

## what is cybersecurity?/

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cybersecurity and physical security

Ensuring cybersecurity requires coordinated efforts throughout an information system. Elements of cybersecurity include

Application security

Information security

Network security

Disaster recovery / business continuity planning

Operational security

End-user education

One of the most problematic elements of cybersecurity is the quickly and constantly evolving nature of security risks. The traditional approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment. Adam Vincent, CTO-public sector at Layer 7 Technologies (a security services provider to federal agencies including Defense Department organizations), describes the problem

he threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk. It's no longer possible to write a large white paper about the risk to a particular system. You would be rewriting the white paper "...constantly

To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach. The National Institute of Standards and Technology (NIST), for example, recently issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and .real-time assessments

**According to Forbes, the global cybersecurity market reached \$75 billion for 2015 and is expected to hit \$170 billion in 2020**