ISSN 2661-2666 (Online) International Scientific Journal Monte (ISJM) DOI: 10.33807/monte.20253301
Volume 10, No.1 (2025): April

THE IMPACT OF INFORMATION MANAGEMENT IN CREATING A SECURE BUSINESS ENVIRONMENT

Ejup Rustemi[1]* Mefail Tahiri[2]

[1]University of Tetova, North Macedonia
[2]University of Tetova, North Macedonia
** ejup.rustemi@yahoo.com*

ABSTRACT

Concerns regarding the safety of information have been around for as long as individuals have been interested in storing and gathering data for their own personal or professional purposes. The situation, however, has never been as severe as it is right now. Internet and other modern technologies have enabled us to arrange information in a way that was before impossible. Within the context of our continual pursuit of success, we make use of them as instruments that supply us with timely and precise observations. There has never been a time when the security of information has been more compromised as it is right now. We discuss the issues that this period presents, and we hope that the measures that are necessary to overcome the obstacles in order to achieve an ideal information security environment are presented in this paper. On the other hand, at the same time as artificial intelligence systems are becoming more advanced, they are also becoming more thoroughly interwoven into the lives of people and into crucial areas of the real world, such as infrastructure, banking, and national security. On the organizations that make use of these technologies as well as on society as a whole, these technologies have the potential to have both beneficial and bad effects.

Key words: *information, security, malware, cybercrime, technology.*

INTRODUCTION

In contemporary society, mobile technology has emerged as a significant subject of discourse and a critical problem concerning security. Mobile gadgets are ubiquitous. It is important to clarify that the word mobile devices include more than just cell phones, as many individuals erroneously perceive cell phones as the sole means of communication and everyday organization. Mobile gadgets encompass a wide array, including watches, eyewear, styluses, tablets, computers, and more.

From a broader perspective, these technologies exemplify a distinctive method of enhancing our lifestyle. They are a vital resource for reading emails, newspapers, and similar materials. They can regulate other devices, including televisions, DVD players, or Blu-ray players. Thus, they must have originated from Heaven due to their exceptional qualities. They are undeniably crucial and enabling; but, they simultaneously provide an unparalleled challenge to information security, particularly when linked to the enterprise aspect of company operations.

THE TERRAIN

Mobile devices present a significant problem in the realm of information security. Global enterprises utilize them to link their operations, facilitating the expedited attainment of their objectives. In this process, they share information essential to their tasks. This would have been optimal in a world characterized by equitable competition, devoid of those whose sole occupation is malevolence. However, we do not inhabit such a reality. Our environment is replete with many competitive opponents who may attempt to violate contracts or illicitly acquire information for use against you. Their primary focal point is mobile devices. If you are curious about the reason, we will present some statistics to elucidate the matter.

A 2013 poll indicated that over 93% of corporations connect mobile devices to their business networks, while about 67% permit personal devices access to enterprise networks. The data originates from 2013, indicating that these figures are likely substantially greater today. Even if they were not elevated, they would undoubtedly be more problematic, given the increasing scope of work conducted via cell phones, tablets, and similar devices; this trend shows no signs of abating (Bergman, 2013). To further elucidate the complexity of the situation, below are some revealing data points. The cited data indicates that up to 79% of organizations report security issues. The expenses incurred from these instances have surpassed $500. 000 for almost 52% of the enterprises, and 45% of those with fewer than 1000 employees had expenses within the $100 level. Zero. Android is characterized as the most susceptible platform, accounting for almost 49% of vulnerabilities. However, what is crucial is the identification of the source of the problem. One would assume that cybercriminals are accountable for the majority of events. Your assertion is incorrect. In 66% of situations, employee negligence was the primary factor contributing to the issues. While firms endeavor to enhance their business strategies to outperform competitors, mobile devices, which should ideally facilitate this process, inadvertently expose the business to persistent security threats and, at times, complete failure (Bergman, 2013).

THE CHALLENGE

Information security is not a novel concept. Safeguarding corporate information has consistently been a fundamental aspect of establishing a robust corporation. However, locations for information storage have undergone significant transformations over time. There was an era when all information was recorded on paper and preserved in extensive archives, which were secured and protected from extraneous influences. Frequently, archives of that nature have been incinerated, obliterating all the information contained within. In other words, those were periods during which one had to confront such issues. That is not to imply that if your house burns today, your computer will remain unscathed. Your computer is no longer merely a tool for storing valuable information; it serves as a conduit for saving that information on more secure database servers, ensuring that even if your computer malfunctions, you can still retrieve your data from another computer or mobile device.

