

CySecLab

**Cyber Security
Laboratory
in T+IN**



THE FIRST SCIENCE AND TECHNOLOGY PARK IN BULGARIA



In a 2015 HBR article: “How Smart, Connected Products Are Transforming Companies”, James Heppelmann (who is CEO of the PTC company) and Michael Porter predicted that **companies’ ability to offer secure products and services will increasingly differentiate them in a crowded marketplace** where the stakes of any failure are high.

OCTOBER 2015

Cybersecurity as an Ability to Compete



2015 Global Megatrends in Cybersecurity

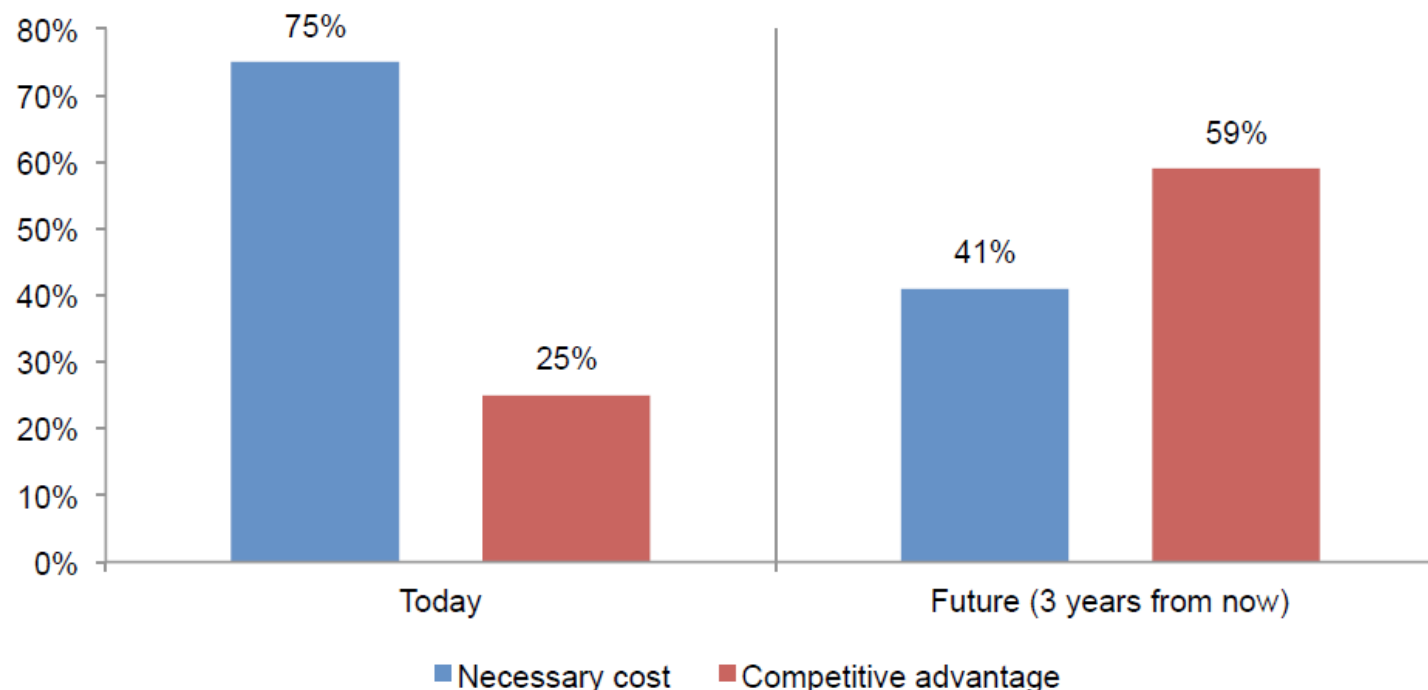
Sponsored by Raytheon

Independently conducted by Ponemon Institute LLC

Publication Date: February 2015

Ponemon Institute® Research Report

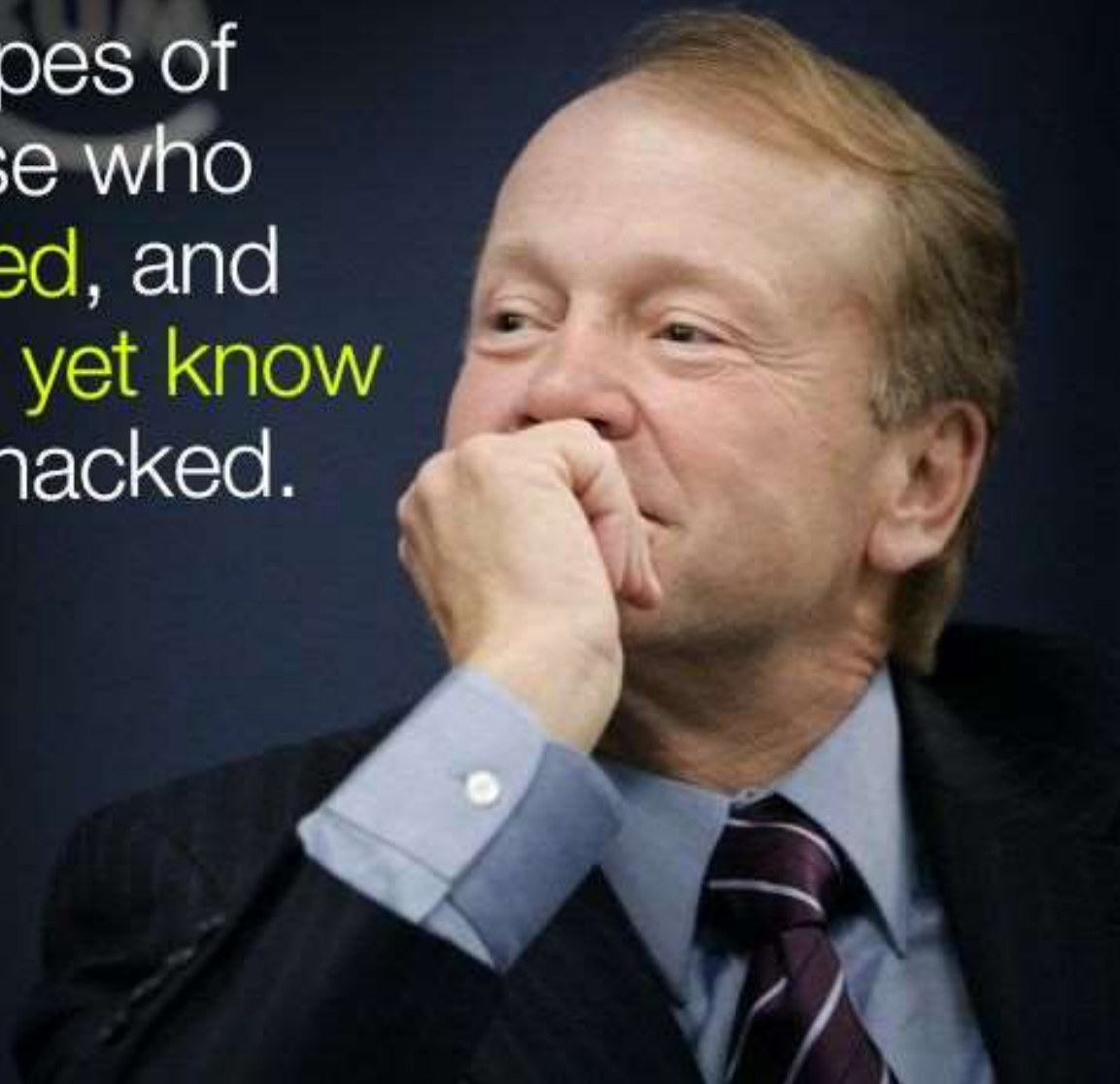
Do your organization's senior leadership view cybersecurity as a necessary cost or a competitive advantage?



