Simplifying Compliance: An Actionable Guide for IT

WHITE PAPER

hexnode

TABLE OF CONTENTS

Introduction

Compliance refers to the processes that businesses take up to ensure they follow the internal rules of the company and the external rules imposed upon by other regulations. With the world going digital, businesses often find themselves in the middle of a data explosion, where data of thousands of users are handled on a daily basis.

Being compliant with industry regulations is crucial because it assures your customers that any data you've collected from them is processed in accordance with laws falling under your jurisdiction and other rules and regulations applicable to your organization.

Despite the improvements we have made towards making data security a more concrete reality, businesses still struggle to successfully implement compliance within the workplace. You can begin by getting a clear understanding of all the regulations that is applicable to your business. This would be easier to make further decisions on the various measures you need to implement to properly secure endpoints and data. This lack of understanding often undermines the value of compliance, which often results in organizations giving it up as low priority.

1

How worried should organizations be?

As an organization, you may find it more challenging to understand who is at risk here and the various threats your business maybe susceptible to.

Some of the industries more susceptible to cyberattacks include:

- Finance
- Health Care
- Education
- SMBs

Cybercrimes equally plague businesses and the average online user. Data miners and hackers are always on the lookout for any predictable patterns. Thanks to the internet, you don't necessarily have to be an IT expert to understand all the risks that comes with taking up a lackadaisical approach to information security.

It can also be quite hard to determine the consequences of those attacks and the costs that results from those attacks.
You also need to have a skilled IT security team as well as a qualified compliance team to determine the controls and other technologies you need to implement to safeguard safeguard your organization and its assets from those attacks.

The global cybercrime cost is expected to grow to 10.5 trillion US Dollars by 2025. These include the damage and destruction of data, loss of productivity, theft of intellectual property, embezzlement and reputational harm.

2

Going Digital: Addressing various compliance challenges

Most businesses don't have enough resources to properly make use of all the data they collect, leading them to store it for an infinite amount of time until they can be used again, which sometimes amounts to never.

Due to the large number of connected devices organizations have amassed a lot more data than they can manage. It can be a struggle to figure out what to do with all this data.

Sometimes the implemented measures may not be in sync with the rate at which the data is being produced and collected by your organization. This can lead to the occurrence of some unforeseeable security incidents in spite of adopting security measures you thought were right at the time.

There'll always be risks associated with storing data for such a long time. Before we get into the challenges, let's take a brief look at some of the commonly followed compliance regulations.

3

Common regulatory compliances for Information Security

In accordance with the terms defined within the GDPR, organizations are required to ensure personal data is only collected for legitimate purposes and should be done under the strictest of conditions.

General Data Protection Regulation (GDPR)

- It is a privacy regulation passed in 2016, to give EU citizens more control over their data.
- It requires businesses to implement and maintain an adequate level of data protection.
- It came into effect in 2016 to replace the old Data Protection Directive which was passed in 1995.
- The regulation is designed to govern the way in which data is collected and processed, while ensuring user privacy at the same time.
- This framework applies to organizations within all the member states and to businesses and individuals beyond EU. If your business is located outside of EU, but processes information of EU citizens or have website visitors from EU, then you would fall under the scope of GDPR.

- In accordance with the terms defined within the GDPR, organizations are required to ensure personal data is only collected for legitimate purposes and should be done under the strictest of conditions.
- They would also be held accountable for the data they handle by ensuring it stays protected against misuse
- Organizations should take up the responsibility and notify the concerned data subjects when data breaches occur.
- GDPR mandates that organizations should conduct a Data Impact Assessment, which helps companies minimize risks related to data protection.
- Data breach notification is another important aspect of GDPR. When a data breach does occur, businesses are required to inform their concerned supervisory authority of it within 72 hours of being aware of the breach.
- A personal data breach is different from a security incident and organizations should be able to clearly understand the difference between the two.
- UK ceased to a part of EU in 2020. UK has its own data protection regulation known as the UK GDPR which is almost similar to the EU GDPR framework with just a few minor differences.

