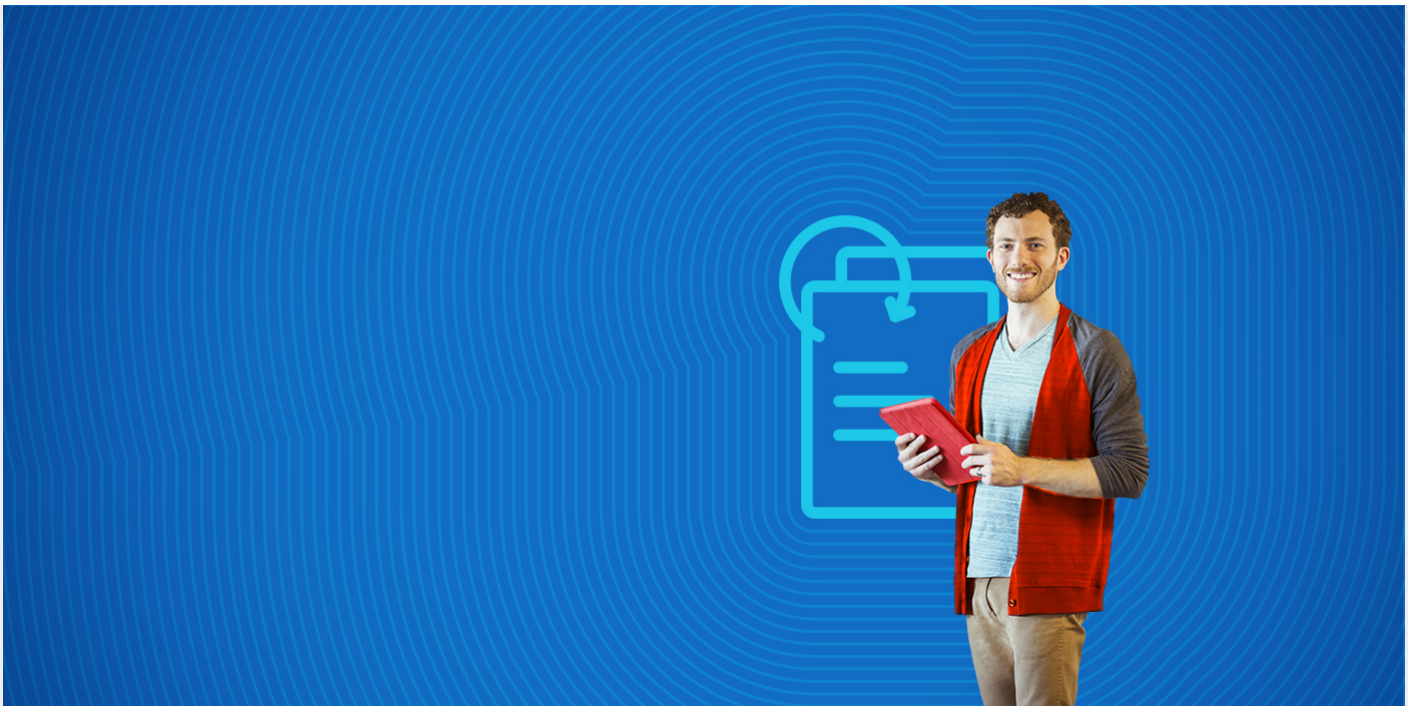
IT SECURITY VULNERABILITY VS THREAT VS RISK: WHAT ARE THE DIFFERENCES?



In today's world, data and protecting that data are critical considerations for businesses. Customers want to ensure that their information is secure with you, and if you can't keep it safe, you will lose their business. Many clients with sensitive information actually demand that you have a rigid data security infrastructure in place before doing business with you.

With that backdrop, how confident are you when it comes to your organization's IT security?

In order to have a strong handle on data security issues that may potentially impact your business, it is imperative to understand the relationships of three components:

- Threat
- Vulnerability
- Risk

Though these technical terms are used interchangeably, they are distinct terms with different meanings and implications. Let's take a look.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

IT security vulnerability vs threat vs risk

David Cramer, VP and GM of Security Operations at BMC Software, explains:

What is a threat?

A threat refers to a new or newly discovered incident that has the potential to harm a system or your company overall. There are three main types of threats:

- **Natural threats**, such as floods, hurricanes, or tornadoes
- **Unintentional threats**, like an employee mistakenly accessing the wrong information
- **Intentional threats**, such as spyware, malware, adware companies, or the actions of a disgruntled employee

Worms and viruses are categorized as threats because they could cause harm to your organization through exposure to an automated attack, as opposed to one perpetrated by humans. Most recently, on May 12, 2017, the WannaCry Ransomware Attack began bombarding computers and networks across the globe and has since been described as the biggest attack of its kind. Cyber criminals are constantly coming up with creative new ways to compromise your data, as seen in the 2017 Internet Security Threat Report.

