ASA

Risk Consultants

Research Note

Building Resiliency in the IT Sector

By: Rashmi Shekhar

Keywords: Critical Infrastructure, DHS, Resilience, Cyber Attacks, Cyber Threats, Risk Mitigation

Abstract – This research note identifies some of the key cyber risks that pose a threat to the functioning of Information Technology in the public and private sectors. Based on a review of the current preventive and remedial measures in place, recommendations for building greater resiliency are proposed.

ASA

Risk Consultants

Introduction

Information Technology (IT) poses one of the potent risks to the critical infrastructure of the nation. The potency stems from the fact that IT is all pervasive. Every industry depends on IT to manage its core business processes. As a result the risks involved in the implementation of IT has ramifications on most of the other critical infrastructure sectors such as healthcare, energy, chemicals, manufacturing, communication and on the economy too.

IT Risks and the Federal Government

On the government side, the IT risks are largely security related. The information systems used in the workplaces of Cabinet Departments deal with sensitive information. For example, consider the Department of Homeland Security (DHS) itself. One of the roles of the DHS is to protect the nation from cyber related crimes. The DHS issues a number of mandates, frameworks and assessments to help organizations and individuals protect, recover from and report cybercrimes and intrusions that could be potentially harmful to the privacy of citizens or the safety of the country. Thus they deal with a vast amount of security related information, making their systems vulnerable to IT related operational risks themselves.

The systems used by the employees who work in the DHS and the data stores and servers face intrusion risks. There are a number of insurgents who would benefit from this kind of information. The factor analysis of information risk (FAIR) framework describes the different ways in which threat agents make use of information assets – "access, misuse, disclose, modify and deny access to legitimate users".[1,2] Considering the nature of information dealt with by the cabinet departments, one or more of these actions could lead to dire consequences.

Information systems can be made secure only to a certain extent. Beyond this the aspect of human limitation comes into picture. From a risk perspective, people are often the weakest link in most organizations. Personnel who work in these offices, especially those with authorized access to sensitive information pose a threat of information leakage, intentional or otherwise.

IT risks include physical security, since physical damage to the storage devices and systems can be as crippling as the loss due to software crashes or cyber intrusions. Factors affecting physical damage are further discussed in the section on IT Risks in the Private Sector below.

In addition to the security threats, another important concern related to IT risks is with respect to its widespread use in the operation of other safety critical sectors such as power generation, healthcare and the nuclear sector.[3] Industrial control systems such as SCADA (supervisory control and data acquisition) are responsible for controlling and monitoring critical infrastructure components such as power and nuclear generators, water purification plants, waste management plants, chemical treatment plants and so on. Thus the other critical infrastructure sectors identified by the DHS depend upon the working of IT. In these sensitive and mission critical contexts, there is no room for system and process based errors.

Current Risk Mitigation Policies and Systems

A number of federal agencies and regulations have been put in place to help mitigate IT risks to the critical infrastructure of the nation. The Department of Homeland Security's National Cyber Security Division (NCSD) was constituted in order to develop and implement an effective risk management and response program. [4]

The government networks are currently protected by intrusion detection software called EINSTEIN developed by the United States Computer Emergency Readiness Team (US-CERT) of the NCSD. [5,6,7]

EINSTEIN acts like a filter and controls the packets that are allowed to access and be transported through the network. [8,9,10] CERT is also developing a collection of network IDS signatures – patterns that identify potentially harmful service requests – based on mining of historical attack logistics and the unique characteristics of previously identified threats. These signatures will be used by EINSTEIN to detect threats and inform the relevant authority. [11]

The Federal Information Security Management Act (FISMA) requires that all government agencies put into action a risk management plan to protect the information assets and systems operated by them. This process also includes frequent auditing and reviewing by the heads of these agencies to ensure compliance and to stay on top of rising security risks. The National Institute of Standards and Technology (NIST) has outlined a set of steps for ensuring compliance with the FISMA. This includes thoroughly analyzing the information assets to be protected, design and refinement of controls, testing and implementation of controls followed by constant monitoring.

