National Cybersecurity Awareness Month

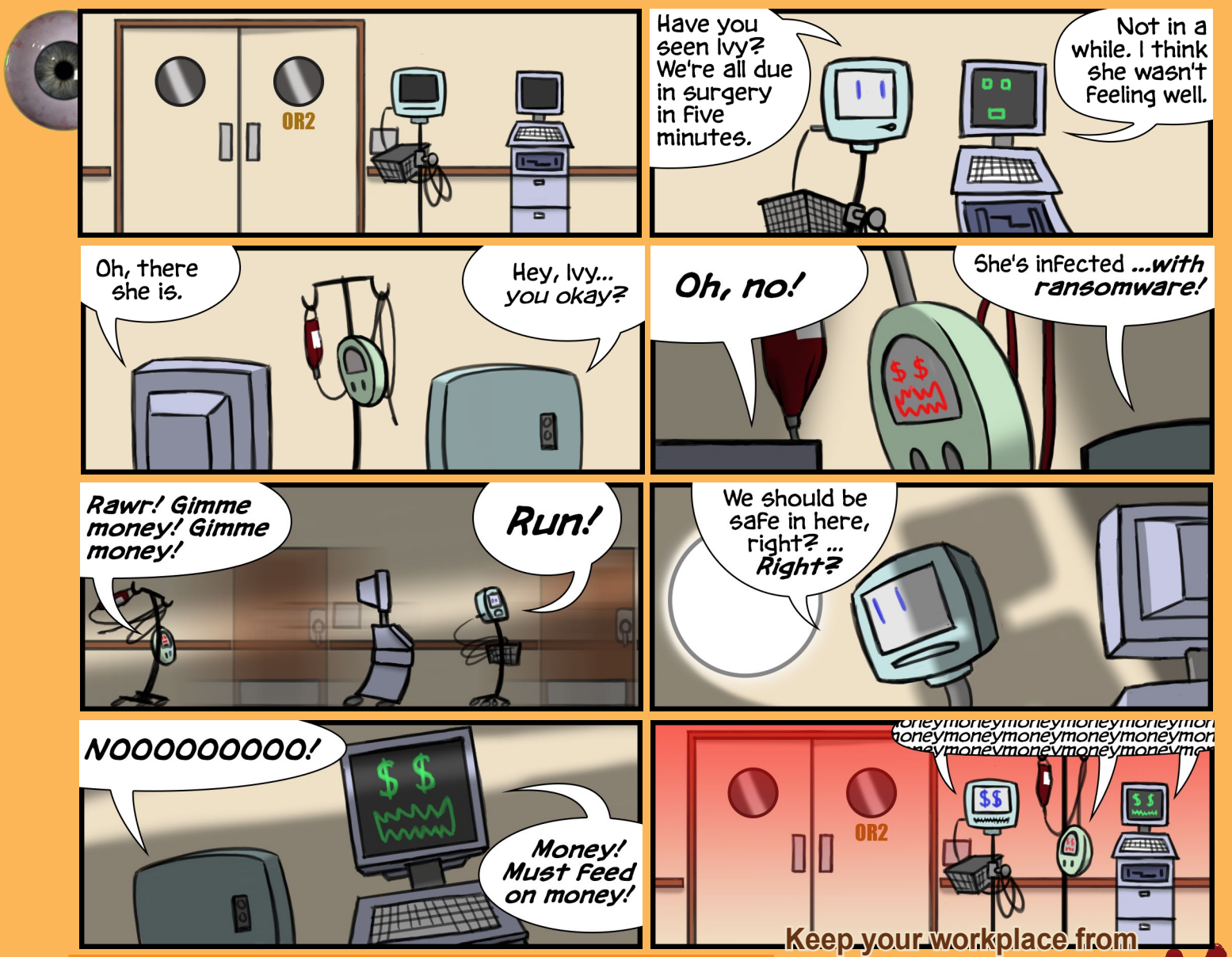
National Cybersecurity Awareness Month

OCTOBER 2017

WEEK 5

Protecting Critical Infrastructure from Cyber Threats

Hospitals are not only an APPEALING victim for cyber criminals because of valuable patient data, but also a LIKELY victim because they often rely on older equipment that runs on outdated or unsupported software. The combination of appeal and probability makes IHS and other healthcare providers prime targets for cyber threats like ransomware, a type of malware that uses encryption to prevent access to files, networks, and systems until the victim pays a ransom...



Hospitals are perfect extortion victims because they must maintain timely access to medical files, and so much of their critical, life-saving equipment is networked together. Just this past year, the British healthcare system was targeted by the WannaCry ransomware attack, where 48 British medical facilities were infected by the virus. The consequences are scary! Patient records held hostage! Equipment failing mid-operation! And emergency software patches might mean taking patients off life-sustaining machinery!

Keep your workplace from becoming a horror show!

- *Back up data regularly to an external drive!*
- *Beware of social engineering scams!*
- *Think twice before clicking!*
- *Keep software patches up to date!*
- *Use strong passwords!*
- *Switch off unused Wi-Fi and Bluetooth connections!*

For more info, contact cybersecurity@ihs.gov