JBA

JOURNAL OF BUSINESS ANALYTICS

Dursun Delen
Sudha Ram
Richard Vidgen

Journal of Business Analytics

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tjba20

Cybersecurity Threats and Organisational Response: Textual Analysis and Panel Regression

Anand Jeyaraj, Amir Zadeh & Vikram Sethi

To cite this article: Anand Jeyaraj, Amir Zadeh & Vikram Sethi (2021) Cybersecurity Threats and Organisational Response: Textual Analysis and Panel Regression, Journal of Business Analytics, 4:1, 26-39, DOI: 10.1080/2573234X.2020.1863750

To link to this article: https://doi.org/10.1080/2573234X.2020.1863750

Published online: 26 Dec 2020.

JOURNAL OF BUSINESS ANALYTICS
2021, VOL. 4, NO. 1, 26–39
https://doi.org/10.1080/2573234X.2020.1863750

ORIGINAL ARTICLE

Cybersecurity Threats and Organisational Response: Textual Analysis and Panel Regression

Anand Jeyaraj, Amir Zadeh and Vikram Sethi

Information Systems, Raj Soin College of Business, Wright State University, Dayton, OH, USA

ABSTRACT
This study examines the relationship between cybersecurity threats faced and cybersecurity response planned by organisations. Classifying cybersecurity threats into four types – physical threats, personnel threats, communication and data threats, and operational threats – this study examines organisational responses to such threats. Using textual data on cybersecurity threats and response gathered from the 10-K reports published by 87 organisations, topic modelling was conducted to assess the threats and response. A cross-sectional time-series regression model fitted on the topic weights showed that cybersecurity response was influenced by cybersecurity threats, beyond the time-invariant control and period variables. Specifically, physical threats and operational threats influenced the technical response; physical threats, communication and data threats, and operational threats influenced the non-technical response; and personnel threats influenced the overall response. Implications for research and practice are discussed.

ARTICLE HISTORY
Received 2 September 2020
Accepted 3 December 2020

KEYWORDS
Cybersecurity threats; cybersecurity response; topic modelling; panel regression

1. Introduction

Cybersecurity is of considerable interest to information technology (IT) and information systems (IS) research and practice. Organisations have experienced several coordinated and highly visible cybersecurity attacks that have resulted in considerable losses. For instance, EquiFax Corporation had data loss for 145 million customers, Facebook, Inc. experienced data exposure of 540 million users, and Marriott International had a breach that impacted 5 million guests as reported in various news outlets (Glaser, 2019; Gressin, 2017; Lyles, 2020). Consequently, organisational leaders emphasise cybersecurity as one of their major concerns (McLaughlin & Gogan, 2018).

Extant research on cybersecurity is multi-faceted and has striven to identify threats to cybersecurity, mechanisms of breaches and attacks in cybersecurity, impacts of cybersecurity breaches, and guidelines for cybersecurity responses for organisations. Jenab and Moslehpour (2016) summarise the extensive literature on various topics such as network security, information security, and cloud security. Gordon et al. (2008) describe the capital allocations in cybersecurity systems and the installation of the Chief Information Security Officer positions within organisations for cybersecurity oversight and management. Prior studies have found that cybersecurity breaches have generally had negative consequences on organisations although there are exceptions (e.g., Kannan et al., 2007). These include lost market value, lost share price, and negative stock market return (e.g., Campbell et al., 2003; Cavusoglu et al., 2004; Garg et al., 2003; Goel & Shawky, 2009; Telang & Wattal, 2007). Therefore, organisations may be expected to place considerable emphasis on securing their data and systems, and guard against cybersecurity threats, attacks, and breaches.

Despite considerable research on various aspects related to cybersecurity, attention to the relationship between cybersecurity threats and organisational response to cybersecurity threats has been scant. Due to the diversity in cybersecurity threats and potential responses by organisations, this study examines the impacts of four different types of cybersecurity threats on two types of organisational response to cybersecurity threats. The empirical analysis is based on topic modelling of the textual data about threats and response extracted from the annual 10-K reports published by organisations, and a cross-sectional time-series (XT) regression analysis to understand organisational response to cybersecurity threats.

The remainder of the paper is organised as follows. The next section introduces the related literature informing this study. The research model and research methods are described in the subsequent two sections. These are followed by the results and discussion sections, and the conclusion section wraps up the paper.

2. Related literature

Cybersecurity has been variously defined in prior literature. Craigen et al. (2014) describes it as "the

CONTACT Amir Zadeh amir.zadeh@wright.edu Information Systems, Raj Soin College of Business, Wright State University, Dayton, OH 45435, USA

organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Following a synthesis of various definitions found in industry and academia, Schatz et al. (2017) described cybersecurity as the guidelines, policies, and collections of safeguards, technologies, tools, and training to protect the confidentiality, integrity, availability of data and assets used in cyberspace. It is the body of technologies, processes and practices designed to protect networks, computers, software and data from attack, damage or unauthorised access (Longley, 2019; Toch et al., 2018).

Considerable research has been done in the related areas of cybersecurity threats, breaches, and attacks. Cybersecurity threat refers to "the possibility of a malicious attempt to damage or disrupt a computer network or system" (Imran et al., 2018). It is an event that could result in breaches in information confidentiality, integrity, and availability, and result in damage to information systems resources. Distinguishing between external and internal threats, human, environmental and technological threats, malicious and non-malicious threats, and accidental and intentional threats, Jouini et al. (2014) portrayed threats such as destruction of information, corruption of information, theft, loss of information, illegal usage, disclosure of information, denial of use, and elevation of privilege. Gerić and Hutinski (2007) classified various threats such as privacy intrusion, loss of infrastructure support, and unauthorised access into broad categories: physical security, personnel security, communication and data security, and operational security. Cybersecurity breach is the "unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of confidentiality, integrity, and availability of the affected data" (Sen & Borle, 2015). Several methods such as malware, phishing, eavesdropping, sniffing, Trojans, denial-of-service attacks, and SQL injections may be used for breaches (Imran et al., 2018; Jang-Jaccard & Nepal, 2014). Cybersecurity attack may be viewed as "the materialization of a threat or the exploitation of a vulnerability" (Kumar et al., 2008). It is done with goals of stealing information, tracking user information, or taking control of a system, and includes hardware, network, or application attacks (Lala & Panda, 2001; Toch et al., 2018).

Prior research has proposed a variety of countermeasures that may feature in organisational cybersecurity response. Such responses by organisations are typically multi-faceted – they may include safeguards to prevent or reduce the likelihood of cybersecurity attacks, mechanisms to detect and contain cybersecurity attacks, and procedures to recover from cybersecurity disasters and reduce net losses (Paul & Wang, 2019; Sen & Borle, 2015). Cybersecurity response can be categorised as technical response and non-technical response (Kwon & Johnson, 2013).

Technical response may be viewed as IT-based solutions instituted within organisations to counter cybersecurity threats. These include firewalls, anti-virus software, anti-malware, encryption, network monitoring, safeguarding, auditing, virus detection, and intrusion detection systems to detect and counter cybersecurity threats (Chen et al., 2011; Kumar et al., 2008; Paté-Cornell et al., 2018). Countermeasures for specific aspects of the technological infrastructure may also be appropriate – for instance, hardware infrastructure may benefit from hardware watermarking and tamper-resistant hardware, software infrastructure may employ secure coding practices and code obfuscation, and network infrastructure may involve intrusion prevention and virtual private network (Jang-Jaccard & Nepal, 2014). IT-based solutions are largely automated, implemented on all computing devices, and strictly enforced within organisations, and users are expected to be in compliance.

