1-2023

Predictive taxonomy analytics (LASSO): Predicting outcome types of cyber breach

Jing Rong GOH
Singapore Management University, jrgoh@smu.edu.sg

Shaun S. WANG

Yaniv HAREL

Gabriel TOH

Citation

GOH, Jing Rong; WANG, Shaun S.; HAREL, Yaniv; and TOH, Gabriel. Predictive taxonomy analytics (LASSO): Predicting outcome types of cyber breach. (2023). *Journal of Cybersecurity*. 9, (1), 1-15.
Available at: https://ink.library.smu.edu.sg/soe_research/2688

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2023, 1–15
https://doi.org/10.1093/cybsec/tyad015
Research paper

Research paper

Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach

Jing Rong Goh [1,2,3,*], Shaun S. Wang [2,4], Yaniv Harel [5] and Gabriel Toh [6]

[1]School of Economics, Singapore Management University, Singapore 188065, [2]Risk Lighthouse International, Singapore 051531, [3]Accredify, Singapore 339213, [4]Department of Finance, Southern University of Science and Technology, Shenzhen 518055, China, [5]Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University, Tel Aviv 6997801, Israel and [6]Cyber Risk Management [CyRiM] Project, Nanyang Business School, Nanyang Technological University, Singapore 639798

*Correspondence address. School of Economics, Singapore Management University, Singapore 188065; E-mail: jrgoh@smu.edu.sg

Received 15 December 2020; revised 15 October 2022; accepted 20 June 2023

Abstract

Cyber breaches are costly for the global economy and extensive efforts have gone into improving the cybersecurity infrastructure. There are numerous types of cyber breaches that vary greatly in terms of cause and impact, resulting in an extensive literature for individual cyber breach type. Our paper seeks to provide a general framework that can be easily applied to analyze different types of cyber breaches. Our framework is inspired by the taxonomy approach in the cybersecurity literature, where it was proposed that an effective set of taxonomy can provide a direction on supporting improved decision-making in cyber risk management and selecting relevant cybersecurity controls. Our paper extends upon the current approach by using this taxonomy to model and predict the associated breach outcomes, given the occurrence of a cyber breach. Specifically, our paper applies least absolute shrinkage and selection operator (LASSO) within a taxonomy framework. Using a proprietary database of known cyber breaches, we show that this analytical tool performs well in out-of-sample predictions and a stable model that generates consistent predictions. For each cyber breach outcome type, we also provide the list of keywords that are useful in predicting the outcome type. We envision researchers, insurers, underwriters, and cybersecurity professionals can use (or expand on) our list of keywords, or use our method to yield their own set of keywords. Practitioners who seek to mitigate their cyber risk may use these keywords as a guide towards the specific attack surfaces that might be most susceptible to the corresponding breach. Our paper lays the groundwork for researchers to better apply the taxonomy approach within cybersecurity research. We also perform regression analysis to identify industries that are most susceptible to various cyber breach events. Our results corroborate with the literature, where some industries are indeed more likely to be impacted by certain types of cyberattacks.

Introduction

The rising prevalence of cyber breaches have led to an increasing amount of targeted research surrounding cyber risks. There is a wide variety of cyberattacks, such as data breaches on some of the largest institutions around the world, ransomware,[1] business email compromise,[2] cyberthefts,[3] Distributed Denial of Service (DDoS) attacks,[4] among many others.[5] These different cybercrimes are costly for the economy: McAfee and the Center for Strategic and International Studies approximate that costs arising is at least $600 billion in 2017 [1], and exceeds $1 trillion in 2020 [2], which implies that nearly 1% of global GDP is lost to cybercrime annually; and the World Economic Forum predicts that $5.2 trillion in global value is at risk from cyberattacks from 2019 to 2023 [3].

Given the increasingly high cost of cybercrimes to the global economy, much attention has been devoted to better understand cyber breaches and associated costs. However, due to the wide variety of cybercrimes, it may be challenging to conduct meaningful analysis. Although there exists a wide variety of cybercrimes and that their root cause(s) may differ, our central hypothesis is that the root cause(s) for the same type of cyber breaches may overlap. This implies there are specific attack surfaces that are particularly at risk for specific cybercrimes, and also there are attack surfaces that are not as critical for specific type of cyberattacks. Considering this institutional background outlining cyber breaches and our hypothesis, our paper will identify whether such an overlap occurs, and if so, what these specific attack surfaces are for different types of cybercrimes.

The cybersecurity literature is rich in variety of cyber breach incidences. For data breaches, analysis has shown that neither size nor frequency of data breaches have increased, instead it is the severe and low-frequency events that have led to heightened attention in data breaches [4]. Other findings suggest that the firm's location and industry sector may be used to assess the data breach risk of a firm [5]. For ransomware, the literature has documented that from 2013 to mid-2017, the market for ransomware payments only has a small number of players responsible for majority of payments [6]. Studies have also shown that an organization's sector has an impact on severity of ransomware attacks, whereas size of an organization had no bearing [7]. For monetary losses, studies showed that for retail consumers, scams result in the largest impact on victims, relative to payment-related fraud [8]. For business interruption, the literature suggests that premium incentives can be granted by an insurer toward their clients to mitigate large business interruption costs arising from aggregation risks [9]. In our review, we also noted a common theme that suggests the industry sector does affect the cyber breach in areas such as data breaches [5] and ransomware [7]. In particular, a paper has also described that different industries have different level of technical vulnerability and number of bugs in their system. This is simply because there exists greater inherent complexity in certain industries [10]. Thus, this inspired us to conduct a short analysis involving industry sectors toward the end of our paper as well and we find similar results where industry sector does matter in affecting outcome types of cyber breaches.

In our non-exhaustive review above, we see that there is indeed a rich variety of cyber breach literature and analysis on their causes and how to mitigate these breaches. In particular, we see that numerous studies tend to focus on specific types of cyber breaches. This allows for a more focused and in-depth analysis on individual cyber breaches. However, we propose that there is currently a lack of a more general framework that can be uniformly applied across different types of cyber breaches. This problem is exacerbated by the different datasets used by different researchers in their statistical analysis, which leads to a lack of uniformity and consistency. Therefore, we are motivated to prepare a dataset where observations are recorded in a standardized manner. We do so by coming up and applying a unique taxonomy coding (e.g. unauthorized access, unauthorized publication, unauthorized transfer, etc). Specifically, in building up our database, we required all observations to have verifiable external references. At the same time, we compiled a non-exhaustive list of cyber incident trigger taxonomy via an iterative and manual process. We looked at each cyber breach event individually and identified the root cause(s) for the breach based on the assessment of our subject matter experts, and is supplemented by findings from reports available online. Each cyber trigger taxonomy is then aggregated to the cyber incident within each datapoint. The list of taxonomy is built on that of ref. [11], and new terminologies were also introduced to paint a complete picture of the cyber breach event. We then coded each of this taxonomy into the database for each observation. This taxonomy helps enlarge the relevant (uniform) data sample for statistical data analysis and allow us to use the taxonomy setting to accurately predict the outcome type of cyber breach event (given that a breach event occurs). Outcome types predicted in this paper include *3rdPartyTransfer*, *BreachedRecords*, *AssetsAffected*, *LocationAffected*, *PersonEmployeeAffected*, *InaccessibleModifiedSystems*, *OperationsDisrupted*, *Attributedby3rdPartyEcosystem*, *IncidentResponseCost*, *RecoveryCost*, and *CompromiseAssessment*.[6] Our strategy in coding each of the taxonomy into the database provides a novel direction for researchers on an improved application of taxonomy within cyber breach literature. Broadly speaking, one contribution of our paper is that it takes a novel application of an analytical method and apply it to the taxonomy setting within a predictive model. Specifically, this methodology involves utilizing the taxonomy as the list of predictive features. We then pass these predictive features through the learning model that is implemented by the least absolute shrinkage and selection operator (LASSO) [12] and is trained by the training sample. The LASSO method then automatically select the most important predictive features within the taxonomy that corresponds to the outcome type of cyber breach. Furthermore, we test this model against four different types of information criterion (i.e. AIC, BIC, AICc, EBIC). We also conducted all our tests with undersampling to account for the class imbalance bias. The predictions from the selected model are consistently accurate in both the within-sample and the out-of-sample predictions.

1 Ransomware is a type of malware that blackmails to either publish victim's data or perpetually block access until a ransom is paid. In more recent years, in light of the effects of COVID-19 and an increase in Work-from-Home arrangements around the world, there is also an increase in ransomware attacks and their associated impacts.