The Computer Fraud and Abuse Act was written with the intention to prohibit access to computers meant for use by the

departments or agencies of the United States. However this law has been criticized for being too broad and outdated. [12] Currently an amendment called 'Aaron's Law' has been proposed, in honor of Aaron Swartz. [13]

The risks posed by the personnel working in the federal offices has been mitigated by policies for thorough background checks performed on individuals who are employed at these offices, selective information disclosure based on rank of the individual and thorough screening of outside individuals who need to enter the premises.

Recommendations for greater resiliency

People and the lack of information about things that can go wrong are a major cause for IT risks, particularly security related ones. Training and education can be effective in mitigating a large number of these threats. Legislation that mandates training with respect to the dos and don'ts of IT systems as a part of induction programs for all companies and industries would be a good way to reach out to more people. Education regarding the ethical and safe use of IT must also be made a part of the high school curriculum. On the government side, processes for increased security must be established, both physical and cyber.

Operational Risks in IT – The Private Sector

In the private sector, IT risks impact not only the company's business and the economy, but in extreme cases can even threaten the security of the nation. There are two aspects to security related risks. First, risks that effect the functioning of the business processes and second, security risks that affect the privacy of consumers.

For online retail giants the operational risks are largely in the systems and processes domain. These organizations are known to store large volumes of data related to customer and vendor information, transaction histories, supply chain information, inventory information and so on in data warehouses. These information objects are critical to the functioning of the business. The information systems that handle all these processes must be infallible. Any errors in processing, particularly transaction and inventory processing can lead to grave economic losses.

Other system risks include the breakdown of the key non-functional requirements of such systems - availability, reliability and recovery.

Data is one of the most important assets of an organization. A number of factors contribute to the risk of data loss – breakdown of servers, operating systems and application software; natural disasters

like earthquakes and hurricanes; physical damage to the data stores as a result of electric circuit malfunctions due to power surges or faulty communication infrastructure; accidental misplacement of artifacts such as laptops and portable data storage devices and so on. Apart from processing data such as transaction information, the work performed by employees on a daily basis is also liable to loss. This could be as a result of inadequate saving processes, accidental overwriting and so on.

To protect against the risk of data loss, companies maintain redundant data stores. Geographically dispersed and redundant data centers help in reducing the possibility of data loss from natural disasters and dependency on power. But on the flip side, the more redundant data centers there are, the more vulnerable the data becomes to security threats such as physical and cyber breaches. Thus decisions about the number of sites and their locations must be carefully made keeping these trade-off considerations in mind. Adequate security measures need to be instituted at each site.

There are technology specific and company culture specific risks to be considered as well. For example, businesses are now largely moving into the cloud and mobile services platform. The wireless

nature of these services poses additional threats to the information. Many IT companies today follow the work from home or the 'bring your own device' program (BYOD) that allows employees to use their personal device to connect to the corporate networks and perform their tasks. This increases vulnerability of networks and data as a lot of responsibility is placed on humans – the weakest link – to safeguard the resources. Intel has a security model that includes controls such as authentication, antivirus and antimalware, restricted access to company resources, encrypted data storage. [14] They also talk about educating employees on the risks, their impact and preventive measures to be taken.[15] These are a good set of controls that companies implementing BYOD and work from home options can apply. The policy must also address issues such as wiping out the device in case of suspected threats and clearly identify who is responsible and accountable for the resources and their potential compromise. [16,17]

Companies like social networking sites, online retail websites, email providers etc. provide personalized services to users by requiring them to login using unique credentials. With personalization comes the risk of identity theft, a serious operational risk faced by companies that deal with sensitive information such as addresses, credit card

information and details about personal lives of the consumers are dealt with. By gaining unauthorized access to a person's profile a cybercriminal can pose as another person to perform unlawful activities. These could range from posting inappropriate content, downloading inappropriate or unlawful information to communicating information of a threatening nature via email or chat applications. Over the past two years there has been a rise in the number of hacking attempts made at IT organizations. [18] This is external operational threat that is rising in severity. The risk of unauthorized access is increased once again due to the weakest link in the system – the people. Employees who have the authorization to manage security firewalls are a threat because they have the potential to intentionally or unintentionally open them up.

