A Critical Analysis of Information Security -A Case Study of Cognizant Technology Solutions

Anvar Shathik J.[1, 2] & Krishna Prasad K.[3]
[1]Research Scholar, Srinivas University, Mangaluru, Karnataka, India
[2]Assistant Professor, Department of Cloud Technology and Data Science,
College of Engineering & Technology, Srinivas University, Mukka, Mangaluru, India
[3]College of Computer Science and Information Science, Srinivas University, India
Email: anvarshathik@gmail.com

Area of the Paper: Computer Science.
Type of the Paper: Research Case Study.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed In: OpenAIRE.
DOI: http://doi.org/10.5281/zenodo.3928673.
Google Scholar Citation: IJCSBE.

How to Cite this Paper:
Anvar Shathik, J. & Krishna Prasad, K. (2020). A Critical Analysis of Information Security -A Case Study of Cognizant Technology Solutions. *International Journal of Case Studies in Business, IT, and Education (IJCSBE), 4*(1), 155-171.
DOI: http://doi.org/10.5281/zenodo.3928673.

International Journal of Case Studies in Business, IT and Education (IJCSBE)
A Refereed International Journal of Srinivas University, India.

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

A Critical Analysis of Information Security -A Case Study of Cognizant Technology Solutions

Anvar Shathik J.[1, 2] & Krishna Prasad K.[3]
[1]Research Scholar, Srinivas University, Mangaluru, Karnataka, India
[2]Assistant Professor, Department of Cloud Technology and Data Science,
College of Engineering & Technology, Srinivas University, Mukka, Mangaluru, India
[3]College of Computer Science and Information Science, Srinivas University, India
Email: anvarshathik@gmail.com

ABSTRACT

Security was not a major concern of the past in Information Technology Organizations. But presently, due to the vast growth in fraud and hacking techniques, the security of organizations is a great concern. Organizations usually spend millions every year just to protect their environment and to maintain security. Yet, no company claims to be a hundred percent secure as fraudulent techniques are more tricky and latest. As the hackers are becoming hard and tricky, the major Information Technology (IT) Organizations are willing to pay a large sum of money for providers offering services of enterprise security schemes. The hackers are always ready to intrude into the company's valuable information sources. As per the recent survey by 'Security Week', nearly seventy percentages of respondents have faced a security threat which ended up in the loss of valuable information or the collapse of functioning last year. An employer of the company can indeed be a major attacker than an outside intruder. An employee of the company is already having all privileges to use resources of the company while various other ways are needed for an outer intruder for accessing the same company's network or data. Cisco, the networking giant has a major focus on Enterprise Security Policies. The company has seen a valuable improvement in the last few decades, which shows the importance of security. Cisco had recently released data that showed a lack of security policies in about 23 percentages of companies worldwide. More than 70% of Information Technology persons say that their organizations lack behind in areas of security policy. Large numbers of IT people fail to practice security policies as they are not easily understandable. For every organization, policies are the building blocks. They function as road maps which each employee of the company uses in various ways. Developing a well-defined policy requires artistic skill. Federal agencies have a Statutory obligation is available for federal agencies for maintaining day-to-day security policies. The primary Information Security Officer (ISO) is usually pledged for implementing these policies and the Chief Executive Officer (CEO) of the Company as well. The best security policies consider the vision and mission of companies, the important assets that need security, and security threats imposed against certain factors. All these come under risk management which needs defect identification by business impact policies. The weakness of a company has to be identified to find the vulnerability ratio of that company. Designing a security policy is not a nightmare once the major scope of policy design is identified. The major challenge lies in identifying the scope and threat areas for security policy. The policy is nothing but a collection of guidelines and procedures on what and how it can be implemented. In this paper, we are analyzing how Cognizant Technology Solutions (CTS) maintaining its standards, policies, technologies, and management policies which are defined for securing data of an organization.

Keywords: Security, Information Security, Cyber security, InfoSec, Security Analysis, Cyber threats, Vulnerability, Security policy, Cloud Security, Cyber Maturity.

1. INTRODUCTION :

For information technology organizations, security was not a major concern of the past. But the protection of companies is still a major concern because of the large growth in fraud and hacking techniques. Each year, companies normally spend millions only on environmental protection and safety. Yet no company claims to be 100% free as fraudulent methods are more complex and latest. Thanks to the complex and complicated activities of the hackers, the big IT companies are ready to pay large sums for vendors providing client security services. The hackers are always ready to enter valuable data sources of the business. In compliance with receipt [1]. In the last few decades, this business has seen a significant improvement, demonstrating the value of the security. Cisco recently released data indicating that around 23 percent of organizations worldwide had a lack of security policies. About 70 percent of IT people say that there is a lack of safety policy in their organizations. Many IT workers refuse to enforce security policies because they are not easily understood. Policies are the building blocks for each organization. They serve as road maps which are used in different ways by each employee of the company. To establish a given strategy, you have to have an artistic ability. Federal authorities have a legal responsibility to implement day-to-day security policies for federal agencies [2]. The primary information security in charge, and the Executive officer in chief of the organization, are largely responsible for implementing these policies. The best safety strategies take into account the vision and purpose of businesses, critical resources that endanger security and protection. All of these are subject to risk management, which includes business impact strategies to recognize defects. The weakness of a company has to be identified to find the vulnerability ratio of that company. Designing a security policy is not a nightmare once the major scope of policy design is identified [3]. The major challenge lies in identifying the scope and threat areas for security policy. The policy is nothing but a collection of guidelines and procedures on what and how it can be implemented. In this paper, we are analyzing how Cognizant Technology Solutions (CTS) maintaining its standards, policies, technologies, and management policies which are defined for securing data of an organization [4]. The major expectations for defining an enterprise security policy are:

1. Knowledge about the company
2. Identification of scope as well as agenda
3. Identification of targeted audience
4. Keeping it general, high and broad
5. Making sure that policies are quickly translated to guidelines and procedures
6. Awareness of outside drivers
7. Realistic approach
8. Ensuring backups
9. Avoiding controversies

2. OBJECTIVES :

1. To identify and analyze the security issues and different threats in an organization
2. To analyze the cyber threat defense and how it helps to build security into new applications.
3. To analyze the Security testing and security Myths in an organization.
4. To identify the steps to prevent cyber-attacks by using penetrating testing.
5. To identify the essential steps to keep security testing effective and affordable

3. RESEARCHMETHODOLOGY :

This research was carried out concerning the on-line scholarly documentation and the company's websites related to information security. By properly reviewing the many journal papers and the documents from the various web resources, the relevant data are collected and conceptually analyzed the security threats discussed in various journals and web resources, Formulated the operative design and to keep security testing effectively. This paper discussed some threats and steps to be taken to prevent threats.

