Correlating Learning Culture with Awareness and Response to Information Security in Software Industry

NADEEM AKHTER, Dr. EKBAL RASHID, Dr. BIRENDRA GOSWAMI

Ph.D. Research Scholar,
Sai Nath University,
Ranchi, Jharkhand, India
Associate Professor, Dept. of CSE
RTC Institute of Technology,
Ranchi, Jharkhand, India
Professor, Dept. of Science and Technology
Sai Nath University,
Ranchi, Jharkhand, India

nadeemakhin@yahoo.com, ekbalrashid2004@yahoo.com ,bg.ranchi@gmail.com

Abstract

The creation, management, and distribution of information resources are becoming increasingly important to the global economy. Therefore, it is crucial for organizations to take seriously the protection of their information resources to function in this global society. And employees with their awareness and response are largely responsible for the protection of information resources. The objective of this study is to investigate the impact of learning culture of employees within organizations to Awareness and Response to Information Security Breaches. The material analyzed is collected through survey with information technology professionals within software industry. The findings show that Organizational learning culture are demonstrated to have a great impact on its employee awareness and ability to respond to information security breaches. We proposed a framework to analyze that Organizations which have prioritized and invested in learning culture (represented by Learning Culture Quotient - LCQ) had training as a continuous form of education which was planned, mandated, and measured (represented by Mandated Training Quotient - MTQ). This had a direct impact on the employee's knowledge of Information security thereby leading to better awareness and response to information security breaches (represented by Awareness and Response Quotient - ARQ). We used scatter plot to confirm the linearity and coefficient of determination (r^2) to assess a definitive correlation between the 3 variables – LCQ, MTQ and ARQ.

The findings strengthen the notion in related research that cultural aspects especially the learning culture of organizations have great influence on how information security and incidents are managed and can be avoided.

Keywords

Organizational culture, learning culture, information security, incidents, Scatter plot, coefficient of determination, transitive property of equality

Introduction

Information security, or InfoSec, is the term used to describe the procedures and devices created and used to safeguard confidential business data against modification, maintenances, disruptions, and destruction [1].

Infosec is a set of procedures designed to protect data from unauthorized access or modification [2] both during storage and transmission from one device or location to another. It may also occasionally be referred to as data security. Keeping information secure has become more crucial as data has grown to be one of the most valuable commodities in the 21st century.

Cybersecurity and Infosec are frequently mixed up. Although Infosec only refers to the procedures created for data security, infosec is an essential component of cybersecurity. Cybersecurity is a more generalized term including Infosec.

It cost millions of dollars in finding and addressing the breach, the price of downtime and lost revenue, and the long-term reputational harm to a company and its brand are among these expenses. Customers' "personally identifiable information (PII)", such as national identification numbers (such as Passport Number, Social Security numbers etc.), names, addresses, and credit card numbers are the targets of cybercriminals who then sell these records in unregulated online black markets. Because of compromised PII, customers frequently lose trust. This can lead to penalty or legal action or both.

Principles of Information Security

The so-called CIA triad—confidentiality, integrity, and availability—best sums up the fundamental principles of information security. [2]

Confidentiality - When thinking about "information security", confidentiality springs to mind first. Data is "confidential" when those who have been given permission to access it are able to access; for confidentiality it is important to track down and prevent unauthorized users from accessing the data. Techniques for ensuring confidentiality include authentication (using password and tokens), encryption, firewalls and other defense and deterrence against attacks.

Integrity – Maintaining data accuracy and preventing improper modification, whether intentional or unintentional, are two aspects of integrity. Since hackers can't access data they can't change, many techniques used to ensure confidentiality also protect data integrity. Integrity of data can be checked using checksums, and if necessary, data can be restored using version control tools and routine backups. An integrity in depth defense can be provided using additional tools. Integrity also includes the idea of non-repudiation, which calls for the ability to demonstrate that data has been kept accurate, particularly in legal contexts.

Availability - Contrary to confidentiality, availability requires both ensuring that only users who are authorized can access data and preventing any unauthorized users from doing so. A solid backup strategy must be put in place, and computing & network resources must be sufficient to handle the volume of data to be accessed.

In a perfect world, data would always be secure, up to date, and accessible. However, one must frequently assess which "information security" principles to prioritize, which necessitates evaluating data. For example, prioritizing confidentiality when storing sensitive medical data, whereas a financial organization might prioritize data integrity to make sure that bank accounts are not accidentally credited or debited [2] or through malicious means.

Some of the more known Information Security measures [3].

