Interreg Baltic Sea Region

Co-funded by the European Union

RESILIENT ECONOMIES AND COMMUNITIES

CAIDX

CAIDX TOOL #2

SECURE DATA

- Experiences from the last five years and predictions for the future

A handbook for laymen to facilitate their work on AI in the healthcare and to efficiently communicate with data security/IT experts

Table of Contents

Introduction **3**

Report Sources **4**

Extent of Data Breaches **5**

Target Sectors and Societal Impact **6**

The Nature of Attacks – Modus Operandi **7**

Protective Measures **11**

Educational programs *11*

Background checks of associates *11*

IT Assessment Management (ITAM) *11*

Preventive technical recommendations *12*

Monitoring *12*

Incident Response Plan (IRP) *13*

Encryption *14*

DevSecOps Approach *15*

Paying Ransom **17**

Data Storage **19**

On-premise server solutions *19*

Cloud-based server solutions *19*

Summary **22**

Introduction

After being introduced as a military project for information transfer in 1969 by the Defense Advanced Research Projects Agency arch Projects Agency – The APRANET, the first e-mail sent 1971 and the subsequent first introduction of a web-page by Tim Berners-Lee at CERN August 6, 1991 the world has stayed connected. The opportunities have expanded beyond everyone's belief at the time of introduction, boosting development, making a lot of new developments not only more efficient, but also what was impossible possible.

Even before the introduction of internet, John von Neumann of the University of Illinois introduced the concept of Automata, self-replicating programs. John von Neuman later constructed the first computer virus. In fact, the first detected computer virus, the Creeper virus, was detected on the internet forerunner APRANET, making computer viruses older than public internet itself. The computer viruses thus presented themselves as the first threat on internet. Soon, viruses were vectors for data breaches and is one of the many routes to take control, copy, steal data and finally even cryptate data and giving grounds for black mailing.

As internet is an integrated part of healthcare data structures, they are at risk for cyberattacks; a risk which can be mitigated but not completely depleted. The current report is the work under the CAIDX consortium funded under EU Interreg and is intended to serve as a supportive tool to introduce AI developers, users and administrators within healthcare to help administrate their efforts minimizing the risk of data breaches and to reduce the risk of harm to the patients and healthcare systems.

While the report is intended to minimize direct risks it also, as importantly, intends to increase the awareness of alterative risk assessment. What are we causing or what consequences does it have to avoid the risks we try to avoid by not pursuing data sharing and AI development and implementation.

The main objective is to summarize current experiences in laymen terms to facilitate insight of the problem and facilitate communication between laymen and experts.

Report Sources

The current work is based on five leading international reports, published between 2020-2024 (references 1-5) and six articles, published between 2021-2025 (references 6-11).

1. Verizon: Data Breach Investigations Report, 2023. https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf
2. Ponemon Institute LLC, sponsored by IBM Security: Cost of a Data Breach Report, 2023.
3. Gov.uk: Cyber security breaches survey, 2023. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023
4. Ernest Young: Cybersecurity: How do you rise above the waves of a perfect storm? 2021. https://www.ey.com/en_cn/insights/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm
5. ENISA: Artificial Intelligence Cybersecurity Challenges, 2020. https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
6. CrowdStrike: 10 malware detection techniques, 2023. https://www.crowdstrike.com/en-us/cybersecurity-101/malware/malware-detection/
7. Amatas: Top Malware Detection Techniques – Key Methods Explained, 2025. https://amatas.com/blog/top-malware-detection-techniques-key-methods-explained/
8. RedHat: What is DevSecOps? 2023. https://www.redhat.com/en/topics/devops/what-is-devsecops
9. Microsoft: What is DevSecOps? 2025. https://www.microsoft.com/en-us/security/business/security-101/what-is-devsecops
10. National Defence Magazine: Ethical Legal Implications of Paying Ransoms, 2021. https://www.nationaldefensemagazine.org/articles/2021/8/17/ethical-legal-implications-of-paying-ransoms
11. Forbes: Why paying ransoms is typically a bad idea, 2021. https://www.forbes.com/councils/forbestechcouncil/2021/07/12/why-paying-ransomware-is-typically-a-bad-idea-and-what-you-can-do-instead/

Extent of Data Breaches

There is an increasing trend of data breaches. The number of data breaches has surged significantly. For instance, 2023 saw a 72% increase in data breaches compared to 2021 and 3,205 publicly reported data compromises affected over 353 million individuals. The increasing number of breaches is accompanied with rising costs. The average cost of a data breach reached an all-time high of $4.88 million in 2024, marking a 10% increase from the previous year. By 2025, the global cost of cybercrime is projected to reach $10.5 trillion, growing at a rate of 15% annually.

