Study to identify threats to Information Systems in organizations and possible countermeasures through policy decisions and awareness programs to ensure the information security. L...

Article · August 2016

2 authors:

Sunesh Hettiarachchi
11 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Samanthi Wickramsinghe
Horizon Campus
25 PUBLICATIONS **11** CITATIONS
SEE PROFILE

Study to identify threats to Information Systems in organizations and possible countermeasures through policy decisions and awareness programs to ensure the information security.

Sunesh Hettiarachchi[1], *Samanthi Wickramasinghe*[2]
[1] Tech Computers, Colombo 5, Sri Lanka
[2] Horizon Campus, Malabe, Sri Lanka

ABSTRACT

Accurate and up-to-date information is considered as the most essential asset to any organization. Global State of Information Security Survey-2016 indicates that 38% more security incidents were reported in 2015 than 2014. With the above considerations, it is evident that strong information protection system is an essential attribute in business organization. Especially the need is much more with business expansions, business diversifications and globalizations.

Due to the technology advances in Information Systems and Information Communication Technology, the protection of the organizational information assets is a *must achieve* business goal. Therefore, protecting the organizational assets from many different threats is the main function of any business organizations.

The most critical issue in information security of an organization is to set up a strong *security policy* by addressing all the critical success factors. Further, having a strong security policy does not ensure that information system is completely secured from all type of threats and risks. It is also vital to conduct proper awareness programs and training sessions to keep the users informed about the importance of *highly-protected* information systems and *business success*. Also ISO-27002 recommends that the information security responsibilities should be clearly defined to ensure the information by implementing and managing properly.

This paper illustrates threats to Information Systems in organizations and possible countermeasures through policy decisions and awareness programs to ensure the information security.

PROBLEM STATEMENT

With business expansion and diversification, business managers concentrate more on their product and service quality. They pay less or no attention on protection of information is considered as just another business responsibility. This creates a huge hole in information security and increase the level of risk factor in the organization.

RESEARCH HYPOTHESIS

This paper highlights two hypotheses to find solutions to increase the security level of information systems in organizations.

a) *Different types of threats for information systems.*
b) *Possible countermeasures through policy decisions and awareness to safeguard information systems.*

METHODOLOGY

Data collection : The required data for the research was collected from the following sources:

- Primary sources: Person-to-person interviews.
- Secondary sources: Research papers, journals and Internet.

Conceptual model: Two variables were identified to construct the model. They are *Types of threats* and *appropriate security measures.*

LIMITATION

Primary data collection restricted due to limited time and data collection was restricted to senior managers.
Secondary data collection was restricted to limited number of books available on the relevant field and Internet.

1.0 INTRODUCTION TO THE INFORMATION SECURITY

Due to the lack of documentation and characterization, assets in the organization would breach the security of the information system. According to Ciampa [Ciampa, 2012], *"an organization not only protects its information by classifying its assets but it also identifies its vulnerabilities in order to protect them from any threat".*

Significant financial losses in many organizations incurred due to vulnerability of various types of threats.

Information security damages can varies from minor losses to even entire information system destruction. The International Standardization Organization for (ISO) defined as, *"security is the set of measures to ensure confidentiality, integrity, and availability of information"*. At present, organizations are strive to understand what the threats are and how to find necessary measures to combat them to protect their information assets.

It is clear that the risk factors, level of security varies from organization to organization. For example in Medical/Health, Defense, International Security and Information Technology sectors are classified as the high level of security whereas Banking, Education, Telecommunication and Transportation sectors are denoted moderate level of security.

With all the precautions, organizations will be able to secure their security objectives effectively. The main consideration of implementing the most appropriate security measure which helps to organization to reduce possible damages and losses. Likewise, vulnerability analysis, safeguard analysis, risk analysis, risk management and risk mitigation are also important aspects when focusing on security of information system. Disaster Planning is also playing a vital role during security of information system because organizations have to take actions to minimize damages and avoid potential disasters to control which cause organizations.

In addition to this there should be an appropriate Information Security Policy for any organization. The information security policy covers all the types of policies: program policies, system-specific policies and issue-specific policies. During the policy implementation process, procedures, guidelines and standards are described within the organization. It assists for users, system personnel and others to secure their information systems effectively.

2.0 VULNERABILITIES, THREAT AND RISKS TO THE SECURITY OF INFORMATION SYSTEMS

Vulnerability is the level of exposure to threats whereas threats correspond to the type of damage that could be existence. Vulnerability is the weakness of information and information systems can be lead to attacks by modification, destruction, disclosure, interruption and interception which are described as:
1. Destruction: Due to malicious intensions, information, hardware, and software can be destroyed.

