



slington college
(इस्लिङ्टन कलेज)

Module Code & Module Title
CC4004NI Cyber Security Fundamentals

Assessment Weightage & Type
50% Individual Coursework

Year and Semester
2022 Spring

Student Name: Rounak Pradhan

London Met ID: 22066975

College ID: NP01NT4A220198

Assignment Due Date: Tuesday, 9 May 2023

Assignment Submission Date: Tuesday, 9 May 2023

Word Count: 4097

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

1. Introduction	1
1.1. Overview of ransomware attacks:	1
1.2. Short summary of Report.....	3
2. Section 1: Research into theft of personal Data	3
2.1. Facts of Ransomware attacks when and why was company targeted.....	3
2.2. Effect on customer	5
2.3. Deployed of ransomware on Acer's company	6
2.4. Errors made by company	8
3. Section 2: Personal data loss in a cyber-attack	9
3.1. Action taken by a company of cyber-attack resulting in a data breach	9
3.2. Fine imposed on the company by Governing bodies	11
4. Section 3: Chief Information Security:.....	12
4.1. Prevention of data breach	12
4.2. Preventive measures.....	13
4.3. What measures should I take for it not to happen again?.....	14
5. Conclusion	16
6. References	17
7. Appendix:	19

Table of figures

Figure 1 : Accenture (Gatlan, BLEEPINGCOMPUTER, 2021)	2
Figure 2: Acer data leak (Abrams, 2021)	5
Figure 3: Acer ransom demand on Tor payment site (TechTargey, 2021)	6
Figure 4: a general workflow for types of ransomware (Gantenbein, 2020)	7

List of Abbreviation

Raas	Ransomware-as-a-service
SaaS	Software-as-a-service
PII	Personality Identifiable Information
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
TFEU	Treaty On the Functioning of the European Union
CISO	Chief Information Security Officer

1. Introduction

1.1. Overview of ransomware attacks:

Ransomware as a service(RaaS) is a malicious variation on the business paradigm of software as a service(SaaS). It is a subscription-based business in which purchasers, known as ransomware affiliates, acquire or rent pre-developed ransomware tools to carry out ransomware assaults (Trend Micro, 2021).

The ransomware inventor distributes the software to clients known as affiliates, who utilize the software to keep people's data hostage with no technical competence . The usage of RaaS allows affiliates to reach an area of extortion activities that was previously only available to the writers.

This business model allows malware authors to increase their earning from their program while incurring less personal risk than if they used it themselves. Offering their software to others absolves them of the final offense by allowing someone else to conduct the act of ransom.

RaaS, like ransomware, is often a criminal activity that is almost always unlawful anywhere in the globe (Kerner, 2021).

A form of virus called ransomware is used by attackers to hold data hostage until a ransom is paid. Ransomware attacks can devastate businesses by stealing data to sell on the Dark Web, exposing private information, or erasing it completely if they are not stopped or discovered quickly after infection. Information about customers, finances, intellectual property, and employees is frequently the target of assaults and may still be stolen even after the attackers have been paid off (FORTRA, 2018).

Global leader in IT consulting Accenture stated that users of the LockBit ransomware stole data from its systems during an assault that occurred in August 2021.

The company's financial report for the fourth quarter and entire fiscal year, which ended on August 31, 2021, made this information public (Gatlan, Bleepingcomputer, 2021).

