Industry Specific Education for Human Error Related Data Breach Prevention

Jordan Cherry (24572974), Sebastian Kinley (24554596), Zachary Zerafa (24557656)

University of Technology Sydney, Australia, 2024

5440 words

Contents

Executive summary

The research proposal aims to discern the efficacy of educating employees on cybersecurity in an industry-centric manner rather than a uniform, generic approach; the hypothesis is that industry-centric has superior results. Candidates with little cybersecurity experience are selected, and split into a test and control group where the former will receive a cybersecurity training video that is industry-centric, and the latter receives a uniform training video. They are then tested with scenarios that could potentially arise in their industry, and quantitative research methods will determine the validity of the hypothesis.

1. Introduction

Since the start of the 21st century, the infrastructure of society has been reliant upon computer networking to exchange information in an incredibly efficient and reliable manner. Such dependence on networking inadvertently leads to the existence of data breaches by threat actors; malicious entities that intentionally contribute to harming some targeted computing system.

Despite the benefits available from computer networking, it is also necessary for organisations to furnish measures to deter threat actors to truly benefit from such technology. Solutions for data breach prevention include anomaly detection systems, employee education, appropriate permissions settings, strong encryption and password settings, and a conservative network structure.

Due to the differing nature of data harboured by each industry, there is discrepancy within the frequency and intensity of data breach attempts in addition to certain attack vectors.

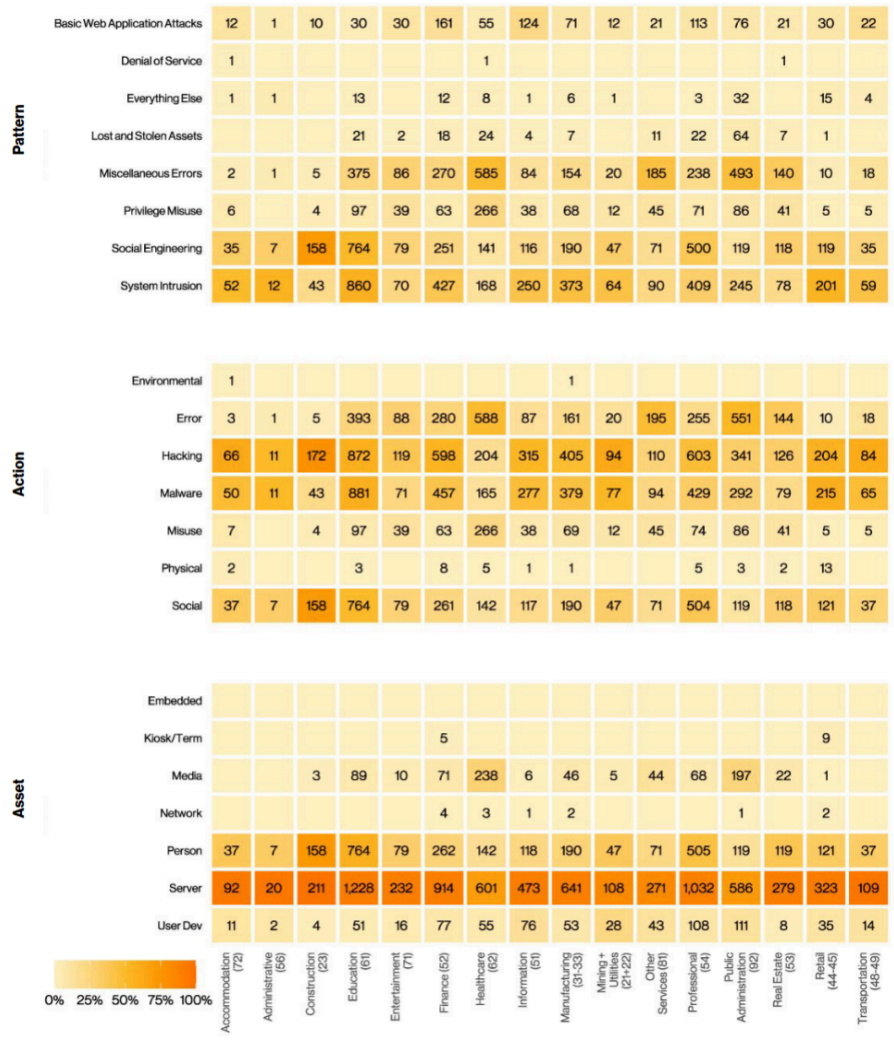

Figure 1: Attack Vector Frequency by Industry

Human error comprises 74% of all cybersecurity attacks and is a common threat to all industries, albeit through differing means.

This brings into question a serious problem for which research may provide an answer; how can human error based attack vectors be mitigated for various industries by optimising cybersecurity education for the relevant nature of threats an industry faces? This is the research problem that inspired the following research project.

