Why Should Security Train My Staff?

Melvin Sumon Chandra
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
melvinsumonchandra@student.utwente.nl

ABSTRACT

The human element is an overlooked aspect of cybersecurity in an organisational context. To increase the security in an organisation, they tend to launch a security awareness program (e.g. a series of e-learning) aiming to teach their staff to behave more secure (e.g. not click on a link of a phishing email or to report security incidents at the security department). This article aims to analyse the benefits of security interventions which then leads to the reduction in vulnerability of an organisation in terms of economic benefits. A literature review is done to compile research done on the benefits of security awareness training, and a simulation study is carried out to create a model which illustrates how investments in security awareness can affect the expected monetary benefits from such investments. Based on the model, the rate of change of the expected benefits slowly decreases for an increasing amount of investments. The results further suggest that organisations should aim for the optimal amount of investment where the difference between the benefits and investment costs are maximised.

Keywords

Security awareness, cyberattack, organisation, cybersecurity, economic benefits

1. INTRODUCTION

1.1 Background

Cyberattacks have been an ongoing issue over the past decade, especially for companies and organisations which relies on their private belongings to be secured safely. This has raised concerns, especially as cyber threats are emerging from all sides in different forms. Companies have invested heavily in their cybersecurity areas in order to prevent unwanted security breaches in their organisation, although this has proved to be insufficient to completely protect their valuable private resources. Since the COVID-19 pandemic, the US Federal Bureau of Investigation (FBI) has reported a 300% increase in reported cybercrimes, as a result of the increase of remote working which leads to vulnerable networks [7]. Employees and staff of many organisations are in general the main target of these cyberattacks, as they are believed to lack the knowledge and awareness in cybersecurity. A study from International Business Machines (IBM) shows that 95% of cybersecurity breaches are due to human error [13]. These human errors can be caused by different actions, such as clicking on suspicious links from phishing emails and using weak password combinations. Sheng et al. found that gender and age are the two key demographics that predict susceptibility [22]. They concluded that women and employees within the age group of 18 to 25 are much more likely to fall for phishing than others.

These type of mistakes not only put the individual at risk but at the same time endangers the organisation they are working for. Hence, companies and organisations need to offer security awareness programs for their employees in order to teach their staff to become more aware and prepare them with the knowledge needed to avoid these cyber attacks. It is also important to note that gaining knowledge from these security campaigns does not necessarily mean that the employees are motivated enough to behave according to the knowledge they received, as mentioned by Khan et al. [15]. Information security is a business process that requires a cultural change for most of the employees, and one of the ways to do this is by informing them on the importance of information as an asset and property of their organisation [26].

The security awareness program is created to provide cybersecurity education which is generally designed for employees of organisations with the aim of protecting the organisation's data and assets from unwanted security incidents. The goal is to familiarise a company's workforce with various security threats and how to handle such issues with regards to the formal procedure. Different tools and techniques can be used to provide education and training for the employees. Some of the most common methods include presentations, posters, video games, computer-based training (CBT), etcetera. Khan et al. were able to rank different security awareness training methods based on their effectiveness [15].

1.2 Related Work

In order to collect literature related to the research domain, Scopus, Google Scholar, and Science Direct were used. Using the search terms such as 'security awareness' and 'cybersecurity', several articles can be found which can be used as references for this research.

The work by Thomas Peltier [26] discusses the key elements and factors to consider when implementing a security awareness program in order for it to be successful. On a similar note, a few articles also managed to evaluate the current situation of security interventions through different means in terms of their effectiveness [2, 15]. An-

28^{th} *Twente Student Conference on IT* Febr. 2^{nd}, 2018, Enschede, The Netherlands.

other article acknowledged the need for effective security awareness programs [1] and a couple offered improvements in order to make them more effective [14, 17]. Similarly, Stanton et al. analysed the user behaviour changes after security awareness training [23].

Updating their work from 2012, Anderson et al. [3] managed to utilise their framework for analysing the costs of cybercrime in 2019, where cyber attacks are much more varied. There is also a couple of pieces of literature that explores cyber risks and losses from the perspective of insurance [27, 6] where a method to infer cyber loss distributions from insurance prices was introduced.

Previous studies by Lerums et al. have introduced a simulation model for analysing the effectiveness versus the cost of cybersecurity options [18]. The model has successfully calculated the overall probability of success and the overall costs of all defence mechanism.

Gordon and Loeb constructed an economic model that determines the optimal amount to invest to protect a given set of information [9]. Their findings have shown that the optimal amount to spend on information security is an increasing function of the level of vulnerability of such information.

