Building a cybersecurity framework for your enterprise

hexnode

TABLE OF CONTENTS

1

Introduction

Some stats to digest:

- Almost half of these attacks target small businesses, 43% to be exact.
- 64% of them were web-based.
- 62% were social engineering and phishing attacks.
- 59% contained malicious codes.
- 51% were denial of service attacks.

How prevalent are cyberattacks?

We've all heard about the frequency of cyberattacks, but how frequent are they? The University of Maryland was the first to bring out a study that properly quantified the interval in which hackers could exploit systems within the US.

According to the study, an attack happens every 39 seconds. That is a lot. Cyberattacks rank as one of the top rated risks across both public and private sectors. The pace at which these attacks occur have has steadily grown with the pandemic and the growth of IoT devices.

As an organization, you need to be extra vigilant in terms of detecting and mitigating these attacks on time. This can be quite challenging as the rate of detection of these attacks is low, 0.05% in the US, according to World Economic Forum's Global Risk Report, 2020.

Recent incidents of cyberattacks

March 2022

The National Research Council, the largest state funded research agency in Canada disclosed their networks were penetrated by hackers.

Hackers were successfully able to launch a DDoS attack on a well-known Israeli telecommunication provider which resulted in the shutdown of many Israeli government websites.

February 2022

Many oil terminals in ports across Belgium and Germany were targets of a cyberattack that prevented them from processing incoming barges. Hackers were able to penetrate the networks of the UK Foreign Office.

January 2022

A hacktivist group based in Belarus was able to hack into the networks of the Belarusian railway, which resulted in the encryption of the railway servers and the destruction of data held within the backup server.

Multiple DDoS attacks targeted a Minecraft tournament held in Andorra, affecting the country's internet service provider, disrupting the 4G and internet services of many of its customers.

> “ Some recent well-known cyberattacks
>
> - Spear phishing – Twitter
> - Abuse of privileged account – Microsoft
> - Insider data theft – Shopify
> - Third-party vendor attacks – Jet2

2

How do you ensure protection?

A cybersecurity framework can be defined as a set of policies and procedures defined by cybersecurity professionals and organizations to improve the security measures and controls businesses need to take to protect their networks, users and devices.

It's important for businesses to clearly understand and implement the right security measures to ensure their assets remain safe from hackers and other vulnerabilities. So, how do you go about it? How do you make sure you choose the right controls that fit in with the needs of your company and other interested parties?

There are various cybersecurity frameworks in place that guides organizations on the implementations they need to follow.

Executive Order – Why it matters

The need to prioritize cybersecurity came to light with the attacks on SolarWinds and Colonial Pipeline.

The signing of the Executive Order (EO) was the result. The Executive Order also aims at making it easier for IT and OT providers to effectively communicate cybersecurity and other breach information with government officials.

> “ Signed in on May 12, 2021 by the Biden administration, it stressed the need for organizations to modernize their security defenses in improving cybersecurity.

What does the Executive Order talk about?

It talks about:

- Strengthening the systems within the federal government.
- Modernizing security implementations to improve cybersecurity.
- Removing multiple barriers to ensure smooth communication of breaches and cybersecurity incidents to the government.

The order further consists of requirements and recommendations businesses should meet. It also defines the timelines in which these objectives should be met. Let’s take a deeper look into these:

Increase Information Sharing

It aims at removing barriers in effectively communicating breaches. It smoothens the way in which IT service providers can share information related to cybersecurity vulnerabilities spotted within government networks. This would also help IT service providers develop the habit of promptly reporting cybersecurity incidents. Information related to various threats and vulnerabilities should be shared with agencies such as CISA and the FBI.

Recommendations:

- Requires logging events and the retention of relevant data.
- Recommends the implementation of an Endpoint Detection and Response (EDR) solution.
- Improve the detection rate of cybersecurity incidents.

- Develop procedures where reports on cybersecurity incidents can be immediately shared with agencies.
- Document policies where providers establish their requirements related to logging, log retention and log management.

Modernize cybersecurity

Cyberattacks keep evolving. It only makes sense to modernize your security defenses to keep pace with these newly emerging attacks.

