Information Security

Name:

Institution:

Instructor:

Course:

Date:

Introduction

Information in any organization is the most important asset after the human resources. Risk and security management is data centric. Efforts of protecting networks and systems are all aimed at achieving three outcomes, and they include integrity, data availability, and confidentiality. It should be noted that infrastructure security controls are not 100 percent effective. "In a layered security model, it is often necessary to implement one final prevention control wrapped around sensitive information: encryption" (Balkin & Zarsky, 2006). Arguably, encryption should not be considered as a security panacea, as it cannot solve all data- centric issues of security. However, it is a one control among the many others. Cryptography is a science which applies logic and mathematics to design encryptions methods that are strong. Concerns for information security and confidentiality in a university IT environment were expressed as early as 1975 (Kerievsky, 1976). Colleges and universities have been a target for cyber-attacks for two main reasons: first, because of the vast amount of computing power they possess, and second, because of the open access they provide to their constituents and to the public. As the IT industry changes so are the opportunities for risks. Although encryption has obvious benefits in, for example, cloud storage, the way that it is sometimes deployed in these services is questionable.

Cybercrimes are multifaceted and vary from negligent to disgruntled insiders to external hacking. The 2013 Verizon Security Consultants recently gave an insight report on the risk areas in America. From the samples of 620 breaches, the external attackers were responsible for the majority of data breaches. 92% of data breach is as a result of the external agents. 14% implicate, while insiders with business partners are responsible for 1% of the data breaches. In terms of the methods of the attack, 92% used a malware or a hacking form, while 29% leveraged on social

tactics (Brenner, 2007). One can locate the immediate inception of cyber attack elsewhere in the USA, in a foreign nation, in the local area or cyberspace. For an instance, Al Qaeda could be planning its attacks somewhere in Europe while obtaining financial and logistical support from Eastern Asia or Northern Africa. The same group could do reconnaissance in their targeted USA city while recruiting and training operatives in Yemen. In a bid to beat intelligence, they could be doing so while sending their progressive reports to yet a different location probably in West Africa. In order to identify this kind of worldwide distributed network of threat there is an ardent need for collaborative information from evaluators located in regions that terrorists seek to strike, operate or plan. If this is done then the information gathered by homeland police who patrol neighborhoods in the USA communities can be incorporated into the picture of global events obtained by federal agencies and then use an intelligence statement that is not sensational to warn the public of any impending strikes (Harding, 2014).

On the other hand, attacks overlap with cyber terrorism, but this depends on the context. When talking about cyber terrorism and cyber attacks, one of the major underlying issues is the correct differentiation between the two terms. In most cases, the two terms are interchangeably used, and this brings a lot of confusions to those not familiar with the context. If an individual observes a specific case and its context, then the confusion might be exacerbated further by the application of similar terms such as cyber warfare. It is not very easy to make distinctions between attacks on computer networks done by terrorists from hackers 'cyber crimes. This happens because attackers try to exploit the weak spots within the system regardless of the essence of real motives. This notwithstanding, however, there are trends that can help in making the difference between the two acts. In most cases, for instance, computer terrorist network attack has focused on email bombing and website defacement (Schiller, 2010).

This paper will use Claflin University as an example to illustrate the above assertions.Currently; Claflin University doesn't have a comprehensive IT security risk management policy or guidelines that will guide the business process in the event of an IT security threat.

The policies that will be developed through this project will provide a roadmap for effectively protecting the availability, integrity and confidentiality of Claflin University's Information Systems. A comprehensive information security policy can effectively address the risks to information systems and provide a foundation for mitigating security concerns and incidents. As Claflin expands it's teaching and learning through online courses, it is more susceptible to security risks. The policies that will be developed through this project will protect Claflin's information security assets and will help continue the business process.

RISK IDENTIFICATION

In this case, the research will identify the various risks on the university's IT system. It should be noted that risks tend to occur in the IT system when vulnerabilities such as weaknesses or flaws in the IT system are exploited by treats such as environmental, human and natural factors. Accordingly, the process of identifying risks will consist of three components, and this will include;

- Identifying the vulnerabilities in the IT systems and their environments
- Identifying credible threats which can affect IT systems
- Pairing of the vulnerabilities with threats so as to identify risks that are exposed to the IT system

Identification of Vulnerabilities

In this case, the first component of identification of risks is by identifying vulnerabilities in the IT system and its surrounding environments. There are various frameworks and methodologies of determining the vulnerabilities of the IT system. The methodology will be selected on the basis of the IT system phase in its life cycle as follows:

- Project Initiation Phase- in this case, the vulnerabilities will focus on the organization of the information technology security policies, the vendor's security products analysis, IT requirement definition and planned procedures
- Project Definition Phase- in this phase, identification of the vulnerabilities will be expanded in order to include specific information. The assessment of the planned information technology features will be described in the system and security design system documentation.
- Implementation Phase- in this case, the identification of vulnerabilities will include the analysis of technical and security features, as well as the procedural security control that is used in protecting the system. The evaluations will include activities such execution of security self-assessments, affective of applications of automated vulnerabilities/ assessment/scanning tools and conducting third party penetration tools. It should be noted that the mixture of the above components will be used in getting a more comprehensible vulnerabilities list.