Social networking websites have additional security requirements. They must provide sufficient security options on their applications for users to moderate the content they share with different groups of people.

Companies that develop software and applications like Microsoft, Amazon etc. also face liability risks pertaining to patents and intellectual property. They also face the risk of litigation from

consumers for issues such as breach of security, malfunctioning products and so on.

Failure to guard against these risks will result in economic losses and loss of brand value of the company. It could also result in loss of business opportunity due to mismanaged IT resources.

The IT sector has infrastructural dependencies on other sectors like the Communications sector and the Energy sector. The energy sector is the source of power and the communications sector handles the risks related to the network and internet infrastructures. Breakdowns in either of these sectors will result in automatic breakdown of all the IT systems within the perimeter of operation of the failed energy and communication sources. These are additional external risks that must be accounted for in a risk assessment plan, both by the private organizations as well as the government.

Current Risk Mitigation Policies

There are a number of effective IT risk assessment frameworks and controls devised by standards organizations. These frameworks include ITIL, ISO 20000, ISO 9000, COBIT, VAL IT and others. The frameworks provide guidelines for managing different aspects of IT risks. The VAL IT framework deals more with IT risks from the business

perspective - leveraging IT to gain competitive advantage and the various factors to consider while taking a business decision based on IT. [19]

The Risk IT framework is an extension of COBIT and VAL IT published by the ISACA in 2009. [20] It covers the entire domain of IT related risks, not just focusing on IT security. [21] The frameworks and guidelines set out by these organizations help in preparing to face IT risks.

With the recent breaches in cyber security seen in commercial organizations, federal regulation to ensure that these companies protect their information assets has gained more importance than ever before. In addition to the business risks associated with these kinds of breaches, they also pose a severe threat to the economy, privacy of citizens and national security.

Federal laws to safeguard against these type of cyber threats has not been passed as yet, although senators have been lobbying for laws such as the Cyber security Act and the CISPA. While the CISPA is still being pushed for, President Obama has signed a Presidential Policy Directive that provides for sharing of cyber security related information

between the private sector and the federal government in order to better protect the nation from these attacks. [22]

The National Institute of Standards and Technologies (NIST) is currently working on cyber security regulations for private businesses to use as a guideline in order to ensure security of their critical resources.[23] They have also published a set of controls for the different nuances of information security, such as the NIST Special Publication 800 30.

Recommendations for greater resiliency in the private sector

The security of the system needs to be frequently updated. Cyber threat is an entirely different league of security threats. Safeguarding against these requires specialized knowledge and tools. Every company that uses IT must recruit specialists in IT security, or outsource it to a security management firm. In either case, the IT risk control policies must be framed very specific to the operations of that company. While COSO and COBIT are excellent frameworks for framing these policies, the companies and their security partners must go beyond them and analyze the specific situation inherent in the company. COSO and COBIT can be treated as a basic requirement that must be complied with.

Despite being aware of the threats many companies do not strictly enforce prevention measures, especially at the individual employee level. Employees might cancel processes like automatically scheduled machine scans and updates if this happens to interfere with their normal working. Regular maintenance of the servers and workstations, and power backup utilities has become more important than before. Exercising effective controls and strict vigilance at every level will go a long way in building resilience.

The potency of IT risks needs to be recognized at the top level. They need to be considered at the same level as market risks, credit risks and so on by the top management. [24] IT risks are often relegated to lower level team leaders or project managers. With the increase in the number of attacks in the recent past, companies must recognize the need to integrate solutions for IT risks within the overall risk management framework of the company, and also consider these risks while making business decisions such as investing in a novel technology. This recommendation is in accordance with the guidelines outlined in the Risk IT framework. [25]

The security assurance plans must span the entire lifecycle of the information asset. Security must be a priority that is monitored from

the beginning stages to the stage when the system is decommissioned or disposed of. Responsible management of decommissioned systems and the information that they contain must be outlined in the risk assessment plan. This holds good for the government side as well as the private sector.