> A security incident refers to an event that fully compromises the integrity, confidentiality and availability of the information whereas a personal data breach refers to the disclosure of data to an unauthorized party.

Payment Card Industry Data Security Standard (PCI-DSS)

- Defines a set of requirements organizations should follow to ensure that processing, storage and transmission of credit card information is done in a secure manner.
- It was passed in 2006 to secure account information being handled during the transaction process.

- Just like any other compliance regulations, PCI DSS also comes with a set of requirements for companies to follow. These include:
    - the use of firewalls
    - implementing adequate password protection
    - using encryption to protect the cardholder data and transmission of cardholder data
    - restricting data access to a strict “need-to-know” basis
    - having unique IDs when accessing the data
    - maintaining access logs for periodic reviews
    - documenting policies on the processing and storage of information within the company

- Being PCI DSS compliant gives your customers the assurance that your systems are secure leading to improved customer trust.

Health Insurance Portability and Accountability Act (HIPAA)

- Comes with necessary administrative, technical and physical safeguards which guides organizations on the security measures they need to implement to keep ePHI safe.

> “ This came into effect in 1996 and helped set the standard for organizations to protect their HIPAA database.

- Security rule was put in place to protect the privacy of patients and at the same time for organizations to implement adequate security measures to keep these data safe.
- They allow organizations to implement policies, procedures and various other technical controls to minimise the risk to patient ePHI.
- The HHS requires organizations to implement physical and technical safeguards to protect

sensitive information. Some of these include:

- using encryption to protect ePHI
- implementing strict access control measures
- maintaining a proper audit trail over the hardware and software assets of your organization
- implement web filtering to block access to sites prone to malware and phishing attacks
- setting up restrictions on lost or stolen devices
- documenting and implementing the required policies
- assign responsibilities
- conducting periodic risk assessments
- providing security awareness training
- have processes in place to manage information security incidents
- ensure data can be easily retrieved and accessed.

Health Information Technology for Economic and Clinical Health (HITECH)

- It was signed into law as part of the American Recovery and Reinvestment Act (ARRA) bill in 2009.
- It mandated the strict enforcement of the privacy and security rules of HIPAA through audits.
- Successful implementation of the provisions defined within HITECH can be done by following the three phases. They guide organizations to be compliant with the Act. The first phase covers the requirements and objectives organizations should meet to collect and share private data by a covered entity.
- HITECH helps ensure security and privacy for patients due to its strict enforcement of HIPAA's Privacy and Security Rule.

> "These objectives are further split into three categories, these include:
>
> - core objectives
> - menu objectives
> - clinical quality

> Some of the benefits HITECH provides to patients include:
>
> - giving access to protected health information
> - notifying patients of data breaches related to the patient's PHI.

- Breaches affecting 500 or more patients should be reported to the United States Department of Health and Human Services (HHS).
- Some of the best practices of HITECH compliance include:
  - creating an awareness program to ensure privacy of the Personal Health Information (PHI)
  - implementing the practice of least privilege to limit access to data on a strict "need to know" basis
  - helping organizations to review their internal controls and procedures to ensure that they are implementing the best practices to secure PHI and other sensitive data.

Sarbanes Oxley Act (SOX)

> Stands for Services and Organization Controls. It was introduced by AICPA and is based on the Trust Services Criteria.

- It reports on how secure the controls are for a service organization.
- It is an auditing procedure to ensure data is being adequately protected to ensure user privacy.
- Customer data is managed based on five "Trust Service Principles", these include:
  - Security
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy
- Unlike PCI DSS, the requirements of SOC are not rigid. They would be unique to the business practices of the organization.

- After the assessment is done by the auditor, reports will be generated clearly defining how the service provider manages the data.

> “ The two types of reports would be Type I and Type II. Type I gives an overview of the systems and evaluates whether the design is in alignment with the applicable trust principle.

