Cybersecurity risks are typically defined by two main components:

- Cyber threats - Any potential method of cyber-attack that can lead to the theft, unauthorized access, damage, or disruption of a digital asset, network, or device. Examples include; ransomware, data leaks, phishing, malware, insider threats, cyberattacks.
- Vulnerabilities - A vulnerability is any weakness or flaw within a system that cybercriminals can exploit to steal data or gain unauthorized access.

Though commonly used interchangeably, cyber risks and vulnerabilities are not the same. A vulnerability is a weakness that results in unauthorized network access when exploited, and a cyber risk is the probability of a vulnerability being exploited.

What is the difference between vulnerability assessment, penetration testing, and cybersecurity risk assessment?

Vulnerability Scan
A vulnerability scan uses a computer program to assess computers, systems, and networks for security weaknesses, also known as vulnerabilities. These scans are typically automated and give a beginning look at what could possibly be exploited.

Vulnerability scans can be instigated manually or run on a scheduled basis and will be completed in as little as several minutes to as long as several hours.

Vulnerability scans are a passive approach to vulnerability management because they don't go beyond reporting on vulnerabilities that are detected. It's up to the business owner or their IT staff to patch weaknesses on a prioritized basis or confirm that a discovered vulnerability is a false positive, then rerun the scan.

Penetration Test
A penetration test simulates a hacker attempting to get into a business system through hands-on research and the exploitation of vulnerabilities. Actual analysts, often called ethical hackers, search for vulnerabilities and then try to prove that they can be exploited. Using methods like password cracking, buffer overflow, and SQL injection, they attempt to compromise and extract data from a network in a non-damaging way.

Penetration tests are an extremely detailed and effective approach to finding and remediating vulnerabilities in software applications and networks. A good way to illustrate the benefits of a penetration test would be to use an analogy from the medical world. When something is wrong inside your body you can go get an X-ray to help diagnose your problem. The image produced by a simple X-ray machine can detect an obvious break in bone structure but is fuzzy and not good for seeing soft tissue damage. If you really want to find out in detail what might be going on inside a body, you need to have an MRI done that results in a detailed 3D model of bone and soft tissues together. That is similar to the difference between a simple vulnerability scan (fuzzy X-ray) and a penetration test (detailed MRI). If you really want to find deep issues in your application or network, you need a penetration test. And if you

modify your systems and software over time, a regular penetration test is a great way to ensure continued security.

In contrast, much of penetration testing is done manually, which explains why it is costlier. Also, a penetration test exposes weaknesses and tries to exploit them.

Which is better: vulnerability assessment or penetration testing?
Both tests work together to encourage optimal network and application security. Vulnerability scans are great weekly, monthly, or quarterly insight into your network security (the quick X-ray), while penetration tests are a very thorough way to deeply examine your network security (the periodic detailed MRI). Yes, penetration tests are expensive, but you are paying a professional to examine every nook and cranny of your business the way a real world attacker would, to find a possibility of compromise.

Although the needs of each organization differ, generally speaking, regular penetration testing may reveal more information regarding how your system can be hacked compared to a vulnerability scan**.**

Because of this level of detail, penetration testing is often a requirement in many security standards (PCI DSS, HIPAA, FedRAMP, SOC 2 Type2, etc).

Cybersecurity Risk Assessment
A cybersecurity risk assessment identifies, analyzes, and evaluates risk across the organization's entire cybersecurity posture including policies and people. It takes into consideration the impact and likelihood of a threat exploiting a vulnerability. A risk assessment also requires a skilled professional to conduct properly. The purpose is to answer the following questions:

- What are our organization's most important information technology assets?
- What type of data breach would have a significant impact on our business, whether from malware, cyber-attack, or human error? Customer information.
- Can all threat sources be identified?
- What is the level of the potential impact of each identified threat?
- What are the internal and external vulnerabilities?
- What is the impact if those vulnerabilities are exploited?
- What is the likelihood of exploitation?
- What cyber-attacks, cyber threats, or security incidents could affect the business's ability to function?
- What is the level of risk my organization is comfortable taking?

A risk assessment offers businesses a report on their risk rating and recommended controls to reduce their risk. It is a more comprehensive look at an organization's vulnerabilities, outlining the complete view of its exposure. This process requires more than tools, but a cohesive look at a business' threshold of risk with analysis by a seasoned professional.

Cloud9™ DATA SOLUTIONS

We are an extension of your team saving you significant time and money improving your Cybersecurity posture.

ADVISE, DEPLOY, MANAGE

About Cloud9Data Solutions

For over two decades (established 2001) Cloud9 Data serves over 2,200 business, non-profit, EDU, and healthcare clients throughout North America and Europe.

We offer a wide range of cybersecurity technology and managed services including:

Advisory, Assurance, & Compliance

- Cybersecurity Risk Assessment
- Penetration Testing
- Vulnerability Scanning & Assessment
- Regulatory Compliance Audits
- Virtual CISO & DPO Services

Recovery

- Data Back Up & Recovery as a Service
- Disaster Recovery as a Service
- Ransomware Protection & Recovery

Protection

- Endpoint Protection
- EDR, MDR, & XDR
- Managed Email Security
- Managed Network & Cloud Security
- Managed Firewall
- Managed SEIM
- Patch Management
- SOC as a Service
- Employee Cyber Awareness Training