Personal integrity has been an increasing concern in a more and more digitalized world and the EU adopted and extensive regulatory package, General Data Protection Regulation (GDPR) in 2016. The data breaches represent a threat to integrity which is confirmed by the fact that 46% of the latest 110 data breaches involved personal identifiable information, such as tax identification numbers, emails, phone numbers, and home addresses.

Target Sectors and Societal Impact

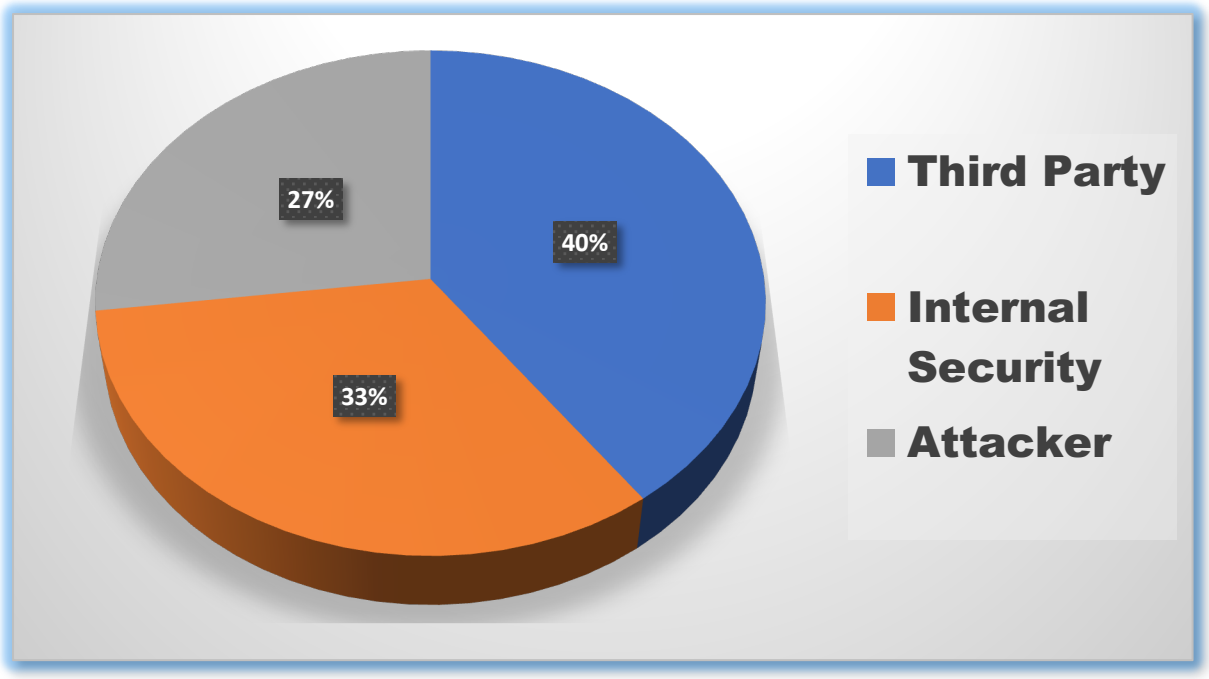
Prime targets are the sectors that represent high value, such as healthcare, financial institutions, retailers, technological companies and government, including educational agencies. The technological companies do represent a category of which much of the competence to resist attacks reside. Still, some of the highest profile companies like Apple, Meta and X were all been affected the last year.