Recommendations:

- Review standards, tools and best practices for greater software supply chain security.
- Define all critical software.
- Publish guidelines on the minimum standards with which vendors should test their software source code.
- Implement a zero-trust architecture.
- Evaluate types and sensitivity of unclassified data in agencies.
- Implement multi factor authentication and encryption.
- Identify practices for software supply chain security.

> “ Some of the recommended practices include implementing a zero-trust security model, rapidly shifting to secure cloud service providers and deploying other security measures such as multi factor authentication and encryption.

What does the EO recommend to improve collaboration between government agencies and private sectors?

- Create a Cyber Safety Review Board where members would be leaders from the private sector and government officials.
- Develop operating procedures to conduct and plan cyber vulnerability and incident response activities.

3

What are cybersecurity laws and regulations?

Cybersecurity guidelines

- SEC Guidance
- Federal Acquisition Regulation System

Getting a clear picture on the various cybersecurity laws and regulations would be a good place to start. It helps businesses define the objectives they need to take up to improve their security infrastructure.

Some of the cybersecurity laws and regulations include:

- Gramm-Leach-Bliley Act of 1999
- Federal Information Security Modernization (FISMA) 2014
- Cybersecurity Information Sharing Act (CISA) 2015
- Federal Risk and Authorization Management Program (FedRAMP)
- California Consumer Privacy Act (CCPA)
- California Privacy Rights and Enforcement Act (CPRA)
- EU Cybersecurity Act

4

Cybersecurity Compliance Frameworks vs Regulatory Compliance Frameworks

Compliance based frameworks:

- HIPAA
- SOX
- PCI DSS
- SOC Reports
- GDPR

Cybersecurity based frameworks:

- NIST cybersecurity framework
- CIS
- ISO 27K family of standards

The difference

When seen at a glance, the frameworks of both regulatory compliance and cybersecurity may seem similar. Though both calls for the same types of security implementations, they are quite independent of each other.

For instance, compliance focuses on the types of data handled and stored by the company whereas regulatory requirements prioritize its protection. By being compliant an organization ensures that it complies with the minimum security requirements.

This includes documenting policies, implementing security controls and assessing the identified risks. A cybersecurity framework on the other hand, consists of tools and processes that are used to protect the information and the assets used for storing and processing the information.

5

Understanding the different frameworks

The NIST cybersecurity framework can be chosen by organizations with a mature security program whereas businesses just starting out can choose CIS controls

The three types of frameworks include:

- Control framework
- Program framework
- Risk framework

Organizations can choose the right cybersecurity framework based on the maturity of their security program. The NIST cybersecurity framework can be chosen by organizations with a mature security program whereas businesses just starting out can choose CIS controls that define the baseline of security controls organizations need to implement.

Control framework

Control frameworks provide a baseline set of controls that helps organizations to strategize their security efforts. They help teams to evaluate the current state of the technical controls and help them prioritize the controls they need to take up to make it better.

NIST 800-53:

The Federal Information Security Management Act (FISMA) passed in December 2002, required NIST to develop a set of guidelines to improve the information security of systems being used within the federal government.

These guidelines are now being used by organizations and are referred to as NIST Special Publication (SP) 800-53. The early 2000s were plagued with many data breaches which prompted the passing of the E-Government Act, which eventually lead to the creation of NIST 800-53.

> “ NIST 800-53 consists of a set of recommended security and privacy controls that guides the organizations to meet the requirements set by FISMA.