These threats may be uncontrollable and often difficult or impossible to identify in advance. Still, certain measures help you assess threats regularly, so you can be better prepared when a situation does happen. Here are some ways to do so:

- **Ensure your team members are staying informed** of current trends in cybersecurity so they can quickly identify new threats. They should subscribe to blogs (like Wired) and podcasts (like Techgenix Extreme IT) that cover these issues, and join professional associations so they can benefit from breaking news feeds, conferences, and webinars.
- **Perform regular threat assessments** to determine the best approaches to protecting a system against a specific threat, along with assessing different types of threats.
- **Conduct penetration testing** by modeling real-world threats in order to discover vulnerabilities.

What is a vulnerability?

A vulnerability refers to a **known** weakness of an asset (resource) that can be exploited by one or more attackers. In other words, it is a known issue that allows an attack to succeed.

For example, when a team member resigns and you forget to disable their access to external accounts, change logins, or remove their names from company credit cards, this leaves your business open to both intentional and unintentional threats. However, most vulnerabilities are exploited by automated attackers and not a human typing on the other side of the network.

Testing for vulnerabilities is critical to ensuring the continued security of your systems. By identifying weak points, you can develop a strategy for quick response. Here are some questions to ask when determining your security vulnerabilities:

- Is your data backed up and stored in a secure off-site location?
- Is your data stored in the cloud? If yes, how exactly is it being protected from cloud vulnerabilities?
- What kind of network security do you have to determine who can access, modify, or delete information from within your organization?
- What kind of antivirus protection is in use? Are the licenses current? Is it running as often as needed?
- Do you have a data recovery plan in the event of a vulnerability being exploited?

Understanding your vulnerabilities is the first step to managing your risk. (Learn more about vulnerability management.)

What is risk?

Risk is defined as the **potential** for loss or damage when a threat exploits a vulnerability. Examples of risk include:

- Financial losses
- Loss of privacy
- Damage to your reputation Rep
- Legal implications
- Even loss of life

Risk can also be defined as:

Risk = Threat x Vulnerability

Reduce your potential for risk by creating and implementing a risk management plan. Here are the key aspects to consider when developing your risk management strategy:

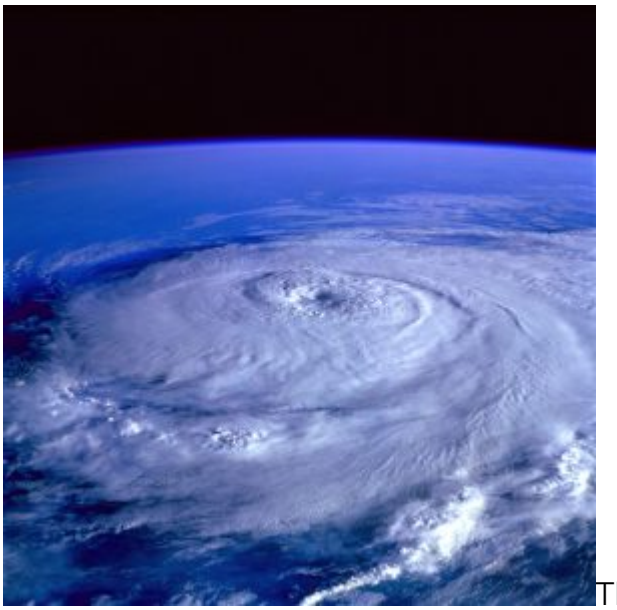
- **Assess risk and determine needs**. When it comes to designing and implementing a risk assessment framework, it is critical to prioritize the most important breaches that need to be addressed. Although frequency may differ in each organization, this level of assessment must be done on a regular, recurring basis.
- **Include a total stakeholder perspective**. Stakeholders include the business owners as well as employees, customers, and even vendors. All of these players have the potential to negatively impact the organization (potential threats) but at the same time they can be assets in helping to

mitigate risk.

- **Designate a central group of employees** who are responsible for risk management and determine the appropriate funding level for this activity.
- **Implement appropriate policies and related controls** and ensure that the appropriate end users are informed of any and all changes.
- **Monitor and evaluate policy and control effectiveness**. The sources of risk are ever-changing, which means your team must be prepared to make any necessary adjustments to the framework. This can also involve incorporating new monitoring tools and techniques.

Threat, vulnerability, and risk: an example

To summarize the concepts of threat, vulnerability, and risk, let's use the real-world example of a hurricane.



The **threat** of a hurricane is outside of one's control. However, knowing that a hurricane could strike can help business owners assess weak points and develop an action plan to minimize the impact. In this scenario, a **vulnerability** would be not having a data recovery plan in place in the event that your physical assets are damaged as a result of the hurricane. The **risk** to your business would be the loss of information or a disruption in business as a result of not addressing your vulnerabilities.

Accurately understanding the definitions of these security components will help you to be more effective in designing a framework to identify potential threats, uncover and address your vulnerabilities in order to mitigate risk.

Additional resources

For related reading, explore these resources:

- BMC Security & Compliance Blog
- Introduction To Enterprise Security
- What is Security Threat Modeling?
- Threat Remediation Explained
- DevSecOps? The Role of Security in DevOps Architecture

The Game Plan for Closing the SecOps Gap from **BMC Software**