2 Business email compromise (i.e. wire transfer fraud) forms another significant portion of cyberattacks. This is a sophisticated scam that targets businesses that often work with foreign suppliers and/or businesses which regularly perform wire transfer payments. These scams commonly involve multiple fraudsters who seek to compromise legitimate business email accounts via social engineering or computer intrusion methods to conduct unauthorized funds transfers.

3 With the increasing prevalence of cryptocurrency, the industry has suffered from major cyber thefts in recent years as well.

4 DDoS is an attack where attackers deploy a large number of online bots that send an extremely large number of requests, packets, or messages to the targets, which deny service to legitimate users including employees or customers.

5 We provide a non-exhaustive list of specific examples with numeric information on loss amounts for these type of breaches in Table A1.

6 Refer to Table 1 for specific outcome type features definitions.

Another significant contribution is the list of cyber incident trigger keywords that we generated[7] and was used to accurately predict the outcome types cyber breach events. This is of practical importance for underwriters, as they may now use (or expand on) our list of *keywords* (or apply the methodology to yield their own set of *keywords*) to draft (1) more effective and targeted underwriting agreements, and (2) more concise pre-purchase survey forms. This is because this set of keywords can be useful in predicting the outcome types of a cyber breach event. In addition, the selected taxonomy can also help companies (or individuals) who seek to mitigate their risks of cyber breaches as it serves as a guide toward the attack surfaces that might be most susceptible to the corresponding breach. This is pertinent as corporations are looking into optimizing investments into cybersecurity and this emphasizes the value of the predictive methodology given in our paper [13]. However, there are also limitations to our paper and taxonomy approach, which we discuss. Finally, we also conduct a traditional analysis to uncover the susceptibility of different industries suffering from different outcome-types of cyber breach events.

The rest of our paper is organized as follows. In the "Literature review" section, we conduct a literature review on the multiple strands of related research. In the "Data description and methodology" section, we provide a description of the data and methodology. The "Key results and analysis" section describes the analysis and explains the key results. The "Discussion and conclusion" section provides a discussion and concludes.

Literature review

Our paper extends upon three strands of literature. First, we explore the cyber breach literature that has received significant attention in recent years. Reference [14] provides an economic model concerning security investment for a firm and this model has been widely discussed among researchers [15, 16]. In response to their paper, ref. [17] discussed potential difficulties in measuring the reduction in vulnerability arising from security investments, and instead suggested to map the level of security investments to changes made in the level of security. There is also a growing literature on empirical research specific to cybersecurity breaches [4, 18, 19]. There are also papers in the literature that seek to identify the impact of cyber breaches [20, 21, 22]. Another contribution of our paper to this stream of literature is that we provide a machine learning methodology in analyzing cyber breaches. This is aligned with the multidisciplinary approach that has been highlighted to be important in cyber research [23, 24].

Second, we also extend upon the taxonomy of cyber breach literature. There have been efforts made to define the impacts of cyberattacks [25, 26]. Reference [27] analyzed 180 cyber insurance policies from New York, Pennsylvania, and California and documented relatively more variation in contract exclusions. This suggests that the taxonomy might indeed serve as a useful tool for underwriters when it comes to drafting contracts, especially in the section of exclusions, which can guide them to focus on the attack surfaces that matter. More recently, ref. [11] proposed that the underlying reason that the potential impact of cyberattacks is uncertain is due to a lack of effective metrics, tools, and frameworks that assist in our understanding of the harm organizations face from cyberattacks. Their paper conducted an extensive literature search and identified various types of harm and created a taxonomy of cyber harms encountered by organizations. They then propose that an effective taxonomy should provide a direction on better understanding the harms for organizations and help support improved decision-making in risk management as well as selecting relevant security controls. This is one of the stream of literature that our paper contributes to. Specifically, our paper extends upon their approach by basing the predictive features upon an exhaustive list of taxonomy, and then use this taxonomy to model and predict the associated breach outcomes, given the occurrence of a cyber breach event.

Third, the model used in our paper is based on machine learning literature. Machine learning is a fast growing literature, with applications in diverse fields [28]. There has also been some work done in the cybersecurity literature that applies concepts of supervised machine learning such as regression trees [19]. Specifically, in our paper, due to the relatively smaller sample dataset that we have (a common problem shared among most other cyber breach events database), we apply the LASSO in the model [12] with the AIC.[8] Reference [29] took a novel perspective by expanding on earlier literature by using *exploits in the wild* as their outcome variable, rather than the commonly used *published exploits* in the literature within their model to maximize utility of their predictive models. This is similar in approach to ours as new terminologies were consistently introduced to the *taxonomy* in order to provide a more holistic perspective of the event. As another contribution of our paper, we apply machine learning literature to analyze the fast-changing and quickly expanding field of cyber breach literature. Specifically, a novel perspective introduced in our paper is that we do not focus solely on software vulnerabilities, but also include vulnerabilities in business processes (such as personnel vulnerabilities, social engineering) when it comes to predicting cyber breach outcome type. This is intuitive as business processes form a critical segment of cyber breach vulnerability. Furthermore, we do not only focus on whether a cyber breach occurs, but we take it a step further by providing information on what type of outcomes will occur, given that a cyber breach does take place. The relatively high dimensional feature vector also includes different perspectives of a cyberattack, which helps to provide a more well-rounded view of the cyber breach event.

Data description and methodology

Data description

The primary data source is compiled by the Insurance Risk and Finance Research Center (IRFRC) for the Cyber Risk Management (CyRiM) project. The team at IRFRC conducted an extensive data verification and the database is proprietary to CyRiM. CyRiM Project receives most of their proprietary data through their collaboration with various industry partners, such as global insurance companies, cyber risk consulting companies, as well as a Fortune500 telecommunications and media company, among many others. Furthermore, we supplement the database by retrieving additional cyber breach events that were reported in various news sources, media outlets, and internet websites (such as Hackmageddon) [11]. In the compilation of the database, we required all observations to have verifiable external references.

For each cyber breach event, we compiled a non-exhaustive list of cyber incident trigger taxonomy via an iterative and manual process. Our trigger taxonomy is one of the more comprehensive list in the literature and industry. When we were constructing our database and defining the appropriate cyber incident

7 These keywords and the associated definitions can be found in Table 1.

8 A detailed description of the LASSO methodology, and consideration of different information criterion (i.e. AIC, BIC, AICc, and EBIC) can be found in the online appendix.

triggers, we reviewed the common schema provided in the literature and publicly available databases. For example, in the Privacy Rights Clearinghouse database [30], they defined eight types of breach with "CARD", "HACK", "INSD", "PHYS", "PORT", "STAT", "DISC", and "UNKN"[9]; in the Identity Theft Resource Center annual results [31], they used a more comprehensive classification of 19 types of root cause of compromise, but apart from "Phishing/Smishing/BEC", "Ransomware", "Malware", "Other-not specified", and "NA", all other variables have fewer than 100 occurrences. We also reviewed Gemalto Breach Level Index Report [32], which reported six breach source classifications: "Malicious Outsider", "Accidental Loss", "Malicious Insider", "Hacktivist", "State Sponsored", and "Unknown". We also had the opportunity to review the recent OTCAD (Operational Technology Cyber Attack Database) [33], which used four attacker classifications: "targeted attack", "untargeted attack", "disgruntled employee", and "unknown". We benefitted greatly from this preliminary analysis, but we quickly found that these lists on the public domain was not broad enough for classifying our database that had a greater variety of cyber incident triggers. Thus, using the knowledge set that we have acquired, we proceeded to look at each cyber breach event individually and identified the root cause(s) for the breach based on the assessment of our subject matter experts, and is supplemented by findings from reports available online. Each cyber trigger taxonomy is then aggregated to the cyber incident within each datapoint. The list of taxonomy is built on that of ref. [11] as well as our prior analysis of other publicly available databases, and new terminologies were also introduced to paint a complete picture of the cyber breach event. We then coded each of this taxonomy into the database for each observation. Objectively, it is also important to note that this dataset is not exhaustive, and may be subjected to discovery bias as it is limited by what is shared with us by our partners.