While areas of lesser interest, when it comes to costs generated to data breachers, such as media, communication and hospitality stagnates in interest the most affected sector, healthcare systems, is also the sector where the costs rise most steeply. This is unfortunate for many reasons. Beside the vulnerability and national strategic importance healthcare is a sector where individuals show their greatest vulnerability. In a report from World population review on happiness, one of the aspects that stands out among the top five countries on the list is the access to healthcare. Indicating that a rumbling trust for healthcare is detrimental for trust in society as a whole. **It is therefore instrumental for all countries to protect healthcare.**

The Nature of Attacks – Modus Operandi

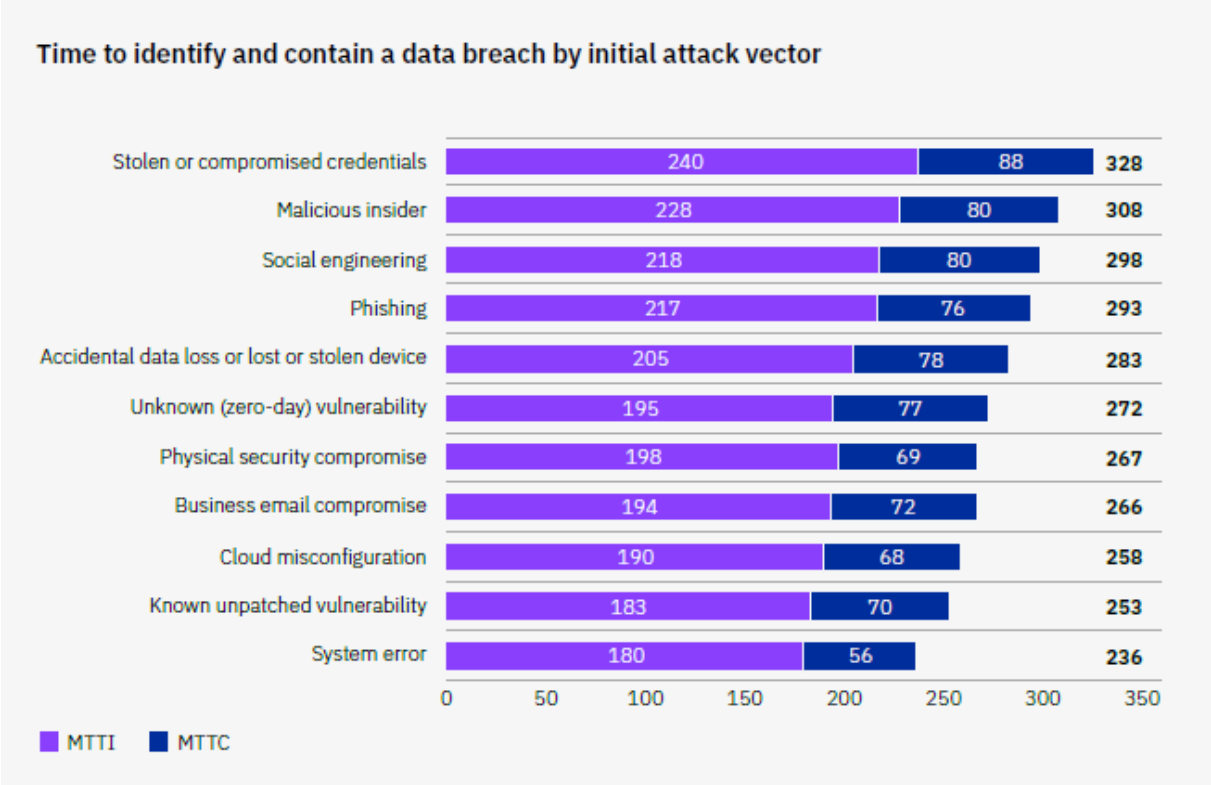
While the attacks have increased the costs and are most commonly inflicting healthcare, the complexity or time to detect and to manage has been practically constant about 280 days for recovery of which 2/3 of the time represents time to detect.

Most commonly, the attack is revealed by actors outside of the organization, either the attackers themselves or benign third parties.



Proportion of parties that reveal the attack (based on Ponemon Institute's "Cost of a Data Breach Report 2023", sponsored by IBM Security).

The most common attack vector is phishing, a type of cyberattack where attackers use deceptive methods to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal details. Stolen credentials, most commonly stolen through phishing, is the most common way to get access to servers. Moreover, attacks through stolen credentials are the hardest to detect, for obvious reasons.



Days to detect a data breach. MTTI = Mean Time to Identify; MTTC = Mean Time to Contain (reprinted with permission from Ponemon Institute's "Cost of a Data Breach Report 2023", sponsored by IBM Security).

