HOLMESGLEN INSTITUTE OF TAFE

HACKING OF SMART CITY CRITCAL INFRASTRUCTURE

A Report by Kelly and Rebecca

KEY TOPICS

- Introduction
- Smart City Infrastructure
- Cyber Threats to Smart City Infrastructure
- Case Studies
  - The Industroyer Attack
  - The Atlanta Ransomware Attack
- Consequences Of Cyber Attacks on Smart Cities
- Mitigation and Cybersecurity Strategies
- Future Trends
- Conclusion and Questions

WHAT IS SMART CITY CRITICAL INFRASTRUCTURE?

- Services and systems supporting societal and economic functions
- Utilisation of advanceddigitasl technology for better resource management

INTERNET OF THINGS (IoT)

Connects various systems for improved functionality

SENSOR NETWORKS

Vital for real-time data collection and management

SMART TRAFFIC MANAGEMENT SYSTEMS

- MINIMISE ROAD CONGESTION
- IMPROVE SAFETY
- USES IOT DEVICES: RFID TAGS, CCTV CAMERAS, CONNECTED TRAFFIC LIGHTS

SMART UTILITIES

- MONITOR AND MANAGE ELECTRICITY, WATER, AND GAS SUPPLY
- MINIMISE WASTE AND SYSTEM DOWNTIME
- USES CONSUMER FEEDBACK AND VARIOUS SENSORS TO ENSURE SUPPLY MEETS DEMAND

RISKS AND VULNERABILITIES

Increased opportunities for cybercriminals due to interconnected devices

COMMON WEAKNESSES

Poorly managed access controls

Oudated software

Inadequate response plans

Potential Consequences of Cyber Attacks

- **TRAFFIC MANAGEMENT SYSTEMS**

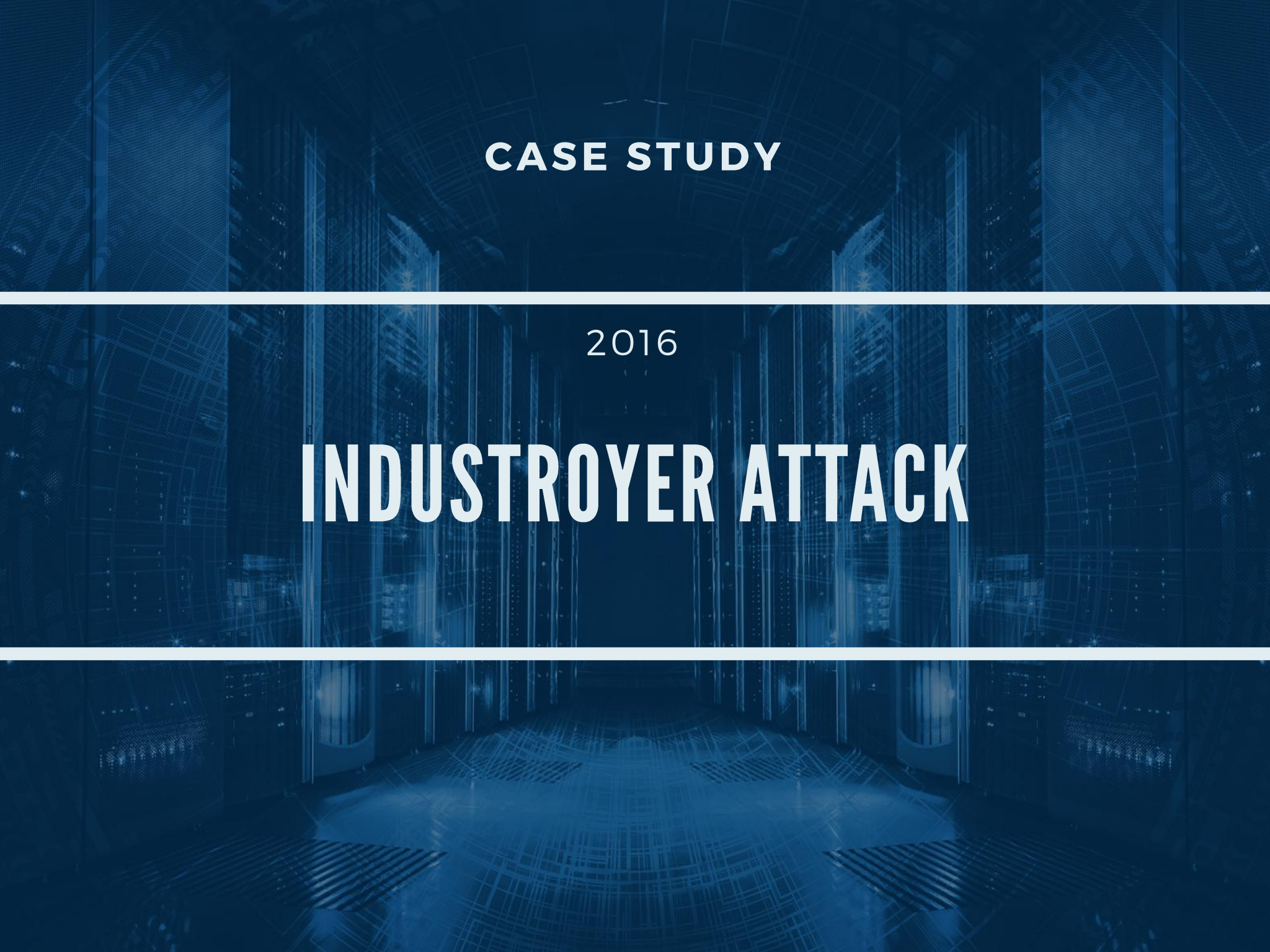
  Data manipulation leading to congestion and emergency service delays

