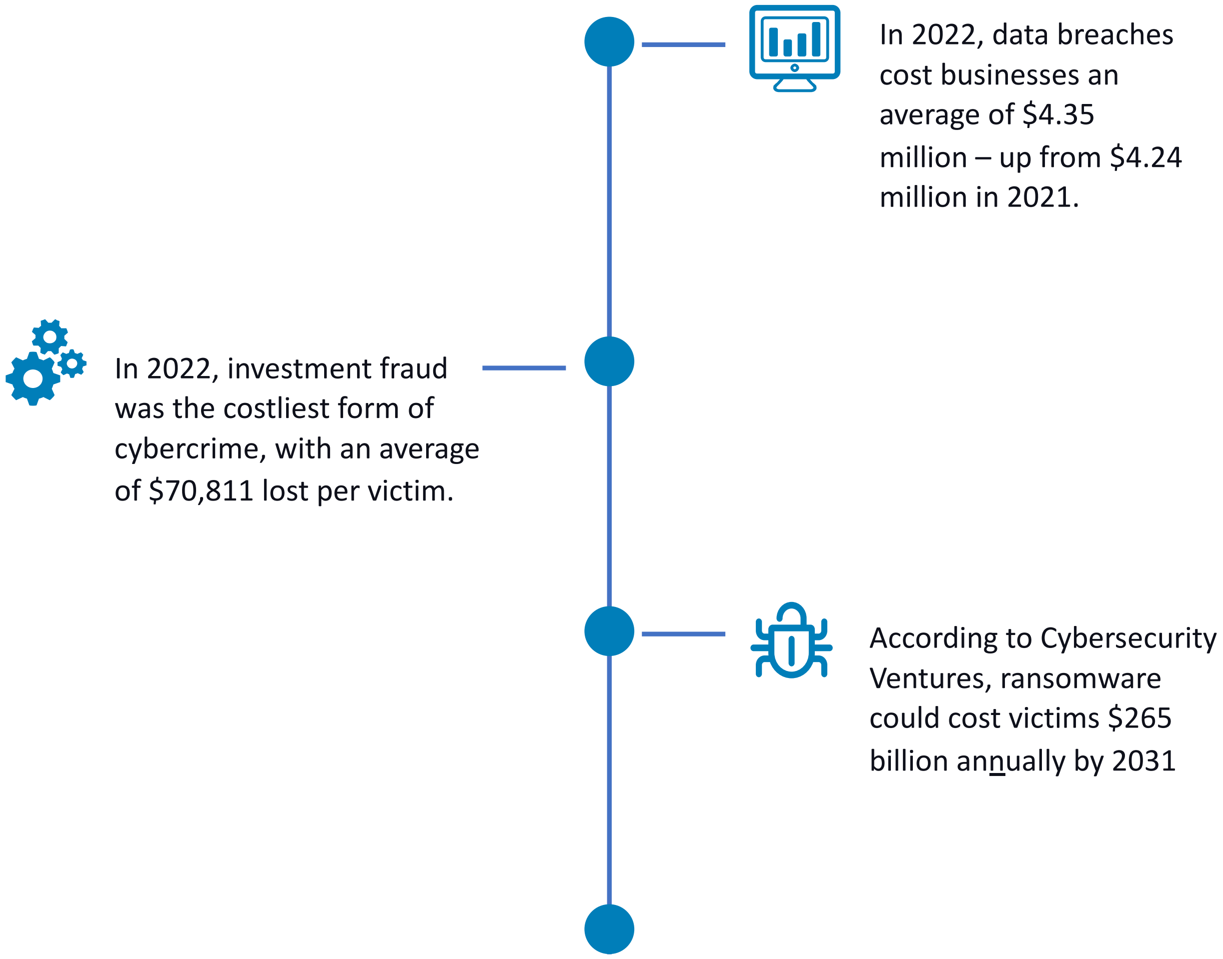
Cybersecurity

The Way Forward

Cybersecurity

Consider This:



In 2022, data breaches cost businesses an average of $4.35 million – up from $4.24 million in 2021.

In 2022, investment fraud was the costliest form of cybercrime, with an average of $70,811 lost per victim.

According to Cybersecurity Ventures, ransomware could cost victims $265 billion annually by 2031

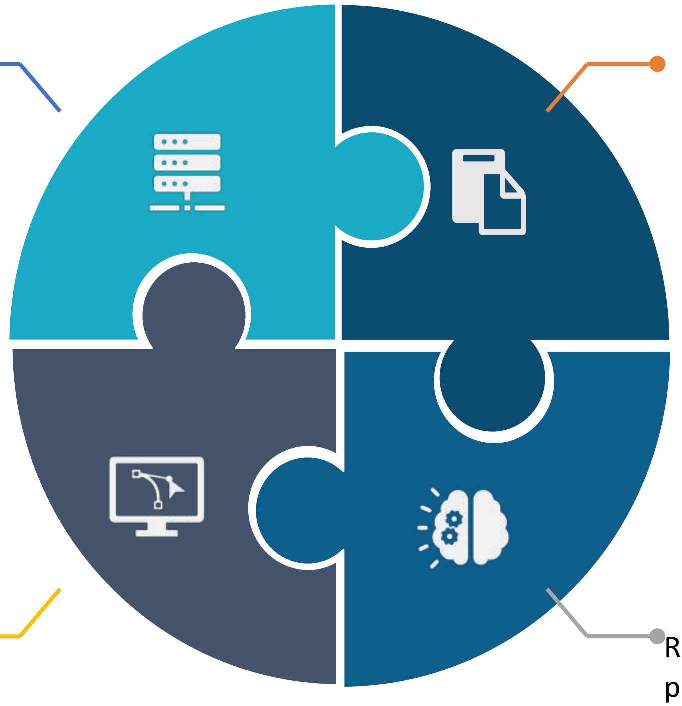
- **Cyber Security is one of the building blocks of an organization’s digital presence.**
- Organizations constantly invest in technologies to run their business, adding more layers to their IT systems to support remote work, improve customer experience or create opportunities.
- The scope of a cyber-attack is constantly growing.
- The days of single adversaries are long gone. Now there are sophisticated organizations with integrated tools leveraging AI and machine learning.

