IT Fundamentals for Business Professionals

Focus Area: Cybersecurity and Social Implications
Format: Conceptual (no labs or hands-on activities)

This course explored the intersection of cybersecurity, business strategy, and social responsibility. While it was more theory-driven than technical, it offered valuable insights into how cybersecurity risks are not just technical challenges but major business and societal concerns.

One of the core takeaways was the idea that data breaches, ransomware attacks, and digital surveillance have ripple effects that go beyond organizational losses. They affect public trust, human rights, and even democratic systems. For professionals moving into governance, risk, and compliance (GRC), this kind of big-picture thinking is crucial.

The course also emphasized that cybersecurity is no longer just the IT department's responsibility. Business leaders, legal teams, and risk officers are expected to understand cybersecurity implications when making decisions, from how customer data is handled to how suppliers are vetted. This aligned well with my background in criminal justice and legal compliance, reinforcing that my experience in understanding institutional systems, ethics, and policy carries real value in a security-focused business environment.

Although there were no labs or hands-on exercises in this class, the broader context it provided helps frame why technical measures matter. Tools, protocols, and access controls only go so far without a clear understanding of the social systems they're meant to protect.

This course supports my transition into cybersecurity by reinforcing the importance of ethical risk management and organizational accountability , areas that will be central to my work in compliance and digital forensics.