techwave

Secure your Digital Presence with the highest level of Cyber Protection

Cyber-attacks are an alarming threat to all types of businesses & organizations. The risk of a cyber-attack is not just a risk to your company but also to your privacy. Hence, cybersecurity is crucial for every business.

If you are looking for tools to fight against cyber threats, then Techwave's tools & technologies with adequate controls will help your organization stay protected.

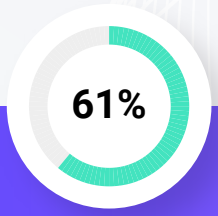
Index

Introduction

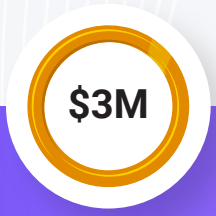
Cyberattacks have become increasingly common and severe over the past few years. Hence, cybersecurity is a crucial concern for businesses today, particularly for small and medium enterprises.

Also, the stake for businesses has grown exponentially, making it essential for everyone in the company, from the CEO to entry-level employees, to be aware of cybersecurity risks and best practices.

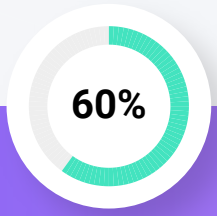
According to Data Breach 2022 Report



Small businesses experienced a cyber-attack in recent times



Average data breach cost per individual incident



SMEs go out of business within 6 months of a cyber-attack

The reports show that cyber-attacks are widespread, and the cost of recovery can be crippling for a small business. Hence, it's not surprising that several SMEs collapse post a cyber-attack.

Thus, ignoring crucial steps for data protection could put your entire company at risk.

Why is Cybersecurity Important?

Cybersecurity protects critical data from cyber attackers. This includes sensitive data, governmental and industry information, personal information, personally identifiable information (PII), intellectual property, and protected health information (PHI).

Did You Know Fintech's are the Prime Target of Cyber Attacks?

The finance sector is a major target for cybercriminals because it offers many opportunities to make money through theft, fraud, and extortion.

In addition, nation-state-sponsored groups are increasingly targeting the finance sector to gain political and ideological power.

The Consequences of Cyber Crime

Individual

Leak of confidential information, monetary loss due to online theft

Business

Reputational Damage, Loss of revenue, Operational Disruptions

Government

Breach of military secrets or other sensitive information

Organizations must adopt a proactive approach to security operations and implement a comprehensive cybersecurity transformation process. This will enable them to improve services while reducing costs and risks.

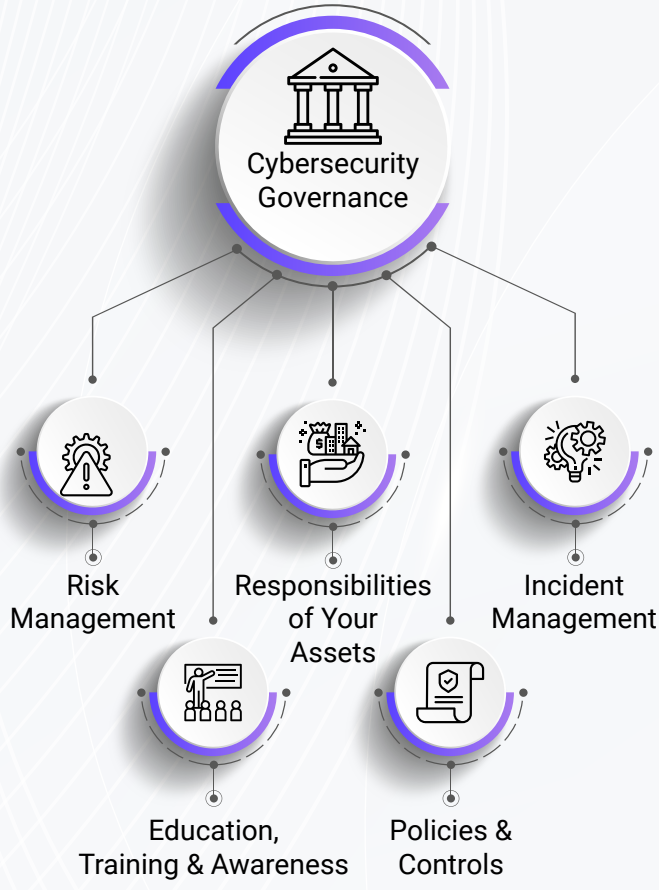
Cybersecurity Governance

01 Cybersecurity governance gives a strategic way to direct and control your organization's approach to security.

02 This means defining the level of risk they are willing to take, building an accountability framework, and ensuring a clear chain of command regarding decision-making.

