Table of Contents

Introduction

This article highlights the Business & Communication Insurance (B&C Insurance) mitigation strategy. After prioritising risks or threats, a mitigation plan will be developed. In order to develop goals for risk, a model will be applied to classify various risk variables and analyse them based on their effect on the organisation. In addition, defined categories of risk such as

hacking, spy and phishing will be evaluated. In addition to this STRIDE model, the case of the insurance firm will be studied, and mitigation measures such as setting up of a high-tech cyber protection framework that guarantees that only permitted individuals have access to their individual accounts will therefore be proposed.

Prioritising the Risks

Different researchers have used multiple models for prioritising risks. One of the models was to determine different risk variables and then score each variable following their significance and impact on the organisation. In the Business and Communication case, risk variables can be Strategic plan risk, client's data leakage risk, and leakage of the company's confidential information such as financial and its internal strategy risk variable. Every variable will be scored, and at the end, the overall score will be identified. The overall score helps in determining the degree of threat either it is normalised or not based on a predefined scale. An example of such a model is shared in figure 1, where risks 3 and 4 are prioritised based on assigned scores (Hinkelmann, 2012). Moreover, after determining the overall score, every risk variable is prioritised based on the highest score. In the case of an insurance company, a highly prioritised risk is the leakage of clients' information that is considered an important resource of the organisation. Second priority will be given to strategic planning and in the last unauthorised access to an internal strategy. Moreover, in other scenarios, risk variables can be personnel and funding related depending on the company's operations and cybersecurity system, and accordingly, variables are prioritised (Martins & Lambe, 2013)

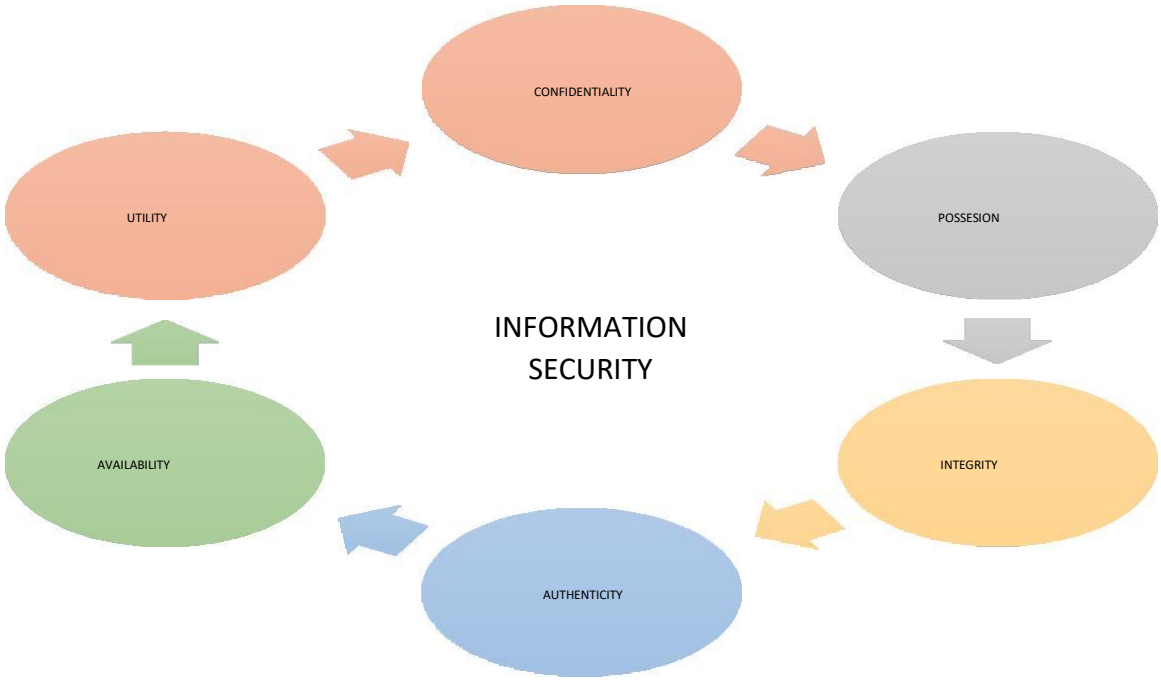

Figure 1. Parkerian hexad

The six elements were identified explicitly by Parkerian hexad related to ISOs and stressed that companies concentrate on those elements highlighted: control or ownership, secrecy, usefulness, honesty, integrity and utility. These components protect businesses, as mentioned in the case of insurance companies, from such cyber-attacks. Organisations understand, however, that they cannot fully defend themselves from certain attacks and threats, even though they can avoid threats because of the factors above. Furthermore, it calls on businesses to prioritise data protection, networks, processes and analyse the opportunities available to reduce the risk of cybercrime.