Some version of **phishing modalities** are:

1. **Deceptive Emails**: Attackers often send emails that appear to be from legitimate sources, such as banks, social media platforms, or trusted companies. These emails typically contain links to fake websites designed to steal information.

2. **Fake Websites**: The links in phishing emails lead to websites that mimic the appearance of legitimate sites. These fake sites prompt users to enter their credentials or other sensitive information.

3. **Urgency and Fear**: Phishing messages often create a sense of urgency or fear, urging recipients to act quickly to avoid negative consequences, such as account suspension or unauthorized transactions.

4. **Personalization**: Some phishing attacks use personalized information to make the messages more convincing. This can include using the recipient's name or other details obtained from previous breaches or social media.

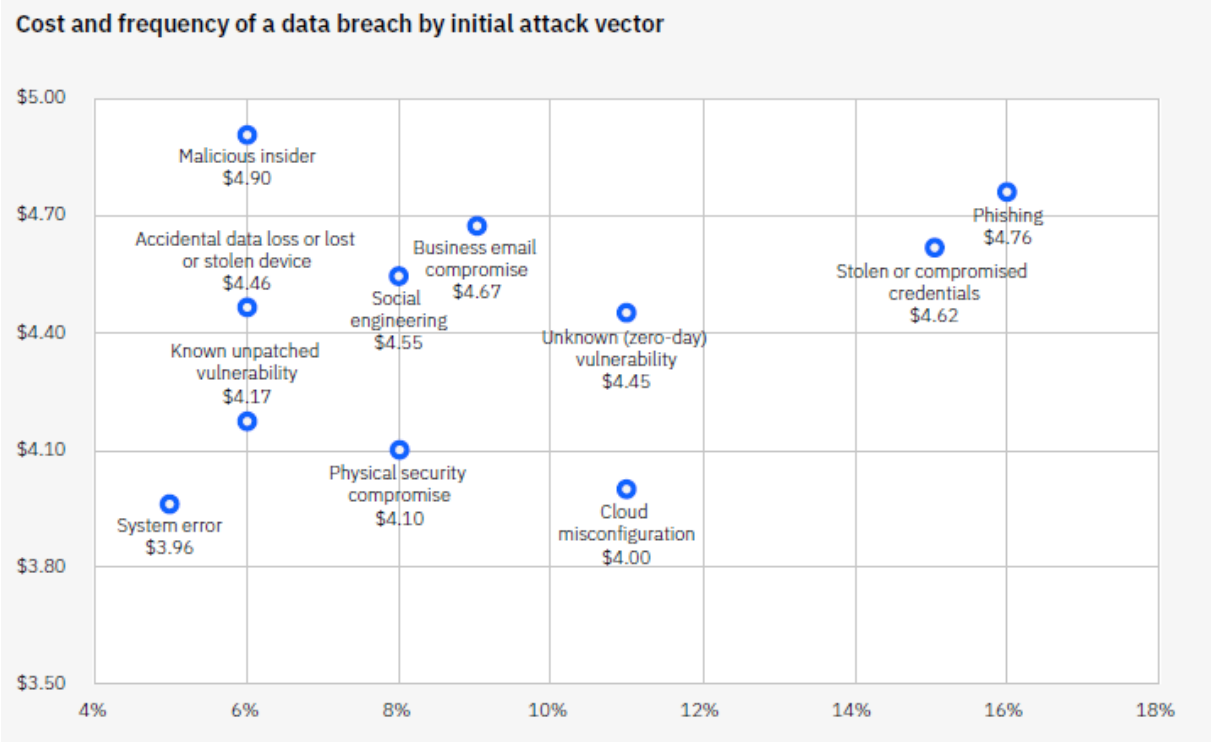
5. **Spear Phishing**: A targeted form of phishing where attackers focus on specific individuals or organizations, often using detailed information to craft highly convincing messages.

Phishing is one of the most common and effective methods used by cybercriminals due to its simplicity and the potential for significant impact. It's important to be cautious with unsolicited emails and verify the authenticity of any requests for sensitive information.