03 In coming years, managing cybersecurity risk will require businesses and their operations to change radically to make themselves more secure and build security controls.

04 All organizations are different, and each board needs to set its direction and tone for cybersecurity based on the organization's nature and risk appetite.



For this reason, a principles-based approach is necessary to govern cybersecurity. It allows each board to establish its direction within a recognized framework.

Governance Principles to Adopt for Cybersecurity

Education, Training, and Awareness

Many organizations need to fully understand why they could be potential targets for attacks, what vulnerability factors expose them to attackers, and how attacks could impact them. This lack of awareness can leave organizations vulnerable.

Training Methods

Set cybersecurity training goals for each employee and plan the training at least once a quarter.

Use real-life examples, games, and storytelling to capture attention and interest and ensure materials and resources are easily accessible.

Ensure that each team member knows whom to contact if they have queries or concerns.

Policies & Control

A holistic approach to cybersecurity goes beyond just building and operating effective security controls.

Recognized frameworks, such as those published by the US National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO), can help define required cybersecurity controls.

It must reduce the complexity of the technology stack and data sets that those controls apply to, both inside and outside the organization.

It's essential to take a broader approach that also looks at meaningful measurement metrics and the extent of exposure to potential cyber threats.

Asset Responsibilities

Every asset, from laptops to mobile devices to wireless printers and apps, has the potential to leave your organization vulnerable.

So, every team member should understand the risks and best practices for handling data, devices, and systems securely by following these steps.

Step 1

Create a map of your key data and technology assets

Step 2

Identify the systems and physical assets within your organization

Step 3

Determine who is responsible & what is required to safeguard the asset

Risk Assessment

01 Conducting a comprehensive risk assessment is key to understanding your organization's specific threats and vulnerabilities.

02 Techniques such as 'red team testing' by skilled penetration testers are highly recommended to assess the strength of individual critical controls and systems.

03 After discovering areas of weakness – like outdated systems or recent phishing tactics, take steps to address these issues and improve your organization's security program.

04 Lastly, measure the speed at which you can address the identified issues.

Incident Management

01 Incidents must be tracked and reported accurately to learn from them and eliminate their possibility in the future.

02 Organizations must be able to respond appropriately to reports of vulnerabilities that could make products, services, or internal processes vulnerable to attack.

03 This includes well-planned strategies that address technical, business, reputational, management, legal, and regulatory risks.

04 The approach to incidents and vulnerabilities must also consider suppliers and service providers and not just focus on the organization.