Determination of risk likelihood

The main goal of this step is to assign the likelihood rating of low, moderate and high to each and every risk that has been identified in the table above. It should be noted that the rating is a judgment which is subjective and it is based on the likelihood that vulnerability may be exploited by

credible threats. The factors to be considered include: Threat-source capability and motivation, in case of threat by human beings.

Cyber-crimes are multifaceted and vary from negligent to disgruntled insiders to external hacking. The Verizon Security Consultants 2013 recently gave an insight report on the areas of risks in America. From the samples of 620 breaches, the external attackers were responsible for the majority of data breaches with 92% being attributed to the external agents. 14% implicated insiders with business partners being responsible for 1% of the data breaches.

In terms of the methods of the attack, 92% used some malware or hacking form, while 29% leveraged on social tactics. 75 percent of all the data breaches took more than one month to be discovered while 96% of the initial attacks were not difficult to execute. On the other hand, the past few decades have seen attackers from "maladjusted teenagers intent on vandalizing websites or disrupting networks to individuals and groups motivated by commercial gain and state-sponsored groups seeking to steal intellectual property and/or to disrupt infrastructure of rivals or enemies" (Halder, & Jaishankar, (2011).

Part B. Security summaries

1. Malicious code

This type of cyber threat is broad and consists of several threats to cyber-security. The malicious code is any softwere, firmware, hardware that is intentionally inserted or included in a system for harmful purposes. The malicious code is commonly known as malware and it includes worms, computer viruses, key loggers, Trojan horses, Rootkits, BOTs as well as any exploits of any software security. The malicious code also includes spyware. Spyware is a deceptive program which is installed without any authorization to monitor the activities of the consumers without their

knowledge (Wright, Joe, and Harmening , 2009). Notably, it can be used in sending unwanted popupads to users, in monitoring the habits of online users as well as usurping control of Internet browser users. It should, however, be noted that spyware is normally installed alongside with something users want to be installed. Users acknowledge the installation of the spyware but don't consent the monitoring tactics of the device.

Risk identification identifies credible risks threats to the information technology systems and its environment. It should be noted that a threat will only be considered to be credible if it has the ability of exploiting identified vulnerabilities. The table below contains are some of the examples of threats. Accordingly agencies need to consult the various sources of threats information, and this includes NIST SP 800-30. This is aimed in identifying all credible threats in the information technology system, but not creating universal lists of general threats. It should be noted that the physical deterrents such as biometric devices, card access keys an locks may be used to prevent criminal gangs from gaining physical accesses of computer network systems. The use of strong password both for computer's BIOS and computer system can be effective measures of fighting cyber criminals with accessing physically a computer machine.

2. Network attacks

An attack on network is any action that is taken to deny, disrupt, destroy or degrade information residing in computer networks and on a computer. The attack can be of four forms, and these include interception, fabrication, modification and interruption. Fabrication is the creation of some kind of deceptions so as to deceive unsuspecting users. On the other hand, interception entails the intrusion of transmission and redirecting it for unauthorized uses. Attacks can either be passive or active. Active attacks entail the modification of transmissions to a system. On the other hand, passive attacks involve the monitoring of the attacks. The two forms can both used in obtaining

information of the users, which can be used in stealing the identity of the user. The common types of network attack include Distributed Denial of Services, Denial of Services, packet sniffing, ICMP Flood, TCP SYN Flood, and IP spoofing. The Cryptography technique can be used in fighting cybercrime. In this case information is encrypted using the algorithm known as cipher to mask the information that is on transit or in storage. For instance, tunneling can take a payload protocol like Internet Protocol (IP) and then encapsulate it in the encrypted protocol over Secure Sockets Layer, Virtual Private Network , Layer 2 Tunneling Protocol, Transport Layer Security, Internet Protocol Security or Point-to-Point Tunneling Protocol in order to ensure that there is a secure date transmission. It should, however, be noted that encryption can be used on the file level by employing protocols such as Triple DES, Data Encryption Standard, and Advanced Encryption Standard so as to ensure the storage information is secure. Moreover, the network testing vulnerability performed by automated programs or technicians can be employed to test on a full scale devices, passwords and systems used in networks to assess the extent of their security. Additionally, the network tools of monitoring can be employed in detecting of suspicious traffic or intrusions on both small and large networks.

