DIGILIENCE 2019

THE ROLE OF THE HUMAN FACTOR IN CYBER SECURITY: RESULTS FROM AN EXPERT SURVEY IN BULGARIA

PROF. DR. SC. YANTSISLAV YANAKIEV
Defence Institute “Professor Tsvetan Lazarov”

ASSOC. PROF. DR. DIMITRINA POLIMIROVA
National Laboratory of Computer Virology, BAS

2-4 October 2019, Sofia, Bulgaria
RESULTS FROM AN ONLINE SURVEY WITH CYBER SECURITY EXPERTS

CARRIED OUT IN THE FRAMEWORK OF THE PROJECT

“CYBER SECURITY AND OPPORTUNITIES FOR APPLICATION OF INNOVATIVE TECHNOLOGIES IN THE WORK OF PUBLIC ADMINISTRATION IN BULGARIA”
First International Scientific Conference
"Digital Transformation, Cyber Security and Resilience"

- 92 completed surveys
- 15.7% activity

- 95 Business organizations
- 369 Public administration
- 121 Academic organizations

2-4 October 2019, Sofia, BULGARIA
**Structure of the Questionnaire**

1. **Expertise** 12%
   Current state and development of human resources

2. **Innovations** 10%
   Innovative technologies

3. **Current state** of the equipment and resources 29%

4. **Policies** 31%
   Governance and policies

5. **Interaction** 18%
   Interaction between the three main sectors: government, academia and industry.

First International Scientific Conference
"Digital Transformation, Cyber Security and Resilience"

2-4 October 2019,
Sofia, BULGARIA
State and Development of Human Resources

Level of expertise of the staff responsible for cybersecurity:
- Corresponds to the needs: 30%
  - High: 13%
  - Low: 17%

Positions held:
- Management/Leadership
- Expert
- Research

Level of expertise of the respondents:
- Corresponds to the needs: 42%
  - High: 18%
  - Low: 15%
Need to pay special attention to the role of the human factor in cyber security

When was your organization's last cyber security training?

- 82% Yes
- 17% No
- 1% I can not decide

- 59% There have been no such training
- 21% They are made periodically in accordance with security policies
- 11% In the last year
- 5% In the last 3 months
Do you think that change and development in the recruitment, education, training of personnel, retention and extracting lessons learned in the field of cyber security practices in Bulgaria are needed?

Suggestions:
- Need for certification programs;
- Comply with the requirements and capabilities of the administration, not only purely theoretical;
- Practical orientation;
- Adequate funding;
The three most important issues currently in the field of cyber security in Bulgaria:

- Staff capacity in the IT units: 64%
- The quality of information systems in the administration: 45%
- The funds allocated for cybersecurity: 48%
- Excessive outsourcing of IT security: 24%
- Gaps in legislation: 24%
- Other: 5%
Has your organization encountered any of the following issues?

- Data lost by the ransomware: 34
- Infection of systems via external device (USB drive, mobile device, etc.): 24
- Infection of systems via email spam: 40
- Break into the system via social engineering: 9
- No: 1
The most important areas that require research in cyber security

- Blockchain technology: 13
- Effective and efficient management of information resources: 31
- Malware protection: 38
- Building cloud infrastructures: 30
- Artificial Intelligence: 24
- Systems Design: 25
- The role of the human factor in cyber security: 50
- Personal identification systems: 24

First International Scientific Conference
"Digital Transformation, Cyber Security and Resilience"

2-4 October 2019, Sofia, BULGARIA
The most unpleasant types of attacks are:

- Distributed Denial of Service (DDoS): 16%
- Data loss from a mobile device: 5%
- Data theft: 25%
- Violation of the physical integrity of systems and networks: 20%
- Targeted attacks: 18%
- Other: 12%
THANK YOU FOR YOUR ATTENTION!

Prof. Dr. Sc. Yantsislav Yanakiev
Defence Institute “Professor Tsvetan Lazarov”

Assoc. Prof. Dr. Dimitrina Polimirova
National Laboratory of Computer Virology, BAS