**IOT & Cyber Security**

~Week 1~

**Digitalization – What are the security implications of the digital economy?**

A fully digital enterprise is a company that has adopted a complete digital approach. Digital tools and technologies are used to conduct all business operations. Digital technologies can increase performance, “by cutting maintenance time and costs” (Wei et al and Spermic, 2019). Digital technologies, such as Artificial intelligence and Internet of Things empower companies to have a competitive advantage in the business sector.

The digital economy has many security implications that individuals, businesses, and governments need to consider. Some of the key security risks associated with the digital economy include:

1. **Cybersecurity threats:** The digital economy is vulnerable to a wide range of cybersecurity threats, including malware, phishing attacks, ransomware, and other types of cyber-attacks. These threats can compromise sensitive data, disrupt critical infrastructure, and cause financial losses.
2. **Data privacy concerns:** The digital economy generates vast amounts of data, and there are often concerns about how this data is collected, stored, and used. There are risks that personal data could be accessed or misused by unauthorized parties, leading to privacy violations.
3. **Intellectual property theft:** The digital economy relies on the creation and distribution of intellectual property, such as software, music, and other digital content. This can make it vulnerable to intellectual property theft, which can lead to financial losses and damage to reputation.
4. **Fraud and financial crimes:** The digital economy is also at risk of fraud and financial crimes, such as money laundering and financial scams. These crimes can have serious consequences for individuals and businesses.
5. **Disruptions to critical infrastructure:** The digital economy relies on complex systems and networks to function, and disruptions to these systems can have significant impacts. For example, a cyber-attack on a power grid could disrupt electricity supply, while a cyber-attack on a transportation system could disrupt travel.

Overall, it is important for individuals, businesses, and governments to be aware of these security risks and take appropriate steps to protect themselves and their assets. This can include adopting good cybersecurity practices, implementing data privacy measures, and being vigilant against fraud and financial crimes.

**Q & A Section**

**Q-1) What is a 'fully digital enterprise'?**

A fully digital enterprise is a business that has fully embraced digital technologies in all aspects of its operations. This includes using digital tools and platforms to automate and streamline processes, as well as using digital channels to interact with customers, partners, and suppliers.

A fully digital enterprise may use a wide range of digital technologies, including cloud computing, artificial intelligence, machine learning, and the Internet of Things (IoT). These technologies can enable the business to be more efficient, flexible, and responsive, and can help it to better understand and meet the needs of its customers.

A fully digital enterprise may also be characterized by its use of data-driven decision making and a focus on continuous innovation. By collecting and analyzing large amounts of data, a fully digital enterprise can gain insights that can inform business strategy and help it to stay ahead of the competition.

Overall, a fully digital enterprise is one that can use digital technologies to transform its operations and create value for its customers, employees, and shareholders.

**Q-2) What are the cyber-security challenges/concerns with a fully digital enterprise?**

A fully digital enterprise is likely to face a range of cyber-security challenges and concerns. Some of the key risks include:

1. **Cyber-attacks:** A fully digital enterprise is likely to be a target for cyber-attacks, as attackers may see it as a more valuable target due to its reliance on digital technologies. This could include attacks such as malware, phishing, ransomware, and other types of cyber threats.
2. **Data breaches:** A fully digital enterprise is likely to have a large amount of sensitive data, such as customer information, financial data, and intellectual property. There is a risk that this data could be accessed or stolen by unauthorized parties, leading to a data breach.
3. **System disruptions:** A fully digital enterprise may be vulnerable to disruptions to its systems and networks, which could be caused by cyber-attacks or other technical issues. These disruptions could have significant impacts on the business, including financial losses and damage to reputation.
4. **Regulatory compliance:** A fully digital enterprise may be subject to a range of regulations related to data privacy, cybersecurity, and other issues. It is important for the business to ensure that it is compliant with these regulations to avoid fines and other penalties.

Overall, it is important for a fully digital enterprise to be aware of these cyber-security challenges and take steps to address them. This can include implementing strong cybersecurity measures, regularly reviewing, and updating security protocols, and training employees on how to identify and prevent cyber threats.

**Q-3) What are the cyber security challenges for a bricks and mortar SME wanting to become a digital enterprise?**

There are several cyber security challenges that a bricks and mortar small and medium-sized enterprise (SME) may face as it looks to become a digital enterprise. Some of the key challenges include:

1. **Limited resources:** Many SMEs may have limited resources, including budget and personnel, to devote to cyber security. This can make it difficult to implement and maintain strong cybersecurity measures.
2. **Lack of expertise:** SMEs may also lack in-house cybersecurity expertise, which can make it challenging to identify and address potential threats.
3. **Complexity:** As a bricks and mortar business transitions to a digital enterprise, it may need to adopt a range of new technologies and systems, which can increase the complexity of its IT environment. This can make it more difficult to secure and manage.
4. **External threats:** A fully digital enterprise is likely to be more vulnerable to external cyber threats, such as malware, phishing attacks, and ransomware. It is important for business to be aware of these threats and take steps to prevent them.

Overall, it is important for a bricks and mortar SME looking to become a digital enterprise to carefully consider its cyber security needs and take steps to address them. This can include implementing strong cybersecurity measures, regularly reviewing, and updating security protocols, and training employees on how to identify and prevent cyber threats.

**Q-4) Do you agree with the views expressed, especially in light of the 'energy crisis' experienced worldwide in 2022?**

I have come to the same conclusion with all the views expressed. Since the energy crisis is concern that the world’s demand on the natural resources, as a possible solution, governments and people as individual have to work together to make use of renewable resources as a priority. Some of the causes to energy crises are increase of population and war between countries. Linear increase of the world population and the Russian invasion of Ukraine made it inevitable.

**References used for the answers:**

* <https://atos.net/en/lp/the-security-challenges-of-digital-transformation>
* <https://www.helpnetsecurity.com/2021/07/07/smes-cybersecurity-challenges/>
* [https://www.conserve-energy-future.com/causes-and-solutions-to-the-global-energy-crisis.php#:~:text=The%20energy%20crisis%20is%20the,years%20to%20replenish%20the%20stores](https://www.conserve-energy-future.com/causes-and-solutions-to-the-global-energy-crisis.php#:~:text=The%20energy%20crisis%20is%20the,years%20to%20replenish%20the%20stores.).