Available online at: http://www.advancedscientificjournal.com
http://www.krishmapublication.com
IJMASRI, Vol. 1, issue 1, pp. 271-276, Apr. -2025
https://doi.org/10.53633/ijmasri

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY ADVANCED SCIENTIFIC RESEARCH AND INNOVATION (IJMASRI)

ISSN: 2582-9130 **IBI IMPACTFACTOR 1.5** **DOI: 10.53633/IJMASRI**

RESEARCH ARTICLE

SECURITY COUNTER MEASURES IN THE CYBER-WORLD

Naveen Kumar A[1] Vijaya Babu B[2] and Praveen B[3]

[1,2,3] *PG & Research Department of Computer Science, St. Ann's College of Arts and Science, Tindivanam -604 001*

Abstract

As a result of increasingly automated procedures, the Internet of Things, and everyday activities carried out via mobile devices, the internet, and other ideas introduced by technological advancement, businesses and individuals are becoming more and more reliant on technology. However, given the speed at which technology is developing, cyber threats pose a significant threat that calls for prompt, ongoing action. Corporate and individual users of the internet are continuously fighting to maintain a suitable level of protection over their assets since cybercrime is a persistent and growing danger. With the ultimate goal of defining security countermeasures that organizations from specific business sectors could implement to concentrate their limited resources and budget on mitigating the right risks, this paper outlines the correlations and patterns found in the analysis of 4,785 attacks that have been deployed globally in recent years.

Keywords: security; controls; cyber-attacks; data analysis; logistic regression

Introduction

Rapid technological advancements present new hazards and difficulties. Technology has never been more important for daily routines and activities. This is seen in the usage of information systems in enterprises' IT-dependent processes, real-time mobile reporting, and growing reliance on IoT devices. However, the impact that a possible catastrophe could have grows along with the significance of IT in our personal and professional life

Review of Literature

Many writers have tackled the security issues that exist in cyberspace. According to P. W. Singer and A. Friedman (2014), an organization's perception of incentives has a direct impact on how it will handle risks and vulnerabilities. [3] Similarly, Gordon, Loeb, Lucyshyn, and Zhou examined the cost-benefit analysis of security decisions. According to the report, "underinvestment in cyber security poses a serious threat to the national security and to the economic prosperity of a nation." As a result, incentives should be reinforced to encourage businesses to invest more in cyber security. William Pilgrim (2014) examines how human behavior might contribute to increased

cyber-security, outlining the primary steps people can take to enhance cyber-hygiene and, consequently security.

In his description of the primary frameworks and standards pertaining to cyber-security, Purser (2014) draws the conclusion that the speed at which standards are developed is significantly slower than the speed at which technology is evolving and that governments and organizations must work together to ensure that standards are robustly and quickly adapted to the new challenges that technology presents.

National rules and regulations, such as the Health Information Trust Alliance (HITRUST) in the US and the Data Protection Act in the UK, also promote information security. These typically center on how businesses manage people's private information to protect and preserve data privacy. The geographical delineation of states is strongly tied to rules, and as internet usage transcends
physical boundaries, provisions and coverage may vary from one location to another.

Methods of Research

Hypothese

Our research's primary goal was to pinpoint security-specific countermeasures that companies in particular industries may use to make sure their little funds and resources are going toward reducing the appropriate risks.

Three hypotheses served as the foundation for the study:

Hp1: There is a relationship between the target's business sector and the kind of attacks used. In order to enable the design and implementation of security controls in the areas where they are most needed, testing this hypothesis aims to identify the sorts of attacks that are used against specific business sectors.

HP2: There is a connection between the victim's business sector and the security breaches. on order to support concentrating the limited resources and budget on minimizing the appropriate risks, testing this hypothesis aims to discover the primary root causes that permit security breaches in organizations operating in specific business sectors.

Hp3: There is a relationship between the target's business sector and the attack source.
The purpose of testing this hypothesis is to determine the primary attack sources in order to facilitate improved information security control management and monitoring.

Data Collection

The data was statistically analyzed to test the hypothesis. One of the largest competitors in the global security market, Verizon, centrally managed 4,785 security incidents for the study's population under the VCDB project. The data set includes security breaches that Verizon gathered in what is thought to have been one of the earliest attempts to compile pertinent security event data and make it publicly accessible.

The distribution of attacks by victim countries. It reveals that while attacks occur all over the world, the United States, Great Britain, Canada, India, Australia, New Zealand, Republic of Korea, Ireland, Japan, Israel, Denmark, China, Turkey, and Russia are the most frequently targeted regions.

Data Analyzing

Dedicated software provided great support for the analysis. The data was organized and cleaned using Microsoft Excel to guarantee accuracy and completeness. Only the variables thought to have a statistical relationship with the business sector were included in the analysis, despite the database having comprehensive information about the incident, attacker, and victim. These variables included the victim's business sector, the attack pattern and actor, the root cause of the security breach, and the discovery method.