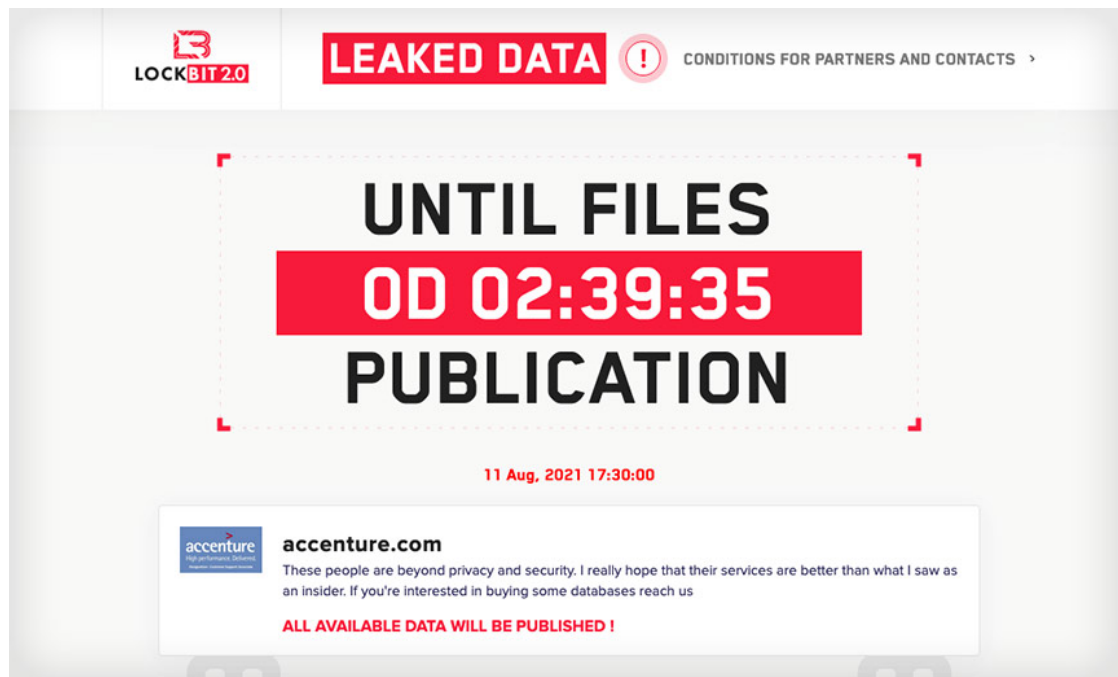


Figure 1 : Accenture (Gatlan, BLEEPINGCOMPUTER, 2021)

The impacted systems, Accenture, were restored from a backup. In a statement given to CNN, a spokeswoman hinted that the incident was found through monitoring and that it had no effect on the business' operations or the systems of its customers. An insider at the organization helped steal 6TB of data, according to a tweet from Cybel, a dark web and cyber crime monitoring outfit. In reality, LockBit 2.0 is aggressively seeking insiders and offering them millions of dollars in compensation.

After the first payment deadline of four hours passed, some of the data was briefly made available. Fortunately, Tor was down at the moment. The next deadline was likewise missed by LockBit.

The ransomware's most recent version is called LockBit 2.0. According to Felipe Duarte, a security researcher at Appgate, the latest version has the ability to use group policies to encrypt whole Windows domains. After that, it infects other networked computers, disables antivirus software, and launches ransomware. Additionally, it sets a ransom note as the background image, which is an attempt to find insiders willing to aid and abet a LockBit ransomware attack in exchange for the promise of millions.

According to crime intelligence company Hudson Rock, 2,500 partner and employee PCs were impacted. (Morgan, Cyber Security Hub, 2021)

1.2. Short summary of Report

- Facts of ransomware attacks
- Investigation made by national and international governing bodies on data breach
- Action made by a cyber attack

2. Section 1: Research into theft of personal Data


2.1. Facts of Ransomware attacks when and why was company targeted

The Acer ransomware attack occurred on March 19, 2021, when the company's network was breached by cybercriminals. The greatest ransom demand in history was made in response to the REvil ransomware attack against Acer. By taking advantage of a Microsoft Exchange server vulnerability that Acer had

neglected to address, the attackers were able to enter the network. The attackers installed ransomware after they had gained the data on Acer's systems and requesting a ransom in return for the key to unlock it. (Din, 2023)