2. Disclosure: *"Unauthorized disclosure has a serious impact on maintaining security and privacy of the system"* (Dhillon, 2006). It happens when unauthorized access to information and reveal the confidential information in the systems.

3. Modification: arises when unauthorized users modify the information available in the systems.

4. Interruption: Due to unavailability access to the computer network it occurs. Eg. Denial of Service (DoS).

5. Interception: happens when unauthorized users copying information and transmitting data which exist in the information system.

The lead sign of vulnerability is an attack on information systems. "*Vulnerability could be assessed by identifying flaws and weaknesses that could possibly be increased the threats"* (Dhillon, 2006).

The weaknesses of information systems are the origins of the breaches in information security which can lead to financial losses, brand name damages, loss of confidence with the customer & partner, and could also results the organization even closure of business (Nyachama, 2005).

It is evident that **74%** of the total losses are caused by: viruses, unauthorized access, laptop or hardware theft and theft of proprietary information *(11th Annual Computer Crime and Security Survey in 2006).* Even though the **90%** of security controls are focused on external threats, a research conducted by the McCue shows that **70%** of frauds are committed by insiders than outsiders.

2.1 Types of Threats

Information systems are vulnerable to many threats. For better understanding and complexity of the threat problem, Whitman and Mattord (2003) have classified threats into five (5) general categories as mentioned below:

- Unintentional threats
- Environmental threats/Natural disasters
- Technological threats
- Management failure
- Deliberate act

Denial of Service, laptop Theft, Telecom Fraud, Unauthorized Access, Virus, Financial Fraud, Insider Abuse, System Penetration, Sabotage, Theft/loss of Proprietary Info, Wireless Network Abuse, Website

Defacement, Web Application Misuse, Bots, DNS, Instant Messaging Abuse, Password Sniffing, Theft/loss of Customer Data are the most significant threats according to the classification of Annual Computer Crime and Security Survey in 2008 (Shahri & Ismail, 2012).

A threat can be in internal, external or combination of internal and external threats. The figure 1 illustrates the detailed description of all possible internal and external threats caused to any information system. The top portion of the figures describe the internal threats and the bottom portion provide a detailed impact on internal threats which are having serious effects to the information system. Detailed description of external and internal threats are mentioned in appendix 1.

2.1.1 External Threats

The individuals or organizations working outside of a company cause for the external threats. The most external threats to information systems is natural disasters. External attacks occurs through connected network or physical intrusion. The figure 1, shows the major threats to the Information system security. Eg. Natural Disasters, Man-made disasters, unauthorized users, Malware, Denial of Service and etc.

2.1.2 Internal Threats

According to the figure 1 the major impact on information systems are internal threats. The internal parties have rights to access the most of the assets in the organizations, therefore, a result of an employee action or failure can cause for many destructions.

Eg. Employees, ex-employees, temporary workers, etc.

3.0 COUNTERMEASURES WHICH MAY BE EMPLOYED TO COMBAT THE SECURITY THREATS

Any organization would like to develop the resources and capabilities to minimize threats to the information systems. Therefore an effective countermeasure plan should be the main objective to address this issue. There are no counter measurements for complete eradication of vulnerabilities but organization should have prevention and detection methods to reduce threats and risks in early stages.

Another important aspect is that the organizational behaviours threats for their information systems are varied among companies and therefore, different level of security measures are needed to achieve main principles such as confidentiality, integrity and availability of information systems.

Objectives in relation to security an information systems are the most important aspect in any organization. Security objectives must comprise of vulnerabilities, security policies, threat controls and countermeasures.

A countermeasure is a mechanism to mitigate the possible risk or safeguard from vulnerabilities of the information system. It can be a hardware component, password management, mechanisms for access control, antivirus software, digital signatures, encryption of confidential information (cryptography) and software configuration. Having an antivirus software is not enough to eliminate risk but to keep it up-to-date is a good step as a precaution.

The tables in appendix 2 classify, types of threats and countermeasures can be taken to eliminate the respective threats.

According to the Global State of Information Security Survey 2016, 54% Chief Information Security Officers (CISO) are in charge of the security programme. *"The CISO or Chief Security Officer (CSO) is responsible and accountable for risks, and is expected to deliver a minimum information security posture across the organization. Doing so demands a new level of management skills."* Skills & competencies of security leaders are illustrated in figure 2. Many organizations are incorporating strategic initiatives to improve security and reduce risks.

ISO 27001 and the US National Institute of Standards and Technology (NIST) Cybersecurity Framework are the two most frequently implemented guidelines. According to the guidelines, it enables organizations to identify and prioritize risks, measure the maturity of their cybersecurity practices and have a better communication internally and externally.