- It's not necessary for organizations to follow all five trust principles, they just need to follow ones that are applicable to them. Type II covers the detailed operational effectiveness of those systems.
- SOC 2 certification is supplied by external auditors.
- A brief summary of each of the trust principles are as follows:
- **Security** – it protects the system resources against unauthorized access. It requires organizations to implement access control, 2FA, firewall and other technical controls to safeguard data and prevent the occurrence of any security breaches.
- **Availability** – refers to the accessibility of the system as mentioned within the SLA and contract. It involves criteria that may affect service availability such as network monitoring, security incident handling etc.
- **Processing integrity** – it checks whether the system has achieved its intended purpose and the data processing activities are accurate, timely and authorized.
- **Confidentiality** – data access is restricted only by an authorized person or a set of authorized parties. Encryption is used to protect the confidentiality of the information during transmission and at rest. Other measures include firewalls and strict access controls.
- **Privacy** – it addresses the system’s collection, use, retention, disclosure, and disposal of information in accordance with the organization’s privacy notice as well as the criteria defined within AICPA’s Generally Accepted Privacy Principles.

Risks that come with not complying with these regulations

- Fines and penalties
- Reputational damage
- Revenue loss
- Lawsuits
- Disclosure of PHI
- Breach of Payment Card Data
- Lack of Data Privacy Rights
- Business disruption

4

Building a strong foundation: Security measures to implement within the workplace

The ultimate goal of this awareness program shouldn't just be to strengthen your organization's security defences, it should also be focused on clearly communicating your organization's values regarding protecting the interests of your customers and other interested parties.

The first step to build a strong security foundation within an organization is to raise awareness of cybersecurity and its latest threats among employees. This way your organization can prevent the occurrence of multiple risks that could arise from adopting poor security practices.

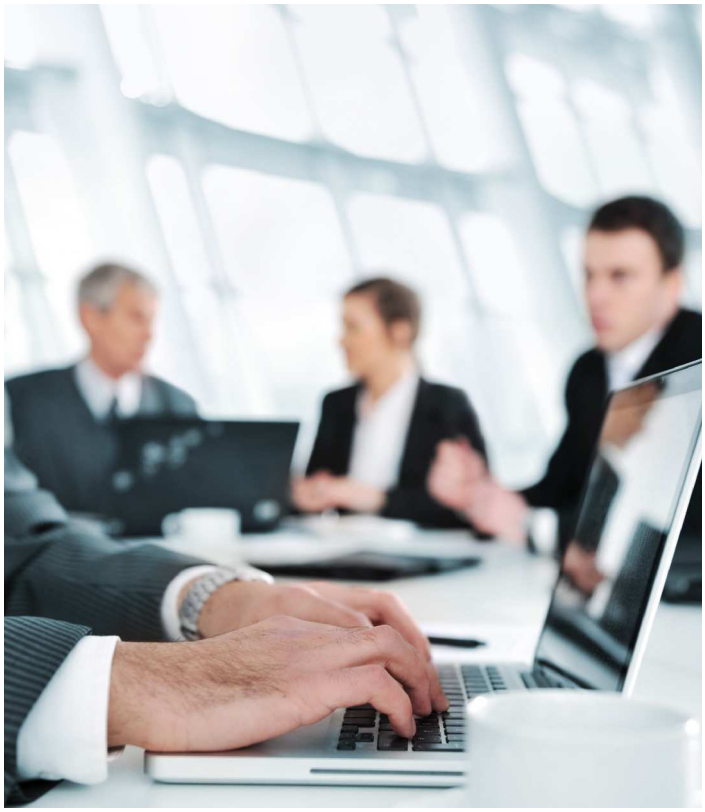
Checklist on creating a security-oriented culture:

- Hire a team with the right legal, compliance and technical expertise to guide the organization.
- Define a scope for your compliance project.
- Clearly define and document an action plan that would help you achieve the goal.
- Maintain logs to monitor the effectiveness of every stage of your project.
- Set deadlines for each stage.

- Evaluate security measures by administering adequate technical and administrative controls.
- Carryout periodic mock scenarios to test the effectiveness of the security awareness program.