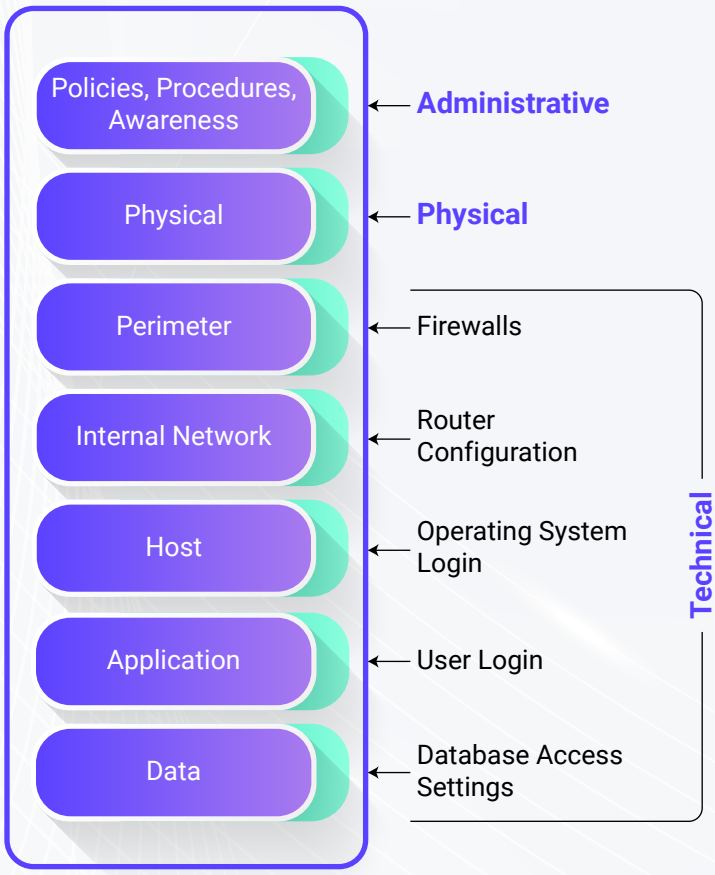
Cybersecurity Strategies

There are many strategies that organizations can adopt to protect their assets, such as the defense-in-depth approach, which consists of multiple layers of security, or the 3-tier network security model.

By implementing these measures, organizations can ensure the safety of their data and resources.

Defense-in-Depth Strategy

- The "defense-in-depth" information assurance strategy provides multiple backup security measures if a control fails or a vulnerability is exploited.
- This strategy is borrowed from the military defense strategy, which aims to delay an attack rather than defeat it with one strong line of defense.
- Defense-in-depth security architecture is a comprehensive network security approach that considers physical, technical, and administrative controls.
- By taking a layered approach to security, you can better protect your network against various threats.



Digital Certificate

A Digital Certificate is an electronic file that uses a key pair to authenticate the identity of websites, individuals, organizations, users, devices, or servers.

It is also called a public key certificate or identity certificate. The certificate contains the subject's identity as well as a digital signature.