4. RELATED WORKS :

The introduction of information security policies that define requirements, limitations, and obligations for information users and technical tools with a view that promoting avoidance, identification, and sensitivity to security incidents is a basic proposal to resolve the threat related to these circles [1]. Information Security is one of the highest demanding and interesting professional growth in the world today. Information protection is referred to simply as InfoSec and refers to the access, use, release, interruption, alteration, inspection, recording, or destroying of information against unauthorized access [2], [3]. Cognizant Technology Solutions (CTS) maintaining its standards, policies, technologies, and management policies which are defined for securing data of an organization [4]. The study shows that competitive stresses, regulatory stresses, and mimetic pressures have a positive impact on compliance with IS in a company [5]. Penetration testing is a systematic security evaluation that determines the security weaknesses of a network from software to infrastructure used for network operations by hackers. This will help to safely evaluate and determine vulnerabilities of operating systems, infrastructure, and applications by malfunctioning, unsafe coding, poor design, and misapplication of safety policies and methods [6][7]. Effective encryption is proposed to prevent a leak and can withstand high rates of ongoing leakage in semantic encryption. It can build such a security system by dissimulating partial code text in such a safe manner that we cover the secret key with a little more hardware security [8][9]. One of the key components of Cognizant's Security Testing Service is to provide full security testing services, guarantees that the systems are secure from safety risks and that customers are protected from information and confidentiality [10]. Cyber Threat Defense (CTD) is a scalable, next-generation security service to allow businesses to cope with the lack of time, resources, and security skills. This platform model is designed to operate seamlessly with leading providers of public cloud, making it easier for businesses to move from new software architectures to new regulatory requirements [11]. Suggested model of attack to explore security by using terms such as goals, actors, assault, Tactics, Techniques, and Procedures (TTP) actors threatened and their interrelationships. The STIXviz instrument is used to show the applicability of the smart grid network model assaults and the mechanism to collect intelligence threats [12][13]. Core Unified Risk Framework is an excellent approach that is used to compare the various methods by introducing new problems and tasks for each method examined [14]. We can change the internet architecture to reduce the risk of data attacks. By linking to yourself, instead of the Internet, if we talk about several organizations, they are safe from attacks. The Network Security can be simple or complex depending upon the requirements [15].

Table 1: Researchers contribution to Information Security

S.No.	Year	Author(s)	Findings/Focus
1	2007	Sattarova Feruza Y. & Tao-hoon Kim [19]	Component Security Assurance furnishes the illustrative depiction of some inter models such as the security system model, security module assurance demonstrates the relationship between e-business and model security.
2	2014	Rajinder Singh & Shakti Kumar.[20]	The architecture of the Internet can be modified to avoid risk and attack. Many organizations are protecting themselves by modifying the self to the intranet by avoiding the Internet to free from attack.
3	2017	Gaute Wangen *et al.* [21]	Core Unified Risk Framework is the intelligent approach which is used to compare the various methods by introducing new problems and tasks for each method examined
4	2018	Mario Luca Bernardi *et al.* [22]	The novel approach was established which is based on process mining techniques to the identification of complex malware and malware phylogenies. The reporting model, known as SEF, collects traces of malware and trustworthy applications from systems

			that constitute a fingerprint for their complex behaviour.
5	2019	Qiyu Wu *et al.* [23]	Suggested a secure, publicly verifiable cloud storage data stream outside-sourced system, namely DSO-PVI. It is suitable in the framework for offshoring unlimited outsourcing data streams and anybody with the public or a general key can able to test the sustainability of the query results obtained by the cloud server.
6	2019	Abel Yeboah-Ofori & Shareeful Islam [24]	Proposed attack model to examine the protection of these structures using concepts such as aim, actors, attacks, TTP, threat actors, and their interrelationships. STIXviz tool is used to prove the applicability of the model attacks in the smart grid network and organizational structure for gathering threat intelligence.
7	2020	Danie Schlette *et al.* [25]	Cyber threat intelligence yields significant information about cyber threats. A remarkable aspect of practical application has been the exchange and collaborative generation of CTI through sharing platforms. CTI aids to identify the attack and prevent them.
8	2020	Jia Xu1 & Jianying Zhou [26]	Efficient encryption is a semantic-safe encryption scheme proposed to avoid leakage that can withstand high continuous leakage. It manages to construct such a security scheme by concealing partial ciphertext so safe that we cover up the secret key by using a little more security hardware.
9	2020	Li, W., Wang, Y., Li, J. *et al* [27]	Challenge trust mechanisms can measure the confidence of the node by assessing the link between the challenges sent and those received.
10	2020	Iraklis Leontiadis & Ming Li [28]	The cryptographic technique is proposed with three convertible tags which are converted the data into key then convert the previous layer to the next layer from an untrusted converter.
11	2020	Sun, L., Xu, C., Zhang, Y. *et al* [29]	The consumer uses only symmetric primitive keys to process the whole information, and only the offshored data has to be stored by the server. It often frees consumers of the high cost of measuring the authenticator and reduces the overhead power considerably.
12	2020	Mahsa Nooribakhsh *et al.* [30]	Some factors that influence the performance of DDoS attack-detector systems are the consumption of the memory, computer expenses, and fidelity of the threat to the location of the threats and observation.

5. OVERVIEW OF THE CHOSEN COMPANY :

Cognizant is an American international IT services company, providing electronic, technical, consulting, and administrative services. Cognizant is part of the NASDAQ-100 and CTSH exchanges. Headquarter was established in Teaneck, United States of America (USA) in 1994. It served external customers in 1996 as Dun & Bradstreet's internal Engineering unit. The initial public offering took place in 1998succeedingin a series of corporate reorganizations. After the Y2 K and DOT-K boom of the early 1990s, the company grew through vital software growth and maintenance support, as companies concentrate on difficult business metrics, such as income and revenue. Cognizant had a rapid growth phase during the 2000s and in 2011 it became a Fortune 500 company. [8].

