Analysis of the Data Breach at NordTech Solutions

Student Name: Zaid Al Jaderi

Course Name: Security and Law

Date: September 13, 2025

Table of Contents

1. Introduction

In a world under 2025, the digital economy for both smaller and larger companies has become dependent on various digital services, this applies to both data-driven services and other solutions. *As UNCTAD (2025) highlights, "Globally, the growth has been driven by expanding digital services, rising demand for software solutions and emerging tech talent and start-up ecosystems".* These solutions are today practically the norm for companies, where most are moving to digital services, such as cloud-based solutions. But since the world today uses digital systems, the increased use in recent times has brought not only opportunities but also risks, these risks, especially when it comes to personal data and other sensitive information, need to be handled and protected more effectively.

Something companies need to consider are the significant consequences for the various customers they have, since data breaches today are very common, and they can lead to several consequences for both these customers but also economic losses, other repercussions such as damaged reputation for the company, legal consequences, but also for their business operations.

With that said, this report will attempt to analyze a realistic scenario. The scenario and the report will be about NordTech Solutions, which is a fairly medium-sized IT company in Norway, where the scenario is that the company is exposed to a data breach. This data breach occurs through a phishing attack, which compromised login credentials from an employee who is senior with them.

Through this intrusion by the attacker, both personal information from their customers was stolen, but also financial information was stolen. Because of this occurrence, there are consequences for the company which are both ethical as well as legal problems that they must consider.

The purpose and idea of this report is to create a complete analysis of this incident, and the focus will be on four different main areas as a starting point: First and foremost, compliance with NIS2 and GDPR, ethical responsibilities, but also the legal aspect. The final outcome will lead to recommendations for the company NordTech and how they can minimize risks for this to happen again, but also how they should strengthen their security and try to rebuild customer trust.

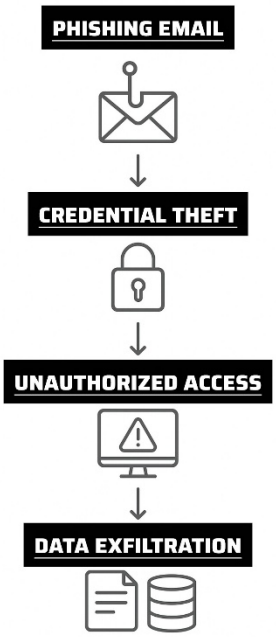
2. Description of the incident

NordTech Solutions' own IT security team detected unusual activity in their network, this happened at the beginning of February 2025. By analyzing this activity, it turned out that a senior employee had unintentionally shared their own login credentials, this happened via a phishing attack that created this problem. Those who hacked the senior’s credentials then gained unauthorized access to NordTech’s internal systems and were able to steal several personal details about their customers.

The data that was stolen concerned not only addresses but also customers and their names, contact information. Even information about customers’ financial details was stolen, such as partial bank information but also their invoices.

These consequences were not only significant, they were harmful: NordTech's customers were exposed to several risks such as financial fraud, risks around identity theft. This damaged the company's reputation significantly, and authorities had to get involved, precisely because of the scope and sensitive information that was exposed for these customers.

NordTech had to face drastic and immediate challenges here, both regarding their reporting, security, and also their customer communication, in order to prevent further future intrusions. This incident proves how serious it is and what consequences accompany a data breach, where the company handles a lot of sensitive information that gets stolen.



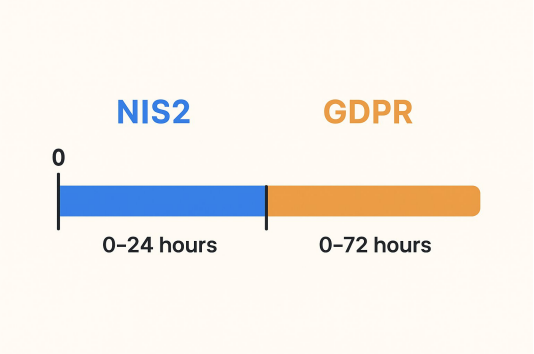
(Al Jaderi, Z. (2025). Illustration of attack chain – phishing email → credential theft → unauthorized access → data exfiltration, generated using ChatGPT. Unpublished image.)