3. Network abuse

Generally, these are fraudelant activities which are commited with aid of computers. One of the most common forms of this abuse is SPAM. In this case, a person emails a list of users with phishing attacks or unsolicited advertisements. In this case, an individual attempts to use social engineering to get sensitive information which can be used in identity theft, passwords, usernames etc. In pharming, the traffic of a website is redirected to a bogus website, and this is mainly done by exploiting the vulnerability of Domain Name System servers (Balkin et al, 2006). In order to focus

on the efforts of risk management, one should be comprehensive when developing the lists of the risks to the information technology system. Moreover, the list should be limited to the pairs of credible threats and actual vulnerabilities. For instance, "Oracle 9i will stop responding when sent a counterfeit packet larger than 50,000 bytes" (Brenner, 2007). It should be noted that the above flaw contains vulnerability. A computer criminal or a malicious use might be tempted to exploit the above vulnerability in order to stop the information technology from functioning. Accordingly, this will constitute a treat. The vulnerability threats combine in creating a risk in that an information technology system becomes unavailable. Notably, "If an IT system running Oracle 9i is not connected to a network, however, such as the certificate authority for a Public Key Infrastructure system, then there is no credible threat, and so no vulnerability-threat pair to create a risk" (Brenner, 2007). The threats of cyber security have become more complex in the modern world; hence companies must first understand them. The key areas of cyber security investments and levels of acceptable risks need to be taken into considerations. Companies must prepare for successful cyber attacks, and should ensure that they have enough resources and skills to identify and isolate the problems, determine the investigation levels and maintain the normal functioning of the business. Notably, the security measures will make companies to be more resilient and not restricted to core businesses.

4. NEURAL NETWORKS

Neural networks are used to prevent organizational frauds through data mining. This is achieved by tracking inconsistencies in transaction activities for payment transactions for online consumer businesses, or by banking institutions. The modern technology is expanding daily in every part of the world. This has improved the communication systems which has benefitted many

especially the business entrepreneurs. With the many advantages of the modern technology, fraud has dramatically increased. As a result many businesses have lost billions of dollars mysteriously. Prevention technologies have been established as the best way to tackle fraud but fraudsters have with time found their way through. Some of the fraud activities most fraudsters have indulged in are money laundering, e-commerce credit card scam, telecommunication frauds well as computer intrusion (Neumann, 2003, 87). .

The neural network is an information processing model controlled by the way the nervous system such as the brain receive and synthesizeinformation. The important elements to the artificial neural network are the neurons. They are highly interconnected processing elements that work together to tackle a similar problem. The development of the neural networks was before the advent of the computers. They have been useful since they are able to extract patterns as well as trends that are difficult to be noticed by humans.

Today, neural networks have been largely put in use to prevent fraud in the banking industry. During payment of salaries in the banks fraud has evolved constantly. The fraudsters are always on the lookout for any loopholes in the payment system so as to take advantage. They seek to maximize on the results of their activities. Those who offer payment services, issuers,banks as well as merchants have adopted neural networks as the main tool to prevent fraud. Fraud detection is a process that is done in the banks that enables the separation of transactions that are vulnerable to fraud and those not. The patterns in the data are used to do this. The Bayesian models together with the neural networks are used in different ways for fraud detection (Bermúdez et al, 2005).

5. **Data mining techniques**

Data mining techniques have been widely put in used to prevent and detect financial frauds. The implementation of the techniques to detect fraud has to follow the traditional information. This

is the flow of data mining; which starts with selection of feature selection, representation, data collection and management, pre - processing, data mining, post-processing, and finally performance evaluation. Data mining techniques succeed in detecting fraud because they use past circumstances of fraud to form models to be used to detect the jeopardy of fraud (Moore, 2005).

Financial statement fraud is one of the main financial frauds that are rampant worldwide and it has caused big companies to collapse due to financial losses. This has left a bad picture on the efficiency of corporate governance as well as the quality and credibility of financial reports. This fraud of financial statement fraud is a serious issue in the businesses globally (Abidogum, 2005).A neural network that detects fraud is an essential application of Data Mining. Both researchers' and practitioners have accepted that the analytical procedures, data mining techniques along with traditional reviewing procedures are necessary to prevent and detect financial statement fraud. The probability of the occurrences of threats based on the previous experiences or statistical data in the case of environmental and natural threats It should be noted that other factors can also be used in estimating the likelihood. Notably, these may include historical records and information for security organizations like US-CERT.

In modern world market, more and more organizations and government departments are increasingly linking their operational process to cyber infrastructures. As a result, an effective security cyber system is important to the institutional and organization's ability to protect their assets which may include intellectual property, reputation, customers and staff. Most organizations believe that by investing in a sophisticated technical solutions means that they are well protected from cyber attacks.

Organizations need to address the challenges of cyber threats in the world today. In this case, business and government leaders should ensure that they have an integrated approach to

security of their cyber. The cyber securities need to be tailored to a particular risk and business profile that does not only address the technical aspects of their profile, but also organizational elements and people.

List of references

Andress, Jason. Winterfeld, Steve.,2011, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. London: Syngress

Abidogum, O.,2005."Data mining, fraud detection and mobiletelecommunications: Call pattern analysis with unsupervised neural networks".PhD thesis, University of the Western Cape, Cape Town, South Africa.

Brenner, S. (2009). *Cyber Threats: The Emerging Fault Lines of the Nation State*. Oxford University Press

Bermúdez, L.; Pérez, J.; Ayuso, M.; Gómez, E.; Vázquez, F. A.,2007. Bayesian dichotomous model with asymmetric link for fraud in insurance. Insurance: Mathematics and Economics, vol. 42 (2): 779-786.

