Privacy and Protection of Customer Information: BeTrust Loyalty Programme

Ahlam Alhalafi [1] and Dr.Prakash *Veeraraghavan*[1] †,

La Trobe University, Computer Science and IT, Melbourne, Australia

Abstract

Digital risk management is an unavoidable concern for businesses. Digitizing corporate operations will be an important trend. It will fast-track due to inexorable technological advancement and human experience. The varying risk management methods must upgrade to digital risk management. Digitalization provides a chance for companies to reimagine the future of operational risk management.

Keywords: *Information security, Cyber economy, digital transformation, Risk management, Network security.*

1. Fact-Finding

Jack is in charge of backup preparation in BeTrust and has created a single copy of the database on a USB stick. Strong winds damaged the local electrical supply on March 5th. From 10 a.m. until 2 p.m. that day, all structures in the neighborhood lost power. Jack did not make a backup for this week, and his USB stick only included data from the previous week. Therefore, the company's data for the current month was corrupted. IT experts claim that any data already in backup could no longer be restored. This incident resulted in a significant data loss.

Jone, on the contrary, is concerned about a lack of intrusion detection systems (IDS) and the use of a free antivirus that Jack discovered on the internet. On May 10th, a hacker exploited the flaw and infiltrated the companies using free antivirus, including BeTrust. The firm experienced considerable data loss and destruction.

Alex is the head of BeTrust's financial sector. She prepares all transfers and tax documents on her computer. A coffee spill destroyed her computer on August 15th. Since Alex's laptop held all the consumer information, the company could not recover new transaction details that were not backed up.

Likert-scale Questionnaire

This questionnaire aims to promote staff engagement and activity by focusing on content interaction. Furthermore, it is a sort of user feedback recycling. The questionnaire has the following list of questions:

- Q1: BeTrust's loss of data due to an unexpected event with no backup could have devastating consequences for the company's operations. (Reply between 1-5, 1 = strongly agree and 5 = strongly disagree)
- Q2: Does the organization's staff have an adequate understanding of Information Security and Network Security? (Reply between 1-5, with 1 showing an adequate and five showing basic)
- Q3: Is there a need for periodic spot checks on the availability of information processing facilities?
- Q4 : Do you think the company is handling customer information reasonably, and to what extent is it reasonable/unreasonable?
- Q5: In case of a virus attack, how well do you think BeTrust security technology can prevent it?
- Q6: Is there a need to invest more in assets, such as laptops?
- Q7: For sensitive documents, are common enhanced protection mechanisms sufficient? Is it all the system's fault?

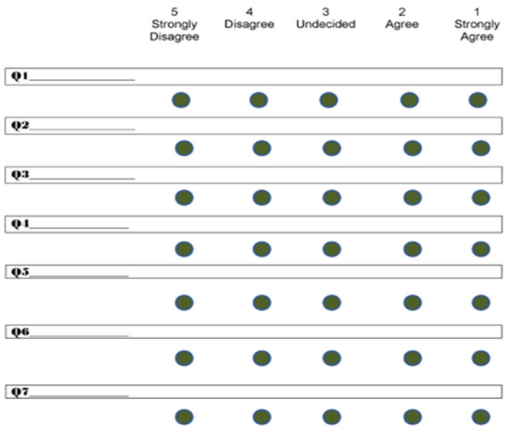

Figure 1.

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.87

2. Real-World Attack

Calce, now 25, was a high school student in Canada when he decided to launch a DDoS attack on several big-profile commercial websites. According to industry experts, the attacks caused a $US1.2 billion damage price. He was arrested and sentenced to eight months in open detention in 2001 while still a minor, thus restricting his actions (Harris and Younggren, 2011, p.26). Calce has since worked as a columnist and published a memoir about his ordeal.

Hackers got access to multiple Google business systems, stealing confidential information. Google said in a blog post that it has "evidence to suggest that one of the attackers' primary goals was accessing the Gmail accounts of Chinese human rights activists." The focus was on the Chinese government, which has long been accused of flagrantly violating human rights. With the launch of 'www.google.cn' in 2006, Google joined the Chinese market and agreed to China's strict Internet censorship policy. Google moved its servers for google.cn to Hong Kong in March 2010.