210 individuals each belonging to some industry will be partitioned into a control or test group, where they are shown either a generic cybersecurity training video or a cybersecurity video tailored to their industry respectively. After 2 weeks, the participants will be prompted with phishing schemes and other error-inciting prompts that they will likely encounter in their industry within the subsequent weeks and the timeliness and 'correctness' of the responses will be examined and compared across the different industries and the test group.

As with all research projects, it is required that the research method is refined such that the end results and conclusions are of sound basis. This is achieved by iteratively and inquisitively reflecting on each proposition for the research method; Which factors can induce bias towards the test? What is the nature of the data that will be collected? How can the data be interpreted to make meaningful conclusions about the hypothesis? The resolutions allowing the research project to avoid such hindrances and reach superior standards are discussed thoroughly throughout the article.

Ultimately, the main finding for the research method was a quantitative approach; a scoring model whose efficacy is determined by statistical inference testing (primarily the Student t-test and Fisher's F-test)

The primary aim of the research experiment is to define and apply a metric to evaluate the efficacy and cost of industry based cybersecurity training in contrast to generic cybersecurity training, within the scope of mitigating human error related attack vectors.

By achieving this, the pursuit of this line of research is validated in its utility for organisations seeking cost effective measures for protecting their data without compromise on quality.

This report will discuss the aims and objectives of the research project in greater detail, explore the context of literature that has inspired the research project, and dissect the research method and justification for its soundness.

2. Research Aims & Objectives

Despite the vast variety of techniques available to counter data breaches, the research experiment considerations are restricted to human error based attack vectors, a prominent example of which is phishing. Additionally, there are several means through which these attacks can be prevented; this research experiment confines itself to educational means rather than automated anomaly detection systems.

The primary aim of the research experiment is to define and apply a metric to evaluate the efficacy and cost of industry based cybersecurity training in contrast to generic cybersecurity training, within the scope of mitigating human error related attack vectors. This aim's objective is to validate the pursuit of related research in the future.

Derived from this prime aim, the following supporting objectives are deduced:

1. Define a metric in such a way that restricts bias from factors that cannot feasibly be controlled (a salient example encountered in this experiment is the effect of persons with a background in cybersecurity).
2. Understanding quantitative and qualitative relationships between industries or the control group regarding the ability to evade human error.
    - In order to enable accurate measuring and comparison of training outcomes from different industries to gain provide insight into which / how different industries gain value from cybersecurity training.
3. Infer optimised ratios of information adequately tailored to the cybersecurity training for diverse industries.
    - For example, inferring the ideal ratio between phishing, access control, or malware awareness content per industry, to optimise the value of the training agenda whereby excess content that may dilute understanding or confuse trainees can be disregarded.
4. Inform future cyber-security training research and development by presenting experiment-based consultation for industry-specific cyber-security training systems.

3. Background

The current background from which this research project is inspired is a collection of business reports and academic articles that emphasise the role of human error in creating attack vectors, the efficacy of cybersecurity education, and the distinction of cybersecurity requirements between industries. The corpus of literature on these three factors is abundant, however a research experiment constructed to highlight the relations between such factors is seldom present, and this knowledge gap has potential to be fulfilled by the proposed research project.

Multiple articles allude to how each industry has its own set of motivations, methodologies and consequences relating to data breaches, and qualitative surveying is the standard method through which these studies differentiate the effects of data breaches with respect to industry.

Verizon (2024) is perhaps the superior report that has served as a prime motivator for many of the ideas expressed in this research proposal. It provides recent quantitative data and presents little bias.

We now discuss such articles in relation to the recurring ideas within the research project.

3.1 Motivations

The motivations of specific threat actors are numerous, with financial and espionage being the two leading motivations. (Verizon, 2024). The idea of industry specific motivations can be seen through this report, as an industry such as Financial and Insurance had 95% financial and 5% espionage as their actor motivations, whilst Public Administration had 71% financial and 29% espionage.

3.2 Threat Actors

Additionally in the Verizon (2024) report, threat actors can be seen to vary across industries as well. Threat actors are categorised in the report as external or internal, based on whether the threat actor originated from outside or inside the organisation and its network of partners respectively. Threat actors can be seen to vary through industry, with threat actors for Educational Services being 68%, whilst external threat actors for an industry such as retail were 96%. Additionally, threat actors heavily vary based on incident classification, which will be discussed below.

3.3 Data breach Attacks Between Industries

Verizon (2024) discusses three lenses relating to how an industry is attacked; the pattern of the attack used to conduct the data breach, the category of action the attack belongs to, and

the asset which was the point of failure for an attack to succeed. For instance, Basic Web Application Attacks (including XSS and SQL injection) and Denial of Service attacks are patterns under the hacking category that abuse caveats of the server's structure.

These classifications have their own threat motivation, threat actor, data compromised, and industry statistic, showing various changes between different incident types.