Balkin, J., & Zarsky, T., 2006. Cybercrime: Digital Cops in a Networked Environment, New York University Press, New York.

Brenner, S., 2007. Law in an Era of Smart Technology, Oxford: Oxford University Press

Grabosky, P. (2006) Electronic Crime, New Jersey: Prentice Hall

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. ,2004. The Economic Impact of Cyber-Attacks. Congressional Research Service, Government and Finance Division. Washington DC: The Library of Congress.

Halder, D., & Jaishankar, K., 2011. Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global

Jaishankar, K., 2011. Cyber Criminology: Exploring Internet Crimes and Criminal behavior. Boca Raton, FL, USA: CRC Press, Taylor and Francis Group.

Luong, K., 2006, The other side of identity theft: Not just a financial concern. Proceedings of the 3rd Annual Conference on Information Security Curriculum Development. Kennesaw, GA: ACM.

Loibl, T., 2005, Identity Theft, Spyware, and the Law. Proceedings of the 2nd Annual Conference on Information Security Curriculum Development. Kennesaw, GA: ACM..

Neumann, G., 2003, "Computer Security in Aviation," presented at International Conference on

Aviation Safety and Security in the 21st Century, White House Commission on Safety and Security

Novak, C. ,2007, Investigative response: After the breach. Computers & Security. v. 26, n. 2, p. 183.

Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

Mann and Sutton (1998). Netcrime: More change in the Organization of Thieving. British Journal of Criminology; 38: 201-229.

White, G., & Long, J. (2010). Global information security factors. International Journal of Information Security and Privacy (IJISP), 4(2), 49-60. doi:10.4018/jisp.2010040104

Willemssen, C., (2000). "FAA Computer Security". GAO/T-AIMD-00-330. Presented at Committee on Science, House of Representatives

Wright, Joe; Jim Harmening (2009). *Computer and Information Security Handbook*. Morgan Kaufmann Publications. Elsevier Inc.

Screenshots

Identifying Cyber Vulnerabilities

Today's world is more interconnected than ever before. Yet, for all its advantages, increased connectivity brings increased risk of theft, fraud, and abuse. As Americans become more reliant on modern technology, we also become more vulnerable to cyber attacks such as Corporate Security Breaches, Spear Phishing, and Social Media Fraud. Cybersecurity is a shared responsibility, and each of us has a role to play in making it safer, more secure and resilient.

Collaborating to Enhance Cyber Security

To address the evolving threats and increased risks of cyber crimes, DHS works directly with public and private partners to enhance cybersecurity. We work to promote cybersecurity awareness and digital literacy amongst all Internet users.

DHS also collaborates with the financial and other critical infrastructure sectors to improve network security. Additionally, DHS components such as the U.S. Secret Service and U.S. Immigration and Customs Enforcement (ICE), have special divisions dedicated to combating cyber crime.

Combating Cyber Crime

The Secret Service maintains Electronic Crimes Task Forces (ECTFs), which focus on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes. The Secret Service's Cyber Intelligence Section has directly contributed to the arrest of transnational cyber criminals responsible for the theft of hundreds of millions of credit card numbers and the loss of approximately $600 million to financial and retail institutions. The Secret Service also runs the National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cyber training and information to combat cyber crime.

ICE's Cyber Crimes Center (C3) works to prevent cyber crime and solve cyber incidents. From the C3 Cyber Crime Section, ICE identifies sources for fraudulent identity and immigration documents on the Internet. C3's Child Exploitation Section investigates large-scale producers and distributors of child pornography, as well as individuals who travel abroad for the purpose of engaging in sex with minors.

Law Enforcement Cyber Incident Reporting

The Law Enforcement Cyber Incident Reporting resource provides information for State, Local, Tribal, and Territorial (SLTT) law enforcement on when, what and how to report a cyber incident to a federal entity. The document also provides information on federally sponsored training opportunities and other useful resources available to SLTT law enforcement.

Losing Control of Cloud Data

As companies move data to the cloud, trade-offs between security and usability hamper business

Highlights:

- Business data is regularly stored in the cloud without any security beyond that provided by the cloud storage firm
- While private-key encryption is an option, encrypting data in the cloud robs businesses of much of the cloud's utility
- Searchable encryption continues to have trade-offs between security, functionality, and efficiency

With the rapid shift from business-owned to employee-owned information technology (IT), companies increasingly have to face the challenges of protecting data dispersed among workers' devices and consumer-grade cloud services. The evolution of IT to a mobile, distributed ecosystem means that most companies have data seeping out into the cloud. Even though seven out of every ten IT managers have either confirmed or assumed that employees are saving business data to the cloud[1], few companies are doing anything about the issue.

Yet, consumers and businesses are not the only ones using the cloud. The broad adoption of cloud services has allowed cybercriminals to use reputable services to bypass many of the digital defenses erected by companies. In addition, technically sophisticated cybercriminals have created their own cloud services, so that anyone intent on utilizing compromised systems can sign up and immediately lease a botnet or purchase other illicit services.