The second-most modality of an attack is **Malware**. It includes viruses, worms, and ransomware, and is highly prevalent. Email is a common vector for malware delivery. Malware encrypting the Data source and then request a ransom to unlock it, is usually referred to as **Ransomware**. **Denial-of-Service (DoS) Attacks**, attacks the functionally of the CPU or server by overload (volume-based attacks), through weaknesses in the network protocols (protocol attacks) or making specific services or application as a target to make them dysfunctional (application layer attacks)

Social Engineering is a third strategy whereby the attacker in an elusive way manipulates the victim to lower or compromising security. Attackers use phishing as described either through phishing (as described above), the more individualized phishing (spear phishing), directed through texting/SMS (Smishing), phone calls (vishing).

Malicious insider is an associate that turns his or her back towards the employer and working as a, or together with, data breachers.



Cost in million USD and frequency of a data breach, by initial attack vector (reprinted with permission from Ponemon Institute's "Cost of a Data Breach Report 2023", sponsored by IBM Security).

Physical harm and infringement: Especially with insiders but also without, physical harm is a real and often underestimated threat. Physical infringement can be administered through **the introduction of local storage devices** such as hidden USB drives of hard drives. **Key loggers** are devices introduced into keyboards reveal keystrokes to reveal logins or sensitive information directly. A third mode of **rogue physical access points** reachable by Wi-Fi or even through SIM-card access.

Protective Measures

Educational programs

To be effective, educational programs need to be *accessible, on demand, compulsory and reoccurring*.

Digital educational platforms represent an efficient way to train associates in how to protect them against attack vectors of different kinds and by being updated regularly, keeping up with the most common threats, ideally 2 – 4 times a year. To ensure the impact on employees at large, trainings should be accompanied with test to pass.

Key contents should encompass:

- Update on historical but also most recent data breached, including consequences and mistakes
- Phishing techniques including social engineering
- How to make and keep your credentials safe

Background checks of associates

It is impossible to completely secure your organization from malicious insiders, but background checks could prevent the most obvious cases. Checkups should in their frequency and to their extent be proportional to the sensitivity of the position of the associate being targeted.

IT Assessment Management (ITAM)

Crucial to protect against, assess and contain/address a cyber-attack is to have a full oversight of which equipment and computers have access to your system, and how your system is configured, including its current security updates. This is crucial to address your attack as forcefully and precisely as possibly.

Preventive technical recommendations

To be able to contain the attack as precisely as possibly, a micro-segmentation put in place ahead of an attack is crucial. That will be part of an Incident Response Plan (IRP; see below). IRP needs to be put under exercise repeatedly.

Monitoring

Time to detect is on average 200 days, according to the IBM's Cost of a Data Breach Report from 2023. The success of the response of an attack is dependent on, among other things, time. Monitor systems for constant monitoring internet traffic is key to success. Intelligence is key to be prepared for attacks even before you have been impacted. Usually, data security staff have access on regular, periodical, security intelligence. As being outlined later, this is one of the major reasons why healthcare data in clouds is safer than *on-premise* servers.

Staff monitoring should be selected in regular checkups by:

- Randomization/sampling
- Users' internet traffic

Monitoring is also a major protection strategy against malicious insiders.

Detection strategies have involved:

- **Signature-Based Detection**: This method uses known digital signatures of malware to identify threats. It relies on a database of known malware signatures to detect and block malicious files.

- **Behavior-Based Detection**: Instead of looking for specific signatures, this approach monitors the behavior of programs and systems to identify suspicious activities that may indicate malware.

- **Anomaly-Based Detection**: This technique involves establishing a baseline of normal system behavior and then detecting deviations from this baseline, which could indicate the presence of malware.

- **Heuristic-Based Detection**: Analyzes the behavior and characteristics of code to detect potential threats.

- **Machine Learning and AI-Based Detection**: Advanced algorithms and artificial intelligence are used to analyze large datasets and identify patterns that may indicate malware. These methods can adapt and improve over time.

- **Sandboxing**: Suspected malware is executed in a controlled, isolated environment (sandbox) to observe its behavior without risking the actual system.

- **Hybrid Detection Techniques**: Combining multiple detection methods, such as signature-based and behavior-based detection, to improve accuracy and effectiveness.

Incident Response Plan (IRP)

When an attack has been identified, it is on average 200 days since the start of the attack. In some of the attacks, ransom attacks in special, time to act is much shorter. A preemptive response plan will shorten the time to contain the attack and thereby minimize the harm.