Canfield and Fischhoff demonstrated an approach for assessing the benefits and costs of interventions given the vulnerability of users towards phishing attacks [4]. Their approach uses the Monte Carlo simulation which in the end estimates greater net benefit for interventions targeted for vulnerable users and suggested that interventions to reduce response bias have greater net benefit than interventions to increase sensitivity.

1.3 Problem Statement

Despite being one of the most important assets of an organisation, employees are one of the weakest links in the security chain [14]. As written in the *Security Awareness: Best Practices to Secure Your Enterprise* book, the impact of information security breaches coming from people inside an organisation is bigger than all other sources combined. This should alarm organisations to consider offering security awareness programs within the organisation. However, companies tend to overlook the security awareness factor mainly due to the feeling that the use of advanced security technology is enough to protect them from unwanted and unexpected cyber-attacks [1] and the idea of spending more money on security education is not appealing for them. In addition, both findings from Tan et al. and Alshaikh et al. mentioned that organisations are still compliance-driven - they have security awareness programs out of formality and not out of motivation to actually protect their organisation from cyber attacks [25, 2].

Most companies fail to invest in cybersecurity education for their employees [17] and security awareness among the employees are lower than expected. This allows cybercriminals to target this vulnerable group to attack and gain money and private information from these companies. Most of the time, the damage costs from these cyber-attacks are higher than the costs to organise security awareness programs. Anderson et al. presented their framework for analysing the cost of cybercrime [3], and indicated that the defence costs are lower than the direct and indirect loss from cybercrime combined.

Consider a scenario where a company of 50 employees is interested in investing in a security awareness program. However, they lack the information on the benefits of offering such awareness programs and have actually never experienced any security incidents since the company was founded one year ago. This leads to the question of whether offering a security awareness program is worth the money, and if they are actually beneficial for the company.

1.4 Research Questions

This thought process from the problem statement has lead to the following research question:

How does security awareness programs help in reducing the costs of security incidents?

This can be answered with the help of the following sub-questions:

1. What are the benefits of organising security awareness programs for employees and the organisation?
2. How does the total cost of organising security awareness programs relate to the expected monetary benefits?

2. METHODOLOGY

2.1 On Answering Research Question 1

To help answer the first research question, a literature review is done. As previously mentioned, the literature is collected through Scopus, Google Scholar, and Science Direct. In order to focus on answering the first research question, the keyword 'benefit' is added to the search terms to filter out unrelated papers and articles. A detailed discussion of the literature review is shown in the Results section.

2.2 On Answering Research Question 2

2.2.1 Research Approach

The approach taken for this research is to conduct a simulation study, in which large data points will be generated and analysed using the SPSS Statistics software based on a given data set. The purpose of this study is to acquire a model that illustrates how investments in security awareness can affect the expected monetary benefits from said investments. The model considers how the probability of occurrence and success of cyberattacks together with the cost of impact from such attacks (data loss, recovery price, etc.) play a role in the expected monetary benefits from having security awareness programs.

The concept itself is influenced by the work of Lawrence A. Gordon and Martin P. Loeb on the 'Economics of Information Security Investment' [9] where they have presented an economic model that determines the optimal amount to invest to protect a given set of information. The information security in their model is largely interpreted for the technical aspect of security defence such as the software and hardware security investments (encryption, firewalls, etc.), while this model focuses more on the human aspect of cybersecurity through security awareness programs.

2.2.2 Data Collection

Several variables will be considered for the first step in creating the data set, but only some of the parameters will be used for the simulation process. To deduct which parameters to use for the creation of the initial data set, data collection will be done.

The first step is to study the prices of offering a security awareness program. Unfortunately, there is a lack of academic research on this specific topic. Hence, a different approach is used to find the related information needed

to create the data set. A simple Google search with the search term 'security awareness program price' resulted in numerous results. When most of the results tend to disclose their plan and pricing, KnowBe4, where according to their website is 'the world's first and largest New-school security awareness training and simulated phishing platform', was able to provide their service plans and pricing levels on their website [16]. This information can be used as the base for the data set.

Their prices are based on the subscription levels - Silver, Gold, Platinum, and Diamond. As the level increases, more features and training are offered. Organisation Size is also taken into account for their pricing plan. In general, the prices per seat decreases as the organisation size increases. As might be expected, the prices per seat also increase as the subscription level increases. The information collected from their web page was sufficient to start building upon the first data set with the Organisation Size, Package Level, Price (USD), and the Total Cost of Training (total investment) as the initial data set. The Total Cost of Training is obtained as a product of the Organisation Size and Price per seat for the training.

In Gordon and Loeb's model, three main parameters are considered. They each represent the loss conditioned on a breach occurring, the probability of a threat occurring, and the probability that a threat once realised will be successful [9]. For this particular model, a similar concept will be introduced.

