



NEGLECTING DATA SECURITY WHAT YOU RISK

Ignoring Data Security Carries Risks

The proliferation of data for businesses and individuals has upped the ante for data security, making it a critical piece of all security strategies. Organizations often focus their time and budget on physical and network security, unfortunately ignoring the major tenets of data security. This negligence can place groups in precarious situations where their data is vulnerable, putting their businesses and customers at risk.

The traditional approach to cybersecurity often resembles a 13th-century castle — strong perimeter defenses but vulnerable once breached. This approach is like building towering walls and deep moats, but leaving the treasure vault unlocked.

A more effective strategy takes a layered approach that combines hardware, firmware, and software. Let's take a closer look at each of the layers.

1. Confidentiality



Confidentiality stands as one of the most wide-ranging considerations we must take into account; it is not just about erecting digital walls, but is also about safeguarding the crown jewel: your data.

At a high level, confidentiality refers to the protection of sensitive data — such as personal details, financial information, or intellectual property — from unauthorized access or disclosure. While this may seem obvious, it is often overlooked even by the most well-known companies in the industry. For example, the [2017 Equifax data breach exposed](#) the personal financial information of more than 100 million individuals. A vulnerability in Equifax's web application framework enabled hackers to gain unauthorized access to the systems of those people.

A prominent technique to ensure data confidentiality is access controls: barriers that regulate who can access specific data, and subject to particular circumstances. On one hand, you have physical access controls, which refer to tangible measures — measures which prevent unauthorized physical access to sensitive areas where

data is stored or processed. On the other hand, logical access controls are based on the digital aspect of access, such as password protection and multi-factor authentication.

Like vault doors within your castle, you can employ encryption — the process of converting plain text or other forms of data into a coded version. This makes data unreadable to anyone without the proper decryption key.

Ultimately, secure data communication requires a combination of encryption, secure protocols, and authentication measures to ensure that data remains inaccessible to unauthorized parties. Protocols like Secure Sockets Layer (SSL) and Transport Layer Security (TLS) serve as the guarded pathways within the castle, ensuring that data remains inaccessible to potential eavesdroppers during transmission.

2. Integrity



Data integrity is akin to the art expert ensuring your Rembrandt isn't a forgery: it ensures information is accurate, consistent, and reliable throughout its lifecycle.

This means that data is to remain unaltered and uncorrupted, maintaining its original form without unauthorized changes. Additionally, data integrity requires the information to be verifiable, allowing for validation of its accuracy and consistency. Together, these principles form the foundation of trustworthy information systems, supporting accurate decision-making and standards compliance.

One real-world example in which data integrity was overlooked is the [2017 Barts Health NHS Trust exploit](#). A flaw in the hospital's database system caused data to be overwritten incorrectly. This resulted in a loss of data integrity, and patient records were altered or lost. The hospital, with no way to verify that the records were still accurate, needed to cancel hundreds of operations and appointments, delaying treatment for many patients.

To ensure that the data entered into a system is accurate and conforms to specified formats or standards, companies employ data validation as an integrity countermeasure. Forms of data validation include checksums (i.e., utilizing mathematical algorithms to verify data integrity), digital signatures (i.e., employing cryptographic techniques to authenticate the data and its source), and access control (i.e., implementing restrictions on who can access or modify data).

3. Availability



Data availability ensures that the data, like the crown jewel, is accessible when needed but securely stored away otherwise. This is among the core principles of information security, often paired with confidentiality and integrity.

Consider the [Amazon Web Services \(AWS\) incident in 2012](#). On October 22, 2012, AWS experienced a significant outage in one of its major data centers located in northern Virginia. The outage made customer data unavailable and affected several high-profile services that relied on AWS for their operations, including Netflix, Reddit, and Pinterest.

To ensure availability, it is good practice to have backup and disaster-recovery mechanisms in place to restore data in case of accidental loss or catastrophic failure. This could include high-availability systems that minimize downtime through the use of failover clusters and load balancing, much like designing multiple escape routes within a castle.

Other options include implementing redundant storage, where multiple copies of data are stored in different devices or locations to ensure continuous access even if one storage component fails. In some cases, storage may even be geographically dispersed to protect against regional disasters.

4. Compliance



Compliance is the legal framework that governs the data, ensuring that an organization adheres to a set of specified rules or regulations which are often mandated by government or industry-specific guidelines. Failure to comply is akin to breaking the law, with penalties and legal actions.

In 2018, British Airways suffered a significant data breach in which hackers intercepted sensitive information from more than half a million customers. Later investigations would reveal that the security system was in breach of the General Data Protection Regulation (GDPR).



Specific data protection regulations that help ensure compliance include:

- » **GDPR (General Data Protection Regulation):** EU regulation for data protection and privacy, mandating how personal data is handled within the European Union.
- » **HIPAA (Health Insurance Portability and Accountability Act):** U.S. law setting standards for protecting sensitive patient data, mainly in healthcare.
- » **FIPS (Federal Information Processing Standards):** U.S. government standards outlining requirements for cryptographic modules used by federal entities.
- » **Common Criteria:** International standard for evaluating computer security, providing a framework for security assurance.
- » **CSfC (Commercial Solutions for Classified):** NSA program enabling the use of commercial products to protect classified information, ensuring they meet specific security requirements.
- » **NIST/BSI:** NIST (U.S.) and BSI (Germany) provide frameworks and guidelines for cybersecurity, shaping how organizations approach data security.

5. Reputation and Trust



The reputation of a castle or kingdom depends on its ability to protect its assets and subjects. A data breach not only results in financial loss but also erodes trust, much like a castle that fails to protect its inhabitants loses its standing.

Similarly, data breaches can have severe consequences for an organization's reputation, extending far beyond immediate financial loss. When a breach occurs, sensitive information may be exposed, leading to a loss of trust among customers, partners, and stakeholders.

The damage to an organization's reputation can be profound and long-lasting. Customers entrust organizations with their personal and financial information, expecting it to be handled securely. A breach shatters this trust, leading to questions about the organization's competence and commitment to data security. It's not just the financial loss that hurts the organization; the erosion of trust can lead to a loss of customers and difficulty in attracting new ones.

Take the case of the [2013 Yahoo data breach](#) as an example. The breach exposed usernames, email addresses, telephone numbers, dates of birth, hashed passwords, and additional confidential information. Worse, however, was the fact that the full extent of these breaches was not disclosed until 2016, which led to a significant loss of trust amongst Yahoo's users and the general public.

As a result, Verizon — who was in the process of acquiring Yahoo — reduced its purchase price by \$350 million, a clear indication of the damage to Yahoo's value caused by the breaches. The reputational damage was notably more severe than their financial loss. The organization, its engineers, vendors, and other associated parties experienced a substantial loss of trust from the general public.

Hence, prioritizing data security is a powerful way for organizations to prevent a damaged reputation. Demonstrating a commitment to data security can enhance customer confidence and loyalty.



Ensuring Data Security for the Future

As we've seen, effective data security is not merely about building higher walls; it requires a multi-layered approach that protects from the inside out. Just as a castle must employ a combination of physical barriers, laws, and escape routes, Intelligent Memory uses hardware, firmware, and software to implement its IMTrusted™ Data Security toolkit.

In our next article, we will discuss IMTrusted, its features and capabilities, as well as how it can help any organization provide a solid data security foundation for its storage solutions.

