RANSOMWARE IN HEALTHCARE FACILITIES: THE FUTURE IS NOW

Nikki Spence, Marshall University
David P. Paul, III, Monmouth University
Alberto Coustasse, Marshall University

Presented at the 2017 ABR Conference in Atlantic City, NJ
INTRODUCTION

- What is ransomware?
INTRODUCTION

- How is it spread?
INTRODUCTION

Attacks: on individuals

Attacks: on organizations

Ransomware Locks Down Hotel Rooms
INTRODUCTION

- How widespread is it?
INTRODUCTION
INTRODUCTION

- Why healthcare facilities?
  - EHRs
  - Criticality of information
  - Lack of funds spent on IT security
Results

- The first documented case of hospital ransomware was at Surgeons of Lake County in 2012.
- A similar attack occurred two years later in 2014 at Clay County Hospital.
- In both events, the extent of ransomware attack was not detailed; a ransom was believed to be paid in both cases, but the amounts were never disclosed.
Results

- It was not until the highly publicized ransomware attack at Hollywood Presbyterian Medical Centre in February of 2016 that hackers actively began to target healthcare facilities
  - Staff was unable to access patient records, X-rays, and other equipment, or to restore equipment from backup data and was forced to pay the ransom
  - Initial reports claimed that a ransom of $3.6 million was demanded, but was negotiated down to approximately $17,000 or 40 bitcoins
Results

- To pay or not to pay, that is the question
  - Paying a ransom, however, did not ensure that cybercriminals will provide the encryption key for the locked files
  - In the case of Kansas Heart Hospital, the ransom was paid, but the key was not provided
  - Instead, the cybercriminals demanded a second, larger ransom, which was not paid
Results

What problems could arise as a result of a ransomware attack?
- Malpractice suit
- Reputation loss and loss of future business
- Cost and expense losses
- Loss of patient PHI (HIPAA)!!!
Results

What should healthcare facilities take?

- Disaster mitigation - Backup (offline, cloud, etc.)!
  - Unfortunately, backups are a “moment in time”
  - In the meantime, problems with paper
- Risk mitigation - Prevention
  - Education of staff, docs, administration