Statistical Investigation into the Relationship between Cyber-Attacks and the Type of Business Sectors

Andreea Bendovschi
Bucharest University of Economics
Bucharest, Romania
Piata Romana nr. 6, Bucuresti, 010374
Romania

Ameer Al-Nemrat
University of East London
University Way, London E16 3RD
United Kingdom

Bogdan Stefan Ionescu
Bucharest University of Economics
Bucharest, Romania
Piata Romana nr. 6, Bucuresti, 010374
Romania

Abstract

The concept of cyber-security increases in priority among companies and organisations of all sizes or business sectors. As cyber-attacks are continuously developing, security officers struggle to sustain an acceptable control over the entity's systems, data and underlying infrastructure, being restricted by time, budget and resources. The present paper performs an analysis covering various industries, aiming to identify patterns and correlations in terms of attacks and the respective sector. The results could be considered as insights that might help directing the limited budget and resources towards the right risks and mitigating controls, thus preventing attacks most likely to target certain industries.

Keywords: Cyber-attacks, information security, statistical analysis, logistic regression.

1. Introduction

Although cyber-attacks are continuously developing, the general level of awareness and understanding of the various threats posed by cyber-space to its users is extremely low [14]. Given the permanent increase in the use of internet services, this consideration becomes even more dangerous to individuals and organisations, allowing the number of deployed attacks to reach incredible values. A study performed by PriceWaterhouseCoopers in 2015 estimates the number of world-wide attacks at a rate of over 117,000 per day [8].

On the same note, McAfee Labs forecasts that by 2019 over 50 billion devices will be connected to the internet [7], thus offering hackers a wide variety of attacking opportunities.

Several definitions have been given to the cyber-attacks, including by the U.S. National Academy of Sciences, which defines the concept as *"deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks"*[13]. More specifically, the term targeted cyber-attack refers to *"a class of dedicated attacks that aim at a specific user, company, or organization to gain access to the critical data in a stealthy manner"*, while broad-based attacks are random, and usually target large groups of users instead of a preliminary selected individual/company/organization.[13] A joint study performed by CERT-UK and GCHQ Organisations in 2015 (*Common Cyber-Attacks: Reducing the impact)* outlines that most cyber-attacks follow the same approach, survey, deliver, breach, affect. [4]

In terms of root-cause, attackers are often not the only ones to blame for the success of the attack. Unaware people, faulty processes and technology vulnerabilities usually play an important part in collecting useful information, preparing and deploying the attack. In 2013, Cenzic company has detected one or more major security vulnerabilities in 96% of the analysed applications, according to *2014 Application Vulnerability Trends Report*, with a median of 14 vulnerabilities per application [3].

1. Literature review

The technological evolution offers new practices and solutions, enabling companies' process improvement but also brings along new challenges that entities need to understand and address. [2, 15] The international literature offers useful information that allows understanding cyber-attacks. Scott J. Shackelford, 2014, outlines the two main drivers enabling cybercrime to develop: on one hand, the vulnerability of systems, networks, processes and humans that govern the information management; on the other hand, the international laws supporting the safe use of information technology often proves to be "ambiguous and nonbinding". [11] Cyber-security has not only become a hot subject to the world wide researchers and professionals, but also became a matter of national importance. By 2013, more than 50 states had published official strategic information on cyber-crime and cyber-security. [5] The international literature further splits into addressing various types of cyber-attacks, depending on their final purpose. Thus, concepts like cyber-crime, cyber-espionage, cyber-terrorism, and cyber-war have been analysed in detail. [1, 6, 10, 12, 18]

Wang and Liu designed a model for simulating various attack scenarios and defences in order to quantify and compare potential attack cost, impact and gain in an objective way. [16] Although there are numerous authors that have addressed the ways in which companies can improve their security, they all agree on the fact that "absolute security" is a utopia. [12, 18, 9] Though general best practices can easily be adopted by all entities, regardless of their business sector [17], authors have not identified any study trying to identify correlations between cyber-attacks' characteristics and the business sector the targeted entity operates into, thus allowing to focus on covering these vulnerabilities that are most often the target or the weakness that enable cyber-crime to be deployed.

2. Research Methodology

The study commenced with a theoretical research, aiming to provide a high-level overview of cyber-attacks and related concepts. During the literature review stage, the authors could not identify any similar research previously performed, thus the theoretical research had its limitations in terms of similar studies and conclusions to serve as a foundation of the study.