The Global State of Information Security® Survey 2016 reports 91% have adopted a risk-based security framework as illustrated in figure 3 and Cybersecurity framework and the benefits of security frameworks are illustrated in figure 4. The Global State of Information Security® Survey 2016 further reports that 69% uses cloud based cyber security services as a sophisticated tool for cybersecurity safeguards. Cloud providers invested in advanced technologies for data protection, privacy, network security and identity and access management progressively.

Adoption of cloud-based cybersecurity services on Real-time monitoring & analytics, Advanced authentication, Identity & access management, Threat intelligence and

End-point protection are 56%, 55%, 48%, 47% and 44% respectively as shown in the figure 5.

Many Businesses organizations are investing in core safeguards to better defend against evolving threats as illustrates in figure 6.
Prevention is better than cure. Thus, many organizations invest to setup correctly configured firewall. It prevents unauthorized use and access to your network from untrusted networks. It indicates the status of DOS attack, Recent Malware and FTP Virus alerts, and details of top hosts, top destination countries and top domains details as clearly illustrated in figure 7.

4.0 AWARENESS PROGRAMS TO ENSURE THE INFORMATION SECURITY.

Sri Lanka CERT and TechCERT established to provide an effective response and to ensure suitable vigilance for computer security incidents and to implement positive measures to protect the information infrastructure.

Sri Lanka CERT offers three (3) broader service types such as Responsive Services, Awareness Services and Consultancy Services. Their awareness services are intended to aware publics on the importance of Information Security by providing followings facilities.

Alerts - to disseminate information on Computer Viruses, Hoaxes, Security Vulnerabilities & Exploits other security issues, and where possible, to provide short-term recommendations for dealing with the consequences of such attacks.
Seminars & Conferences – to provide awareness about the most current Information Security issues, Security Standards and best practices. This reduces the probability of being successfully attacked.

Workshops – to increase the awareness of Information Security through technically oriented and targeted for IT professionals, who perform daily tasks related to Information Security.

Knowledge Base - to provide a range of Knowledge Resources such as documents, articles, news items, etc published on the Sri Lanka CERT|CC website

TechCERT implements customized and fully-integrated information security technologies and services across the enterprise IT infrastructure. The TechCERT Managed Security Services through

Protection of customer IT resources from external cyber-attacks and from inside-attackers.
Protection of vital data and information belonging to customer and prevent financial losses and harm to reputation
Compliance of customer IT policies and practices with IT laws and regulations of the country
Operational availability of disaster recovery and business process continuity under severe service disruptions

Other than the above services, Website Security Assessment, Digital Forensics Investigations, TechCERT LAN Mapper, Database Security Assessment, Mobile Application Security Audit, Penetration Test, Comprehensive Server Security Assessment, Firewall Audit and PCI-DSS and PA DSS Assessments services are also offered.

5.0 CONCLUSION

It is clear that the risk factors, level of security varies from organization to organization. For example in Medical/Health, Defense, International Security and Information Technology sectors are classified as the high level of security whereas Banking, Education, Telecommunication and Transportation sectors are denoted moderate level of security.

Organizations are facing many issues due to several security threats. Disclosure of confidential information, unauthorized access, unauthorized modification, system failures or data corruptions and infection of malicious software are the most dangerous threats to any information systems. Therefore, as an organization, it should have a sound knowledge to recognize the nature of the threats and risk level to mitigate or prevent them by applying appropriate strategies.
With all the precautions, organizations will be able to secure their security objectives effectively. The main consideration of implementing the most appropriate security measure which helps to organization to reduce possible damages and losses.

Likewise, vulnerability analysis, safeguard analysis, risk analysis, risk management and risk mitigation are also important aspects when focusing on security of information system. Disaster Planning is also playing a vital role during security of information system because organizations have to take actions to minimize damages and avoid potential disasters to control which cause organizations.
In addition to this there should be an appropriate Information Security Policy for any organization. The information security policy covers all the types of policies: program policies, system-specific policies and issue-specific policies. During the policy

implementation process, procedures, guidelines and standards are described within the organization. It assists for users, system personnel and others to secure their information systems effectively.

6.0 ACKNOWLEDGEMENT

We would like to express our sincere thank to Prof. Colin N. Peiris, Vice-Chancellor of the Horizon Campus, Mr. Ajitha Wanasinghe, CEO of the Horizon Campus and Mr. Thishakkya Liyanage, Systems Engineer of the Horizon Campus for providing relevant information and constant support during the meetings.

I would like to thank Ms. Samanthi Wickramasinghe's constant support for finding information, doing relevant formatting of the paper as a Co-Author and encouragements to complete the paper before the deadline.