The final dataset contained 4,785 occurrences, all of which were valid, complete, and accurate records. SAS Studio was used to import the data for statistical analysis. The first model included every variable the

authors thought had a statistical connection to the business sectors, such as

Industry = Pattern + Actor + Root cause + Discovery method (1).

Where the dependent variable (y) is the industry and the independent variables (x) are the pattern, action, actor, root cause, and discovery method.

The Logistic Regression

A logistic regression model, which Hastie et al. (2008) define as "used mostly as a data analysis and inference tool, where the goal is to understand the role of the input variables in explaining the outcome" [10], was thought to be the most effective way to accomplish the goal of the study. Starting with all variables, a stepwise model was built, taking into account only statistically representative variables for each model. As shown in Table 1, a distinct model was thus produced for each of the areas that were examined.

PRIMARY OUTCOMES AND ADVICE

The outcome was a distinct model for every company area. As a result, each was examined independently.

Accomdation and food service

The findings indicated that, with a likelihood of more than 88%, payment card skimming is the most likely attack type to be used. However, with a likelihood of 9.34%, privilege misuse is comparatively unlikely to happen. Therefore, safeguarding client data from both internal and external attackers should be the main priority for lodging and food service businesses.

However, educating employees and clients about this particular risk and urging them to notify the appropriate team if they notice any strange activity or devices could also assist improve the security of payment systems and procedures.

Finance and Insurance

In contrast to other sectors that use card payments, the banking and insurance industries are frequently the targets of payment skimming attempts, which have a greater than 87% chance of being detected by the internal fraud detection service. Though it is unlikely to be carried out inside, foreign attackers are most likely to use the ATMs to carry out the attack. The security of payment card operations, customer data protection, and privacy may all be improved by closely monitoring the ATMs and raising consumer knowledge of the dangers of card skimming.

Given the expense, incentives might be needed to motivate businesses to increase the security of their operations and devices.

Retail Traders

The findings indicated that there was a greater than 90% chance that an attack would be launched on the point of sale if it was directed at a retail establishment. Card skimming may also fall under this category; however POS malware is the most common method. Often referred to as memory-scraping malware, it is a piece of software that searches the computer's memory for card data and stores it in a specific spot that the attacker can quickly access. The fact that data is only encrypted during the authorization phase and not during the card swiping or reading process is exploited by the malware.
By implementing more sophisticated and secure systems, like EMV technology, retail businesses can lower this risk. An EMV card creates a unique transaction code each time it is used, therefore duplicating it would be pointless because the same code cannot be used twice, unlike magnetic-stripe cards, which are easily duplicable once data is received.

A portion of the answer lies with the manufacturers of payment systems, who should constantly work to guarantee the implementation of cutting-edge and secure technology, as well as with consumers, who should stay up to date with the most recent developments in safe payment methods.

Public sector

Results indicate that internal staff negligence is the most likely root cause, with a probability greater than 80%, even though no single pattern is primarily used on public sector organizations (public administration, educational services, health and social assistance, administrative, and waste management). Consequently, a number of suggestions could be made to deal with this problem. First and foremost, information security rules should be well-documented in every organization. These could include, but are not limited to: password management, internet and email use, software and hardware use, data privacy and protection, etc.

RECOMMENDATIONS AT THE GENERAL LEVEL

Security is more than just putting controls in place, even while the study clearly identifies the primary threats and security lapses that each business sector faces. Regardless of the industry in which the organization operates, the authors think that there are some actions that could assist raise the overall degree of security.

Risk Management Framework

Establishing and maintaining a risk management framework is a crucial step in guaranteeing information security. Risk management is "the program and supporting processes to manage information security risk to organizational operations (including mission, functions, and reputation), organizational assets, individuals, other organizations, and the public," according to NIST SP 800-39, Managing Information Security Risk.

The NIST risk management model, which is detailed in NIST special publication 800-37 Revision 1, Guide for Applying the Risk Management methodology to Federal Information Systems: a Security Life Cycle Approach, is one methodology that businesses could use. The six-step method used by the framework to build the risk management process is as follows: [12] Information systems can be categorized, security controls can be chosen to be implemented, security controls can be implemented, security controls can be assessed, information systems can be authorized, and security controls can be monitored.

Standard and Legislation

The preceding sections showed how laws and norms don't always manage to keep up with the quick advancement of technology. Amazon is a real-world example; despite having SAS 70 certification, the company has experienced significant security issues in recent years. [13] Scott J. Shackelford (2014) provides another example, stating that the international law pertaining to information technology frequently turns out to be "ambiguous and According to the authors, a collaborative effort between national and EU authorities as well as IT and security experts will help norms and laws keep up with technical advancements, hence promoting the safe use of information systems.