The empirical research was based on the collection and analysis of statistical data regarding cyber-attacks reported all over the world in recent times. This analysis used a dataset centralized by Verizon, one of the biggest international security companies, based on attacks and security incidents detected world-wide in the recent years. A population of 4,785 attacks was analysed, providing information regarding the attack itself, the attacker, the target, vulnerabilities that allowed the attack to take place, impact and estimated damage, etc.

The raw data was cleansed and rearranged using MS Excel, by taking out all fields not to be included in the analysis, ensuring completeness of information and consistency of data formats for all records. Data was then grouped for significance and analysis purposes. Thus, business sectors were classified based on the root (first 2 digits) of the NAICS (North American Industry Classification System) code. A high-level analysis outlined that some of the business sectors did not have enough records in order to ensure statistical significance, thus several business industries were taken out of the analysis. Finally, data was turned from code (numerical values) to string, in order to facilitate the analysis and interpretation. The resulted dataset comprised of the victim's business sector (with the values displayed in Table 1), the attack pattern (values being displayed in Table 2), actor (presented in Table 3), root cause (with the values displayed in Table 4) and discovery method (presented in Table 5).

After cleansing and rearranging the data, the next step was the statistical analysis. Several statistical tests were considered for the analysis; however the authors decided that a logistic regression would best serve the objective of the research - to determine the correlation between attacks attributes (pattern, actors, root causes and discovery methods) and business sector.

The regression is a statistical measure determining how strong the relation is between one dependent variable (Y) and one or more independent variables (X). The relation is usually denoted under a regression model, as below:

Y = a + b1X1 + b2X2 + B3X3 + ... + BtXt + u

Where:
Y - The dependent variable (predicted variable);
X - The independent variable(s) (using to predict Y);
a - The intercept;
b - The slope;
u - The regression residual.

Based on the variables, several regression types could be defined; however, the logistic regression was chosen for the purpose of this research. A logistic regression generates a dichotomous variable (having solely two possible values). For the present research, the resulting variable could only have two values: 1 (if the attack took place) or 0 (if the attack didn't take place).

Since multiple variables could be considered for the regression, the stepwise model was believed to best satisfy the purpose of defining a model for each of the analysed business sectors. A stepwise regression is based on flexibility, adding or removing variables in order to determine the most significant model. The initial model for each of the analysed business sectors included all variables, which were individually analysed and excluded if not relevant for the model. Thus, resulted models differ from one business sector to another.

Using SAS software, a logistic regression was developed using the stepwise model for each of the business sectors, with the following initial variables.

Industry = Pattern + Actor + Root_Cause + Discovery_Method.

Where:
Industry – the dependent variable (y)
Pattern, Action, Actor, Root_Cause, Discovery_Method - independent variables (x).
For accommodation and food services, the stepwise logistic regression had the output presented in Table 6.
The results based on a population of 74 attacks, can be transposed into a model as follows:

Accomodation and food services = -5.2310 + Crimeware * 2.0972 + pattern.Payment Card Skimmer * 1.8056 + pattern.Point of Sale * 4.7086 + pattern.Privilege Misuse * 1.4227 + Discovery_method.External Customer * 1.5356 + Discovery_method.External Fraud Detection * 2.6093

From all analysed variables, the interpretation can be that there is a relation between the accommodation and food services industry and several patterns (crimeware, payment card skimmer, point of sale, privilege misuse), as well as discovery methods (external customers and external fraud detection).

An essential step in the analysis was determining the p value, used for testing a statistical hypothesis (if p value is lower or equal to the significance level of the test, denoted α, than the hypothesis must be rejected as data is not consistent with the assumption of the null hypothesis being true). Since our confidence level was set to 95%, thus α being equal to 5% (100%-95%), and as the p value is lower than 0.05 for all variables, we conclude that the results are statistically significant.