7.0 REFERENCES

1) Ahmad, A. (n.d.). Type of Security Threats and It's Prevention. *Computer Technology & Applications - ISSN:2229-6093*, Vol 3 (2), 750-752.
2) Ciampa, M. (2012). *Security Guide to network security fundamentals (4th edition).*
3) Dhillon, G. (2006). *Principles of information system security: Texts and Cases (1st ed.).*
4) Johnston, A., & Warkentin, M. (2010). FEAR APPEALS AND INFORMATION SECURITY. *MIS Quarterly*, 549-566.
5) Kumar, R., Park, S., & Subramaniam, C. (2008). Understanding the value of countermeasures portfolios in information systems security. In *Information Systems Security*.
6) Mouna Jouini, L. B. (2014). Classification of security threats in information systems. *Classification of security threats in information systems.* 5th International Conference on Ambient Systems, Networks and Technologies.
7) Nyachama, M. (2005). Enterprise vulnerability management and its role in information security management. *Information Security Management*, 29-56.
8) Onwubiko, C., & Lenaghan, A. (2007). Managing Security Threats and Vulnerabilities for Small to Medium Enterprises. *IEEE International Conference on Intelligence and Security Informatics* .
9) Rainer, K., & Cegielski, C. (2009). Introduction to Information Systems.
10) Shahri, A., & Ismail, Z. (2012). A Tree for Identification of Threats as the First Stage of Risk Assessment in HIS. *Information Security*, 169-176.
11) Venkata, M. K., Sharif, M. K., & Badri, H. (2012). A Study of Risk Management of an Information System by Assessing Threat, Vulnerability and Countermeasure. *International Journal of Advanced Research in Computer Science and Software Engineering*.
12) The Global State of Information Security® Survey 2016