Cybersecurity as an Emerging Competitive Advantage

There are two types of companies: those who **have been hacked**, and those who **don't yet know** they have been hacked.

John Chambers
Chief Executive Officer of Cisco



- Research **weaknesses** in the **information and communication systems** in both the **public** and the **private sector**, identification and simulation of critical aspects arising from the **digital dependency** of the business and the society, as well as development of **models** and **platforms** for **simulation**, **detection** and **prevention**;
- Research and development of **methods** and **solutions** to ensure **security**, **sustainability** and **resilience** of critical information and IT systems;
- Design and elaboration of **secure and sustainable models** as well as **informational solutions** for both the **public** (e-government) and the **private** (business) sectors on national and international level;
- Development and provision of a center for **training** and **testing** in the sphere of **informational security** and **cyber resilience**, prevention and defense against cyber threats.

The MISSION of the Cyber Security Lab is to increase the competitiveness of the Bulgarian economy through creation and development of cybersecurity capacity for R&D

CySecLab



THE FIRST SCIENCE AND TECHNOLOGY PARK IN BULGARIA

Development of innovative models, methods and tools for:

- Testing and **assessing cyber security** – of components, systems and organizations (penetration tests);
- **Cyber attack simulations** and methods for protection and prevention in complex infrastructures and systems;
- **Training and education programs**, models for simulation and technical platforms.

The VISION of the laboratory is in five years to become a regional competence center for cybersecurity in Eastern Europe, able to perform complex research activities and to establish international partnerships with the world leaders in the cybersecurity domain.

Projects (selected list):

- Information security audit of a software solution developed by a fast growing **start-up in STP Incubator**, supported the company to sign a contract with leading international organization (completed).
- Organizing of a **networking events and demonstrations** between leading companies in IS from Israel and potential partners from Bulgaria.
- **“Back to Cyber Future”** International conference
- Research and development of early **warning system for Information security threats for Bulgarian organizations** (first phase of the project expected to start in January 2018)
- Ensuring all aspect of information security of an **innovative IoT platform** to be developed by an Bulgarian SME that received an award of excellence from EC (submitted)
- Creation of Competence center for cyber defense solutions (submitted)

*CySecLab@STP is Referred to in the National Cyber Security Strategy
“Cyber Resilient Bulgaria 2020” (July 2016)*


CySecLab

NT
THE FIRST SCIENCE AND TECHNOLOGY PARK IN BULGARIA

ESI European Software Institute
Center Eastern Europe

SEI Partner
Carnegie Mellon

CMMI Institute Partner
powered by Carnegie Mellon

 **SEI Partner** | **Carnegie Mellon**

 **CMMI Institute Partner**
Powered by Carnegie Mellon

ESI European Software Institute
tecnalia

OMG
OBJECT MANAGEMENT GROUP

Carnegie Mellon University
isr institute for SOFTWARE RESEARCH


Software Engineering Institute
Carnegie Mellon

CERT



 **DEFENCE INSTITUTE**
"PROFESSOR TSVETAN LAZAROV"



 **competence**

Partnerships

 **BASSCOM**

ICT Cluster
BULGARIA

and many others...

CySecLab



THE FIRST SCIENCE AND TECHNOLOGY PARK IN BULGARIA

Holistic approach to cybersecurity and resilience research + trainings + services

- **Professional Trainings**

- Web Security (Top 10 Web Threats for Dev / QA, Advanced Web Threats)
- Mobile Security (Top 10 Threats for iOS / Android)
- Infrastructure Security (LAMP Security Configuration, Docker & SELinux, ...)
- Application / Systems Security (Secure Coding in C/C++, Linux Binary Security)

- **Cyber Resilience: trainings and appraisals** (SEI, Carnegie Mellon - CERT RMM)

- **Academic Courses** (3 universities): Active security (red team), Cybersecurity and Business Resilience