The data runs from 2014 to 2019, with a total of 3189 observations of unique cyber breach events. The distribution of the observations across different years are presented in Table A2. We note a concentration of observations from 2016 to 2019, as that is also the period of the CyRiM project. Each observation records the target of the cyber breach, a brief description of the breach, the industry type (i.e. target class), the country, the type of attack (i.e. attack class), a list of cyber incident trigger taxonomy. Each observation also includes 11 *outcome events* such as *AssetsAffected* (if assets were affected and specific amount if available), *LocationAffected* (if physical or digital locations were affected and specific amount if available), *PersonEmployeeAffected* (if personnel/employees were affected and number if available), *InaccessibleModifiedSystems* (if there were inaccessible/unauthorized/modified records or systems and specific amount if available), *BreachedRecords* (if there were any breached records and specific amount if available), *3rdPartyTransfer* (if there were any monetary loss to unauthorized 3rd party and specific amount if available), *OperationsDisrupted* (if operations were disrupted), *Attributedby3rdPartyEcosystem* (if the breach could be attributed to the 3rd party ecosystem, i.e. vendor/client/partner/cloud/social media), *IncidentResponseCost* (if there were any incident response cost), *RecoveryCost* (if there were any recovery cost), and *CompromiseAssessment* (if there were any compromise assessment).

Based on these data, we seek to understand if the list of cyber incident trigger taxonomy can be used to predict the outcomes of the breach. We divide the cyber incident trigger taxonomy by first developing the full list of unique taxonomy used within each taxonomy type, and generate dummy variables for each of the unique terms identified. Using this method, we managed to yield a total of 39 dummy variables/features from the cyber incident trigger taxonomy. Table 1 provides the detailed definition of the 11 outcome events variables and the 39 cyber incident trigger variables, alongside the frequency of occurrence of each variable across our 3189 data points.

With our comprehensive list of taxonomy, we hope that this may serve as a foundation for other researchers when conducting similar research. For example, when other researchers conduct analysis of their databases, they may utilize our incident taxonomy (along with its detailed definition list) as a starting point to define the incident taxonomy of their databases. At the same time, as the field of cybersecurity research is fast changing, we do expect that our taxonomy is non-exhaustive and may be lengthened and improved upon by our colleagues in the future. Following the same line of reasoning, we argue that a continual improvement in the taxonomy is the best way forward in the field of cybersecurity research. This is because in cybersecurity research, there will always be cyber attackers who will come up with novel and creative cyber triggers. Thus, to ensure that the research remains current and pertinent, a continual improvement in the taxonomy is critical and relevant.

Methodology

The sample dataset consists of 3189 observations and a total of 39 features that can be included in the model. This gives rise to two striking concerns: (1) overfitting problem and (2) inability to determine, which features are the best features that can be used to predict the outcomes of the breach. Furthermore, this problem is exacerbated when we have a class imbalance problem (i.e. unequal distribution of outcomes) within certain breach-outcome types. We address the class imbalance problem by conducting all of the analyses with undersampling.[10]

Our solution in mitigating the two striking concerns is to reduce the regression objective function by dropping the ones that contribute little to the fit. To specify this mathematically is to implement the LASSO in the model [12]:

$$\min \frac{1}{n}\sum_{i=1}^{n}\left(y_i - x'_i\beta\right)^2 + \lambda \sum_{j=1}^{p}\left|\beta_j\right|,$$

where n is the number of observations; each observation has a single outcome, denoted by y_i, and p covariates, denoted by the covariate vector $x_i = (x_{i1}, x_{i2}, \ldots, x_{ip})$; β is the coefficient vector, denoted by $\beta_i = (\beta_1, \beta_2, \ldots, \beta_p)$, and λ is the tuning parameter (i.e. it captures the penalty associated with selecting more features). As it is well documented in the literature, the LASSO performs the model selection for us. This helps to mitigate the second problem above. Furthermore, as the model will drop variables that contribute little to the fit, the resulting model will have less features, which help to mitigate the overfitting problem (i.e. first problem above).

In the predictive model, we use the logistic link function, as the outcome features in the model are dummy variables that only take the value of 0 or 1. The reason we use only dummy variables and not order of magnitude as our outcome variable is simply due to database constraints. Some firms may not choose to report the specific number of records that have been breached, while others may have discovery delays and report that the number of physical or digital assets

9 Refer to PRC's website for variable definition.

10 Refer to online appendix for more details on class imbalance problem.

Table 1: This table provides the definitions for all outcome event variables and cyber incident trigger variables

No.	Variable name	Definition	Count
	Outcome event		
A.	*3rdPartyTransfer*	Takes the value of 1 if there were any money lost to an unauthorized third party, 0 otherwise.	267
B.	*BreachedRecords*	Takes the value of 1 if there were any records transferred to an unauthorized third party, 0 otherwise.	1474
C.	*AssetsAffected*	Takes the value of 1 if there were any physical or digital assets affected by the cyber incident, 0 otherwise.	2180
D.	*LocationAffected*	Takes the value of 1 if there were any physical or digital location affected by the cyber incident, 0 otherwise.	2185
E.	*PersonEmployeeAffected*	Takes the value of 1 if there were any employees or stakeholders affected by the cyber incident, 0 otherwise.	321
F.	*InaccessibleModifiedSystems*	Takes the value of 1 if there were any records affected by the cyber incident, 0 otherwise.	687
G.	*OperationsDisrupted*	Takes the value of 1 if there were any business interruption attributed to the cyber incident, 0 otherwise.	2108
H.	*Attributedby3rdPartyEcosystem*	Takes the value of 1 if the onset of cyber incident is attributed to an authorized stakeholder/third party who is not within the direct contract and management of the victim's entity, 0 otherwise.	368
I.	*IncidentResponseCost*	Takes the value of 1 if there were any direct technical investigation, forensics costs, as well as notification costs to third parties, 0 otherwise.	1830
J.	*RecoveryCost*	Takes the value of 1 if there were direct technical restoration costs as well as business centric costs to third parties, 0 otherwise.	2231
K.	*CompromiseAssessment*	Takes the value of 1 if unconfirmed cyber incident indicators claimed/reported by third parties, which require a thorough assessment to validate if indicators reported were true, 0 otherwise.	554
	Cyber incident trigger		
1.	*Account Hijack*	Defined as a trigger when there is an attempt for business accounts to be taken over by another party for malicious intent and purposes.	458
2.	*Business Email Compromise*	Defined as a trigger when there is an attempt to utilize corporate email accounts to facilitate losses to the company.	195
3.	*Business Extranet Compromise*	Defined as a trigger when there is an attempt to utilize the organization's extranet (i.e. controlled, private network) to facilitate false transactions.	152
4.	*DDoS Attack*	Defined as a trigger when there is an attempt to disrupt normal traffic of company's server, service, or network by overwhelming the IT infrastructure with a flood of internet traffic.	195
5.	*Delayed Notification*	Defined as a trigger when there is a lack of immediate and/or timely notification of the vulnerabilities to relevant decisionmakers and/or key stakeholders.	96
6.	*Messaging Platform Vulnerability*	Defined as a trigger when the losses arise from vulnerabilities from messaging platforms.	75
7.	*Misrepresented Authentication*	Defined as a trigger when there is an attempt to grant false authentication for business approvals.	136
8.	*Misrepresented Request for Credentials*	Defined as a trigger when there is an attempt for requests of username and password credentials for the intent to compromise admin, super user accounts, user, or business authority accounts.	147
9.	*Misrepresented Social Media Accounts*	Defined as a trigger when there is an attempt to utilize compromised social media accounts to push malicious and/ or misrepresented information to the followers and/or the public.	39
10.	*Prolonged Period of Exposure*	Defined as a trigger when a compromised systems environment has been actively exploited over a given period of time without the company being aware.	46
11.	*Targeted Attack*	Defined as a trigger when malicious actors purposefully exploit and compromise their known victim/organization.	33
12.	*Database Vulnerability*	Defined as a trigger when there is technical vulnerability in the database which can be exploited resulting in the cyber event.	26
13.	*Unauthorised Access*	Defined as a trigger when someone gains access to a company's resource without approval from the system owner.	2485
14.	*Unauthorised Action*	Defined as a trigger when someone performs retail activities without approval from the actual user account holder.	373
15.	*Unauthorised Broadcast*	Defined as a trigger when someone performs a mass communication through a compromised account without approval from the system owner.	121
16.	*Unauthorised Change*	Defined as a trigger when someone performs a configurational change to the system without approval from the system owner.	1084
17.	*Unauthorised Monetary Transaction*	Defined as a trigger when someone performs monetary transfers without approval from the system owner.	298

