**Case study on ransomware**

**University of Leicester (2024)**

In August 2024, the University of Leicester in the UK was hit by a ransomware attack that disrupted its online services and access to academic records. The attackers used a variant of the "Ragnar Locker" ransomware, which encrypted critical data and demanded a substantial ransom in cryptocurrency. The university’s IT team worked to isolate the affected systems and restore services from backups. The attack raised concerns about the security of academic institutions and their ability to safeguard sensitive information.

### ****Honda Motor Co. (2024)****

In July 2024, Honda Motor Co. experienced a ransomware attack that significantly impacted its global operations. The ransomware variant, "LockBit," encrypted files across various departments, leading to production delays and operational disruptions. Honda's response involved shutting down affected systems to prevent further spread and working with cybersecurity experts to restore operations. This incident underscored the vulnerabilities in manufacturing sectors and the potential for significant operational disruption.

### ****Health Service Provider (2024)****

A large health service provider in the US was targeted in early 2024 by a ransomware attack from the "Conti" group. The attack led to a temporary halt in patient services, including access to medical records and scheduling systems. The attackers demanded a multimillion-dollar ransom, and the incident highlighted the severe consequences for critical infrastructure, especially in healthcare where downtime can affect patient care and safety.

### ****Local Government Agencies (2024)****

Several local government agencies in the US were attacked by a ransomware strain known as "BlackCat" in June 2024. The attack caused significant disruptions to public services and administrative functions. The agencies faced challenges in coordinating responses and restoring systems due to the encrypted data and the complexity of their IT environments. The incident illustrated the growing trend of targeting municipal and governmental bodies, which can have broad and impactful consequences for public services.