In the realm of enterprise information security, there is a specific aspect that warrants examination. Corporate servers contain not just employee information but also customer data. This complicates the matter at hand. To earn customer trust, organizations must assure clients that their personal information will be safeguarded and utilized solely for the company's purposes to enhance service delivery. This is more easily articulated than executed. Large corporations manage extensive data sets from which they must extract critical insights to enhance their understanding of client needs. The majority of organizations offer several services via mobile applications, which are promoted as the future of the company-customer relationship (Urbas, Krone, 2006). While this may be accurate, it also presents a significant obstacle to orchestrate and execute such a work. The primary concern is that the organization needs to identify the suitable security solution to safeguard its servers against external threats. Every substantial and reputable organization likely employs experts who can assess all available possibilities and select the most suitable one. This constitutes the uncomplicated aspect of the assignment. The challenge is in instructing clients on safeguarding themselves while accessing their accounts via mobile devices. To do this, organizations must educate their clients on the utilization of more complicated passwords by implementing systems that reject weak passwords, such as the user's name or sequential numeric patterns like "12345...". However, a certain consumer does not only utilize the services of a single organization; individuals engage with services from diverse companies. Consequently, they will encounter the use of several apps that adopt disparate security approaches, complicating management of the issue.

Numerous applications installed on mobile devices are complimentary and mostly generate revenue through adverts. A significant number of cybercrime incidents are claimed to have been perpetrated using advertising channels. To circumvent this issue, numerous app developers offer a premium version of the same application to prevent security vulnerabilities or to eliminate inconveniences. This should not be underestimated, since statistics data from security firms indicate that in recent years, malware attacks on mobile devices have increased by almost 273%. Although more prevalent systems like Android and Windows are typically more susceptible to attacks, every Wi-Fi-enabled device remains vulnerable to cyber threats.

Numerous firms provide their staff with mobile devices equipped with particular software, enabling security personnel to remotely erase the device's storage in the event of theft, thereby safeguarding any potentially sensitive information contained inside. As always, the situation is not as favorable as it appears. A recent survey indicates that 28% of the workforce utilizes personal mobile devices, complicating their management by employers. There is a significant likelihood that these specific personnel will utilize social networking platforms like as Facebook, Twitter, or LinkedIn, hence increasing the device's vulnerability to external influence.

Thus far, we have focused on mobile gadgets themselves; however, what about the individual utilizing them? The human element constitutes a significant aspect of information security, as it is often challenging to anticipate when an employee may misuse a device or deliberately disclose information to external parties. For the company to function, it must grant certain employees access to critical information that might potentially be disclosed or sold, thereby enabling individuals to blackmail the company.

Ultimately, it is unequivocal that information security is an exceedingly intricate phenomenon that can determine the success or failure of a whole organization.

EMBRACING WIRELESS TECHNOLOGY WITH DILIGENCE

Wireless technology represents a significant advancement in enhancing connectivity and communication. The technology facilitates data transfer rates of up to 54 Mbps, significantly surpassing the HSDPA rate of approximately 14.4 Mbps. These figures are likely to fluctuate over time, influenced by the demands of governments and large corporations for enhanced Internet connectivity. This implies that when data transfer volume escalates, security problems will intensify. The accelerated transmission will also result in expedited data theft.

Data indicates that between 2007 and 2010, over 300,000 applications were generated. These applications generate revenues in the billion-dollar range, rendering the field highly desirable. Cybercriminals consistently seek methods to exploit the billions, utilizing wireless technologies for this purpose. From this perspective, mobile devices constitute a security minefield (Karen, Souppaya, Scarfone, 2013).

Surveys conducted by security firms, including McAfee and Trend Micro, indicate a 1200 percent increase in mobile malware. What is more troubling is that these figures are increasing on a monthly basis. Companies like as Google and Apple are diligently filtering applications in their app stores due to the proliferation of malware-laden programs that have infiltrated these platforms. Cybercriminals are exploiting them to extract information from mobile devices, a threat that can impact us all.

This does not imply that PCs and Macs are entirely impervious to potential attacks; however, modern operating systems are increasingly integrating mobile and stationary devices. Nonetheless, these devices are typically linked via home networks, which are considerably more secure than connections through public wireless or carrier networks. In such instances, the likelihood of a man-in-the-middle (MiTM) attack is significantly heightened (Karen, Souppaya, Scarfone, 2013). In summary, enhancing the security of our information necessitates collaborative efforts from all stakeholders, including ourselves, internet service providers, mobile device makers, and mobile operating system developers, among others.

DEVICES AND THE WORKPLACE

The most instances of cybercrime occur in the absence of adequate control over the equipment utilized. This holds true from a personal standpoint and, undoubtedly, entails greater risk from a company viewpoint. Exercising control over installations and the connectivity of devices to the Internet establishes a more robust foundation for advancing a secure environment, thereby aiding in the protection of our precious information.

There are numerous instances in which employees utilize their personal gadgets at the workplace. This phenomenon is referred to as BYOD, or Bring Your Own Devices. These technologies are utilized in professional settings as frequently as in domestic environments or other locations. Employees frequently relinquish their phones to their children, who, unaware of the potential presence of important information, may inadvertently click and download something that could jeopardize the data stored within the device. Company-issued devices are governed by stringent regulations about permissible installations and connectivity protocols, whereas BYOD devices are more susceptible to malware assaults due to the absence of such stringent guidelines for users regarding appropriate content and configurations.

Cybercriminals require a gadget to facilitate the theft of information from mobile devices. They predominantly utilize tiny applications to breach those gadgets. These apps are referred to as malware and spyware, both of which can be categorized as digital viruses, although many IT professionals often distinguish between the two.