- **Cyber Schools & CTFs**

- International Summer School on Cryptography and Cybersecurity (www.cryptobg.org)
- Summer School on Cybersecurity (www.cyberbg.org)
- CTF*BG - National/educational CTF, Cyber Games, with Defense Institute (<https://thecybergames.net>)

- **Cyber Security & Resilience Research**

- CyberMap – <https://cyreslab.org/projects/cybermap> - an overview of Bulgarian Cyber Space
- SoS - Systems-of-systems – analysis and simulation of complex interdependent systems
- Emerging security challenges – AI & ML approach, IoT and IIoT

- **Simulations & Cyber Exercises**

- Exercise as a service platform
- JEMM-like server & playground
- Cyber picture monitor

- **Cyber Ranges** - part of the ECHO Consortium (H2020-SU-ICT-2018-2020) and Cybersecurity Competence Network

- Academic cyber range (for trainings)
- Energy (gas & oil distribution) simulation

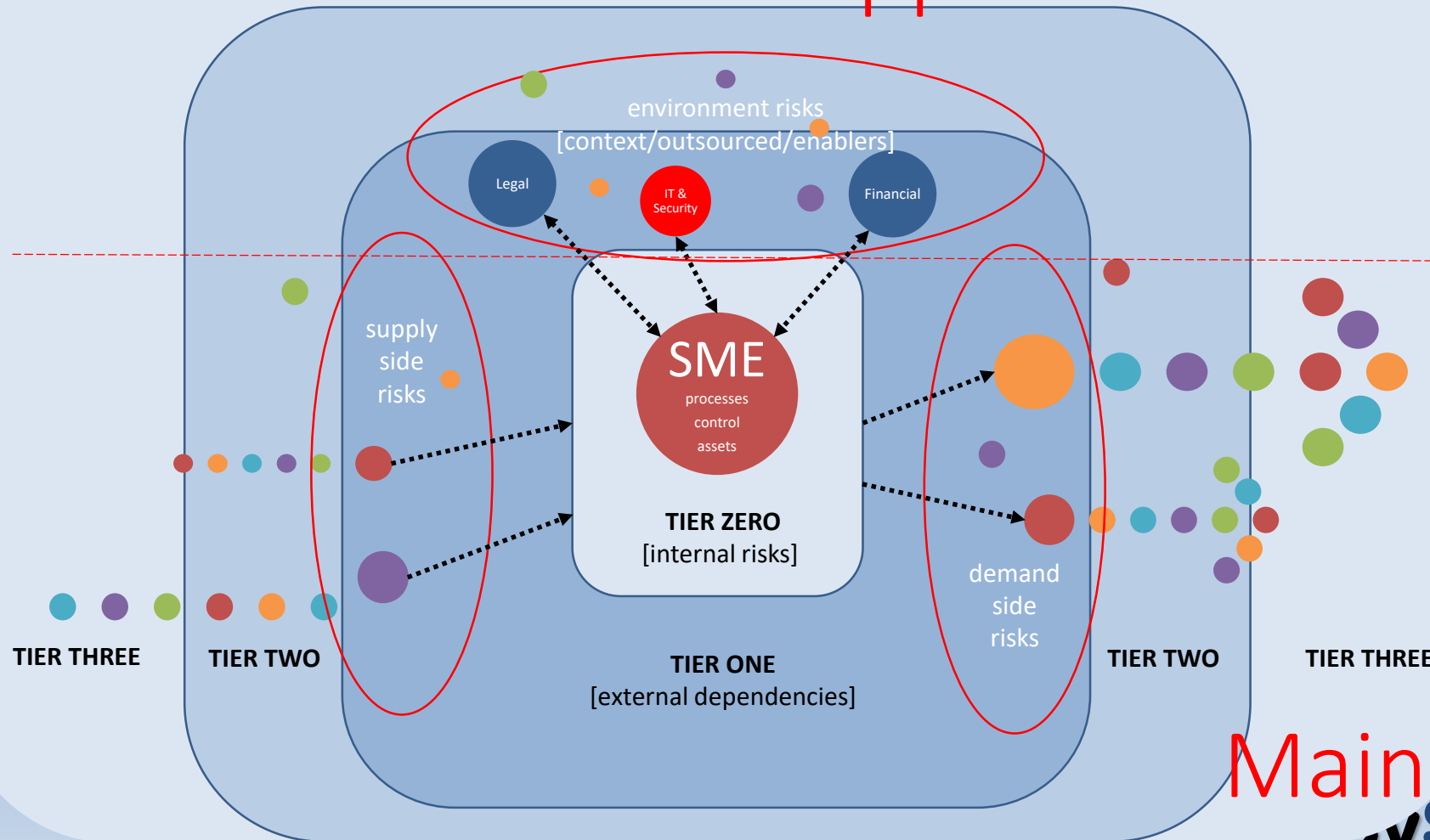


CySecLab

NT
THE FIRST SCIENCE AND TECHNOLOGY PARK IN BULGARIA

Supply/value chains as SoS - anatomy, roles, dependencies (SMEs role/risks)

Support activities + risks (hidden)



Main activities + risks

Based on "Value chain" model (Michael Porter)

SecLab

THE FIRST SCIENCE AND TECHNOLOGY PARK IN BULGARIA

Supply/value chains vulnerabilities and attacks

- **Hardware** - difficult to update – RottenSys malware > 5 mln mobile phones, 2018)
- **Software – 10 times increase 2017-2019**
- **Third-party (service providers)**



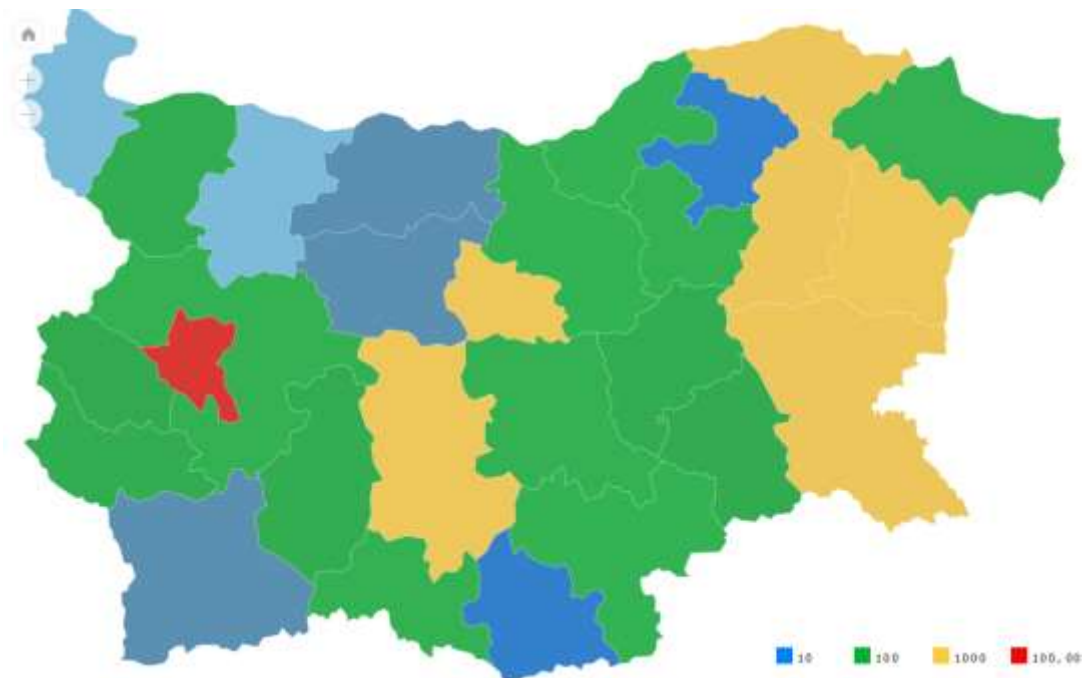
Digital interconnectivity = “web of digital dependencies”

