Interdisciplinary Term Paper

IDS300W: Interdisciplinary Theory and Concepts

April 28th, 2023

The internet has changed a lot in the past couple decades. Most of the things we do in our daily lives are affected by the internet or are affiliated with the internet. With this popularity and innovation brings the reliance to it. With that said, companies now rely heavily on the internet, which can possibly put their confidential information at risk. Cybercriminals and their attacks have risen by over %81 over the global pandemic in 2020 (Businesswire, 2021). When most companies had to rely on the internet to function and continue their operations. Companies need to protect their confidential information against cybercriminals in order to keep their operations in business. Then we ask ourselves, how can a small business with limited resources effectively protect their confidential information from cybercriminals?

Determining how a company will protect its confidential information with limited money and resources will take more than just one discipline. This will instead be researched through the lens of interdisciplinary research. After reviewing which disciplines provided the best insight into the problem, I found that cybersecurity, economics, and information technology disciplines provided the best insight.

**Literature Review**

Looking at this problem from a cybersecurity perspective, according to an article written by betanews, a cybercriminal can infiltrate 93% of companies' networks (Barker, 2022). This is an alarming rate when we talk about the protection of companies' confidential information. Then we begin to think, if companies with a mass amount of resources can get breached, what chances do companies with limited resources have?

According to a cyber report done by Accenture, 43% of all cyber attacks are aimed at small companies. In the same report, it is stated that only a mere 14% are ready and prepared to defend themselves. This is very alarming for all small businesses, since they are targeted because of statistics like these. (Linkedin,2022) Cybercriminals know that only a small percentage of small businesses are willing to adequately invest in their cybersecurity department.

Through the lens of cybersecurity, this problem needs to be addressed and mitigated through the use of the implementation of technological measures to ensure that there is no unauthorized access or destruction of confidential data. Some of these technological measures could include antivirus software, firewalls, and threat detection software. These measures are put in place to safeguard the confidential information that the companies hold. Moreover, the protection of confidential information is not just a technological issue but also a human one. According to techradar, employees are often one of the main reasons why cybercriminals get into a system and steal information.

An economics perspective, will look at this problem and try to provide a solution that is as cost-friendly as possible. Economics will determine an optimal level of investment into the cybersecurity and information technology departments in order to properly solve the problem. However, when looking at the statistics, small companies have an approximate downtime of eight hours, according to cybersecurity-magazine. A small company has limited resources as it is, and can by no means take eight hours of downtime. Small companies have limited resources and may hope that they can avoid investing money in cybersecurity so they can further grow their company. However, in recent years and as the statistics show, the risk is too high, and a company can possibly lose everything if a company's cybersecurity is disregarded.

When small businesses have limited resources, investing in the best possible security measures is very difficult. The cybersecurity perspective prioritizes the security of the company's information. Therefore, the cybersecurity approach may recommend investing in the most effective cyber approach/solutions. However, from an economic perspective, investing in the most effective approach may not be possible. The company may have to consider cost-effective options. The economic perspective may recommend investing in affordable security options rather than the most effective ones. The difficulty comes when a smaller company has to invest into cybersecurity but only has a limited amount of resources.

From an information technology perspective, this will prioritize certain pieces of information over others. This perspective can help a company allocate a certain amount of resources where it needs it the most. As it relates to small businesses, this is very important as they have limited resources compared to larger companies. Information technology can also categorize information to determine what's most important.

This leads into data classification, which is a vital component to any company's cybersecurity. Data classification ensures that a company can allocate resources to the most important information instead of allocating resources equally, which will be costly and ineffective. Information technology will also help companies monitor information databases to ensure that there have not been any breaches, and the security of the information has stayed intact. Information systems can implement access control to ensure that only authorized personnel have access to certain information. This can be done through the use of various cybersecurity measures like firewalls and intrusion detection systems.

Cybersecurity and information technology are similar in some ways, as explained above, but they differ when it comes to prioritization. The information technology perspective is mainly focused on the technology infrastructure and determining if it is functional/efficient. While the cybersecurity perspective will focus on ensuring that the information is secure. When talking about the resource/financial concerns previously mentioned, and how small companies have to spread their resources among their cybersecurity department wisely. This continues when we talk about the funding of the information technology department and the technological infrastructure. The constant battle for small companies will be how they invest effectively in each of their departments while ensuring that they have invested enough to secure their network against cybercrime.