Acer was targeted for an unknown purpose, although it is likely that the attackers chose the corporation because of its scale and the valuable personal information it stored. The international technology corporation Acer manufactures a variety of goods, such as laptops, desktop computers, and tablets. With 7,000 employees, \$7.8 billion in yearly revenue in 2019, and \$3 billion in profits in Q4 2020, Acer is one of the most well-known companies to experience ransomware assaults. It is unclear why Acer was specifically targeted, but ransomware attacks have been more prevalent in recent years as hackers target business they think to be weak and likely to pay a ransom to prevent the publication of private information. Names, addresses, phone numbers, email addresses, and payment card information are among the data the corporation holds about its huge customer base. (HOPE, 2021)

Acer Inc.



Acer.com - is a Taiwanese multinational hardware and electronics corporation specializing in advanced electronics technology, headquartered in Xizhi, New Taipei City. Its products include desktop PCs, laptop PCs tablets, servers, storage devices, virtual reality devices, displays, smartphones and peripherals, as well as gaming PCs and accessories under its Predator brand. Acer is the world's 6th-largest PC vendor by unit sales as of January 2021

CUSTOMER_CODE	8 digit Accou	One Customer with multiple Location	Credit Currency	Site Credit Limit	CUSTOMER_NAME	CUSTOMER_LOCAL_NAME
10000011	10000011	N	USD			
10000017	10000017	N	USD			
10000022	10000022	N	JPY			
10000030	10000030	N	USD			
10000037	10000037	N	JPY			
10000042	10000042	N	USD			
10000051	10000051	N	USD			
10000056	10000056	N	USD			
10000057	10000057	N	USD			
10000059	10000059	N	USD			
10000069	10000069	N	USD			
10000097	10000097	N	USD			
10000120	10000120	N	USD			
10000182	10000182	N	USD			
10000189	10000189	N	USD			
10000192	10000192	N	USD			
10000293	10000293	N	USD			
10000336	10000336	N	USD			
10032452	10032452	N	JPY			
10032453	10032453	Y	JPY			
10032486	10032486	N	JPY			
10032544	10032544	N	JPY			
10032545	10032545	N	JPY			
10032546	10032546	Y	JPY			
10032546	10032546	Y	USD			

Figure 2: Acer data leak (Abrams, 2021)


2.2. Effect on customer


Customer of Acer were significantly impacted by the hack because many of them had their personal information taken. The attack was reported by the REvil ransomware group, who sought a \$50 million payment, one of the highest at the time that was recorded. The hackers rejected Acer's offer of \$10 million in compensation. Interestingly The hackers also provided a 20% discount if the business paid by Wednesday. Attackers would provide a decryptor, a vulnerability report, and erase the stolen files in exchange for the firm. The hackers also warned the corporation to avoid SolarWind's demise during the chat between Acer representatives and the attacker gang. There is no guarantee that the attackers would not have decrypted the data or not sold it


on the dark web even if the ransom was paid. Theft of personal information effects on people, such as identity theft, financial fraud, and reputational harm. They posted pictures of what appear to be financial spreadsheets, bank paperwork, and correspondence as possibly stolen materials on their website (Greig, 2021).

The image is a screenshot of a ransomware demand page. At the top, a red banner reads "Your network has been infected!". Below this, there are three columns of text and icons. The first column shows an icon of three document folders and text stating that documents, photos, databases, and other important files are encrypted. The second column shows a padlock icon and text stating that to decrypt files, the user needs to buy "General-Decryptor" software. The third column shows a document with a question mark icon and text instructing the user to follow instructions below, warning that time is limited. In the center, it states the price of "General-Decryptor" is for all PCs on the infected network. At the bottom left, a countdown timer shows "8 days, 19:07:29" remaining, with footnotes stating that the price will be doubled if not paid on time and that time ends on March 28, 16:30:11. At the bottom right, the current price is listed as 214151 XMR (approx. 50,000,000 USD), and the price after the time ends is 428302 XMR (approx. 100,000,000 USD).

Your network has been infected!