2018 (CSO Online)

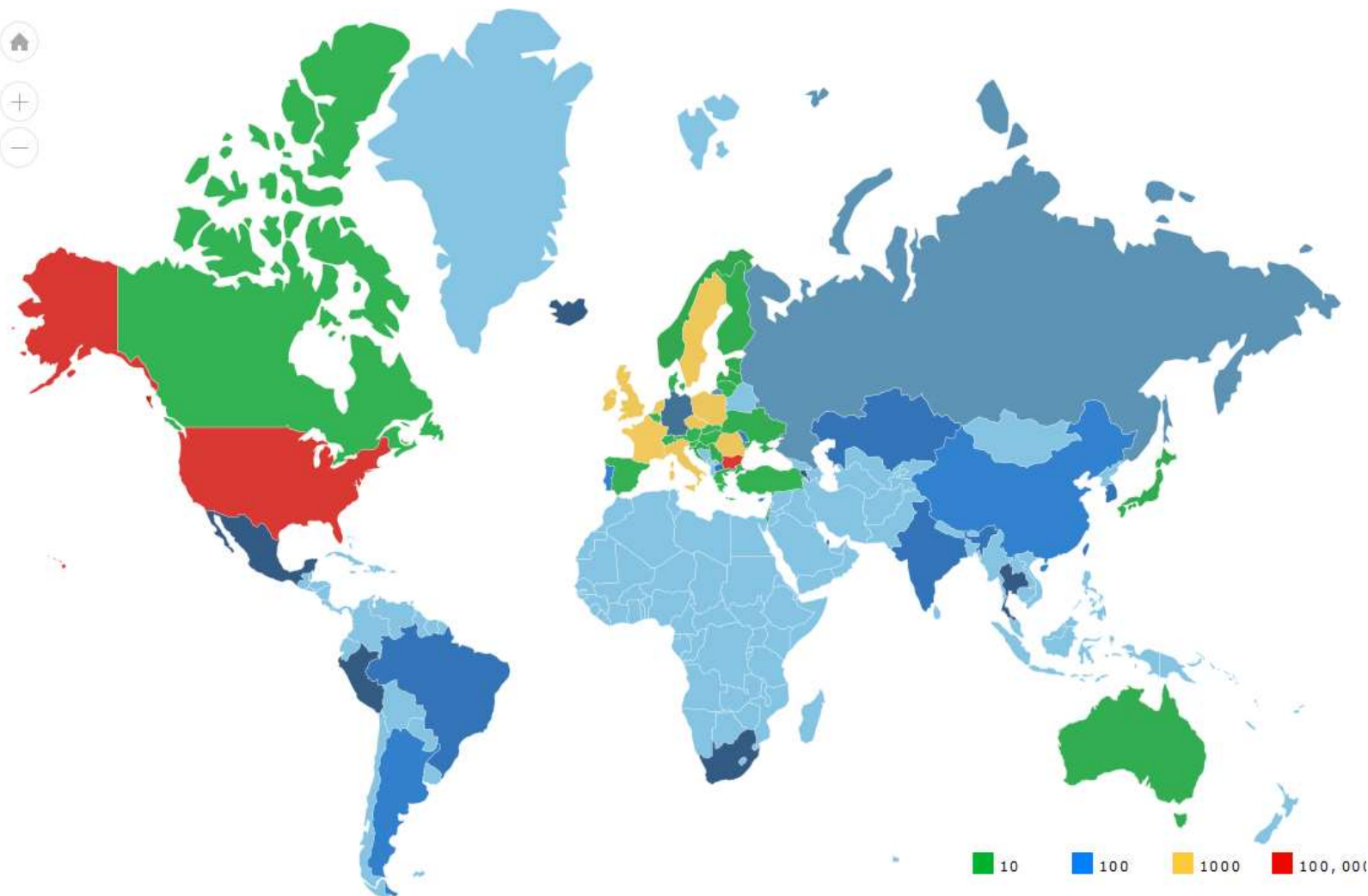
56% of organizations had a breach caused by a service provider

only **35%** of organizations had a list of third parties they **share sensitive information with**