Non-technical response refers to non-IT solutions developed by organisations to counter cybersecurity threats. These include continuous and relevant user training and education, with frequent bulletins containing new and relevant information, annual exercises, and examples of consequences due to cybersecurity breaches (Connolly & Wall, 2019; Gupta et al., 2018). Training programs have the potential to raise cybersecurity awareness among employees and equip them to identify threats and apply correct procedures to prevent breaches and take action for recovery. In addition, organisations may institute computer security and incident response teams, develop security policies for secure practices, and invest in cyber-insurance products (Ahmad et al., 2015; Connolly & Wall, 2019; Mukhopadhyay et al., 2013). Non-technical response also includes cybersecurity management processes (e.g., report third-party breaches) to support timely and effective response to cybersecurity incidents. Finally, organisations may strive to develop and institutionalise a cybersecurity culture, which could be instrumental in instilling cautious and attentive behaviours by users consistent with the internal security policies (Alshaikh, 2020; Da Veiga et al., 2020).

3. Research model

3.1. Cybersecurity response

Cybersecurity response refers to those organisational actions to prevent, monitor, detect, mitigate, and manage cybersecurity threats, and recover in the event of a cybersecurity breach (Longley, 2019; Somani et al., 2017). It includes actions or countermeasures for attack prevention, attack detection, and attack mitigation and recovery (Lezzi et al., 2018; Somani et al., 2017). Such countermeasures may limit physical access to IT infrastructure, block access over networks, or enable recovery from intrusion (Rees et al., 2011). Both IT and non-IT countermeasures targeting different aspects including software, hardware, data, and network as well as physical facilities, personnel, regulation, and risk transference may enable organisations to deter and prevent cybersecurity threats (Yeh & Chang, 2007). Therefore, this study examines technical and non-technical cybersecurity response in addition to the overall cybersecurity response.

3.2. Cybersecurity threats

Based on prior literature, the research model includes four types of threats – physical, personnel, communication and data, and operational – that can intrude organisations.

Physical threats refer to potential intrusions or lapses in the physical infrastructure related to information resources within the organisation (Gerić & Hutinski, 2007). These threats include insufficient or nonexistent protection on wires and communication cables that may enable wiretaps and eavesdropping; degradation of infrastructure and software services resulting from natural disasters, physical assault, or malfunctions; and garbage digging of unwanted and discarded resources such as unerased media and non-shredded paper (Gerić & Hutinski, 2007; Grobauer et al., 2010; Rees et al., 2011). Potential responses to handle physical threats include properly securing physical locations, responsibly disposing media and paper with sensitive data, building redundancies to recover from losses due to natural disasters, and training individuals to follow protocols for securing infrastructure and resources.

Personnel threats describe potential intrusions or lapses in handling, training, or monitoring personnel dealing with information resources (Gerić & Hutinski, 2007). These threats include individuals attempting to guess passwords for other users; masquerading as others with false identities; manipulating to gain access to useful information such as user names and passwords; extorting others to gain access to restricted and classified information; and illegally copying software for personal uses (Gerić & Hutinski, 2007; Jouini et al., 2014; Yeh & Chang, 2007). Potential responses for handling personnel threats include awareness campaigns that inform users about illegal use, policies, and cybercrime; training programs on password security, coping mechanisms, and responsible use; and monitoring users for erratic behaviours, deviations, and non-compliance.

Communication and data threats represent potential intrusions or lapses in deploying, administering, and monitoring the infrastructure relating to communication and data (Gerić & Hutinski, 2007). These include attacks on data that compromise confidentiality, integrity, and availability; attacks on software through malicious software such as computer viruses, worms, Trojan horses, and back doors; and attacks on computer networks using denial of service or distributed denial of service (Gerić & Hutinski, 2007; Imran et al., 2018; Jang-Jaccard & Nepal, 2014; McLeod & Dolezel, 2018). Potential responses for dealing with communication and data threats include various technical solutions such as secure firewalls, network infrastructure security, network traffic monitoring, antivirus software, anti-malware tools, and anti-phishing software. Organisations may also develop plans for recovering from denial-of-service attacks, and training programs for users to quickly respond from such attacks.

Operational threats refer to potential intrusions or lapses in planning, deploying, and monitoring protocols for operations that support information resources (Gerić & Hutinski, 2007). These include changing data fraudulently and without authorisation; spoofing by exploiting weaknesses in the Internet and communication infrastructure to obtain data; sniffing network traffic by examining packets for sensitive data such as user names and passwords; searching the network systems using malicious software to obtain data for unauthorised activities; and misusing privileged access typically available for administrators and restricted users (Gerić & Hutinski, 2007; Jang-Jaccard & Nepal, 2014; Paoli et al., 2018). Potential responses to operational threats include establishing authentication and authorisation protocols for users, using advanced encryption methods for data and network communication, applying secure network protocols, examining system logs for violations in access to resources, and ensuring users are trained to recognise phishing and spoofing campaigns.

3.3. Control variables

The research model also contains three control variables. First, a variable to represent the headquarters location of the organisations was included in the research model. Due to the climate for innovation in the Eastern and Western coasts, organisations in those regions are more likely to engage with advances in cybersecurity and incorporate them in their everyday practices. Second, a variable to represent whether the organisation dealt with business-to-consumer (B2C) commerce was also included. Since B2C organisations interact with and facilitate transactions by customers, they are likely to attribute greater importance to cybersecurity infrastructures. Third, a variable to differentiate between information-intensive organisations and others was used in the research model. Information-intensive organisations typically belong to the IT, finance, and healthcare sectors, which rely largely on information products that have to be managed, shared, and protected – which would place greater emphasis on cybersecurity responses. Fourth, a variable to distinguish between organisations that have previously experienced security breaches from others was included. This is because organisations that have encountered cybersecurity breaches may be more inclined to place greater emphasis on cybersecurity responses. Finally, slack resources were included as a control variable since organisations with access to such resources may experiment with various cybersecurity responses and engage with it differently than others.

4. Research methods

Text mining and statistical analysis techniques were employed for data collection, data cleansing and preparation, topic modelling, and data analysis. The major steps in our research methodology are shown in Figure 1.

4.1. Sample

Organisations listed in the Standard & Poor's 100 (i.e., S&P-100) rankings were considered for the study. The rankings in each year from 2014 to 2018 were used to identify those organisations that had been listed over a period of time. Our sample included 87 organisations that had been listed between those years. Appendix A lists the organisations in our sample.