For example, Lost and Stolen Assets had 88% internal and 12% external, with a majority of the data being compromised being Personal data. Whilst Denial of Service naturally had 100% external threat actors. Kurtis & Aryes (2008) also discuss this idea, discussing how educational systems may be more susceptible to inside threats.

	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	30,458	919	1,298	28,241	10,626	617	986	9,023
Accommodation (72)	220	16	9	195	106	16	9	81
Administrative (56)	28	7	7	14	21	6	4	11
Agriculture (11)	79	5	0	74	56	4	0	52
Construction (23)	249	17	6	226	220	12	5	203
Education (61)	1,780	82	630	1,068	1,537	56	618	863
Entertainment (71)	447	16	2	429	306	10	1	295
Finance (52)	3,348	75	122	3,151	1,115	54	87	974
Healthcare (62)	1,378	54	21	1,303	1,220	41	18	1,161
Information (51)	1,367	79	62	1,226	602	49	19	534
Management (55)	22	4	1	17	19	4	1	14
Manufacturing (31–33)	2,305	102	81	2,122	849	62	49	738
Mining (21)	30	1	2	27	20	1	1	18
Other Services (81)	462	13	5	444	417	8	5	404
Professional (54)	2,599	205	102	2,292	1,314	124	73	1,117
Public Administration (92)	12,217	56	115	12,046	1,085	39	27	1,019
Real Estate (53)	432	35	5	392	399	29	2	368
Retail (44–45)	725	90	47	588	369	55	32	282
Transportation (48–49)	260	21	38	201	138	17	12	109
Utilities (22)	191	17	11	163	130	12	6	112
Wholesale Trade (42)	76	22	21	33	54	17	14	23
Unknown	2,243	2	11	2,230	649	1	3	645
Total	30,458	919	1,298	28,241	10,626	617	986	9,023

Table 2. Number of security incidents and breaches by victim industry and organization size

Figure 2: Total data breaches by industry

Similarly, Curtin & Ayres (2009) provides deep analysis in how the nature and frequency of attacks vary across industries, claiming that hijacking host machines is a common problem within the educational industry, however a more prevalent issue in the healthcare industry is hardware theft.

3.4 The Effects of Data Breaches

The effects of data breaches are monumental and multifaceted, involving financial, reputational and legal repercussions for the business. Zhang et al. (2022) estimated that the costs of a data breach could range from approximately $4.23 million for cybercriminals and up to $4.5 million for nation-state actors. Additionally, Chen et al. (2023) found that 87% of

customers would abandon a specific business if it was revealed they were incorrectly managing their data, displaying high reputational damage. Finally, legal ramifications can be seen through Ishii & Komukai (2016), who discuss the differing legal frameworks across the USA, UK and Japan, highlighting how this can affect the consequences of a breach. Particularly, the USA was seen to contain a lack of traceability, and Japan and the UK were seen to not have proper enforcement of their policies.

3.5 Mitigation Techniques

Ultimately, effective mitigation techniques are directly related to all of the aspects above, as mitigation aims to combat data breaches. Zhang et al. (2022) proposed several strategies to combat data breaches, such as robust access control measures, proper data classification, and the proper training of employees. However, the author does not address industry related statistics when addressing these mitigation techniques. This research gap could be fulfilled by mapping mitigation techniques for industries towards the problems and causes that are most frequent to them. The National Institution of Standards and Technology (NIST) Cybersecurity Framework provides an insight into techniques to manage and reduce cybersecurity risks. This outline will be used as a framework for techniques to follow (National Institute of Standards and Technology, 2024). Additionally, Malasowe et al. (2024) addresses specific mitigation techniques for specific attacks. Such an example is regular security training and awareness programs, which are cited as effective strategies against phishing attacks and social engineering assaults, which will be the topic of this research's first testing method.

4. Research Significance & Application

The chosen research project seeks to demonstrate a relationship between human error, industry and cybersecurity education that can bear fruitful results to organisations who aim to ensure their employees are less likely to be a point of failure in their cybersecurity system.

4.1 Significance

The success of demonstrating such a relationship between industry and cybersecurity education has potential to revolutionise the conventional approach of organisations towards the protection of their data. By providing education to employees regarding cybersecurity information most related to their context, memory retention is optimised by only specifying cybersecurity issues that are relevant to the industry the employee operates within and therefore augments to the . Human error as previously mentioned constitutes a primary cause of data breaches and can potentially result in millions worth of damages (relative to the organisation's magnitude).

As mentioned in the background, Ncubukezi's (2022) qualitative data suggests a lack of confidence in human related cybersecurity practices and their particular rising salience out of the context of COVID 19 from which it was written, with overwhelming agreement of ignorance to cybersecurity and high frequency of human error attack vectors in the general workplace. This research project would become a successor that explicitly addresses these concerns raised by developing an educational system that most effectively trains employees for their related context.