 Your documents, photos, databases and other important files encrypted

 To decrypt your files you need to buy our special software - **General-Decryptor**

 Follow the instructions below. But remember that you do not have much time

General-Decryptor price
the price is for all PCs of your infected network

You have **8 days, 19:07:29**

* If you do not pay on time, the price will be doubled
* Time ends on **Mar 28, 16:30:11**

Current price **214151 XMR**
≈ 50,000,000 USD

After time ends **428302 XMR**
≈ 100,000,000 USD

Figure 3: Acer ransom demand on Tor payment site (TechTargey, 2021)

2.3. Deployed of ransomware on Acer's company

The most common way ransomware enters your network is through a download from a spam email attachment. The ransomware application is then launched as a result of the download. Other methods of entry include social engineering

and web-based downloads of malicious software, which can be done directly from a site or by clicking on “malvertising”, or fraudulent advertising that launch the ransomware. Malware can also be transmitted via chat messaging or detachable USB drives. (Gantenbein, ExtraHop, 2020)

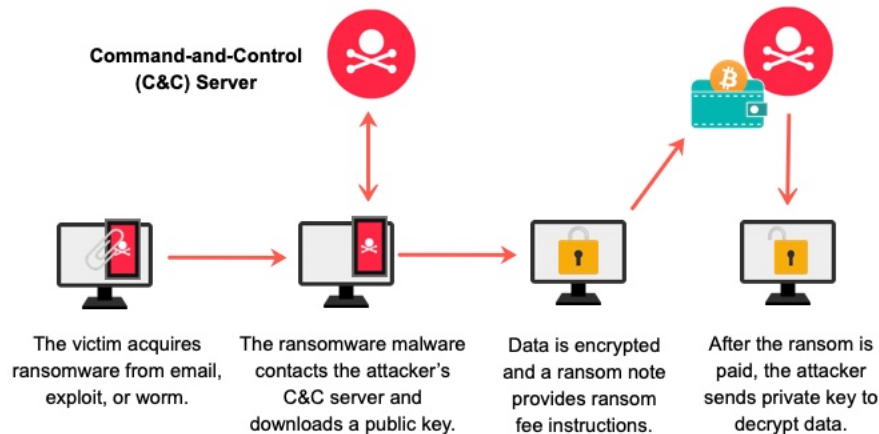


Figure 4: a general workflow for types of ransomware (Gantenbein, ExtraHop, 2020)

The ransomware was infected with the ransomware using a “dropper” program. In a zip file that appeared to be a legitimate software update, the dropper was concealed. The dropper was activated when the user opened the file, and it downloaded and installed the ransomware on the computer. Cybercriminals frequently utilize social engineering techniques to deceive consumers into installing dangerous software. The ransomware was deployed on Acer's system through a malicious software program called “REvil”, which is a type of ransomware-as-a-services(RaaS) that allows cybercriminals to rent access to their ransomware software.

A malicious actor is detected attempting to compromise an Acer Exchange mail server. It may be some time before Acer confirms whether REvil utilized that approach to access its network. It's extremely possible, given that up to 125,000 Exchange servers could still be vulnerable as of March 10th. In general,

there are several ways that ransomware attack might infiltrate computer systems. Typical approaches include phishing emails, exploiting security weakness, advertising malware, and Remote Desktop Protocol (RDP) attacks. Human error, such as employees clicking on phishing websites or using weak passwords, frequently contributes to the effectiveness of ransomware attacks. (Mathews, 2021)

2.4. Errors made by company

Acer made a number of mistakes that contributed to the ransomware assault, one of which was the failure to patch a Microsoft Exchange server vulnerability. Microsoft discovered the flaw in the beginning of 2021, and a security patch was made available. Acer, however, neglected to implement the fix, making its systems open to intrusion. This emphasizes how crucial it is to maintain systems updated with the most recent security patches in order to guard against cyberattacks. Acer might also not have had a through cybersecurity plan, which made them susceptible to online assaults. (hope, 2021)

Ransomware is increasingly targeting large corporations, especially those with strong financial results. In order to protect themselves from ransomware, business can:

- If anything unexpected happens and you need to restore all systems to their previous state, keep reliable backups of the entire network.
- Up to and including management, all staff should receive cybersecurity and safety training.
- Disallow external devices from connecting to your network if they might be malware-infected.
- Never open attachments or links in emails.

