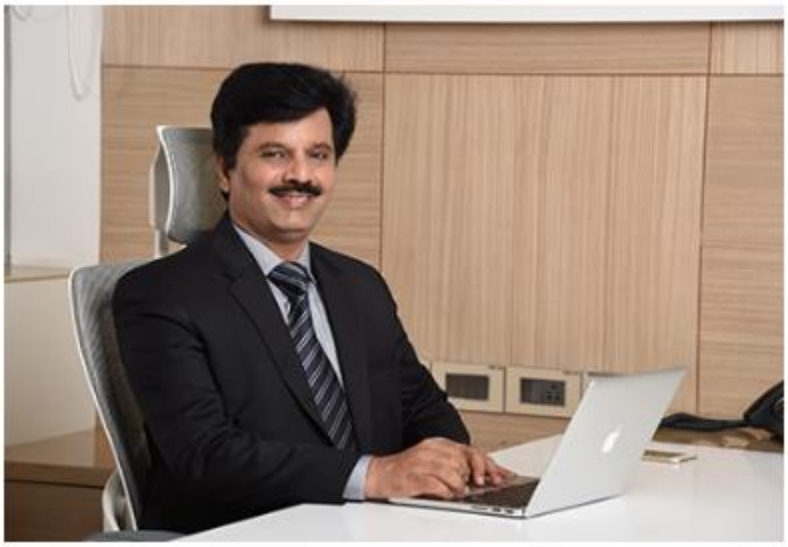
Realizing the Vision of a Cyber Safer Country - Steps to Prevent Cyber-Attacks!

Dr. Kailash Katkar, Managing Director & Chief Executive Officer, Quick Heal Technologies Limited



In the digital age, technology has been dramatically transformed almost every aspect of our lives. From connecting people and resources around the world, facilitating remote work and learning, to opening up opportunities for innovation and growth. However, along with the benefits, there are also significant risks, particularly in the form of cyber-attacks.

Recently, the frequency and complexity of cyber-attacks have increased, and are now a significant threat to individuals and organizations worldwide. The consequences of a successful cyber-attack are severe, not just limited to an individual's or business's financial loss or reputational damage, they are also capable of disrupting economies.

It is expected to see a greater uptick in the emergence of more evolved cyberthreats, such as an increasing number of spyloan applications carrying our financial frauds, exploitation of remote work and cloud dependency for infiltrations, and the adoption of new and advanced tools and techniques by threat actors. A rise in Crime as a Service (CaaS), Malware-as-a-Service (MaaS) and Ransomware-as-a-Service (RaaS) is also anticipated in the coming months. All this highlights the urgent need for smart and futuristic cybersecurity solutions for both – individuals and enterprises.

Technology Advancements Adding to Cybersecurity Complexities

The accelerated digitization is the new mantra for growth for the government, enterprises, educational institutions, and sadly it is the same for the cyber attackers as well. For example, while cloud computing has provided organizations with the ability to store and process large volumes of data, it has also introduced new security risks that need to be addressed. IoT devices are widely used in various industries,

but they are often vulnerable to cyberattacks. To reduce such risks, enhanced security measures, such as access controls, data encryption, device authentication, secure boot, and firmware updates need to be implemented.

Artificial Intelligence (AI), while being a great enabler, has itself become a cybersecurity challenge, since it can also be exploited by cybercriminals to launch more sophisticated attacks. This has prompted the deployment of AI-based security measures to prevent such attacks. A survey by International Data Corporation (IDC) estimates that AI in the cybersecurity market will reach a market value of $46.3 billion in 2027, registering a CAGR of 23.6 percent.

To address the increasingly sophisticated cybersecurity challenges, governments and businesses must take proactive steps to protect themselves from cyber threats. The Union Budget of 2023 has rightly recognized the importance of being a knowledge and technology-driven economy, and the initiatives such as setting up three AI centers, a national digital library and digital platform for agriculture are crucial steps in the right direction.

While most organizations and home users have certain cybersecurity solutions deployed, their efficacy varies. Most free versions of antivirus software can be bypassed by modern-day threat actors which are deploying increasingly sophisticated techniques to infiltrate into systems and steal valuable data.

Cyber Securing Individuals

However, it is essential to recognize that individuals and organizations are the most vulnerable of all times. Thus, they must take a proactive approach to protect themselves from ever evolving cyber threats. Firstly, it is extremely important for all of us to recognize the need for adopting cyber safety and then adopt the relevant solution for our digital protection.

Individuals can be cyber secure by simply following these steps:

•Educate yourself about cyber safety.
•Use strong and unique passwords.

•Always choose the full version of paid antivirus over the free or basic version that doesn’t guarantee complete protection.

•Configure the software correctly during installation, if required get help of an expert.

•Keep your Antivirus software and security systems updated.

•Be cautious of any cyber scams such as phishing scams.

•Avoid public Wi-Fi.

•Back up your data.

Cybersecurity is a shared responsibility, and all employees should be trained on best practices for protecting data and IT assets. This includes training on how to identify and report suspicious activity

Ensuring Organizational Cybersecurity

Most organizations today are realizing the need to factor in cybersecurity into their budgets. They are beginning to realize that in comparison to the damage a cyber-attack can cause, the cost of deploying security measures is fractional. They are also understanding that cyber safety of the data and IT assets is not just the responsibility of IT experts alone, it is rather a shared responsibility organization wide.

Some steps for enterprises to follow to stay ahead of the curve:

•Develop a cybersecurity strategy: This involves identifying the organization's IT assets, evaluating their risk levels, and developing a plan to mitigate those risks.

•Deploy security tools: There are a variety of security tools available, including firewalls, antivirus software, and intrusion detection systems. These tools can help to detect and prevent cyber-attacks.

•Keep software up-to-date: Outdated software can have vulnerabilities that can be exploited by cybercriminals. It's important to keep all software up-to-date with the latest security patches and updates.

•Implement strong access controls: Access controls are essential for preventing unauthorized access to sensitive data and IT assets. This includes strong passwords, multi-factor authentication, and limiting access to only those who need it.

•Train employees: Like I said, Cybersecurity is a shared responsibility, and all employees should be trained on best practices for protecting data and IT assets. This includes training on how to identify and report suspicious activity.

•Conduct regular risk assessments: This is an ongoing process that involves regularly evaluating the organization's IT assets and identifying any vulnerabilities or threats.

•Monitor and respond to incidents: Even with strong security measures in place, incidents can still occur. It's important to have a plan in place for responding to incidents and minimizing the damage. This includes monitoring for suspicious activity and having a response team in place.

By following these steps, enterprises can stay ahead of the curve in cybersecurity and protect their data and IT assets from cyber-attacks.

Overcoming Cybersecurity Challenges
The lack of cyber safety awareness in our country is a pressing concern that demands our immediate attention.

It is heartening to see that our government is also focused on realizing the vision of a cyber safe country. Let’s work together to create a safe and secure digital ecosystem for everyone and empower one and all, with the knowledge and skills required to stay safe in the digital world.