4.2 Benefit

The benefit offered by this research project is value optimization for cybersecurity training; it ensures confidence to stakeholders that an investment in cybersecurity training that the knowledge imparted towards employees has maximum practicality towards defending from attacks that are major threats to the specific industry of the organisation.

By taking in consideration factors that have high influence on cybersecurity relevance such as industry, a remodelling of cybersecurity education to reflect this phenomenon can increase the value of a training session without augmenting to cost; intelligent allocation of knowledge resources addresses the needs of an organisation more effectively.

4.3 Innovation

Identifies innovation of proposal and justifies claims with reference to background.

Previous literature has dealt with the relationship between the nature of cyber attacks and industry as well as the prevalence of human error in allowing the occurrence of data breaches. Verizon (2024) provides quantitative results that map frequencies of certain attacks to certain industries, however fails to mention a constructive solution towards mitigating these attacks within the specific contexts. Zhang et al. (2022) hypothesise methods of data breach prevention, of which education was a major topic. Despite the constructive concepts, the report fails to recognise possibly subtle factors that could have major implications on how to put such measures into practice.

This research project essentially combines these detached observations from the background reports to form a constructive research project that is a prototype to a robust cybersecurity education course, with heavy consideration of the industrial context of an employee. It draws inspiration from previously published articles which demonstrate the existence of such phenomena and accounts for them in a project that aims to become an actual tool in data breach prevention; In contrast to actions taken in the background, this is a direct approach in changing the ignorance of cybersecurity rather than documenting it.

5. Research Methods

The researchers hypothesise that mitigation techniques which are catered specifically towards industry's data breach statistics, will perform better than mitigation techniques generic mitigation techniques that do not account for industries data breach statistics.

However, due to the nature of the scope of this hypothesis, this project will begin with an initial pilot test. This pilot test will focus entirely on the mitigation techniques regarding human error. This is due to the ease in which this outcome can be achieved compared to all other potential mitigation techniques in the data breach field.

The researchers hypothesise that individuals who participate in industry specific data breach training will perform better than individuals who participate in generic data breach training, for all industries.

5.1 Outline

This research proposes a new learning method for handling human error in data breaches. This specific research proposal will create a learning method that incorporates data breach statistics from specific industries, such as data breach methods, types of data, threat actors, and threat actor motivations and how all of these can change based on the various industries.

To obtain practical results from the experiment, it is essential that the research process is meticulously examined to eradicate potential factors inducing bias, the nature of data is well defined and relevant such that logical conclusions relating to the research problem can be drawn from them.

To successfully carry out this endeavour, this research project's research method includes a metric to evaluate the difference between the current overall, generic training approach, and this proposed industry-specific training approach.

The method below outlines the research problem, the research design, the participants, the equipment, the procedure, the evaluation metrics, and the ethical considerations. This framework seeks to create repeatability through a structured outline, and reliability through isolating the independent variable of the training program, to evaluate the efficacy of industry-specific cybersecurity training.

5.2 Research Design

This study follows a quasi-experimental field experiment design as participants are divided into fixed industry groups. The study has a quantitative data approach.

This study also further utilises the quasi-experimental approach through its use of an intervention between two tests. The pre-training test is a baseline measurement, whilst the post-test is used as an impact assessment, measuring the differences between the two.

Whilst ideally a field experiment involves real scenarios, the inability to perform a real data breach or measure during a data breach necessitates this study to be simulated, which is still classified as a field experiment. This study design is fixed. As the primary aim of the study is to isolate the variable of training type, every other factor needs to be fixed to maintain consistency. This allows for reliable comparisons between pre-intervention and post-intervention tests.

This study will incorporate a quantitative data approach, as answers to tests will overall be answers that can be labelled as correct or incorrect, or timed values.

This study will use surveys with performance measurements of speed and accuracy to assess the differences between groups. These types of data, and procedures to measure the differences between groups will be outlined below.

5.3 Data

As this research project follows a quantitative research method, all data is numerical and the analytical techniques used are built on statistical inference.

The industries to collect data from are chosen due to their status as having the highest frequencies of threatening data breaches. These industries are Education, Finance, Healthcare, Information, Manufacturing, Professional and Public Administration.

Pre-screening Test

The pre screening survey is a 10 question online survey that is performed when someone is signing up for the study. An example question would ask something such as: What is your current level of knowledge regarding phishing attacks? These 10 questions each have five answers, these being:

- No knowledge
- Hardly any knowledge
- Some knowledge
- Good knowledge
- Expert knowledge

Additional demographic questions will be asked, including the participant's name, industry, and level of education.

These 10 questions will go into an overall score of 40, with each answer being scored from zero to four, assigning the score of zero to the response ‘no knowledge’ and the score four to ‘expert knowledge’, with intermediate scores mapped appropriately. This test will eliminate high responses, and aim to establish a natural bell curve of participants to eliminate future outliers.