The probability of an attempted breach is defined as the Probability of Occurrence of an attack in the model. To find relevant information to fit the current data set, insights from threat reports were used. However, due to the lack of information and data on cyberattacks in general, a more specific type of cyberattack is considered. Phishing is considered to be the most common cyberattack and both organisations and individuals are vulnerable to such threats. In 2019, 65% of U.S. organisations experienced a successful phishing attack according to Proofpoint's 2020 State of the Phish annual report [21]. Symantec's threat report was able to provide the numbers for the probability of occurrence, which also happens to differ for different ranges of organisation size [24]. In their 2019 Internet Security Threat Report, data is provided on the email phishing rate per user by organisation size (in a year). 1 in 52 users (1.92%) are targeted in an organisation size of 1 to 250. 1 in 57 users (1.75%) are targeted in an organisation size of 251 to 500. 1 in 30 users (3.33%) are targeted in an organisation size of 501 to 1000.

Generally, an organisation cannot control threats but must rely on legal and political authorities for protection. This does mean that the probability of occurrence tends to be constant. It can, however, try to reduce the impact of attacks (e.g., through network segmentation or limiting permissions across the network) or its vulnerability (e.g., through behavioural interventions) [4]. For this model, the vulnerability of an organisation is defined as the Probability of Success of an attack. Attackers can initiate cyberattacks on companies, but these attacks are not always successful and can be prevented through security measures. For the purpose of the model, a similar assumption to Gordon and Loeb's paper is made such that organisations can influence the Probability of Success of cyberattacks through investments in security awareness programs but not for the Probability of Occurrence.

Data collection for the Probability of Success is more challenging. The success rate of phishing attacks is unknown, though controlled experiments often achieve alarmingly high success rates [19]. As a result, an approximation is used for the data on the probability of success. In this stage, an approximation input is acceptable as the data set will be simulated for the analysis. In an organisation size of 1 to 250, the probability of occurrence of a cyberattack is at 40%, 45% for an organisation size of 251 to 500, and 50% for an organisation size of 501 to 1000.

As mentioned before, the vulnerability of an organisation can be reduced. Through means of investments in security awareness programs, the probability of success of an attack could decrease significantly. In other words, the Probability of Success (after intervention) is dependent on the Total Cost of Training. The general assumption for this model is that an investment in a security awareness program will always lead to a decrease in the Probability of Success. Similarly, due to the lack of information, an approximation is used to describe the decrease in the Probability of Success (after intervention).

The last parameter required for the data set is the expected monetary loss to the organisation due to the security breach. It is depicted as the Cost of Impact in the model. The most common causes of monetary loss are data loss, customer loss and damage to company reputation [5]. Although the cost of impact depends on several different factors and can change over time, for simplicity the parameter will be a fixed estimate. Compiled from Continuum [5], SMBs that have between 10 to 49 employees report a business cost of $41,269 due to a cyberattack, $48,686 for 50 to 249 employees and $64,085 for 250 to 1000 employees.

From the data collection step which has been completed, an initial data set has been compiled in which will be used in the next step for the simulation process. An illustration of part of the data set is shown in Table 1.

2.2.3 Data Analysis

Based on the collected data set, a predictive model on how the total cost of training affects the economic benefits of security awareness will be generated and analysed. To account for uncertainty in the inputs to predictive models and evaluate the likelihood of various outcomes of the model in the presence of that uncertainty, data simulation is conducted [12]. The original 80-point data set will be simulated in order to create a new data set containing a hundred thousand data points. The simulation itself will be done in SPSS Statistics, which uses the Monte Carlo method.

SPSS provides its own simulation tool and interfaces for working with the simulation called Simulation Builder. For this simulation, simulated data can be created without a model. From all the fields in the original data set, only six will be simulated. This includes the Organisation Size, Cost of Impact, Probability of Occurrence, Probability of Success, Probability of Success (after intervention), and the Total Cost of Training. Once completed, a new file containing a hundred thousand data points is generated.

Gordon and Loeb defined the probability of the loss occurring as the product of the vulnerability and threat probabilities. Hence, the product between the Probability of Success, Probability of Occurrence, and Cost of Impact represents the expected monetary loss given the absence of security awareness program investments.

Thus, the expected benefits of an investment in security awareness, denoted as EBIS, are equal to the reduction in an organisation's expected monetary loss given the invest-

Table 1. Part of the initial data set.