1. Data Classification – Classification of sensitive and critical data and maintaining/managing them.
2. Strict Access Controls - Because privileged account misuse is one of the major reasons for data breaches, access must be restricted to essential systems, accounts, and data in accordance with the Principal of Least Privilege (PoLP). Additionally, access should be revoked once it is no longer required.
3. Monitoring Privileged Account Access - Need to ensure to carefully monitor all access to privileged accounts and get instant notifications when it any suspicious set of events happens. Ex. Access from outside office network, accessing inactive accounts etc.
4. Encrypting Sensitive Data – Data which are classified as sensitive must be encrypted, both while storing or transmitting. Encryption is simplest and effective ways to prevent unauthorized access to confidential and sensitive data, but it is also one of the strategies that is most frequently disregarded.
5. Security Awareness & Response Training - Vitally important because insiders are largely to blame for security incidents. Employees need to be made aware of the value of the basic hygiene of using good password and trained to recognize shady phone calls, SMS messages, and email messages. They must look out for emails sent from open email addresses, emails with errors in the grammar and spelling, and emails that convey urgency. Never click on links to shady websites or download attachments from enigmatic senders as an employee.
6. Network Segmentation - Network segmentation divides a network into smaller sub-networks, whereas network segregation isolates critical networks from outside access. Network segmentation and segregation are crucial components of a 0-trust architecture, that operates under the premise that all users accessing are potentially and characters and need be identified whenever they access vital resources.

7. Cloud Security – It is a broad concept that covers a variety of security measures, such as putting in place strict access controls, encrypting sensitive data, also thoroughly going over all security settings and contracts related to cloud service provider. All sensitive data kept in the cloud must be able to be found, categorized, and monitored by carefully selected security solutions.
8. Application Security - Web applications frequently have vulnerabilities, which is why it is needed to install regular updates and run patches. The vulnerabilities that existed in contemporary applications include flawed access control techniques, cryptographic errors, and security misconfiguration.
9. Patch Management - All programs and systems need to be patched as soon as possible. Use an automated patch management solution to make sure nothing is missed if the business utilizes a lot of proprietary software.
10. Physical Security - Server rooms and workstations must be properly secured with locks, alarms, ID badges, CCTV cameras, and any other security measures that will prevent unauthorized access, even though they are not as crucial as they once were.

Despite the numerous security measures security incidents are on a rise that results due to unauthorized access of hardware assets and data. This only happens when an intruder is able to bypass the security measures with ill intention [4].

Information that is confidential has great value. On the dark web, it is frequently sold; for instance, names and credit card numbers can be purchased and used for fraud or identity theft. It is not surprising that security breaches can result in significant financial losses for businesses. For large corporations, the cost is typically close to $4 million [4].

Depending on how access to the system was obtained, there are various types of breaches. Here are some of the more popular ones…

1. A system vulnerability, such as an outdated operating system, is attacked by an exploit. The use of outdated and unsupported versions of Microsoft Windows in businesses, for example, leaves legacy systems that haven't been updated particularly open to exploits.
2. It happens frequently when an employee leaves a computer, phone, or file unattended where they shouldn't have, and it gets stolen. Additionally, it might compromise patient or customer information in addition to the new prototypes that may have been needed to be kept a secret.
3. Password theft is another incredibly common but incredibly damaging problem. It is surprising to learn how frequently this occurs. Some employees leave computer passwords on post-It notes, making them accessible to anyone, which could lead to shady employees accessing the files elsewhere.
4. Access can be obtained through phishing emails and malware attacks. One employee clicking a link in a phishing email is all it takes for malicious software to start spreading across the network.
5. Keyloggers are malicious programs that can be inserted into computer or sent via email by cybercriminals and record everything that’s typed using the keyboard. The information is given back to the hackers, who use it to access private information.
6. It is also possible to gain access through social engineering. For instance, a hacker might call a worker and pretend to belong to IT helpdesk, asking for the password so they can "fix" the computer.
7. Attacks on websites that appear to be extremely genuine are known as phishing. For instance, they might create a website that is a copy of PayPal and ask someone to log in to make a change. And that someone can giving the hacker one’s password if they log in without realizing that they aren't just accessing their account.

Few examples of security breach along with data breach .

1. Equifax - A website application flaw in 2017 led to the company losing the personal information of 145M Americans. This contained their names, Social Security numbers, and license numbers.
2. Yahoo – 3B user accounts were compromised in 2013 because of phishing attempts that gave hackers access to the network.
3. Facebook - Internal software flaws resulted in the loss of personal information for 29 million users in 2018. Since the accounts that were compromised included the one belonging to the company's CEO Mark Zuckerberg, this security breach was especially embarrassing.

4. Marriott Hotels - It disclosed a security breach in 2018 that may have compromised the information of 500 million customers. Although the company's guest reservation system had been breached in 2016, it took another two years for the problem to be discovered.

A data breach can cost a lot of money, but as more companies are targeted and exposed, the potential financial losses are becoming more obvious. Modern businesses of all sizes may suffer severe financial losses as a result of a data breach. Variables like incident type and severity, regulatory requirements, company size, industry, and region can all have a significant impact on the potential financial impact of a data breach on a company.