Pre-Training Test

The pre training test is a 20 question, generic in person survey that is performed right before the training program. This will take a similar approach with style of questions to the post-training test, with examples being seen further below. This pre-training test aims to be a benchmark comparison between all participants, rather than a measurable pre-training test result comparison on the same scale. However, this result will be measurable as a comparison with the same participants' post-training test result specifically in the context of their results relative to other participants. This allows for all participants in the same industry to take the exact same test, without having any potential bias. A proposed bias that could come about from the pre-training test being industry specific, is that during the control groups training program, if a control participant had just performed a test containing industry specific questions only, there may be a bias towards their focus on the generic test. Thus, it was concluded that the pre-training test would be generic.

Training Videos

The industry-specific training video will be 30 minutes, prioritising information more closely related to the participants' industry. The ratio between the different types of data breach prevention education will be adjusted based on the data provided in Verizon (2024) which highlights the frequency of different attack patterns for various industries (see figure 1 in introduction).

The generic video will also be 30 minutes, encompassing a broad range of data breach topics. This video will still cover all information needed for the test, however with time spent on other information for non-relevant attacks.

These videos aim to outline common data breach attack types, and mitigation techniques often associated with these. These techniques are drawn from various sources, particularly The NIST Cybersecurity Framework 2.0, which will have examples in the example questions seen further below.

Post-Training Test

The post training test is a 20 question, specialised in person survey that is performed right after the training program. This test will contain questions specific towards an individual's industry, both for control and test subjects. This test allows for the results of the training program differences to be measured. The post-training tests will follow a similar structure to the industry specific training videos, simulating industry specific data breaches through asking questions directly related to each industry's highest frequency data breach types.

Pre and Post Training Question Examples

Some examples of questions that would be included in the post training test would be:

Question for Finance Industry:

Scenario: You receive an email that appears to be from the IT department, requesting you log in to verify account details. The email includes a link, warning of unauthorised access. What do you do?

Requires provided answer to include: the email to be forwarded to a manager and the IT team, as well as not clicking the link.

This is drawn from the NIST strategy “Information on adverse events is provided to authorised staff and tools”, as keeping managers and IT professionals in the loop is essential to detecting data breach attempts. (National Institution of Standards and Technology, 2024).

Question for Healthcare Industry

Scenario: You are updating patient records in a hospital at the end of your shift, accidentally sending information to the wrong department via email. What should you do to prevent this mistake in the future?

Requires provided answer to include: double-checking email address before sending

This is drawn from the NIST strategy “Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced”, as patient information is a responsibility a healthcare worker holds, and thus understanding of the implications of a mistake is essential. (National Institution of Standards and Technology, 2024).

Question for Education Industry

Scenario: You store student grades and sensitive information on a personal computer that is not password protected. What is the most secure action to prevent breaches of personal information?

Requires provided answer to include: Storing data on a secure, university-managed system

This is drawn from the NIST strategy “The confidentiality, integrity, and availability of data-at-rest are protected”, as actions taken to actively protect sensitive information must be performed (National Institution of Standards and Technology, 2024).

These questions above are aimed at addressing common attack types of specific industries. These questions would be the exact same style for the pre-training tests, giving questions for all different industries to everyone. These questions would not reappear in the post-training test, but they would be the same in difficulty.

Question time length

An additional variable measured will be length of time to complete each question. This will not be disclosed to the participant as knowledge of them being timed could potentially influence a participant's actions to not be correctly indicative of their natural response.

5.4 Participants

This study will take 210 participants for the test. The participants will be equally divided from the seven different industries outlined above. Thus each industry will have 30 representatives.

Each industry will have their participants split into two groups randomly, these being the test group and the control group. Additionally, a prescreen test that is outlined below will look to find participants from the industry without excessive data breach knowledge. This seeks to reduce the likelihood of outliers as this research aims to measure the learning effects of a new system. Excessive knowledge of the case prior to research could impede on the researcher's ability to accurately measure changes between both the control and test group, as well as between pre and post test measurements.

Additionally, the aim of this study is to increase data breach mitigation techniques, and thus should be catered towards and performed on low level employees who are responsible for information who may not possess data breach knowledge.

5.5 Resources

The resource project will require several pieces of equipment, primarily for hosting the learning videos and the surveys.

Video Creation Software: Tools to create the two types of cybersecurity training videos. These two types of videos are the generic video, and the tailored videos. There will be one generic video, and seven tailored videos.

Room: A spacious room that can seat 15 people, allowing them to not see each other's screens.

Online Survey Platform: A survey tool utilised will be Google Forms. There will be eight different surveys in total, these being the pre screening test, and seven tailored surveys based on the seven industries.