Implementing the recommended measures in addition to following the well established guidelines of standards organizations such as ISACA and NIST will take the nation a step forward in building a more resilient future on the IT side.

References

[1] CSO. "IT risk assessment frameworks: real-world experience" *CsoOnline.com*. Web. 8 May 2013. <http://www.csoonline.com/article/592525/it-risk-assessment-frameworks-real-world-experience?page=2 - 2>
[2] Wikipedia. "Factor analysis of information risk" *Wikipedia.org*. Web. 8 May 2013.
[3] Wikipedia. "Cyber-security regulation" *Wikipedia.org*. Web. 8 May 2013. <http://en.wikipedia.org/wiki/Cyber-security_regulation>
[4] Wikipedia. "National Cyber Security Division" *Wikipedia.org*. Web. 8 May 2013. <http://en.wikipedia.org/wiki/National_Cyber_Security_Division>
[5] Search Security. "What is EINSTEIN" *TechTarget.com*. Apr 2010. Web. 8 May 2013. <http://searchsecurity.techtarget.com/definition/Einstein>
[6] DHS. "Privacy Impact Assessment EINSTEIN Program" *Dhs.gov*. Sep 2010. Web. 8 May 2013. <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf>
[7] Wikipedia. "Einstein (US-CERT program)" *Wikipedia.org*. Web. 8 May 2013.
[8] Search Security, n. pag.
[9] DHS, n. pag.
[10] Wikipedia, "Einstein (US-CERT program)", n. pag.
[11] Wikipedia, "Einstein (US-CERT program)", n. pag.
[12] Business Insider. "The Law Used To Target Aaron Swartz Doesn't Make Sense Anymore" *BusinessInsider.com*. Jan 20 2013. Web. 8 May 2013. <http://www.businessinsider.com/computer-fraud-and-abuse-act-reform-2013-1>
[13] Business Insider, n. pag.
[14] Intel. "Five Steps to Consumerization of IT" *Intel.com*. Oct 2012. Web. 8 May 2013.
[15] Intel, n. pag.
[16] Intel, n. pag.
[17] Subramaniam, Rajesh. "BYOD: Organizational Impacts of Mobile Computing and Convergence." *AnnieSearle.com*. Web. 8 May 2013. <http://anniesearle.com/web-services/Documents/ResearchNotes/ASA_Research_Note_BYOD-OrganizationalImpactsofMobileComputingandConvergence_November2012.pdf>
[18] Luco, Devin. "Malware Analysis: A Look Into the Past and Future." *AnnieSearle.com*. Web. 8 May 2013. <http://anniesearle.com/web-services/Documents/ResearchNotes/ASA_Research_Note_MalwareAnalysis-ALookIntothePastandFuture_November2012.pdf>
[19] ISACA. "Val IT Framework for Business Technology Management" *Isaca.org*. Web. 8 May 2013.
[20] ISACA. "Risk IT Framework for Management of IT Related Business Risks" *Isaca.org*. Web. 8 May 2013. <http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx>

[21] ISACA, "Risk IT Framework for Management of IT Related Business Risks", n. pag.
[22] The White House. "Fact sheet: presidential policy directive on critical infrastructure security and resilience" *Whitehouse.gov*. 12 Feb 2013. Web. 8 May 2013. <http://www.whitehouse.gov/the-press-office/2013/02/12/fact-sheet-presidential-policy-directive-critical-infrastructure-security>
[23] ExecutiveGov. "NIST Drafting Private Sector Cyber Framework; Ari Schwartz Comments" *ExecutiveGov.com*. 13 Mar 2013. Web. 8 May 2013. <http://www.executivegov.com/2013/03/nist-drafting-private-sector-cyber-framework-ari-schwartz-comments/>
[24] ISACA, "Risk IT Framework for Management of IT Related Business Risks", n. pag.
[25] ISACA, "Risk IT Framework for Management of IT Related Business Risks", n. pag.