Companies must increase resources for the authentication, instead of stressing the secret details, of the credibility of individual information. Experts would claim that privacy cannot be overlooked, so businesses have to choose carefully. It is necessary to remember that priority should be given to honesty over secrecy, and the regulatory implications should be possible under sanction or penalty. The tools for cyber-attacks have been restricted to businesses. This needs to be handled carefully, and the risk must be prioritised accordingly (Boyes, 2015)

404 402 406

RISK	LEVEL	ACCESS COMPLEX	AUTHENT.	IMPACT	LIKELIHOOD	CONTROL EFFECT.	TIME TO ACT	OVERALL SCORE
RISK 1	1	3	3	2	1	4	1	4.67
RISK 2	3	1	2	1	1	3	2	3.33
RISK 3	1	2	1	1	1	1	1	21.00
RISK 4	2	1	3	1	2	4	1	14.00
RISK 5	1	2	1	1	2	1	2	4.33
RISK 6	1	2	1	2	1	3	2	3.67
RISK 7	1	1	1	1	3	2	1	4.67
RISK 8	2	3	1	1	3	4	1	3.33
RISK 9	2	1	2	2	1	1	3	3.00
RISK 10	1	2	1	2	1	1	1	4.33

Figure 2. Example of model

Apart from protecting and prioritising the most critical items, clear measures can be taken to deter individual cyber assaults by exchanging threat information. Companies in particular industries must exchange information by setting up a Security Council as a protective tool to deter cyber-attacks. The concept behind the establishment of an information-sharing council is clear. Take a case of a business and communications insurance firm exchanging cyber-attacks, through a common strategy and priority approach and solution models, with other insurance firms that have the same digital assets which other players in the industry will prevent from using the same nature of the cyber-attack.

Identified Categories of the Risk

The threats facing business and communications insurance companies have been listed in various categories, such as; hacking, malware, social engineering, espionage, and more precision phishing Phishing is described as an external party entity or business that receives emails. External parties have easy access to internal networks, primarily due to inappropriate processes in an organisation to deal with cyber-attacks.

In the case of enterprise and communication, there are also no particular forms of cyber risk, as it is any kind of accidental information leakage, sensitive data loss, a malicious attempt at attacks on the digital infrastructure and any attempt at modifying or stealing customers' privately held data for the economic gain. The scope of cyber risk has been noted, and there are varying viewpoints and divisions about cyber threats. It is difficult to characterise. Some business's view cyberattacks as someone trying to link to their device anonymously. In comparison, some businesses see it as unwanted third-party access. In the other hand, others consider that because of cyber incidents, a loss of data or digital

properties. Therefore, in a certain sector or organisation, it is very difficult to standardise or categorise the risk, because everyone has different opinions and meanings. Standardised companies such as MITRE, ISO and NIST are indicating this issue and disparity in meanings. It is necessary to have reliable, straightforward terms of the potential of cyber-attack for the purposes of establishing a separate cyber-risk information institution. A diverse view of cyber event concept would restrict data analysis and cyber risk-related consistency (Andress, 2011)

Standard Mitigations

For e-mail-received mitigation attacks such as phishing by the CEO of Business & Communication Insurance (B&C Insurance) mitigation measures are needed to communicate externally and internally the level of risk associated with cyberattacks that is critical for an organisation's awareness of how cyber-attacks can be treated. The advantage and cost analysis of cybersecurity investigations is also important to establish a mitigation matrix. As we know, no free lunch is available, so there is always trade between protection and some other aspects to be considered in the production of mitigation plans. Often you must choose between comfort, direct expense, time and advance technology. So, businesses have one option to choose (Chia, 2012). A company's business and communication insurance must either pay the premium or invest in high cyber safe technologies to safeguard sensitive data to safeguard customers and employees' confidential data against any further leakage. In order to retrieve the missing data and protect it from further data leakage, the Business and Communication Insurance company must invest in high cybersecurity technologies. A hacker must be able to save some data in its system, so the organisation must pay for some money in order to make sure that the hacker does not leak the information to another group.