Table 1: Continued

No.	Variable name	Definition	Count
18.	*Unauthorised Propagation*	Defined as a trigger when someone performs a mass propagation of political ideals through a compromised account without approval from the system owner.	79
19.	*Unauthorised Publication*	Defined as a trigger when someone performs a publication on the system without approval from the system owner.	615
20.	*Unauthorised Redirection*	Defined as a trigger when someone performs a redirection of service through a compromised system account without approval from the system owner.	137
21.	*Unauthorised Resale*	Defined as a trigger when someone resells digital assets (usually data) without approval from the system owner.	344
22.	*Unauthorised Scanning*	Defined as a trigger when someone conducts security scanning on an organization's external/internal facing services for vulnerabilities to exploit without approval from the system owner.	143
23.	*Unauthorised Trade*	Defined as a trigger when someone trades digital assets (usually data) without approval from the system owner.	131
24.	*Unauthorised Transaction*	Defined as a trigger when someone transacts without approval from the system owner.	436
25.	*Unauthorised Transfer*	Defined as a trigger when someone successfully transfers digital assets/data without approval from the system owner.	1223
26.	*Unauthorised URL Direction*	Defined as a trigger when someone performs a redirection of a web service through a compromised DNS entry link without approval from the system owner.	63
27.	*Unauthorised Use of Credentials*	Defined as a trigger when someone uses the username and password credentials without approval from the actual user account holder.	89
28.	*Unauthorised Use of Data*	Defined as a trigger when someone uses the data without approval from the actual user account holder.	341
29.	*Unsecured MongoDB*	Defined as a trigger when the default (and unsecured) configuration of MongoDB and its industry equivalent noSQL DB is being used.	31
30.	*Vulnerability Exploit*	Defined as a trigger when known technical vulnerabilities are exploited.	121
31.	*Vulnerability Incomplete Installations*	Defined as a trigger when default installations and system configurations are used without additional hardening of systems.	83
32.	*Phishing Email*	Defined as a trigger when an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information/data.	129
33.	*Social Engineering*	Defined as a trigger when someone conducts a digital/physical act that influences the victim to take an action that may or may not be in the best interests of the victim.	157
34.	*Phreaking*	Defined as a trigger when the attacker hacks into secure telecommunication networks resulting in mobile phone cloning, bluejacking, and other forms of mobile phone hacking.	45
35.	*Website Vulnerability*	Defined as a trigger when the web frontend has technical vulnerabilities which are exploited.	138
36.	*Remote Desktop Protocol Vulnerability*	Defined as a trigger when hackers exploit a technical vulnerability to connect to a system from a separate location via the internet.	94
37.	*SQL Injection*	Defined as a trigger when the attacker uses malicious SQL code for backend database manipulation.	65
38.	*Skimming*	Defined as a trigger when attackers steal cardholder's personal payment information via physical/digital methods.	131
39.	*Content Management System Vulnerability*	Defined as a trigger when the CMS has technical vulnerabilities which are exploited.	56

that were affected is more than what was originally reported. Other database constraints involve difficulty to quantify and combine different types of cyber breach events. For example, a firm that experiences 100 breached records of personal identifiable information and 1000 breached records of credit card information—simply defining the total number of 1100 breached records may be misleading here. More importantly, we feel that our paper lays the initial groundwork to conduct similar analyses moving forward. It will be interesting indeed to have more granular definitions in future research works that apply similar analytical strategy as that presented in our paper.

In our analysis, we first divide the full sample into the training sample and testing sample in the ratio of 80:20. We then run the regression model on the training sample to allow the model to *learn* the important features that are key to predicting the corresponding type of cyber breach outcome. After learning the important features, we apply the trained model to the testing sample in order to predict the corresponding outcome. We then measure accuracy of predictions made by the trained model. We utilize two types of accuracy measures, (1) *TruePN* and (2) *F1-score*, refer to Fig. 1 for definitions, where:

$$TruePN = \frac{TP + TN}{TP + FP + TN + FN}$$

$$F1 - Score = \left\{ \frac{1}{2} \left[\left(\frac{TP}{TP + FN} \right)^{-1} + \left(\frac{TP}{TP + FP} \right)^{-1} \right] \right\}^{-1}.$$

		Actual	
		Positive	Negative
Predicted	Positive	True Positive (TP)	False Positive (FP); Type I error
	Negative	False Negative (FN); Type II error	True Negative (TN)

Figure 1: This figure illustrates how *TP, FP, TN,* and *FN* are defined..

Table 2: This table provides the results for the LASSO model under the Akaike information criterion

Information criterion: *AIC* summary	Within-sample fit				Out-of-sample prediction				No. of features selected	
	TruePN		*F1-score*		*TruePN*		*F1-score*			
	Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD
3rdPartyTransfer	0.8368	0.0090	0.8150	0.0067	0.8272	0.0333	0.7995	0.0276	21.30	2.71
BreachedRecords	0.8850	0.0030	0.8894	0.0028	0.8806	0.0140	0.8852	0.0144	28.40	1.78
AssetsAffected	0.7784	0.0154	0.7759	0.0185	0.7699	0.0230	0.7659	0.0264	25.20	1.48
LocationAffected	0.7725	0.0046	0.7665	0.0067	0.7598	0.0235	0.7535	0.0283	19.50	4.72
PersonEmployeeAffected	0.7201	0.0154	0.7227	0.0144	0.6906	0.0368	0.6870	0.0505	17.40	1.84
InaccessibleModifiedSystems	0.7451	0.0050	0.7662	0.0042	0.7463	0.0275	0.7673	0.0313	16.70	3.95
OperationsDisrupted	0.7528	0.0073	0.7551	0.0108	0.7374	0.0159	0.7397	0.0158	27.90	0.99
Attributedby3rdPartyEcosystem	0.6640	0.0164	0.6217	0.0664	0.6462	0.0244	0.5880	0.0706	17.10	2.73
IncidentResponseCost	0.8031	0.0050	0.7975	0.0049	0.8038	0.0162	0.7983	0.0165	14.50	12.59
RecoveryCost	0.8083	0.0060	0.8155	0.0067	0.8045	0.0226	0.8143	0.0207	28.00	2.00
CompromiseAssessment	0.7720	0.0163	0.7866	0.0154	0.7503	0.0217	0.7648	0.0267	24.70	4.76
Average	0.7762	0.0094	0.7738	0.0143	0.7651	0.0235	0.7603	0.0299	21.88	3.59

It details the mean and SD of the number of features selected, as well as the *TruePN* and *F1-score* for both the within-sample fit and the out-of-sample prediction.

Key results and analysis[11]

Predictive taxonomy analytics using LASSO

The first part of the analysis is to identify the consistency in predictive accuracy of the LASSO under *AIC*.[12] We randomly separated the training sample and the testing sample using 10 different seed values, this allows us to test the stability of the model's accuracy. We present the mean and SD of the results from the 10 different random samples. We focus on the *TruePN* and *F1-score* and found that the SD for the different features are relatively small. The results are presented in Table 2.

The average SD across different outcome features is 2.35 and 2.99% for *TruePN* and *F1-score*, respectively. Furthermore, as the mean *TruePN* and *F1-score* across all different outcome features is 76.5 and 0.7603%, respectively, this implies an associated coefficient of variation of 3.08 and 3.93%, respectively. Thus, this shows that the results are generally well clustered. Overall, these results show that the accuracy of the model is consistent across different seed values, which provides support for the robustness of the results.

Hence, the first part of the analysis above shows that the predictive accuracy of the LASSO under *AIC* is *sufficiently* and *consistently* high. The practical implication is that there exists a set of selected *keywords* (i.e. cyber incident trigger taxonomy) in our taxonomy that can be used to accurately predict the outcome of the cyber breach, given that a cyber breach occurs. This is of practical importance for researchers, insurers, and underwriters, as they can now use (or expand on) our list of *keywords* (or apply the methodology explained above to yield their own unique set of *keywords*) to predict cyber breach outcome types. The next part of the analysis focuses on what these keywords are and the implication that this brings to the industry.

Keyword analysis and implication for underwriters, insurers, companies, and individuals

In the previous section, we trained the model with a total of 39 unique features, and have the model automatically select the most important features for us (i.e. *feature selection*), under the *AIC* with undersampling to mitigate the class imbalance bias. We also show in the previous section how accurate these features are when it comes to predicting outcomes of a cyber breach event. In this section, we seek to shed light on what these selected features are and seek to provide a framework that stakeholders can use when it comes to managing cyber risks.

Specifically, each outcome variable type within each sample (i.e. recall we have 10 random samples generated by 10 different seed

11 Figure 1 shows True Positive (*TP*), True Negative (*TN*), False Positive (*FP*), and False Negative (*FN*) distributions.

12 We demonstrate the LASSO under AIC has the best predictive accuracy relative to other information criterion in the online appendix.