Against that backdrop, companies face a number of threats created by the ubiquity of the cloud.

File sharing and other cloud services still have questionable security

Companies continue to deal with the acceleration of so-called "shadow IT," the adoption of cloud services by employees who are seeking to make their work more efficient. With unknown and unmanaged services, productivity may improve, but important business data is left outside the protection of the corporate network, potentially placing the information at more risk. Dropbox, Box.com, and Google Drive are file-sharing services regularly used by employees that could allow outsiders to gain access to unencrypted data.

Companies first need to gain more visibility into the movement of business data. The average company's employees use more than 500 cloud services and most firms do not have a risk-based policy in place, according to data from Skyhigh Networks[2]. Cybercriminals are already using many services to exfiltrate data from inside the business or to gain access using trusted online services, such as reputable websites or file-sharing services from which malware can be downloaded. Inventorying a business's cloud use is a good first step.

IT security professionals

[1] Marko, Kurt, "Backing Up Mobile Devices May Be A Nonissue," InformationWeek report, August 2013, http://reports.informationweek.com/abstract/2/11155/Business-Continuity/Research:-Backing-Up-Mobile-Devices-May-Be-A-Nonissue.html

[2] Skyhigh Networks, "2013 Cloud Adoption and Risk Report," company blog post, August 2013, http://info.skyhighnetworks.com/2013CloudAdoptionRiskReport_RegistrationWS.html

should also look to secure access to sensitive data in the cloud by using two-factor authentication, making access to the data more difficult for attackers. Other threats exist as well: the cloud service can itself be compromised or become subject to a legal request by a sovereign government for data access. In those cases, companies need to implement encryption before the data is exported to the cloud, said Sasha Boldyreva, associate professor in the School of Computer Science at Georgia Tech.

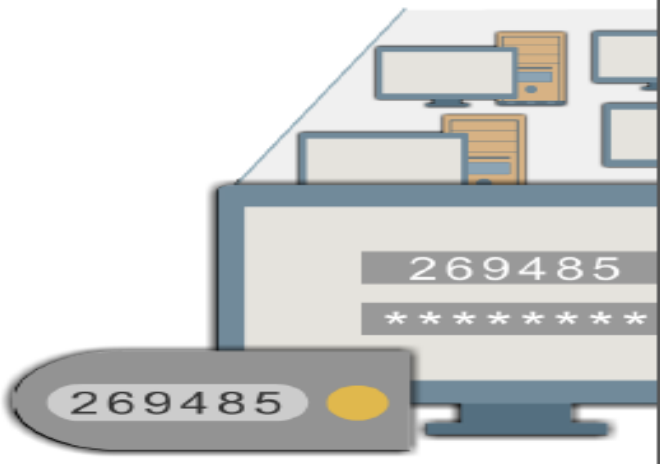
Protecting data against malware using the cloud

In 2009, a group of online hackers with links to China compromised Google and a number of other high-tech companies, stealing business information. Since then, nation-state-related attacks have only increased: From the Stuxnet attack on Iran's nuclear processing capability to the Syrian Electronic Army's hacktivism campaign to the ongoing collection of intellectual property by the Chinese[4].

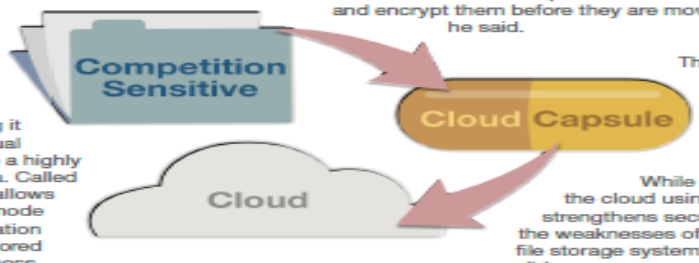
In this environment, companies and government agencies need to protect information from data-stealing malware while still allowing employees to continue to do their jobs.

The cloud can actually help. Pairing the reliability of cloud storage with strong encryption can create a system that is both secure and reliable even when using the public Internet. Some companies have already created cloud proxies that encrypt information as it is moved to a file-sharing service, such as Dropbox.

Georgia Tech researchers have developed a system that can use the cloud for online storage, and by pairing it to a secure and separate virtual machine instance, can create a highly secure way of accessing data. Called "CloudCapsule," the project allows a user to switch into secure mode using the exact same workstation and access encrypted files stored in the cloud. To allow fast access to the stored files, each file is encrypted and stored separately, said Billy Lau, a research scientist with the Georgia Tech Information Security Center (GTISC).



"It allows the user to import sensitive files into this capsule and encrypt them before they are moved into the cloud," he said.



The system has transparent integration with Google Drive and Dropbox, but can be used with any cloud storage. While encrypting data in the cloud using CloudCapsule strengthens security, it retains the weaknesses of any encrypted file storage system: data is less accessible.