For administrative and support, waste management and remediation services, a total population of 105 attacks was analysed as presented in Table 7. The following results were obtained:

Administrative_and_support_waste = -3.7802 + actor_Partner * 0.7850 + root_cause_Carelessness * -1.4391 + discovery_method.External Fraud Detection * 1.7233 + discovery_method.Internal Infrastructure Monitoring * 3.0872

As the p value is lower than 0.05 for all variables, we conclude that the results are statistically significant.
For educational services, a total population of 264 attacks was analysed, the results are outlined in Table 8. The following model resulted:

Educational Services = -2.6249 + pattern.Cyber-Espionage * -2.7439 + pattern.Privilege Misuse * -1.2687 + actor.Internal * 0.4113 + root_cause.Carelessness * -2.2019 + discovery_method.Internal IT Review * 1.5569

For health and social assistance, a total population of 947 attacks was analysed. The results are outlined in Table 9, based on which the following model resulted:

Health and social assistance = -1.6529 + pattern.Cyber-Espionage * -3.6982 + pattern.Denial Of Service * -2.4580 + pattern.Lost And Stolen Assets * 1.7518 + pattern.Privilege Misuse * 0.2923 + pattern.Web Applications * -1.9329 + root_cause.Carelessness * -0.9427

For finance and insurance services, a total population of 425 attacks was analysed. The results obtained are outlined in Table 10, and translated in the following model:

Finance and insurance = -1.4819 + pattern.Cyber-Espionage * -3.2751 + pattern.Lost And Stolen Assets * -0.3645 + pattern.Payment Card Skimmer * 1.7492 + actor.External * -0.5871 + actor.Internal * -0.9125 + root_cause.Carelessness * -1.1455 + discovery_method.External Disclosure * -0.9674 + discovery_method.Customer * 0.6067 + discovery_method.Internal Fraud Detection * 1.7175

For the information sector, a total population of 393 attacks was analysed, as presented in Table 11, based on which the following model was obtained: For the public administration services, a total population of 1591 attacks was analysed, the results being outlined in Table 12, based on which the following model was obtained:

Public Administration = -1.7626 + pattern.Lost And Stolen Assets * -0.5695 + actor.Internal * 1.4133 + root_cause.Carelessness * 2.0112 + discovery_method.External Actor Disclosure * 0.7020 + dicsovery_method.ExternalCustomer * -0.8052 + discovery_method.External Suspicious Traffic * 1.6580

For the retail sector, a total population of 171 attacks was analysed. Based on the results outlined in Table 13, the following model was obtained:

Retail trade = -3.5387 + pattern.Crimeware * 1.4378 + pattern.Payment Card Skimmer * 2.4608 + pattern.Point Of Sale * 2.7010 + pattern.Privilege Misuse * 1.0068 + pattern.Web Application * 1.5008 + actor.Internal * -1.2738 + root_cause.Random Error * 2.6461 + discovery_method.External Actor Disclosure * -2.0562 + discovery_method.Fraud Detection * 1.5508

The last step was to determine probability and odds of the resulted model to be deployed should an attack occur in the respective business sector. For each of the business sectors, probabilities and odds were determined as for identifying the model with the greatest odds of being deployed.

Several scenarios were developed and analysed in terms of probability and odds. The scenarios were based on the regression model resulted as described above for each of the analysed business sectors, and each scenario contains a combination of one pattern, one actor, one root cause and one discovery method. If for a certain business sector not all categories (pattern, actor, root cause, discovery method) are available (e.g. all actors were excluded from the model for not being relevant), the scenarios would only contain one of each available categories. Scenarios were presented as a table, each variable being set to either 1 (if part of the scenario) or 0 (if kept out of the scenario). For example, scenario 1, summarised in Figure 1, can be described as: *A point of sales attack discovered by the external fraud detection has a probability of 88.96% of occurring* (point of sales and external fraud detection variables are set to "1", while Crimeware, payment card skimmer, privilege misuse and external customer variables are set to "0").

3. Results and Discussion

3.1. Accommodation and food services

Based on the regression model resulted for the accommodation and food services industry, 8 scenarios were developed and analysed in terms of probability and odds of being deployed, as presented in Figure 2. Since for accommodation and food services industry no actors or root causes were included in the final model, the scenarios contain a combination of one pattern (namely crimeware, payment card skimmer and point of sales) and one discovery method (external customer, respectively external fraud detection). The results outline that, if an attack would be deployed in the accommodation and food services industry, there is an 88.96% probability of it being a payment card skimmer attack, and discovered by the external fraud detection services. At the other end, for a privilege misuse incident to occur and be discovered externally by customers, the probability is low (9.34%), while odds are 0.10303.

3.2. Administrative and support, waste management and remediation services

For the administrative and support, waste management and remediation sector, results displayed in Figure3 show that an attack deployed by a business partner and discovered through internal infrastructure monitoring has a probability of 52.30 of occurring.