Table 3: This table illustrates the significance of cyber incident trigger variables in the model where *BreachedRecords* is the outcome variable for ten different seed values

Seed Values	111	222	333	1	2	3	11	22	33	123
Features	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Account hijack		+*	+	+	+	+	+	+	+	
Business email compromise	−***	−***	−***	−***	−***	−***	−***	−***	−***	−***
Business extranet compromise		+***	+***	+***	+***	+***	+***	+***	+***	+***
DDoS attack	−***	−***	−***	−***	−***	−***	−***	−***	−***	−***
Delayed notification	+***	+***	+***		+***		+***	+***		+***
Messaging platform vulnerability			+***	+***	+***	+***		+***	+***	+***
Misrepresented authentication		−***	−***			−***			−***	−***
Misrepresented request for credentials	−*	−		−*	−				−*	
Misrepresented social media accounts	+	+	+		+	+***	+	+**		+
Prolonged period of exposure	−	−	−				+**			−
Targeted attack	+		+***		+	+	+	+		+***
Database vulnerability	+***	+***	+***	+***	+***	+***	+***	+***	+***	+***
Unauthorized access	−***	−***	−***	−***	−***	−***	−***	−***	−***	−***
Unauthorized action	−***	−***	−***	−***	−***	−***	−**	−***	−***	−***
Unauthorized broadcast										
Unauthorized change	−***	−***	−***	−***	−***	−***	−***	−***	−***	−***
Unauthorized monetary transaction	+	+	+	+	+		+	+	+	
Unauthorized propagation										
Unauthorized publication	+*	+	+**	+	+*	+	+**	+**	+**	+**
Unauthorized redirection	+***	+***	+***	+***	+***	+***	+***	+***	+***	+***
Unauthorized resale	+**				−		+			
Unauthorized scanning	−***	−***	−***	−***	−***	−***	−***	−***	−***	−***
Unauthorized trade		−***	−***	−***	−***		−***	−***	−***	−***
Unauthorized transaction	+	+**	+*	+***	+***	+**	+**	+*	+**	+**
Unauthorized transfer	+***	+***	+***	+***	+***	+***	+***	+***	+***	+***
Unauthorized URL direction	+*		+	+*	+	+		+	+	+
Unauthorized use of credentials			−				−			+
Unauthorized use of data			+***							
Unsecured MongoDB	+***	+***	+***	+***	+***	+***	+***		+***	+***
Vulnerability exploit										
Vulnerability incomplete installations					+***			+***		
Phishing email	+***	+***	+***	+***	+***	+***	+***	+***	+***	+***
Social engineering	+	+	+***	+	+	+	+	+*	+	+
Phreaking	+***	+***	+***	+***	+***	+***	+***	+***	+***	+***
Website vulnerability	+***	+***		+*	+***	+*	+**	+**	+***	+**
Remote desktop protocol vulnerability	+***	+***	+***	+***	+***	+***	+***	+***	+***	+***
SQL injection	+**	+*	+***	+***	+	+***	+**	+***	+***	+**
Skeeming	+***	+***	+***	+***	+***	+***	+***	+***	+***	+***
Content management system vulnerability		−							−**	

values) is associated with their own list of selected features (i.e. *keywords*). We run this set of selected features within their corresponding training sample and we summarize the sign and significance of the coefficients. The results for outcome variable type *BreachedRecords* is presented in Table 3.

Columns 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10 corresponds to seed values of 111, 222, 333, 1, 2, 3, 11, 22, 33, and 123, respectively. We repeat the analysis for each of the other outcome variable type, and the results are summarized in Table A5. Specifically, in Table A5, results for outcome variable type *3rdPartyTransfer*, *AssetsAffected*, *LocationAffected*, *PersonEmployeeAffected*, *InaccessibleModifiedSystems*, *OperationsDisrupted*, *AttributedBy3rdPartyEcosystem*, *IncidentResponseCost*, *RecoveryCost*, and *CompromiseAssessment*, are presented in Panels A, B, C, D, E, F, G, H, J, and K, respectively. Interpreting the results in these tables is straightforward. For example, in Table A5 Panel A, we present the results for outcome feature *3rdPartyTransfer*. We show that "*Account Hijack*" is selected and positively relates under all 10 columns but is only statistically significant at the 10 and 5% in columns 6 and 8, respectively. It is also intuitive to see that when there is a "*DDoS Attack*," it negatively relates to *3rdPartyTransfer* and is significant at the 1% level across all columns. This strategy can be readily applied across different features to understand, which of the selected features can be used to accurately predict the outcome feature. In addition, we summarized triggers that are statistically significant at the 1% level across all 10 seed values in Table 4. This provides readers a bird's eye view on the most significant triggers for each outcome feature. However, it is to be noted that there are other triggers that are significant at the 5 and 10% level, which are not highlighted in Table 4.

A potential concern in our method here is multicollinearity problems. While LASSO can handle multicollinearity by dropping features, it does not control, which feature to be removed and this may result in unstable feature selection. To mitigate multicollinearity concerns, we construct a correlation matrix of the cyber triggers and the results are presented in Table A6. With 39 cyber triggers, we have 741 unique pairs of cyber triggers, among which only 12 pairs have an absolute correlation value between 0.3 and 0.5 and only one pair has an absolute correlation value greater than 0.5, with the rest

Table 4: This table illustrates the most consistently significant cyber incident trigger variables for each of the outcome event variable

Outcome feature	Breached records	Third party transfer	Assets affected	Location affected	Person employee affected	Inaccessible modified systems	Operations disrupted	Attributed by third party ecosystem	Incident response cost[13]	Recovery cost	Compromise assessment
Significantly positive triggers	• Database vulnerability • Unauthorized redirection • Unauthorized transfer • Phishing email • Phreaking • Remote desktop protocol vulnerability skeeming	• Unauthorized monetary transaction • Unauthorized transaction • Social engineering • Remote desktop protocol vulnerability	• DDoS attack • Unauthorized monetary transaction • Unauthorized publication • Unauthorized redirection • Unauthorized transfer • Phishing email • Remote desktop protocol vulnerability	• DDoS attack • Database vulnerability • Unauthorized monetary transaction • Unauthorized publication • Unauthorized transfer	• Account hijack • Database vulnerability • Unauthorized transfer	• Account hijack • DDoS attack • Unauthorized change • Unauthorized trade	• Delayed notification • Database vulnerability • Unauthorized publication • Unauthorized transfer • Phishing email • Remote desktop protocol vulnerability	• Account hijack • Misrepresented social media accounts	• Database vulnerability • Unauthorized monetary transaction • Unauthorized redirection • Unauthorized transaction • Unauthorized transfer • Phishing email • Remote desktop protocol vulnerability • SQL injection • Content management system vulnerability	• Database vulnerability • Unauthorized transfer • Phishing email • Remote desktop protocol vulnerability	• Unauthorized publication • Unauthorized transfer
Significantly negative triggers	• Business email compromise • DDoS attack • Unauthorized access • Unauthorized change • Unauthorized scanning	• DDoS attack • Unauthorized access	• Unauthorized action • Unauthorized scanning	• Unauthorized action	• Unauthorized publication	• Unauthorized action	• Unauthorized action • Unauthorized scanning • Vulnerability exploit	• Unauthorized action	• Misrepresented social media accounts • Unauthorized action • Unauthorized scanning • Vulnerability exploit	• Unauthorized action • Unauthorized broadcast • Unauthorized scanning	–

[13]For *IncidentResponseCost*, there were no triggers that were significant at the 1% level for all 10 seed values. The triggers included here are significant at the 1% level for at least four seed values.

having little to no correlation indicated by an absolute correlation value that is between 0 and 0.3. Therefore, it is unlikely that multicollinearity had significantly affect our results. However, we propose that in future work, a good strategy to deal with highly correlated variables would be to combine highly correlated features into a single variable.

Taken together, these results provide a grounded methodology for underwriters to identify a list of *keywords* that are mathematically associated with each outcome feature. This is of significant importance for underwriters of cyber insurance products, as their core scope of work is to accurately determine the associated level of risk involved in the client's cybersecurity posture toward different types of cyber insurance product. For example, if a potential client is interested to purchase a cyber insurance product that indemnifies the insured when their records are breached, the underwriter can look at our result in Table 3, Table 4, and Table A5 to improve their assessment of the risk level of the potential client. These tables tell them that the breach of records is significantly more likely, at the 1% level, to be triggered by *"Database Vulnerability"*, *"Unauthorised Redirection"*, *"Unauthorised Transfer"*, *"Phishing Email"*, *"Phreaking"*, *"Remote Desktop Protocol Vulnerability"*, *"Skimming"*; whereas issues such as *"Business Email Compromise"*, *"DDoS Attack"*, *"Unauthorised Access"*, *"Unauthorised Change"*, and *"Unauthorised Scanning"* are significantly less likely, at the 1% level, to result in *BreachedRecords*.