4.2. Data sources

Multiple data sources were employed in this research. To compute the weights for the four cybersecurity threats and the cybersecurity response through topic modelling, the annual 10-K reports of the organisations were obtained from the Edgar database[1] available through the Securities and Exchange Commission (SEC). The EdgarWebR package[2] in R was utilised to download the 10-K reports.[3] These 10-K reports were deemed appropriate data sources for this research since the SEC had issued guidance for cybersecurity disclosures, including specific requirements for such disclosures under risk discussion on the 10-K reports (Ising & Acree, 2011). Accordingly, textual data provided in Item 1 (business overview) and Item 1A (risk factors) were extracted from the 10-K reports for obtaining weights through topic modelling. Data for the NAICS code (industry classification) and debt-to-equity ratio (slack resources) for each organisation were obtained from the *Compustat* database. The number of cybersecurity breaches for each organisation was obtained from the Privacy Rights Clearinghouse website,[4] which has served as the main source of information in cybersecurity research in recent years (Angst et al., 2017; Sen & Borle, 2015).

4.3. Data preparation

The textual data from the 10-K reports were prepared for topic modelling and analysis. A list of keywords representing cybersecurity responses and threats was compiled based on prior literature and industry reports and input into the text parser. Table 1 shows the keywords used in the text analysis. These keywords

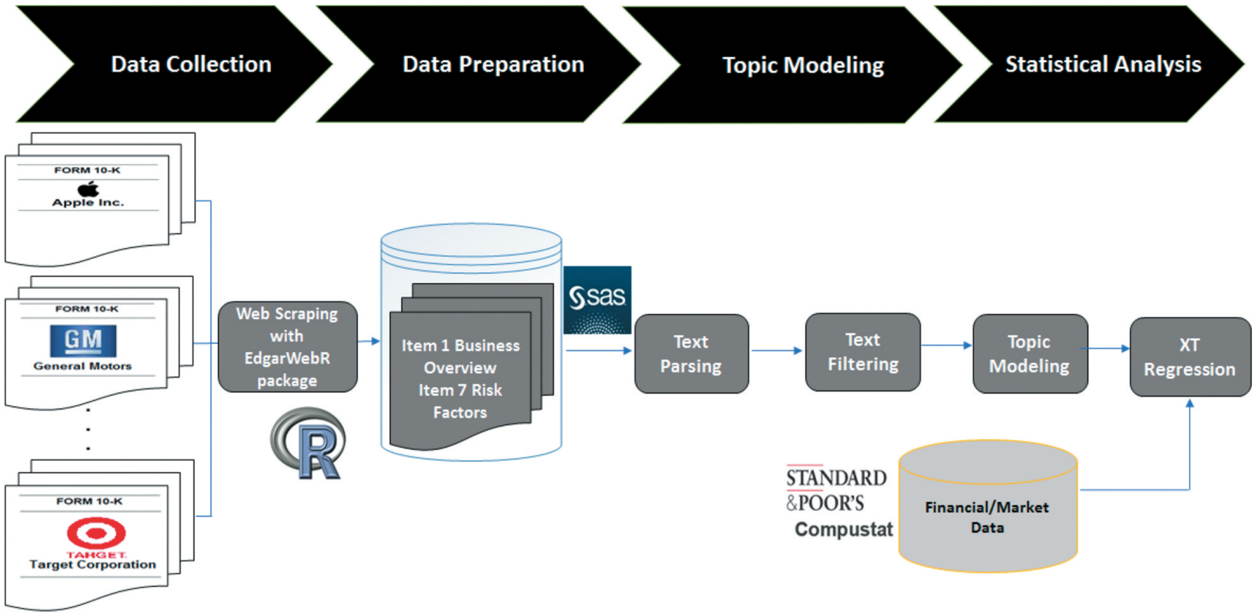

Figure 1. Research methodology.

Table 1. Keywords for textual analysis.

Variable	Keywords
Cybersecurity response	*General*: cybersecurity, cyber security, cyber, security, cloud, sensitive data, sensitive information, sensitive personal information, confidential information, confidential data, personal data, proprietary data, proprietary information, forensics *Technical*: access control, antivirus, audit trail, authentication, authorisation, cryptography, firewall, intrusion detection, scanner, secure gateway, surveillance, two-factor identification, multifactor authentication, encryption, single sign on, disk striping, data encryption, disk mirroring, masking, backup, payment card industry data security standard, PCI DSS, system and organisation controls report, SOC, cloud controls matrix, CSA CCM, identity and access management, auditors, federated identity management, screen scraper, warm site, cold site, hot site, eavesdropping *Non-technical*: chief information security officer, chief security officer, CISO, CSO, security training, regulations, policies, programs, plans, trainings, business continuity, disaster recovery, security controls, evaluation, testing, monitoring, updating, reporting, assessment, audits, alerting, logging, detecting, intellectual property protection, compliance, auditability, traceability, accountability, network security, privacy liability, cyber liability, regulatory
Physical threats	assault, assets, backup, buildings, cable, contaminants, death, disaster, ear tapping, equipment, facility, fire, garbage, humidity, infrastructure, injury, malfunction, natural disaster, physical damage, power interruption, rooms, trash, trash digging, unerased data, unshredded document, unshredded paper, weather, wire, outage, malfunction, earthquake
Personnel threats	alter, blackmail, email, espionage, extortion, false identity, hijack, keystroke logging, malicious insiders, manipulations, masquerading, password, password guessing, phishing, piracy, privacy, ransomware, social engineering, steal, username, e-privacy
Communication and data threats	availability, backdoor, bomb, botnet, confidentiality, data availability, data confidentiality, data integrity, DDOS, Denial of Service, destruction of data, distributed denial of service, DOS, hoax, integrity, loss of data, malware, sabotage, Trojan, Trojan horse, virus, worm, man in the middle
Operational threats	authorise, authorised access, authorised use, cracking, crime, data fraud, errors, fraud, hacker, hacking, increased access, obsolete, omission, outdated, privileged access, rootkit, sniffing, spoofing, spyware, tampering, unauthorised access, wiretapping, unauthorised use, unauthorised person, unauthorised release, unauthorised disclosure, unauthorised, misuse, malicious code, malicious software, disruptive software

were used in topic modelling (described later) to compute the weights for cybersecurity response and cybersecurity threats for each organisation. Appendix B contains examples of snippets of cybersecurity response found in 10-K reports.

Natural language processing (NLP) algorithms for parsing, tokenisation, stemming, synonyms, and parts of speech were used to transform the 10-K documents into a single document-term matrix (DTM). The n-gram algorithm was employed to detect and capture multi-term phrases. To make the approximate matching efficient, the term table was reviewed to consolidate abbreviations, words, and phrases that were synonyms to each other. This process reduced the size of the DTM semantically and provided a consistent representation of the data extracted from multiple 10-K reports. The resultant DTM contained the frequency of terms from 10-K reports.

A term weighting function was then applied to the DTM to evaluate the importance of terms or phrases within a specific 10-K reports and how they are distributed across all 10-K reports in the corpus. Evangelopoulos et al. (2012) argued that, among the several weighting methods that can be used for information retrieval and text mining, the entropy method may be appropriate for short text documents whereas the term frequency–inverse document frequency (TF-IDF) method may be better suited for a large collection of documents. Thus, the TF-IDF method was used to assign weights to terms, computed as: $w_i = \log_2\left(\frac{1}{P(t_i)}\right) + 1$, in which the TF–IDF weights were proportional to the frequency with which terms occurred in individual documents, but were adjusted by the frequency with which the terms appeared across all documents. This process yielded a weighted term-document frequency matrix (TDFM), in which the stop words and frequently-used terms received smaller weights and were subject to filtering. To ensure none of the keywords for cybersecurity threats and responses were filtered out, they were manually selected to remain in the final TDFM.