The foundation of an organization's capacity to safeguard information, data, and the privacy of its employees and clients is its security culture. Some businesses are starting to understand it. They are recognizing that effective enterprise-wide security requires a strategic, long-term approach, focusing more on communication and culture than exhortations from IT and a constant stream of new policy mandates. They are moving beyond tactical, episodic approaches to security

Today, we work to find solutions to tomorrow's issues. Every organization's heartbeat is its workforce. Employees feel valued when their growth is invested in through ongoing support, education, and skill development. For highly technical organizations, having a culture that supports learning is essential to luring and keeping top talent. The benefits of learning culture extend to the employees as well as the organization. Encouragement of employees to comprehend the guiding principles, functional areas, and competencies of the company is a top priority for a learning culture. These priorities in a learning culture make sure that workers are continually upskilling to improve their skill sets and knowledge base for their current and future roles.

Literature Review

This section explains the research that has been done on information security. Studies where cultural factors especially learning culture are thought to have an impact on the efficacy of information security will receive particular attention.

Since the beginning of the field of cybersecurity, the CIA triad of Confidentiality, Integrity, and Availability has been used as the practical definition of information security and later cybersecurity[8]. When the field of cybersecurity first emerged, risks related to it were not well understood. Computers weren't connected to a (local) network, and the Internet didn't even exist, when the CIA triad was first proposed. Our use of computers has changed significantly over time. We no longer carry a single, disconnected, room-filling computer; instead, we carry multiple, always-connected computers in our pockets. Computers now play a role in most physical processes in one way or another. The nature of enemies has drastically changed [7]. In the 1990s and the early 2000s, network edges were where traditional security was provided. This strategy was no longer viable with the introduction of mobile devices and the rising popularity of “bring your own device” (BYOD) policies. Although the perimeters of security have expanded along with it, the overall security strategy has not. This has only served to reinforce the propensity for individualistic security strategies.

Numerous studies have been done to find out what elements are crucial when attempting to get high-quality information security protection.

Based on security procedures and organizational factors, the author [13] conducted a survey study to examine the efficacy of information security practices. Their findings suggested that smaller and medium-sized businesses devote fewer person-hours to information security each week. Effective information security requires strong top management support because it raises the level of sophistication of security software. The survey also revealed that financial institutions take more precautions about information security than organizations in other industries.

The authors [10], suggested that other security parameters, such as organizational and physical security, will improve because of improvements in communications management and security policy. Using questionnaires, their study investigated information security in small and medium-sized businesses in Turkey. These findings were then contrasted with those of comparable studies conducted in other nations. The authors[10] further emphasizes the value of adhering to international policy standards and implementing them across the board. Cultural differences

were not considered in this study, and the authors emphasize that additional questions about cultural differences in future studies would be helpful for a better understanding.

The authors' [11] research primarily examined organizational aspects and how they might impact information security. Their findings demonstrated that factors like employee ignorance of information security, a lack of specifications when formulating a policy, the caliber of the testing team, and inadequate requirement definitions can have an impact on the general information security in businesses. The findings imply that organizational factors play nuanced roles in information security system vulnerability in ways that technical fixes cannot address. The authors [11] continue to suggest that it's critical that management understand the complex roles that organizational factors play and that information security vulnerabilities aren't just the result of technical issues. An integrated, multi-layered strategy is required for the design and management of information security systems to improve performance.

According to the authors [12], the security management must balance the need to enable the business with other priorities such as ensuring compliance and maintaining cultural fit. Organizational integration, social alignment, and technical competence are three types of activities included in the socio-technical strategy used by the companies the researchers studied to achieve the same. The authors[12] further stress that due to the complexity of information security, it should be approached as a business issue rather than a technical one to achieve effective results.

By addressing each party's responsibility, the authors provided several recommendations for improving security at the individual and organizational levels [20]. Because of growing threats, data security is the main concern. People need to understand the best security practices and how to stay safe while using the internet. [20].

The authors' [9] study confirms that organizational culture has substantial impact on information security, and it also reinforces the use of current information security handling techniques. Even though the banks in the various nations use the same international standards, their implementations and results vary. The ability of a company to adapt to changes depends on both how complex its systems are and how open it is to change.

Organizational culture is still a complicated phenomenon, and scholars have put a lot of effort into trying to understand and define it over the years [14]. Many academics appear to concentrate on the shared attitudes that shape the individuals who make up an organization, even though they all define the concept slightly differently.

An organizational culture can have both positive and negative effects. It can be utilized to achieve organizational goals if managed well [15]. When organizational culture and objectives are in line, employees make decisions based on fundamental presumptions that are appropriate for the intended ends, which can be the primary reason for organizational failure if poorly managed[16]. Because of this, it's also interesting to think about how various organizational cultures may affect employees' decisions to use the methods recommended by their company to achieve information security goals, i.e., to comply with the advised information security policy.

The authors (25) analyze a specific kind of Organizational culture called the “Clan culture” is characterized by a friendly working environment where the employees are open, spend a great deal of time promoting social cohesion, and show personal engagement. The way the organization structures its business allows for maximum freedom and personal growth for each employee. In this kind of organization, decisions are frequently made by consensus and leadership is based on mentoring. Loyalty and tradition are essential to the organization's unity [17].

