Corporate Governance Committee

Cyber Security Risk Management

Friday 24 July 2020

Jayne Glasgow
Chief Digital and Information Officer
Corporate Resources
Leicestershire County Council

The Risk

"If the Council does not manage its exposure to cyber risk, then decisions and controls cannot be taken to mitigate the threat of a successful cyber-attack."

The Context

- Cyber Security is the protection of information systems:
  - Includes hardware, software, and network infrastructure
  - All data contained within and services they provide
  - Protection from unauthorised access, harm or misuse
    - Intentional or accidental
- Cyber incidents can be very disruptive
- Local Authorities have been victims
- Cyber risk is persistent
  - Constantly evolving threats
  - Ongoing need to manage and mitigate

Covid-19: Cyber Threats

- Phishing emails
  - Using the subject of COVID-19 as a lure
- Malware distribution
  - Using COVID-19 themed lures
  - Ransomware
- Attacks against newly (and often rapidly) deployed remote working technology
- Registration of new domain names containing coronavirus or COVID-19 related wording
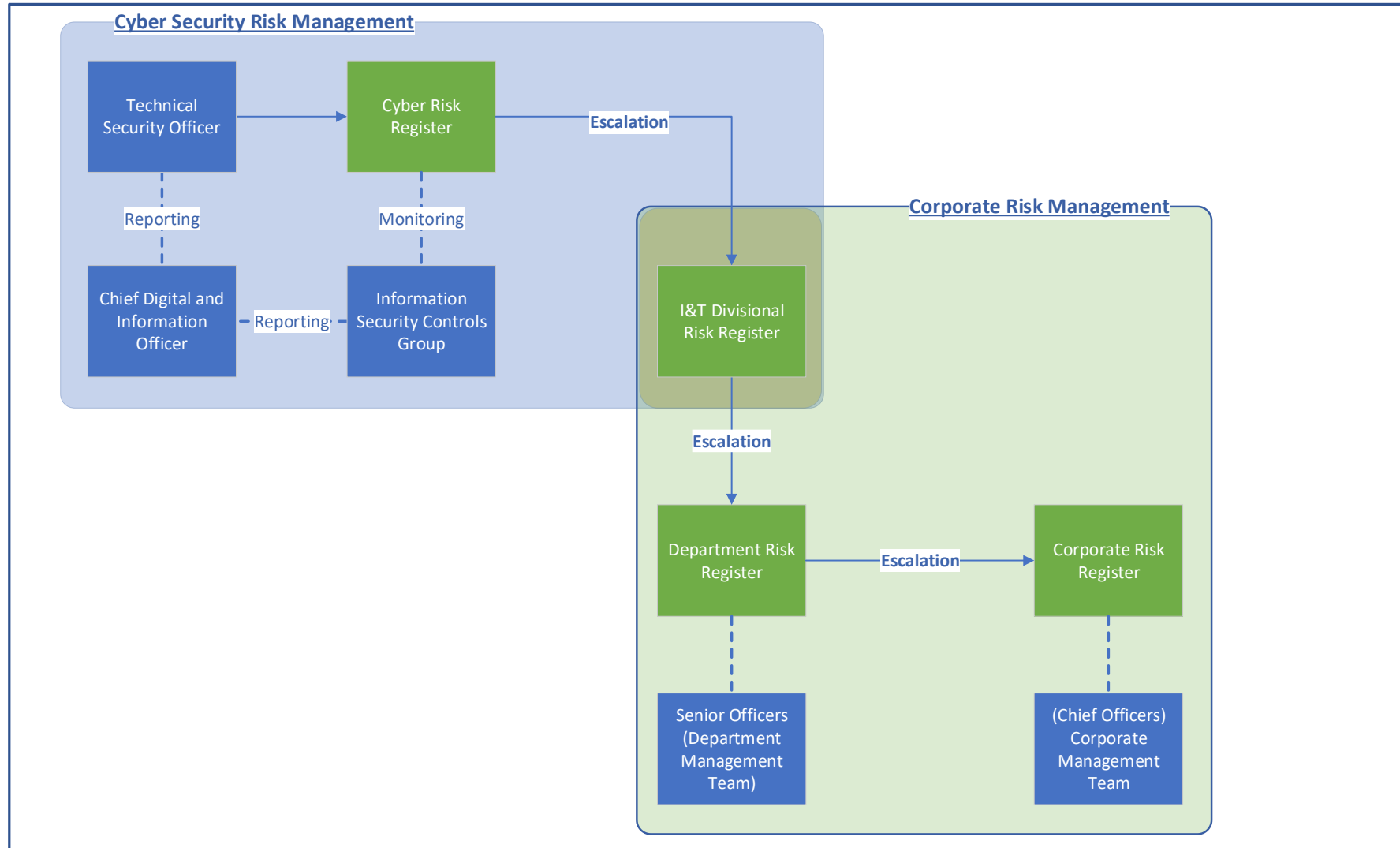
Response to Covid-19

- Used proven technology to support increase in homeworking
  - Improved process for keeping laptops updated with security patches
- Bolstered incident response plans
  - Including cyber incident process
- Active threat monitoring
  - Sharing information with other councils (Warning, Advisory and Reporting Points - WARPs)
  - National Cyber Security Centre (NCSC)
- Monitoring for use of non-approved technology
- Increased staff communication to counter the threats
  - Threat of phishing emails
- Improved resilience of the general network and infrastructure

How are cyber risks managed?

- Technical Security Officer role
  - Identify emerging threats and risks
  - Maintain cyber risk register
  - Ongoing activities to implement mitigations

- Cyber security is integrated into the organisational risk management process
  - Risks escalated up the chain – I&T Register > Department Register > Corporate Register
  - Quarterly risks update to Department Management Team
  - 6 monthly risk updates to Corporate Management Team

- Information Security Controls Group
  - Forum for cyber security policy, risk, strategy and best practice
  - ICT Audits
  - Regular system health checks by an external body

- All new technology and systems subject to security risk assessment prior to implementation
  - Internal Audit function

Risk Process Overview

Questions