4.4. Topic modelling

Using the predefined keywords for cybersecurity response (and technical response and non-technical response) and cybersecurity threats, the document topic weight for each 10-K report was calculated in order to measure the strength of association of a 10-K document to the pre-defined topics. Different techniques such as Latent Dirichlet Allocation (LDA) and Latent Semantic Indexing (LSI) may be used for topic modelling, with its pros and cons. While LDA entails greater mathematical complexity, its practical use may be limited (e.g., Evangelopoulos et al., 2012); however, a properly-tuned LSI produces better results than LDA with fewer features for tuning (e.g., Gefen et al., 2017). In this study, the LSI topic modelling technique was applied to the weighted TDFM to determine how the 10-K documents were related to cyber security response. This was accomplished using Singular Value Decomposition (SVD) to decompose the weighted TDM into a dense but reduced dimensional representation. All terms representing cybersecurity response were combined to form the cybersecurity topic which emerged as a SVD dimension in the SVD dimensional transformation. The term topic weight was calculated for each term, which was the coordinate of the term in the SVD dimension. The document topic weight of a 10-K report towards cybersecurity response was computed as the normalised sum of TF–IDF weightings for each term in the document multiplied by their term topic weights. Thus, topic modelling yielded seven separate weights for each 10-K report (i.e., organisation) – three weights represented the overall response, technical response, and non-technical cybersecurity response, and the others for four types of cybersecurity threats.

4.5. Measures

The measures for the study variables are shown in Table 2. For the dependent variable (cybersecurity response, and its categories, technical response and non-technical response) and the independent variables (i.e., the four cybersecurity threats), the data was obtained through topic modelling algorithms. The coast headquarters (HQ) location was coded as 1 if the company had its headquarters located in a Western or an Eastern state of the United States. The B2C variable was based on whether the organisation dealt directly with customer transactions through an online web site. To model information-intensive organisations, the industry sector for the organisation based on the North American Industry Classification System (NAICS) was used – specifically, the organisations competing in the IT, finance, and healthcare sectors were coded for this variable. A categorical variable as coded to represent whether the organisation had previously encountered cybersecurity breaches. The debt to equity ratio was used to represent slack resources. Data for the response variable, the four threats, and slack resources were obtained for each year from 2014 to 2018.

4.6. XT regression

Data were analysed using the XT regression methods using Stata 15. Both time-varying data (i.e., the response, the four threats, and slack resources) and time-invariant data (for the control variables) were used. The conversion from wide-form (i.e., one row for each organisation) to long-form (i.e., one row for each time period for each organisation) data yielded a balanced short panel (i.e., many organisations, few time periods), which was used in XT regression analysis. The sample size for our balanced panel is 435 (i.e., 87 organisations for 5 years); however, data on slack resources was not available for all organisations in all years. Multiple models with different combinations of independent variables and control variables were tested. The dependent variable was cybersecurity response for the main models, and technical response and non-technical response for the additional models. All regression models were examined using the random-effects option.

5. Results

The results of the main XT regression models are shown in Table 3. Model (1) refers to the regression model with both the time-invariant and time-varying control variables. Model (2) represents the regression model that also includes the period effects, represented by categorical variables for each period excluding 2014 (which serves as the base). Model (3) also includes the four threats to Model (1) while Model (4) also includes the four threats to Model (2) – these models show the effects of the cybersecurity threats without and with period effects.

Model (1) explained 11.5% of the overall variance in cybersecurity response. Cybersecurity response of information-intensive organisations was higher compared to other organisations. The other control variables including slack resources were non-significant. Model (2) explained 13.1% of the overall variance in cybersecurity response. Cybersecurity response was higher for information-intensive organisations and marginally higher for organisations with headquarters in the coastal regions of United States than other organisations. The variables representing the period effects, except for year 2015, were significant. These effects show that cybersecurity response was higher in each period relative to 2014 (except for 2015, which was not significantly different from 2014). Model (3) explained 32.7% of the overall variance in cybersecurity response. Organisations headquartered in the coastal regions of the United

Table 2. Study variables.

Variable	Operationalization
Cybersecurity Response	Weight for cybersecurity response (including technical and non-technical response) extracted from the organisation's annual report, for each year from 2014–2018
Physical Threats	Weight for physical cybersecurity threats extracted from the organisation's annual report, for each year from 2014–2018
Personnel threats	Weight for personnel cybersecurity threats extracted from the organisation's annual report, for each year from 2014–2018
Communication and Data Threats	Weight for communication and data cybersecurity threats extracted from the organisation's annual report, for each year from 2014–2018
Operational Threats	Weight for operational cybersecurity threats extracted from the organisation's annual report, for each year from 2014–2018
Coast HQ [=1]	Time-invariant categorical variable representing if organisation headquarters (HQ) was located in the Western or Eastern coast of the United States
B2C organisation [=1]	Tim-invariant categorical variable representing if organisation dealt with business-to-consumer (B2C) transactions directly with customers
Info intensive org [= 1]	Time-invariant categorical variable representing if organisation competed in the IT, finance, or healthcare sectors
Prior breach [=1]	Time-invariant categorical variable representing if organisation experienced prior cybersecurity breach
Slack Resources	Debt to Equity Ratio for organisation extracted from Compustat, for each year from 2014–2018

Table 3. Results of the main XT regression models.

Variable	Model (1)	Model (2)	Model (3)	Model (4)
Coast HQ [=1]	0.02 (1.79)	0.02 (1.74*)	0.02 (1.93*)	0.02 (1.95*)
B2C org [=1]	0.01 (0.37)	0.01 (0.36)	−0.01 (−0.91)	−0.01 (−0.70)
Info intensive org [=1]	0.33 (2.40**)	0.03 (2.40**)	0.02 (1.63)	0.02 (1.71*)
Prior breach [=1]	−0.00 (−0.17)	−0.00 (−0.16)	−0.01 (−0.48)	−0.01 (−0.45)
Slack resources	−0.00 (−0.09)	−0.00 (−0.43)	0.00 (0.02)	−0.00 (−0.28)
Year 2018		0.02 (4.81***)		0.01 (3.14***)
Year 2017		0.02 (3.56***)		0.01 (2.18**)
Year 2016		0.01 (2.47**)		0.01 (1.76*)
Year 2015		−0.00 (−0.50)		−0.00 (−0.63)
Physical threats			0.26 (4.43***)	0.21 (3.57***)
Personnel threats			0.26 (3.15***)	0.18 (2.20**)
Communication and data threats			0.32 (2.52**)	0.34 (2.75***)
Operational threats			0.25 (3.03***)	0.22 (2.80***)
N	423	423	423	423
Within R^2	0.001	0.110	0.144	0.193
Between R^2	0.138	0.138	0.360	0.352
Overall R^2	0.115	0.131	0.327	0.325
Wald X^2 (df)	12.86** (5)	53.95*** (9)	99.52*** (9)	120.29*** (13)

Dependent variable: Cybersecurity response
Each cell contains the b-coefficient and the t-statistic in parentheses
***p < 0.01, **p < 0.05, *p < 0.10

States had a marginally higher cybersecurity response compared to other organisations. The remaining control variables and slack resources were non-significant. All four types of cybersecurity threats exerted significant effects on cybersecurity response. Model (4) explained 32.5% of the overall variance in cybersecurity response, with similar period effects as in Model (2) except for 2016. Cybersecurity response for information-intensive organisations and those headquartered in coastal regions of the United States showed marginally higher effects relative to others.