ENISA (2019) – Supply Chain in Cyber Threat Intelligence (CTI) Program – “key threat”



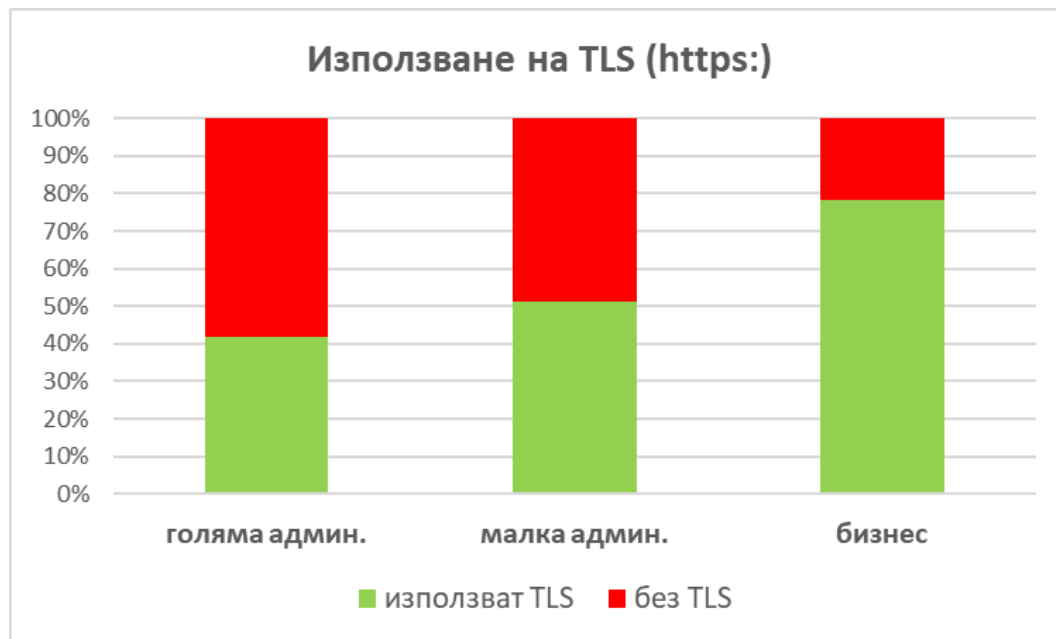
Административна карта на България, показваща струпването на домейни по административни райони на територията на България. Цвета на всяка област нагледно отразява броя хостове.



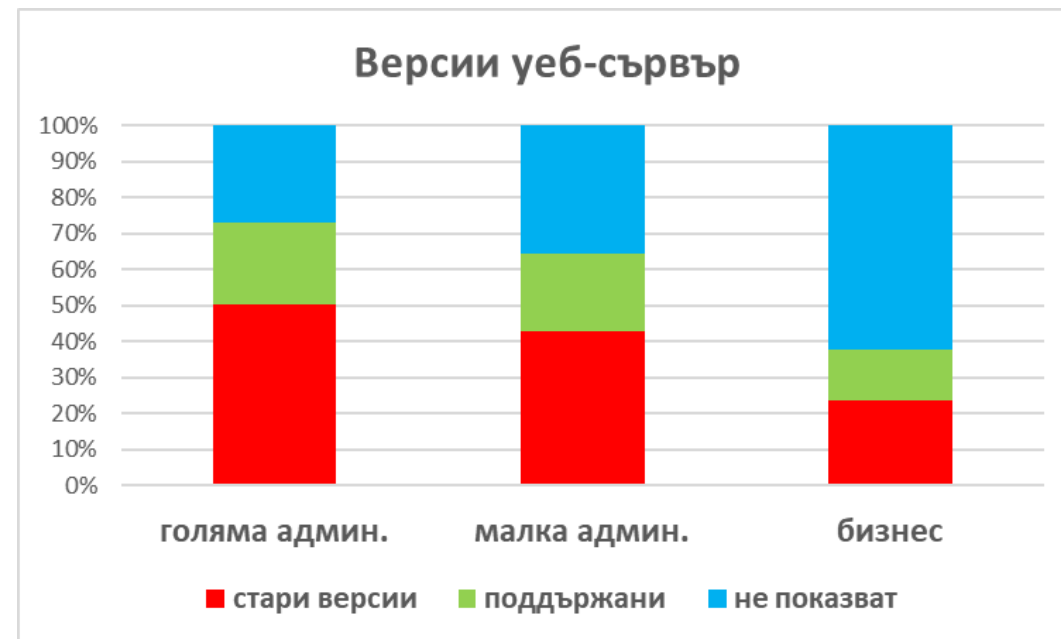
Глобална административна карта. Показва струпвания на хостове в глобален размер по държави. Цвета на всяка държава нагледно отразява броя хостове.