Spyware, as the nomenclature implies, is utilized to surveil consumers. They are typically employed as keyloggers to acquire passwords and similar information.

Malware frequently inflicts significant damage to the device's operating system, including resetting it, erasing its storage, and similar actions. They pose significant risks, since we may lose critical information pertaining to our enterprises and transactions.

The threat is not exclusive to corporations and enterprises; information theft poses significant risks to people who save personal data on their mobile devices. Numerous instances have occurred where hackers have appropriated images of prominent individuals and subsequently extorted substantial amounts of money to prevent their disclosure.
Since the inception of malware with the emergence of LibertyCrack in 2000, which impacted Palm OS devices by inducing a hard reset, these apps have significantly grown in tandem with advancements in mobile software and hardware (Karen, Souppaya, Scarfone, 2013).

Currently, malware such as DroidDream, NickySpy, and SMSZombie exhibit increased sophistication through various methods of targeting mobile devices.

Given the existence of millions of malware variants, we should anticipate an unparalleled failure in the domain of information security. However, such is not the situation. Indeed, significant network breaches have occurred in recent years, like the assault on Sony's PlayStation Network and, more recently, Yahoo's email system; yet, corporations are effectively safeguarding their customers' information. The manner in which we individually utilize our mobile devices presents a distinct issue. Companies that produce their own devices maintain greater control over them, enabling a stable and secure security environment. Charting our own course will undoubtedly subject us to greater risks, as has been consistently demonstrated.

THE FUTURE

Microsoft's appointment of Satya Nadella as CEO signified a profound transformation. Nadella's background in Microsoft's Cloud division indicated the company's recognition of the future potential in that sector. Other firms, such Apple and Google (now Alphabet), were already significantly invested in cloud technology, and their mobile strategies were aligned accordingly. Although Microsoft expressed interest in that specific technology, the company maintained a conventional approach in the broader market, recognizing its longstanding dominance in the PC sector with its Windows operating system. The acquisition of Nokia's mobile division was perceived by many as the commencement of Microsoft's anticipated resurgence in the mobile market. Over time, we realized that this was incorrect, necessitating a revision of Microsoft's plans. The company opted to provide its productivity services across various platforms, including iOS and Android, rather than directly competing with mobile devices. Among the primary offerings were Office 365 and Microsoft's latest web browser, Edge.

You may wonder how this relates to information security. The pertinent issue is not Microsoft's challenges as an IT enterprise, but rather the significance of Cloud services. Office 365 is likely the most prevalent online office suite. It is closely linked to Azure, the company's innovative Cloud platform that is continually expanding. Nadella's motto of "Cloud first, mobile first" appears to be yielding positive results. However, what is crucial for us as users is the ongoing efforts of organizations to enhance information security. Their primary objective is to utilize mobile devices as a conduit for accessing data stored on servers, which are generally more secure than local data storage. This does not imply the cessation of information theft; nonetheless, it represents a significant advancement toward more secure data interchange. The matter of data storage on cloud servers undoubtedly raises privacy issues regarding data management; nonetheless, for the time being, we must place our trust in these substantial corporate entities to ensure the security of our information.

CONCLUSION

The domain of information security encompasses a wide array of intricate challenges that might occupy entire volumes. In summary, we have addressed the most significant concerns we encounter daily, which I believe we have accomplished. This statement indicates that users, particularly ordinary individuals, are caught in a conflict between cybercriminals and huge corporations, with no clear resolution anticipated. Currently, the majority of conflicts are resolved favorably for those users, and we sincerely anticipate this will culminate in a definitive victory, barring any unforeseen complications. Information is crucial in the contemporary economy. It constitutes the foundation for corporate processes, innovation, and competitive advantage. Consequently, safeguarding information is a crucial business purpose.

Nonetheless, information is susceptible to attacks. Cyberattacks, data breaches, and human errors may result in security incidents that cause data loss, operational disruptions, and reputational harm. Consequently, safeguarding information is a fundamental corporate purpose. Through the use of information security measures, enterprises may safeguard their data and attain their organizational objectives.

References and bibliography

1. Various authors; The impact of mobile devices on information security – a survey of IT professionals; Dimensional Research; 2013
2. Various authors, Managing security in a mobile world; PWC; 2012
3. Bergman, Neil; Stanfield, Mike; Rouse, Jason; Scambray, Joel; Mobile hacking exposed; McGraw Hill; 2013
4. Various authors; The impact of mobile devices on information security – a survey of IT professionals; Dimensional Research; 2013
5. Ibid
6. Bergman, Neil; Stanfield, Mike; Rouse, Jason; Scambray, Joel; Mobile hacking exposed; McGraw Hill; 2013
7. Urbas, Gregory; Krone, Tony; Mobile and wireless technologies: security and risk factors; Australian Institute of Criminology; 2006
8. Souppaya, Murugiah; Scarfone, Karen; Guidelines for Managing the Security of Mobile Devices in the Enterprise; U.S. Department of Commerce; 2013