The results of the additional XT regression models involving technical response and non-technical response are shown in Table 4. Models (5) and (7) included the control variables and the four types of cybersecurity threats while Models (6) and (8) also include the period effects. The dependent variable was technical response in Models (5) and (6) and non-technical response in Models (7) and (8).

Model (5) explained 31.8% of the variance in technical response. The technical response of information-intensive organisations was higher relative to other organisations. The other control variables and slack resources were non-significant. Among the cybersecurity threats, all threats except communication and data threats had significant effects on the technical response of organisations. Model (6), which added the period effects to Model (5), explained 31% of the variance in technical response. The results for control variables were similar to Model (5). The variables for the period effects were significant in 2018 and 2017, marginally significant in 2016, and not significant in 2015 relative to 2014. Physical threats and operational threats influenced technical response but the other two types of threats were non-significant. Model (7) explained 29.2% of the variance in non-technical

Table 4. Results of the additional XT regression models.

Variable	Model (5)	Model (6)	Model (7)	Model (8)
Coast HQ [=1]	0.03 (2.57***)	0.03 (2.65***)	0.02 (1.57)	0.02 (1.59)
B2C org [=1]	−0.01 (−1.05)	−0.01 (−0.87)	−0.01 (−0.79)	−0.01 (−0.58)
Info intensive org [=1]	−0.00 (−0.37)	−0.00 (−0.30)	0.02 (1.77*)	0.02 (1.84*)
Prior breach [=1]	−0.00 (−0.05)	−0.00 (−0.03)	−0.01 (−0.91)	−0.01 (−0.89)
Slack resources	0.00 (0.85)	0.00 (0.54)	−0.00 (−0.46)	−0.00 (−0.75)
Year 2018		0.01 (3.44***)		0.01 (2.99***)
Year 2017		0.01 (2.10**)		0.01 (2.08**)
Year 2016		0.01 (1.87*)		0.00 (1.31)
Year 2015		−0.00 (−0.28)		−0.02 (−0.61)
Physical threats	0.21 (4.38***)	0.18 (3.58***)	0.17 (3.06***)	0.12 (2.28**)
Personnel threats	0.17 (2.56**)	0.11 (1.60)	0.17 (2.34***)	0.11 (1.40)
Communication and data threats	0.13 (1.27)	0.15 (1.47)	0.38 (3.31***)	0.40 (3.56***)
Operational threats	0.27 (4.05***)	0.25 (3.86***)	0.23 (3.10***)	0.21 (2.87***)
N	423	423	423	423
Within R^2	0.124	0.178	0.125	0.170
Between R^2	0.348	0.332	0.327	0.318
Overall R^2	0.318	0.310	0.292	0.291
Wald X^2 (df)	87.38*** (9)	109.03*** (13)	99.52*** (9)	103.39** (13)

Dependent variable: Technical response (Models 5 and 6) and Non-technical response (Models 7 and 8)
Each cell contains the b-coefficient and the t-statistic in parentheses
***p < 0.01, **p < 0.05, *p < 0.10

response. The non-technical response of information-intensive organisations had marginally higher effects compared to others. The remaining control variables and slack resources were non-significant. All four cybersecurity threats showed significant effects on the non-technical response of organisations. Model (8), which added the period effects to Model (7), explained 29.1% of the variance in non-technical response. The results were similar to Model (7) for both control variables and slack resources. The variables for the period effects showed significant effects in 2018 and 2017 and non-significant effects in 2016 and 2015 relative to 2014. All types of cybersecurity threats except personnel threats showed significant effects on the non-technical response.

6. Discussion

6.1. Findings

This research was aimed at understanding the relationship between cybersecurity threats and cybersecurity response by organisations. The details about the cybersecurity threats and responses were extracted from the textual data on the 10-K reports published by organisations and subjected to topic modelling. The topic modelling results were used in a XT regression analysis to determine the impact of threats on cybersecurity response. Based on the results of Models (3) through (8), the control variables generally exerted non-significant or marginally significant effects on cybersecurity response, except for the significant effect on technical response for organisations headquartered in the coastal regions of the United States. Based on Models (4), (6), and (8), the period effects were significant in the near term (i.e., 2018 and 2017), marginally significant or non-significant in the longer-term (i.e., 2016 and 2015). Table 5 depicts the results of cybersecurity threats as seen in Models (3) through (8).

Physical threats, communication and data threats, operational threats, and personnel threats exerted significant positive effects on the overall cybersecurity response of organisations, based on Models (3) and (4). The effects of cybersecurity threats in Model (3) are consistent in Model (4) after allowing for period effects. These results indicate that organisations may routinely monitor and manage their cybersecurity responses to handle different types of threats, which can be expected. Since physical threats are generally related to the infrastructure (e.g., power supply, buildings), hazards (e.g., damage by water and fire, natural disasters), and security (e.g., securing dumpsters, shredding paper), organisations may enact contingent plans for protection against or recovery from physical threats. Resources may be allocated to handle other contingencies due to disasters. For instance, multiple data centres may be set up in different locations to spread the risk of threats and to achieve redundancies in the event of data loss from disasters (Van Cleeff et al., 2011). This could be attributed to cloud-based infrastructures with a shared responsibility model[5] where physical security, host infrastructure, and network controls are the responsibility of the cloud service provider (Shahzad, 2014). Personnel threats due to illegal use, policy violations, and improper safeguards may be addressed through training programs and awareness campaigns on cybersecurity to inform and train users to minimise threats and hazards. Communication and data threats such as malicious software, unauthorised access, denial-of-service attacks, and cracking/hacking may be handled using a combination of tools. Considering the extent to which organisational activities are conducted online using Internet-based applications, and the potential for attacks and breaches using various means such as viruses, worms, malware, botnets, and Trojans is high, several tools such as firewalls, antivirus software, and anti-malware systems may be routinely implemented by organisations. Operational threats such as unauthorised access, malicious software, and cracking/hacking may be countered using authorisation mechanism and protections against intrusion.

The analysis based on technical response and non-technical response revealed additional insights. Model (6) shows that physical threats and operational threats had significant effects on technical response while communication and data threats and personnel threats remained non-significant. Model (8) indicates that physical threats, communication and data threats, and operational threats influenced non-technical response whereas personnel threats were not significant. These results suggest that physical threats and operational threats were handled using a combination of both technical response and non-technical response whereas communication and data threats were addressed using non-technical response. A combination of technical and non-

Table 5. Summary of findings.

