
FOURTH
DIMENSION
expect more
What Are
Cybersecurity
Services?

Cybersecurity refers to a company's protection against unauthorized or criminal activities via electronic data. Cybersecurity services are the overall processes put in place to achieve security and protect against common cyber threats.

These are common threats that cybersecurity services target can include:

- Malware or malicious software is a program installed into a system to compromise the data's availability, integrity, and confidentiality. These programs are discreet but have become one of the most significant external threats that businesses face today.
- Ransomware: Ransomware is also a type of malware that limits access to your system through encryption and then asks for a "ransom." It decrypts your system and regains access.
- Phishing: Cybercriminals use the Phishing technique to gain data by impersonating respectable business personnel. They'll usually send you an email with a warning about your account and a link to a bogus website asking for passwords or any essential pieces of information.
- Distributed denial of service (DDoS) attacks obstruct network access by flooding a network with traffic requests, slowing website response time. It's frequently employed as a diversionary tactic while crooks engage in other forms of cybercrime.

Problems Cybersecurity Solutions Solve

Businesses of any size and type experience an array of possible security vulnerabilities every day. Cybersecurity solutions can mitigate problems such as these:`

- **Human error:** Employee error — not malicious intent — is the biggest reason for data breaches. Web filtering and other cybersecurity tools lessen the risk of human error by stopping employees from accessing harmful sites and falling prey to phishing schemes.
- **External threats:** Hackers are increasingly skilled in finding ways to get around traditional firewalls and steal your data. Cybersecurity services ensure your firewalls, antivirus software, and other solutions are continually up-to-date and ready to protect your infrastructure.
- **Insider criminal activity:** Unfortunately, one of the most challenging realities for small and large businesses is stealing data from within the organization. It is better to use security solutions to safeguard your information from the inside and provide access only to those who need sensitive data.
- **Unsecured cloud storage:** With the popularity of cloud servers, cloud storage security breaches are also on the rise. However, network security services ensure that the cloud systems have proper security to avoid any data breaches.
- **Third-party app security:** Not all third-party apps are created, keeping your company's safety in mind. Also, many third-party apps don't come with sufficient updates or security measures. Therefore, cybersecurity weeds out these apps as unsafe and puts security checks that many apps lack.

What Your Company Can Do

Industry Practices that companies must adopt:

- Use antivirus software at all times and make sure it automatically scans your emails and removes any media (e.g., flash drives) for ransomware or malware attacks.
- Keeping all systems patched with security updates.
- Using security products or services that will block access to ransomware sites on the web.
- Use third-party software to configure operating systems only to authorized applications to run on systems to prevent ransomware from working.
- Restrict or prohibit the use of personal devices on your organization's networks unless s unless you're taking extra measures to assure security.

What Your Employees Can Do

Employees can follow these tips for their work systems:

- Use of standard user accounts instead of administrative privileges whenever necessary.
- Avoid using personal applications and websites on work computers, such as email, chat, and social media.
- Avoid opening any file or clicking on links from unknown sources without checking them. Ask employees to run an antivirus scan on a file to scrutinize it.

How Can You Recover Quickly from A CyberAttack?

Despite all of these protective measures, bad actors may still worm their way into your systems. Your organization needs to be prepared for these attacks by taking steps to ensure that the information isn't corrupted or lost and that normal operations can resume quickly.

Cybersecurity Pundits are recommending that organizations follow these steps to accelerate their recovery:

- Develop and implement an incident recovery plan
- Role and Responsibilities are clearly defined for any decision-making.
- Carefully plan, implement and test a data backup for restoration strategy.
- Ensure to secure backups of all your essential data
- Make sure to take backups and keep them isolated to save from ransomware attacks.
- Maintaining an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement

About Fourth Dimension Technologies

Fourth Dimension Technologies empowers communities and nonprofits to use technology to serve the world better. We create custom IT solutions tailored to your organization's needs using our "Proprietary transformation model." Being a leading provider of technology and solutions for nonprofits and their communities, we design budget-friendly technology services that maximize your nonprofit's return on investment, so you can better serve the community.

www.fourdtech.com
marketing@fourdtech.co.in