SAFEGUARDING SUCCESS: MASTERING SECURITY COMPLIANCE

www.ais-mn.com

TABLE OF CONTENTS

AN INTRODUCTION TO SECURITY COMPLIANCE

Businesses today face a critical challenge in addressing security issues. With data breaches on the rise, businesses must recognize the value of investing in IT security to protect their customers and their reputations. Concerning this, compliance in IT security is essential for meeting industry standards and safeguarding sensitive data. Compliance and security are close in concept but have their own distinct functions within a business. IT security is the actual operations or implementations to protect against cyber attacks, data breaches, and other threats while IT compliance is what ensures that a business' IT security measures are meeting regulatory requirements and industry standards.

Security compliance regulations are designed to ensure that businesses are implementing adequate security measures to protect their data and IT systems. They are also industry-specific or related to specific regulations. Compliance involves the implementation of technical, administrative, and physical controls that safeguard the confidentiality and integrity of the business data. Let's break those three controls down:

Technical	Administrative	Physical
Firewalls	Policies & Procedures	Security Cameras
Encryption	Training	Biometrics
Network Authentication	Employee Clearance and Evaluations	Alarm Systems
Access controls		ID Cards
		Visitor Management

With proper IT security and compliance, a business is better prepared for any cyber attacks or possible data breaches. If a business lacks either, there can be harsh consequences that put both customer and reputation at risk.

A DECADE OF DATA BREACHES

Info gathered be tech.co, Forbes, and infosecinstitute.com

To put into perspective exactly how damaging cyber attacks can be to both customers and businesses with a decade of data breaches that affected millions.

- The Equinox data breach of May 2014 saw hackers steal credit data for 150 million people.
- From 2014 to 2018, repeated attacks on Marriott Hotels' data resulted in **hackers stealing data from 500 million** of their customers.
- In 2016 it was disclosed that led to a billion account credentials flooding the black market. It was discovered that:
  - A LinkedIn breach affected around 117 million accounts
  - A Myspace breach affected 427 million accounts
  - A VK breach affected 93 million accounts
  - A Dropbox breach affected 69 million users
- T. Mobile was victim to **four breaches in 2023**. Each compromised customer or employee data and each attack varied in scope and severity.
  - First, an exploited API vulnerability lead to 37 million customers having their data stolen.
  - Second, another attack led to 836 customers' data being compromised
  - Third, 90GB of personal employee data from an Independently owned T-Mobile was leaked on the dark web.
  - Fourth, a system glitch led to the leak of personal data of fewer than 100 customers.
- In January 2024, a project management software platform, Trello, had their data leaked across the dark web. This leak included **over 15 million email addresses, names, and other sensitive data.**

THE SIX FUNDAMENTAL GOALS

Security compliance is an essential aspect of any business's operational framework. With it being so heavily focused on protecting data, the core goals are a direct reflection of that and by adhering to compliance standards, businesses can establish a secure and resilient digital environment.

The six fundamental goals of security compliance are:

- Assisting in Risk Management
- Establishing A Strong Security Infrastucture
- Ensuring Security Best Practices
- Preventing Data Breaches
- Providing a Framework for Comprehensive Security Programs
- Building and Maintaining Trust

DIFFERENT TYPES OF SECURITY COMPLIANCE

To gain an even greater understanding of what security compliance is meant for and what data is protected, let's dive deeper into a variety of notable security compliance frameworks.

- **HIPAA (Health Insurance Portability and Accountability Act)** - in 1996, the United States passed this federal law to safeguard the personally identifiable health information of citizens. These legal requirements guarantee that healthcare providers, health plans, and other covered entities put in specific security measures that preserve the integrity and confidentiality of sensitive patient data which is also referred to as Protected Health Information (PHI).

- **GDPR (General Data Protection Regulation)** - a data protection and privacy regulation that governs how European Union individuals' personal information is used, processed, and stored. While it focuses on EU persons, GDPR requires businesses worldwide to implement the necessary technical controls that help ensure the confidentiality, integrity, and availability of data. GDPR encourages privacy and grants individuals the right to access, restrict, or get data erased if the situation deems fit. Some of the key requirements of GDPR are:
  - Consent to collect personal data with the level of consent varying according to the type of data being collected.
  - Data minimization by stipulating that the collection of personal data must be related to a well-defined business objective.
  - Individuals whose data is being collected have the right to know why their data is being collected, how it is being processed and to know when their personal data has been breached.

DIFFERENT TYPES OF SECURITY COMPLIANCE

- **NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF) -** this framework is a set of guidelines and cybersecurity practices that was developed to give configured guidance for managing and reducing any cybersecurity-related risks. This is not a mandatory compliance and any business that wishes to lower their total risk can apply this approach. NIST CSF focuses on five major risk-based cybersecurity management functions: protect, detect, respond, recover, and minimize risks.