Threats	Cybersecurity response		Technical response		Non-technical response	
	Model (3)	Model (4)	Model (5)	Model (6)	Model (7)	Model (8)
Physical threats	***	***	***	***	***	***
Personnel threats	***	***	**	n.s.	***	n.s.
Communication and data threats	***	***	n.s.	n.s.	***	***
Operational threats	***	***	***	***	***	***

Models (4), (6), and (8) include period effects
***p < 0.01, **p < 0.05, *p < 0.10, n.s.: non-significant

technical response seems intuitive for handling physical threats and operational threats. For instance, organisations may employ two-factor identification (technical response) and user training (non-technical response) to guard against the operational threat of unauthorised access, and data backup and (technical response) and disaster recovery plan (non-technical response) to recover from the physical threat of natural disasters. Such a combination of technical and non-technical response could also be expected for communication and data threats – e.g., anti-virus and anti-malware software (technical response) and user training (non-technical response) could be used to guard against viruses and worms. But results involving communication and data threats influenced non-technical response only, which seems counter-intuitive. This could be attributed in part to the taken-for-granted reality of technical responses in organisations (e.g., the anti-virus software is installed and active on all computing devices) and the need to routinely educate users on the potential cybersecurity dangers, strategies to recognise potential attacks, and recovery mechanisms in the event of breaches.

Personnel threats were significant in Models (5) and (7) when period effects were not included, but became non-significant in Models (6) and (8) when period effects were included. Personnel threats in the forms of keystroke logging, phishing, and hijacking may require organisations to engage in considerable effort and expense to institute training programs, instal monitoring software, and increase cybersecurity awareness. Specific responses such as authentication (to prevent authorised access), access (to prevent theft), and encryption (to prevent sniffing) may be ongoing efforts within organisations to counter personnel threats. Therefore, the period effects may capture such ongoing efforts rendering personnel threats non-significant. Model (4) also showed that personnel threats influence overall cybersecurity response, even though Models (6) and (8) did not show significant effects for the technical and non-technical responses.

Collectively, findings show that cybersecurity responses by organisations are significantly influenced by the types of cybersecurity threats, after controlling for organisational differences, slack resources, prior security breaches, and different time periods. Findings also show that the cybersecurity responses differed by the types of cybersecurity threats, i.e., organisations did not engage in one-size-fits-all strategy in developing cybersecurity response portfolios. Specifically, organisations applied a combination of technical and non-technical solutions to handle different types of cybersecurity threats. Organisational responses to personnel threats were also largely ongoing efforts. These findings, based on industry-leading organisations featured on the S&P-100 rankings, can serve as useful references for organisations as they navigate challenges in the cybersecurity domain.

6.2. Limitations

The findings of the study should be interpreted in light of its limitations. First, the research utilised secondary data gathered from 10-K reports. While the 10-K reports may be considered as important documents put forth by the organisations to satisfy regulations (imposed by the SEC, for instance) and appeal to the shareholders, they could be biased in different ways. Also, the descriptions in the 10-K reports were not developed to answer specific questions related to cybersecurity. Further, the 10-K reports served as the data source for both threats and response, which could inflict bias; future research may incorporate other data sources for variables such as capital investments in cybersecurity. Second, the research applied topic modelling techniques on textual data that are heavily dependent on the specific algorithms. Since the assumptions and weighting methods underlying the various topic modelling algorithms can differ, the potential for bias exists. Third, the keywords developed to represent cybersecurity response and cybersecurity threats could be biased. Although care was taken in identifying the keywords and the lists were refined with discussions between the authors, it is nevertheless possible that alternate lists may be possible with further iterations. Moreover, it may be possible to develop more elaborate types of cybersecurity threats and cybersecurity response than shown in this study. Fourth, the sample used in this research includes organisations from the S&P-100 rankings, which is a set of large, industry-leading organisations. The findings of the study may not be generalisable to other populations although they can offer guidance for other organisations. Finally, due to the focus on the S&P-100 organisations, the sample size for the study may be considered low. Future studies could employ a larger sample from S&P-500 or Fortune 500 rankings.

6.3. Implications for research

This study offers several implications for research. First, the notion of cybersecurity response developed for this research serves as a useful way by which to gauge how organisations handle cybersecurity threats. It is one of the first attempts to examine organisational response and may serve to launch research efforts to gain deeper insights. However, it may be possible to develop other ways to characterise cybersecurity response, which could be a fruitful avenue for further research. Cybersecurity response was also examined using two subtypes: technical response and non-technical response, consistent with the notions of IT and non-IT responses to cybersecurity threats and attacks. While such a classification provided a finer analysis of cybersecurity threats and responses, a more accurate mapping of the types of threats to the types of response may yield more helpful guidance for organisations. Second, this research adopted the classification of threats into the physical, personnel, communication and data, and operational threats found in prior literature, and related them to cybersecurity response. Although such categories are expected to be mutually exclusive, and efforts were undertaken to ensure that the categories are not overlapping, it is possible that the categories are somewhat related to each other. For instance, “password guessing” is considered a personnel threat since an individual may engage in guessing the passwords of other users and attempt to gain unauthorised access to protected resources; however, it can be accomplished from remote locations using the Internet-based communication infrastructure. Further, there may be opportunities for a finer classification – for instance, communication and data threats may be separated into communication threats and data threats – which could result in deeper insights into threats on cybersecurity. Finally, the preliminary findings of this research based on textual analysis of archival data in 10-K reports may be further validated using primary data collection methods such as interviews, focus groups, and surveys. While the 10-K reports do provide cybersecurity-related information due to the SEC guidelines, it is possible that the information provided could be incomplete or insufficient for a conclusive understanding of cybersecurity. Future research can be carried out using other corporate filings with SEC such as 8-K form which may provide additional information on cybersecurity threats and organisational response. A larger data set can also be used to perform a longitudinal analysis and further verify the findings of the current study.

6.4. Implications for practice

The analysis on leading organisations ranked on the S&P-100 list shows that cybersecurity response was influenced by physical threats, personnel threats, communication and data threats, and operational threats. Several implications for practice can be drawn from the findings of this study. First, organisations may institute cybersecurity response to counter threats regardless of whether they have experienced prior breaches in cybersecurity or have access to slack resources, both of which did not influence cybersecurity response. Cybersecurity response should be an ongoing effort that includes mechanisms to monitor and prevent disasters and also recover from adverse events if the need arises. The importance of prioritising cybersecurity response cannot be understated since modern organisations are heavily reliant on their IT infrastructures for their operations. Second, organisations should institute cybersecurity response portfolios regardless of their industry or operations, since this study found no differences in cybersecurity response between organisations in information-intensive industries and others, or between organisations with B2C operations and others. While it may seem that organisations in information-intensive industries such as finance, healthcare, and IT, and organisations providing customer-facing B2C operations may be more prone to cybersecurity threats, and be more interested in instituting encryption and network protocols for safeguarding sensitive customer data, cybersecurity threats are a reality for all types of organisations. Finally, organisations should consider a combination of both technical response and non-technical response in their cybersecurity response portfolios. While cybersecurity portfolios are primarily driven by technical responses, e.g., extensive sets of software tools such as anti-malware, anti-virus software, firewalls, authentication/authorisation tools, and intrusion detection software, attention to non-technical responses such as user training programs, awareness campaigns, and disaster recovery programs gain considerable importance due to the diversity of cybersecurity threats faced by organisations. Organisational users have to be knowledgeable on and trained in potential threats such that they can prevent breaches or quickly take corrective actions to recover from actual breaches.

