www.privacyromania.ro

January 29-30, 2021

PRIVACY ROMANIA 2021

Romanian National Conference on Privacy and Data Protection

YOUR EMPLOYEES AND INFORMATION SECURITY DECISIONS

ASCPD

Asociația Specialiștilor în Confidențialitate și Protecția Datelor

Adriana CEAUȘESCU

Data Protection and Information Security Specialist

Infoshare Consulting, ASCPD Member

INFOSHARE
DATA MANAGEMENT & INFORMATION SECURITY
COMPANIE CERTIFICATA
ISO 27001 ISO 9001

Your Employees And Information Security Decisions

AGENDA

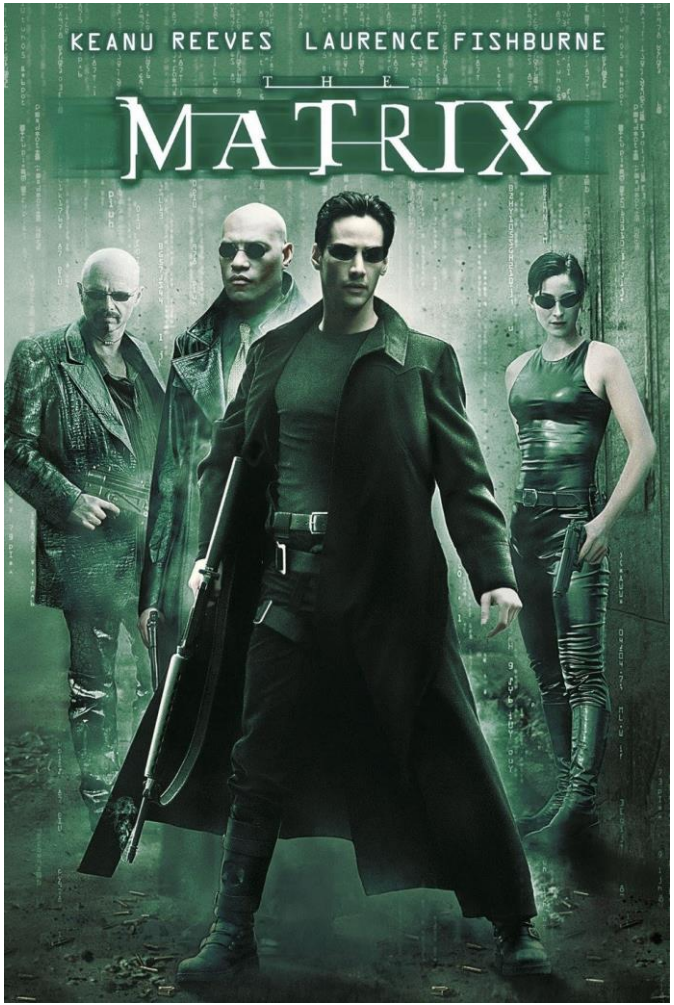
1. Aspects of information security
2. Human behavior and information security
3. How employees make decisions regarding information security
4. 5 ways to develop a security culture
5. The Ten Commandments of Security Employee Training and Awareness

29th of January
ADRIANA CEAUSESCU
www.infoshare.ro

1. Aspects of information security

- Information security is viewed by employees as a technical discipline.
- It is an enigmatic discipline that defies understanding
- Information security depends on people
- From the employee's point of view, information security is about hackers, attacks, and ransomware.

Hello, Matrix!



2. Human behavior and security information

In a survey of IT security practitioners*

- **97%** agreed that their greatest vulnerability was human behavior.

This percentage has increased from 93% in 2015 and **88% in 2014.**

To reduce this vulnerability

- 24% of the respondents use fear;
- 41% adopt best practices
- 83% use policies, training, and awareness, to become a part of the information security solution.

Source : *https://www.readitquik.com/news/security-2/human-behavior-a-major-threat-to-organizational-cybersecurity/*

3. How employees make decisions regarding information security

- **Information security is a secondary consideration** for employees,
- When security mechanism cause additional workload, they will favor non-compliant behavior in order to complete their primary tasks quickly,
- They tend to be aware of how their behaviour can pose an increased risk, but feel justified these workarounds because the **organization has failed to provide them with a proper technical implementation**.
- The more a security policy implementation facilitates **employee values and priorities,** the better it **fosters employee incentives** and strengthens the security culture.
- In order to achieve alignment between security and employee perspective, the process of **formulating security policies must be focused on employees' behavior.** A security professional should remember that employee performance is goal-oriented.
- The common **reasons for non-compliant behavior** are a good starting point and must be explored further and in detail. They are at the very core of the security design and must be common knowledge for designers and policymakers.*

* The psychology of information security - Leron Zinatullin

5 ways to develop a security culture from top to bottom

1. Instill the concept that **security belongs to everyone**
2. Focus on **training**, **awareness and beyond** - (see next slide for details)
3. **Reward and recognize** those people that do the right thing for security
4. Build **security community**
5. Make security **fun and engaging**

5. The Ten Commandments of Security Employee Training and Awareness

1. Information security is a people, rather than a technical, issue.
2. If you want them to understand, speak their language.
3. If they cannot see it, they will not learn it.
4. Make your point so that you can identify it and so can they.
5. Never lose your sense of humor.
6. Make your point, support it, and conclude it.
7. Always let the recipients know how the behavior that you request will affect them.
8. Ride the tame horses.
9. Formalize your training methodology.
10. Always be timely, even if it means slipping schedules to include urgent information.

INFOSHARE

DATA MANAGEMENT & INFORMATION SECURITY

COMPANIE CERTIFICATA

ISO 27001 ISO 9001

Thank you!

ADRIANA CEAUSESCU

www.infoshare.ro