The ability of an organization to grow and succeed while the individuals who make it up succeed and thrive in their careers depends on maintaining a strong culture of learning [6]. When organizations prioritize and invest in learning culture, employees are better enabled with a wholistic view of information security. In lot of cases Employees can assess their actions as well as their peers’ actions which could lead to a breach. This is also called human firewall and is the best mechanism to avoid a breach.

It should come as no surprise that some sectors and organizations have observed a stagnation or decline in their security cultures during the pandemic. New security concerns and issues emerged as more businesses adopted the work-from-home model, making communication and education somewhat more difficult. And of the most important aspect of Organizational Security measure is the Culture of learning [5].

The author [19] concluded that employees undergo continuous learning by receive training on various information security practices at various times, perhaps once every quarter, organizations should make sure that employees receive it at least once a year.

According to the author [18] regarding this level of organizational learning, there are four action imperatives:

(1) Develop systems to record and share knowledge
(2) Offer long term strategical leadership for learning.
(3) Empowering individuals to work toward a common goal and vision.
(4) Bind the company to its eco system / environment.

Learning is "the way in which people make meaning of situations they encounter, and the way in which they acquire and apply the knowledge, attitudes, and skills they need to act in new ways"[18]. Opportunities for continuous learning include self-directed learning, learning from colleagues, computer-assisted learning, day-to-day work experiences, unique project assignments, and personal insights. However, employees must be open to change, adaptation, growth, and taking charge of their own professional decisions to engage in continuous learning [18]. Through better planning for informal learning, learning how to learn, on-the-job training or coaching, action learning, reflective planning, and classroom instruction, organizations can create opportunities for continuous learning.

Addressing the connection between learning culture and information security is important and directly related to our research question; however, this kind of research does not go into the potentially contrasting effects of different organizational culture types. The paper supports the assertions made that this aspect has not been for only briefly addressed in previous research when it comes to understanding the effects of various learning culture.

Significance of the Study

This quantitative correlational study aimed to examine employee's awareness and readiness to respond to information security incidents in Software Organizations. The study design targeted employees across all designations who go through mandated and measured training programs. This had a direct correlation on employee's reactions to potential information security breaches or incidents. The study examined the relationship between Organizations learning culture and employee awareness and response readiness to information security. The outcome of this study is significant for Software Organizations to prioritize and focus on the area that has the most impact on creating awareness among its employees and better response to any information security breach.

Methodology

This correlational study aimed to examine employee's awareness and response readiness for information security in software organizations. The study design targeted employees across different levels across different software organizations, studying their learning culture, mandated trainings and employee's awareness of information security and readiness to respond to information security incidents. The study examined the relationship between Organizations Learning Culture, their Mandated Training and employee 's awareness & readiness to information security.

The participants completed an online survey to determine organizations learning culture, organizations training mandates and change in employees' awareness & response before and after trainings.

The population of this study included employees from software organizations. Therefore, the population size can vary, so we will assume that more than half of the population can impact information security for maximum variability so p=0.5. It was first necessary to set the confidence level to determine the appropriate sample size. The author(s) set the confidence level to 95% and an acceptable margin of error is 5%. And the author(s) calculated the sample size using Cochran's Formula.

Since p = 0.5 so q = 0.5 (since q = 1-p). With 95% confidence, and at 5 %—plus or minus—precision, so e = 0.05. A 95 % confidence level gives us Z value of 1.96.

$$n_0 = \frac{z^2 pq}{e^2}$$

(1)

$((1.96)^2 (0.5) (0.5)) / (0.05)^2 = 385.$

So, a random sample of 385 software professionals in our target population was enough to give us the confidence levels we needed.

The authors constructed a framework of 3 theories – Organizations who have prioritized and invested in learning culture (Learning Culture Quotient - LCQ) had training as a continuous form of education which was planned, mandated, and measured (Mandated Training Quotient - MTQ). This directly impacted the employee's knowledge and awareness of Information security thereby leading to better awareness and response to information security breaches (Awareness and Response Quotient - ARQ).

The survey was responded by 436 IT professionals across all designations/titles. The authors analyzed the culture of learning across different organizations in Software Industry across different titles from individual contributors to leaders. Impetus on continuous training which was measured and mandated was also analyzed. The author further analyzed any correlation with employee's awareness and response readiness for information security incidents before and after the trainings.

<u>These were the research Questions as part of survey</u>

RQ1 - General
What is your designation or HR Title in your Organization?

RQ2 – Learning Culture

Your organization invests and prioritizes Learning to create a Learning Culture for overall development.

RQ3 – Mandated Training

Your organization provides training goals to all employees for X hrs. of training to be completed annually and/or measures the training taken by employee as part of the process.