[4] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017," Cisco Web site, Feb. 6, 2013, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

Cyber Technology and Information Security Laboratory (CTISL)

A new generation of cyber warriors has suited up for battle and is targeting U.S. interests. GTRI is a leader in developing the technologies that secure, defend, and respond to threats within our country's information, distribution, and network systems on the virtual battlefield. GTRI experts are tackling tough security issues within military and non-military networks, developing new tools and methods for securing information, educating and increasing awareness in the cyber domain, and applying leading technologies in network design to keep us safe now — and in the future.

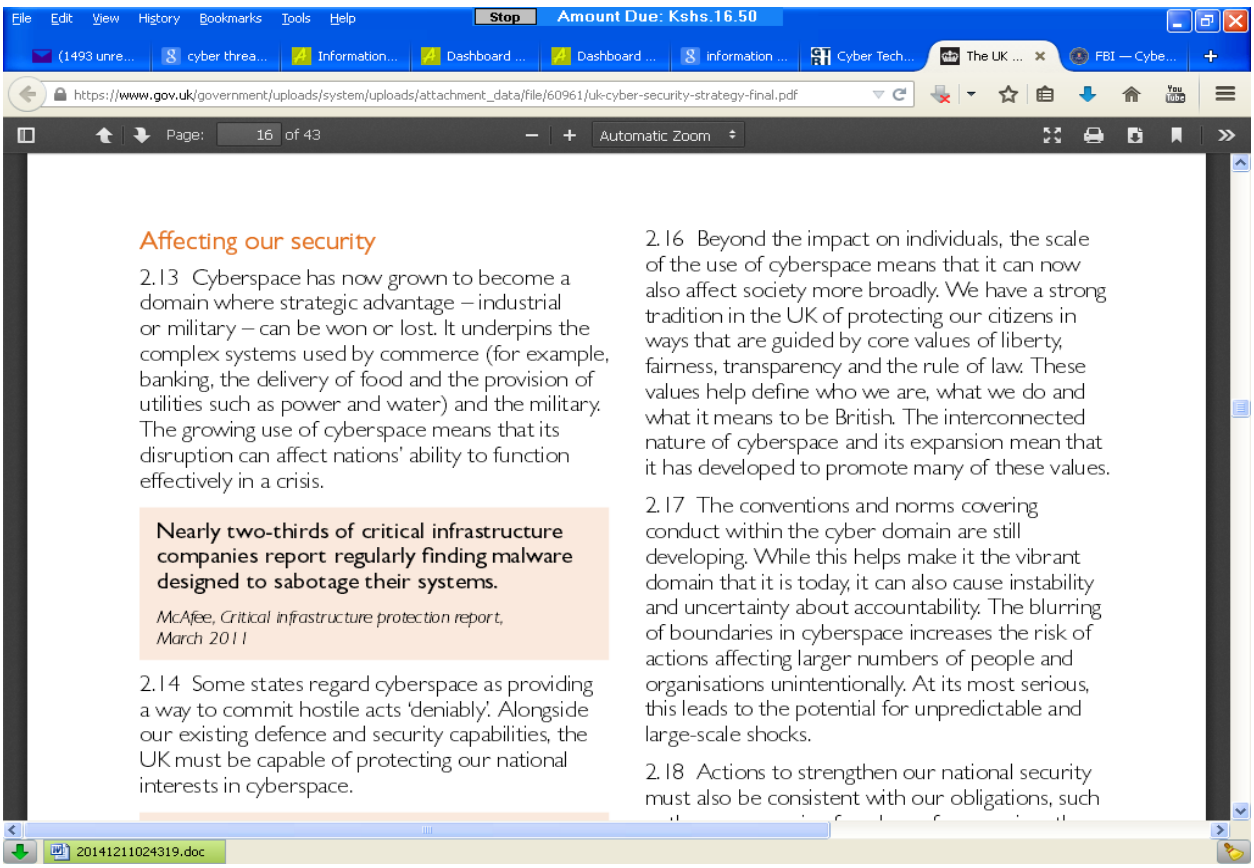
The Cyber Technology and Information Security Laboratory (CTISL) conducts applied research focused on cyber threats and countermeasures, secure multi-level information sharing, resilient command and control network architectures, reverse engineering, vulnerability identification, and high performance computing and analytics. CTISL engineers develop and apply cutting edge technologies in computing, network architectures, signal and protocol analysis, network forensics, malware analysis, and reverse engineering (hardware and software) to solve the tough problems. CTISL brings this knowledge to the classroom by providing professional education offerings across the cyber landscape.