This means that when the underwriters are assessing the risk levels of the potential client, they know that they should, e.g. pay more attention to potential technical vulnerabilities in the database (i.e. "*Database Vulnerability*"); pay more attention on whether training programs are in place to educate system owners to not click on fraudulent emails (i.e. "*Phishing Email*"); and pay more attention on whether operation controls are in place to prevent attackers from stealing cardholder's information (i.e. "*Skimming*"). Similarly, underwriters also know that they should, for example, pay less attention on whether training programs are in place to minimize attempts made to utilize corporate email accounts to facilitate losses to the company (i.e. "*Business Email Compromise*"); pay less attention on cyber security defense architecture such as multi-level protection strategies (e.g. firewall, VPN, content filtering, etc) that reduce the risk of DDoS attacks (i.e. "*DDoS Attack*"); and pay less attention on operation controls in place to reduce the risk of someone gaining access to a company's resource without approval from system owner (i.e. "*Unauthorised Access*"). Our result can help underwriters zoom in quickly on the cybersecurity risk postures that matter for the potential client. At the same time, our results will allow underwriters to draft more effective documents (e.g. underwriting contracts and prepurchase survey forms) in assessing and underwriting the cybersecurity risk levels of the potential client. That said, we like to highlight that our example above is specific toward underwriters who are only assessing the risk level of *BreachedRecords*. However, when underwriters are assessing the cyber risks of other cyberattack outcomes, they are advised to take on a more holistic perspective and account for a wider set of cyber incident triggers. At the same time, it is also important for users to refer to the definition table of our taxonomy. This is because different individuals may have different interpretations for the various cyber incident trigger, such as "Unauthorized Access". Therefore, it is important for users of our results to refer to our definition table and ensure that their definitions of cyber incident triggers are aligned with ours before using the results in this paper to make key decisions.

Following a similar logic, these results are also of great significance to cybersecurity companies and cybersecurity risk management teams. The objective of these cybersecurity professionals is to improve and secure the cybersecurity risk posture of the firm towards different types of cybersecurity risks. For example, if the firm is particularly vulnerable to having their records breached, or they are particularly interested to ensure their records are well protected. Our results here can help the cybersecurity professionals quickly identify the cybersecurity risk postures that matter for the firm (i.e. the same as the ones mentioned above). Thus, this helps them focus on improving and securing the risk postures that are critical in protecting the firm from having their records breached.

LASSO discussion

A reason why LASSO was more useful in our setting, relative to a traditional regression model, was because it can help to improve the goodness of fit of our model, and consequently improve the predictive power of our model. For example, using our *BreachedRecord* outcome variable, we first ran a multiple linear regression using the 12 cyber incident trigger variables that were significant at the 1% level across all 10 seed values (Table 3), we arrived at an *F*-statistic that is 367.16. Next, we ran a second multiple linear regression using all 39 cyber incident trigger variables, the *F*-statistic deteriorated to 120.17. At the same time, the adjusted-R^2 also experienced only a marginal improvement from 0.5799 to 0.5935.

Another traditional strategy in running regressions is to employ a theory-driven approach, where we identify which cyber incident triggers are likely to result in the outcome variable. We then test our intuition by running the regression model. Even though this strategy may have been employed for our paper, we decided against it as it may introduce confirmation bias [34], where we include variables that confirm our initial beliefs and unknowingly exclude other relevant variables. Therefore, we used LASSO and successfully arrived at models that were accurate in its out-of-sample prediction, coupled with several interesting results, as documented in Table 3, Table 4, and Table A5.

Finally, as the cost of collecting and storing information decreases, we foresee that data on cyber breaches will increase significantly in the future. This signifies the importance of utilizing non-traditional methodologies to analyze big data.[14] We hope that our paper may encourage our colleagues to utilize novel and creative methodologies to uncover even more interesting results.

Regression on industry type

Inspired by prior literature, we seek to identify industries that might be most susceptible to specific cyber breaches. Following methodology from prior literature, we apply standard traditional regression analyses and include all industries in the regression model. To account for potential-omitted variable bias, we control for year-fixed effects,[15] and the model is as follows:

$$CyberBreachOutcome_t = \alpha_0 + \alpha_t + IndustryType_t + \epsilon_t,$$

where *CyberBreachOutcome* is the 11 outcome features used in the earlier analyses, *IndustryType* is the breached firm's industry, α_0 is the constant term, α_t controls for the year fixed effects, ϵ_t is the error term, and we use the robust standard errors. The results are presented in Table 5.

As the coefficients represent a relative difference between different industries, it may be more interesting to identify how each indus-

14 Refer to online appendix for a more detailed discussion on why LASSO was selected over traditional regression approaches.

15 We drop the year-fixed effects and results remain consistent and are presented in Table A7.

Table 5: This table provides the results of a standard regression where *IndustryType* is the breached firm's industry, and the 11 columns of results corresponds to each of the 11 outcome event variables.

Variables	(1) *3rdParty Transfer*	(2) *Breached Records*	(3) *Assets Affected*	(4) *Location Affected*	(5) *PersonEmployee Affected*	(6) *Inaccessible Modified Systems*	(7) *Operations Disrupted*	(8) *Attributedby 3rd Party Ecosystem*	(9) *Incident Response Cost*	(10) *Recovery Cost*	(11) *Compromise Assessment*
Academic/education	0.076***	0.417***	0.632***	0.632***	0.357***	0.177***	0.597***	−0.041*	0.616***	0.590***	0.097***
	(0.024)	(0.042)	(0.031)	(0.031)	(0.038)	(0.039)	(0.034)	(0.022)	(0.036)	(0.033)	(0.036)
Business and professional services	0.352***	0.710***	0.583***	0.549***	0.233***	0.075	0.563***	0.039	0.644***	0.639***	0.214***
	(0.055)	(0.030)	(0.039)	(0.050)	(0.064)	(0.064)	(0.051)	(0.053)	(0.049)	(0.027)	(0.072)
Critical infrastructure/critical information infrastructure	0.032	−0.055	0.151*	0.153*	0.082*	0.162**	0.173**	−0.040	0.277***	0.141*	−0.028
	(0.035)	(0.058)	(0.082)	(0.082)	(0.046)	(0.072)	(0.081)	(0.037)	(0.081)	(0.081)	(0.053)
Defense/private physical security contractor	0.012	0.304**	0.353***	0.356***	0.132*	0.087	0.365***	0.052	0.496***	0.419***	0.315***
	(0.011)	(0.120)	(0.102)	(0.102)	(0.070)	(0.102)	(0.102)	(0.086)	(0.105)	(0.091)	(0.111)
	0.056***	0.328***	0.530***	0.537***	0.052***	0.264***	0.528***	0.023	0.441***	0.547***	0.071*
Entertainment/media/marketing/loyalty/membership											
	(0.019)	(0.043)	(0.033)	(0.033)	(0.019)	(0.039)	(0.034)	(0.029)	(0.041)	(0.032)	(0.037)
Finance—banking/insurance/investment management	0.211***	0.227***	0.371***	0.371***	0.129***	0.238***	0.349***	0.110***	0.313***	0.374***	0.062*
	(0.031)	(0.041)	(0.042)	(0.042)	(0.028)	(0.038)	(0.042)	(0.034)	(0.044)	(0.040)	(0.036)
Government/state administration/public goods	0.048***	0.180***	0.361***	0.361***	0.102***	0.201***	0.364***	−0.025	0.306***	0.400***	0.018
	(0.014)	(0.031)	(0.032)	(0.033)	(0.018)	(0.028)	(0.032)	(0.019)	(0.033)	(0.031)	(0.026)
Healthcare	0.074***	0.534***	0.676***	0.672***	0.330***	0.225***	0.695***	−0.017	0.717***	0.656***	0.068**
	(0.022)	(0.037)	(0.027)	(0.028)	(0.035)	(0.038)	(0.027)	(0.024)	(0.029)	(0.028)	(0.033)
Information technology/emerging technologies/suffix-tech (eg. FinTech, InsurTech)	0.136***	0.319***	0.464***	0.474***	0.071***	0.192***	0.462***	0.133***	0.428***	0.504***	0.146***
	(0.023)	(0.035)	(0.034)	(0.034)	(0.020)	(0.031)	(0.034)	(0.029)	(0.036)	(0.032)	(0.031)
Primary industries/mining	0.017	0.377	0.538***	0.542***	0.035***	0.144	0.216	0.224	0.753***	0.224	0.380
	(0.011)	(0.275)	(0.027)	(0.027)	(0.012)	(0.274)	(0.275)	(0.274)	(0.026)	(0.275)	(0.274)
Food-related/agriculture /wholesale	0.151**	0.549***	0.608***	0.606***	0.143**	0.272***	0.627***	0.249***	0.658***	0.609***	0.209***
	(0.060)	(0.065)	(0.054)	(0.057)	(0.063)	(0.076)	(0.055)	(0.078)	(0.061)	(0.047)	(0.076)