- Before making any decisions or disseminating information, double-check everything (Roberts, 2021).

In conclusion, a combination of flaws in the company's systems and cybercriminals' use of social engineering techniques led to the Acer ransomware attack. Customers of Acer were significantly affected by the assault since personal information was taken and might have been sold on the dark web/ Organizations must take precautions to secure their systems and maintain them up to speed with the most recent security fixes in order to avoid such assaults in the future.

3. Section 2: Personal data loss in a cyber-attack

3.1. Action taken by a company of cyber-attack resulting in a data breach

What is data Breach and How does it happen?

A data breach is a situation in which information is taken from a system without the owner's knowledge or consent. A data breach could happen to a small business or a major corporation. Credit card numbers, customer information, trade secrets, and information pertaining to national security are examples of sensitive, proprietary, or confidential information that may have been stolen.

The consequences of a data breach might include harm to the target company's reputation as a result of a perceived "betrayal of trust." If related data are among the information stolen, victims and their customers can also sustain financial damages (Trend Micro, 2016).

To compete in the modern workplace, businesses are becoming more and more dependent on data systems like cloud computing and remote working. While this data use gives organizations more power, it also exposes companies, clients and third party-vendors to more cybersecurity risks, like data breaches.

Following a cyber incident, how a company responds to a data breach can have a significant impact on its liability, reputation, and business continuity. This guide will help firms in preparing a through reaction to a data breach (Toohil, 2021)

To comprehend the implications of a data breach, consider some of the most typical causes of data leaks and breaches:

- Weak passwords
- Phishing
- Ransomware
- Social engineering scams
- Software misconfigurations

Once cybercriminals have gained access to a company's files and systems, they may be able to leak billions of stolen and leaked records to the dark web. When sensitive information, such as personality identifiable information(PII), is exposed or compromised, it can lead to more significant issues, such as financial fraud or identity threat.

The company should follow a clear incident response plan, which typically involves the following steps:

- Contain the breach: Containing the incident and preventing future unauthorized access to the system or data should come first. This could entail turning off affected services, resetting passwords, or isolating compromised networks or systems.

- Investigate the breach: To ascertain the origin and scope of the breach, what information was compromised, and what steps the attacker took, the organization should conduct a thorough investigation. This business will be able to use this find systematic weakness and take the necessary precautions to stop further intrusions.
- Notify affected parties: Customers or employees who may have been impacted by the breach should be informed as quickly as feasible, and information regarding the nature of the breach, the data that was compromised, and the precautions they should take should be provided.

Overall. A company should be proactive data breaches by implementing appropriate security measures and training employees on cybersecurity best practices. However, in the event of a breach, a timely and effective response can help mitigate the impact and prevent further damage (Chin, 2023).

3.2. Fine imposed on the company by Governing bodies

Depending on the industry, the type of breach, and the significance of the data loss, a firm that suffers a data breach may be required to notify the appropriate law enforcement authorities in order to remain in compliance with federal or state law.

Data protection legislation, such as the Data protection Act of 2018, the General Data protection Regulations(GDPR), and the Health insurance Portability and Accountability Act Of 1996(HIPAA), motivate business to report data breaches within a certain time frame (chin, 2023).

With recent allegations of data breaches, the European Union's General Data Protection Regulation(GDPR) is gaining increased attention and anticipation. Weeks before its implementation, security experts are beginning to examine breaches through the perspective of the GDPR's higher rules.