- **DENIAL OF SERVICE (DOS)**

  Disrupt service supply
  Prevent detection of faults and compromised systems

- **COMPROMISED DATA-HANDLING SERVICES**

  Theft, manipulation, or deletion of sensitive information
  Erosion of public trust and saftey risks



CASE STUDY

2016

INDUSTROYER ATTACK

Overview of the Industroyer Attack

DATE

December 17, 2016

TARGET

Pivnichna substation near Kyiv

ATTACKER

Russian cyberwarfare group Sandworm

IMPACT

Power cut to approx. 20% of the city

EXECUTION OF THE ATTACK

MALWARE USED: Industroyer (CrashOverride)

Techniques:

- Opened circuit breakers causing power outage
- Data wipe program to disable computers
- Denial of Service attack on protective relays
- Exploited outdated firmware vulnerability

IMPLICATIONS AND LESSONS LEARNED

COMPLEXITY OF INDUSTROYER

- Modular toolkit with various functionalities
- Proof of concept for future attacks

RESPONSE AND RECOVERY

- Power restored within an hour
- Highlighted the need for improves cybersecurity measures

FUTURE THREATS

- Potential for more advanced attacks
- Importance of robust protection for critical infrastructure

CASE STUDY

2018

ATLANTA RANSOMWARE ATTACK

WHAT HAPPENED?

SAMSAM RANSOMWARE

BACKGROUND

- Attackers were able to gain access to Atlanta's City Hall digital services

NATURE OF THE ATTACK

- Ransomware attack
- Attackers demanded $50,000 bitcoin

IMPACT OF THE ATTACK

- mass service outages
- data loss
- loss of reputation & public trust
- recovery effort costing $17 million

What happened next?

EXPOSED VULNERABILITIES

- attackers gained access through password-cracking / weak passwords
- was able to go undetected for a long time as a means of corrupting more systems and files

OUTDATED BACKUP SYSTEMS

- made the recovery effort difficult.

LED TO AN OVERHAUL OF SECURITY PROTOCOLS

- stronger passwords, combined with multifactor authentication
- reduced privilege rights to employees
- implemented regular security audits


CONSEQUENCES OF CYBER
ATTACKS ON SMART CITIES

CONSEQUENCES

ECONOMIC IMPACT/ FINANCIAL CONSEQUENCES

MONEY FOR RANSOM. FINANCIAL IMPACT IN RECOVERY AND RESTORATION EFFORTS

OPERATIONAL DISRUPTIONS

MASS SERVICE OUTAGES

LOSS OF PUBLIC TRUST AND CONFIDENCE

IMPACT TO REPUTATION & PUBLIC OUTCRY


PREVENTATIVE MEASURES AND
CYBERSECURITY STRATEGIES

Role of Government and Policy Frameworks

Governments are important as they;

- Establish national security standards
- Fund research
- Foster collaboration between public and private organisations
- Encourage international collaboration
- Create and enforce law
- Provide education and awareness

Australian Cyber Security Centre (ACSC)

The ACSC began operations in 2014 and has since become the Australian Government's technical authority on cyber security.
Services that the ACSC offers include:

- The Australian Cyber Security Hotline, which is contactable 24 hours a day, 7 days a week, via 1300 CYBER1 (1300 292 371)
- Publishing alerts, technical advice, advisories and notifications on significant cyber security threats
- Cyber threat monitoring and intelligence sharing with partners, including through the Cyber Threat Intelligence Sharing (CTIS) platform
- Technical advice and assistance to help Australian entities respond to cyber security incidents
- National exercises and uplift activities to enhance the cyber security resilience of Australian entities
- Collaborating with Australian organisations and individuals on cyber security issues through ASD's Cyber Security Partnership Program.

Importance of Public-Private Partnerships

- **THE CYBER THREAT INTELLIGENCE SHARING (CTIS)**
  - a threat information sharing platform.
- **DIGITAL IDENTITY AND THE TRUSTED DIGITAL IDENTITY FRAMEWORK (TDIF)**
  - a foundation for establishing secure, trusted digital identities.
- **SECURITY OF CRITICAL INFRASTRUCTURE (SOCI) ACT**
  - provides the government with significant powers to respond to cyber-attacks on critical infrastructure.

Other Preventative Measures

- CONTINUOUS MONITORING
- INCIDENT RESPONSE PLANNING


FUTURE TRENDS AND
CHALLENGES

Evolving Cyber Threats with Emerging Technologies

BENEFITS OF 5G

- speed
- connectivity

VULNERABILITIES

- expanded attack surface
- more vectors/ attack points

BENEFITS OF AI

- ease of access
- complete tasks faster

VULNERABILITIES

- entering in sensitive data

Other Challenges

- BALANCING INNOVATION WITH SECURITY
- THE ROLE OF INTERNATIONAL COLLABORATION AND KNOWLEDGE SHARING


PROSPECTS FOR SMART CITIES
BEYOND 2024


CONCLUSION