7. Conclusion

This study examined the relationship between cybersecurity threats and cybersecurity response, including technical response and non-technical response, within organisations. Textual data available in published annual 10-K reports of organisations were used to assess the cybersecurity threats and responses using topic modelling, the results of which were examined using XT regression models. Cybersecurity responses by organisations were influenced regardless of prior security breaches or access to slack resources. These findings offer preliminary evidence of the nature of cybersecurity threats and their relationships to cybersecurity response.

Notes

1. https://www.sec.gov/edgar/searchedgar/companysearch.html
2. https://cran.r-project.org/web/packages/edgarWebR/edgarWebR.pdf
3. The source code to batch download 10-Ks is available upon request.
4. https://privacyrights.org

5. https://aws.amazon.com/compliance/shared-responsibility-model/

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

Amir Zadeh http://orcid.org/0000-0002-3171-5629

References

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*(6), 717–723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*(2020), 102003. https://doi.org/10.1016/j.cose.2020.102003

Angst, C. M., Block, E. S., D'arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, *41*(3), 893–916. https://doi.org/10.25300/MISQ/2017/41.3.10

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448. https://doi.org/10.3233/JCS-2003-11308

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 69–104. https://doi.org/10.1080/10864415.2004.11044320

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly*, *35*(2), 397–422. https://doi.org/10.2307/23044049

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *87*. https://doi.org/10.1016/j.cose.2019.101568

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organizational information security culture—perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Evangelopoulos, N., Zhang, X., & Prybutok, V. R. (2012). Latent semantic analysis: Five methodological recommendations. *European Journal of Information Systems*, *21*(1), 70–86. https://doi.org/10.1057/ejis.2010.61

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74–83. https://doi.org/10.1108/09685220310468646

Gefen, D., Endicott, J. E., Fresneda, J. E., Miller, J., & Larsen, K. R. (2017). A guide to textual analysis with latent semantic analysis in R with annotated code: Studying online reviews and stack exchange community. *Communications of the Association for Information Systems*, *41*(21), 450–496. https://doi.org/10.17705/1CAIS.04121

Gerić, S., & Hutinski, Ž. (2007). Information system security threats classifications. *Journal of Information and Organizational Sciences*, *31*(1), 51–61. https://hrcak.srce.hr/21445

Glaser, A. (2019). *Another 540 million Facebook users' data has been exposed*. Slate. Retrieved March 10, 2020, from https://slate.com/technology/2019/04/facebook-data-breach-540-million-users-privacy.html

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404–410. https://doi.org/10.1016/j.im.2009.06.005

Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C., & Zhou, L. (2008). Cybersecurity, capital allocations and management control systems. *European Accounting Review*, *17*(2), 215–241. https://doi.org/10.1080/09638180701819972

Gressin, S. (2017). *The equifax data breach: What to do*. Federal Trade Commission. Retrieved March 10, 2019, from https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

Grobauer, B., Walloschek, T., & Stocker, E. (2010). Understanding cloud computing vulnerabilities. *IEEE Security & Privacy*, *9*(2), 50–57. https://doi.org/10.1109/MSP.2010.115

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z

Imran, M., Arif, T., & Shoab, M. (2018). A statistical and theoretical analysis of cyberthreats and its impact on industries. *International Journal of Scientific Research in Computer Science Applications and Management Studies*, *7*(5), 1–7.

Ising, E. A., & Acree, A. G. (2011). SEC issues guidance on cybersecurity disclosures. *Insights*, *25*(4), 34–37.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jenab, K., & Moslehpour, S. (2016). Cyber security management: A review. *Business Management Dynamics*, *5*(11), 16–39.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, *12*(1), 69–91. https://doi.org/10.2753/JEC1086-4415120103

Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems*, *25*(2), 241–279. https://doi.org/10.2753/MIS0742-1222250210

Kwon, J., & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry.

Journal of the American Medical Informatics Association, *20*(1), 44–51. https://doi.org/10.1136/amiajnl-2012-000906

Lala, C., & Panda, B. (2001). Evaluating damage from cyber attacks: A model and analysis. *IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans*, *31*(4), 300–310. https://doi.org/10.1109/3468.935047

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for industry 4.0 in the current literature: A reference framework. *Computers in Industry*, *103*, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

Longley, A. (2019). Understanding and managing cyber security threats and countermeasures in process industries. *Loss Prevention Bulletin*, *268*, 2–6.

Lyles, T. (2020). *Marriott discloses another security breach that may impact over 5 million guests*. The Verge. Retrieved March 10, 2020, from https://www.theverge.com/2020/4/1/21203313/marriott-database-security-breach-5-million-guests

McLaughlin, M., & Gogan, J. (2018). Challenges and best practices in information security management. *MIS Quarterly Executive*, *17*(3), 237–262. https://aisel.aisnet.org/misqe/vol17/iss3/6

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57–68. https://doi.org/10.1016/j.dss.2018.02.007

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk Decision Models: To insure IT or not? *Decision Support Systems*, *56*, 11–26. https://doi.org/10.1016/j.dss.2013.04.004

Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime Law Social Change*, *70*(4), 397–420. https://doi.org/10.1007/s10611-018-9774-y

Paté-Cornell, M., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis*, *38*(2), 226–241. https://doi.org/10.1111/risa.12844

Paul, J. A., & Wang, X. (2019). Socially optimal IT investment for cybersecurity. *Decision Support Systems*, *122*, 1–12. https://doi.org/10.1016/j.dss.2019.05.009

Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for cybersecurity risk planning. *Decision Support Systems*, *51*(3), 493–505. https://doi.org/10.1016/j.dss.2011.02.013

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 53–74. https://doi.org/10.15394/jdfsl.2017.1476

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314–341. https://doi.org/10.1080/07421222.2015.1063315

Shahzad, F. (2014). State-of-the-art survey on cloud computing security challenges, approaches and solutions. *Procedia Computer Science*, *37*, 357–362. https://doi.org/10.1016/j.procs.2014.08.053

Somani, G., Gaur, G. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future. *Computer Communications*, *107*, 30–48. https://doi.org/10.1016/j.comcom.2017.03.010

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, *33*(8), 544–557. https://doi.org/10.1109/TSE.2007.70712

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys*, *51*(2), Article 36, 1–27. https://doi.org/10.1145/3172869

van Cleeff, A., Pieters, W., Wieringa, R., & van Tiel, F. (2011). Integrated assessment and mitigation of physical and digital security threats: Case studies on virtualization. *Information Security Technical Report*, *16*(3–4), 142–149. https://doi.org/10.1016/j.istr.2011.08.003

Yeh, Q., & Chang, A. J. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management*, *44*(5), 480–491. https://doi.org/10.1016/j.im.2007.05.003

