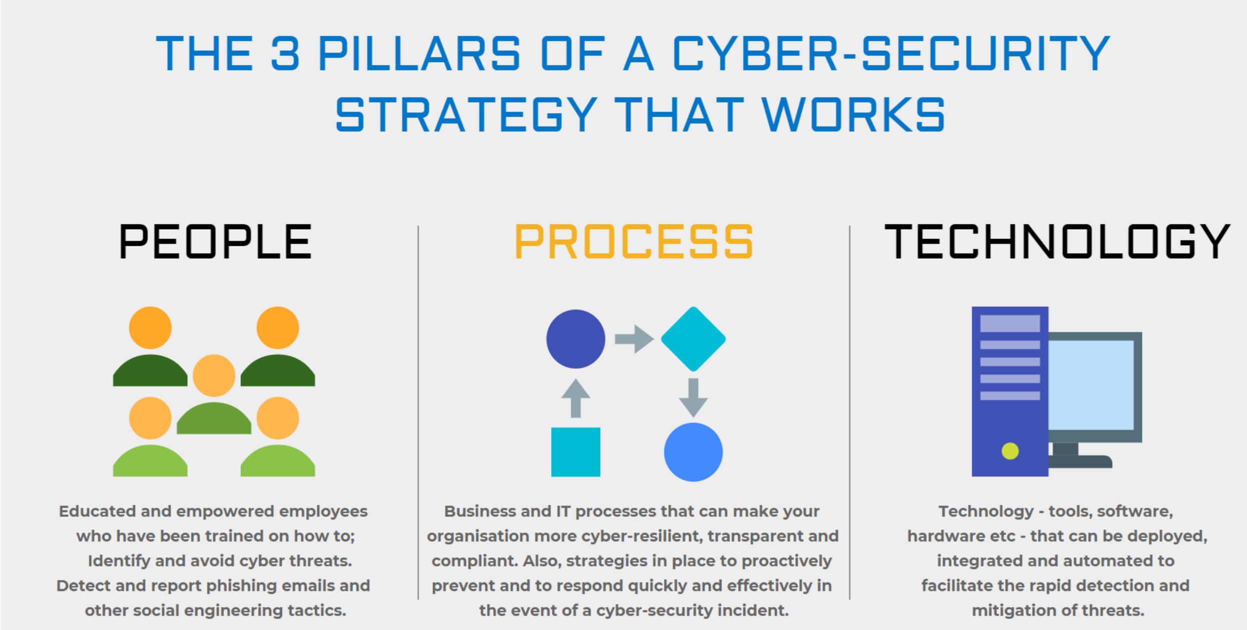
Cybersecurity Model:

Secure your organization with the Three Pillars Cyber Security model. These three pillars of Cyber Security are people, processes, and technology. Should all work together to build a sturdy defense network. You should have strong mechanism to protect your organization with help of People, Process and Technology.



THE 3 PILLARS OF A CYBER-SECURITY STRATEGY THAT WORKS

PEOPLE

Educated and empowered employees who have been trained on how to; Identify and avoid cyber threats. Detect and report phishing emails and other social engineering tactics.

PROCESS

Business and IT processes that can make your organisation more cyber-resilient, transparent and compliant. Also, strategies in place to proactively prevent and to respond quickly and effectively in the event of a cyber-security incident.

TECHNOLOGY

Technology - tools, software, hardware etc - that can be deployed, integrated and automated to facilitate the rapid detection and mitigation of threats.

People:

People are, statistically speaking, the most important pillar of your cybersecurity strategy. Research suggests up to 90 percent of all cybersecurity breaches are caused or aided by human error. IT teams are trained with the latest cyber security skills and qualifications to implement the controls, technologies, and best practices for your organization.
Cyber Attackers use highly sophisticated methods of targeting front-line employees and even CEOs. That is why most of security breaches are blamed on human error, proving people to be the weakest link in Cybersecurity. However, with right processes & training programs they can be turn into HUMAN FIREWALL which will Immensely help us in tackling cyber security threats.

Everyone in the business needs to be aware of their role in preventing and reducing cyber threats, Cyber security is a business issue and everyone has a role to play. A crucial step in preventing and reducing cyber threats is ensuring that all your staff understand their cybersecurity role. Your team needs to be aware of company policies to mitigate and respond to cyber risks. They also need to know how to identify possible phishing attempts. Your people should always be mindful of the importance of using only secured and company-approved devices. Communicate any new processes for handling sensitive data to all staff. Ensure that your IT and cybersecurity staff have the latest skills and qualifications. They should be competent and carry out a regular risk assessment.

95%
of all successful cyber attacks
is caused by human error
Source: IBM Cyber Security Intelligence Index

Process:

Bring in a coherent structure, and way of working to mitigate risks or deal with threats in real-time. Continually update documents because hackers are constantly evolving their attack techniques. Processes are key to the implementation of an effective cyber security strategy. this should be defined, repeatable, and improvable steps you document and train on to perform a function. This pillar of cybersecurity ensures that their cybersecurity have strategies in place to proactively prevent and to respond quickly and effectively in the event of a cybersecurity incident. there are many processes & programs in cybersecurity. A company's processes refer to activities, roles and documentation. These are the procedures that the organization uses to ensure and track cybersecurity. You need to constantly review and update strategies to deal with any new cyber threat.

Technology:

Technology without a doubt raises the levels of defense. However, if implemented without proper planning, or a limited understanding of the environment it is intended to defend, it will become a root cause of many more problems. This pillars in cybersecurity involves putting the right systems in place to automate processes and make them smarter and more effective. There are a host of technologies that security teams can implement in order to layer their defenses. Perimeter firewall, IDS/IPS, Application Gateway firewall, physical security, Deception, Mail security, DNS Security, Secure DMZs. Network firewall, UTM, Secure remote access, NAC, Inline Patching, Wireless access control, VOIP security. Perimeter Security, Network Security, End Point Security, Application Security, Data Security, Security operation and Cloud Security.