13) https://www.techcert.lk/en/managed-security-services

14) http://www.cert.gov.lk/services.php

8.0 FIGURES

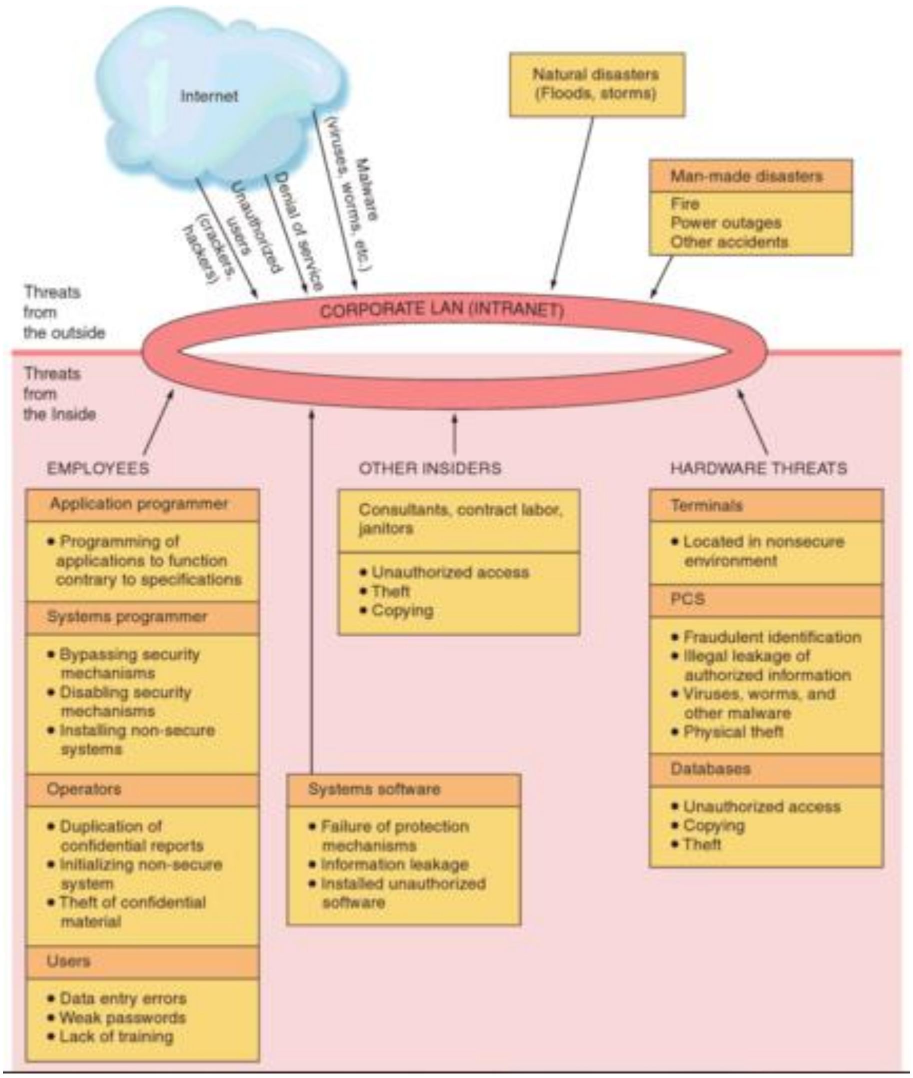

Internet
Natural disasters (Floods, storms)
Man-made disasters
Fire
Power outages
Other accidents
(crackers, hackers)
Unauthorized users
Denial of service
Malware (viruses, worms, etc.)
Threats from the outside
CORPORATE LAN (INTRANET)
Threats from the Inside
EMPLOYEES
OTHER INSIDERS
HARDWARE THREATS
Application programmer
• Programming of applications to function contrary to specifications
Systems programmer
• Bypassing security mechanisms
• Disabling security mechanisms
• Installing non-secure systems
Operators
• Duplication of confidential reports
• Initializing non-secure system
• Theft of confidential material
Users
• Data entry errors
• Weak passwords
• Lack of training
Consultants, contract labor, janitors
• Unauthorized access
• Theft
• Copying
Systems software
• Failure of protection mechanisms
• Information leakage
• Installed unauthorized software
Terminals
• Located in nonsecure environment
PCS
• Fraudulent identification
• Illegal leakage of authorized information
• Viruses, worms, and other malware
• Physical theft
Databases
• Unauthorized access
• Copying
• Theft

Figure 1: Security threats Source: (Rainer & Cegielski, 2009)

