SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Performing Cybersecurity Risk Assessment in Hospitals

Online

CYBERWARE4HEALTH - Cybersecurity Awareness in Healthcare Employees

George Doukas
National Technical University of Athens

16/12/2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

Risk Management

Risk Management is a series of steps that help an organisation to understand and manage uncertainty.

- What is a Risk?

  Risk is a potential problem. it might happen, it might not.

- Why Risk Management is important?

  Because lots of things can go wrong. Understanding the risk and taking proactive measures to avoid or manage it is a key element to avoid undesired situations.

Risk Management

Clarifying Key Terms

- **Assessment -** A judgment based on an understanding of the situation; a method of evaluating performance
- **Risk Analysis -** A systematic and ongoing process of identifying threats, controls, and vulnerabilities—as well as their likelihood of impact—to arrive at an overall rating of risk
- **Vulnerability -** A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
- **Threat -** The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

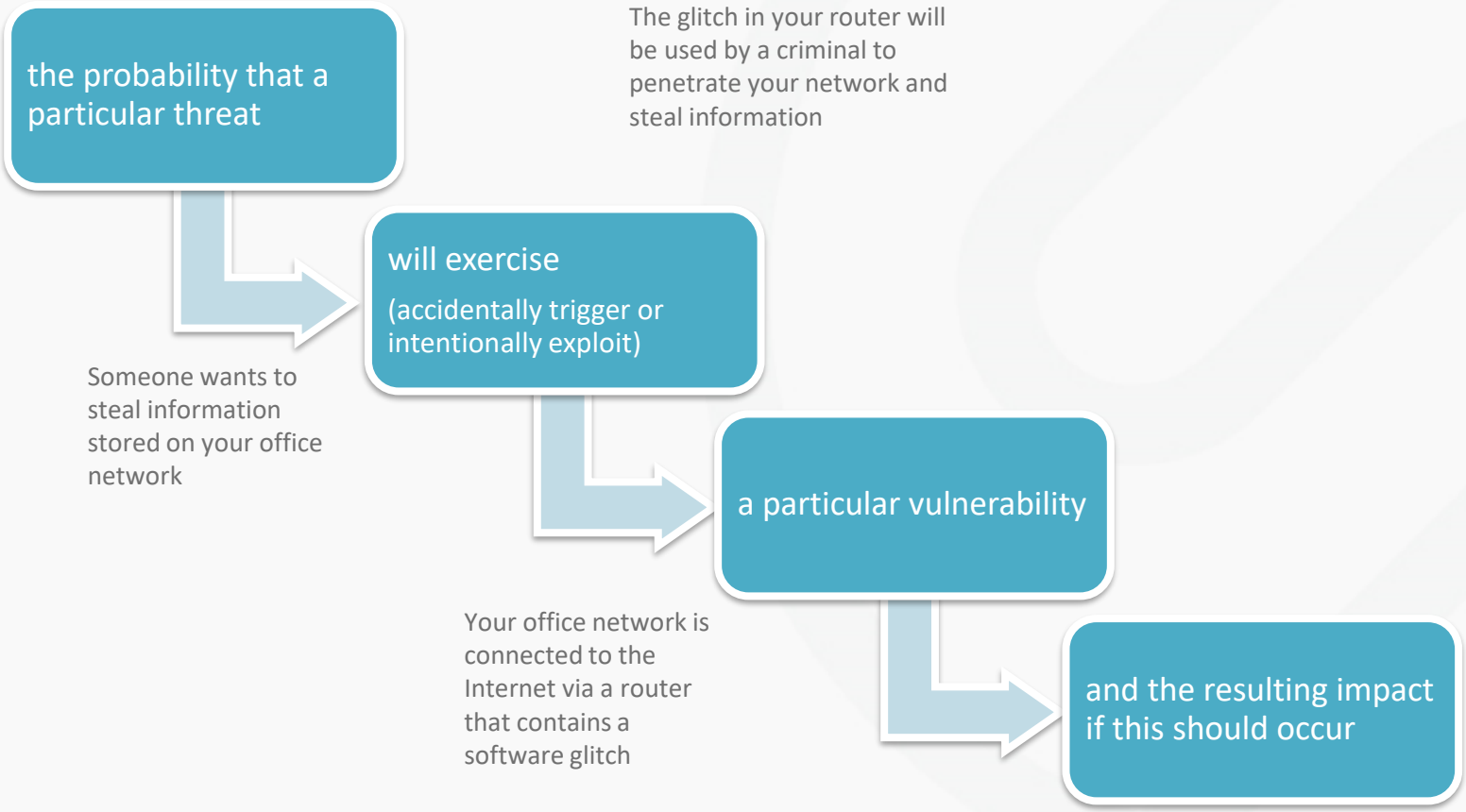
  Natural threats - Floods, earthquakes, lightning strikes