Organisation Size	Package Level	Price (USD)	Total Cost of Training	Probability of Occurrence	Probability of Success	Probability of Success (after intervention)	Cost of Impact
50	Silver	$18,00	$900,00	1,92%	40,00%	30,00%	$41.269,00
50	Gold	$21,75	$1.087,50	1,92%	40,00%	25,00%	$41.269,00
50	Platinum	$25,50	$1.275,00	1,92%	40,00%	20,00%	$41.269,00
50	Diamond	$30,50	$1.525,00	1,92%	40,00%	15,00%	$41.269,00
100	Silver	$16,00	$1.600,00	1,92%	40,00%	30,00%	$48.686,00
100	Gold	$19,25	$1.925,00	1,92%	40,00%	25,00%	$48.686,00
100	Platinum	$22,50	$2.250,00	1,92%	40,00%	20,00%	$48.686,00
100	Diamond	$27,50	$2.750,00	1,92%	40,00%	15,00%	$48.686,00
150	Silver	$13,00	$1.950,00	1,92%	40,00%	30,00%	$48.686,00
150	Gold	$15,50	$2.325,00	1,92%	40,00%	25,00%	$48.686,00
150	Diamond	$18,00	$2.700,00	1,92%	40,00%	20,00%	$48.686,00
150	Platinum	$23,00	$3.450,00	1,92%	40,00%	15,00%	$48.686,00
200	Silver	$13,00	$2.600,00	1,92%	40,00%	30,00%	$48.686,00
200	Gold	$15,50	$3.100,00	1,92%	40,00%	25,00%	$48.686,00
200	Diamond	$18,00	$3.600,00	1,92%	40,00%	20,00%	$48.686,00
200	Platinum	$23,00	$4.600,00	1,92%	40,00%	15,00%	$48.686,00
250	Silver	$13,00	$3.250,00	1,92%	40,00%	30,00%	$48.686,00
250	Gold	$15,50	$3.875,00	1,92%	40,00%	25,00%	$48.686,00
250	Diamond	$18,00	$4.500,00	1,92%	40,00%	20,00%	$48.686,00
250	Platinum	$23,00	$5.750,00	1,92%	40,00%	15,00%	$48.686,00
300	Silver	$13,00	$3.900,00	1,75%	45,00%	32,50%	$64.085,00
300	Gold	$15,50	$4.650,00	1,75%	45,00%	27,50%	$64.085,00
300	Diamond	$18,00	$5.400,00	1,75%	45,00%	22,50%	$64.085,00
300	Platinum	$23,00	$6.900,00	1,75%	45,00%	17,50%	$64.085,00
...	...	...	...	...	...	...	...
550	Silver	$12,00	$6.600,00	3,33%	50,00%	35,00%	$64.085,00
550	Gold	$14,25	$7.837,50	3,33%	50,00%	30,00%	$64.085,00
550	Diamond	$16,50	$9.075,00	3,33%	50,00%	25,00%	$64.085,00
550	Platinum	$21,50	$11.825,00	3,33%	50,00%	20,00%	$64.085,00
600	Silver	$12,00	$7.200,00	3,33%	50,00%	35,00%	$64.085,00
600	Gold	$14,25	$8.550,00	3,33%	50,00%	30,00%	$64.085,00
600	Diamond	$16,50	$9.900,00	3,33%	50,00%	25,00%	$64.085,00
600	Platinum	$21,50	$12.900,00	3,33%	50,00%	20,00%	$64.085,00
...	...	...	...	...	...	...	...
950	Silver	$12,00	$11.400,00	3,33%	50,00%	35,00%	$64.085,00
950	Gold	$14,25	$13.537,50	3,33%	50,00%	30,00%	$64.085,00
950	Diamond	$16,50	$15.675,00	3,33%	50,00%	25,00%	$64.085,00
950	Platinum	$21,50	$20.425,00	3,33%	50,00%	20,00%	$64.085,00
1000	Silver	$12,00	$12.000,00	3,33%	50,00%	35,00%	$64.085,00
1000	Gold	$14,25	$14.250,00	3,33%	50,00%	30,00%	$64.085,00
1000	Diamond	$16,50	$16.500,00	3,33%	50,00%	25,00%	$64.085,00
1000	Platinum	$21,50	$21.500,00	3,33%	50,00%	20,00%	$64.085,00

Table 2. Parameter Estimates generated from the Curve Estimation.

Equation	Parameter Constant b0	Estimates b1
Logarithmic	-778.913	122.732

ment in extra security awareness. In other words:

$$EBIS = [\text{Probability of Success} - \text{Probability of Success (after intervention)}] \times \text{Probability of Occurrence} \times \text{Cost of Impact}$$

EBIS ultimately allows for the reduction of costs for security incidents. To illustrate the relationship between the investments in security awareness and the EBIS, a scatter plot of the EBIS against the Total Cost of Training is generated. With the Curve Estimation tool from SPSS, the model summary and parameter estimates are also generated together with the scatter plot and an illustration of the line of best fit. The model summary is shown in Figure 1 and the parameter estimates in Table 2.