Обобщена графика визуализираща наличието на сигурна връзка (HTTPS)



Версии на уеб-сървъри (обобщени)



Доклад за ИПА (Институт за публична администрация) – пилотна справка уязвимости на уеб-сървъри публична администрация (регистрирани в „.bg“):

- Група „**малка админ.**“ – интернет сайтове (сървъри) на централна администрация (министерства, централни ведомства) – 28 бр.
- Група „**голяма админ.**“ – разширена група, добавени са и сайтове на местна администрация – общо 197 бр.
- Група „**бизнес**“ – случайна извадка от бизнес организации (индустрия, НПО) – 202 бр.

A proof: BG-GB Cyber Shockwave exercise

- Industry (Gas and oil distribution) >>> State (3 ministries, 3 agencies)
- Technical + Tabletop (4 main attack vectors + misinformation)
- Small (business) is BIG (threat)
- Context: EU elections (but CYBRID by nature, any time ...)

Tested:

EU Blueprint (ENISA), Cybersecurity Incident Taxonomy, AI & ML pilot

Asymmetry demonstrated:

RED team(+ simple AI/ML) <> **BLUE** team (Industry + State)

Supported by: UK Embassy, NCSC, UK companies/consultants

What's next: regional Cyber Shockwave 2020



- BG National Cyber Security Strategy “Cyber Resilient Bulgaria 2020” (2016)
- BG Cyber Security Act (Nov 2018) – including transposition of EU NIS Directive – Operators of Essential Services, Digital Services Operators
- BG June 2019 – Ordinance “Cybersecurity Act” (State e-Gov Agency), compliance, standards, assessments
- EU – GDPR (2018), NIS Directive (2018), Cybersecurity Act (June 2019) – role of ENISA, European Cybersecurity Certification Scheme

Legal requirements, norms

From capacity to capabilities:



cyber (CTF) competitions, exercises (+industry)
academic courses and labs, workshops, summer
schools and camps

CSAW'15



ecLab



THE FIRST SCIENCE AND TECHNOLOGY PARK IN BULGARIA



Software Engineering Institute



International Capacity - CryptoBG*

International Summer School on Cryptology and Cyber Resilience

<https://www.cryptobg.org> 9-16 July 2017



With the support of



Lab



THE FIRST SCIENCE AND TECHNOLOGY PARK IN BULGARIA

Contacts:

Dr. George Sharkov

g.sharkov@sofiatech.bg

gesha@esicenter.bg

Head, CySecLab (Cyber Security Lab), Sofia Tech Park

Director of ESI CEE

*National Cyber Security Coordinator (BG Government,
2014-2017) & Adviser PM*

Cyber Defense Adviser to the Minister of Defense

Yavor Papazov

yavor@esicenter.bg

Tech Team Lead,

CySecLab (Cyber Security Lab), Sofia Tech Park