Cyber Attack Risk Presentation

Audit Committee – July 2017

Dave Mansfield

Head of Technology



What is a Cyber Attack

"An attempt by hackers to damage or destroy a computer network or system – or to incapacitate them until a 'ransom' is paid."





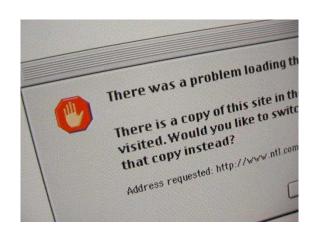
Why is this such an issue now?

- Hackers (criminals) are continuously adapting and improving their methods
- HCC and other organisations are experiencing increased numbers and complexity of attacks
- Several high profile cases (NHS / Lincolnshire...)
- A more mobile and technology dependent workforce





Types of attack (examples)





- Viruses
- Worms
- Trojan Horses
- Ransomware
- Denial of service attacks

Hackers



What do we need to do to protect?



- Good frontline technology to identify and protect against intrusion
- Up to date software and relevant patches
- Good staff awareness and action
- Ability to respond quickly and effectively to contain if/when attacked
- Constantly learning from incidents and improving approach as hackers develop new approaches



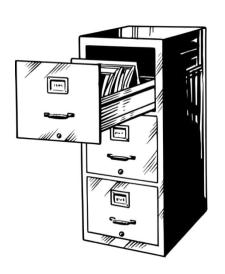
The Current Position



- HCC has been subject to attack this is increasing
- So far our defences have been able to repel or deal with all attacks
- Our systems are patched and kept up to date through regular mechanisms
- We do not have old XP systems attached to network
- PSN compliance successfully awarded

The Current Position (2)





- Staff are constantly reminded of their responsibilities in avoiding
- We follow industry updates and apply continuous learning
- Our Systems and Network are partitioned to prevent cross organisation propagation
- We learn from real life incidents such as Lincolnshire and NHS



But we must not be complacent



- Our protective systems need to be continually improved and adapted to meet the growing and changing threat
- Staff need to be kept up to date and on their guard
- We need to learn from our own experiences and those of others
- We need to be successful against a multitude of different and varying attacks. The hacker only needs to get lucky once......



Our plans for continuous improvement

 Further investment in latest front line protection and detection software and services



 Staff awareness programme and communications – including "cold calling" tests





We are also starting a SIAS audit of this area.



Our plans for continuous improvement

Additional resource in the ICT security team.



 A strict compliance approach regarding "maverick" and "legacy" software







Thank You... Questions?

