Security: Advances In Technology Bring Increased Risks

• Instead of protecting a single main frame, you now need to protect many individual devices.

• Insider Threats –
  – Improper or shoddy implementation of IoT system
  – Overwhelmed property managers
  – Tenants or individuals intentionally or unintentionally bypassing security controls or incorrectly operating systems

• Outsider Threats –
  – Terrorism
  – Increased risks resulting from high-profile or high-value clients that might be targeted by hackers
  – IoT botnets
Business Risk due to Cybersecurity Breaches

- Target was hacked when hackers entered company’s network by stealing credentials of third-party HVAC vendor.
- In 2013 researchers found that Google’s building management system was connected to the internet without latest software patch and they were able to obtain the administrative password.
- Infected IoT vending machines and light bulbs shut down internet at major university.
- Hacking of Iran’s Natanz enrichment facility caused centrifuges to be destroyed.
Privacy Implications and Regulatory Concerns

• Identification of building users and tracking of movements raise general privacy and security concerns.

• General Data Protection Regulation (GDPR) (will become effective in May 2018)
  
  o GDPR will apply to buildings including location tracking and sensor technology.
  
  o Access control systems could include name, photo, location, department, privilege, and potentially biometric information of an employee.
  
  o Be aware of where data is maintained for EU or UK buildings.

• FTC IoT enforcement actions