What to include when defining the scope of your project?

> When defining the scope of your compliance project, it's always important to consider all the obligations you hold to your employees and customers.



This would give them the assurance that your business continues to remain operational during man-made or natural disasters and the data you collect from customers are handled in accordance with all the requirements defined within the regulatory compliances applicable to your organization.

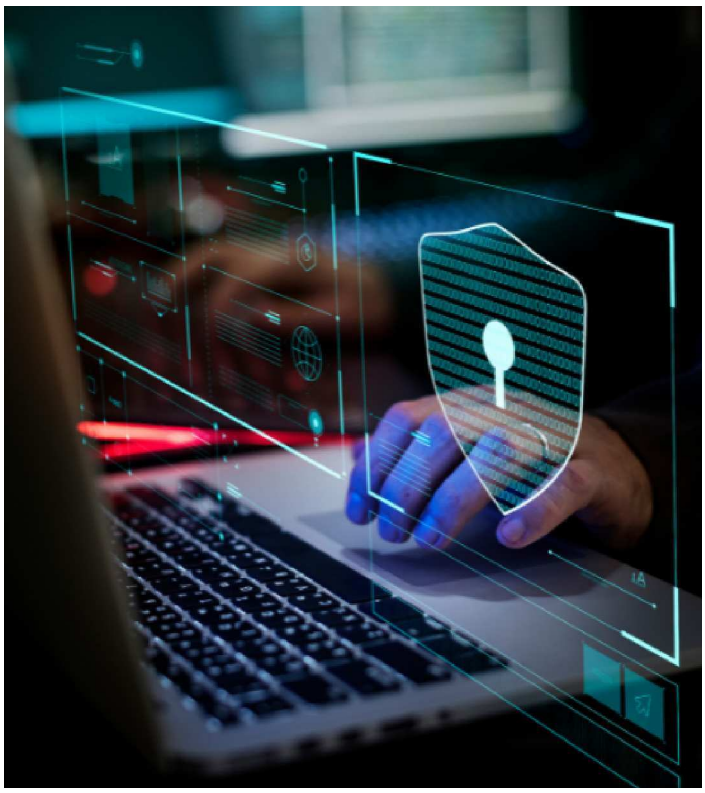
Business obligations:

Business continuity: document a business continuity plan that details all the measures you have in place to ensure your services remain accessible to end users. Critical data should be backed up and tested for recovery at periodic intervals.
Information processing facilities are areas where systems that processes information are stored, these could be your workstations, networks etc. Sufficient redundancies should be maintained to make sure these systems could be relocated to another secondary location should the primary location be inaccessible at the time.

Risk management: create a list of all risks applicable to your organization. Get inputs from all teams within your organization and have a clear understanding of all the blockers and potential threats they would come across.

Once the list of risks has been prepared, they should be assessed in order to understand the impact they could have on the overall functioning of your business.

> The final step of the risk management process would be to continually treat and monitor the risks.



Security awareness: conduct a security awareness program at periodic intervals to improve knowledge on information security, data protection and cybersecurity. You can send in feedback forms or conduct tests at the end of each session to evaluate the effectiveness of the program.

Use of right controls: define and document all the technical and administrative controls you would be using to adequately carry out the security measures. This would include documenting the right policies and procedures and ensuring employee devices are ably password protected and encryption enabled.

Data protection: have all the right measures in place to ensure client and company confidential data stays protected against unauthorized access, disclosure or modification. You can implement a data classification policy to categorize and label all the data you handle.

Document an access control policy to limit access to data on a strict 'need-to-know' basis. A log should be maintained to continually monitor the access rights.

> A data loss prevention policy should be maintained to protect the transmission of data within organization approved networks.

Ease-of-use: complexity should not be synonymous with compliance. Organizations should always make it clear of what is expected from employees. Compliance should be woven within the foundations of your business operations and your employees should be provided with the flexibility to easily reach out to any members of your IT Security or Compliance team to get a clear idea of what they need to do in order to adequate protect sensitive data they handle on a daily basis.

