Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

## Evaluarea Rentabilității Investițiilor în SI (ROSI)

# La disciplina „Managementul și Auditul Securitații Informaționale”

A efectuat: st. gr. SI-211 Stanislav Chirita

A verificat: Bulai Rodica

Chișinău – 2024

Here's the information you have filled in:

Q. Select your industry:

R. Hospital, Clinic, Doctor Office

Q. Type of incident:

R. System errors/malfunctions

Q. Short description of potential incident:

R. These errors could disrupt computer systems used for patient management, scheduling, electronic medical records, or other aspects of the administration and delivery of medical services.

Q. Existing security measures:

R. authentication system, regular backups of electronic medical records and critical systems

Q. How long would the negative impacts of this incident last?

R. a few days

Q. Locations and business units that would be affected with this incident:

R. the hospital, the patients

Q. Business processes that would be affected by this incident:

R. Patient registration and scheduling

Q. Data that would be affected by the incident:

R. documents in electronic format, personal data of patients

Q. Physical assets that would be affected by the incident:

R. Computer equipment and systems

Q. Currency

R. USD - US Dollar

Q. Cost of external services:

R. 200

Q. Cost of purchasing equipment/goods/materials

R. 500

Q. Employee costs of resolving the incident

R. 0

Q. Legal and/or contractual penalties

R. 0

Q. Description of other costs not mentioned above

R.

Q. Amount of other costs

R. 0

Q. Average margin in your revenues (% of your revenues)

R. 0

Q. Lost revenues from existing clients

R. 0

Q. Lost revenues from potential clients

R. 0

Q. Insurance claims

R. 0

Q. Total cost of single incident = Single Loss Expectancy (SLE)

R. 700.00

Q. How often could such an incident occur

R. Every 3 months

Q. One year risk exposure to this incident = Annualized Loss Expectancy (ALE)

R. 2800.00

Q. Description of security measure(s)

R. Multi-factor authentication: Using multi-factor authentication to validate the identity of users before they are allowed access to medical systems and data. This could include authentication with passwords and unique security codes sent to mobile devices or security tokens.

Q. Incident frequency after security measure(s) are applied

R. Every day

Q. % of reduction of Total cost of single incident

R. 0

Q. Purchase value of security measure(s)

R. 300

Q. How many years would this/these security measure(s) be used?

R. 3

Q. Value of security measure(s) after their usage

R. 200

Q. Annual cost of external parties needed for security measure(s)

R. 1000

Q. Annual number of employee's man-days required for security measure(s)

R. 300

Q. Average annual cost of one employee

R. 250

Q. Number of annual working days for one employee

R. 250

Q. Description of other costs of protection not mentioned above

R. Security monitoring and management costs: Implementing systems and solutions to monitor and manage information and network security may involve additional costs to acquire, implement and maintain.

Q. Annual amount of other protection costs

R. 1000

Q. Annual cost of protection of this/these security measure(s)

R. 2333.33

Q. Total cost of single incident (SLE) - after security measure(s) have been applied

R. 700.00

Q. One year risk exposure to this incident (ALE) - after security measure(s) have been applied

R. 255500.00

Q. Risk reduction

R. -252700.00

Q. Return on Security Investment (ROSI) - in absolute amount

R. -255033.33

Q. Return on Security Investment (ROSI) - as percentage of protection costs

R. -10930.02

Concluzie: Un rezultat negativ al Return on Security Investment (ROSI) sugerează că investiția în măsuri de securitate nu este suficientă pentru a compensa costurile asociate. Este crucial să se evalueze cu atenție eficacitatea măsurilor de securitate implementate și să se identifice dacă există oportunități de optimizare sau îmbunătățire. Costurile legate de implementarea și menținerea măsurilor de securitate depășesc beneficiile obținute în reducerea riscului de incidente de securitate. Lipsa unei strategii de securitate cibernetică bine definite sau implementarea ineficientă a măsurilor de securitate poate contribui, de asemenea, la rezultatul negativ al ROSI.