5.1 BUSINESS MODEL

Cognizant announced the Chennai branch as the head office and overseas delivery center. Just like many other IT service companies, Cognizant pursues a worldwide R&D and Off-Shore Outsourcing model of service. The firm operates several offshore production facilities in the US, Europe, and South America outside the United States and close to the shores. Early years, Cognizant became active with the support of the Dun & Bradstreet brand in several American and European businesses. The senior managers of the company considered the company a high-end customer service provider at the same level as the six main modern system integration systems, but at reduced rates [9].

5.2 SERVICES

Cognizant offers IT services, information security services, consultancy services, ITO services, and BPO services. These include analytics, integration of technologies, supply chain management, business & technology consulting, company information, digital enterprise, application development & maintenance, services for IT infrastructure, company resource planning, storage of information, client relations management, outsourcing for research & development, engineering & production services, and testing services. Cognizant has three major company sectors are digital systems, digital innovation, and technology [10].

5.3 SERVICE LINES OF CTS

Software Provider, Online Company, Business Products, Virtual Marketer, CRM Advisory, Health Care IT, Smart devices, Internet, Project Management, HR Services, Customer Experience, Facilities, Digital Technology (Innovation and User Design), BPO Service, Phone, and Web Apps. Digital insurance, Insurance Payer Technology, Business Profit pattern Systems, accounting consulting services, financial management services, financial services, automation of sales, recording of the drug, advertising, engineering SAP consulting, mortgage processing. Operation of the Oracle Retail Merchandising, scheduling and development suite, Business consulting for entertainment and entertaining businesses, System integration, Life Sciences Analytics, Program &Project management consultancy. [10].

5.4 EMPLOYEE COUNT AND BRANCHES

Cognizant has expanded its branches in 166 locations all over the world. The total count of the employees is 281600, according to the year 2018 and operations in over 37 countries. The company employs 15000 people in India but in Chennai alone, it has more than 50,000 at different locations. The remaining business centers in India are Bangalore, Coimbatore, Gurgaon, Noida, Kochi, Kolkata, Mangalore, Mumbai, and Pune. Other business centers include the UK, Hungary, the Netherlands, Spain, China, Philippines, Canada, Brazil, Argentina, and Mexico. [12].

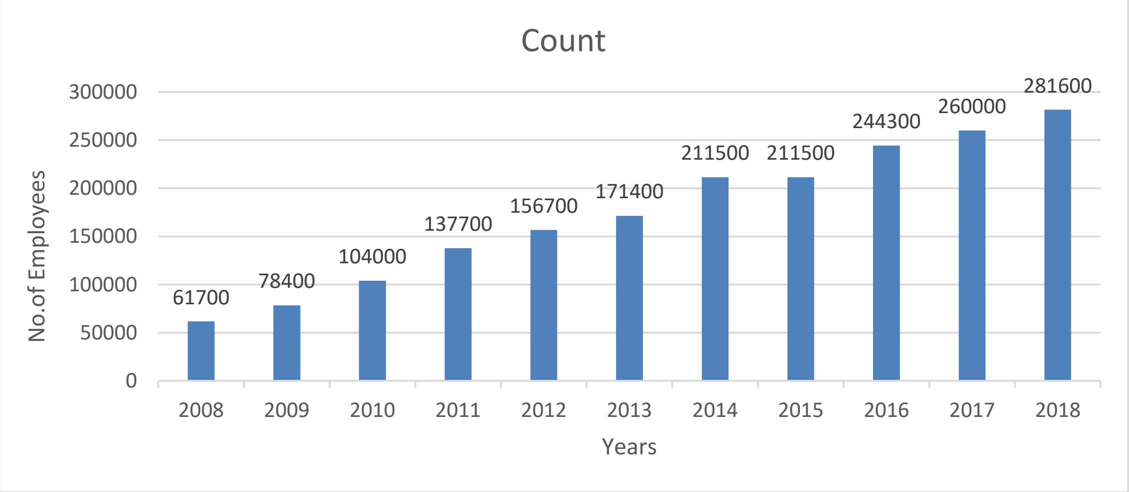


Fig.1: Employee growth over the years [12]

5.5 DATA CENTERS

In 2012, the company will be able to optimize the technology for a range of applications. It has named the Virtual Data Center Service (VDCS), a managed on-demand platform that provides true company computing in a cloud-based environment. VDCS is built on a best-of-breed infrastructure that features facilities, network, security, compute, storage, and hosting area network connectivity — all monitored and managed to ensure the multi-tiered security, robust quality, and superior service levels you seek in a customized cloud solution [7]. The cloud services team will have the ability to define, customize and deploy your digital data center in several hours, on request. In 2015, Cognizant surveyed 15-plus global companies across industries, including life sciences, retail, manufacturing, and technology, with revenues over two billion. The results of the survey revealed important takeaways on Bring Your Own Device (BYOD), adoption and associated policies. For example, only five of the companies surveyed had well-defined BYOD guidelines for all device formats (e.g., mobile, tablets, and laptops) and user types. BYOD programs were predominantly focused on mobile devices; Contingent workers who were not on the payroll were largely excluded from the program [9].

6. ANALYSIS OF SECURITY TESTING :

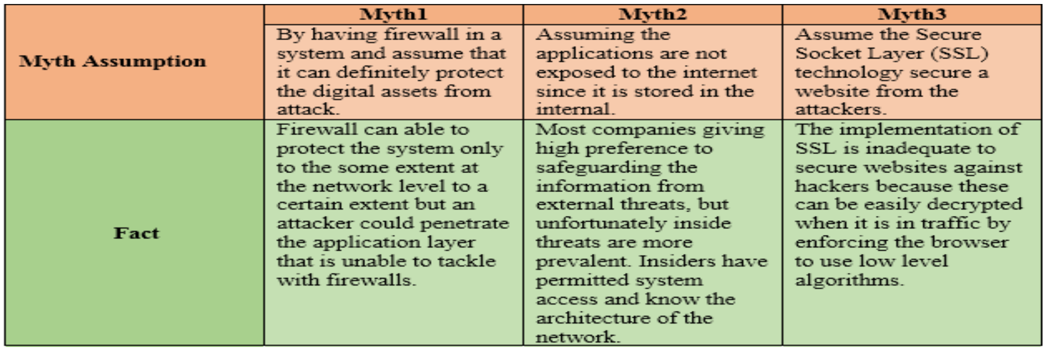
Evaluating IT systems and network vulnerabilities is a difficult task in today's digital interconnected world. Through the following best practices and protocols for penetration testing, companies can tackle safety gaps proactively and efficiently until hacking destroys consumer trust, brand reputation, and financial well-being [10]

6.1 ABOUT COGNIZANT SECURITY TESTING

Security Testing Service is one of the most important components of Cognizant Security. It also offers end-to-end security testing services, guarantees that IT systems are secure from security threats, and that information and confidentiality are secured from their clients [6]. The group includes more than 300 accredited safety testers who successfully delivered safety test commitments to more than 100 customers. The emphasis of application security assessments is the comparative analysis of vulnerabilities against a variety of criteria, including the top ten list OWASP (open web application security). The tools for security testing avoid safety weaknesses in the modern digital world and boost the organization's power [11].