RQ4 – Mandated Training

Your organization mandates learning and training for Compliance (esp. Information Security)

RQ5 – Mandated Training

Your organization conducts continuous periodic (annual or semi-annual) mandatory training on Information Security to help building awareness.

RQ6 – Mandated Training

Your organization conducts continuous periodic (annual or semi-annual) mandatory training on Information Security to help in identifying information security breaches (ex. Phishing).

RQ7 – Awareness and Response

Is there a significant difference in the number of secured responses (SR) the employee performs (with reference to information security) before and after the training?

RQ8 – Awareness and Response

Is there a significant difference in the number of un-secured responses (UR) the employee performs (with reference to information security) before and after the training?

RQ9 – Awareness and Response

Is there a difference in Employee Awareness of the various information security situations (EA) before and after the training?

Learning Culture Quotient – LCQ

RQ2 was used to assess LCQ. The responses to RQ2 were translated to "Agree", "Disagree" and "Neutral". Numerical values were assigned for efficient analysis.

Agree was translated as 1, Disagree was translated as 0 and Neutral was not assigned any value.

Mandated Training Quotient - MTQ

4 questions from RQ3 to RQ6 was used to assess MTQ. The responses to RQ3 , RQ4, RQ5 and RQ6 were translated to "Agree", "Disagree" and "Neutral". Numerical values were assigned for efficient analysis.

Agree was translated as 1, Disagree was translated as 0 and Neutral was not assigned any value.

An average of responses to each question across the Job title was used to arrive at a numerical number rounded off to 0 or 1. Any average number from 0.50 to 0.99 was round to 1 and average of 0.01 to 0.49 was rounded to 0.

Awareness and Response Quotient - ARQ

3 questions from RQ7 to RQ9 was used to assess ARQ.

The responses to RQ7 were translated to "IncreaseActionSecure", "DecreaseActionSecure" and "Neutral". Numerical values were assigned for efficient analysis. IncreaseActionSecure was translated as 1, DecreaseActionSecure was translated as 0 and Neutral was not assigned any value.

The responses to RQ8 were translated to "DecreasesActionInsecure", "IncreaseActionInsecure" and "Neutral". Numerical values were assigned for efficient analysis. DecreasesActionInsecure was translated as 1, IncreaseActionInsecure was translated as 0 and Neutral was not assigned any value.

The responses to RQ9 were translated to "IncreaseEmployeeAwareness", "DecreaseEmployeeAwareness" and "Neutral". Numerical values were assigned for efficient analysis. IncreaseEmployeeAwareness was translated as 1, DecreaseEmployeeAwareness was translated as 0 and Neutral was not assigned any value.

An average of responses to each question across the Job title was used to arrive at a numerical number rounded off to 0 or 1. Any average number from 0.50 to 0.99 was round to 1 and average of 0.01 to 0.49 was rounded to 0.

We calculated LCQ, MTQ and ARQ for all 436 responses grouped by Designation/HR Titles.

Designation/HR Titles	**Count**	**LCQ**	**MTQ**	**ARQ**
Developers/Engineers/Business Analysts	84	79	70	75
Lead - Developers/Engineers/Business Analysts	93	80	82	83
Leaders - Directors/VP ++ (any function)	62	56	52	48
Others	45	36	41	42
Project Managers/Scrum Masters/Program Managers	101	90	90	94
Security Teams	29	29	29	20
Shared Service - DBA/Infrastructure	7	6	6	5

Solution Architects/Business Architects	15	15	13	5

Table 1 - LCQ, MTQ and ARQ for all respondents grouped by Designation/HR Titles.

We used scatter to correlate LCQ with MTQ and MTQ with ARQ. Additionally, we also calculated Coefficient of Determination (r^2) to correlate LCQ with MTQ and MTQ with ARQ to assess the final correlation between LCQ and ARQ.

Step1 - we analyzed the correlation between LCQ and MTQ using scatter.

Designation/HR Titles	**LCQ (X)**	**MTQ (Y)**
Developers/Engineers/Business Analysts	79.00	69.75
Lead - Developers/Engineers/Business Analysts	80.00	82.00
Leaders - Directors/VP ++ (any function)	56.00	52.25
Others	36.00	40.50
Project Managers/Scrum Masters/Program Managers	90.00	90.25
Security Teams	29.00	28.50
Shared Service - DBA/Infrastructure	6.00	6.00
Solution Architects/Business Architects	15.00	12.50

Table 2 – LCQ and MTQ grouped by Designation/HR Titles.