Data Analysis Software: Python, with appropriate libraries such as SciPy and StatsModel will be necessary for analysis of the scoring data and performing hypothesis testing and statistical inference.

Computer: Each individual will have a personal computer that has access to the online survey platform.

Projector: A projector to display the training videos in the room.

5.6 Scheduling

The research project will span a 6 month period and consist of the following 6 phases.

1. **Recruitment & Prescreening**
    a. Recruit 210 participants from seven high-risk industries
    b. Conduct pre screening before recruitment, ensuring limited knowledge of cyber security
2. **Assigning & Conducting training**
    a. Randomly assign each industry to have 15 control and 15 test subjects
    b. Before the training pre-test to establish a baseline of cybersecurity knowledge for each participant through a generic pre-test
    c. Control Group Training: Provide participants with the generic cybersecurity training video
    d. Test Group Training: Provide participants with the industry specific cybersecurity training video
3. **Testing**
    a. After the training, conduct a post-test with questions and simulated scenarios, catered specifically towards scenarios of the participants industry
4. **Scoring**
    a. Record results of the test and time logs of how long each response took.

b. Use the scoring metric to evaluate each participant's 'score' and use this sample to determine the distribution of each combination of test/control group and industry.

5. **Data Analysis**
    a. Assume variance and mean of sample as that of the population.
    b. Test for normality of distributions.
    c. Employ t-tests and F-tests to determine inequality test and control groups.
    d. Discern which groups have a superior score.
6. **Reporting**
    a. Consolidate and interpret findings to determine the effects of industry specific training on data breach detection

It is expected that the recruitment phase is the most difficult phase to control chronologically; Locating individuals willing to participate has the most uncertain outcome and may require additional incentive to be fulfilled. To account for this, two Gantt charts have been developed projecting how a project may proceed depending on how long it takes to complete this initial stage.