To have an incidence response plan in place in advance is key to be able to defend yourself without any hesitance it. This plan should clarify/identify:

- The team responsible, down to the individual roles

- How the micro-segmentation is constructed and how it can be managed

- The current strategy to monitor
- The training programs needed, accompanied with the implication of these
- Toolbox and indication for each tool
- How the data network and its servers are being sectioned followed by a
    - Short containment plan (stop the spreading of the breach)
    - Long-term containment plan (further spreading, plan to analyze)
- Reserve system plan/strategies
- Eradication plan with:
    - Root Cause Identification: plan to identify the cause that the attack could impact the system and to eliminate that cause
    - Removal of the malicious code plan: strategy for the removal and eradication of the malicious code
    - Securing Vulnerabilities: to systematically identify weaknesses other than the ones used in the attack and how to eliminate them
- Restoration plan:
    - Strategy for the overall restoration and stepwise (by priority) entering normal operational mode
    - Post incidence test plan: what checks are needed to give clearance for normal operational use

Encryption

Any encryption or pseudonymization or even anonymization will not only make the data less useful for the data breacher, but it will also make it less likely to be harmed when attacked. Thus, only credential-protected patient information is an outdated strategy that gives a suboptimal protection of patients' integrity.

DevSecOps Approach

DevSecOps is the most cost-saving approach when inflicted by an attack. It describes a strategy in which the security practices are included in every phase of software development and where software development includes the later operational partners in the development. It ensures a maximally tailored safety based on the configuration, setting and likelihood of threat that the customer organization phases. It includes:

1. Culture and Collaboration:
    - **Shared Responsibility**: Security is everyone's responsibility, not just the security team's. This cultural shift encourages collaboration among developers, security professionals, and operations teams.
    - **Training and Awareness**: Regular training sessions to keep all team members informed about the latest security practices and threats.

2. Automation:
    - **Continuous Integration/Continuous Deployment (CI/CD)**: Automate the integration and deployment processes to include security checks at every stage.
    - **Security Testing**: Integrate automated security testing tools into the CI/CD pipeline to identify vulnerabilities early.

3. Shift-Left Security:
    - **Early Involvement**: Incorporate security considerations from the initial stages of development, including during planning and design.
    - **Code Reviews and Static Analysis**: Perform regular code reviews and use static analysis tools to detect security issues early in the development process.

4. Continuous Monitoring and Feedback:
    - **Real-Time Monitoring**: Implement continuous monitoring of applications and infrastructure to detect and respond to security incidents promptly.

- **Feedback Loops**: Establish feedback loops to continuously improve security practices based on monitoring results and incident analysis.

5. Compliance and Governance:
    - **Policy Enforcement**: Ensure that security policies and compliance requirements are enforced throughout the development lifecycle.
    - **Audit and Reporting**: Maintain detailed logs and reports to demonstrate compliance with security standards and regulations.

6. Incident Response:
    - **Preparedness**: Develop and regularly update an incident response plan to handle security breaches effectively.
    - **Post-Incident Analysis**: Conduct post-incident reviews to learn from security incidents and improve future responses.

By integrating these practices, DevSecOps aims to build secure software more efficiently and effectively, reducing the risk of vulnerabilities and enhancing overall security posture.

Paying Ransom

The ever-returning question about ransomware attacks is whether you should pay ransom or not.

The problem has several aspects – one being of course the costs and consequences of having your system brought down. But even if you pay ransom there are considerable post-incidence costs related to re-securing your data and data environment to ensure that your data haven't been corrupted. Your environment needs to undergo similar changes and assessments as if you wouldn't have paid the ransom. Therefore, as established in the IBM Cost of a Data Breach Report from 2023, the costs of a ransomware incident, not taking the costs of the ransom sum itself, are similar whether you pay ransom or not. In addition, if you pay ransom, you make you even further vulnerable to new attacks because:

1. **Encouragement**: Paying the ransom signals to attackers that their tactics are effective and profitable, encouraging them to continue targeting you or other victims.

2. **Repeat Attacks**: Once attackers know you are willing to pay, they may target you again, either immediately or in the future, with the expectation that you will pay again.

3. **No Guarantee**: There's no guarantee that paying the ransom will result in the recovery of your data. In some cases, attackers may not provide the decryption key, or they may leave malware behind for future attacks.

4. **Funding Criminal Activities**: Paying the ransom funds criminal enterprises, enabling them to enhance their tools and techniques, making future attacks more sophisticated and widespread.