6.2 REPUDIATION OF SECURITY MYTHS AND WORKING

Across every field of the new digital world today, data plays an important role and proactively plugging vulnerability. Organizations also implemented more efficient ways to provide data and software resources to end-users in and outside their firewalls quickly and safely. Safeguarding these large amounts of data from cyber-attacks for most organizations is a lengthy process. Although most organizations are introducing firewalls, SSL encryption, and security policies, they still experience cyber-softbacks now and then [10][12]. The above events show that cyber-attacks are not industry-specific and can cause business interruptions and, potentially, violate product privacy or cause financial harm which could threaten any company's very life. Attacks involving client data loss and a steal of significant firm data start with the discovery that the company was infiltrated, and then there are questions about the damage caused by the breach. Already too delay to protect the firm and its customer's early security testing can help companies find weaknesses in the software and infrastructure before cybercriminals hit. Periodic penetration checks help unravel the current security status of the company. Early safety testing can help companies detect application vulnerabilities and infrastructure before cybercriminals hit the software development process [12].



	Myth1	Myth2	Myth3
Myth Assumption	By having firewall in a system and assume that it can definitely protect the digital assets from attack.	Assuming the applications are not exposed to the internet since it is stored in the internal.	Assume the Secure Socket Layer (SSL) technology secure a website from the attackers.
Fact	Firewall can able to protect the system only to the some extent at the network level to a certain extent but an attacker could penetrate the application layer that is unable to tackle with firewalls.	Most companies giving high preference to safeguarding the information from external threats, but unfortunately inside threats are more prevalent. Insiders have permitted system access and know the architecture of the network.	The implementation of SSL is inadequate to secure websites against hackers because these can be easily decrypted when it is in traffic by enforcing the browser to use low level algorithms.

Fig.2 : Security Myths [12]

6.3 PENETRATIONTESTING

In a nutshell, penetration testing is a systematic process that determines a system's safety vulnerabilities, from software to infrastructure which hackers use for system operations. This helps to analyze and test the weaknesses in operating systems, services, and software safely by malfunctioning, unsafe coding, poor design features, and misapplication of security policies and procedures [2]. It is also an attempt to evaluate them. Penetration checks protect consumers from cyber-attacks on company assets. Clients can be protected from cyber-attacks by penetration testing. The vulnerabilities found by standards Open Web Application Security Project (OWASP), System Admin, Audit, Network, and Security (SANS), and Open Source Security Testing Methodology (OSSTM) are specified. This testing also helps industry heads to realize the real-world effect of such vulnerabilities [14].

Penetration screening can be used to prevent this from happening.

1. Identify security violations that can lead to business loss.
2. Ensured that systems adhere to industry standards and regulations including ISO 27001 PCI DSS, NIST, FISMA HIPAA, and Sarbanes-Oxley.
3. Allow a corporation, through its commitment to proper due diligence and enforcement, to avoid punishment for non-compliance

6.4 PROCESS OF PENETRATION TESTING

The process of penetration involves the different steps and methods to perform the testing [11].

6.4.1 Steps involved in Penetration Test:

Planning: The initial step is to decide the nature and goals of the test to be conducted and to specify test methods. Additional details were also required, such as the network, domain name, etc.

Scanning: The next step is to understand how different intrusion attempts would respond to the target application. Generally, that is dealt with.

Static analysis: A specification for the program is tested to find out how it operates. I will search the entire code in a single pass. Dynamic Analysis: Code scrutiny of an executing application. It is the best convenient method of scrutinizing because it enables the application output to be displayed in real-time.

Access Control: This process employs an Internet applications threats to detect the vulnerabilities of the aim, namely site scripts, Structured Query Languages injections, and unauthorized. Testers then try to use these vulnerabilities to realize the harm they might cause, typically using the increased privileges, data robbery, traffic interception, etc.

Managing Access: The goal is to check whether the weakness may be utilized to maintain an enduring existence in the pattern being exploited ample time to enable a dreadful actor to acquire profound rights or not. The concept is to mimic sophisticated persistentmenaces, which frequently linger in a network for months to access the company's most important data.

Analysis: The detailed report will be obtained by using the penetration test such as Specific exploited vulnerabilities, accessed sensitive data, and the time the pen check will remain undetected in the network. This information is analyzed by the security staff for the protection against future attacks to help configure the WAF settings of a firm and other application security options.

6.4.2 Testing Methods

There are different methods are existing to perform the Penetrating Testing [12].

External Testing

External penetration tests are targeted at an on-line asset of a client such as a web application itself, the organization's Web site, and DNS. The goal is to collect useful data and access it.

Internal Testing: An internal check simulates a malicious intruder attack by a tester behind its firewall, with access to the code. This isn't just about simulating a creep employee. An employee whose authorization was compromised as a result of a phishing attack may be a situation that can begin.

Blind Testing: In a blind test, a tester only gets the client's name. This enables the security analyst to examine how a real application attack would occur in real-time.

Double-blind Testing: Security workers are not previously familiar with a pretended attack in the test. As in the real world, they'll have no time to defend themselves before an attempted break.

Targeted Testing: In this testing, all the testers and security analysts are working together to keep their behaviour calculated. This is a valuable training exercise that gives security team feedback to the hacker in real-time.

6.4.3Safety assessment methodology.

The following safety assessment criteria include the safety evaluation methodology:

1. Open Web Application Security Project (OWASP)
2. OWASP Application Security Verification Standard (ASVS).
3. System Admin, Audit, Network, and Security (SANS)
4. Open Source Security Testing Methodology (OSTMM).
5. Web Application Security Consortium (WASC) guidelines.