The next step of the research is to conduct regression analysis using the simulated data set containing the EBIS. Regression analysis is defined as a set of statistical processes for estimating the relationship between a dependent variable (or outcome variable) and one or more independent variables (or predictors). This also allows for the creation of the predictive model which will also be analysed. In the case of this model, EBIS is the outcome variable of the model. The Probability of Success (after intervention) has not been included in the regression analysis since it might cause overlap in the analysis as they are correlated. Recall that the Probability of Success (after intervention) is dependent on the Total Cost of Training. Having the Total Cost of Training in the model is enough to represent both variables.

Table 3. Parameter Estimates generated from the Nonlinear Regression.

Parameter	Estimate	Std. Error
Constant	466.370	12.906
Organisation Size	-0.215	0.002
Cost of Impact	0.016	0.000
Probability of Occurrence	266.563	1.420
Probability of Success	-65.176	0.453
Total Cost of Training	155.378	0.532

The nonlinear regression method is used as an alternative from the normal linear regression, which will be discussed further in the Results section. The result of the regression includes parameter estimates which allow the construction of the model expression of EBIS using the previously indicated predictors. They will be used for predicting the dependent variable from the independent variable through the regression equation. The generated result is illustrated in Table 3.

However, the results from Table 3 are unstandardised coefficients because they are measured in their natural units and as such the coefficients cannot be compared with one another to determine which predictor has the most influence in the model as they can be measured on different scales [8]. As a result, a different approach is offered to determine the influence and significance between the predictors. Using the Automatic Linear Modelling tool from SPSS, a predictor importance graph is produced which is shown in Figure 2.

A detailed discussion of all the regression results will be done in the Results section.

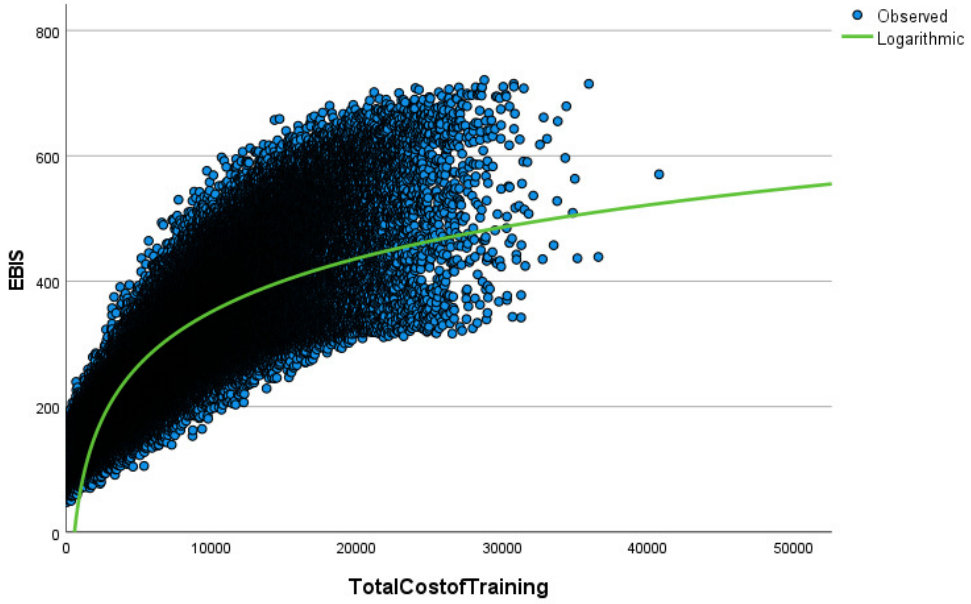

Figure 1. Curve Estimation of the EBIS against the Total Cost of Training.

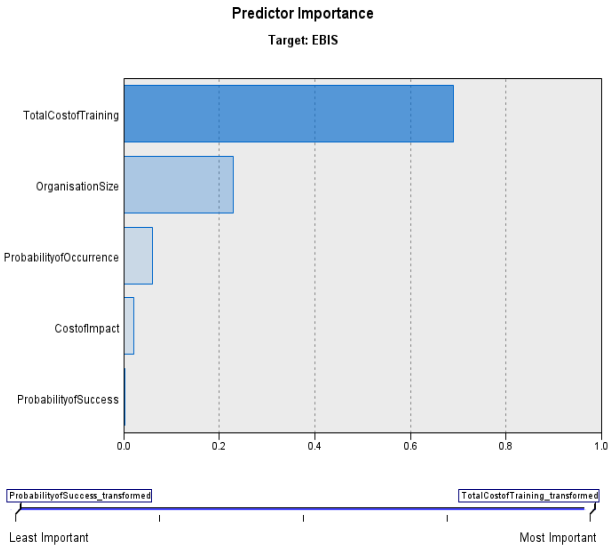

Figure 2. Predictor Importance.