Therefore, organisations activating in this sector should more carefully treat their business partners, and make sure sufficient controls are in place to avoid unauthorised access to the entity's information and assets (e.g. logical access granted to contractors or third parties should be timely terminated once the agreement is off or it is no longer required).

3.3. Educational services

For the educational services, the results displayed in Figure4 show that an internal actor being the attacker has a probability of 34.15%. Also, cyber-espionage and privilege misuse patterns could be deployed, but the probability is quite low.

3.4. Health and social assistance

Among the health and social assistance scenarios, attacks may fall into the lost and stolen assets pattern with a probability of 52.47%. Figure 5 shows all designed scenarios. Adding carelessness as the root cause results in a probability of 30.07%, which is relatively high comparing to the other scenarios.

3.5. Finance and insurance

Figure 6 presents the main scenarios designed for the finance and insurance sector, which is predominantly threatened by payment card skimmer attacks, most frequently being discovered by the internal fraud detection (the scenario has a probability of 87.92%). Adding to the scenario an external actor and the root cause of carelessness, the probability reaches 56.27%. All other scenarios are less likely to occur.

3.6. Public Administration

In public administration sector, as can be seen in Figure 7, carelessness plays an important role as a root cause for the attacks. Results show that if an attack occurs, there are 171:1 chances (or a probability of 99.42%) that it is performed by an internal actor, due to staff carelessness, and discovered through suspicious traffic analysis. Most frequently (98.98%), attacks and incidents fall under the pattern of lost and stolen assets.

3.7. Retail trade

Results from Figure 8 show that the most probable root cause of attacks in the retail industry is the random error. Thus, there are 29:1 chances that if an attack targets a retail company it would fall in the point of sales pattern, being allowed by a random error, and potentially discovered by the external fraud detection services. Adding to the scenario the internal actor would reach a probability of 88.95%.

4. Conclusions

The study outlined that there is a relation between attacks and some of the business sectors. This study may be the basis of an in-depth analysis with the purpose of providing insights and open the way towards a systematic channelling of the limited security budget towards the right internal controls. For example, in the public the pattern of lost and stolen assets has a high probability of occurring, while the main root cause is carelessness. These facts may support the conclusion that there is a low level of general awareness of staff with regards to the internal controls, as well as a poor commitment towards the organisation's assets and information. The main recommendation would thus be to ensure regular training for all staff as well as increase the level of documentation and awareness of internal processes, procedures and controls in place over the public sector.Other concluding examples could be the finance and insurance sector, in which payment card skimmer attacks discovered by external fraud detection services have a high probability of occurrence, or that most incidents in the retail industry are caused by random error.

Future research will commence with the results of this study in order to develop insights and recommendations for each of the business sectors, thus allowing professionals to better understand what to expect from the cyber-world, appropriately define the risks and focus their limited resources and budget on implementing appropriate controls, in order to enhance security of information and cyber space.

References

Akhgar, B., Stainforth, A., Bosco, F. (2014).Cyber-Crime and Cyber-Terrorism – Investigator's handbook. Elsevier, 25-78.

Akhgar, S., Yates, B. (2013). Strategic Intelligence Management. 1st Edition, Butterworth-Heinemann, 56-255.

Cenzic (2014). Cenzic, Application Vulnerability Trends Report: 2014.[Online] Available:www.cenzic.com.

CERT-UK, GCHQ Organisations (2014).Common Cyber-Attacks: Reducing the impact.[Online] Available:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf.

Klimburg, A. (editor) (2012).National cyber-security framework manual.NATO CCD COE Publications, [Online] Available:https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

Lahneman, W. J., Arcos, R. (2014), The art of intelligence: simulations, exercises and games. Rowman&Littlefield, 18-59.

McAfee Labs (2014). Threats Predictions 2015.[Online] Available: http://mcaffee.com.

PriceWaterhouseCoopers, InfoSecurity (2014). 2014 Information Security Breaches Survey, [Online] Available: http://www.pwc.co.uk.

Rehman, A. U. (2014).Understanding the significance of cyber-security threats. VFAST Transactions on Education and Social Sciences, 4, 2, 1-6.

Richards, J. (2014). Cyber-war: the anatomy of the global security threat. Palgrave Macmillan, 9-23.

Shackelford, S. J. (2014).Managing cyber-attacks in international law, business and relationships. Cambridge University Press, 5-10.

Singer, P. W., A. Friedman (2014).Cyber security and cyber war – what everyone needs to know. Oxford University, 35-197.