Web Application Security Consortium (WASC) for Web Application Protection Consortium. Such guidelines describe penetration testing using the following steps: hackers that can jeopardize web applications protection would not only gain access to sensitive data but also gain access to the key for the corporate information architecture [12].

7. FORMULATING AN EFFECTIVE STRATEGY :

A systematic safety check methodology can help detect vulnerabilities in systems and networks. Understand the security architecture and check the software instead of concentrating on OWASP and SANS vulnerabilities.

Verify that the program has followed main security standards like:

1. Safe failure.
2. Profound security.
3. Privileges isolation.
4. Reasonable right.

The solution will include screening for all grades and horizontal layers of a multi-plus architecture, including network, OS, database container frames, and the client container housed in the framework. Fire Walking: sending out generated network packets to predict the Firewall rules. Important sample tests are: [6]

- Penetration checking for a web application.
- Evaluation of Web Service.
- Penetration checking of the file.
- Penetration check for the network.
- Checks for OS hardness

Ideally, checking all the grades and components involved is a good practice but there is little time or budget to carry out all the tests [10]. The hazard analysis can be conducted in such situations:

1. Analyze the magnitude of changes to each process.
2. Analyze threats in the same components from previous safety scans.
3. Evaluate a risk warning on specific components.

The optimal level of security verification is cost-effective through a risks-based comprehensive approach [14].

8. THE OUTLAY OF SECURITY :

The value of security accidents is determined by the kind of accident and the number of events. In particular, year after year, safety accidents are rising. The best important kinds of events include Worm, spyware, and other malicious programs, according to security software provider Kaspersky [10].

- Existing software insecurity.
- Accidental or non-accidental data sharing by workers.
- Phone worker’s failure or theft.
- Intrusion or intrusion of the network

Compared with the price of protection, the cost of a security violation will always be prohibitive. A constantly changing countryside of threats harms today and future security budgets. Kaspersky also confirmed that “about 90 percent of organizations work with confirming that they regularly face incidents of protection that range from malware threats to DDOS attacks to forced intrusion attacks [11].

8.1 PHISHING -

This type of attack involves trapping or enticing a person to disclose responsive information in electronic communication for malicious goals. The simplest example is the “Nigerian message” scams in this category [12].

8.2 MALWARE

Malicious software attacks occur if small portions of code, or standalone installable code, are entered and run according to a default cause or case, causing more complex data or processing infringements wherever they happen. One of these is the malware attacks by the “Dyre or Dridex Trojan” which involves redirection using an MS Office attachment that contains an infected macro [13].

8.3 DDOS

One of the most effective weapons on the Web is a distributed denial-of-service (DDoS). The way to work here is essential to overload a website by hitting existing IP addresses with an inundation of service requires to stop the website’s infrastructure from being modified and result in a website failure. Banks and financial institutions were faced with a variety of such attacks each week [08].

8.4 PREMEDITATED HACKING

Such advanced types of continuous threats include attempts to target or steal faulty intellectual properly from a website or request. The attacker uses a combination of phishing, ransomware, and attacks on DDOS. This kind of threat generally succeeds if the intruder can gain a view of network operations, authorized IP addresses, and exits and take advantage of inherent vulnerabilities to access non-encrypted confidential data [10].

8.5 NETWORK “WORMS”

Travelling networks are primarily virus links for traveling data packages which are either distributed or used for computer memory by launching remote copies of the same program. In addition to the most common kinds of attacks, most app-based attacks, including Structured Query Languages injection, authentication, and hash cracking and cross-site scripting, are used. The figure provides a list of things that should be included in vulnerability assessments when looking at applications [12].

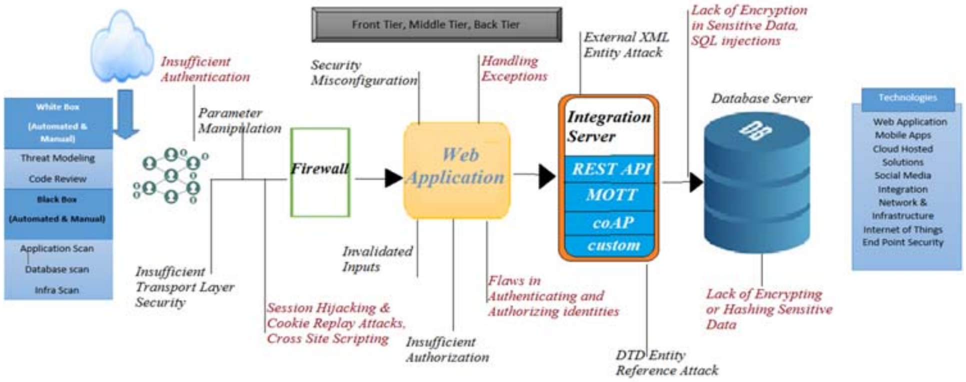

Front Tier, Middle Tier, Back Tier
White Box (Automated & Manual)
Threat Modeling
Code Review
Black Box (Automated & Manual)
Application Scan
Database scan
Infra Scan
Insufficient Authentication
Parameter Manipulation
Security Misconfiguration
Handling Exceptions
External XML Entity Attack
Lack of Encryption in Sensitive Data, SQL injections
Firewall
Web Application
Integration Server
REST API
MOTT
coAP
custom
Database Server
DB
Technologies
Web Application
Mobile Apps
Cloud Hosted Solutions
Social Media
Integration
Network & Infrastructure
Internet of Things
End Point Security
Insufficient Transport Layer Security
Session Hijacking & Cookie Replay Attacks, Cross Site Scripting
Invalidated Inputs
Insufficient Authorization
Flaws in Authenticating and Authorizing identities
DTD Entity Reference Attack
Lack of Encrypting or Hashing Sensitive Data

Fig.3 : Assessment of Potential Threats [12]

9. KEEPING SECURITY TESTING EFFECTIVE AND AFFORDABLE :

The overall quality control plan must contain a large part of the costs of combating cyber-crime. Nonetheless, true penetration testing depends on the organization's dynamic technology scenarios as well as the human and manual resources demanded to supply and to finish an effective testing approach. IP-based testing is one such process. To demonstrate consider the most difficult patterns for penetration testing involve an in-depth grasp of workload flows through Internet Protocol addresses posing a security attack. After the traffic volume is measured, a cost per testable service can be estimated, depending on the networks linked to the external network [1].