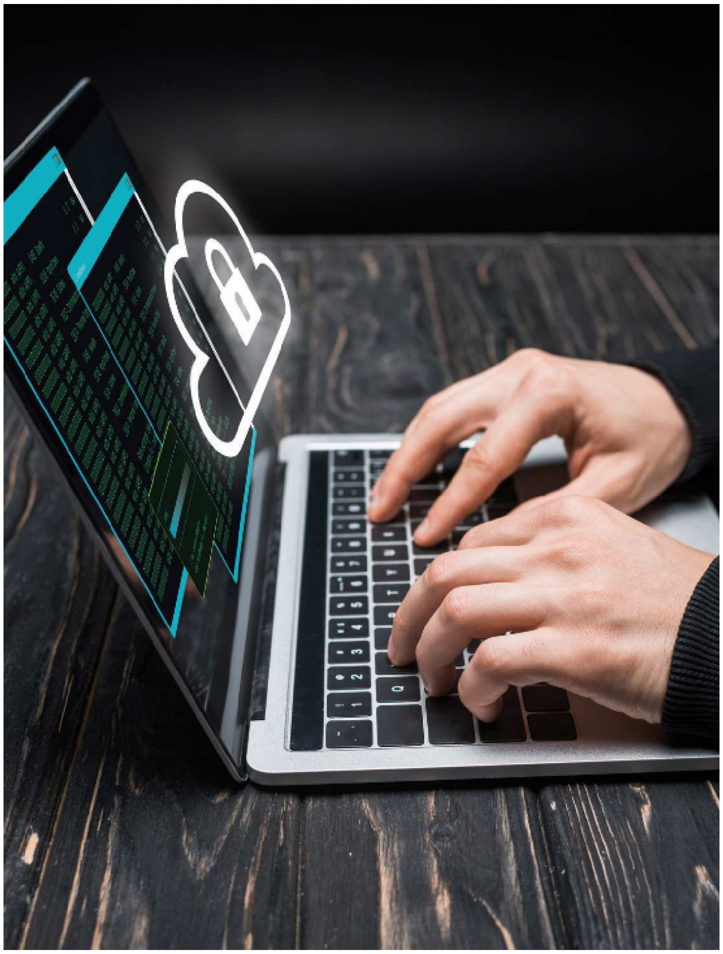
The controls are divided into three classes based on impact, these include low, moderate and high. These are then further broken down to 18 security control families where organizations can take up controls that are applicable to them.

CIS Controls (CIS):

They are a set of cybersecurity best practices organizations need to implement to prevent attacks and other vulnerabilities. These practices were formulated by cybersecurity experts with knowledge gained dealing with actual attacks.

These controls can be used to achieve various goals defined by multiple regulatory compliance and cybersecurity frameworks. There are 18 CIS controls in total, split into three categories – basic, foundational and organizational.

Program framework



This would be a better option for organizations that already have a security program in place. Implementing a program framework helps them to assess the current state of their security implementation. In addition to building up a comprehensive security program, it also simplifies the communication that needs to be held between the management and the team. Some of the program frameworks include:

ISO 27001:

ISO 27001 is a part of the ISO/IEC 27000 series that guides organizations on the best practices they need to implement to improve the confidentiality, integrity and availability of Information Security Management Systems (ISMS).

There are 114 controls in total split into 14 domains. Organizations are not required to implement all 114 controls, instead they can choose the ones that are applicable to their workflow. These are documented in a Statement of Applicability, where organizations list out all the controls applicable to them.

NIST CSF:

It sets the guidelines organizations need to follow to improve their cybersecurity structure. It defines the recommendations and standards organizations need to follow to better identify, respond and recover from these attacks.

During the identification process, organizations should make a list of assets they need to protect.

> “ The framework is split into five functions or capabilities, these include:
>
> - Identify
> - Protect
> - Detect
> - Response
> - Recover

Protection covers all the implementation safeguards. The detection stage ensures organizations have enough processes in place to detect the presence of any cybersecurity incidents. Respond includes all the techniques used to react and assess the impact of cybersecurity incidents. Recover includes all the implementations taken up to ensure business continuity.

Risk framework

> “ The steps within the risk management process include the identification, measurement, and treatment of risks in addition to prioritizing security measures to mitigate or treat those risks.