Access to ubiquitous data is increasing.

The Internet of Things made it possible for mobile apps, remote work, and other connected devices to work on quick access to data, increasing the chances of a breach.

Organizations collect large amounts of data from their consumers to understand purchasing and consumer behavior, and cyber-attacks target this sensitive information.

The cloud, remote work, and IoT have many vulnerable points.



Zero Trust Architecture

A **ZTA** focuses on users, assets, and resources, granting access through strict policies.

Users have access to the data environment but not all sensitive data.

Homomorphic Encryption

Allows users to work with encrypted data without decrypting it, ensuring secure access to large data sets.

Helps organizations meet stringent data privacy regulations and requirements.

Elastic log monitoring

Solution of using several open-source platforms together to pull log data from anywhere in the organization to a single location.

Search, analysis, and visualization of data can then take place in real-time.

Behavioral Analytics

Recognizes that employees are potential vulnerabilities.

It allows for risk-based authentication and authorization.

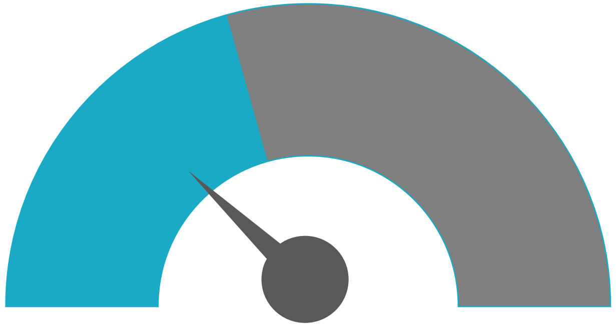
Orchestrates preventive and incident response measures.

Massive data sets and decentralized data logs make it a challenge for active data monitoring.

Sophisticated Attacks

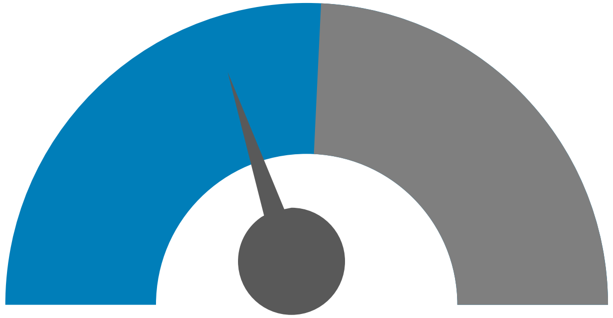
Cyber-criminals are using AI, machine learning, and advanced technologies for cyber-attacks, and organizations need to scale up and do the same. Organizations should take a risk-based approach to automation to counter cybercrime.

Automation



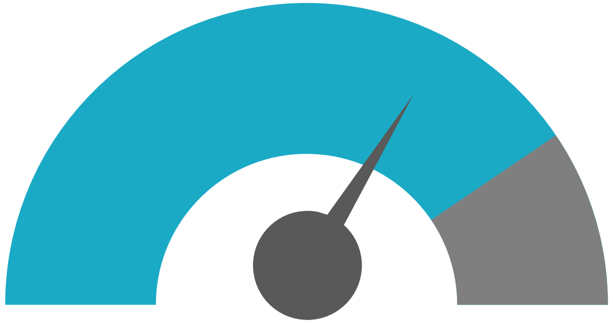
Automation for low-risk processes frees up resources for high-value activities.

Tech Changes



Include robust infrastructure and data repositories, automated responses to malicious encryption, and advanced multifactor authentication to reduce the potential damage from an attack.

Org Changes



Thorough contingency plans and executive response decisions help make business responses automatic.

Gaps in resources, knowledge, and a cybersecurity talent pool

- Cyber risk management has not kept up with rapidly evolving cyber-crime with gaps in cybersecurity talent, knowledge, or expertise.
- High-profile breaches and privacy concerns have also resulted in stricter compliance and regulatory requirements.
- **Secure Software Development*****:*** Rather than treating cybersecurity as an afterthought organizations must make it a part of software development from inception.
- **Use of third-party cloud platforms:** Such as platform as a service, infrastructure as a service, and hyperscalers to manage infrastructure, and migrate workloads. It helps secure organizational resources and simplify cyber security. Cloud providers handle routine security, patching, maintenance activities, automation capabilities, and scalable services.
- **Infrastructure and security as code:** The standardizing and codifying infrastructure and control engineering processes simplify the management of hybrid and multi-cloud environments. E.g.: orchestrated patches, rapid provisioning, and de-provisioning.

Cybersecurity losses are an inevitable cost of doing business in a digital age. Organizations need to look at anticipatory compliance; study and plan for potential attacks instead of being reactionary

DIGITAL FABRIC®

THE TI FRAMEWORK

INFO@DIGITALFABRIC.IN