Appendix A. List of Organisations in Sample

Ticker	Company	Headquarters	GICS Sector
MMM	3 M Company	Minnesota	Industrials
ABT	Abbott Laboratories	Illinois	Health Care
ABBV	AbbVie Inc.	Illinois	Health Care
ACN	Accenture plc	Ireland	Information Technology
ALL	Allstate Corp	Illinois	Financials
GOOGL	Alphabet Inc	California	Communication Services
MO	Altria Group Inc	Virginia	Consumer Staples
AMZN	Amazon.com Inc.	Washington	Consumer Discretionary
AXP	American Express Co	New York	Financials
AIG	American International Group, Inc.	New York	Financials
AMGN	Amgen Inc.	California	Health Care
AAPL	Apple Inc.	California	Information Technology
T	AT&T Inc.	Texas	Communication Services
BAC	Bank of America Corp	North Carolina	Financials
BRK.B	Berkshire Hathaway	Nebraska	Financials
BIIB	Biogen Inc.	Massachusetts	Health Care
BA	Boeing Company	Illinois	Industrials
BMY	Bristol-Myers Squibb	New York	Health Care
COF	Capital One Financial	Virginia	Financials
CAT	Caterpillar Inc.	Illinois	Industrials
CVX	Chevron Corp.	California	Energy
CSCO	Cisco Systems	California	Information Technology
C	Citigroup Inc.	New York	Financials
KO	Coca-Cola Company (The)	Georgia	Consumer Staples
CL	Colgate-Palmolive	New York	Consumer Staples
CMCSA	Comcast Corp.	Pennsylvania	Communication Services
COP	ConocoPhillips	Texas	Energy
COST	Costco Wholesale Corp.	Washington	Consumer Staples
CVS	CVS Health	Rhode Island	Health Care
DWDP	DowDuPont	Michigan	Materials
EMR	Emerson Electric Company	Missouri	Industrials
EXC	Exelon Corp.	Illinois	Utilities
XOM	Exxon Mobil Corp.	Texas	Energy
FB	Facebook, Inc.	California	Communication Services
FDX	FedEx Corporation	Tennessee	Industrials
F	Ford Motor	Michigan	Consumer Discretionary
GD	General Dynamics	Virginia	Industrials
GE	General Electric	Massachusetts	Industrials
GM	General Motors	Michigan	Consumer Discretionary
GILD	Gilead Sciences	California	Health Care
GS	Goldman Sachs Group	New York	Financials
HAL	Halliburton Co.	Texas	Energy
HD	Home Depot	Georgia	Consumer Discretionary
HON	Honeywell Int'l Inc.	New Jersey	Industrials
INTC	Intel Corp.	California	Information Technology
IBM	International Business Machines	New York	Information Technology
JNJ	Johnson & Johnson	New Jersey	Health Care
JPM	JPMorgan Chase & Co.	New York	Financials
LLY	Lilly (Eli) & Co.	Indiana	Health Care
LMT	Lockheed Martin Corp.	Maryland	Industrials
LOW	Lowe's Cos.	North Carolina	Consumer Discretionary
MA	Mastercard Inc.	New York	Information Technology
MCD	McDonald's Corp.	Illinois	Consumer Discretionary
MDT	Medtronic plc	Ireland	Health Care
MRK	Merck & Co.	New Jersey	Health Care
MET	MetLife Inc.	New York	Financials
MSFT	Microsoft Corp.	Washington	Information Technology
MDLZ	Mondelez International	Illinois	Consumer Staples
MS	Morgan Stanley	New York	Financials
NKE	Nike	Oregon	Consumer Discretionary
OXY	Occidental Petroleum	California	Energy
ORCL	Oracle Corp.	California	Information Technology
PEP	PepsiCo Inc.	New York	Consumer Staples
PFE	Pfizer Inc.	New York	Health Care
PM	Philip Morris International	New York	Consumer Staples
PG	Procter & Gamble	Ohio	Consumer Staples
QCOM	QUALCOMM Inc.	California	Information Technology
RTN	Raytheon Co.	Massachusetts	Industrials
SLB	Schlumberger Ltd.	Netherlands	Energy
SPG	Simon Property Group Inc	Indiana	Real Estate
SO	Southern Co.	Georgia	Utilities
SBUX	Starbucks Corp.	Washington	Consumer Discretionary
TGT	Target Corp.	Minnesota	Consumer Discretionary
TXN	Texas Instruments	Texas	Information Technology
BK	The Bank of New York Mellon Corp.	New York	Financials
DIS	The Walt Disney Company	California	Communication Services
FOXA	Twenty-First Century Fox	New York	Communication Services
USB	U.S. Bancorp	Minnesota	Financials
UNP	Union Pacific	Nebraska	Industrials
UNH	United Health Group Inc.	Minnesota	Health Care
UPS	United Parcel Service	Georgia	Industrials
UTX	United Technologies	Connecticut	Industrials
VZ	Verizon Communications	New York	Communication Services
V	Visa Inc.	California	Information Technology
WBA	Walgreens Boots Alliance	Illinois	Consumer Staples
WMT	Walmart	Arkansas	Consumer Staples
WFC	Wells Fargo	California	Financials

Appendix B. Illustrative Text from 10-K Reports for Cybersecurity Response

Organisation	Snippet from 10-K Report	Term	Term Weight	Topic Relevance
PEP	We continue to devote significant resources to network security, backup and disaster recovery, and other security measures, including training, to protect our systems and data, but these security measures cannot provide absolute security or guarantee that we will be successful in preventing or responding to every such breach or disruption.	network security	1.515	0.104
HON	We seek to deploy comprehensive measures to deter, prevent, detect, respond to and mitigate these threats, including identity and access controls, data protection, vulnerability assessments, product software designs which we believe are less susceptible to cyberattacks, continuous monitoring of our IT networks and systems and maintenance of backup and protective systems.	access control	0.87	0.75
MO	Our safeguards include employee training, testing and auditing protocols, backup systems and business continuity plans, maintenance of security policies and procedures, monitoring of networks and systems, and third-party risk management.	backup	1.97	0.51
GS	Financial institutions regulated by the NYDFS require (i) establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of their information systems; (ii) implement and maintain a written cyber security policy setting forth policies and procedures for the protection of their information systems and non-public information; and (iii) designate a Chief Information Security Officer.	CISO	0.83	0.865
V	We are investing in more proactive malware and threat identification to help stop fraud and data loss before it occurs.	identification	1.00	0.2
MDLZ	We continue to devote focused resources to network security, backup and disaster recovery, enhanced training and other security measures to protect our systems and data; we are also in the process of enhancing the monitoring and detection of threats in our environment.	disaster recovery	1.348	0.667
AAPL	The company has implemented systems and processes intended to secure its information technology systems and prevent unauthorised access to or loss of sensitive data, including through the use of data encryption and authentication technologies.	encryption	1.447	0.666
PG	We assess potential threats and vulnerabilities and make investments seeking to address them, including ongoing monitoring and updating of networks and systems, increasing specialised information security skills, deploying employee security training, and updating security policies for the Company and its third-party providers.	security training	1.479	0.571
AMGN	We continue to monitor adverse events and product complaints reported following the use of our products through routine post-marketing surveillance and studies when applicable.	surveillance	1.00	0.1
LMT	Our enterprise risk management program includes intrusion detection and cyber security mitigation plans, and our disclosure controls and procedures address cyber security and include elements intended to ensure that there is an analysis of potential disclosure obligations arising from security breaches.	intrusion detection	1.21	0.545
MO	Our safeguards include employee training, testing and audit trail protocols, backup systems and business continuity plans, maintenance of security policies and procedures, monitoring of networks and systems, and third-party risk management.	audit trail	0.76	0.98
V	We are also advancing the adoption of multi-factor authentication as a more secure alternative to passwords, which can be guessed or stolen.	multi-factor		
	authentication	1.11	0.9	