teliapp

Uh oh. Call the *cybersecurity* team immediately.

Understanding Technology Roles & Their Differences; Who's Who?

Did the *InfoSec* Team approve this policy?

Better call the *IT* department for help.

Get the *network* engineers to work on this.

CONTACT

401 North Wood Avenue
Second Floor, Linden, NJ 07036

Phone: (732) 354 1773
Email: development@teliapp.com

teliapp.com

Understanding the Difference between Network Engineering, Cybersecurity, Information Technology, and Information Security.

Understanding these differentiated disciplines is essential for organizational resilience. Let's imagine your technology teams operate like the staff of a large, modern building, such as an apartment complex or corporate tower. Each department has a clear, vital role in keeping the structure secure, functional, and productive for everyone inside. Here's how these technology roles map to the everyday roles you'd encounter in such a building.

Network Engineering

Network engineers manage and maintain your technology's overall infrastructure. Their core focus is building and upholding the digital network, ensuring stable data movement. Their goal is to provide a stable, high-performance, and scalable network foundation for all technology. Responsibilities include designing architecture, configuring hardware (routers and switches), troubleshooting outages, and managing infrastructure upkeep.

Your Maintenance & Infrastructure Crew

Network engineers are akin to a building's maintenance and infrastructure crew. Your maintenance team designs, builds, and maintains the building's electrical, plumbing, HVAC, and elevator systems. So too, your network engineers design, build and maintain your network's physical and digital pathways so that they remain reliable, scalable, and working. They also manage data traffic flow and monitor access across network segments.

Cybersecurity

Cybersecurity personnel are responsible for the safety and security of your technology infrastructure. Their core focus is protecting the organization, its data, and its people from digital threats. Their goal is to manage risk, and to ensure system confidentiality, integrity, and availability. Responsibilities include defense via security tools, threat monitoring, access control, incident response, and implementing policies and compliance.

Your Armed Guards & Emergency Response Units

A cybersecurity team is just like an armed security and emergency response unit that monitors your digital and technology infrastructure. Just as an armed security force monitors surveillance feeds, investigates suspicious activity, and responds to active threats, so too your cybersecurity team handles both internal and external intruders who may be attempting to break into your technology infrastructure.

Information Technology (IT)

IT technicians ensure that your technology enables your team's productivity. IT teams focus on deploying, managing, and supporting technology systems to maximize employee productivity. Their goal is to maximize the uptime and usability of end-user systems and applications. Responsibilities include end-user support, device and account management, software management, and data management and backup.

Your Concierge & Front Desk Staff

Think of your IT technicians as the building's concierge and front desk staff. They manage daily operations, enabling productive living and work. Just as a concierge handles access controls within the building, your IT department manages access logs and service requests, and ensures that only authorized personnel have the required access to spaces. Just like the building's concierge, the IT department liaisons with other departments for security and network related requirements.

Information Security (InfoSec)

The information security team develops technology related governance and policies. Their core focus is systematically protecting all information assets from unauthorized use or destruction. Their goal is to ensure data confidentiality, integrity, and availability, by establishing strategic policy frameworks. Responsibilities include risk management, defining controls and compliance, overseeing data governance, auditing processes, and ensuring legal and regulatory adherence.

Your Building Safety, Insurance Underwriters & Policy Makers

An InfoSec team is akin to a building's safety inspectors, policy makers, and insurance underwriters; they ensure the entire building meets safety and regulatory requirements before an incident occurs. They assess risks (for example, fire suppression system adequacy), set standards (for example, apartment door lock strength), ensure compliance with municipal safety codes, classify high and low security areas, and review audit logs from the concierge, security and maintenance teams.