Specific Resolutions and their Significance

One of the first things to do is to assess the cyber incident by the day the CEO receives the emails as the management team has been designed to look at this and has discovered that hackers have information from 200,000 customers so that he or she might even be revealing the details to others. This will also undermine the credibility of a company and therefore, the confidence of customers. In addition, a hacker can modify the company's other strategic details or steal other sensitive information by accessing an internal computer system (Andress, 2014) The next move for a corporation is to pay hackers for the information safety of 200,000 customers, then instal a high-tech cyber-security system to deter possible cyber-attacks. It is necessary to establish this system through specialists who ensure the authorisation to access the system of the company through the strict assurance of an approved identity, and each person will have access to his/her account without access to an official account of another company. Officials of each company will be responsible for their activities and acts.

Techniques to Mitigate the threats

The term safety implies security against attacks by an external individual or an insider or in other words, protecting against attacks by intruders. Companies and nations worldwide spend millions on protecting network violations where attacks are intended to have an adverse effect on network assets such as hardware, software and information. Security of properties is the main safety target. Network or computer security means the safety and detection of unauthorised and unlawful use of one's network or computer. Via confidentiality, authentication, honesty and the connection to legitimate users, a network is therefore considered secure. The company insurance for business and connectivity needs to pursue a three-tier plan for a good network of structures.

- Prevention: keep cyber threats from succeeding.
- Detection: Telling authorities and detecting them when an attack happened.
- Mitigation: the management team must be able to cover cyber-attack damage.

A network risk analysis that can be performed is critical for creating a stable network. In other words, the harm caused by an assault must be assessed. It is important to recognise all possible threats and assess the extent of security measures, before adapting and deploying secure network infrastructure, to address the impact of a cyber-attack. There are many methods for establishing the model to resolve possible threats affecting computers or the network (Khonji et al., 2013). The expected and systematic way to define and minimise multiple risk factors must be used. There are different methods for developing model threats and methods for developing a simulation of threats (Xing et al., 2015). Stride, which stands for spoofing, deception, repudiation, knowledge disclosure, denial of services and rights, is one of the best methods for a business and communication company.

- Spoofing: A situation where a person masks his original identity and appears to be someone else's name is "spoofing" (Schuckers, 2002). In the case of an insurance agency, a hacker might have accessed the system with a different identity and may claim to be someone else.

- Manipulation: a condition where data are maliciously modified. If the insurance company has access to customer details, it is likely that the hackers will change customer data and other strategic company data and sell it to the other parties.

- Repudiation: an act that rejects a particular occurrence. This category is since the device can identify the individual responsible for unauthorised access or illegal resource change. On the other hand, repudiation is characterised as a situation where no one takes the blame for performing such actions, and the consumer has not been able to locate the person responsible for such illegal action, as it has become difficult to identify who sent an email to an insurance undertaking. If these reasons are to be considered, an organisation must continue to verify all network system operations and records. Relevance and auditing are important for this. Therefore, after entering a particular act, this aspect of the STRIDE model ensures that the consumer is adequately responsible. Bad inspection procedures

have allowed hackers to access information from 200000 customers in the case of an insurance firm.

- Disclosure of information: data leakage or infringement may affect the confidentiality of data. For example, any sniffing or dropping of the data may take place by various methods of data encryption by the organisation. This model feature helps users reveal certain data in order to make it easy for a hacker to access the data.

- Service denial: Hackers tried to interrupt the network infrastructure to allow people to access the system and network in a way that made it hard for them. In general, hackers send several packets of falsified packets into the machine or network that block the network (Wood & Stankovic, 2002). Tens of millions of Internet addresses have been investigated using this technology (Lau et al., 2000).The future challenge to the insurance company is to instal a well-developed cybersecurity system immediately by its management team to defend the company against this loss.

- Privileges elevation: an act that allows the unauthorised person access to the network infrastructure and that can more accurately access data than the approved party and the hacker can do whatever he or she wants (Mirza Ahmad et al., 2002). This is due to a lack of protection and surveillance. The same is true of the insurance firm, with the CEO receiving an email along with details from 200 customers as a threat.

The STRIDE model has supported the team in finding deficiencies and thoroughly assessing the cyber-attack and inadequately designing a strategy to resolve future threats as well.

Table 1. Consequences vs Risk likelihood

	Consequences					
Likelihood	Doomsday	Catastrophic	Major	Moderate	Minor	Insignificant
Almost certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	E	M	L	L
Rare	E	H	E	M	L	L

Countermeasures

Cyber threats are complex and target both small and large groups, which cause different distractions. Such distractions include electric blackouts, machinery breakdown for business processes, violation of company secrets, or even legislation. B&C Insurance Firm shall first define the extent of risk as seen in Table 2, before taking countermeasures.