Table 5: Continued

Variables	(1) *3rdParty Transfer*	(2) *Breached Records*	(3) *Assets Affected*	(4) *Location Affected*	(5) *PersonEmployee Affected*	(6) *Inaccessible Modified Systems*	(7) *Operations Disrupted*	(8) *Attributedby 3rd Party Ecosystem*	(9) *Incident Response Cost*	(10) *Recovery Cost*	(11) *Compromise Assessment*
Non-government organizations/charities/volunteers	0.002	0.233***	0.387***	0.389***	0.093***	0.166***	0.359***	0.014	0.293***	0.394***	0.024
	(0.009)	(0.056)	(0.049)	(0.049)	(0.031)	(0.052)	(0.050)	(0.037)	(0.057)	(0.049)	(0.048)
Manufacturing	0.112**	0.580***	0.554***	0.570***	0.253***	0.105*	0.535***	0.056	0.607***	0.610***	0.092
	(0.046)	(0.050)	(0.051)	(0.050)	(0.061)	(0.060)	(0.056)	(0.050)	(0.055)	(0.035)	(0.058)
Real estate/property/construction	0.211**	0.501***	0.590***	0.560***	0.107	0.364***	0.569***	0.050	0.508***	0.621***	0.195
	(0.087)	(0.074)	(0.034)	(0.032)	(0.076)	(0.137)	(0.033)	(0.102)	(0.107)	(0.029)	(0.137)
Online/e-commerce	0.021	0.491***	0.471***	0.475***	0.010	−0.073	0.458***	−0.040	0.570***	0.483***	0.280***
	(0.027)	(0.078)	(0.047)	(0.047)	(0.016)	(0.055)	(0.051)	(0.045)	(0.070)	(0.047)	(0.082)
Pharmaceuticals/supplements	0.017	0.711***	0.538***	0.542***	0.035***	0.310	0.549***	0.390	0.753***	0.557***	−0.287***
	(0.011)	(0.025)	(0.027)	(0.027)	(0.012)	(0.356)	(0.027)	(0.356)	(0.026)	(0.026)	(0.024)
Tourism and hospitality	0.106**	0.613***	0.543***	0.545***	0.124**	0.197***	0.539***	−0.002	0.695***	0.559***	0.320***
	(0.048)	(0.064)	(0.062)	(0.063)	(0.051)	(0.073)	(0.065)	(0.051)	(0.054)	(0.057)	(0.076)
Retail/retail wholesale/trade	0.111***	0.621***	0.607***	0.606***	0.059	0.116**	0.579***	0.141**	0.637***	0.592***	0.122*
	(0.043)	(0.054)	(0.050)	(0.053)	(0.037)	(0.058)	(0.058)	(0.059)	(0.062)	(0.044)	(0.066)
Single individual	0.014	−0.068***	−0.060**	−0.061**	−0.002	0.044**	−0.052*	0.126***	−0.098***	0.002	−0.078***
	(0.012)	(0.025)	(0.029)	(0.029)	(0.012)	(0.022)	(0.028)	(0.024)	(0.026)	(0.030)	(0.020)
Telecommunications	0.004	0.293***	0.463***	0.465***	0.208**	0.156	0.477***	−0.057	0.362***	0.472***	0.275**
	(0.012)	(0.112)	(0.066)	(0.066)	(0.086)	(0.100)	(0.066)	(0.049)	(0.106)	(0.067)	(0.110)
Transportation/logistics/warehousing	0.126**	0.327***	0.538***	0.535***	0.157***	0.211***	0.509***	−0.004	0.454***	0.551***	0.165**
	(0.053)	(0.078)	(0.058)	(0.058)	(0.059)	(0.075)	(0.063)	(0.050)	(0.082)	(0.051)	(0.077)
Others	–	–	–	–	–	–	–	–	–	–	–
Constant	0.888***	0.290***	0.536***	0.458***	−0.035***	0.190***	0.421***	0.110***	0.363***	0.361***	0.287***
	(0.046)	(0.030)	(0.034)	(0.027)	(0.012)	(0.023)	(0.058)	(0.019)	(0.062)	(0.027)	(0.024)
Year FE	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Robust standard errors in parentheses											
*** $P < 0.01$, ** $P < 0.05$, * $P < 0.1$											

Table 6: This table highlights the industry types that are most statistically and economically significant in the regression analysis where the outcome variable is *BreachedRecords*

Outcome feature	*BreachedRecords*		
Rank	Industry type	Coefficient	Significance
1	Pharmaceuticals/supplements	0.711	***
2	Business and professional services	0.71	***
3	Retail/retail wholesale/trade	0.621	***
4	Tourism and hospitality	0.613	***
5	Manufacturing	0.58	***
6	Food related/agriculture/wholesale	0.549	***
7	Healthcare	0.534	***
8	Real estate/property/construction	0.501	***
9	Online/e-commerce	0.491	***
10	Academic/education	0.417	***
11	Entertainment/media/marketing/loyalty/membership	0.328	***
12	Transportation/logistics/warehousing	0.327	***
13	Information technology/emerging technologies/suffix-tech (eg. FinTech, InsurTech)	0.319	***
14	Defense/private physical security contractor	0.304	**
15	Telecommunications	0.293	***
16	Non-government organizations/charities/volunteers	0.233	***
17	Finance—banking/insurance/investment management	0.227	***
18	Government/state administration/public goods	0.18	***
19	Single individual	− 0.068	***

try rank, relative to another industry, in terms of susceptibility to different cyber breach event types. Specifically, we focus only on industry types with coefficients that are at least 10% level of significance and rank these industry types from the largest coefficient to the smallest coefficient. Our results for outcome feature *BreachedRecords* is presented in Table 6 and the results for all other outcome features are presented in Table A8.[16]

The analyses shed light on how underwriters can better manage underwriting risks of cyber insurance policies. For example, they might seek to charge a higher premium (or lower coverage) for "*Business and Professional Services*" looking for *3rdPartyTransfer* cyber insurance coverage, and they might consider providing a discount in premium (or higher coverage) for "*Government/State Administration/Public Goods*" looking for cyber insurance covering *3rdPartyTransfer*.

The results are also useful for companies (individuals) who seek to mitigate their risks of cyber breaches. Companies can seek to identify the industry that they are in and aim to invest more in the cyber defenses for the breach event types that they are most susceptible to. This can help to increase the efficiency of the firm's cyber security investments and bring them closer toward the *Security Production Frontier* [35].

Finally, in future research, it may be interesting to include interaction between cyber triggers and industry types within the LASSO model. We may also run the model on subsamples for firms in the same industry. This will allow us to compare the predictive power of the cyber triggers on specific outcome types across different industries.

Discussion and conclusion

Our results are important for researchers, insurers, underwriters, and cybersecurity professionals as it empowers them to engage in an effective strengthening of the cybersecurity architecture, as well as drafting more effective contractual cyber risk agreements.

16 Refer to online appendix for detailed description of results presented in Table 6 and Table A8.

Limitations

Despite the positive results in our research, we would like to draw the reader's attention to two potential caveats of our paper. First, like all statistical and machine learning analyses, there exists a likelihood of false alarm, or more commonly known as false positives. We have sought to minimize the likelihood of this problem by using undersampling techniques as well as using *F1-score* to test prediction accuracy. Although these techniques do not diminish the issue entirely, after consultations with industry experts, we note that it is better to detect more false alarms in the early stage than to miss a real breach. This is because the cost of detecting false alarms is less than that of mitigating a breach that occurs.

Second, the results in our paper are based on historical data. Therefore, it might be possible that any associated relationships identified here may evolve quickly over time, thus diminishing the immediate usefulness of our paper. Furthermore, the taxonomy is dynamic and may differ across different domains. This may lead to challenges in generalizing the findings and care should be taken when using the taxonomy generated in this paper. However, we propose that our paper's objective is to provide a starting point that allows ongoing and longer term analysis to be possible. The most important contribution of our paper is not simply the list of taxonomy generated, but rather is the technique that we use in selecting the list of taxonomy. We want to highlight that even if the underlying behavior of cyberattacks changes, the methodology proposed in our paper can remain a good strategy that may be used by relevant stakeholders to conduct up-to-date analysis.