  Human threats - Unintentional, like accidentally deleting a file OR intentional like installing malicious software

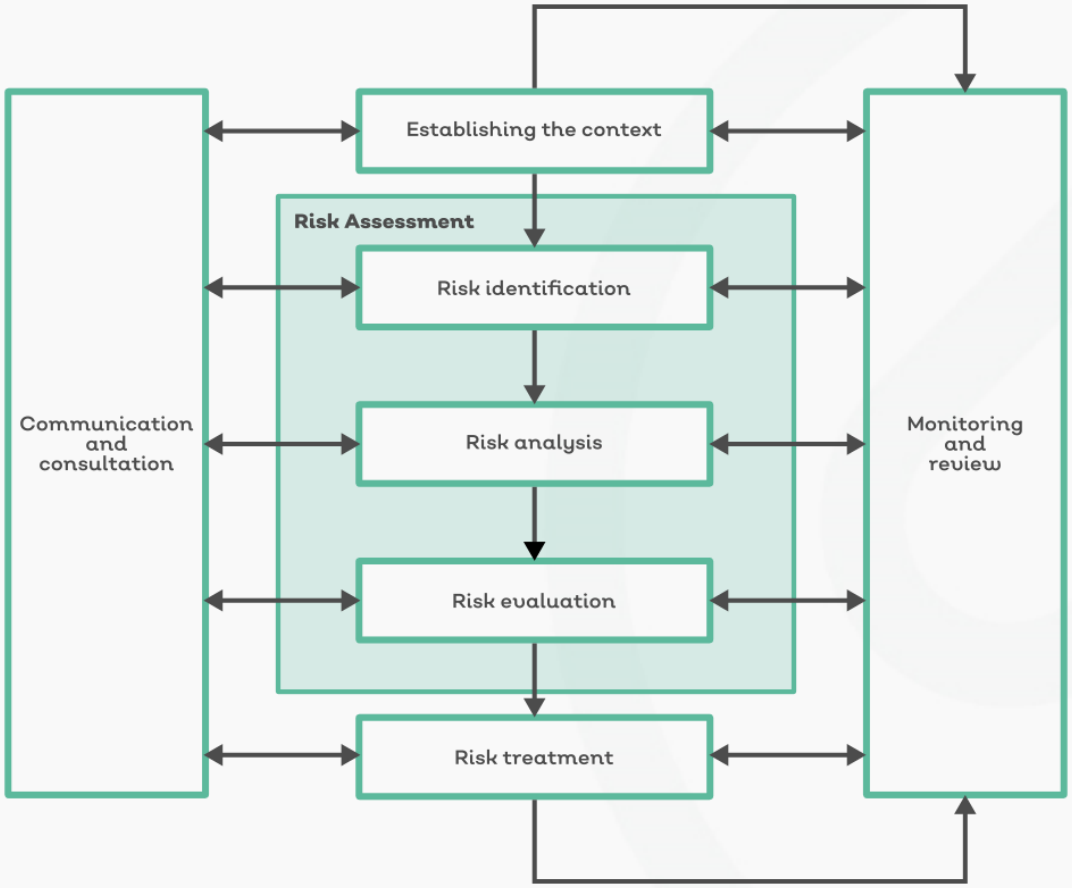
  Environmental threats - Power outage, Internet connectivity failure, office evacuation due to chemical spill

Risk is

The likelihood that a specific threat will occur



Risk Management Framework



* ISO 31000 Risk management — Principles and guidelines

Risk Identification

System Characterisation

- System characterisation is the process of identifying the information assets that require a risk analysis.