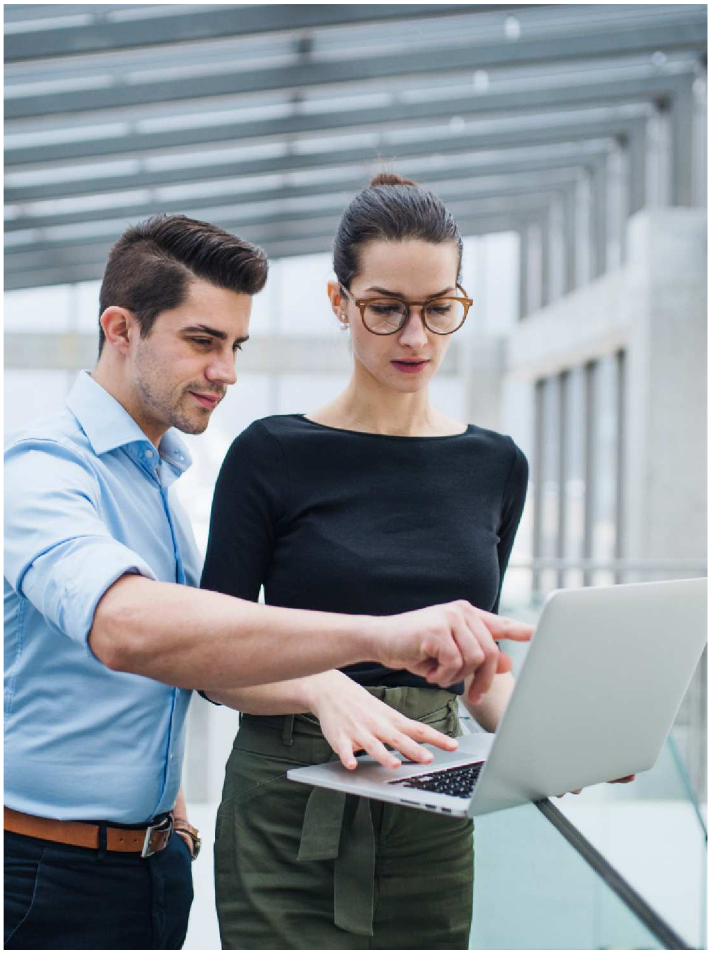
They define the measures organizations need to assess and manage the risks they have identified. It helps to define a proper structure for risk management. Some of the risk frameworks include:

NIST 800-39:

It sets the guideline for information security risk management. The risk management cycle is explained with the help of three tiers. These include the organizational tier, business process tier and information systems tier.

The organization tier defines and prioritizes all business processes needed to manage security risks. This tier looks into the establishment of responsibilities and risk management strategies. In order for the risks to be effectively managed, each risk should be aligned to a business process.

After the risks are aligned to specific business processes, the business process owner should consider threats to each process and the consequences of these threats.



It is in the last tier that risk analysis and security measures are implemented to safeguard the information systems.

NIST 800-37:

It is a risk management framework for information systems and organizations. Rev 2 of this guideline was published in December 2018. It covers the risk management framework and the processes that needs to be followed to apply the risk management framework to the information systems.

> “It looks into the management of security, privacy, risk and consists of guidelines to categorize information and the adequate controls needed to implement, evaluate and monitor the risks.

NIST 800-30:

The purpose of this special publication is to conduct risk assessments in accordance with the recommendations set by NIST. The guidelines are written down specifically in a language that could be easily understood by the management.

This helps them to make better decisions on implementing the right cybersecurity measures. It first requires organizations to conduct a baseline risk assessment to understand the current status of the systems. This would be helpful in identifying specific security issues and making improvements accordingly.

ISO 27005:

It describes how risk assessments should be conducted to safeguard information security in accordance with the requirements set by the ISO 27001 standard. It requires organizations to give proper evidence on how the risks are managed and controls taken to mitigate or treat those risks. According to ISO 27005, the risk management process can be divided into six components, these include:

- Context establishment
- Risk assessment
- Risk treatment
- Risk acceptance
- Risk communication and consultation
- Risk monitoring and review

FAIR:

FAIR or Factor Analysis of Information Risk is a framework that identifies probable risks as well as evaluates the chances for these risks to transition from probable risks to real risks.

> “ The model consists of four components, these include – threats, assets, organization, and the external environment.

This allows businesses to take the measures they need to be prepared to deal with or mitigate these risks. The four stages of the FAIR risk assessment include:

- Identification of inherent components of the risk scenario.
- Evaluation of Loss Event Frequency.
- Evaluating Probable Loss Magnitude.
- Deriving and articulating risks.