3. Quantitative Analysis

This section will identify the most significant hazards and quantitatively analyze them. The ALE (Annual Loss Expectancy) model will examine the vulnerabilities. Four dangers must be explored to comprehend BeTrust's information system management. The asset's value and the single loss expectancy can rate the risks (SLE). SLE is the maximum amount of money we may lose in a single attack. The ALE model helps conduct the cost-benefit analysis (CBA). ALE is the amount we may expect to lose from a specific type of attack for a year. The predicted number of attacks per year is the Annual Rate of Occurrence (ARO). The value of ALE was calculated by multiplying the ARO by SLE. The difference between ALE before and after control, subtracting the annualized cost of security (ACS), is CBA.

Inadequate Backup

The risk of insufficient backup activities came first. For instance, Jack made a single duplicate of the database on a USB stick without any other options. SLE is approximated to be $250,000. In A.12.3.1, ISO/IEC 27001(2013, p. 16) explains the attacks and offers control mechanisms for data backup. A digital preservation system must be built to keep data eternally without data loss (Barateiro et al. 2010,p. 7). For instance, consider One Drive's storage space or other similar companies' services. The annualized cost was stated to be $10000 per year.

		Before (Without) Control			After (With) Control		Control			Benefit	ROSI	Decision
Vulnerability/Threat Description	Value(AV) ($)	Single Loss Expectancy (SLE)($)	Annualized Rate of Occurrence (ARO)($/yr)	Annualized Loss Expectancy (ALE)($/yr)	Annualized Rate of Occurrence (ARO)($/yr)	Annualized Loss Expectancy (ALE)($/yr)	Description	Cost ($)	Annualized Cost of Security (ACS)($/yr)	Cost Benefit Analysis (CBA)	Return on Security Investment (ROSI)	Type
Inadequate backup	5000000	250000	0.5	125000	0.2	50000	A.12.3.1	50000	10000	25000	2.5	Transfer
Lack of IDS and network segments	600000	18000	3	54000	0.5	9000	A.9.1.2	30000	6000	15000	2.5	Mitigate
Loss of customer data	1000000	100000	0.25	25000	0.1	10000	A.18.1.4	10000	2000	5000	2.5	Mitigate

Figure 2:

The number of ARO can be reduced from one attack every two years to one every five years. From $12500 to $50000, the ALE was lowered. This attack has a CBA of $25000. The control is worthy because there is a $25000 gain.

Lack of IDS and Network Segments

The danger of not having IDS and network segmentation came in third. In A.9.1.2, ISO/IEC 27001(2013, p. 16) explains IDS and network segmentation will guarantee users only access allowed network resources and services. In the context of BeTrust, current equipment may not be able to keep up with everyday use and development speed. The SLE is priced at $18,000. The ALE is $4000 and $9000 before and after control, respectively. Besides, CBA is $15,000, while ARO drops to 0.5 after control. This tactic of control is appropriate.

Loss of Data

Comparing SLE and asset value, the danger of losing customer data is rated eighth. In A.18.1.4 of ISO/IEC 27001 (2013, p. 16), it is stated that companies should protect their customers' personally identifiable information. The protection minimizes the damage to the company's reputation caused by the loss of customer data. Companies must exercise restraint in general if they want to respect the privacy of individual clients. However, Jack pointed out that while businesses recognize the value of user data in enhancing competitiveness, users want to store and use their data efficiently. Also, they don't want their data to be exploited or leaked. BeTrust was advised to observe all privacy rules and protection of personally identifiable customer information, boost transparency about data usage, and adopt technical means to protect legally collected data. A single attack may cost the corporation $100,000. The ARO differed by $0.15/year. After control, the ALE was almost quadrupled, saving the organization $15,000. Businesses must protect their

digital assets to prevent reputational risks (Barateiro et al., 2010, p. 5).

Budget, Risk Appetite, and Residual Risk

Due to the risk-based decision-making, the possibility of failure can be reduced, or performance can be impacted. It is dependent on the cost from the standpoint of budget. Maintaining a healthy balance between cost and expense is beneficial to a company's risk management choice. Risk analysis is far more straightforward than other approaches. It's also a technology that can assist in resolving and dealing with dangers that arise as a result of the strategy's aim and possibility (Barateiro et al., 2010, p. 6). From the standpoint of Risk Appetite. True Trust is a good match for the images. They are more likely to occur in small-to-medium-sized businesses. Residual risk is the risk that remains after risk management has been adopted. The majority of the decisions are mitigated in this scenario. So, these are the hazards that can be readily managed. They have a lower chance of being classified as residual risk.