Sood, A., Enbody, R. (2014).Targeted Cyber-Attacks: Multi-staged Attacks Driven by Exploits and Malware. Elsevier, USA.

Uma, M., Padmavathi, G. (2013). A survey on various cyber-attacks and their classification. International Journal of Network Security, 15, 5, 390-396.

Wall, D. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press 2007, 8-58.

Wang, P., Liu, J. (2014). Threat analysis of cyber-attacks with Attack. Journal of Information Hiding and Multimedia Signal Processing, 5, 4, 778:787.

Westerman, G. (2013).Your Business Is Never Too Small For A Cyber-attack, Here's How To Protect Yourself. Forbes, [Online] Available:http://www.forbes.com/sites/forbesleadershipforum/ 2013/05/13/your-business-is-never-too-small-for-a-cyber-attack-heres-how-to-protect-yourself/.

Yar, M. (2013).Cybercrime and society. Sage Publications, Second Edition. 9-67.

Appendix 1 – Tables and figures.

Variable name	Description
Accommodation and food service	NAICS sector 72
Administrative and support, waste management and remediation services	NAICS sector 56
Agriculture, forestry, fishing and hunting	NAICS sector 11
Arts, entertainment and recreation	NAICS sector 71
Construction	NAICS sector 23
Educational services	NAICS sector 61
Finance and insurance	NAICS sector 52
Health care and social assistance	NAICS sector 62
Information\s	NAICS sector 51
Management of companies and enterprises	NAICS sector 55
Manufacturing	NAICS sector 31-33
Mining, quarrying and oil and gas extraction	NAICS sector 21
Other (public) services (except public administration)	NAICS sector 81
Professional, scientific and technical services	NAICS sector 54
Public Administration	NAICS sector 92
Real estate, rental and leasing	NAICS sector 53
Retail trade	NAICS sector 44-45
Transportation and warehousing	NAICS sector 48-49
Utilities	NAICS sector 22
Wholesale trade	NAICS sector 42-43

Table1. Data set description – Business sectors

Variable name	Description
DOS (Denial of Service) attacks	Includes all attacks aiming to cause inoperability of hardware and software equipment through traffic flooding techniques
Web application attacks	Is represented by all attacks performed through a web application.
Cyber-espionage	Includes attacks performed through unauthorized access to the entity's network, data or systems, in order to gain access to data (most of the times classified) with the purpose of espionage.
Insider and privilege misuse	Represents attacks or incidents caused by abuse or misuse of the logical access rights to the entity's systems, network, data, etc. that would thus compromise the confidentiality, integrity and availability of information.
Physical theft and loss	Represents any damage through intended or accidental misplacement of information assets.
Payment card skimmers	Includes all incidents/attacks consisting of a device being physically implanted to a magnetic stripe data reading equipment (e.g. ATMs, POS terminals, etc.).
Point-of-sale intrusions	Represented by attacks through remote access in environments where payment transactions are conducted through the use of a card-present purchase system (POS) – except card skimming, which is included in the previously described pattern.
Crimeware	Includes all attacks with any other objectives than cyber-espionage, and of any other types than the previously described patterns (e.g. malware, etc.).
Miscellaneous errors	Is represented by any unintended actions leading to security breaches being developed or exploited.
Random error	No identified reason or fault.

Table2. Data set description – attack patterns

Variable name	Description
Internal	The attack was deployed by an employee or executive of the entity.
External	The attack was deployed by an actor that has no business relationship with the entity.
Partner	The attack was deployed by a contractor, former employee, or other party that has (or had) any business relationship with the company.

Table3. Data set description – actors

Variable name	Description
Carelessness	Lack of proper commitment or acknowledgement of the entity's policies and security requirements by staff.
Inadequate personnel	Inadequate or insufficient staff.
Inadequate processes	Faulty processes.
Inadequate technology	Faulty technology resources, systems or network vulnerabilities, inadequate or insufficient technological resources.

