Commercially accessible threat checking sustains might be integrated with brought together logging arrangements and observing software to generate mechanized cautions. For more mind-boggling risk management existing security apparatuses might be naturally empowered to perform propelled connections identified with threat information and to change over acquired data into actionable alarms. These strategies connected might be utilized to robotize not simply threat checking and cautions, but rather assist security occasions recognized, for example, malware, or finish measurable examination, and also more intricate threat appraisals. The displayed framework of persistently advancing cyber threat risk management capability model may maintain an organization during the time spent executing better security systems to dodge cyber-attacks of criminals that make it past the effectively existing access controls instruments. For instance, an all-around created cyber threat risk management model will incorporate wellbeing components against unapproved information conveyance, and also protection contradicted to unapproved information access [7]. The compelling finish of these highlights prompts the utilization of technologies and procedures that screen outbound information activity for both substance and destination specifically. This can be designed as an alarm point if data is being exchanged to an area outside of the typical operational condition, where the organization has not been available previously.

5. ROLE OF SOCIAL MEDIA IN CYBER SECURITY AND TECHNIQUES

As we turn out to be more social in an undeniably associated world, organizations must discover better approaches to secure individual information. Social media assumes a colossal part in cyber security and will contribute a great deal too individual cyber threats. Social media appropriation among staff is soaring as is the threat of attack. Since social media or social networking sites are relatively utilized by a large portion of them consistently it has turned into an immense stage for the cyber criminals for hacking private information and taking profitable data. In this present reality where we're brisk to surrender our own information, organizations need to guarantee they're similarly as speedy in recognizing threats,

reacting in real time, and keeping away from a rupture of any sort. Since individuals are effortlessly attracted by these social media the programmers utilize them as a trap to get the information and the data they require. Thus individuals must take proper measures particularly in managing social media keeping in mind the end goal to keep the loss of their information.

6. PROACTIVE CYBER SECURITY: CONCEPTS, IMPLEMENTATION, AND LEGALITY

Both the concepts and the language of "active protection" and "proactive cyber security" are established in military customs. For example, antiquated as well as contemporary Chinese military commanders have upheld the concepts in their most battle ready frame, and the U.S. military likewise received an active resistance teaching during the late twentieth century. As in other fighting areas, cyberspace offers militaries chances to take part in proactive protection. For instance, proactive protection might be operationalized through dynamic strategies, similar to technologies that detonate upon contact with antitank rockets, or through electronic measures, for example, sticking an enemy's radar. In any case, an audit of the military's utilization of active cyber barrier measures and the troublesome issues identified with deciding when such measures may legitimately be utilized are past the extent of this Article.

Or maybe, here we center around the utilization of active cyber safeguard measures by businesses since this term has "saturated the private sector." This area initially discuss about the development of proactive cyber security as sought after by private sector organizations and individuals in the ahead of schedule to mid-2000s. Since unadulterated protection has dependably been trying in the realm of cyber security, a few substances started to investigate the utility of more proactive actions during this period, yet mechanical, economic, and legitimate obstacles implied that such cases were generally phenomenal or possibly extraordinarily publicized [8].

7. SURVEY OF THE PROACTIVE CYBER SECURITY INDUSTRY

To pick up comprehension of industry standards that might arise, this segment audits the aftereffects of a study of private sector proactive Cyber security practices. We made Figure 3.5 with publicly accessible data drawn from twenty-seven arrangements offered by twenty-two organizations that advance Cyber security items, services, or research. The most boundless practices crosswise over studied organizations are on the left half of the outline, while practices on the correct side are less normal. The stacked section speaks to those organizations that positively express that they offer the appropriate cyber security item or service and is trailed by, if pertinent, an extra segment (in red), which demonstrates the number of firms that imaginable offer that item or service based on elucidations of

information accessible on site promoting and item depiction materials. We don't contend that these discoveries speak to authoritative industry practice or the positive ID of industry standards, developing or something else. There are hundreds, if not thousands, of firms offering cyber security arrangements overall such a large number of that some have even addressed whether a cyber-security bubble is fermenting.