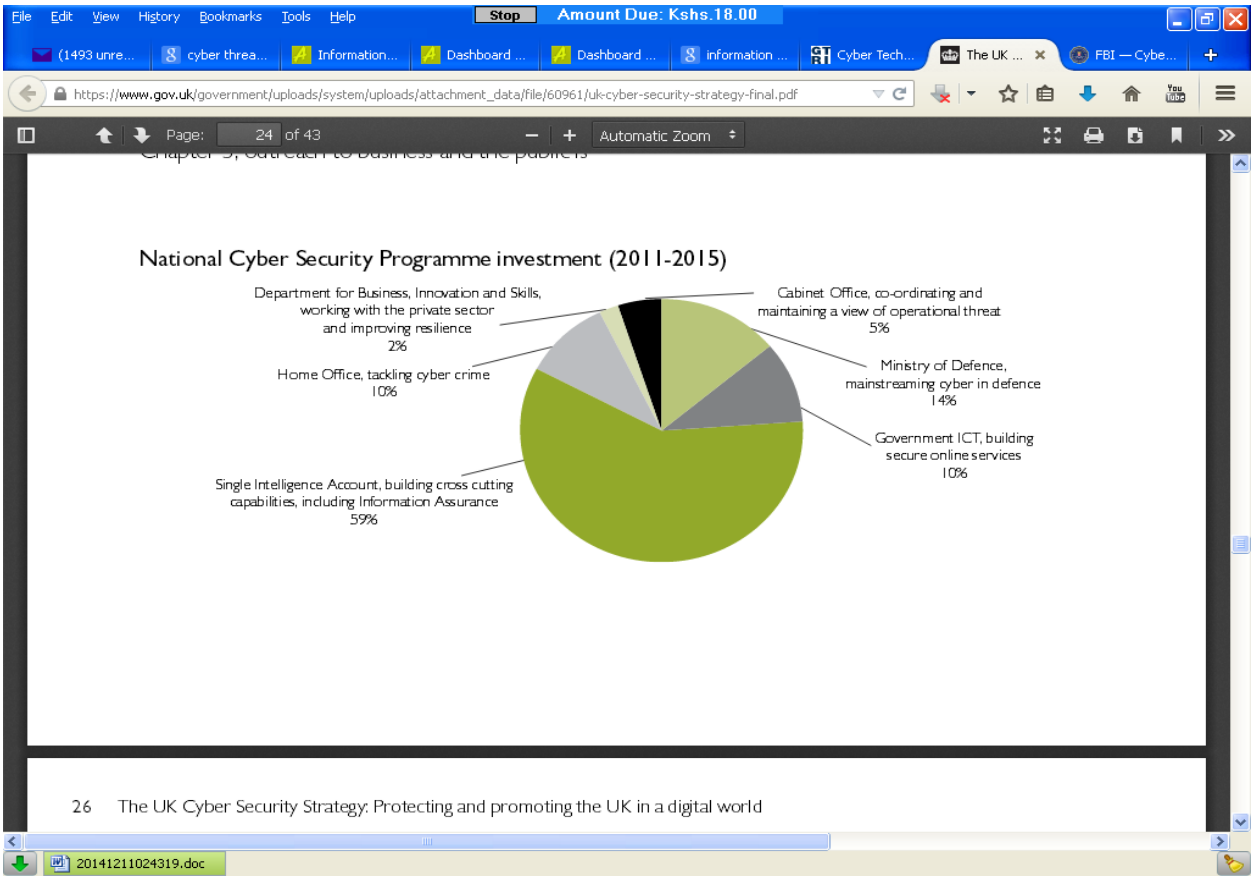
CTISL has six strategic thrusts:

High Performance Computing (HPC) and Analytics
The Innovative Computing Division (ICD) designs, develops, and applies HPC techniques to advance the field of parallel computing and to support ultra-fast analytics in support of "Big Data" problems, real-time deep packet inspection, insider threat detection, password cracking, and high speed relational mapping of feature sets. ICD has extensive experience with diverse aspects of high throughput computing systems, including GPU computing, massively parallel systems, high performance software libraries, middleware, compilers, low-level optimization, and platform design for diverse application domains including cryptanalysis, network analysis, signal processing, and more.

Multi-Level, Secure Software Systems and Collaboration Tools
CTISL's Secure Information Systems (SIS) Division concentrates on the design and development of secure real-world, multi-level information sharing applications. Both hardware and software design methodologies are combined to deliver information exchange solutions that pass the rigorous testing required to operate on the nation's most secure networks. SIS solutions are nationally recognized within the government as state-of-the-art, affordable, secure, and scalable.

Professional Education, Outreach and Awareness
Although much hype exists about the threat of cyber attacks, many organizations still fail to understand the costs of data exfiltration, network disruptions, and other nefarious actions that may result from a cyber attack. Perimeter protection, although necessary, is not enough. CTISL is dedicated to "Equipping and Educating the Good Guys." To that end, CTISL cyber security experts provide tailored educational opportunities, hacker competitions, emerging threat conferences, threat landscape reports, and other outreach activities. We believe that effective information security programs must first be grounded in education and training as threats become more and more sophisticated.