  Major applications

  - Electronic health record (EHR) [chief operating officer and/or chief information officer]
  - Laboratory information system [director of laboratory]
  - Pharmacy system—medication dispensing carts [director of pharmacy]

  Support systems that support one or more applications. They are usually ‘owned’ by the information technology (IT) department.

  - Computer workstations
  - Laptops and tablets
  - Smartphones and other mobile devices
  - Network (wired and wireless)
  - E-mail system

Risk Identification

System Characterization

- An organisation's risk analysis should **initially** focus on systems that have the greatest effect on healthcare operations as well as systems that pose the greatest risk for the organisation.
- Another method for identifying the systems on which the healthcare organisation should focus is to rank applications systems based on risk factors, such as:
  - Number of users (i.e., the greater the number of users, the higher the risk)
  - Type of information (i.e., the more sensitive the information, the higher the risk – Social Security Numbers, HIV data, bank account numbers, credit card data, etc.),
  - Use of the information (i.e., patient care, research, business intelligence, patient accounting, etc.)
  - Availability of the information (e.g., hosted in the cloud via the Internet, standalone system, virtualized servers, mirrored SAN, etc.)
  - Mobility of the information (i.e., the more mobile, the greater the risk – portable media, smartphone, tablet, laptop, etc.)
  - Effects on the organization and patients if the system is not available
  - Other factors that might indicate that a system has a higher relative risk for the organization (i.e., system frequently goes down, system provide interconnectivity to other applications and system such as an interface engine, etc.

A risk analysis can be time-consuming. Therefore, healthcare organisations should **initially** focus on the 'critical few' versus the 'trivial many.' However, all applications and systems (including biomedical devices) containing ePHI **must eventually** be assessed.

Risk Identification

Threat Identification

- Once assets have been categorised, the next step is to identify threats. There are three types of threats:
  - **Acts of nature** (e.g., lightning, earthquakes, hurricanes, and tornadoes)
  - **Acts of humans** (e.g., carelessness, human errors, unauthorized access, identity theft; tampering; hacking into data; and theft of equipment by internal workforce members, external hackers, and visitors)
  - **Environmental** (e.g., hardware failure, power outage, inoperable air conditioning that leads to overheating, break in the network cable, and water leaking from the ceiling)

- Once identified, the reasonably anticipated threats are matched to a particular asset.

Risk Identification

Control Assessment and Vulnerability Identification

- Vulnerabilities and controls should go hand in hand, and it's often easier to combine the identification of both into one step.

  If an asset is already in use, then a healthcare organisation should first conduct a control analysis.

  If an asset is new and not currently active, then the healthcare organisation should perform a vulnerability identification first because some of the security controls may not have been implemented fully yet.

Risk Identification

Threat	Control	Vulnerability
1. Theft or loss	File encryption is used to protect some of the data stored on the hard drive.	Power-on passwords and other access control devices are not being used. Security devices (physical or technical) for tracking lost or stolen laptops are lacking.
2. Malicious code (e.g., virus, worm, Trojan horse, spyware)	Antivirus software is loaded on laptops.	Antivirus software does not get updated regularly. Users have local administrator rights and can disable or turn off the antivirus software and download executable programs.

In general, controls may be categorized as:

Preventive - Inhibiting a threat, such as access controls, encryption, and authentication requirements

Deterrent - Keeping the casual threat away, such as strong passwords, two-tiered authentication, and Internet use policies

Detective - Identifying and proving when a threat has occurred or is about to occur, such as audit trails, intrusion detection, and checksums

Reactive - Providing a means to respond to a threat that has occurred, such as an alarm or penetration test

Recovery - Helps retrieve or recreate data or applications, such as backup systems and contingency plans

Risk Identification

Likelihood Determination

- The likelihood determination must be made with consideration of the existing security safeguards and controls.

Example definitions of likelihood ratings:

Likelihood Level	Likelihood Definition
Very High (4)	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
High (3)	The threat-source is motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium (2)	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low (1)	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exploited.