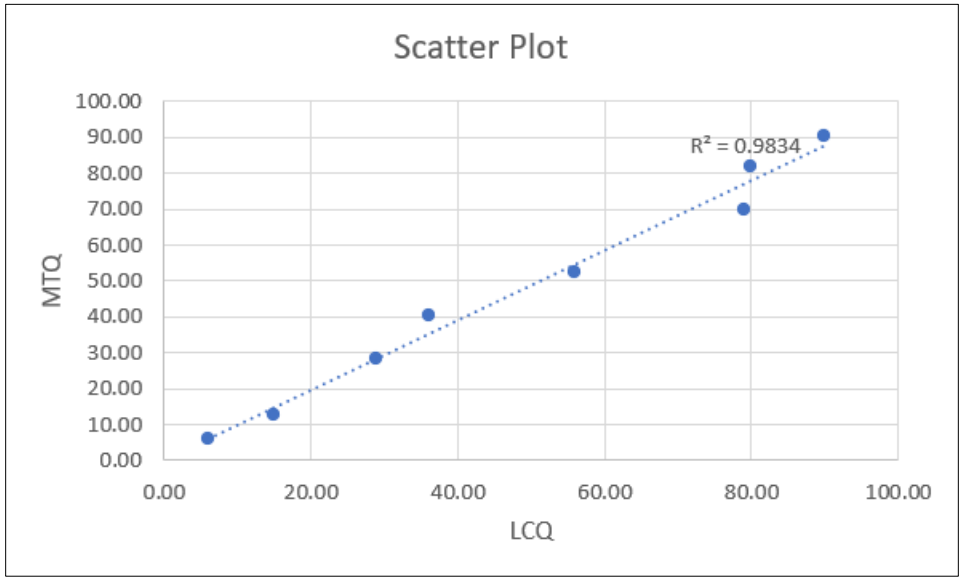

Fig1 – Scatter Plot with LCQ and MTQ

Step2 - we analyzed the correlation between LCQ and MTQ by calculating Coefficient of Determination (r^2) using mathematical formula.

$$r^2 = \left(\frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{n\Sigma x^2 - (\sum x)^2} \times \sqrt{n\sum y^2 - (\sum y)^2}} \right)^2$$

(2)

LCQ as x

MTQ as y

And n = 8 (number of unique grouped titles)

Coefficient of Determination (r^2) = 0.9834

Step3 - we analyzed the correlation between MTQ and ARQ using scatter.

Designation/HR Titles	**MTQ (X)**	**ARQ (Y)**
Developers/Engineers/Business Analysts	69.75	74.67
Lead - Developers/Engineers/Business Analysts	82.00	83.00
Leaders - Directors/VP ++ (any function)	52.25	48.00
Others	40.50	42.00
Project Managers/Scrum Masters/Program Managers	90.25	93.67
Security Teams	28.50	20.00
Shared Service - DBA/Infrastructure	6.00	5.33
Solution Architects/Business Architects	12.50	5.00

Table 3 – MTQ and ARQ grouped by Designation/HR Titles.

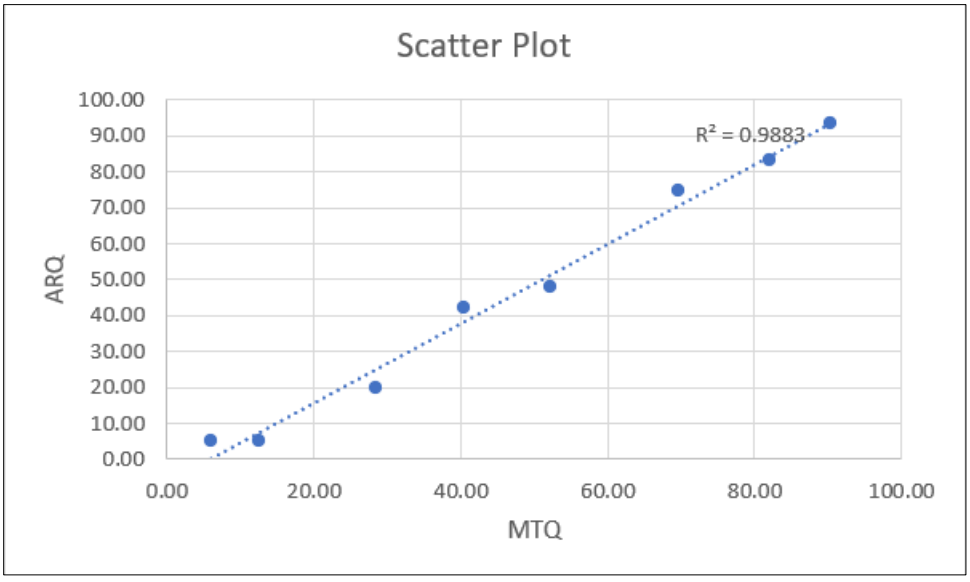

Fig 2 – Scatter Plot with MTQ and ARQ

Step4 - we analyzed the correlation between MTQ and ARQ by calculating Coefficient of Determination (r^2) using mathematical formula.

$$r^2 = \left(\frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{n\Sigma x^2 - (\sum x)^2} \times \sqrt{n\sum y^2 - (\sum y)^2}} \right)^2$$

(3)

MTQ as x

ARQ as y

And n = 8 (number of unique grouped titles)

Coefficient of Determination (r^2) = 0.9883

Step5 - we analyzed the correlation directly between LCQ and ARQ using scatter.