6

How to choose the right cybersecurity framework?

If your business falls under the scope of certain sectors like financial services and healthcare, you will have to adhere to compliance frameworks such as PCI DSS and HIPAA.

Consider applicable regulatory requirements

Being compliant with applicable regulatory requirements not only improves the trust of your stakeholders and customers but also makes your business stand out amongst competitors. Regulatory compliances can vary based on the industry and the region from which you operate. If your business falls under the scope of certain sectors like financial services and healthcare, you will have to adhere to compliance frameworks such as PCI DSS and HIPAA.

Have a clear idea on what you need to protect

This would include all the assets, information systems and data being processed and handled within your company. It's always best to prioritize the assets based on your business processes. This makes it easier to protect various assets based on the criticality and helps teams to prioritize the security measures they need to take up.

Understand what you need to monitor

Implementing a cybersecurity framework is a cyclic process that requires constant monitoring. Make a list of all the processes you need to monitor at regular intervals. Some of these include reviewing access privileges, conducting tests to ensure business continuity and performing recovery tests for backups.

How to manage and respond to security incidents

The way you handle and respond to security incidents says a lot about how mature your security program really is. You need to first document a process that clearly defines what a security incident is and the processes your employees should follow once they detect the presence of such incidences. Communication plays an important role in an incident response procedure.

> “ A good incident response procedure should document an efficient communication channel devoid of obstacles where employees can report the incidents they see.

It should define how internal and external communication needs to be handled. You could create a report after the closure of each incident. This would help your organization understand all the weak points within your security program and take measures to deploy the right implementations to make it more secure.

Ability to recover critical data when incidents occur

Many frameworks call for the need to establish a disaster recovery plan. A disaster recovery plan is essential in terms of how swiftly organizations can begin resuming their daily operations after an incident has occurred. One of the core components of a disaster recovery plan is the evaluation of all business processes and their needs. It requires organizations to conduct a business impact analysis and a risk analysis. This helps them to prioritize and set their recovery objectives. A disaster recovery plan helps organizations to gradually reduce downtime and minimize any financial or reputational repercussions.

> “ One of the core components of a disaster recovery plan is the evaluation of all business processes and their needs.

7

How UEM helps in improving cybersecurity?

Admins are expected to manage a plethora of devices such as smartphones, laptops, tablets, PCs, and desktops. Security has been consistently ranked as a priority amongst many IT admins. Ensuring the security of these endpoints has always been an expensive and time-consuming process.

It's common to find a mix of corporate and personal devices in a modern workplace. Although it provides employees with more flexibility, the challenges of managing these devices have grown enormously. On an average, an employee makes use of at least two computing devices to carry out their daily tasks.

Thus, in a typical modern workplace, admins are expected to manage a plethora of devices such as smartphones, laptops, tablets, PCs, and desktops. In addition to endpoint management, security has been consistently ranked as a priority amongst many IT admins.

Ensuring the security of these endpoints has always been an expensive and time-consuming process. The frequency with which these devices are targeted leaves admins with no choice but to make do with what they have.

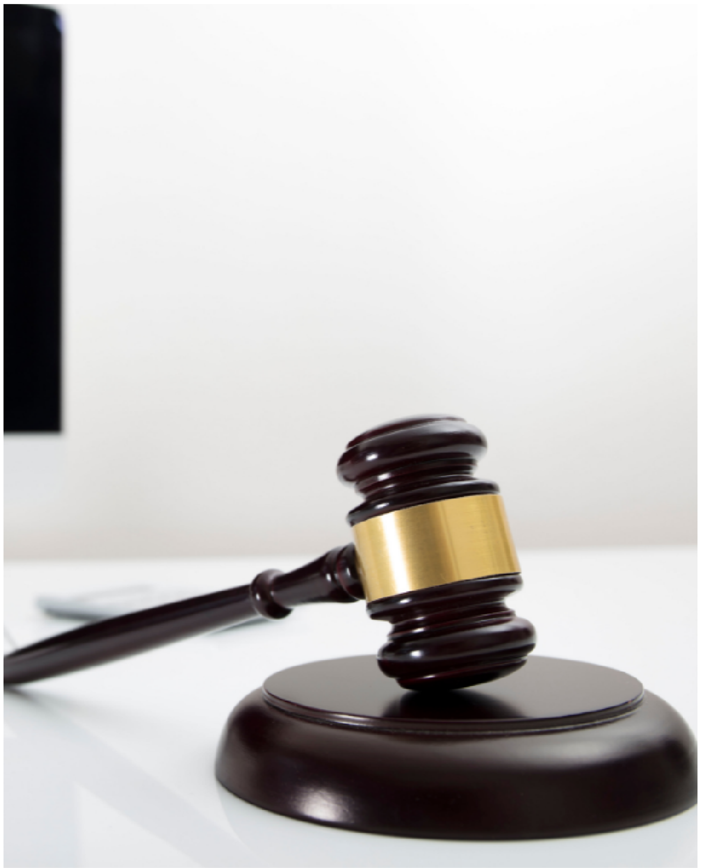
A Unified Endpoint Management (UEM) solution helps answer this problem to a great degree. In addition to providing flexible pricing plans, it helps organizations:

- Easily enroll devices from different platforms.
- Make an inventory of all devices and applications.
- Deploy necessary security configurations.
- Monitor and secure lost devices.
- Patch management through OS and app updates.
- Create secure work containers in BYO devices.

How does Hexnode UEM help organizations on their journey to achieve compliance?

Hexnode is an award winning UEM solution with management capabilities that simplifies the process of ensuring data protection and endpoint security.

> “ Hexnode helps organizations easily implement the requirements stated within the cybersecurity frameworks and be compliant with multiple regulatory compliances such as GDPR, HIPAA, PCI DSS and SOC 2.



These include:

- Identifying non-compliant devices.
- Disenrolling and remotely wiping data from non-compliant devices.
- Enforcing necessary security configurations and restrictions.
- Restricting access to unsecure applications by creating managed app catalogs.
- Remotely manage applications.

- Secure devices by deploying strong password policies.
- Predefining password age to encourage users to update their passwords at regular intervals.
- Remotely encrypt devices to enhance data security.
- Schedule OS updates to keep devices secure.
- Configure Wi-Fi and VPN settings to improve network protection.
- Minimize unauthorized access in personal devices by creating password protected work containers.
- Disable file sharing capabilities.
- Protection of data in transit.
- Secure lost and stolen devices with remote lock and data wipe.
- Activate remote ring to locate lost device.
- Enable location sharing to keep track of lost devices.

- Blacklist and whitelist applications.
- Manage network data usage across endpoints.
- Track per app data usage.
- Remotely enable firewall settings.
- Run device scans at regular basis to check for vulnerabilities.
- Enable web content filtering to restrict access to insecure websites.
- Auto lock devices after a set time period to restrict unauthorized access.
- Remotely activate and disable remote sessions for troubleshooting.
- Manage device and user access to corporate resources.

8

What does the future hold?

85% of SMEs plan to increase their IT security spending till 2023.

According to Gartner, by 2025, 60% of organization would start using cybersecurity risk as a primary determent in conducting third-party transactions and business deals.

Cybersecurity is evolving at a fast rate. Remote work is no longer synonymous with the pandemic, and it is expected that more organizations may opt for hybrid work in the future.

This just makes it more challenging for businesses to adopt the right cybersecurity framework as the addition of more devices would increase the number of implementations they need to securing networks and devices.

Some of the future trends of cybersecurity includes:

- Increased attacks on remote workers and IoT devices.
- Sophisticated ransomware attacks.
- Increased cloud security threats.
- Increased phishing attacks.

Cybercriminals have always taken advantage of the rapid growth of technology. By following the guidelines recommended by the cybersecurity framework of your choice, your business can always stay one step ahead of these attacks by implementing the right security measures in detecting and mitigating those attacks on time.

> “ According to Gartner, by 2025, 60% of organization would start using cybersecurity risk as a primary determent in conducting third-party transactions and business deals.