Fines must be effective, proportionate, and dissuasive in each circumstance. The authorities have a statutory inventory of criteria that they must evaluate when deciding whether and what degree of penalty can be issued. International infringement, refusal to mitigate harm, or lack of cooperation with authorities, among other things, can result in increased penalties. For very serious infractions, as defined in Art. 83(5) GDPR includes fines of up to 10 million euros, or in the case of an undertaking, up to 2% of its total global turnover for the preceding fiscal year, whichever is greater. Especially, The phrase “undertaking is important in European Union(EU) competition law. According to the European Court of Justice, the word refers to any entity that engages in economic activity, regardless of its legal form or how it is funded. This is especially important in the context of Articles 101 and 102 of the treaty on the Functioning of the European Union(TFEU) which are core elements of EU competition law. Article 101 outlaws agreements between undertakings[1][2], concerted activities, and decisions by associations of undertakings that may affect trade between Member states and have the goal or effect of preventing, restricting, or distorting competition inside the EU as their object or effect. Article 102 forbids the abuse of a dominating position inside the EU’s internal market or a significant portion of it.

Furthermore, each Member state must establish rules for other penalties for regulation violations that are not already covered by Art. 83. These are most likely criminal penalties for certain GDPR violations or penalties for violations of national rules based on GDPR flexibility clauses. National penalties must also be effective, proportionate, and deterrent in nature. (intersoft consulting, 2018)

4. Section 3: Chief Information Security:

4.1. Prevention of data breach

As the company’s Chief Information Security Officer(CISO) of the company I would take several preventative measures to prevent a ransomware attack and ensure

that any data breaches are minimized. Here are some alternative steps that could have been taken:

Regular security audits: Security audits should be performed on a regular basis to detect and correct potential vulnerabilities in the company's systems and processes. This contributes to ensuring that security is effective up to date.

Employee education and training: Employees should be taught on the threat of cyber attacks, how to detect them, and how to prevent them. This could include regular data security training sessions and workshops.

Data security policies should be implemented: The organization should have policies in place that describe rules and procedure for handling sensitive data. These regulations should be covered to employees explicitly and enforced through frequent audits.

Update and patch systems on a regular basis: Keeping systems up to speed with the most recent security patches and upgrades can help prevent known vulnerabilities from being exploited by attackers.

Backup your data on a regular basis: To guarantee that it is recoverable in the case of a data breach or other tragedy. It can also protect against data loss caused by system faults.

Overall, when implemented effectively, the steps mentioned earlier can significantly reduce the likelihood of a data breach occurring within the company.

4.2. Preventive measures

A strong password policy is one of the preventative measures I may implement to prevent data breaches or identity theft.

Here are some more examples:

- Limit access to sensitive data: Only offer access to personnel who need it to complete their tasks, and evaluate access privileges on a regular basis to verify they are still needed.
- Use multi factor authentication: To access sensitive data, require extra forms of identity, such as fingerprint or security token.
- Data encryption: I would use data encryption to safeguard sensitive data in transit and at rest. Even if an attacker gained network access, this would prohibit unlawful data access.
- Technology and security policies must be implemented and enforced: Create data and technology rules and procedures, and then enforce them throughout your firm.
- Train employees on cybersecurity : Employees should be trained on cybersecurity and data protection best practices, such as safe password management, email management, avoiding phishing scams, and handling sensitive information.

The organization may considerably lower the danger of a data breach and secure its important assets by employing these precautionary steps.

4.3. What measures should I take for it not to happen again?

IF a data breach has already occurred, it is critical to act quickly to mitigate the damage and prevent it from happening again. Here are some actions I can take:

- Conduct an extensive investigation: Determine how the data breach occurred, what information was exposed, and who may have been affected. This will help avoid future data breaches by detecting and addressing weakness in your system.

