Security awareness case study on

A ransomware incident

Scenario

The CEO was livid, purple with rage. "Surely *something* can be done about this ransom-ware? OK I accept that the FBI can't crack the encryption, but can't the NSA put their supercomputers onto this? We're completely crippled – no patient records, no office systems, no customer billing, the dispensary, X-ray and CT-scan departments totally out of action, and the hospital splashed all over the news headlines. We're being portrayed as idiots …" The executives shuffled awkwardly in their seats as a strained silence fell over the most difficult senior management meeting in the hospital's long history. After a moment's pause, the Head of Legal spoke up. "Face it Randy: we're stuffed. The NSA is not an option, and both the FBI and the IT consultants are outgunned. Our only escape from this nightmare is to pay those buggers off. Though it pains me to say, it's just a few thousand dollars. There's a slim chance the Feds might catch up with them at some point but we *need* to get the hospital IT systems back on stream soon otherwise we're all out of a job, and the patients are out on the streets. And we need to decide *right now* otherwise it will be too late. Time's up."

Discussion points

1. Point out the information risk and security aspects of this scenario.

2. Describe the potential impacts of the incident on the hospital and its patients.

Organizational impacts	Patient impacts

3. What lessons can *we* take away from this incident? What if anything should we be doing differently as a result?

Copyright © 2016 IsecT Ltd.

Model answers

Note: these are not definitive, comprehensive answers, nor legal or information security advice. We're simply trying to help you discuss and learn from the case.

1. Information risk and security aspects:

- An information security incident has *dramatically* affected the hospital's business – its operations, money-earning capabilities and reputation
- For reasons not explained to us, the organization has suffered a malware infection, meaning that the antivirus and other preventive controls must either have been absent, weak or failed
- The number and range of IT systems affected implies that they were inadequately isolated, and/or relied upon common elements that failed
- Why weren't they able to recover services and data without paying the ransom? Don't they have adequate backups and business continuity arrangements? Was the incident mismanaged?
- The extortion/ransom demand is obvious, but what else might be going on? Is that just a cover for something even more sinister? The ransomware evidently had full control over the IT systems

2. Potential impacts (just some – you should be able to think of more):

Organizational impacts	Patient impacts
• Reputational damage, brand devaluation • Customer defection/loss of business • Business disruption and distraction from the business of treating sick people • Additional costs (including the ransom and IT consultancy) and loss of income • Additional anxiety and stress • Uncertainties about what is happening and what will happen next	• Potentially life-threatening loss of medical services, drugs, diagnostics *etc*. • Concern about privacy and confidentiality of medical records, identity and financial information held by the hospital • Additional anxiety and stress • Uncertainties about what is happening and what will happen next

3. Lessons:

- Preventive controls cannot be completely relied upon: incidents are likely if not certain to occur.
- Adequate incident management and business continuity arrangements (including resilience, recovery and contingency elements) are clearly essential to cope with serious incidents of any kind (ransomware is just one kind of malware, malware is just one form of information risk, and information risk is just one of many risks of concern to the organization).
- We should review our business continuity arrangements (*e.g*. offline backups), test/exercise and (im)prove them to increase assurance that they will work properly when called upon.

Further information

Browse the intranet *Security Zone* or call the Help Desk for more on malware.

Note: the 100% fictional scenario was vaguely inspired by an actual ransomware incident just last month at the Hollywood Presbyterian Medical Center. It has been dramatized and elaborated upon for security awareness purposes. It implies *nothing* about the actual incident, organization or people.

Copyright © 2016 IsecT Ltd.