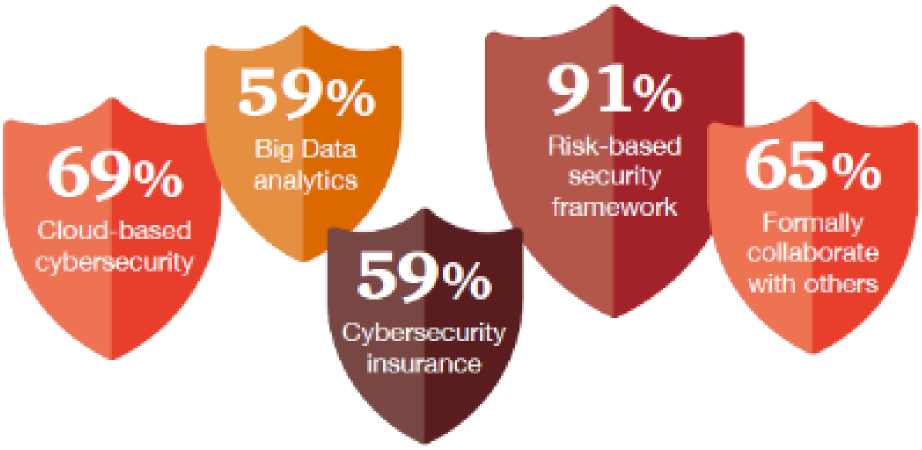


Figure 2: Skills & Competencies of Security Leaders

Figure 3: Adoption of Strategic Security Initiatives

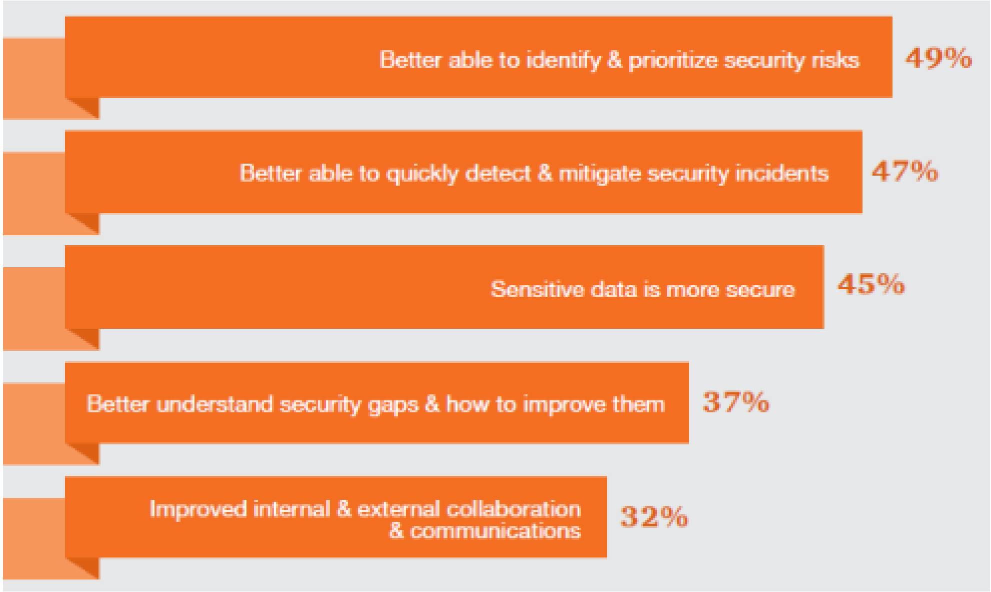


Figure 4: Benefits of Security Frameworks

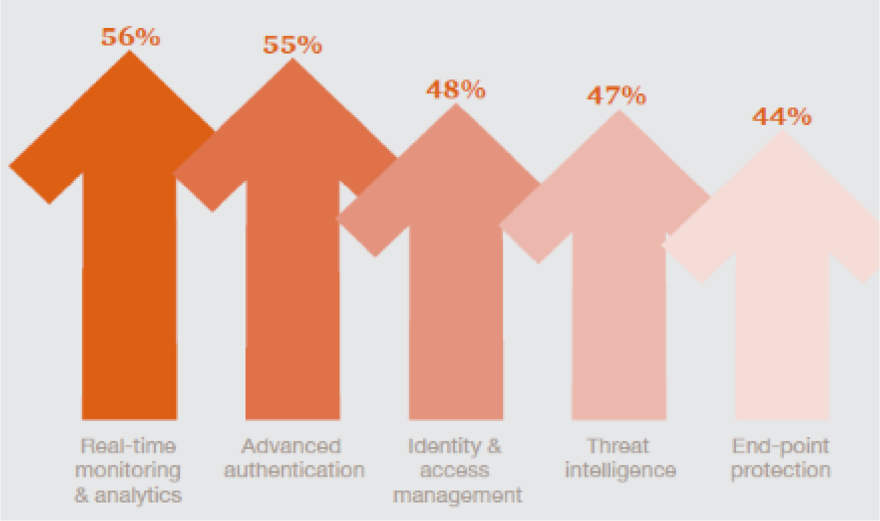


Figure 5: Adoption of Cloud-based Cybersecurity Services

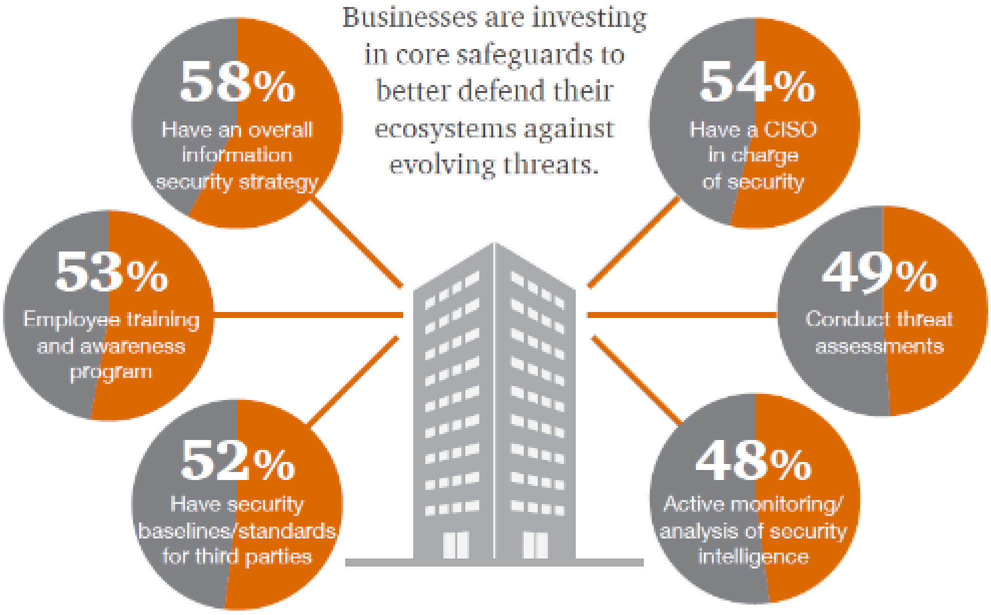
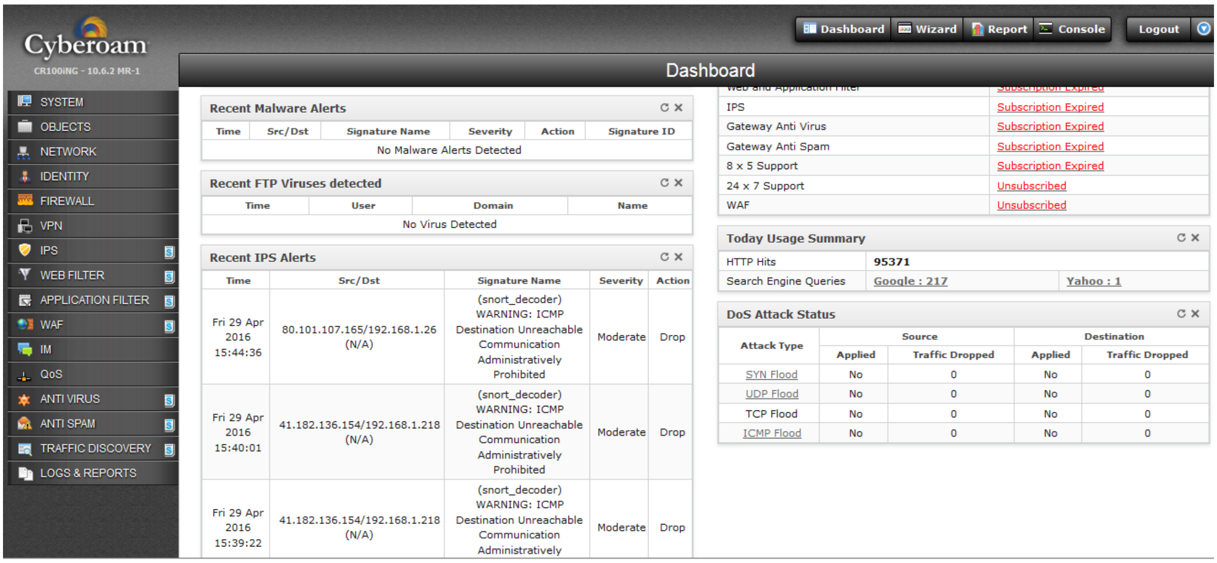