3. RESULTS

3.1 Answering Research Question 1

When a security awareness program is proved to be successful, various benefits can be attained by both the employees and the organisation itself. As mentioned in the article by Everett C. Johnson [14], the major benefit of having a security awareness program is to ensure that the overall security risks are mitigated. This does not necessarily mean that all of the security incidents are diminished, but they are reduced to the point that there will be fewer internal errors which can lead to major security incidents. Security awareness adds and improves the protection of the confidentiality of an organisation's information, such as data and assets. This can be done due to the possibility of detecting potential security breaches before it is initiated. For example, employees would be able to differentiate phishing emails from normal emails and would anticipate such issues in the future which prevents security breaches from occurring.

From an economical perspective, security awareness can be the most cost-effective solution [20], as it allows employees to adopt a more preventive and proactive approach rather than a reactive one [10]. According to Continuum's 2019 report, their respondents' Small and Midsize Business (SMB) organisation report a total business impact cost of $53,987 on average due to a cyberattack [5]. The impact costs are for one cyberattack incident, and often organisations experience more than one incident per year. By investing in security awareness programs, organisations can observe economic benefits from said investments as the impact costs from cyberattacks are minimised. A further discussion on this topic will be conducted in the following sections.

When it comes to the loss concerns SMBs have with regards to a cyberattack, the most common are data loss (50%), customer loss (43%) and damage to company reputation (39%) [5]. With security awareness training in place, these concerns can be prevented. Johnson also mentioned that other benefits of a security awareness program include the increased confidence of (potential) customers, suppliers and shareholders in the organisation's security

[14]. This allows the increase of the company's reputation among the customers and stakeholders, attracting potential customers as well as increasing customer satisfaction, preventing the loss of customers and damage to the company's reputation.

Behavioural changes can also benefit the employees of the organisation even outside their work environment. For instance, Stanton et al. showed that good password practices (changing passwords regularly, using strong passwords) are related to security awareness programs [23]. Having good password practices can help avoid unwanted personal data breaches that are nowadays stored in their personal social media accounts. Similarly, in the case of phishing, individuals would then be able to avoid phishing emails pretending to be companies in order to steal personal data or money.

Johnson added that besides employee morale, the productivity of employees in the work environment also increases. This can be explained as now employees would need less time to distinguish and detect potential security incidents and respond accordingly as they have been trained continuously to react to such situations. Hence, as the productivity increases, profitability towards the company also increases as employees would be able to do more work within the given time, generating additional profits.

3.2 Answering Research Question 2

This section aims to discuss the results of the analysis done in the Methodology section as well as answering the second research question.

In Figure 1, a scatter plot of the hundred thousand data points is presented. The EBIS is plotted against the Total Cost of Training. At a glance, it is noticeable that the rate of the graph is increasing at a decreasing rate. At lower values of Total Cost of Training, the EBIS is increasing at a high rate. However, as the Total Cost of Training increases, the rate of change of EBIS decreases. The graph forms an asymptotic behaviour, whereas the Total Cost of Training increases, the EBIS continues to increase to approach a certain value, but never reaches the limit. The behaviour of the graph suggests a logarithmic relation. Hence, for the Curve Estimation, a Logarithmic Model is preferred. SPSS was also able to provide parameter estimates for the model, which allows the formation of an equation for the predicted best fit curve. A logarithmic model follows the equation Y = b0 + b1 * ln(t). Based on the results from Table 2, an equation for the predicted EBIS based on the best-fit curve estimation is:

$$EBIS = -778.913 + [112.732 \times ln(t)],$$

where t = Total Cost of Training.

Following the logarithmic model for the scatter plot of the data points, it only makes sense to assume that nonlinear regression is used for the analysis. Linear regression would indicate for a linear model expression where the EBIS will increase at a constant rate without a limit, which contradicts the behaviour of the scatter plot itself. This leads to the decision of adding a logarithmic expression to the regression model. Observing the results in Table 3, the parameter estimates allows the prediction model for EBIS, where:

$$\begin{aligned} EBIS = 466.370 - (0.215 \times \text{Organisation Size}) + \\ (0.016 \times \text{Cost of Impact}) + \\ (266.563 \times \text{Probability of Occurrence}) - \\ (65.176 \times \text{Probability of Success}) + \\ [155.378 \times ln(\text{Total Cost of Training})] \end{aligned}$$

The parameter estimates illustrate the relationship between the dependent and independent variables (the EBIS and the predictors). They indicate the change in EBIS that would be predicted by changing 1 unit of the independent variable. For instance, the parameter estimate for the Cost of Impact variable is 0.016. Thus, for every unit increase of 1 USD in the Cost of Impact, the EBIS is predicted to be 0.016 USD higher. It follows a similar pattern for the rest of the independent variables in the model.