Specifically, we envision that other researchers who have better and more refined databases, may apply our methodology to arrive at even more interesting and persistent results than ours. At the same time, we are also working on updating the database. As more data are captured and collected, more parameters may be included in future research as well (e.g. position of person reporting the breach, company size, organization type, disclosure type, size of cyber security department, and cybersecurity protocols), and this can potentially improve the accuracy and predictive power of the models in our paper. Overall, that will ensure continuity and usefulness of our paper in spite of the rapid changes in the cybersecurity landscape.

Conclusion

Our paper applies a general analytical tool in predicting a wide variety of different cyber breach outcome types. This is novel and important because in the study of cybersecurity, there is a wide range of cybercrimes in the field. Thus, having a unified framework allows for a consistent analysis of cyber breaches. The challenge in setting up the analysis is the initial database construction and defining the list of taxonomy. We hope that our work lays the initial groundwork in this space.

Supplementary data

Supplementary data is available at *Cybersecurity Journal* online.

Author contributions

Jing Rong Goh (Conceptualization [lead], Formal analysis [lead], Funding acquisition [supporting], Methodology [lead], Software [lead], Supervision [equal], Validation [lead], Visualization [lead], Writing – original draft [lead], Writing – review & editing [lead]), Shaun Shuxun Wang (Conceptualization [supporting], Funding acquisition [lead], Methodology [supporting], Project administration [equal], Resources [lead], Supervision [equal], Writing – review & editing [supporting]), Yaniv Harel (Validation [supporting], Writing – review & editing [supporting]) and Gabriel Toh (Data curation [lead], Formal analysis [supporting], Project administration [equal], Writing – review & editing [supporting]).

Conflict of interest statement

The authors do not have any conflicts of interest.

Funding

The research work was supported by two research programmes: (1) the Cyber Risk Management (CyRiM) programme, a public-private partnership between the Nanyang Technological University, the Monetary Authority of Singapore, the Cyber Security Agency of Singapore, Aon, Lloyd's, MSIG, SCOR and TransRe; and (2) The Quantification of Cyber Risk programme, jointly awarded by the National Research Foundation of Singapore and Tel Aviv University of Israel.

References

1. McAfee. The Economic Impact of Cybercrime—No Slowing Down. 21 February 2018. [Online]. Available: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html (8 February 2022, date last accessed).
2. McAfee. The Hidden Costs of Cybercrime. December 2020. [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf (8 February 2022, date last accessed).
3. World Economic Forum. This is the Crippling Cost of Cybercrime on Corporations. *World Economic Forum*. [07 November 2019]. [Online]. Available: https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/ (8 February 2022, date last accessed).
4. Edwards B, Hofmeyr S, Forrest S. Hype and heavy tails: a closer look at data breachnes. *J Cybersecur* 2016;**2**:3–14.
5. Sen R, Borle S. Estimating the contextual risk of data breach: an empirical approach. *J Manag Inf Syst* 2015;**32**:314–41.
6. Paquet-Clouston M, Haslhofer B, Dupont B. Ransomware payments in the Bitcoin ecosystem. *J Cybersecur* 2019;**5**.pa
7. Connolly LY, Wall DS, Lang M. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *J Cybersecur* 2020;**6**:1–11.
8. Riek M, Böhme R. The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates. *J Cybersecur* 2018;**4**:1–16. http://dx.doi.org/10.1093/cybsec/tyy004.
9. Khalili MM, Liu M, Romanosky S. Embracing and controlling risk dependency in cyber-insurance policy underwriting. *J Cybersecur* 2019;**5**:1–16.
10. Sridhar K, Ng M. Hacking for good: leveraging HackerOne data to develop an economic model of Bug Bounties. *J Cybersecur* 2021;**7**:1–9. http://dx.doi.org/10.1093/cybsec/tyab007.
11. Agrafiotis I, Nurse JR, Goldsmith M. *et al.* A taxonomy of cyber-harms: defining the impacts of cyberattacks and understanding how they propagate. *J Cybersecur* 2018;**4**:1–15.
12. Tibshirani R. Regression shrinkage and selection via the lasso. *J R Stat Soc Series B Stat Methodol* 1996;**58**:267–88.
13. RiskBased Security. 2020 Mid Year Report Vulnerability QuickView. 2020. https://pages.riskbasedsecurity.com/en/2020-mid-year-vulnerability-quickview-report (8 February 2022, date last accessed).
14. Gordon LA, Loeb MP. The economics of information security investment. *ACM Trans Inf Syst Secur* 2002;**5**:438–57.
15. Anderson R, Moore T. The economics of information security. *Science* 2006;**314**:610–3.
16. Baryshnikov Y. IT security investment and Gordon–Loeb's 1/e rule. *The Workshop on the Economics of Information Security (WEIS)* 2012. https://faculty.math.illinois.edu/~ymb/ps/cyber.pdf (8 February 2022, date last accessed).
17. Böhme R. Security metrics and security investment models. *Adv Inf Comput Secur IWSEC* 2010;**6434**:10–24.
18. Eling M, Schnell W. Capital requirements for cyber risk and cyber risk insurance: an analysis of solvency II, the U.S. risk-based capital standards, and the Swiss solvency test. *N Am Actuar J* 2019;**24**:1–23.
19. Farkas S, Lopez O, Thomas M. Cyber claim analysis using generalized pareto regression trees with applications to insurance. *Insur Math Econ* 2021;**98**:92–105.
20. Campbell K, Gordon LA, Loeb MP, Zhou L. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *JCS* 2003;**11**:431–48.
21. Kamiya S, Kang JK, Kim J. *et al.* What is the Impact of Successful Cyberattacks on Target Firms?. *Fisher College of Business Working Paper No. 2018-03-004*, United States, 2018.
22. Felici M, Wainwright N, Cavallini S. What's new in the economics of cybersecurity?. *IEEE Secur Privacy* 2016;**14**:11–3.
23. Falco G, Eling M, Jablanski D. *et al.* Cyber risk research impeded by disciplinary barriers. *Science* 2019;**366**:1066–9.
24. Harel Y, Ben-Gal I, Elovici Y. Cyber security and the role of intelligent systems in addressing its challenges. *ACM Trans Intell Syst Technol* 2017;**8**:1–12.
25. NIST. *800-30 Revision 1: Guide for Conducting Risk Assessments*. United States: National Institute of Standards Technology (NIST) Special Publication. 2012.
26. Romanosky S, Ablon L, Kuehn A, Jones T. Content analysis of cyber insurance policies: how do carriers price cyber risk?," *J Cybersecur* 2019;**5**:1–19.
27. Romanosky S, Ablon L, Kuehn A, Jones T. Content analysis of cyber insurance policies. *Working Paper* 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929137 (8 February 2022, date last accessed).
28. Qiu J, Wu Q, Ding G. *et al.* A survey of machine learning for big data processing. *EURASIP J Adv Signal Process* 2016;**67**:1–16.
29. Jacobs J, Romanosky S, Adjerid I, Baker W. Improving vulnerability remediation through better exploit prediction. *J Cybersecur* 2020;**6**:1–16. http://dx.doi.org/10.1093/cybsec/tyaa015.
30. Privacy Rights Clearinghouse. Privacy Rights Clearinghouse," Privacy Rights Clearinghouse. [Online]. Available: https://privacyrights.org/data-breaches (8 February 2022, date last accessed).
31. Identity Theft Resource Center. Annual Data Breach Report. Identity Theft Resource Center. [Online]. Available: https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/ (8 February 2022, date last accessed).
32. Gemalto. Gemalto Breach Level Index Report 2017. Gemalto. [Online]. Available: https://marketing.idquantique.com/acton/attachment/11868/f-02f4/1/-/-/-/-/Gemalto%20Breach%20Level

%20Index%20Report%202017.pdf (8 February 2022, date last accessed).
33. Secura–A Bureau Veritas Company. *OTCAD Operational Technology Cyber Attack Database*. 2021. Secura—A Bureau Veritas Company. [Online]. Available: https://www.secura.com/uploads/whitepapers/Secura-White-Paper-OTCAD.pdf (8 February 2022, date last accessed).
34. Nickerson RS. Confirmation bias: a ubiquitous phenomenon in many guises. *Rev Gen Psychol* 1998;**2**;175–220.
35. Wang S. Knowledge set of attack surface and cybersecurity rating for firms in a supply chain. *Working Paper* 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064533 (8 February 2022, date last accessed).