Row Labels	**LCQ(X)**	**ARQ (Y)**
Developers/Engineers/Business Analysts	79.00	74.67
Lead - Developers/Engineers/Business Analysts	80.00	83.00
Leaders - Directors/VP ++ (any function)	56.00	48.00
Others	36.00	42.00
Project Managers/Scrum Masters/Program Managers	90.00	93.67
Security Teams	29.00	20.00
Shared Service - DBA/Infrastructure	6.00	5.33
Solution Architects/Business Architects	15.00	5.00

Table 4 – LCQ and ARQ grouped by Designation/HR Titles.

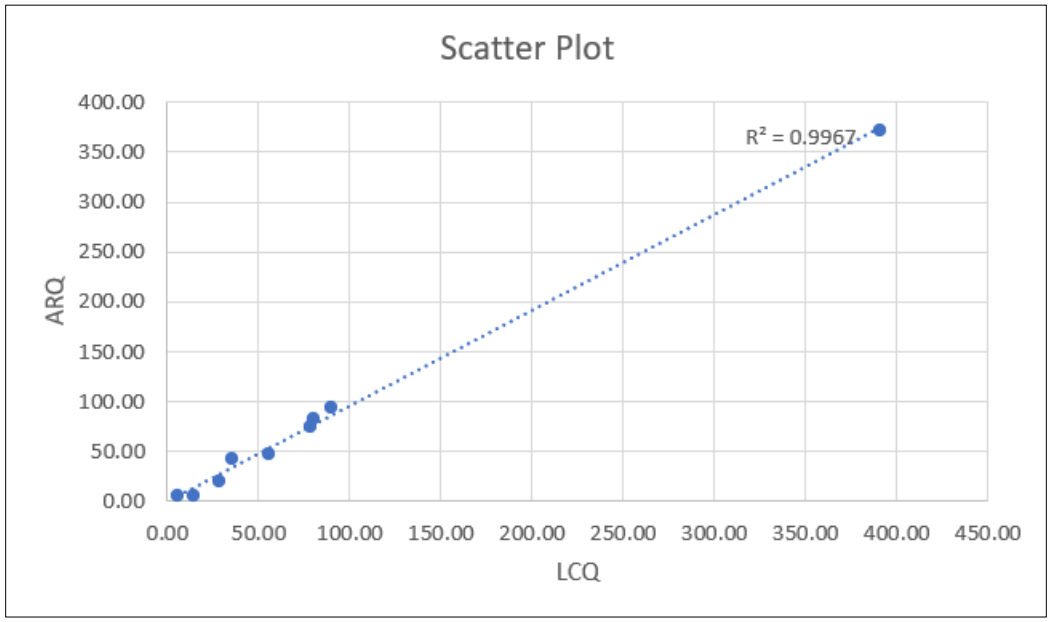

Fig 3 – Scatter Plot with LCQ and ARQ

Step6 - we analyzed the correlation between LCQ and ARQ by calculating Coefficient of Determination (r^2) using mathematical formula.

$$r^2 = \left(\frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{n\Sigma x^2 - (\sum x)^2} \times \sqrt{n\sum y^2 - (\sum y)^2}} \right)^2$$

(4)

LCQ as x

ARQ as y

And n = 8 (number of unique grouped titles)

Coefficient of Determination (r^2) = 0.9964

Result Analysis

We analyzed the correlation between Organizations which prioritized and invested in learning culture (Learning Culture Quotient - LCQ) and training as a continuous form of education which was planned, mandated, and measured (Mandated Training Quotient - MTQ).

The scatter plot had a linear relation between LCQ and MTQ. We also calculated Coefficient of Determination (r^2) using mathematical formula which came out to be 0.9834. This implies that there is a very high degree of correlation between LCQ and MTQ.

We further analyzed the correlation between training as a continuous form of education which was planned, mandated, and measured (Mandated Training Quotient - MTQ) and employee's knowledge and awareness of Information security thereby leading to better awareness and response to information security breaches (Awareness and Response Quotient - ARQ).

The scatter plot had a linear relation between MTQ and ARQ. We also calculated Coefficient of Determination (r^2) using mathematical formula which came out to be 0.9883. This implies that there is a very high degree of correlation between MTQ and ARQ.

There is a high degree of correlation between LCQ and MTQ. There is also a high degree of correlation between MTQ and ARQ. Hence, by transitive property of equality we can safely assume there is a high degree of correlation between LCQ and ARQ.

We double checked by plotting a scatter directly between LCQ and ARQ and calculated Coefficient of Determination (r^2). The scatter plot had a linear relation between LCQ and ARQ. Coefficient of Determination (r^2) using mathematical formula came out to be 0.9964. This implies that there is a very high degree of correlation between LCQ and ARQ.

Hence, it's proven that Organizations in Software Industry having high degree of Learning Culture directly correlates to its employee's better awareness and response to Information Security Breaches.