3. GDPR and NIS2 Compliance

Since NordTech Solutions offers not only cloud services but also IT solutions to various companies, both for larger companies, medium-sized, but also small ones, the company is covered not only by GDPR but also the NIS2 directive. This is important for the company to know and comply with.

3.1 Reporting of Incidents

According to GDPR, a report must be submitted to the supervisory authority within 72 hours after the team has discovered the breach, and this is stated in Article 33. As it clearly states, *"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it" (GDPR-info.eu, n.d.).* Not only that, if the incident and breach pose a high risk to individuals' rights or even their freedom, it is mandatory to also inform those affected by the breach, this is written in Article 34. However, the NIS2 directive sets other requirements, where the law states that incidents that could affect information systems or networks must be reported within 24 hours to a relevant authority. So these breaches for NordTech, where there is a breach in their cloud service or their customer data, must be reported much faster than what GDPR determines or requires. Since NordTech is in Norway, this must be reported to Nasjonal sikkerhetsmyndighet (NSM). As it stands on NSM website, *"The agency's mission is to strengthen Norway's ability to counter espionage, sabotage, terrorism and hybrid threats" (Norwegian National Security Authority, n.d.).*



(Al Jaderi, Z., 2025. Timeline – 0–24 hours (NIS2) vs 0–72 hours (GDPR) [diagram]. Generated using ChatGPT. Unpublished image.)

3.2 Data Protection Impact Assessment (DPIA)

If we read Articles 35 and 36 of GDPR, it is stated that companies must carry out DPIA when it comes to processing large amounts of sensitive data, and also when planning or implementing new technical solution or solutions. It states, *"A DPIA is required at least in the following cases: processing of sensitive data on a large scale" (European Commission, n.d.).* Since NordTech and its company contain a great deal of customer data in their cloud services, DPIA must be implemented and is needed in

order to assess the risks that exist but also ensure proper protection. If DPIA is missing for the company, this can lead to extremely large penalties that will harm the company.

3.3 Potential Fines

The potential fines that may arise according to GDPR, or that may lead to fines, can reach 20 million euros, or also 4 percent of global annual turnover, this is calculated and depending on which is highest applies. NIS2 on the other hand also enables sanctions against a company, if these companies do not meet the requirements that must be applied, such as reporting and security requirements. This means that companies can be subject to both administrative measures but also financial penalties.

3.4 Recommended Actions

What NordTech must do is the following:
They must immediately report the incident to both NSM and also the Data Protection Authority, this according to the respective regulations.
The affected customers must be informed about the breach and its scope as well as risks.
They must also document the entire incident and the breach completely, both the affected data and the actual attack path, but also the corrective measures that were taken.
They must immediately carry out DPIA for their cloud services if these have not already been activated or done.
They must also directly implement security measures that follow the principle of “data protection by design and by default.” In addition, they must apply the requirements that NIS2 demands regarding risk management and resilient networks.

4. Security Policies

This breach shows the shortcomings NordTech has, both the existing security policies but also their implementations.

4.1 Evaluation of current policies

Their authentication: NordTech relies on simple logins, in other words single-factor login, which makes it much easier for unauthorized access.

Failure of training, the breach could partly happen precisely because they did not have sufficient training regarding phishing training for respective staff.

How they handle incidents, their process was reactive rather than preventing it from happening, this indicates the lack of monitoring and also more early warning systems.

4.2 Recommended improvements

1. An implementation of MFA for all their systems.
2. More regular training in security and including phishing simulations.
3. They must also have Zero-Trust, where access must constantly be controlled.
4. More clear response plan for breaches, and clear roles for it, also clearer communication paths and how it is handled during escalation.
5. It is important that they also carry out penetration tests and security reviews by other external experts.
6. They must have cloud security, also role-based access control and constant monitoring, but also encryption.
7. They must also have a simulation of 24-hour reporting, in order to be able to meet the requirements from NIS2.

(Al Jaderi, Z. (2025). Illustration of layer protection model – MFA → training → monitoring → incident response, generated using ChatGPT. Unpublished image.)

5. Ethics and Codes of Conduct

The company NordTech has, in addition to the legal obligations, also an ethical responsibility for its customers, but also for its partners. By having ethical management when it comes to data breaches, it means that the company must show transparency, responsibility, and also proactive measures, in order to minimize the damages that may arise.