- **COBIT (Control Objective for Information and Related Technologies) -** this cybersecurity framework was created to help businesses with IT management and governance. It is a highly processed-oriented framework that creates links between business and IT goals to distribute responsibilities. There are five processes that COBIT follows:
  - Evaluate, Direct and Monitor (EDM)
  - Align, Plan, and Organize (APO)
  - Build, Acquire and Implement (BAI)
  - Deliver, Service and Support (DSS)
  - Monitor, Evaluate and Assess (MEA)

- **PCI DSS (Payment Card Industry Data Security Standard)** - is a set of regulatory standards that were developed in 2006 by the five major credit card companies to create a central standard for maintaining a secure environment for sensitive credit information. To be compliant, this must be validated annually and non-compliance can lead to hefty fines, higher transaction costs, or lost income.

GETTING FAMILIAR WITH COMPLIANCE

As stated before, compliance is going to be dependent on your business and industry. Regardless of which are needed, there are some basic security compliance best practices that all businesses should actively be doing.

Understand Data and Requirements

The best way for a business to protect its data is to classify and understand the risks associated with it. Different types of data pose different types of risks and are commonly classified according to type, risk vulnerability, or overall value. The majority of security compliance frameworks focus on three levels of sensitive data.

Personally Identifiable Information (PII)	Protected Health Information (PHI)	Controlled Unclassified Information (CUI)
• First and last names • Address • Date of birth • Email • Social security number • Passport number • Taxpayer ID • Driver's license • Vehicle plate numbers	• Medical records • Laboratory results • Health plan and insurance records • Appointment history • Prescriptions • Hospital admission records	• Racial or ethnic origin • Religious or philosophical beliefs • Political opinion • Marital status • IP addresses • Sexual orientation • Biometric data • Financial information

All levels of data are part of a five-stage life cycle that is frequented by compliance requirements. The data lifecycle management is broken down into creation, storage, usage, archival, and destruction, and each stage is meant to meet compliance standards.

This beginning stage is also the time to research what compliances your business and state require. If you need guidance you can reach out to IT/cybersecurity experts, your state's regulatory bodies, or a corporate lawyer to help.

GETTING FAMILIAR WITH COMPLIANCE

Develop a Risk Assessment Plan

Risk assessments are already a common practice throughout business functions and security compliance is no different. One of the first steps in proactive cyber security is identifying and addressing vulnerabilities. When adding compliance into the mix, infrastructure must protect sensitive customer and business data that you are responsible for protecting. Be sure to to continuously monitor and reassess frequently to not only ensure proper security but also compliance.

Establish Safety Controls

Managing risk is a huge part of security and compliance. Implementing security measures not only adheres to regulations and standards but also improves the overall cybersecurity structure. These safety controls can be **technical, administrative, or physical** and businesses should choose controls based on their needs due to the data, where it is stored, and its value.

The Value of a Compliance Team

Establishing a dedicated compliance team can help develop a structured approach to meet compliance requirements. This team can help aid in the implementation and maintenance of security compliance while offering overall support to all employees when it comes to it.

The main goal of compliance teams is to recognize and control risks and to ensure compliance. With this also comes team communication when it comes to these procedures. Having individuals dedicated to compliance can help any team member who may not be familiar with security compliance. With collaboration, open communication, and teamwork solutions can be implemented and utilized to their full capability.

WHAT COMPLIANCE BRINGS TO YOUR BUSINESS

When security compliance is done right it offers appealing benefits for businesses that go far beyond requirements and needs. By adhering to security standards and regulations, businesses can:

- Avoid hefty fines and penalties
- Build a foundation of a strong control environment
- Establish trust and maintain or build relationships and reputations
- Improve security culture and operational efficiency
- Mitigate security risk with risk assessments and action plans
- Have thorough management practices
- Create overall more positive internal and external relations
- Improve security culture and operational efficiency

- The Risks of Non-Compliance -

Non-compliance poses a significant threat to businesses and personal data security. Failure to adhere to security protocols and best practices can leave systems and networks vulnerable to exploitation by malicious actors. In more serious cases, non-compliance can have repercussions including **disrupted business activities, severe reputation damage, hefty fines, and even prison time.**

KEY TAKEAWAYS

Security compliance is vital for any business in order to protect sensitive information and uphold the trust of its customers. When businesses choose to make security compliance a top priority it is the ultimate safeguard of integrity and reputation.

Three key points to remember when addressing security compliance are:

1. Ensuring cybersecurity compliance is imperative for protecting sensitive data and mitigating the risk of cyberattacks. Compliance measures help businesses adhere to legal and regulatory requirements, ensuring customer trust and a stable reputation.

2. Regular training and awareness are essential to educate employees about cybersecurity best practices and compliance protocols.

3. Implementing robust security measures, such as encryption and access controls, is imperative for maintaining compliance and safeguarding business assets.

Compliance, Safety, and Success

At AIS, we have the knowledge to ensure that your business meets all security compliance standards and are committed to addressing any inquiries and concerns you may have. Contact us today to discover how we can help ensure your business stays secure and meets all necessary compliance standards.