Conclusion

The study demonstrated that software organizations need to prioritize and invest in learning culture, which is continuous, mandated and measured for its employees. Employees who have been part of such organizations went through periodic trainings which were mandated and measured. This allowed a good understanding of information security, better awareness, and ensured that the employee knows and understands how to respond to information security breaches or incidents. It is recommended that organizations focus on creating a learning culture which has practices to conduct continuous training for all employees, regardless of their position, to stay updated with

information security. The study result highlighted how employees were better equipped to react to information security, given their knowledge and understanding in organizations which had learning culture as a priority.

Future Scope

The researcher suggests carrying out comparable research focusing on employee behavior and information security knowledge from other industries. It would be advantageous to investigate academic institutions across various time periods and nations with fewer restrictions. Medical facilities like hospitals and clinics have various staffing levels, as well as various systems and job responsibilities. Banks and other financial institutions are frequently targeted. Government institutions and Retail businesses are frequently at the receiving end. The main advantage of conducting comparable research on various industries is that they might experience comparable or dissimilar types of attacks, and other industries might be more significant than Software Organizations. Cultural impact and their readiness for Information Security may be different. Another option is to use larger sample sizes, which will aid in the generalization of the research findings by including both the public and private sectors in the study. Additionally, the study should be conducted under more typical circumstances rather than after a pandemic when most workers are working from home or in another circumstance that might skew the results. To learn more about knowledge retention, other studies could check in with the participants a year after the training. The researcher advises conducting comparable studies with organizations that outsource their training and may not have formal policies or whose employees disregard their rules or have organizations who have high number of contractor workforce.

References

[1] What is Information Security? https://www.cisco.com/c/en_in/products/security/what-is-information-security-infosec.html

[2] What is information security? Definition, principles, and jobs https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html

[3] Top 10 Security Measures Every Organization Should Have (2022) https://www.lepide.com/blog/top-10-security-measures-every-organization-should-have/

[4] What is a Security-breach https://www.kaspersky.co.in/resource-center/threats/what-is-a-security-breach

[5] The Importance Of A Strong Security Culture And How To Build One https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/?sh=274950686d49

[6] Building a Culture of Learning in Security Operations https://www.deepwatch.com/blog/building-a-culture-of-learning-in-security-operations/

[7] Jeroen van der Ham. 2021. Toward a Better Understanding of "Cybersecurity". Digit. Threat.: Res. Pract. 2, 3, Article 18 (June 2021), 3 pages. https://doi.org/10.1145/3442445

[8] J. Anderson. 1972. Computer Security Planning Study. Technical Report ESD-TR-73-51. Air Force Electronic System Division

[9] Gabriella E, Elin J (2017). The impact of organizational culture on information security during development and management of IT systems

[10] Yeniman Yildirim, E., et al. (2011), "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey", International journal of information management, Vol. 31, No. 4, 360-365.

[11] Kraemer, S., Carayon, P., & Clem, J. (2009). "Human and organizational factors in computer and information security: Pathways to vulnerabilities", Computers & security, Vol. 28, No. 7, 509-520.

[12] Kayworth, T., Whitten, D. (2010). "Effective Information Security Requires a Balance of Social and Technology Factors", MIS Quarterly Executive, Vol. 9, No. 3

[13] Kankanhalli, A., et al. (2003). "An integrative study of information systems security effectiveness", International journal of information management, Vol. 23, No. 2, 139-154.

[14] Jung, T., Scott, T., Huw, T.O.D., Bower, P., Whalley, D., Mcnally, R. And Mannion, R. (2009), "Instruments for exploring organizational culture: a review of the literature", Public Administration Review, Vol. 69 No. 6, pp. 1087-1096.

[15] Rashid, M.Z.A., Sambasivan, M. and Johari, J. (2003), "The influence of corporate culture and organizational commitment on performance", Journal of Management Development, Vol. 22 No. 8, pp. 708-728.

[16] Bititci, U.S., Mendibil, K., Nudurupati, S., Garengo, P. and Turner, T. (2006), "Dynamics of performance measurement and organizational culture", International Journal of Operations & Production Management, Vol. 26 No. 12, pp. 1325-1350.

[17] Barth, A. And Mansouri, S. (2021), "Corporate culture and banking", Journal of Economic Behavior and Organization, Vol. 176, pp. 46-75.

[18] Watkins, Karen. (1999). Sculpting the Learning Community: New Forms of Working and Organizing. Nassp Bulletin. 83. 78-87. 10.1177/019263659908360410.

[19] Al Zaidy, Ahmed. (2020). Impact of Training on Employee Actions and Information Security Awareness in Academic Institutions. 10.13140/RG.2.2.18935.96168.

[20] Kenning Arlitsch & Adam Edelman (2014) Staying Safe: Cyber Security for People and Organizations, Journal of Library Administration, 54:1, 46-56, DOI: 10.1080/01930826.2014.893116

[21] Survey data is hosted in Git https://github.com/nadeemakhin/InfoSec.git