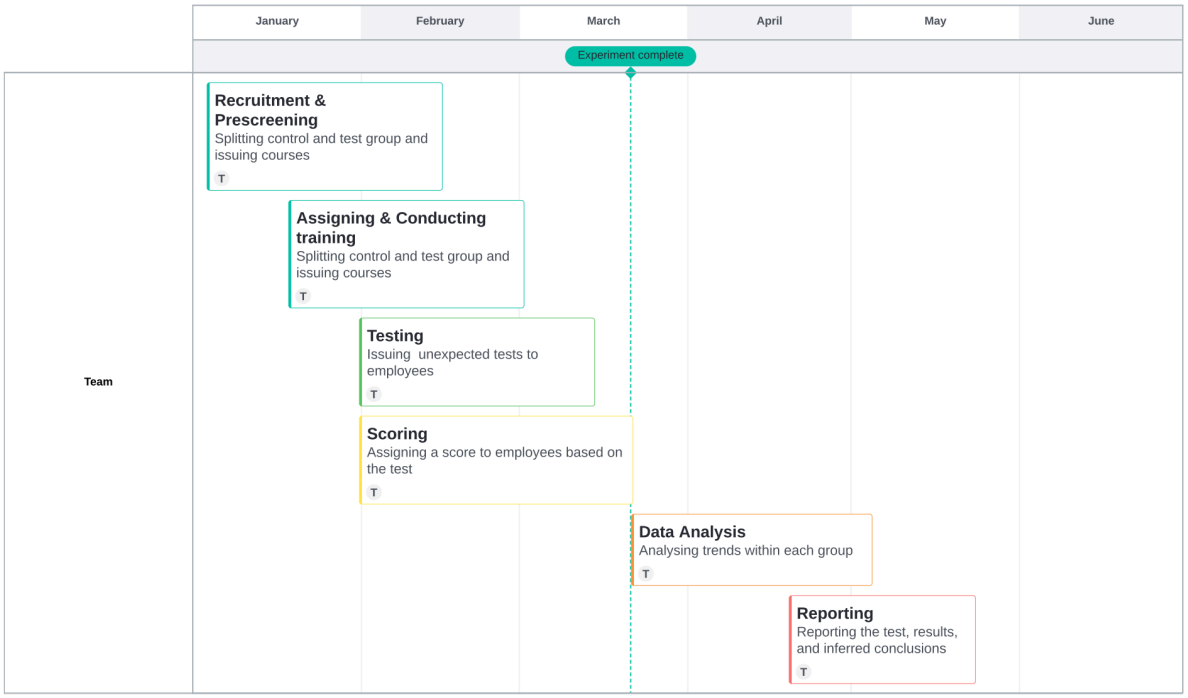

Figure 3: Primary Gantt chart

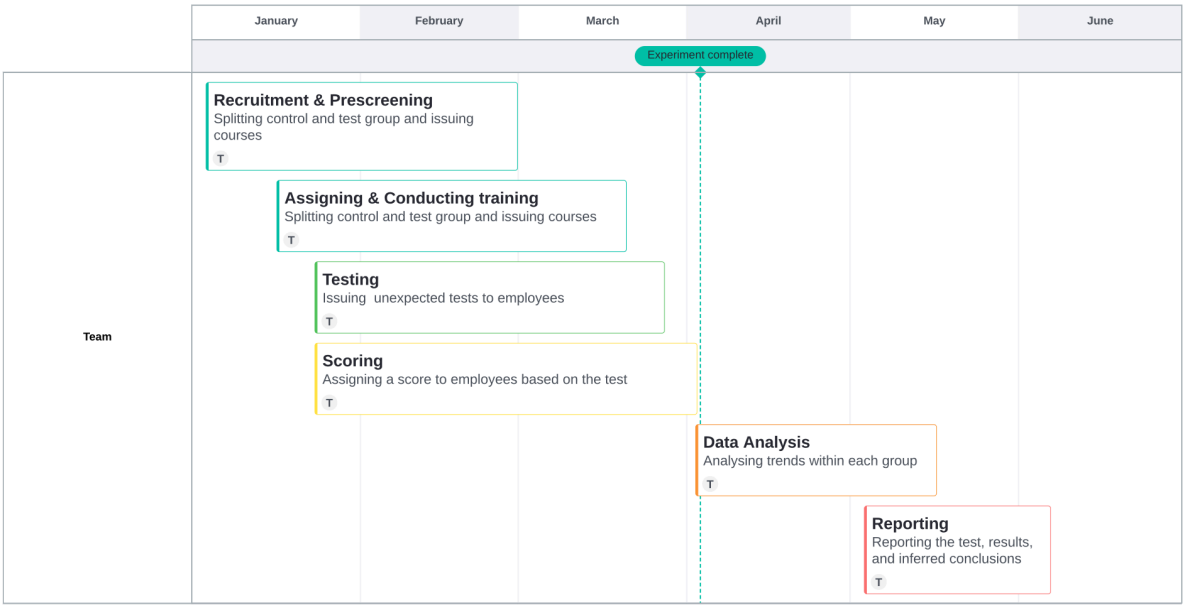

Figure 4: Secondary Gantt chart with extended 'Recruitment & Pre-screening' stage

It is noteworthy that there exists a buffer roughly equivalent to a month in both situations to ensure the timeliness of the project; this accounts for any additional elements of uncertainty that may accumulate throughout other phases of the research project.

Though most phases can initiate concurrently with another (within certain constraints), the data analysis phase cannot initiate in tandem with the scoring phase due to an incomplete set of processed data; analysing data can only be done with any meaning once a sufficient sample is amassed.

5.7 Ethical Considerations

All participants will be informed about their right to confidentiality, and their ability to withdraw from the study at any point if they desire. Data will be anonymized, and informed consent will be obtained prior to any research being performed, to ensure ethical research standards are met. Even though the entirety of the nature of the study will not be disclosed, as indicating to participants that their teaching is part of the control or test group could potentially impede on results, informed consent will still be met as the participants data is still being used in the informed way, just compared to a different group.

5.8 Quantitative analysis

A scoring system will be developed to quantify 'confidence in awareness', which is defined in this research project as the employee's ability to correctly avoid human error attack vectors. It is constructed in such a way that for each of the n tests with weights w_i, if an employee exhibits a **positive response**, for instance flagging a phishing email or denying requests to transmit sensitive information over an unencrypted network will add this weight to the employee's score. **Negative responses** such as clicking on a phishing link or transmitting sensitive information over insecure channels will subtract the weight from the employee's score.

A score of 0 represents 'perfect uncertainty', that is, if in future a human error attack vector, a stakeholder cannot have any prediction of whether the employee will have a positive response nor a negative response. Negative scores represent confidence that an employee will make a negative response in future and positive scores represent confidence that an employee will make a positive response in future.

$$S_{\mathrm{T}}^{\mathrm{Timed}} = \sum_{i=1}^{n} S_i$$

$$S_{\mathrm{T}}^{\mathrm{Untimed}} = \sum_{i=1}^{n} S_i$$

$$S_i^{\mathrm{Timed}} = \frac{(-1)^{1-r} 1800}{T_i} w_i$$

$$S_i^{\mathrm{Timed}} = (-1)^{1-r} w_i$$

$$r = \begin{cases} 1 & \text{positive response} \\ 0 & \text{negative response} \end{cases}$$

Figure 5: Scoring formulae

The sample data of these 'scores' will be processed into conditional probability distributions; mathematical functions that model 'probability density' with some conditional assumption, in this case, whether a participant has received a generic or industry-tailored video. Let V be a random variable of Bernoulli distribution, that is, it equals 1 when the participant has seen an industry-tailored cybersecurity video and 0 if they have seen a generic cybersecurity video. Let there be equal probability of selecting either class of participant. Let X_i be a random variable of the score of some participant from industry 'i'. These X_i can be reasonably modelled as normally distributed random variables due to previously tested empirical

observations (Shalaan & Juma 2021) however it will be required to be verified using either a Shapiro-Wilk test or Pearson Chi squared test.