Table4. Data set description – root causes

Variable name	Description
External - actor disclosure	The attack was disclosed by the attacker itself (e.g. through public brag, blackmail, etc.).
External - fraud detection	The attack was detected by an external party contracted for fraud detection.
External - monitoring service	The attack was detected through the external security incidents monitoring services.
External – customer	The attack was reported by a customer or business partner directly or indirectly affected by the incident.
External - unrelated party	The attack was reported by an external party that is not involved into any relationship with the entity (e.g. law enforcement organisms).
External – audit	The attack was detected by a form of external audit (security audit or scan, etc.).
External – unknown	The attack was detected by an external party; however the method of discovery is not known, or was not reported by the entity.
Internal – antivirus	The attack was internally detected, through notifications provided by the antivirus program.
Internal - incident response	The attack/incident was internally detected through the use of problem and incident management service (while dealing with a different incident).
Internal - financial audit	The attack was internally discovered during the financial audit mission.
Internal - fraud detection	The attack was detected by the internal fraud detection system/service.
Internal – HIDS	The attack was internally detected by the IDS (*Intrusion Detection System*) or file integrity monitoring system.
Internal - IT audit	The attack was internally detected during and IT audit, security audit or scan.
Internal - IT review	The attack was internally detected through reviewing logs (activity, history, etc.).
Internal – NIDS	The attack was internally detected through automated IDS (*Intrusion Detection System*) or IPS (*Intrusion Prevention System*) notifications.
External - law enforcement	The attack was detected through formal notification from law enforcement or government organisms.
Internal - security alarm	The attack was detected through physical access intruder alarm systems alerts.
Internal - reported by user	The attack was reported by internal users, who detected suspicious actions, missing or inaccurate data.

Table5. Data set description – discovery method

Parameter	DF	Estimate	Standard Error	Wald Chi-Square	Pr > ChiSq
Intercept	1	-5.2310	0.2127	604.8580	<.0001
Crimeware	1	2.0972	0.4595	20.8312	<.0001
Paymeznt_Card_Skimmer	1	1.8056	0.5249	11.8334	0.0006
Point_of_Sale	1	4.7086	0.4705	100.1609	<.0001
Privilege_Misuse	1	1.4227	0.2922	23.7080	<.0001
dme_customer	1	1.5356	0.3370	20.7625	<.0001
dme_fraud_detec	1	2.6093	0.4308	36.6919	<.0001

Table 6. Likelihood estimates – Accommodation services

Parameter	DF	Estimate	Standard Error	Wald Chi-Square	Pr > ChiSq
Intercept	1	-3.7802	0.1082	1220.3370	<.0001
actor_Partner	1	0.7850	0.3778	4.3169	0.0377
aev_Carelessness	1	-1.4391	0.5128	7.8752	0.0050
dme_fraud_detec	1	1.7233	0.4472	14.8516	0.0001
dmi_infrastruct	1	3.0872	1.2295	6.3050	0.0120

Table 7. Likelihood estimates – Administrative services

Parameter	DF	Estimate	Standard Error	Wald Chi-Square	Pr > ChiSq
Intercept	1	-2.6249	0.0801	1073.8779	<.0001
Cyber_Espionage	1	-2.7439	1.0056	7.4456	0.0064
Privilege_Misuse	1	-1.2687	0.2413	27.6529	<.0001
actor_Internal	1	0.4113	0.1522	7.3033	0.0069
aev_Carelessness	1	-2.2019	0.3767	34.1652	<.0001
dmi_IT_review	1	1.5569	0.5166	9.0842	0.0026

Table 8. Likelihood estimates – Educational services

Parameter	DF	Estimate	Standard Error	Wald Chi-Square	Pr > ChiSq
Intercept	1	-1.6529	0.0680	590.1643	<.0001
Cyber_Espionage	1	-3.6982	1.0043	13.5604	0.0002
Denial_of_Service	1	-2.4580	0.7161	11.7815	0.0006
Lost_and_Stolen_Assets	1	1.7518	0.0916	365.5134	<.0001
Privilege_Misuse	1	0.2923	0.1108	6.9575	0.0083
Web_Applications	1	-1.9329	0.2551	57.4115	<.0001
aev_Carelessness	1	-0.9427	0.1320	50.9973	<.0001

Table 9. Likelihood estimates – Health services

Parameter	DF	Estimate	Standard Error	Wald Chi-Square	Pr > ChiSq
Intercept	1	-1.4819	0.1458	103.3333	<.0001
Cyber_Espionage	1	-3.2751	1.0066	10.5858	0.0011
Lost_and_Stolen_Assets	1	-0.3645	0.1447	6.3497	0.0117
Payment_Card_Skimmer	1	1.7492	0.2367	54.5941	<.0001
actor_External	1	-0.5871	0.1626	13.0300	0.0003
actor_Internal	1	-0.9125	0.1662	30.1600	<.0001
aev_Carelessness	1	-1.1455	0.2443	21.9852	<.0001
dme_actor_discl	1	-0.9674	0.2348	16.9828	<.0001
dme_customer	1	0.6067	0.1785	11.5547	0.0007
dmi_fraud_detec	1	1.7175	0.7360	5.4459	0.0196

