
ISAUnited

International Security Architects

# Cybersecurity Architecture

www.isaunited.org

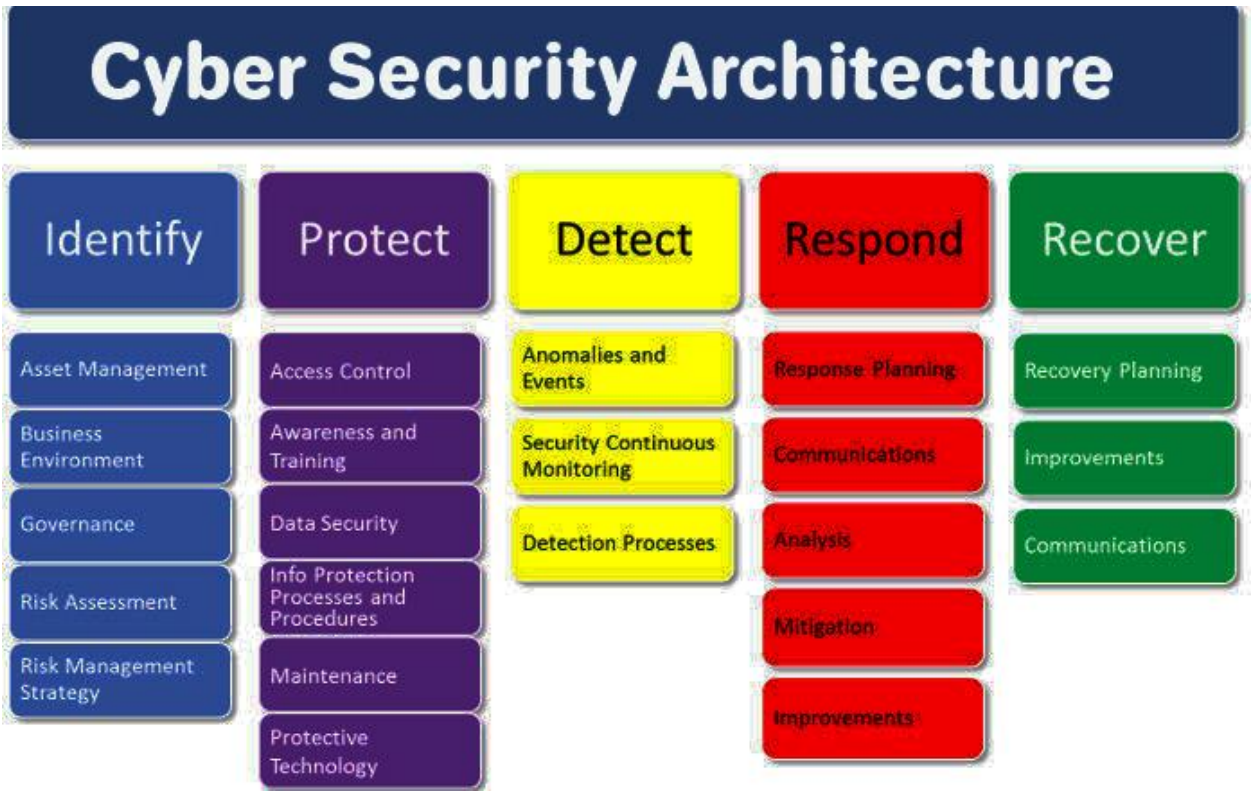
# Cybersecurity Architecture

## Introduction

Cyber security is a strategy for securing technology and systems against external assault and hacking. Businesses typically engage Cyber Security architects to protect sensitive data, which increases consumer trust in the organization. The three most important aspects of cyber security are integrity, privacy, and availability. The term "integrity" refers to the fact that information may only be changed by authorized users; "Privacy" refers to the secrecy that private data must be safe and only accessible to authorized parties, while "Availability" indicates that services or data must be available On Demand within agreed-upon limits. Along with these three elements, one of the most important aspects of cyber security is the use of authentication techniques. A username, for example, identifies an account that a user wishes to access, but it is the password that secures that account (Cisco, 2019).

## Cybersecurity Architecture

The security of every part of an organization's IT infrastructure is guaranteed by a cyber security architecture, which forms the basis of the company's cyber defense. An infrastructure for cyber security safeguards the following environments:




If a company's cyber security architecture adheres to all seven rules of the Zero Trust security model, it can protect its data and IT resources no matter where they are;

Seven Rules

1. Devices
2. People
3. Data
4. Networks
5. Workload
6. Automation & orchestration
7. Visibility & analytics

## Role of Cyber Security Architecture

The main objective of a cybersecurity architecture is to guarantee that your company's most sensitive data, including its critical applications and key network architecture, is effectively protected against any threats or security breaches that may arise in the present or the future. A properly developed and enforced cybersecurity architecture may enhance cybersecurity, help your company comply with ever-stricter data protection regulations as they emerge, and increase your marketability in a market that is becoming more and more cyber-aware. When properly implemented, a strong cybersecurity architecture will be most noticeable in three crucial areas of your business: regulatory compliance, financial performance, and information management in general (*What Is Cyber Security Architecture?* 2022).

## Regulatory Compliance

The deployment of a cybersecurity architecture is required by several data protection standards as proof of compliance. Most businesses are subject to a variety of data standards, especially those operating globally. Most data protection regulations now call for a cybersecurity architecture of some form. A strong cybersecurity architecture should overcome the differences between different regulations' information management needs. Any regulatory organization will almost always see one's mere existence favourably.

## Bottom Line

Consumers are becoming aware of cybersecurity risks and how such issues might influence their life, as was previously said. Make use of the chance to promote your business' outstanding cybersecurity to your clients. Customers are more likely to trust transparent companies, especially those that have already suffered security breaches. The financial line of your company may be protected by a strong cybersecurity architecture, which can also serve as insurance against a variety of potentially disruptive situations. A proactive strategy for cybersecurity is typically considerably more effective than a defensive or a reactive one, as the cost of responding to a security event can frequently be more than the initial expenditure required to establish a cybersecurity architecture.

## Information Management

Your company's success or failure may depend on how it manages its data. Data management procedures may be made more efficient with the added benefit of securing the information network of your systems by integrating a cybersecurity architecture across your whole company. With little to no disruption to the regular operation of your organization, a cybersecurity framework should match the risk management procedure with your overarching business strategy.

## Features of Cybersecurity Architecture

This section will highlight upon some of the key features of Cyber security Architecture.

### The network's components

A device that connects to computers and gateways, as well as other network nodes, is referred to as a network node. Many distinct protocols, including HTTP, and IMAP are used by networks to communicate. To link nodes (point-to-point, chain, circular, and hybrid) on a network, protocols are employed.

### Security Passwords

Firewalls, encryption, and decryption tools are only a few examples of the various kinds of cyber security hardware available. The software bundle comes with antivirus, spyware, and antimalware programs. Aside from other methods like HTTPS and FTTP, network protocols like IMAP and TCP/IP are also secured by encryption. End-to-end encryption, zero-privacy knowledge, and block chain technology are the best data protection options.

### Methods for Data Security that are Standardized

Standardization for an architectural cyber security framework includes.

- The IEC 27000 series
- NIST Risk Management Framework SP 800-37

There are several technical requirements for cyber security architecture examples.

## Instructions and Policies for Security

They are the security guidelines and practices that your company has discussed and put into place. According to this forum, a perfect architecture for cybersecurity should be spaced out and simulated using a language for modelling architecture that is accepted in the industry (e.g., SysML, UML2). One must comprehend the essential processes required, even if just managed to only scratch the surface of cyber security architecture. The exercises performed by the security architecture framework are:

## Architectural Risk Evaluation

This section analyses a major business asset, a risk, and the outcomes of security threats. The security architecture is designed in a way to protect organization's assets and to help the managers in assessing risks objectives.

## Implementation

The cyber security architecture is designed in a way to everything including security norms, considerations of security architecture, and activities if risk management go as per planned.

## Control and Monitoring

It is used to monitor and manage the operating status. as well as via threat and vulnerability management to assess the impact of system security (*What Are the Features of Cyber Security Architecture?* 2022).

## How to Build a Strong Security Architecture Framework

One can protect cybersecurity architecture from corruption by building a strong foundation. A few fundamental stages form the basis of building a solid security architecture framework:

Initially, use an existing enterprise network security architecture: You may find a variety of corporate information security architectural frameworks online and get ideas from them. You can also look at what others have done in the past to create their enterprise security architectures. Essentially, you may take parts of that framework and modify them to suit your needs rather than adopting it as your "start to finish" solution (Ghaznavi, 2017).

- Choose Your Specific Requirements: Instead of attempting to solve every problem with a single framework, it might be good to decide what your major problems or needs are. Then, you can utilize that knowledge to kick-start the design of your security architecture. This aids in concentrating your efforts and easing the transition for your company so that your security framework deployment may be carried out without placing an unnecessary burden on your resources.
- Obtain All Levels of Your Organization's Support for the Cyber Security Architecture Framework: Getting support for the program from employees at all levels of the company, from the CEO down to the front-line staffers managing their daily job lists, is one of the cornerstones of any effective network security architecture deployment.
- Communicate Expectations and Changes Moving Forward Clearly: Effective communication is critical for an organization's objectives to be met, and building a security architectural framework is no different. Being able to communicate

expectations helps you ensure that everyone in your organization is equipped to follow your security architecture framework by ensuring that everyone in your organization is aware of the requirements and outlining the ramifications of noncompliance for both the organization and the individual.

## Cybersecurity Architect

A cybersecurity architect is responsible for building and protecting the cybersecurity architecture. The information technology network of a company, which includes computer systems and data, must have security mechanisms in place, and an architect of cybersecurity oversees planning, developing, and maintaining those systems. They are, in other words, the authority figure and the go-to source for cybersecurity-related issues (Terra, 2019).

## REFERENCES


Cisco. (2019). *What Is Cybersecurity?* Cisco. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Ghaznavi, R. (2017). *How to Build a Strong Security Architecture Framework - Google Search*. ISACA JOURNAL. https://www.google.com/search?q=How+to+Build+a+Strong+Security+Architecture+Framework&oq=How+to+Build+a+Strong+Security+Architecture+Framework&aqs=chrome..69i57j69i176j69i58.448j0j4&client=ms-android-samsung-gj-rev1&sourceid=chrome-mobile&ie=UTF-8

Terra, J. (2019, November 18). *A Step-by-Step Guide to Become a Cyber Security Architect [Updated]*. Simplilearn.com. https://www.simplilearn.com/why-become-a-cyber-security-architect-article

*What Are The Features of Cyber Security Architecture?* (2022). Careerera.com. https://www.careerera.com/blog/what-are-the-features-of-cyber-security-architecture

*What is Cyber Security Architecture?* (2022). Www.knowledgehut.com. https://www.knowledgehut.com/blog/security/cyber-security-architecture