9.1 SAST AND DAST DECODED

In addition to the penetration testing, the software and application levels are usually used in budgets for application design and implementation programs, including Static Access Security Testing (SAST) and dynamic access security testing (DAST). Because SAST and DAST are focused on software, the price of the tool license takes the larger portion of the cost. Pricing considerations frequently considered include but are not limited to: test code lines and the number of scans to perform; types of scanning scenarios; and "false positive" information tests and refusals as well as available help [11].

10. AI ENABLEDPLATFORM AND SECURITY PILLARS :

How a platform approach gets organizations off the treadmill of buying and managing multiple security tools. Organizations were expected to spend more than$114 billion on security products and services in 2018, growing to $124 billion in 2019, with the average organization utilizing more than 70 security products. At the same time, they were hit by more than 6,500 reported data breaches Stakeholders at every stage in the software development life cycle often start thinking about security and data privacy only at the end of the development process, by which time it’s seen as an obstacle to reaching the business goal [10]. They keep adding the latest and greatest technologies in reaction to the latest security threat but never invest in the staff and skills to manage them properly. And over time, they become stuck on a treadmill of more and more security spending for less and less protection. We believe there’s a better way: Proactive, end to end security that enables, rather than stands in the way of, digital transformation. It rests on four security pillars [11].

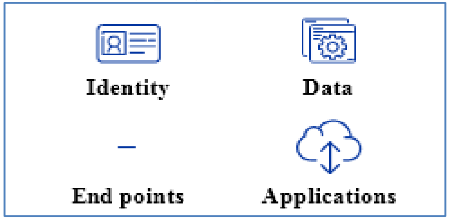


Fig 4. Four security pillars[11]

Each of these security requirements can be met by a cloud-based security platform that frees hard to find security experts from routine work so they can build relationships with business owners and makes security an enabler, not a blocker, of digital transformation. It also makes it easier for organizations to adapt to new business and technology models because the platform is customized to the needs of each leading cloud provider [10].

An AI enables platform automates routine tasks to ensure organizations use their current security tools to the fullest and frees scarce security staff to build relationships with the business. Up-front consulting helps ensure the organization is getting the most from its current tools while identifying gaps and areas for improvement.

Table 2: AI-enabled platform [12]

Pillar	Description	Enterprise's Lack	How a platform fills the gap
Identity	Verify employee or user is who they claim to be and have rights to access the system or data.	Robust user access management, including revocation of credentials upon leaving the organization. Robust privileged access management to protect access to critical systems. Data protection and credential management on employee-or contractor-owned devices, across In-house and cloud platforms and for users logging in through third-party platforms such as Facebook that can potentially track user activity.	Cognizant's Privileged Access Management as a Service (PAMaaS) provides all the planning, implementation, and ongoing management needed to protect your most sensitive accounts, in a flexible, as-a-service model around the world and across private, public and hybrid clouds. It provides higher levels of protection than many legacy solutions with significantly less delay and expense. It also delivers flexibility and scalability so you can grow as quickly as you need.
Data	End to end protection of data, in transit and at rest, with proper encryption and data management, from creation through erasure.	Inventory of corporate data and its sensitivity. Data protection policies, processes, and standards. Policies for data governance, access control, encryption, and encryption across in-house and cloud environments.	The trustworthy and customizable managed data security services portfolio of Cognizant helps companies safeguard their critical data with versatile, scalable, and highly adaptable authentication and tokenization solutions in the most efficient and compliant way.
End Points	Control access Cryptocurrencies to assure the security of any device that accesses corporate applications and data.	The complete and current inventory of endpoints, whether owned and managed by the enterprise or users. Processes and policies to track such devices over time and to ensure unauthorized devices can no longer access the corporate network after users dispose of them or move to another organization. Ability to secure traditional networks while migrating to hybrid and public clouds.	Managed Endpoint Detection and Response from Cognizant Security, provides strong 24x7x365 protection This software prevents threats at the beginning and monitors each file on your endpoints continuously. It detects even the new threats – files and code less – over time, not days, not months.
Applications	Assure applications are hardened against known attacks, patched upgraded to fight new ones.	A plan for older applications not suited to cloud migration that might be too expensive to rework. An understanding of how to secure new application architectures such as containers and micro services. Lack of control into and visibility of SaaS applications that business users adopt without informing IT.	Cognizant's Integrated Vulnerability Management as a Service integrates SAST, DAST, and continuous infrastructure vulnerability examine in a single solution that provides customers with comprehensive visibility into each potential exposure across their distributed network environment.

11. COGNIZANT CYBER THREAT DEFENSE :

Cognizant Cyber Threat Defense (CTD) is a flexible security service of the next generation that helps enterprises overcome the lack of money, time, and skills that hobble their security. This platform-based model is customized to work seamlessly with leading public cloud providers, making it easy for organizations to adapt to everything from new application architectures to new regulatory requirements [7]. CTD offers loads of log reports and warnings of effective, organizational workflows to help you reduce the most important threats. The time it saves automating everyday functions gives your security staff more time to build security into new applications and services from the start, becoming an enabler (rather than an obstacle to) digital transformation. Combined with up-front consultative offerings, CTD: [11]

1. Usually, the installation of one's safety center needs less cost and effort.
2. This offers an immediate and informed view of the security posture of the company through Cyber Threat Protection platform.
3. Entered auditions and advice on the optimal configuration of the system and assistance from Cognizant security experts ensure quicker, more cost-effective and safe safety enforcement and
4. Reduces the need for in-house security personnel to recruit and maintain.

12. SWOC ANALYSIS :

Information security plays a critical role in an organization and prevents the company's capability to operate. A SWOT analysis is a useful tool for guiding a company and providing strategic guidance both for Information security strategy and overall business goals. The strengths, vulnerabilities, opportunities, and risks facing agencies or organizations are included in this report.

