Devolutions

Cybersecurity vs. IT Security: What's the Difference?

TWO FREQUENTLY USED AND OFTEN MISUSED — TERMS: CYBERSECURITY AND IT SECURITY.

There are some words that are often perceived as synonyms (i.e., used interchangeably) but are in truth distinct terms with their own respective definitions and contexts. And in the IT world, arguably the most common example of this involves two frequently used — and often misused — terms: cybersecurity and IT security.

About Cybersecurity

Cybersecurity is rooted in protecting data from threats that could occur over the internet, such as phishing, malware, SQL injections, and so on. To achieve this critical objective, cybersecurity professionals (who have various job titles) are heavily involved in developing and implementing risk mitigation plans, strategies, techniques, systems, platforms, and tools.

In addition, these essential professionals are tasked with ensuring that their organization has an incident response plan. While this is vital, it is not always achieved. Our recently-released State of Cybersecurity in SMBs in 2021/2022 Survey Report found that 40% of SMBs do not have a comprehensive and updated cybersecurity incident response plan. Increasing the cybersecurity budget and/or working with a Managed Services Provider could help SMBs close this gap. The Recommendations section of the Survey Report explores the core elements of an effective cybersecurity incident response plan.

About IT Security

IT security is rooted in protecting access to computers, networks, and information. This includes both physical protection (i.e., preventing unauthorized individuals from accessing the server room) and **data security** (i.e., preventing unauthorized individuals from accessing certain privileged accounts).

A widely-used model that many organizations use to design and deliver their IT security program is known as the CIA triad, which stands for confidentiality, integrity, and availability:

- **Confidentiality focuses on safeguarding sensitive information from unauthorized access.** It also involves categorizing and prioritizing data (and therefore data protection) based on the type and extent of damage that could occur if it is compromised.
- **Integrity focuses on ensuring that data is consistent, accurate, and trustworthy** across every lifecycle stage, which includes: data capturing, data maintenance, data synthesis, data usage, data publication, data archival, and data purging.
- **Availability focuses on ensuring that information is readily and practically accessible to authorized parties**, and in a manner that is aligned with organizational standards and compliance requirements.

The Overlap

At this point, some non-technical readers may be scratching their heads and asking: "I thought we were going to distinguish between cybersecurity and IT security — but even after looking at each one, they still seem like the same thing!" To this, we can only say: "Yes, you make a good point!"

Indeed, in the real world, **there is a significant overlap between cybersecurity and IT security**. They both rely on multiple integrated strategies, tools, practices, policies, and so on to secure and protect information. As a result, in many organizations — especially SMBs — cybersecurity and IT security functions will be rolled into the same team, and even owned by a single individual (a.k.a. the glorious "IT guru" who vigilantly defends the thin digital line between clarity and chaos).

What's more, IT security has been established for several decades and cybersecurity is a relatively newer operational area. (While the conceptual infrastructure of what we now call the internet was laid in the mid-20th century, it was not until the 1990s that it began to take root as a commercial asset.) As such, cybersecurity is often viewed as a subset or an extension of IT security.

Furthermore, it is common for cybersecurity professionals and IT security professionals to work collaboratively; this is especially true when it comes to establishing, enforcing, and evolving robust security across an organization — which is an ongoing effort and not a one-time accomplishment. Of course, we must quickly add that both cybersecurity and IT security professionals LOVE reading Sysadminotaur comics because they get to laugh and cry at the same time!

However,**it is nevertheless wise to view cybersecurity and IT security as distinct — but often overlapping — priorities, because they emphasize different aspects that must be part of an organization's overall security posture and profile**. And the word "must" here is not an exaggeration. The ever-growing reliance on both on-premise and cloud-based systems (especially during the pandemic) to store, share, and solicit information has enabled a level of productivity, business intelligence, and convenience that would have seemed like science fiction only a few decades ago. But it has also exponentially increased the volume of threat vectors, and vastly expanded the size of the attack surface.

The bottom line? Organizations that check all of the necessary cybersecurity and IT security boxes (and these differ from organization to organization, sector to sector, and marketplace to marketplace) greatly increase the likelihood that their future will be safe and successful. Conversely, those that fail to address these priorities may soon find themselves victimized by a costly — and potentially catastrophic — breach. To modify an old and wise saying: An ounce of cybersecurity and IT security prevention is worth a pound of cure!