Table10. Likelihood estimates – Finance and insurance

Parameter	DF	Estimate	Standard Error	Wald Chi-Square	Pr > ChiSq
Intercept	1	-3.5649	0.1356	691.0237	<.0001
Denial_of_Service	1	1.0130	0.2179	21.6189	<.0001
Lost_and_Stolen_Assets	1	-2.2984	0.3153	53.1545	<.0001
Web_Applications	1	0.8010	0.1297	38.1260	<.0001
actor_External	1	1.6580	0.1622	104.5108	<.0001

Table11. Likelihood estimates – Information services

Parameter	DF	Estimate	Standard Error	Wald Chi-Square	Pr > ChiSq
Intercept	1	-1.7626	0.0699	635.4642	<.0001
Lost_and_Stolen_Assets	1	-0.5695	0.1070	28.3010	<.0001
actor_Internal	1	1.4133	0.0840	283.3959	<.0001
aev_Carelessness	1	2.0112	0.1112	327.2126	<.0001
dme_actor_discl	1	0.7020	0.1217	33.2524	<.0001
dme_customer	1	-0.8052	0.1824	19.4959	<.0001
dme_suspicious_	1	3.4792	0.2370	215.4604	<.0001

Table12. Likelihood estimates – Public administration

Parameter	DF	Estimate	Standard Error	Wald Chi-Square	Pr > ChiSq
Intercept	1	-3.5387	0.1385	652.8453	<.0001
Crimeware	1	1.4378	0.3427	17.6023	<.0001
Payment_Card_Skimmer	1	2.4608	0.2861	73.9853	<.0001
Point_of_Sale	1	2.7010	0.4435	37.0867	<.0001
Privilege_Misuse	1	1.0068	0.3163	10.1328	0.0015
Web_Application	1	1.5008	0.2210	46.0949	<.0001
actor_Internal	1	-1.2738	0.2856	19.8940	<.0001
aev_Random_error	1	2.6461	0.8280	10.2116	0.0014
dme_actor_discl	1	-2.0562	0.4397	21.8703	<.0001
dme_fraud_detec	1	1.5508	0.3656	17.9941	<.0001

Table13. Likelihood estimates – Retail trade

Scenario	Pattern				Discovery Method		Probability	Odds
	Crimeware	Payment Card Skimmer	Point of Sale	Privilege Misuse	External Customer	External Fraud Detection		
S 1	0	0	1	0	0	1	**88.96%**	**8.059 89**

Figure1. Scenario example

Scenario	Pattern				Discovery Method		Probability	Odds
	Crimeware	Payment Card Skimmer	Point of Sale	Privilege Misuse	External Customer	External Fraud Detection		
S 1	0	0	1	0	0	1	**88.96%**	**8.059 89**
S 2	0	0	1	0	1	0	**73.36%**	**2.754 4**
S 3	1	0	0	0	0	1	**37.18%**	**0.591 85**
S 4	1	0	0	0	1	0	**16.82%**	**0.202 26**
S 5	0	1	0	0	1	0	**13.13%**	**0.151 1**
S 6	0	1	0	0	0	1	**30.66%**	**0.442 15**
S 7	0	0	0	1	0	1	**23.17%**	**0.301 5**
S 8	0	0	0	1	1	0	**9.34%**	**0.103 03**

Fig2. Scenarios – Accommodation and food services

Scenario	Actor	Root cause	Discovery method		Probability	Odds
	Partner	Carelessness	External Fraud Detection	Internal Infrastructure Monitoring		
S1	1	0	0	1	**52.30%**	**1.09636**
S2	1	0	1	0	**21.89%**	**0.2803**
S4	1	1	0	1	**20.63%**	**0.25999**

Figure3. Scenarios – Administrative services

Scenario	Pattern		Actor	Root cause	Discovery Method	Probability	Odds
	Cyber Espionage	Privilege Misuse	Internal	Carelessness	IT Internal Review		
S 1	0	1	1	0	1	**12.73%**	**0.14582**
S 2	1	0	1	0	1	**3.23%**	**0.0334**
S 3	0	0	1	0	1	**34.15%**	**0.51856**