**Common Ground**

The evidence suggests that small businesses are being attacked at an alarming rate. The information technology and cybersecurity perspectives argue that small companies need to prioritize cybersecurity as a critical aspect of their operations. This may include investing in network security systems like firewalls and employee training programs. Implementing training programs will mitigate the chance of an employee falling victim to a cyberattack. Prioritizing cybersecurity will also include updating and maintaining information technology systems. This will lessen the chance of a potential threat attacking, and stealing valuable information that a small company can’t afford to lose.

While the cybersecurity and economic perspectives may seem different on the surface, they both have the common goal of protecting the company's confidential information. While the cybersecurity perspective focuses on the implementation of cybersecurity measures, the economic perspective focuses on managing the costs and analyzing the benefits of such implementations. They both work together and are crucial partners in developing the most effective cybersecurity strategy to protect the company's data. There are options that will further a company's cybersecurity department, while being cost-effective. Implementing a framework like the NIST framework will set a standard within the company that will reduce the overall cybersecurity risk. According to the FTC, this framework gives a small business an outline to guide them on where to effectively spend their time and money.

The information technology and cyber security perspectives work together to secure the company’s network. This can look like establishing policies and procedures to mitigate insider threats or, as previously stated, providing employee training sessions. According to Forbes, 57% of cyberattacks occur through an employee's email. This could dramatically decrease the number of cyberattacks if a small company looked to implement employee cyber awareness training. This is another example of cost-efficient programs that could mitigate the risk of cyberattacks. Companies need to be aware of the cyber threat around them so that they can give themselves the opportunity to avoid losing information.

Analysis has shown that not implementing cybersecurity measures is a very risky decision. When taking into account how many resources small companies have, losing information can possibly destroy a company. Despite the fact that a high percentage of cyberattacks happen to small businesses, the majority of small businesses still feel that they are unprepared for a cyberattack at the current moment. Cyberattacks can happen at any given moment, and given how frequently they occur, this should outright justify that small companies should invest further in their information technology and cybersecurity departments. While this proposition will not help the company save money in the short term, in the long term, it could possibly save millions of dollars.

Experts from the three disciplines can develop plans to further protect the company from cybercriminals. Through the use of a cost-effective analysis, a company can protect its information while considering the economic benefits of potential cybersecurity investments and the technical aspects of implementing cybersecurity measures. Additionally, conducting a risk assessment is crucial when protecting company information. This risk assessment considers current value, vulnerabilities, and the threat of potential bad actors.

The economic perspective can help prioritize risks to the company's monetary losses, while the cybersecurity perspective will help the company fight against potential threats by identifying vulnerabilities in the system, and the cybercriminals themselves. The information technology perspective will identify crucial information that should be prioritized and the systems that support it.

An integrated approach combines knowledge and expertise from the information technology, economic, and cybersecurity perspectives, this is important for small businesses to look at when protecting their confidential information. Each of these disciplines brings a unique view and skills that can be applied together to develop strategies to help protect companies information assets. Even when all three of these disciplines may differ in some regard.

Overall, if a company is willing to find common ground between the disciplines, there is much success to be had. It is important that a small company leverages the knowledge of each of the three disciplines to create the most effective strategy that suits the individual company. In conclusion, small companies should prioritize cybersecurity efforts as a means to protect their confidential information.

References

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022, February 17). *Cyber risk and cybersecurity: A systematic review of data availability - the Geneva Papers on risk and insurance - issues and practice*. SpringerLink. Retrieved April 28, 2023, from https://link.springer.com/article/10.1057/s41288-022-00266-6

Paoli, L., Visschers, J., & Verstraete, C. (2018, May 16). *The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium - crime, Law and social change*. SpringerLink. Retrieved April 28, 2023, from https://link.springer.com/article/10.1007/s10611-018-9774-y

*Information security spending to exceed $124B 2019*. Gartner. (2019). Retrieved April 28, 2023, from https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Yuryna Connolly, L., Wall, D. S., Lang, M., & Oddson, B. (2020, December 28). *Empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability*. OUP Academic. Retrieved April 28, 2023, from https://doi.org/10.1093/cybsec/tyaa023