$$X_i|V \sim \mathrm{N}(\mu, \sigma^2)$$

$$V \sim \mathrm{Bern}(0.5)$$

Figure 6: Distributions of the proposed random variables

From here, there exists a range of test and estimator statistics that can be used such as the Method of Moments, Maximum Likelihood Estimator and the Student's t-test. Since a normal distribution is being modelled with two population unknowns, a Student's t-test is most adequate as it allows the sample variance to be used as inference for the population mean. Furthermore, by using the sample definition of the variance (where the degree of freedom replaces the sample size) the test statistic obtained by Student's t-test is known as an unbiased estimator, meaning that the average of this statistic for all samples equals the true population parameters exactly.

If the Student's t-test cannot reject the null hypothesis, then as a last resort Maximum Likelihood Estimation can be used to determine an estimator for the population mean assuming the sample variance.

Now that the sample data has been attributed to a model, the mean and variance of the control and test groups can be analysed and trends can be identified.

5.9 Determining success

After the scoring process and the aforementioned data analysis is conducted, the mean and variance of each combination of industry and test/control group will become the primary statistics used to identify trends. The hypothesis that industry based training has more practical effect than generic training can be supported by evidence demonstrating that the test groups have a higher mean score and less variance than the control group.

This can be done by a further application of a Student t-test, showing that with an alpha level of 0.95 the average of the test group scores is unequal to that of the control. This shows that the true population mean of employees receiving industry specific training is unequal and superior to employees receiving merely generic cybersecurity training.

Inequality of variance is similarly tested using Fisher's F-test which compares the ratio of the average of the variances of the test groups and control groups distinctively and again uses an alpha level of 0.95 to discern their inequality.

Hence verifying that the mean score is larger and variance smaller for test groups by the use of inferential statistics is the crux of determining whether the presumed hypothesis in fact reflects reality.

6. Conclusion

This research proposal outlines a novel approach to addressing human error in data breaches through the development of an industry-specific training program. By applying a quantitative research method approach to evaluate the efficacy of industry centric training methods, this study strives to enhance cybersecurity awareness and mitigate the threat of data breaches to the most vulnerable 7 industries.

The quasi-experimental design provides a robust framework for measuring the effectiveness of the proposed intervention. By focusing on industry-specific scenarios, the training program seeks to heighten the effectiveness of data breach mitigation.

Through data collection and analysis, this study aims to measure the impact of a catered cybersecurity training program on employee recall, specifically regarding their ability to recognize and respond to potential data breaches in written scenarios, recording actions that would be taken. Evaluated results may provide insight into how industry-specific training methods may contrast to generic approaches.

Ultimately, this research project is a pioneer in applying data relating to data breaches to cybersecurity training initiatives and supplies the foundation for further research into optimisation of employee training for data breach prevention, inspiring new effective techniques.

7. Reference

2024 Data Breach Investigations Report. (2024, May 7). Verizon Enterprise Solutions. https://www.verizon.com/business/resources/T6fb/reports/2024-dbir-data-breach-investigations-report.pdf

Chen, J., Henry, E., & Jiang, X. (2022). Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. Journal of Business Ethics, 187. https://doi.org/10.1007/s10551-022-05107-z

Curtin, C., & Ayres, L. (2009). Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry. http://web.interhack.com/publications/interhack-breach-taxonomy.pdf

Ishii, K., & Komukai, T. (2016). A Comparative Legal Study on Data Breaches in Japan, the U.S., and the U.K. IFIP Advances in Information and Communication Technology, 474, 86–105. https://doi.org/10.1007/978-3-319-44805-3_8

Juma, M., & Shaalan, K. (2021). Online Social Network Analysis for Cybersecurity Awareness. https://doi.org/10.1007/978-3-030-47411-9_32

Malasowe, B. O., Aghware, F. O., Okpor, M. D., Bassey, E., Erhovwo Ako, R. E., & Ojugo, A. A. (2024). Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech). Nipes.org. https://journals.nipes.org/index.php/njstr/article/download/981/865

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. The NIST Cybersecurity Framework (CSF) 2.0, 2.0(29). https://doi.org/10.6028/nist.cswp.29

Ncubukezit, T. (2022). Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses. International Conference on Cyber Warfare and Security, 17(1), 395–403. https://doi.org/10.34190/iccws.17.1.51

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D. P., & Ghorbani, A. A. (2022). Data breach: analysis, countermeasures and challenges. International Journal of Information and Computer Security, 19(3/4), 402. https://doi.org/10.1504/ijics.2022.127169