5. **Legal and Ethical Concerns**: Depending on the jurisdiction, paying a ransom may have legal implications, and it raises ethical concerns about supporting criminal activities.

In summary, you should avoid paying any ransoms because of a ransom attack.

Data Storage

On-premise server solutions

In general, on-prem servers have been perceived as the safer strategy for your data. This generally relies on several assumptions: your server is located in an underground vault behind heavy steel doors, heavily guarded and has no connection to internet and even more important, no ports at all, not even VPN for people in your organization to connect to the data server.

However, this is almost never true, simply because it doesn't make your data usable. Instead, on-prem servers are connected to the internet and VPN tunnels are widely provided to associates within your organization. Then functionally, you have created a uni-located cloud relying solely on your local security team's competence and access to fresh cyberattack intelligence. The later comes, at its best, in regular but periodical, updates. Local on-prem server environments are rare in high security environments.

With growing businesses, such as healthcare, especially relying more and more on machine learning, you need to upgrade your storage capability in steps, and each step being a costly investment. Thereby, leaving the users with a constant need of over-capacity.

Cloud-based server solutions

Several technical solutions are being provided by the market. All relying on that your data is encrypted, beyond the cloud provider's capabilities to decrypt the data. In healthcare solutions there is therefore a gain only by the fact that the data is pseudonymized and then encrypted.

Clouds do offer benefits beyond these.

1. Enhanced Security:
    - **Advanced Encryption**: Cloud providers use robust encryption methods to protect data both in transit and at rest, ensuring that only authorized users can access it.
    - **Regular Updates**: Cloud services are regularly updated with the latest security patches and features, reducing vulnerabilities.
    - **24/7 Monitoring**: Cloud providers offer continuous monitoring and advanced threat detection to quickly identify and respond to potential security incidents.

2. Scalability:
    - **Elastic Resources**: Cloud storage can easily scale up or down based on your needs, without the need for significant upfront investment in hardware.
    - **Flexible Capacity**: You can adjust storage capacity as your data requirements change, ensuring you only pay for what you use.

3. Cost Efficiency:
    - **Reduced Maintenance Costs**: Cloud storage eliminates the need for physical hardware maintenance, reducing overall IT expenses.
    - **Pay-as-You-Go**: Many cloud services offer a pay-as-you-go model, allowing you to manage costs more effectively. You don’t need to upgrade yourself and only use for storage you use.

4. Accessibility and Collaboration:
    - **Remote Access**: Data stored in the cloud can be accessed from anywhere with an internet connection, facilitating remote work and collaboration.
    - **Real-Time Collaboration**: Cloud platforms enable multiple users to work on the same files simultaneously, improving productivity and teamwork.

5. Disaster Recovery:
    - **Redundancy**: Cloud providers store data across multiple servers and locations, ensuring data redundancy and availability even in the event of a hardware failure.
    - **Backup and Recovery**: Automated backup and recovery solutions in the cloud help protect against data loss and ensure quick restoration.
    - In summary, clouds are superior to on-premise servers with regards to protection against physical threats.

6. Compliance and Governance:
    - **Regulatory Compliance**: Many cloud providers offer compliance with industry standards and regulations, helping organizations meet legal and regulatory requirements.
    - **Audit Trails**: Cloud services often include detailed logging and audit trails, making it easier to track data access and modifications.

7. Environmental and sustainability issues:
    - **CO_2 neutrality:** As of today, Google cloud and Microsoft Azure are cloud providers that are CO_2 neutral.
    - Microsoft Azure claim negative CO_2 balance by 2035, which remains to be seen.

Summary

Some important points are:

- Cyberattacks on healthcare data is an increasing problem
- Healthcare is among the most information sensitive targets
- The great importance of access to data within healthcare makes the healthcare sector one of the prime targets for attacks
- Main initial vector is through stolen credentials and phishing
- DevSec, Staff training, AI and IRP are some of the key protective strategies
- IRP in place will shorten time to identify and contain as well as getting the system up safely again
- Clouds impose an increased cost on recovery, but to the same extent as remote work force do to an on-premise solution
- A high security (including the encryption and pseudonymization) cloud is the safest solution
- Malicious insider a significant problem
- Hybrid warfare is a reality of today