4. Qualitative Analysis

This section will conduct a qualitative analysis based on the results of the quantitative analysis. When employing qualitative analytic methods, the risk is assessed using adjectives rather than numbers." (p148, Karabacak and Sogukpinar 2005). Besides, the section will introduce a risk matrix for qualitative analysis, which will assess risk and evaluate the impact of control implementation. It was necessary to classify the data sample based on the information gained from the ALE analysis. This report will be expected to use the categories in Figures 3 and 4 in the risk matrix, and the risk matrix is depicted in Figure 5.

It categorizes the consequences of each risk into five categories: inconsequential, minor, substantial, significant, and severe. It divides the likelihood of occurrence into five levels: rare, unlikely, moderate, likely, and almost definite for the possibility. It will set thresholds on each level ranging 1-5 under the consequence and probability, the details of which can be found in Figures 3 and 4. It tries to assign the findings in different cells of the risk matrix after assessing the likelihood and consequence of discovered hazards. The cell names are very low, low, medium, high, very high, and extreme.

Consequence		
Name	**Range**	**Level**
Insignificant	0- $5,000 (incl.)	1
Minor	$5,000-$10,000 (incl.)	2
Significant	$10,000-$100,000 (incl.)	3
Major	$100000-$200,000 (incl.)	4
Severe	Above $200,000 (incl.)	5

Figure 3:

Likelihood		
Name	**Range**	**Level**
Rare	1 every 20 years or less (less than 0.05 incl.)	1
Unlikely	from 0.05 to 0.2 (incl.)	2
Moderate	from 0.2 to 1 (incl.)	3
Likely	from 1 to 4 (incl.)	4
Almost Certain	Almost Certain: above 4	5

Figure 4

		Consequence: How severe could the outcomes be if the risk event occurred?				
		1 Insignificant	2 Minor	3 Significant	4 Major	5 Severe
Likelihood: What's the chance the of the risk occurring?	5 Almost Certain	5 Medium	10 High	15 Very high	20 Extreme	25 Extreme
	4 Likely	4 Medium	8 Medium	12 High	16 Very high	20 Extreme
	3 Moderate	3 Low	6 Medium	9 Medium	12 High	15 Very high
	2 Unlikely	2 Very low	4 Low	6 Medium	8 Medium	10 High
	1 Rare	1 Very low	2 Very low	3 Low	4 Medium	5 Medium

Figure 5

Inadequate Backup

Unexpected occurrences will cause serious data loss if regular backup actions are not performed. Internal or external variables might create unexpected events; external elements include damage caused by fire, water, and other natural disasters. Temporary failures such as power loss and irrecoverable failures can cause hardware errors in internal components (Barateiro et al., 2010, p. 10). The SLE of this attack is $250000 due to insufficient backup efforts, and it remains unchanged after the control implementation, which is listed in the 'Severe' category under the 'Consequence' category. Before the control, the

ARO of this attack was 0.5, which falls into the 'Moderate' group within the 'Likelihood' category. After performing suitable backup activities, the ARO of this attack is 0.2, which falls into the 'Unlikely' category within the 'Likelihood' category. The risk assessment was altered from 'Very high' to 'High' in the risk matrix. The number was dropped from 15 to 10. The control appears to be effective, as evidenced by the blue arrow in Figure 6.

Lack of IDS and Network Segment

A corporation appears to be a massive machine. Each component represents a distinct function. As a result, good hardware or software aids in effectively preventing hackers or intrusion. The IDS and network segmentation must value the cost of upgrading based on the discussed risk. Because of the decision-making, this section will concentrate on improving mitigation. Some elements of risk assessment and management are believed to be essential portions throughout building blocks in the era of constructing the comprehensive framework to cyber-security across the control and government (Sean S, B & Joost R, S. 2020, p. 1748). (Sean S, B & Joost R, S. 2020, p. 1748). The network controls should be ensured by analyzing risk management, emphasizing the qualitative because developing a good system is to prevent being vulnerable to an attack.