Table 2: Risk Levels

Risk level	Description
Extreme(E)	It would take detailed analysis and management preparation at the management stage. Daily assessments would include on-going preparation and tracking.
High (H)	Management requires care, but management and preparation should be left to the project managers. Continuous preparation and tracking of annual assessments are possible, but control changes are likely to be generated from current tools.
Medium (M)	Unique tracking and addressing protocols may be handled. Employee supervision is necessary for adequate control and analysis.
Low (L)	It can be administered through routine procedures.

The STRIDE model helps the team recognize vulnerabilities and evaluate cyberattacks consistently and adequately build a strategy to deter possible threats, such as implementing high-tech cybersecurity infrastructure to reduce potential threats

Recommendation

From the point of view of the audit, the analysis of long-term risks for information security was learned (Goel & Pon, 2011). The most general technique is to define and evaluate the findings appropriately on the basis of the judgement of an auditor in order to validate established safety elements. The matrix method is one of Chen and Goel's best methods for risk analysis. The model matrix can be used to evaluate large scope by quantitative analysis. This approach helps an insurance provider to connect risks, vulnerabilities, assets and system management activities, as well as various asset controls (Öɬütçü et al., 2016). In addition, the company's properties are deemed important objects to be secured from outside access. Currently, the insurance provider for business and connectivity is under attack to their networks and data to secure.

As in the first part, the approach of calculation of risk variables is proposed, and the total score then summarised in order to figure out the total score. The risk of losing sensitive data from 200,000 customers is the highest priority. And the strategic risk is the second priority.

The management team would then follow the plan to pay the hacker a little ransom for the protection of hacked data and then concentrate on installing a high-tech cybersafety model to prevent hackers from obtaining more information that could influence the strategic direction of the business. The system must track and allow approved persons to access their accounts only effectively.

Conclusion

A Business and Communication Company mitigation strategy was presented. After prioritising risk and defining risk groups, the proposal to pay a ransom sum and instal a high-tech cybersecurity system was recommended. In addition, the STRIDE model was applied to examine the entire hacking case at the insurance firm and contact to recommend a proper mitigating plan (Deghaili et al., 2011)

References

Andress, J. (2011). What is Information Security? In *The Basics of Information Security*. https://doi.org/10.1016/b978-1-59749-653-7.00001-3

Andress, J. (2014). What is Information Security? In *The Basics of Information Security*. https://doi.org/10.1016/b978-0-12-800744-0.00001-4

Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*. https://doi.org/10.22215/timreview888

Chia, T. (2012). *Confidentiality, Integrity, Availability: The three components of the CIA Triad*. Stackoverflow:Information Security.

Deghaili, R., Chehab, A., Kayssi, A., & Itani, W. (2011). STRIDE. *International Journal of Dependable and Trustworthy Information Systems*. https://doi.org/10.4018/ijdtis.2010010104

Goel, S., & Pon, D. (2011). Information Security Risk Analysis. In *Information Security and*

Ethics. https://doi.org/10.4018/978-1-59904-937-3.ch190

Hinkelmann, K. (2012). Design and Analysis of Experiments. In *Design and Analysis of Experiments*. https://doi.org/10.1002/9781118147634

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. In *IEEE Communications Surveys and Tutorials*. https://doi.org/10.1109/SURV.2013.032213.00009

Lau, F., Rubin, S. H., Smith, M. H., & Trajković, L. (2000). Distributed denial of service attacks. *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*. https://doi.org/10.1109/ICSMC.2000.886455

Martins, J. R. R. A., & Lambe, A. B. (2013). Multidisciplinary design optimization: A survey of architectures. *AIAA Journal*. https://doi.org/10.2514/1.J051895

Mirza Ahmad, D. R., Dubrawsky, I., Flynn, H., Grand, J. "Kingpin," Graham, R., Johnson, N. L., K2, Kaminsky, D. "Effugas," Lynch, F. W., Manzuik, S. W., Permeh, R., Pfeil, K., Puppy, R. F., & Russell, R. (2002). Chapter 3 – Classes of Attack. In *Hack Proofing Your Network*.

Öȶütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers and Security*. https://doi.org/10.1016/j.cose.2015.10.002

Schuckers, S. A. C. (2002). Spoofing and Anti-Spoofing Measures. In *Information Security Technical Report*. https://doi.org/10.1016/S1363-4127(02)00407-7

Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. *Computer*. https://doi.org/10.1109/MC.2002.1039518

Xing, T., Xiong, Z., Qian, H., Medhi, D., & Huang, D. (2015). Cloud Security. In *Cloud Services, Networking, and Management*. https://doi.org/10.1002/9781119042655.ch11