Figure 6: Implementation of Key Security Safeguards



Dashboard

Recent Malware Alerts

Time	Src/Dst	Signature Name	Severity	Action	Signature ID
No Malware Alerts Detected					

Recent FTP Viruses detected

Time	User	Domain	Name
No Virus Detected			

Recent IPS Alerts

Time	Src/Dst	Signature Name	Severity	Action
Fri 29 Apr 2016 15:44:36	80.101.107.165/192.168.1.26 (N/A)	(snort_decoder) WARNING: ICMP Destination Unreachable Communication Administratively Prohibited	Moderate	Drop
Fri 29 Apr 2016 15:40:01	41.182.136.154/192.168.1.218 (N/A)	(snort_decoder) WARNING: ICMP Destination Unreachable Communication Administratively Prohibited	Moderate	Drop
Fri 29 Apr 2016 15:39:22	41.182.136.154/192.168.1.218 (N/A)	(snort_decoder) WARNING: ICMP Destination Unreachable Communication Administratively	Moderate	Drop

Web and Application Filter	Subscription Expired
IPS	Subscription Expired
Gateway Anti Virus	Subscription Expired
Gateway Anti Spam	Subscription Expired
8 x 5 Support	Subscription Expired
24 x 7 Support	Unsubscribed
WAF	Unsubscribed

Today Usage Summary

HTTP Hits	95371	
Search Engine Queries	Google : 217	Yahoo : 1

DoS Attack Status

Attack Type	Source		Destination	
	Applied	Traffic Dropped	Applied	Traffic Dropped
SYN Flood	No	0	No	0
UDP Flood	No	0	No	0
TCP Flood	No	0	No	0
ICMP Flood	No	0	No	0

Figure 7: Firewall Details on Recent Malware, FTP Viruses, IPS Alerts and Status of DOS Attacks