Table 3: SWOC Analysis

STRENGTH	WEAKNESS
• Strong Network controls • Managing the entire security of an organization. • Vulnerability management • Securing the data from unauthorized access and data corruption. • Optimal balance of technology and management • Infrastructure systems with automated safety controls; • Track Record as Industry Pioneers • Able to monitor the Traffic and can protect against Trojans by using Firewalls, Anti-malware, and Anti-virus.	• Weak Application Security • Poor data reliability due to technical issues. • Highly rely on digital Communications • Poor Log Management • Leads to Security breach due to unauthorized access
OPPORTUNITIES	**CHALLENGES**
• To Manage IT Infrastructure in an Organization • To provide Security in cloud computing platforms. • Global Data Security Market is increased due to demand. • Increased in Market value of Cryptocurrencies • Huge development in Cyber vigilance and Digital Trust • Emerging opportunities for digital transformation.	• Digital Inputs are increased in all the areas. • Trends in Digital fraud is increased. • Continuous updating of Threat modelling in the cyber world. • Updating of Network Worms • Development in Hacking Technology. • Increase in Data breach activity. • Phishing Scams and Attacks on the rise Cybercriminals

13. DISCUSSION & SUGGESTIONS :

AI-enabled automates routine tasks is a platform that ensures organizations utilize their current security tools as far as possible, and frees scarce security personnel to build business relationships. Early consultation supports the organization while recognizing weaknesses and places to strengthen, to make the most of the existing instruments. A Cloud Security Platform that makes it difficult to find security experts in routine work can meet each of the above security requirements, allowing them to establish contacts with business owners and making security an enabler of digital transformation, not a blocker. It enables a significant building block for future theory building by using the combined approach to provide the study of security policies by organizations with the process and different views. While the current research body was important in shaping the information, we currently know about organizational safety policy, these lacunae and unstable point out areas in which researchers can create helpful inventions. At last, in the updated policy structure we are proposing a set of new guidelines that future studies should concentrate on. We suggest a simple metric to denote the data found in the STIX study to domain experts. For analysis and verification with the CTI platform data, a DQ metric for the relevant quantity of data should be explained. Besides, the quality assessment criteria for other CTI-formats should be reconfigured and incorporated into a coherent CTI data quality management methodology. Full implementation would likely pose additional issues with the chosen of appropriate algorithms and monitoring of user engagement and expectations apart and not discussed in the core DQ evaluation. Implementation and extension of the dimensions and metrics are important measures to eventually establish a coherent quality assessment framework for CTI including processes for assuring and enhancing the quality of objects on a shared basis.

14. CONCLUSION :

CTS provides security from the software to the infrastructure by using many ways such as penetrating testing, cyber threat defense, etc. In addition to the penetration testing, static access security testing and dynamic access security testing are focused on software. Cognizant Cyber Threat Defense (CTD) is a flexible security service of the next generation that helps enterprises overcome the lack of money, time, and skills that hobble their security. CTS also offers end-to-end security testing services, guarantees that IT systems are secure from security threats, and that information and confidentiality are secured from their clients. Periodic penetration checks help unravel the current security status of the company. Analyzed the different security threats, security Myths, security issues in detail. Penetration screening will be used to determine security violations that can lead to the loss of the business. The overall quality control plan must contain a large part of the costs of combating cyber-crime. True penetration testing depends on the organization's dynamic technology scenarios as IP-based testing well as the human and manual resources demanded to provide and finish an effective testing approach. In addition to the penetration testing, it also uses level security scanning called and static access security testing (SAST) and dynamic access security testing (DAST) to focus on software. A cloud security platform that frees security specialists from routines work to establish contacts with business owners and makes the security system an enabler, not a blocker, to digital transformation can meet the security requirements of the four security pillars such as identity, data, endpoints, and applications. AI enables a platform to automate the repetitive activities ensures that companies use their current security resources in full and enable limited security staff to create a business relationship. To secure the data CTS also provides the “Enterprise Security”. It is a collection of standards, policies, technologies, and management policies that are defined for securing data of an organization. In this technology world, information systems play a vital role in any company. Digital fraud and forensic management of CTS helps in taking cyber security to the next level. Cyber vigilance, cloud security, threat modeling in the cyber world, Cyber security roadmap, and architecture and maturity assessment are well-built security services of CTS.

REFERENCES :

[1] Cram, W. & Proud foot, Jeffrey & D’Arcy, John (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems (EJIS),* 26(6), 605-641. DOI: https://doi.org/10.1057/s41303-017-0059-9

[2] Stefan Marksteiner, Heribert Vallant, KaiNahrgang (2019). Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling. *Journal of Information Security and Applications (JISA*), 49, 102-389 DOI: https://doi.org/10.1016/j.jisa.2019.102389

[3] Mohammed Mahfouz Alhassana, Alexander Adjei-Quaye (2017). Information Security in an Organization. *International Journal of Computer* (IJC), 24(1), 100-116. DOI*:* https://doi.org/10.1515/dim-2017-0006

[4] W. Alec Cram, Jeffrey G. Proud foot, John D'Arcy (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems (EJIS),* 26, 605-641. DOI: https://doi.org/10.1057/s41303-017-0059-9

[5] Ahmed AlKalbani, Hepu Deng, Booi Kam-Xiaojuan Zhang, (2017). Information Security Compliance in Organizations: An Institutional Perspective. *Data and Information Management, (DIM), 1*(2), 104-114. DOI: https://doi.org/10.1515/dim-2017-0006.

[6] Cyber threat defenses in Cognizant (2019). Retrieved from https://www.cognizant.com/cognizant-digital- systems-technology/cyber security-services/cyber-threat-defense on 25/08/2019.

[7] Digital business and Digital Engineering of Cognizant (2018). Retrieved form https://www.cognizant.com/cognizant-digital-business/digital-engineeringon 15/08/2019.

[8] Infrastructure Services of Cognizant (2019). Retrieved from https://www.cognizant.com/cognizant-digital-systems-technology/infrastructure-services on 15/08/2019.

[9] Digital Infrastructure Services of Cognizant (2019). Retrieved from https://www.dealstreetasia.com/stories/cognizant-to-help-ntuc-fairprice-upgrade-digital-Infrastructure-8545 on 10/08/2019

[10] Latest thinking of Cognizant (2019). Retrieved from https://www.cognizant.com/latest-thinking on 12/09/2019.

[11] Security Testing and Cyber security (2018). Retrieved from https://www.cognizant.com/cognizant-digital-systems-technology/cybersecurity-services on 10/08/2019.

[12] Application security and Data protection (2018). Retrieved from https://www.cognizant.com/whitepapers/application-security-safeguarding-data-protecting-reputations-codex1869.pdfon 15/08/2019.