Figure4. Scenarios – Educational services

Scenario	Pattern					Root cause	Probability	Odds
	Cyber Espionage	Denial of Service	Lost and Stolen Assets	Privilege Misuse	Web Applications	Carelessness		
S 1	0	0	1	0	0	1	**30.07%**	**0.43007**
S 2	0	0	0	1	0	1	**9.09%**	**0.09993**
S 3	0	1	0	0	0	1	**0.63%**	**0.00639**
S 4	1	0	0	0	0	1	**0.18%**	**0.00185**
S 5	0	0	1	0	0	0	**52.47%**	**1.10396**

Figure5. Scenarios – Health services

Scenario	Pattern			Actor		Root cause	Discovery Method			Probability	Odds
	Cyber Espionage	Lost and Stolen Assets	Payment Card Skimmer	External	Internal	Carelessness	Actor Disclosure	Customer	Internal Fraud Detection		
S1	0	0	1	1	0	1	0	0	1	**56.27%**	**1.28685**
S2	0	0	1	1	0	1	0	1	0	**29.76%**	**0.42375**
S3	0	0	1	1	0	1	1	0	0	**8.07%**	**0.0878**
S4	0	0	1	0	1	1	0	0	1	**48.17%**	**0.92941**
S5	0	0	1	0	1	1	0	1	0	**23.43%**	**0.30605**
S6	0	0	1	0	1	1	1	0	0	**5.96%**	**0.06341**
S7	0	1	0	1	0	1	0	0	1	**13.45%**	**0.15544**
S8	0	1	0	1	0	1	0	1	0	**4.87%**	**0.05119**
S9	0	1	0	1	0	1	1	0	0	**1.05%**	**0.01061**
S10	0	1	0	0	1	1	0	0	1	**10.09%**	**0.11226**
S11	0	1	0	0	1	1	0	1	0	**3.57%**	**0.03697**
S12	0	1	0	0	1	1	1	0	0	**0.76%**	**0.00766**
S13	1	0	0	1	0	1	0	0	1	**0.84%**	**0.00846**
S14	1	0	0	1	0	1	0	1	0	**0.28%**	**0.00279**
S15	1	0	0	1	0	1	1	0	0	**0.06%**	**0.00058**
S16	1	0	0	0	1	1	0	0	1	**0.61%**	**0.00611**
S17	1	0	0	0	1	1	0	1	0	**0.20%**	**0.00201**
S18	1	0	0	0	1	1	1	0	0	**0.04%**	**0.00042**
S19	0	0	1	0	0	0	0	0	1	**87.92%**	**7.27759**

Figure6. Scenarios – Finance and insurance

Scenario	Pattern	Actor	Root cause	Discovery Method			Probability	Odds
	Lost and Stolen Assets	Internal	Carelessness	Actor Disclosure	Customer	External Suspicious Traffic		
S1	1	1	1	0	0	1	**98.98%**	**96.6987**
S2	1	1	1	0	1	0	**57.13%**	**1.33269**
S3	1	1	1	1	0	0	**85.75%**	**6.01586**
S4	0	1	1	0	0	1	**99.42%**	**170.903**

Figure7. Scenarios – Public administration

Scenario	Pattern					Actor	Root Cause	Discovery Method		Probability	Odds
	Crimeware	Payment Card Skimmer	Point of Sale	Privilege Misuse	Web Applications	Internal	Random Error	Actor Disclosure	External Fraud Detection		
S1	0	1	0	0	0	1	1	0	1	**86.36 %**	**6.32937**
S2	0	1	0	0	0	1	1	1	0	**14.66 %**	**0.17174**
S3	0	0	1	0	0	1	1	0	1	**88.95 %**	**8.04781**
S4	0	0	1	0	0	1	1	1	0	**17.92 %**	**0.21836**
S5	1	0	0	0	0	1	1	1	0	**5.82%**	**0.06174**
S6	1	0	0	0	0	1	1	0	1	**69.47 %**	**2.2755**
S7	0	0	0	1	0	1	1	0	1	**59.66 %**	**1.47875**
S8	0	0	0	1	0	1	1	1	0	**3.86%**	**0.04012**
S9	0	0	0	0	1	1	1	0	1	**70.79 %**	**2.42347**
S10	0	0	0	0	1	1	1	1	0	**6.17%**	**0.06576**
S11	0	0	1	0	0	0	1	0	1	**96.64 %**	**28.7661**

Figure8. Scenarios – Retail trade