8. NETWORK SECURITY

Secure has its etymological roots in without or separated from, and cure to administer to or be worried about. It may be he said a computer system is secure if it is protected from threats, which now a day is doable just if it lives in disengagement. That is the reason it is said that a genuinely secure computer is one that isn't connected to a network or any power. In such a case the quantities of endeavours are limited, i.e., existing shrouded shortcomings that can hit the system are decreased.The security in computer networks is a quickly developing area of concern. The greater part of the important information lives on the network, making network an inescapable substance for survival. There is a multiplication of the networks in the day to day lives, he a scholastic or business condition. These little networks are associated further to wide area networks which like this shapes the premise of the Internet. The Internet is the 'world's biggest accumulation of networks that achieves colleges, government labs, commercial endeavors, and army bases in numerous nations". In spite of the fact that the Internet associates bigger network, for example, those having a place with huge communication organizations [10].

9. CONCLUSION

Substances are in charge of executing and keeping up an integrated approach between its representatives, operational process, and technology resources actualized with a specific end goal to finish effective risk management techniques. Resources must be apportioned to accumulate and process cyber threat investigation information, telling the results and defining cautions for better security controls and measures to be taken by the operational units. Complex cyber risk management forms are repeatable, plainly defined, very much reported, and lined up with organizations bigger IT risk management. Future work will center upon cyber intelligence accumulation strategies and processing calculations, behavioral patterns of cyber attackers, which could oblige altered upgrades to the risk management activity of an organization. As the research of cyber security capacities changing from crude data to actionable intelligence will give valuable cyber threat research. Consequently, such an examination would bolster upgrades in different key threat pointers and measurements identified with IT security investigation. Any cyber-attack can hurt an organization in any number of routes, running from minor harms to a website useful page to closing down center

networks, conferring misrepresentation, and taking intellectual property.

REFERENCES

[1] Gregg Schudel, Bradley Wood, ModelingBehavior of the Cyber-Terrorist, in http : //www.dli.gov.in/data/HACKING _INF ORMAT ION/P RINT ED20P AP ERS /Modeling20Behavior20of20cyber 20terrorist.pdf.

[2] Tim Shimeall, Phil Williams, Models of Information Security Trend Analysis, in http : //www.dli.gov.in/data/HACKING _INF ORMAT ION/P RINT ED20P AP ERS/ models20for20inf20security20T REND20ANALY SIS.pdf.

[3] SushilJajodia, Peng Liu, VipinSwarup, Cliff Wang, Editors, Cyber situational awareness: Issues and Research, in Springer International Series on ADVANCES IN INFORMATION SECURITY.

[4] Maginot Revisited: More Real-World Results from Real-World Tests, FIREEYE (2015), https://www2.fireeye.com/rs/firey e/images/rpt-maginot-revisited.pdf [hereinafter Maginot Revisited (2015)]

[5] Carl F.,(2003), "Intrusion Detection and Prevention", McGraw-Hill, Osborne Media.

[6] . Antivirus - how-antivirus-software-works , http://www.howtogeek.com /125650/ htg-explains-how-antivirus-software-works.

[7] Counteract edge for threat prevention www.forescout.com/product /counteractedge, Accessed date Jan 2012

[8] MithcellRowton,(2005), "Introduction to Network Security Intrusion Detection" , December 2005.

[9] Heberlein L., Dias G., Levitt K., Mukherjiee B., Wood J., and Wolber D.,(1990), "A Network Security Monitor" , Proc., IEEE Symposium on Research in Security and Privacy, Oakland, CA, pp.196-304.

[10] T. Lappas and K. P. ,(2007), "Data Mining Techniques for (Network) Intrusion Detection System" , 2007.