From the observed model, it is noticeable that high investments are not always the best option. Organisations should aim to invest an amount where the difference between the benefits and investment costs are maximised. This can be described as the optimal total cost of training. They can of course invest higher than the optimal amount, but the difference between the benefits and investment costs are not maximised and can even decrease as the investment costs increase above the optimal total cost of training.

Example scenarios can further help demonstrate how the model works. Recall the scenario where a company of 50 employees is hesitant on whether to invest in security awareness programs. For simplicity, data from the initial data set is used for the model input. Assume that they have a $3000 fund to invest in awareness training, but would like to first use half of the fund. Consider another company of 150 employees who lost $10,000 due to a phishing attack with a probability of occurrence at 2% and a probability of a successful attack at 40%. A summary of the scenarios is found in Table 4.

From the scenarios, it is observed that the double amount of investment does not justify the increase in EBIS (approximately $100 in this case), which is why organisations should consider the optimal total cost of training before investing in a security awareness program to maximise the difference between the benefits and investment costs.

Recall that the results in Table 3 are unstandardised coefficients and thus a higher value of parameter estimate in the prediction model equation does not indicate that the variable is more significant compare to another variable with a lower parameter estimate. The predictor importance, shown in Figure 2, helps indicate the relative importance of each predictor in estimating the model. The sum of the values for all the predictors in the model add up to 1.0 since the values are relative. Do note that the predictor importance does not relate to the accuracy of the model, as it just relates to the importance of each predictor in making a prediction and not on how accurate the prediction is [11]. From the result, the Total Cost of Training appears to be the most important predictor in predicting the model with a value of approximately 0.7, followed by the Organisation Size with a value a little above 0.2. The Probability of Success turned out to be the least important predictor in the model.

4. CONCLUSION

4.1 Research Question 1

Table 4. Example scenarios to help demonstrate the model.

Organisation Size	Cost of Impact	Probability of Occurrence	Probability of Success	Total Cost of Training	EBIS
50	$41,269	1.92%	40.00%	$1,500	$2,231.69
50	$41,269	1.92%	40.00%	$3,000	$2,338,98
150	$10,000	2.00%	40.00%	$3,500	$1,841,35
150	$10,000	2.00%	40.00%	$7,000	$1,949,05

While a lot of research on the behavioural aspects of security awareness programs have been made, more work needs to be done which addresses the economic aspects of security awareness. Security interventions are arguably the most cost-effective solution from an economical perspective. Through literature reviews, information on the benefits of security awareness programs has been compiled and analysed. Evidently, organisations offer security awareness training in order to minimise security breaches and incidents which can inflict financial loss upon them. Employees would be able to be more cautious and proactive when dealing with sensitive information, decreasing the likelihood of internal errors which can lead to fatal security incidents. Additionally, customers and stakeholders' satisfaction would increase due to the trust and confidence in the organisation's security. As the reputation grows, new potential customers and stakeholders will be attracted towards the company, increasing revenue. Through security interventions, a boost in employee's morale can be observed as they have been trained continuously to properly react in a different situation, allowing for the increase in productivity and hence growth in revenue.

4.2 Research Question 2

The simulation study in this research has shown that security awareness programs lead to a decrease in the vulnerability of organisations towards cyberattacks, which leads to cost reductions from security incidents. The expected benefits of an investment in security awareness are described as the reduction in an organisation's expected monetary loss given the investments in security awareness. Through the process of data collection and data simulation, a relationship can be made between the EBIS and the Total Cost of Training. One would expect that as the Total Cost of Training increases, the EBIS will also increase. According to the generated results from the regression analysis, an asymptotic function is observed where the EBIS is increasing at a decreasing rate as the Total Cost of Training increases. In other words, the rate of change of the EBIS slowly decreases for a higher value of Total Cost of Training. This shows that organisations should not always go for a high value of investments, but should aim for the optimal amount of investment where the difference between the benefits and investment costs are maximised. This is further proven by the example scenario where doubling the amount of investment does not necessarily double the EBIS.

For further research, consultations with actual organisations with experience in security awareness training are highly recommended, which adds to the accuracy of the data set for the simulation study. Studying the interaction effects between different variables are also suggested which allows for the increase in complexity of the model, leading to more accurate predictions. In addition, further statistical analysis can be conducted to determine the optimal amount of investment based on the model.

.