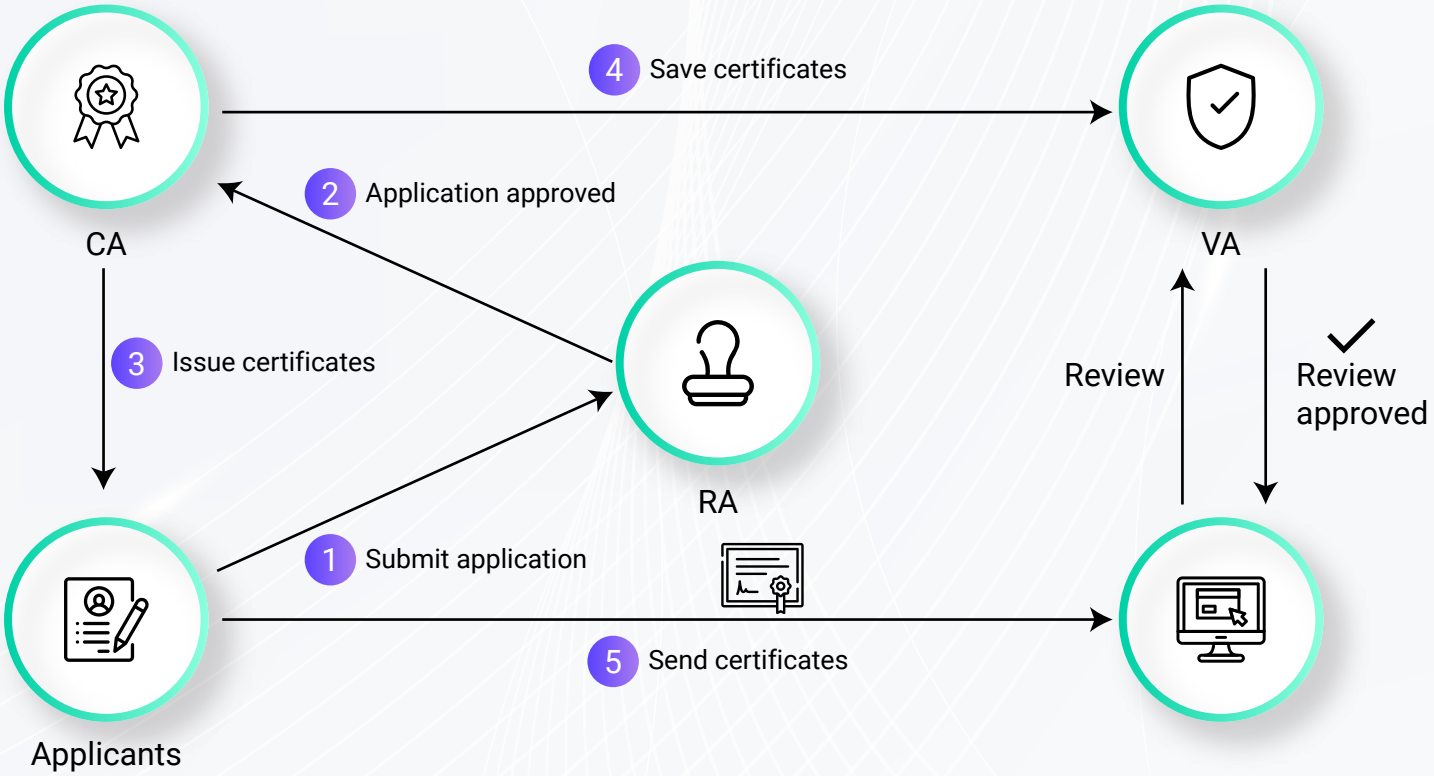
Uses

- Digital certificates offer a high level of security for websites, devices, web servers, signatures, code, software, email, and more.
- They can help encrypt data, activate HTTPS in the URL bar, and prove the legitimacy of a website.
- They help comply with PCI standards, improve website SEO rankings, and strengthen a brand's identity.

How to Get a Digital Certificate?

The digital certificates are issued by an external certification authority. The process of issuing and provision of a digital certificate is explained below.

Digital Certificate Issuance Process



01 Applicants submit certificate requests to the Registration Authority (RA).

02 RA then verifies the applicant's request and forwards it to the Certificate Authority (CA).

03 The CA issues the certificate to the applicants.

04 The CA also submits the same to the Verification Authority (VA) for preservation.

05 The applicant can then send the certificate to the client. Once approved by VA, the process is complete.

Techwave's Approach to Cybersecurity

Techwave is an ISO/IEC 27001- certified organization. Techwave is committed to protect the organizational and clients' information and data from internal and external threats by implementing a framework with adequate controls, tools and processes.

Information Security Objectives Contains

Techwave Cybersecurity Solutions

1. Our security experts have a proven track record of delivering innovative solutions to leading companies across various industries.

2. We excel in assessing the feasibility and performance of business processes and architecture and optimizing and securing them.

3. Our team is dedicated to helping our clients stay ahead of the curve and protect their businesses against potential threats.

4. Our security experts will evaluate your business and IT infrastructure to determine what security measures need to be implemented.

5. We provide a comprehensive road map for Private, Public, and Hybrid Cloud security for your specific business needs and then implement and integrate various security products and solutions.

6. We always follow up our assessment with a strategic plan and proof-of-concept (POC) implementation.

techwave

Techwave is a leading global IT services and solutions company that helps clients worldwide scale their offerings by leveraging its expertise in Digital Transformation, Enterprise Application, and Engineering Services. Founded in 2004, Techwave has 1,400+ employees across 11 countries, and serving 500+ customers.

Global Headquarters

13501 Katy Fwy Suite 1000, Houston,
TX 77079, USA.
Ph: +1 281 829 4831
infoNA@techwave.net

APAC Headquarters

Suite 104, 18-20 Ross Street,
Parramatta, Sydney, NSW 2150, Australia,
Ph: +61 398 678 903
info@techwave.net