APPENDIX 1: EXTERNAL AND INTERNAL THREATS

Table 1: External Threats

Types of Threats		Description
Malware	**Virus and Worm Threats**	Virus is a self-replicated program that spread by attaching copies itself into already existed programs to reproduce many copies itself whereas Worm does not requires a host program even it also replicates by itself. Virus having humorous, innocuous, altering of data and catastrophic behavioral categories. It might disrupts the operating system or applications. Worms designed to propagate through a network.
	Trojan Horse	It comes as a hidden and a safe program which accidently install to the computer and it sabotaged later. Hackers steal confidential information (personal or financial) through Trojans which creates “backdoor” to the information systems and also it can be controlled remotely by a hacker.
	Spyware	This installs without any consent similarly as adware, Trojans and monitors behaviors of accessing the Internet. Through displaying an Ad it downloads the malicious software with bugs which can be caused to an unstable of application or a programme.
Denial-of-Service (DoS)–		May cause in system crash or inability to perform general functions due to the large number of requests or connections to the target.
Un-authorized Access/Users	**Hackers**	They steal confidential information, modify or destroy information by breaking information/computer systems to their personal gain. Hackers are a form of a cyber-terrorists. Black hats hackers violate computer security for personal gains where as white hats hackers are the security experts etc.
	Crackers	Black hats hackers are called as Crackers who has skills and knowledge with computers to obstruct with the confidentiality, integrity and availability of information security systems. Bringing direct harm to information systems is the main intention of Crackers.
	Social Engineering/Phishing Threats	It attempts to steal confidential and financial information through instant messages or fake emails.
Natural Disasters		There are various natural disasters caused severe damaged to information systems. Some of the possible disasters are Earthquakes, Tidal Waves (Tsunami),floods, earth slips, fire (forest fire), lightning, cyclones and also, due to animals and wildlife.
Man-made Disasters		The intention of the man-made disasters impact the infrastructure of the information system which includes riots, civil wars, bomb attacks, and terrorist attacks.

Table 2: Internal Threats

Types of Threats	Description
Human-made threats	Physical faults, interaction faults and developmental faults, are some of the human actions that caused for system faults. • Development Faults – occur during software development and these errors remain undetected throughout hardware development and normal programme. Eg. Software bugs. • Physical Faults –types of faults which affect hardware components. Eg. System failure. • Interaction Faults – arise due to human errors during external interactions on the system. Eg. Mistakes by systems operators or data entry operators, maintenance personnel and others with access to system
Information Disclosure and Unauthorized Modification	It results in loss of credibility of the customers or stakeholders, market share, reputation of the organization by divulging confidential or sensitive information such as health information. Modification of information and software without unnoticeable/undetectable which will be lead the system output even to make the wrong decisions.
Technological Threats	Mainly deals with software and hardware defects of the information system. • Component defects, e.g. failure of hard disks or switches, cable breakage etc. during runtime leading to immediate failure. • Hardware defects/errors in software components can remain undiscovered for a long duration and may not become a problem to run the system. E.g. systems are restarted or a certain constraint applies. • Software errors can cause a system to fail. Eg. an update of the operating system of a central security component can lead to a system malfunction after a required restart.

APPENDIX 2: COUNTERMEASURES WHICH CAN BE TAKEN TO ELIMINATE EXTERNAL THREATS

Table 3: Countermeasures which can be taken to eliminate external threats

Types of Threats		Countermeasures
External	Malware(Virus, Spyware, Adware and Trojans)	• Install Spam Filters Eg. Spam fighter for Outlook and Outlook express • Install Antivirus Software Eg. AVG, Symantec, McAfee, VIRUS fighter…. • Install Antispyware Eg. McAfee Antispyware module, S&D, SPYWARE fighter…. • Use of additional controls, such as firewalls and VPN solutions.
	Unauthorized Access (Hackers, Crackers, Phishing)	• Setup a firewall to eliminate hacking into information system, which filters incoming data through the Internet to network or information system. • Setup a Honeypots system to monitor behaviour of intruders
	Denial-of-Service (DoS)	• Installation of intrusion detection systems (IDS) to detect attacks and trigger alarms via alternative channels. • Use of dedicated, cabled connections for critical applications. • Strict configuration of network access points and communication channels.
	Natural Disasters (fire, flood, earthquake, hurricane, tornado, tsunami, infrastructure failure and etc.) Man-made Disasters (Terrorist attacks etc.)	• Valuable Information store redundantly and backed up on more than one piece of media. • Backups and disaster recovery plans are needed to avoid catastrophic media loss from natural disasters and sabotage.

Table 4: Countermeasures which can be taken to eliminate internal threats

Types of Threats		**Countermeasures**
Internal	Technological Threats Hardware and Software errors/failures	• Take procedures for system recovery, and regular backups • Use of tests to test patches, updates and new software components before install on production systems. • Introduce Redundant Array of Independent Disks (RAID) which are having more data protection, fault tolerance feature, efficient data access, reliability, and high speed.
	Disclosure of Information	• Secure the server to client connections – POP, IMAP over SSH, SSL – https access to webmail – Protection against insecure wireless access • Use strong authorization. • Use strong encryption. • Secure communication links with protocols that provide message confidentiality.
	Unauthorized Access/Modification	• Use strong passwords for all account types. • Use standard encryption to store sensitive/confidential information in information systems. • Use access controls and File Encryption Program to safeguard the confidential data in information systems • Setup an Intrusion Detection System to monitor the behavior of unauthorized users • Use Logical Access Controls Eg. Role based access controls, Identity/Authenticity, Time, Location, Transaction, Service Constraints and Common Access Modes such as Write, Read, Delete, Modify, View privileges