5. ACKNOWLEDGEMENTS

I would like to thank my supervisors, dr. A. Abhishta and dr. J.H. Bullee, whose insightful feedback and suggestions helped me throughout the research. Both of them were able to patiently assist me in formulating the research questions and methodology. For this, I am extremely grateful. I would like to also acknowledge my friends and colleagues who were able to provide a great deal of feedback and support which helped me in completing this research paper.

6. REFERENCES

[1] F. Aloul. The need for effective information security awareness. *Journal of Advances in Information Technology*, 3:176–183, 08 2012.

[2] M. Alshaikh, S. B. Maynard, and A. Ahmad. Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security*, 100:102090, 2021.

[3] R. Anderson, C. Barton, R. Bölme, R. Clayton, C. Gañán, T. Grasso, M. Levi, T. Moore, and M. Vasek. Measuring the changing cost of cybercrime. -, 2019.

[4] C. Canfield and B. Fischhoff. Setting priorities in behavioral interventions: An application to reducing phishing risk: Setting priorities in behavioral interventions. *Risk Analysis*, 38, 10 2017.

[5] Continuum. Undeserved and unprepared: The state of smb cyber security in 2019. Online: `http://info.continuum.net/rs/011-QRO-092/images/Underserved\%20and\%20Unprepared_\%20The\%20State\%20of\%20SMB\%20Cyber\%20Security\%20in\%202019.pdf?hsCtaTracking=912e901a-d33c-4893-afc4-6155565fde54\%7C9e2dc862-075a-4df2-990f-e491d1e15135`.

[6] EIOPA. Cyber risk for insurers - challenges and opportunities, 2019.

[7] FBI. Federal bureau of investigation internet crime complaint center ic3 2020 annual report, 2020.

[8] U. I. for Digital Research and E. S. Consulting. Regression analysis - spss annotated output. Online: `https://stats.idre.ucla.edu/spss/output/regression-analysis/`.

[9] L. Gordon and M. Loeb. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.*, 5:438–457, 11 2002.

[10] B. Hanus and Y. A. Wu. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33(1):2–16, 2016.

[11] IBM. Documentation - predictor importance. Online: `https://www.ibm.com/docs/en/`

spss-modeler/18.1.0?topic=SS3RA7_18.1.0/modeler_mainhelp_client_ddita/clementine/idh_common_predictor_importance.html.

[12] IBM. Spss statistics simulation. Online: https://www.ibm.com/docs/en/spss-statistics/27.0.0?topic=features-simulation.

[13] IBM. Ibm security services 2014 cyber security intelligence index for financial services, 2014.

[14] E. C. Johnson. Security awareness: switch to a better programme. *Network Security*, 2006(2):15–18, 2006.

[15] B. Khan, K. Alghathbar, S. Nabi, and K. Khan. Effectiveness of information security awareness methods based on psychological theories. *African journal of business management*, 5, 10 2011.

[16] KnowBe4. Knowbe4 pricing: Kevin mitnick security awareness training. Online: https://www.knowbe4.com/pricing-kevin-mitnick-security-awareness-training.

[17] K. Korpela. Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, 24:1–6, 06 2015.

[18] J. E. Lerums, L. D. Poe, and J. E. Dietz. Simulation modeling cyber threats, risks, and prevention costs. In *2018 IEEE International Conference on Electro/Information Technology (EIT)*, pages 0096–0101, 2018.

[19] X. R. Luo, W. Zhang, S. Burd, and A. Seazzu. Investigating phishing victimization with the heuristic–systematic model: A theoretical framework and an exploration. *Computers & Security*, 38:28–38, 2013. Cybercrime in the Digital Economy.

[20] T. Peltier. Security awareness program.

[21] Proofpoint. 2020 state of the phish. Online: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf.

[22] S. Sheng, M. Lanyon, P. Kumaraguru, L. Cranor, and J. Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. *Conference on Human Factors in Computing Systems - Proceedings*, 1:373–382, 01 2010.

[23] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton. Analysis of end user security behaviors. *Computers & Security*, 24(2):124–133, 2005.

[24] Symantec. Internet security threat report volume 24 - february 2019. Online: https://docs.broadcom.com/doc/istr-24-2019-en.

[25] T. C. C. Tan, A. B. Ruighaver, and A. Ahmad. Information security governance: When compliance becomes more important than security. In K. Rannenberg, V. Varadharajan, and C. Weber, editors, *Security and Privacy – Silver Linings in the Cloud*, pages 55–67, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[26] C. Thomas R. Peltier CISSP. Implementing an information security awareness program. *EDPACS*, 33(1):1–18, 2005.

[27] D. W. Woods, T. Moore, and A. C. Simpson. The county fair cyber loss distribution: Drawing inferences from insurance prices. *Digital Threats: Research and Practice*, 2(2), Apr. 2021.