Handling data breach and security incidents: clearly document a policy specific to your organization stating all the processes that needs to be followed in the event of a data breach or a security incident. Employees should be briefed on who they need to report to once a breach has occurred or if they suspect there could be a chance for one.

Customer obligations:

Clear communication: businesses should always maintain transparency. Customers should always be kept on the loop and be presented with a clear picture of all the security measures your organization has taken up to ensure their data is in safe hands.

Privacy policy: privacy being of utmost importance to your customers expect businesses to adequately protect their data. Have a well written privacy policy that documents:

- The types of data collected from customers
- The data handling and processing procedures
- Data retention period
- Data disposition

5

How UEM helps in implementing the best security practices

A Unified Endpoint Management solution comes with multiple management capabilities where a wide range of devices from mobile devices, desktops, IoT devices and wearables can be managed from a single platform.

The global Endpoint Security market is expected to be valued at USD 22.21 billion by 2026. More organizations are relying on SaaS based solutions to manage endpoint security and ensure data protection.

It incorporates the use of other technologies such as a Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Content Management (MCM), Identity and Access Management (IAM) and Mobile Security Management (MSM).

How does it help in maintaining IT security?

- Simplifies the way in which multiple devices can be managed.

- Helps improve productivity by giving employees instant access to resources they need.
- Easily deploy, manage and secure public and private apps.
- Quickly resolve user requests with remote troubleshooting.
- Secure lost or stolen devices with remote lock and wipe

A UEM solution makes it easier for organizations to implement and monitor the best practices they need to make sure data is handled in alignment with the business requirements and industry standards, these include:

Encryption

- Ensuring all managed devices are encrypted.
- Flag devices that are not encrypted.

Password security

- Define password policy specific to your organization.
- Prompt users to regularly update their passwords.
- Dissuade users from following a predictable pattern while creating new passwords.

Data protection

- Create containers to separate corporate data and apps from personal space of users.
- Set separate passwords to make sure only authorized users have access to the work container.
- Restrict the copying and pasting of sensitive information to unmanaged spaces within the devices.
- Restrict the sharing of files by disabling bluetooth, USB, NFC and Android Beam.
- Block access to risky websites via web filtering.

Securing lost devices

- Remote lock and wipe data from these devices.
- Remotely enable lost mode on Android and iOS devices.
- Track and continually monitor device location.

Application management

- Create app catalogs and app groups for easier deployment.
- Pre-define app configurations and permissions.
- Blacklist applications not approved by your organization.
- Upgrade and downgrade managed applications.

Device security

- Set adequate restrictions on device functionalities, network and other security settings to ensure endpoint security.
- Maintain continuous compliance checks to make sure all the devices continue to be compliant with the restrictions in place.
- Auto-lock devices after a set period of inactivity.
- Schedule OS updates.
- Configure firewall to protect device from external threats.Identify jailbroken iOS devices and rooted Android devices.
- Identify jailbroken iOS devices and rooted Android devices.

Access and Identity management

- Integrations with Azure AD and Active Directory to restrict access to data based on the authority and role of the user.

Conclusion

Looking ahead: The future of compliance

The cybersecurity threat landscape is changing with threat actors shifting their focus on suppliers and small vendors, thereby increasing the risk of third-party data breaches. The importance of modern privacy laws would just keep increasing in the coming years with Gartner predicting that by 2023, 75% of world's personal information will fall under the scope of these privacy laws.

The rapid rise of technology and digitalisation would make it necessary for organizations to adapt tools and rely on AI to automate some of the workflows. Data analytics would be used to improve monitoring and training among employees. As more customers are prioritising the need for data privacy, compliance will continue to be a top business priority for organizations in the coming years.

Mitsogo Inc., Unites States (HQ), 111 Pine St #1225,
San Fransisco, CA 94111
Tel: Intl +1-415-636-7555, Fax: Intl +1-415-646-4151