5.1 Ethical obligations

Transparency: This is to inform about the scope of the breach and its consequences.
Responsibility: Immediately take full responsibility for shortcomings in security policies of the breaches that occur.
Proactive support: This is extremely important to be able to offer protection such as identity monitoring, as well as advice to the affected customers who have been exposed to breaches.

5.2 The company's code of conduct

• Protect data integrity and confidentiality as core values.
• Clear guidelines for employees' reporting of security incidents.
• Clarify management's responsibility in crisis management and incidents.

6. Cybercrime and Legal Aspects

This data breach constitutes not only a cybercrime under Norwegian law but also under international regulations.

6.1 Nature of the crime

This attack is unauthorized access to information systems which is included in the Norwegian Penal Code §205. This also includes other theft such as financial fraud or even theft of data. The incident also violates NIS2 and GDPR, so this breach can also lead to administrative liability.

6.2 Consequences for the attackers

This attack and the attackers who carried out this breach can face strong legal

actions, which can also result in imprisonment. If the attackers are not in Norway and live/are located outside Norway, international cooperation can occur, therefore according to the Budapest Convention they can still be held accountable.

6.3 Consequences for NordTech

This attack can have criminal consequences for NordTech, this can mean administrative sanctions but also potentially result in fines according to NIS2 and GDPR. The company can also receive complaints as well as claims from the customers affected by this attack. NordTech may also be forced to fix the problems and also document everything they have addressed and be able to prove it, as required by authorities.

7. Conclusions and Recommendations

The breach that occurred at NordTech not only shows the risks associated with cybersecurity but also the complex risks that exist, it also shows the importance of legal compliance and the ethical responsibilities that must be upheld in 2025 and its IT environment. This breach not only exposed the company's sensitive information but also revealed several different shortcomings that the organization had/has.

Summary:

The attack affects several important areas:

1. NIS2 and GDPR: NordTech must immediately report data breaches, but also carry out DPIA, as well as report these breaches and these critical incidents within 24 hours, which is a requirement from NIS2. If this does not happen, the company can face significant fines that can negatively impact the company.
2. Security shortcomings: Their lack of training for their staff on phishing attacks, and insufficient reactive approach to breaches has definitely contributed to

their vulnerability. Also, the lack of multi-factor authentication (MFA) has proven to be a cause.

3. Ethical responsibility: NordTech needs to improve in showing accountability, also demonstrate transparency but provide proactive protection for its customers.
4. Legal aspect: Those who carry out the attack against the company, as well as the company itself, can be held accountable for what occurs. This can result in several consequences, such as penalties like fines or even claims from their customers.

Recommendations:

To improve security and strengthen it, NordTech should implement multi-factor authentication and a strict zero-trust architecture. NordTech should create more clarity by establishing a clear incident response plan, as well as regularly practicing reporting, and being able to report these incidents within 24 hours according to NIS2.

The company should also implement more regular training in security and phishing simulations for its staff; this is extremely important to prevent future breaches or attacks. The company also needs to review regulations and ensure ongoing compliance with NIS2 and GDPR, through careful documentation of all types of security measures that can be carried out and applied.

The company can also openly commit to protecting its customers' data; this shows that they take responsibility and can regain customer trust, as well as explain the measures they have implemented for this. By addressing all of this, these actions can get NordTech back on its feet and even turn this crisis into an opportunity to prove that they have significantly improved their security.

This can demonstrate accountability and also establish themselves as a reliable provider in 2025.

8. Reference

European Commission, n.d. When is a Data Protection Impact Assessment (DPIA) required? Available at: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en (Accessed: 13 September 2025).

GDPR-info.eu, n.d. Article 33 – Notification of a personal data breach to the supervisory authority. Available at: https://gdpr-info.eu/art-33-gdpr/ (Accessed: 13 September 2025).

Norwegian National Security Authority, n.d. About the Norwegian National Security Authority. Available at: https://nsm.no/about-nsm/about-the-norwegian-national-security-authority/ (Accessed: 13 September 2025).

UNCTAD, 2025. World Investment Report 2025: International Investment in the Digital Economy. Geneva: United Nations. Available at: https://unctad.org/publication/world-investment-report-2025 (Accessed: 13 September 2025).