[13] Sustainability and Corporate Social Responsibility of Cognizant (2019). Retrieved form https://www.cognizant.com/about-cognizant/sustainability on 03/09/2019.

[14] Digital Innovation and Digital Workforce (2018). Retrieved from https://www.cognizant.com/digital- workforce-of-the-future on 25/08/2019.

[15] End to end application services (2019). Retrieved from https://www.cognizant.com/cognizant-digital-systems-technology/enterprise-application-services on 15/08/2019.

[16] Balancing the Blockchain Revolution and Block chain Adoption (2018). Retrieved from https://www.cognizant.com/enterprise-blockchain-solutions on 21/09/2019.

[17] History, Services and Business models of Cognizant (2018). Retrieved from https://en.wikipedia.org/wiki/Cognizant on 10/08/2019.

[18] Network Security & Vulnerable Security Aspects (2019). Retrieved from http://www.gjesr.com/august-2014.html on 55/08/2019.

[19] Sattarova Feruza Y. and Prof. Tao-hoon Kim (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering*, *2*(2), 17-32. DOI*:* https://10.12691/education-6-2-10

[20] Information Security in an Organization (2018) retrieved from https://www.researchgate.net/publication/314086143_Information_Security_in_an_Organization on 25/08/2019.

[21] Wangen, G., Hallstensen, C. & Snekkenes, E. (2017). A framework for estimating information security risk assessment method completeness. *International journal of Information Security,*17, 681–699. DOI: https://doi.org/10.1007/s10207-017-0382-0

[22] Bernardi, M.L., Cimitile, M., Distante, D. *et al* (2018). Dynamic malware detection and phylogeny analysis using process mining. *International journal of Information Security,*18(1)**,** 257–284. DOI: https://doi.org/10.1007/s10207-018-0415-3

[23] QiyuWu, FucaiZhou, JianXu & Qiang Wang (2019). Secure data stream outsourcing with publicly verifiable integrity in cloud storage. *Journal of Information Security and Applications*, *49*(1), 1-10. DOI: https://doi.org/10.1016/j.jisa.2019.102392

[24] Yeboah-Ofori, Abel & Islam, Shareeful (2019). Cyber Security Threat Modeling for Supply Chain Organizational Environments. *Future Internet*, 11(3), 1-8. https://doi.org/10.3390/fi11030063.

[25] Schlette, D., Böhm, F., Caselli, M. *et al* (2020). Measuring and visualizing cyber threat intelligence quality, *International Journal of Information Security*, *1*(1), 1-6. DOI: https://doi.org/10.1007/s10207-020-00490-y

[26] Xu, J., and Zhou, J. (2020). Strong leakage-resilient encryption: enhancing data confidentiality by hiding partial cipher text. *International journal of Information Security, 1*(1), 1-12. DOI: https://doi.org/10.1007/978-3-030-29729-9

[27] Li, W., Wang, Y., Li, J. *et al* (2020). Toward a block chain-based framework for challenge-based collaborative intrusion detection. *International journal of Information Security*, *1*(1), 1-7. DOI: http://10.0.3.239/s10207-020-00488-6

[28] Leontiadis, I., Li, M. (2020). Secure and collusion-resistant data aggregation from convertible tags. *International journal of Information Security,*1(1), 1-12. DOI: https://doi.org/10.1007/s10207-019-00485-4

[29] Sun, L., Xu, C., Zhang, Y. *et al* (2020). Public data integrity auditing without holomorphic authenticators from in distinguishability obfuscation. *International journal of Information Security, 1*(1), 1-8. DOI: https://10.0.3.239/s10207-020-00486-8

[30] Mahsa Nooribakhsh & Mahdi Mollamotalebi (2020). A review on statistical approaches for anomaly detection in DDoS attacks, Information Security Journal: *A Global Perspective*, *29*(3), 118-133. DOI: https://10.1080/19393555.2020.1717019

[31] Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014), Current challenges in information security risk management, *Information Management & Computer Security*, 22(5), 410-430. DOI: https://doi.org/10.1108/IMCS-07-2013-0053

[32] ___Tushar KantiSaha, Mayank Rathee, Takeshi Koshiba (2019). Efficient private database queries using ring-LWE somewhat homomorphic encryption. *Journal of Information Security and Applications*, *49*(1), 1-10. DOI: https://doi.org/10.1016/j.jisa.2019.102406

[33] Grining, K., Klonowski, M. & Syga, P (2019). On practical privacy-preserving fault-tolerant data aggregation. *International journal of Information Security,* 18**,** 285–304. DOI: https://10.0.3.239/s10207-018-0413-5

[34] Suleiman Y. Yerima, Sakir Sezer & Igor Muttik (2015). High accuracy android malware detection using ensemble learning, *9*(6), 313– 320. DOI: https://www.doi.org/%2010.1049/iet-ifs.2014.0099

[35] Wen Zeng and Maciej Koutny (2019). Modelling and analysis of corporate efficiency and productivity loss associated with enterprise information security technologies. *Journal of Information Security and Applications,* 49(1), 1-12. DOI: https://doi.org/10.1016/j.jisa.2019.102385

[36] Riesco, R. and Villagrá, V.A. (2019). Leveraging cyber threat intelligence for a dynamic risk framework. *International Journal of Information Security*, 18, 715–739. DOI: https://doi.org/10.1007/s10207-019-00433-2

[37] Herzog, A., Shahmehri, N., Duma, C (2007). An ontology for information security. *International Journal of. Information Security*, *1*(4), 1–23. DOI: https://doi.org/10.4018/jisp.2007100101.

[38] Jorge E. López de Vergara *et al*. (2009). A Semantic Web Approach to Share Alerts among Security Information Management Systems. *Communications in Computer and Information Science*, 72, 27-38. DOI: https://doi.org/10.1007/978-3-642-16120-9_14

[39] Jan Meszaros and Alena Buchalcevova (2017). Introducing OSSF: A framework for online service cyber security risk management. *Computers & Security*, *65*(1), 300-313. DOI: https://doi.org/10.1016/j.cose.2016.12.008

[40] Sara Qamara and ZahidAnwara *et al* (2017). Data-driven analytics for cyber-threat intelligence and information sharing. *Computers & Security,* 67(1), 35-58. DOI: https://doi.org/10.1016/j.cose.2017.02.005.

****