The SLE prior is 18,000 before control - which is "Significant" on the five-level consequence scale. Simultaneously, the ARO prior value is 3 per year, with a "Likely" likelihood of the risk occurring. Overall, there is a "High12" chance that the absolute risk will happen without any control mechanisms in place. The SLE post consequence threat continues at "Significant" after control; however, an ARO post value of 0.5 is categorized as "Moderate." The danger of ALE was reduced from "High12" to "Medium" with more effective control. As a result, companies must purchase hardware to avoid hacking or incursion. It can be seen in Figure 6 as the purple-colored arrow.

Damaged Reputation Due to Loss of Customer Data

A corporation's data loss encompasses various indirect losses, such as a loss of consumer confidence, company reputation, industry credibility, and widespread fear induced by the loss or compromise of customer data. It is critical to implement the appropriate processes, whether caused by human error at BeTrust, application vulnerabilities, or insufficient security safeguards. Before control, the SLE prior was 100,000 and based on five levels of consequence, and it had reached "significant." At the same time, the ARO prior value is 0.25/year, with a "moderate" chance of the risk occurring. ALE prior (Significant, Moderate) = Medium9 was the overall likelihood of the risk arising without any controls. The SLE post consequence danger was classified as "Significant" after controls, while ARO post was classified as "Unlikely." Even though the ultimate risk assessment is still "Medium," by reducing from "Medium 9" to "Medium 6," the risk of ALE post can be deduced to be "Unlikely." As a result, BeTrust must purchase and install licensed software and cloud services to successfully manage backup data. The orange-colored arrow in Figure 6 can be used to verify this.

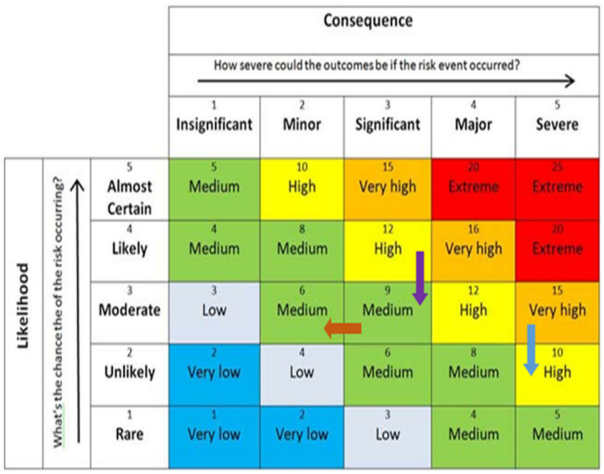

Figure 6:

5. Conclusion

Digital risks have increasingly become a concern that corporations cannot ignore as organizations digitize (p.37, Harris and Younggren, 2011). Failing to protect against digital threats will result in financial, reputational, and customer losses. (p.12, Reamer, 2013) Thus, digital risk management is essential. Not only can good digital risk management help firms avoid excessive losses, but it may also make administration more straightforward and enhance the efficiency of the operations of a company. (Risk Management of Digital Information: An Investigation of File Formats, 2001, p.41)

6. References

[1] Barateiro, J., Antunes, G., Freitas, F., & Borbinha, J. 2010, 'Designing digital preservation solutions: A risk management-based approach', The International Journal of Digital Curation, vol. 5, no.1, pp.2-14.

[2] Harris, E. and Younggren, J., 2011. Risk management in the digital world. *Professional Psychology: Research and Practice*, 42(6), pp.412-418.

[3] ISO/IEC 27001 2013, Information Technology-Security Techniques-Information security management systems-Requirements, ISO/IEC 27001:2013[E], viewed 2 Oct 2020, ProQuest Ebook Central database. pp.1-19

[4] Karabacak, B. and Sogukpinar, I. 2005, ISRAM: Information security risk analysis method, Computers & Security, 24(2), pp.147-59.

[5] Reamer, F., 2013. Social Work in a Digital Age: Ethical and Risk Management Challenges. *Social Work*, 58(2), pp.163-172.

[6] Sean S., B & Joost R., S. (2020). A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Election Power Grid, 40(9), 1744-1761.

[7] *The Journal of Academic Librarianship*, 2001. Risk Management of Digital Information: A File Format Investigation. 27(5), pp.417-418.