Incentives for information sharing

To face the risk, one must first comprehend the hazard. The usefulness of information sharing is demonstrated by the fact that the data analysis used to support this study enabled the authors to identify trends and connections between the features of assaults and the targeted economic sectors. But the event simply demonstrates how reluctant organizations are to divulge private information. "Most organizations would never risk affecting their reputation by publicly admitting their information security was breached, which could affect their reputation and customers' trust," according to P. W. Singer and A. Friedman in their book Cyber Security and Cyber War: What Everyone Needs to Know.

Incentives can be mandated, for instance, by consumers and do not always need to be in the form of legal regulations. Mendicant, the first business to disclose an investigation of security vulnerabilities found at its clients, is used as an example by P. W. Singer and A. Friedman. Even though the conduct was deemed ridiculous at the
time and was predicted to cause the company's trust with prospective clients to decline, it actually improved the entity's reputation, and many businesses

adopted its example as a marketing tactic in the years that followed.

General Awareness

As was already established, businesses see cyber-security from a cost-benefit viewpoint. Most organizations will choose to overlook the risk as long as the costs of addressing it outweigh the advantages of implementing control. Therefore, authors think that in order to take action, a shift in perspective is necessary. Organizations' investment in security would naturally rise in response to market demands if, for instance, information security were a requirement of customers (for instance, individual customers or business partners would include security controls as a mandatory requirement for the development of the business relationship).

Initiatives to raise public awareness have grown in number in recent years. The UK government started a national cyber security campaign in 2014 called "Cyber Streetwise," which offers security tips that all tech users should follow to guarantee a minimum degree of protection.

References

1. Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, Lei Zhou (2015), Externalities and the Magnitude of Cyber security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model, Journal of Information Security, Vol.06 No.01(2015), Article ID:52952, available online at: http://file.scirp.org/Html/3-7800247_52952.htm, accessed 25 September 2015.
2. Hausken, K. (2007) Information Sharing among Firms and Cyber Attacks, Journal of Accounting and Public Policy, 26, 639-688. http://dx.doi.org/10.1016/j.jaccpubpol.2007.10.001 (accessed 24 June 2015).
3. Singer, P. W. and Friedman, A. (2014). Cyber security and cyber war – what everyone needs to know. Oxford University, 35-197.
4. Gordon, L.A., Loeb, M.P. and Sohail, T. (2010) Market Value of Voluntary Disclosures Concerning Information Security. MIS Quarterly, 34, pp. 567-594.
5. William Pelgrin (2014), book chapter – A model for positive change: influencing positive change in cyber security strategy, human factor, and leadership, Best practices in computer network defense: incident detection and response, IOS Press, ISBN 978-1-61499-371-8, pp. 107- 110.
6. Steve Purser (2014),book chapter – Standards for Cyber Security, Best practices in computer network defense: incident detection and response, IOS Press, ISBN 978-1-61499-371-8, pp. 97-106.
7. Data Protection Act 1998 (2015), available online at:http://www.legislation.gov.uk/ukpga/1998/29/data.pdf, (accessed on 15 September 2015).
8. European Network and Information Security Agency (ENISA) (2012), National Cyber Security Strategies – Practical Guide on Development and Execution, available online at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national- cyber-security-strategies-ncsss, (accessed on 12 September 2015).
9. Bendovschi, A., Tinca, A., Ionescu, B., Plescan, D. (2014), Cloud computing – enabling drivers and adoption issues, Proceedings of the 9th International Conference Accounting and Management Information Systems AMIS 2014, ASE, ISSN 2247-6245, pp. 264-265.
10. Hastie, T., Tibshirani, R. and Frienman, J. (2008), The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer, pp. 115 – 128.
11. Dempsey, K., Witte, G., Rike, D. (2014), Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information systems and Organizations, National Institute of Standards and Technology, US Department of Commerce, available online at: http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800- 53r4_summary.pdf, (accessed on 28 July 2015).
12. NIST (National Institute of Standards and Technology), US Department of Commerce (2008), NIST Special Publication 800-53A – Guide for Assessing the Security Controls in Federal Information Systems, pp.13-26.
13. Bendovschi, A., Ionescu, B. (2015), The Gap between Cloud Computing Technology and the

14. Audit and Information Security Supporting Standards and Regulations, Audit financiar, XIII, Nr. 5(125)/2015, ISSN: 1583-5812, pp. 115-121.
15. Scott J. Shackelford (2014), Managing cyber attacks in international law, business and relationships, Cambridge University Press, ISBN: 978-1-107-00437-5, pp. 5-10.
16. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, available online at: https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arr a_with_index.pdf (accessed 19 December 2015).

******