- Change all password: Immediately change all of your passwords, and use strong, unique passwords for each account. Passwords should not be reused, and common names, dates, or phrases should be avoided.
- Enable encryption: Enable encryption for your sensitive data to prevent unauthorized access to the data in plain text.
- Implement security measures: To detect and block any suspicious activity in real time, use security methods such as multi-factor authentication, intrusion detection, and monitoring.
- Review and update your security policies: Make sure that your privacy policies, security procedures, and incident response plans are up to date and effective by reviewing and updating them.
- Monitor network activity: I would use monitoring tools to keep track on network activity and discover suspicious behavior in real time. This would aid in detecting and preventing breaches before they do substantial damage.
- Evaluate Third-party contracts: If the breach was caused by a third-party vendor, I would evaluate the vendor's contracts to confirm that they are fulfilling the company's security standards and, if necessary, take extra safeguards.

By adopting these precautions, you may reduce the likelihood of future data breaches and protect your organizations sensitive information.

5. Conclusion

At last, the ransomware attack on Acer emphasizes the significance of strong security measures to protect sensitive data. Companies must take the appropriate precautions to protect their systems from unwanted access and keep their software up to date. In the event of a data breach, business must notify the appropriate authorities and affected customers, as well as take action to avoid future assaults.

I discovered the importance of proactive measures in preventing cyber assaults through our research, such as setting strong password restrictions, routinely updating software, and educating personnel on cybersecurity best practices. I've also learnt about the role of national and international regulatory organizations in investigating and fining corporations that commit data breaches.

It would be my role as Chief Information Security Officer to guarantee that the organization is taking proactive efforts to avoid cyber attacks and protect personal data. This entails creating a complete cybersecurity plan, conducting frequent risk assessments, and offering ongoing personnel training and education.

Overall, the importance of cybersecurity for enterprises and individuals alike is emphasized in this reach, as is the necessary for proactive actions to avoid cyber assault and secure personal data. We may help to lessen the risk posed by cyber threats and maintain the safety and security of our personal and commercial data by taking the appropriate safe guards and remaining vigilant.

6. References

- FORTRA*. (2018). Retrieved from Core Security : <https://www.coresecurity.com/threat-detection/cyber-attacks/ransomware>
- Gatlan, S. (2021). *Bleepingcomputer*. Retrieved from Bleepingcomputer: <https://www.bleepingcomputer.com/news/security/accenture-confirms-data-breach-after-august-ransomware-attack/>
- Morgan, L. (2021). *Cyber Security Hub*. Retrieved from Cyber Security Hub: <https://www.cshub.com/executive-decisions/articles/accenture-faces-50-million-ransom-demand>
- Morgan, L. (2021). *Cyber Security Hub*. Retrieved from Cyber Security Hub: <https://www.cshub.com/executive-decisions/articles/accenture-faces-50-million-ransom-demand>
- Greig, J. (2021). *ZDNet*. Retrieved from ZDNET: <https://www.zdnet.com/article/acer-confirms-second-cyberattack-in-2021/>
- HOPE, A. (2021). *CPO MAGAZINE*. Retrieved from cpomagazine: <https://www.cpomagazine.com/cyber-security/acer-reportedly-suffered-a-revil-ransomware-attack-attracting-the-highest-ransom-demand-in-history-of-50-million/>
- Roberts, D. M. (2021, March 30). *ID Strong*. Retrieved from ID STRONG: <https://www.idstrong.com/sentinel/acer-computer-giant-hit-hard-by-revil-ransomware---50-million-ransom/>
- Trend Micro*. (2016). Retrieved from Trend MICRO: <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/aligning-with-the-gdpr-data-breach-prevention-and-notification>
- Chin, K. (2023, March 02). *UpGuard*. Retrieved from Up Guard: <https://www.upguard.com/blog/what-should-companies-do-after-a-data-breach#:~:text=Once%20the%20data%20breach%20has,additional%20questions%20regarding%20the%20situation.>

