Social Engineering

Organizational Threats

Coleton Sanheim, D’Artagnan Boocock, Jack Chen, Rhean Propp

**Industry Type**

Healthcare

**Research**

1. What kinds of attacks has this industry experienced in the past?
2. Malware
3. Distributed denial of service attacks.
4. Social engineering
   1. Dumpster diving
   2. Fake IT personnel
5. Disruption
6. Data theft
7. What are the vulnerabilities of this industry?
8. Untrained medical staff.
9. Unaware patients.
10. Lack of physical security controls.
11. Medical IoT devices.
12. Unsecured computers.
13. Password sharing.
14. Convenient access to personal data.
15. How could an organization within this industry manage its risk?
16. Implement regular security training for all staff.
17. Designate security clearances and levels for all staff.
18. Ensure IoT devices have proper security controls enabled.
19. Ensure IoT devices are not left accessible in public spaces.
20. What recommendations would you make to an organization within this industry?
21. Implement a key-card security access system.
22. Train staff to be aware of opening suspicious links and the dangers of social engineering.
23. Perform security reviews on all IoT devices that are used by the employees. Ensure security controls are enabled and proper measures are put in place to prevent exploitation.
24. Train staff to keep an eye on any IoT devices that could be vulnerable to attack.

**Motivations**

1. How do the industrial/organizational threats relate to the motivations and rationales of social engineers?
   1. Money, Cause, Entertainment, Knowledge, Ego, Revenge
   2. Hospitals and clinics are targeted by ransomware attacks as they would more likely to pay than let the data be lost
   3. Attacking a hospital is usually big in the news, and as such is a great target for people with egos and who are looking for notoriety
   4. People might target health services related to a close friend or family’s death, as revenge

**Company**

Alberta Health Services Ltd.

**Departments**

1. Information Technology
2. Operational Leadership
3. Medical Leadership

**Risk Type**

1. Which type of employees would be an internal threat? What kinds of information would they have access to?

* Employees that are part of the information technology team, especially system administrators can be a serious internal threat.
  + System administrators have access to nearly all personal data. They can reset passwords, enter into employee accounts, make changes to the network and hold a lot of power in both controls and perception.
* Leadership Staff
  + Any leadership staff such as CEOs or Managing Directors could directly harm the company through their own use of power and influence.
* Medical Staff
  + Any medical staff will have access to confidential medical records of each patient. They could be bribed into divulging or modifying medical records.

1. How might this type of employee be targeted by an external threat?

* System Administrator
  + An attacker could obtain the username and password credentials to this employee to make network changes or send emails pretending to be this person.
* Leadership Staff
  + An attacker could obtain the credential to the email address of upper management staff. They could use this to their advantage by giving orders to employees in subordinate positions. This could be used to order someone from the financial department to make a transfer to an off-shore account.
* Medical Staff
  + The medical staff are likely the ones with the least amount of training against possible attacks. An attacker could gain access into the system or computers with a keylogger inserted into a medical staff’s computers while they are distracted with an emergency

1. What information could this employee provide to a social engineer?

* System administrators could provide employee names, home addresses, passwords and payment stubs. Enough information could be provided to find social media websites and obtain further information on a target.
* Leadership staff could provide information about how the organization functions.
* Medical staff are able to provide confidential information about a patient’s history.

1. How could an organization use your risk assessment to improve security?
2. Ensure there is a rule of two for administrative staff when signing off on decisions that could severely impact the company.
3. Ensure CEOs and leadership staff are provided with security training that highlights common social engineering practices that are used on them.
4. Implement a logging system for any changes made by the system administrators so they are held accountable for their actions.

**Resources**

<https://www.securitymetrics.com/blog/9-ways-social-engineer-hospital>

<https://www.albertahealthservices.ca/assets/about/org/ahs-org-orgchart.pdf>