File Edit View History Bookmarks Tools Help
Stop
Amount Due: Kshs.18.00
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
Page: 24 of 43
Automatic Zoom
National Cyber Security Programme investment (2011-2015)
Department for Business, Innovation and Skills, working with the private sector and improving resilience 2%
Cabinet Office, co-ordinating and maintaining a view of operational threat 5%
Home Office, tackling cyber crime 10%
Ministry of Defence, mainstreaming cyber in defence 14%
Government ICT, building secure online services 10%
Single Intelligence Account, building cross cutting capabilities, including Information Assurance 59%
26 The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world
20141211024319.doc

Costs of Defending Against Cyber Attacks Remain High

Mitigating the risk of cyber attacks continues to be uncertain and costly, but gaining better visibility into threats and mitigating specific risks can help

Highlights:

- Chasing technology and creating multiple layers of static defenses has driven up security costs
- Companies need to focus on gaining visibility into their networks and the external threats targeting their business
- Shifting focus from devices to data can simplify defensive concepts and better cope with the bring-your-own-device (BYOD) trend, but usability continues to be a problem
- While the market for cyber insurance is growing, fundamental problems continue to prevent broad acquisition of policies to mitigate risk

Over the past decade, companies have moved from deploying a simple firewall, antivirus software, and patch deployment system to adopting a variety of other technologies: security information and event management (SIEM), data loss prevention, identity and access management (IAM), application firewalls, and more recently, mobile device management (MDM). Following the mantra of defense-in-depth, the more layers of technology placed between the attackers and the business, the better.

Yet, a technology-oriented focus has driven the cost of security higher for companies. Despite slow economic growth, IT security budgets will climb five to ten percent higher in 2013. Surveys in the past year have found half[9] to two-thirds[8] of IT security professional expect budgets to increase in the coming year.

Reducing cost while protecting the business will require a more data-driven approach to security. Researchers and businesses that focus on gathering more information on their security state and their current threats can better protect their networks and data while holding down costs. In addition, moving the focus of security from the device to a business's data can simplify defenses. Finally, cyber insurance can act as a safety net for companies, although questions remain over the efficacy of policies and coverage.

Threat intelligence is necessary, but still in early stages

Finding information on attackers is not difficult: blacklists, open-source intelligence, logs from a variety of network devices, malware analysis, social networks and other sources can all give defenders some insight into attackers' techniques, identities and motivations. However, making sense of that data and turning it into intelligence relevant to a specific company or target is difficult. In addition, unless the information can be delivered to the right people in a short amount of time, it may lose value quickly.

- SC Magazine Poll, "Security Budgets In 2013," SC Magazine, http://www.scmagazine.com/security-budgets-in-2013/slideshow/1157/#1
- Prasti, Kari, "Report: Security Budgets Trending Upwards For 2013," CRN, Dec. 7, 2012, http://www.crn.com/news/security/240144099/report-security-budgets-trending-upwards-for-2013.htm

Malicious code runs under the user's authority. Thus, malicious code can touch everything the user can touch, and in the same ways. Users typically have complete control over their own program code and data files; they can read, write, modify, append, and even delete them. And well they should. But malicious code can do the same, without the user's permission or even knowledge.

Malicious Code Has Been Around a Long Time

The popular literature and press continue to highlight the effects of malicious code as if it were a relatively recent phenomenon. It is not. Cohen [COH84] is sometimes credited with the discovery of viruses, but in fact Cohen gave a name to a phenomenon known long before. For example, Thompson, in his 1984 Turing Award lecture, "Reflections on Trusting Trust" [THO84], described code that can be passed by a compiler. In that lecture, he refers to an earlier Air Force document, the Multics security evaluation [KAR74, KAR02]. In fact, references to virus behavior go back at least to 1970. Ware's 1970 study (publicly released in 1979 [WAR79]) and Anderson's planning study for the U.S. Air Force [AND72] (to which Schell also refers) *still* accurately describe threats, vulnerabilities, and program security flaws, especially intentional ones. What *is* new about malicious code is the number of distinct instances and copies that have appeared.

So malicious code is still around, and its effects are more pervasive. It is important for us to learn what it looks like and how it works, so that we can take steps to prevent it from doing damage or at least mediate its effects. How can malicious code take control of a system? How can it lodge in a system? How does malicious code spread? How can it be recognized? How can it be detected? How can it be stopped? How can it be prevented? We address these questions in the following sections.

Kinds of Malicious Code

Malicious code or a **rogue program** is the general name for unanticipated or undesired effects in programs or program parts, caused by an agent intent on damage. This definition eliminates unintentional errors, although they can also have a serious negative effect. This definition also excludes coincidence, in which two benign programs combine for a negative effect. The **agent** is the writer of the program or the person who causes its distribution. By this definition, most faults found in software inspections, reviews, and testing do not qualify as malicious code, because we think of them as unintentional. However, keep in mind as you read this chapter that unintentional faults can in fact invoke the same responses as intentional malevolence; a benign cause can still lead to a disastrous effect.

You are likely to have been affected by a virus at one time or another, either because your computer was infected by one or because you could not access an infected system while its administrators were cleaning up the mess one made. In fact, your virus might actually have been a worm: The terminology of malicious code is sometimes used imprecisely. A **virus** is a program that can pass on malicious code to other nonmalicious programs by modifying them. The term "virus" was coined because the affected program acts like a biological virus: It infects other healthy subjects by attaching