*A complete guide to the risk assessment process*. A Complete Guide to the Risk Assessment Process | Lucidchart Blog. (2018, June 11). Retrieved April 28, 2023, from https://www.lucidchart.com/blog/risk-assessment-process

*Risk assessment and analysis methods: Qualitative and quantitative*. ISACA. (n.d.). Retrieved April 28, 2023, from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods

Barker, I. (2021, December 20). *Cybercriminals can penetrate 93 percent of company networks*. BetaNews. Retrieved April 28, 2023, from https://betanews.com/2021/12/20/cybercriminals-penetrate-93-percent-of-company-networks/

*Cyber Resilient Business*. Accenture. (n.d.). Retrieved April 28, 2023, from https://www.accenture.com/us-en/insights/cyber-security-index

Spadafora, A. (2019, May 8). *90 percent of data breaches are caused by human error*. TechRadar. Retrieved April 28, 2023, from https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error

Lukehart, A. (2021, May 20). *10 Small Business Cyber Security Statistics that you should know – and how to improve them*. Cybersecurity Magazine. Retrieved April 28, 2023, from https://cybersecurity-magazine.com/10-small-business-cyber-security-statistics-that-you-should-know-and-how-to-improve-them/

*Cyber threats have increased 81% since global pandemic*. Business Wire. (2021, November 9). Retrieved April 28, 2023, from https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic

Pratt, M. K. (2023, February 28). *Economic pressures are increasing cybersecurity risks; a recession would amp them up more*. CSO Online. Retrieved April 28, 2023, from https://www.csoonline.com/article/3689008/economic-pressures-are-increasing-cybersecurity-risks-a-recession-would-amp-them-up-more.html#:~:text=Economic%20pressures%20are%20increasing%20cybersecurity%20risks%3B%20a%20recession,...%205%20Prioritize%20based%20on%20current%20risk%20

Delesline III, N. (2021). *It security and cybersecurity: What's the difference?* ZDNET. Retrieved April 28, 2023, from https://www.zdnet.com/education/computers-tech/difference-between-it-security-cybersecurity/

Sotnikov, I. (2020). *Data classification: What it is and how to implement it*. Netwrix Blog. Retrieved April 28, 2023, from https://blog.netwrix.com/2020/09/02/data-classification/

Brooks, C. (2022, October 12). *Cybersecurity in 2022 – a fresh look at some very alarming stats*. Forbes. Retrieved April 28, 2023, from https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=5ae14496b616

M. Rea-Guaman, J. A. Calvo-Manzano and T. S. Feliu, "A prototype to manage cybersecurity in small companies," *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, Caceres, Spain, 2018, pp. 1-6, doi: 10.23919/CISTI.2018.8399252.

Wang, Y., & Wang, L. (2022). Internet Financial Data Security and Economic Risk Prevention for Android Application Privacy Leakage Detection. *Computational Intelligence and Neuroscience : CIN, 2022*<https://doi.org/10.1155/2022/6782281>

Haan, K. (2023, April 22). *Best data analytics tools & software (2023)*. Forbes. Retrieved April 28, 2023, from https://www.forbes.com/advisor/business/software/best-data-analytics-tools/

Vedova, H., & Technology, T. F. T. C. O. of. (2022, October 6). *Understanding the NIST cybersecurity framework*. Federal Trade Commission. Retrieved April 28, 2023, from https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

Ltd, K. C. S. (n.d.). *Why small businesses are targeted more by cyber-criminals*. LinkedIn. Retrieved April 28, 2023, from https://www.linkedin.com/pulse/why-small-businesses-targeted-more-cyber-criminals-#:~:text=Why%20small%20businesses%20are%20targeted%20more%20by%20cyber-criminals,businesses%20can%20lead%20cyber-criminals%20into%20bigger%20ones%20

Thomas, D. S. (2021, November 10). *Cybercrime: It's worse than we thought*. NIST. Retrieved April 28, 2023, from https://www.nist.gov/blogs/taking-measure/cybercrime-its-worse-we-thought

Walkowski, D. (2019, August 22). *What are security controls?* F5 Labs. Retrieved April 28, 2023, from https://www.f5.com/labs/learning-center/what-are-security-controls#:~:text=Some%20common%20examples%20are%20authentication%20solutions%2C%20firewalls%2C%20antivirus,as%20access%20control%20lists%20%28ACLs%29%20and%20encryption%20measures.