- chin, K. (2023). *up guard*. Retrieved from Upguard: <https://www.upguard.com/blog/what-should-companies-do-after-a-data-breach#:~:text=Once%20the%20data%20breach%20has,additional%20questions%20regarding%20the%20situation.>
- intersoft consulting*. (2018). Retrieved from intersoft consulting: <https://gdpr-info.eu/issues/fines-penalties/>
- paloalto networks*. (n.d.). Retrieved from Paloalto Networks: <https://www.paloaltonetworks.com/cyberpedia/what-is-ransomware-as-a-service>
- Kerner, S. M. (2021). *Tech Target*. Retrieved from TechTarget: <https://www.techtarget.com/whatis/definition/ransomware-as-a-service-RaaS>
- Trend Micro*. (2021). Retrieved from TrendMicro: <https://www.trendmicro.com/vinfo/us/security/definition/ransomware-as-a-service-raas>
- Gatlan, S. (2021, October 21). *BLEEPINGCOMPUTER*. Retrieved from BLEEPING COMPUTER: <https://www.bleepingcomputer.com/news/security/accenture-confirms-data-breach-after-august-ransomware-attack/>
- Abrams, L. (2021, March 19). *BLEEPINGCOMPUTER*. Retrieved from BLEEPING COMPUTER: <https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/>
- TechTargey*. (2021). Retrieved from LEMAGIT: <https://www.lemagit.fr/actualites/252498175/Cyberattaque-une-rancon-de-50-millions-de-dollars-demandee-a-Acer>
- Mathews, L. (2021). *Forbes*. *Acer Faced with ransom up to \$100 million after breach networks*.
- Gantenbein, K. (2020, November 13). *ExtraHop*. Retrieved from ExtraHop: <https://www.extrahop.com/company/blog/2020/ransomware-explanation-and-prevention/>

- Nair, P. (2021, October 18). *BANK INFO SECURITY*. Retrieved from Bank Info Security: <https://www.bankinfosecurity.com/acer-taiwan-india-hit-in-2nd-3rd-attacks-2021-a-17754>
- Chipeta, C. (2021, October 18). *UpGuard*. Retrieved from Up Guard: <https://www.upguard.com/news/acer-desorden-data-breach>
- hope, A. (2021, March 23). *CPO MAGAZINE*. Retrieved from CPO MAGAZINE: <https://www.cpomagazine.com/cyber-security/acer-reportedly-suffered-a-revil-ransomware-attack-attracting-the-highest-ransom-demand-in-history-of-50-million/>
- Gantenbein, K. (2020, November 13). *ExtraHop*. Retrieved from Extra Hop: <https://www.extrahop.com/company/blog/2020/ransomware-explanation-and-prevention/>
- Toohil, R. (2021). *Aura*. Retrieved from Aura: <https://www.aura.com/learn/what-is-a-data-breach>
- Din, A. (2023). *Heimdal*. Retrieved from Heimdal: <https://heimdalsecurity.com/blog/companies-affected-by-ransomware/>

7. Appendix:

Acer has announced a 60GB data loss caused by a cyber attack on its Indian headquarters, the multinational technology and electronics company's second big leak this year. The original attack on Acer India's servers was most likely carried out by the hacker organization Desorden on October 5, 2021, accordingly to the most current date seen in the exposed database. Privacy Affair's first revealed the vulnerability on October 13, 2021 (Chipeta, 2021)

Acer acknowledged to information security media group that on Oct. 14, it detected an isolated intrusion on its local after-sales service system in India involving user data, and that it is altering all possibly affected customers. The threat actors claimed in a famous hacker forum that they had stolen 60 GB of files and databases from Acer's India-based servers. According to Acer, this comprises customer, company, account, and financial information. "When we discovered it, we immediately activated our security protocols and ran a full system scan." "We are informing all possibly impacted consumers in India, and the breach in the Taiwan system does not include customer data," said Acer representative Steven Chung to ISMG. The hacker forum note also claims to have access to over 3,000 login detail sets for Acer's resellers and distributors in India (Nair, 2021).