IT Security Vulnerability vs Threat vs Risk: Understanding 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 consideration as the 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 relationship between three central components – Threat, Vulnerability and Risk. Frequently these technical terms are used interchangeably, but although related, they are
distinct terms with different meanings and implications.

What’s the Difference Between an IT Security Vulnerability, Threat and Risk?

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

**Threat**

A threat refers to a new or newly discovered incident with the potential to do harm to a system or your overall organization. There are three main types of threats – natural threats (e.g., floods or a tornado), unintentional threats (such as an employee mistakenly accessing the wrong information), and intentional threats. There are many examples of intentional threats including spyware, malware, adware companies, or the actions of a disgruntled employee. In addition, worms and viruses are also categorized as threats, because they could potentially 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](https://www.bmc.com/us-en/product/it-smart-value/solutions/threat-and-vulnerability-management/bmc-2017-internet-security-threat-report.html).

Although these threats are generally outside of one’s control and difficult to identify in advance, it is essential to take appropriate measures to assess threats regularly. Here are some ways to do so:

- Ensure that 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.
- In addition, penetration testing involves modeling real-world threats in order to discover vulnerabilities.

## 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 be successful. 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 and developing a strategy to respond quickly. 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.

Risk

Risk refers to the potential for loss or damage when a threat exploits a vulnerability. Examples of risk include financial losses as a result of business disruption, loss of privacy, reputational damage, legal implications, and can even include loss of life.

Risk can also be defined as follows:

\[ \text{Risk} = \text{Threat} \times \text{Vulnerability} \]

You can reduce the 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.

Summary

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 potentially hit can help business owners assess weak points and come up with 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’s winds or heavy rains. 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

The Game Plan for Closing the SecOps Gap from BMC Software