Risk Identification

- **Healthcare organizations are encouraged to edit these definitions or create their own definitions for likelihood and impact.** An accurate description of what constitutes a rating of high, medium, or low is important for maintaining consistency when evaluating risk scores. A consistent standard for scoring risks ensures a better prioritization of risk.

Example definitions of Impacts

Impact	Definition
Confidentiality	Disclosure of PHI Access to credit card data used for committing financial fraud Access to Social Security numbers used for identity theft Disclosure of sensitive or proprietary research information
Integrity	Data entry errors Data alteration (intentional or unintentional) Data synchronization errors
Availability	Business interruption Denial of service Loss of productive time and operational delays Replacement of lost information
Opportunity (financial)	Loss of business Loss of competitive advantage or research grant Equipment repair or replacement Increase in insurance premiums
Reputation	Loss of patient confidence Decreased employee morale Loss of faculty confidence
Litigation	Criminal or civil case Regulatory fines or criminal punishment for noncompliance

Risk Analysis

Risk Determination

The purpose of this step is to assign a risk score that is based on **likelihood** of the threat being realized, considering the current controls in place and **impact** to the organization if the threat was successful in exploiting a vulnerability.

- The scoring of risks allows healthcare organizations to prioritize resources and focus on the areas of greatest risk.

- The techniques used to analyse risk are plenty and varied, and it is up to the organisation to define the ones used.
  There are two common approaches to determine risk: qualitative and quantitative.

Risk Analysis

Qualitative Approach

- The qualitative approach rates the likelihood (probability) that a threat will cause an effect as very high, high, medium, or low. The qualitative approach also rates the impact of that threat as very high, high, medium, or low.

The overall risk score is determined by multiplying the likelihood value by the impact value.

Controls are implemented to either reduce the probability that a threat will cause an effect or to reduce the impact of that effect, thereby reducing risks.

	Likelihood (Probability)			
	Very High (4)	**High (3)**	**Medium (2)**	**Low (1)**
Very High Impact (16)	Very High (64)	Very High (48)	High (32)	High (16)
High Impact (8)	High (32)	High (24)	High (16)	Medium (8)
Medium Impact (4)	High (16)	Medium (12)	Medium (8)	Low (4)
Low Impact (2)	Medium (8)	Low (6)	Low (4)	Low (2)

Risk Analysis

Quantitative Approach

- A quantitative risk analysis is an attempt to assign numerical values to the potential losses that might occur. A quantitative evaluation is difficult because it is not easy to determine an accurate value for information or intangible effects, such as harm to a healthcare organisation's reputation.

  Factors to consider when determining the magnitude of effect include:

  - The value of the asset being protected.
  - An estimation of the frequency that a threat may occur across a specified time.
  - An approximation of cost (i.e., measureable costs and intangible costs) resulting from each occurrence of the threat being realized.

Risk Analysis

- It’s up to each organisation to determine how to define the measurement of the level of risk, and this will impact how it will measure and analyse risks.

- Although a systematic procedure is followed for conducting a risk analysis, there is a certain amount of judgment in the analysis part of the process of all methods.

Risk Evaluation

- **Risk evaluation takes the risk criteria and measures against the risk analysis to determine:**
  - Effectiveness of criteria definition
  - Which risks are highest priority
  - How to approach the next steps (risk treatment)
  - Success of risk analysis process (are there any knowledge gaps remaining?)
- **The outcome of a risk evaluation could result in several actions:**
  - assign further analysis,
  - maintain (or not) existing controls,
  - reconsider the objectives of the risk strategy in alignment with the organisation objectives.

Risk Treatment

- Once risks have been identified, analysed, and evaluated, the appropriate risk treatment should be applied to reduce, remove, or retain each risk depending on a range of factors.

- Organisation might choose to retain a risk if it is inevitable, unavoidable, or lies within the accepted risk tolerance level.

- The risk tolerance and risk appetite of any organisation have a strong impact on the risk treatment, as some may choose to retain more significant risks than others if the potential positive outcomes are worth the balance.

Monitor, review and report

- An integral part of ensuring continuous quality and improvement in process, efficiency, and output is to monitor strategic goals and performance on a regular basis.

SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Thank you

Presenter Name: George Doukas
Organisation: National Technical University of Athens
Email: gdoukas@epu.ntua.gr

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing