



Cyber Noesis

# Still building the human firewall ... *Are we doing something wrong?*

**Konstantinos Papadatos,**

Founder / Managing Director - Cyber Noesis

MSc Infosec, CISSP-ISSMP, CISM, ISO27001 LA, ISO27005 RM, PMP, MBCI, CDPO, Lead SCADA Security Manager

Infocom Security 2022 – 06/07/2022

# Contents



About Cyber Noesis



CyberSecurity Awareness Mistakes



Putting all Pieces Together



# About us

Cyber Noesis was established in **2015** by a group of cyber security specialists with more than 100 years combined experience.

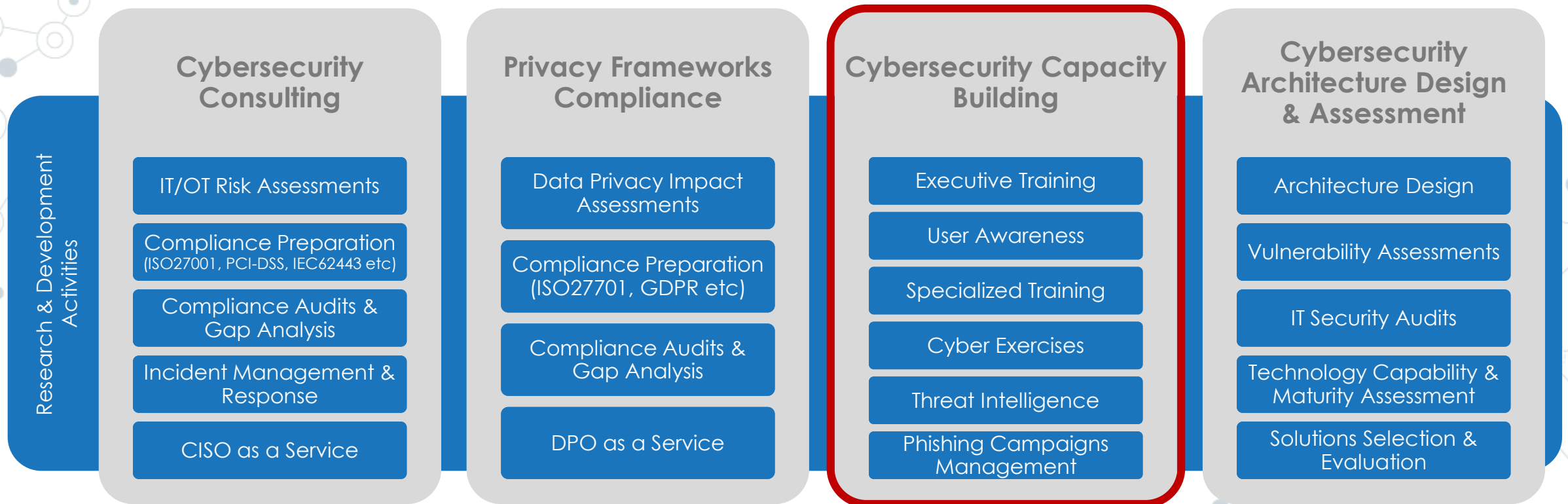
Specialization in:

**Enterprise Security & Industrial Security**



# Our Solutions

By developing this unique skill set in our resources, we can provide a suite of cyber security assessment services that can comprehensively evaluate all potential attack paths into mission critical infrastructures.



# Our Competitive Advantage

Our firm retains experienced cyber security professionals that have a blend of expertise in **Risk Assessments, Architecture Review & Design, Compliance with Regulatory Frameworks, Cybersecurity Capacity Building** as well as **OT systems security** backgrounds.

International  
Exposure

Over 100  
Cybersecurity  
Projects

Team of 15+  
Cybersecurity  
Experts

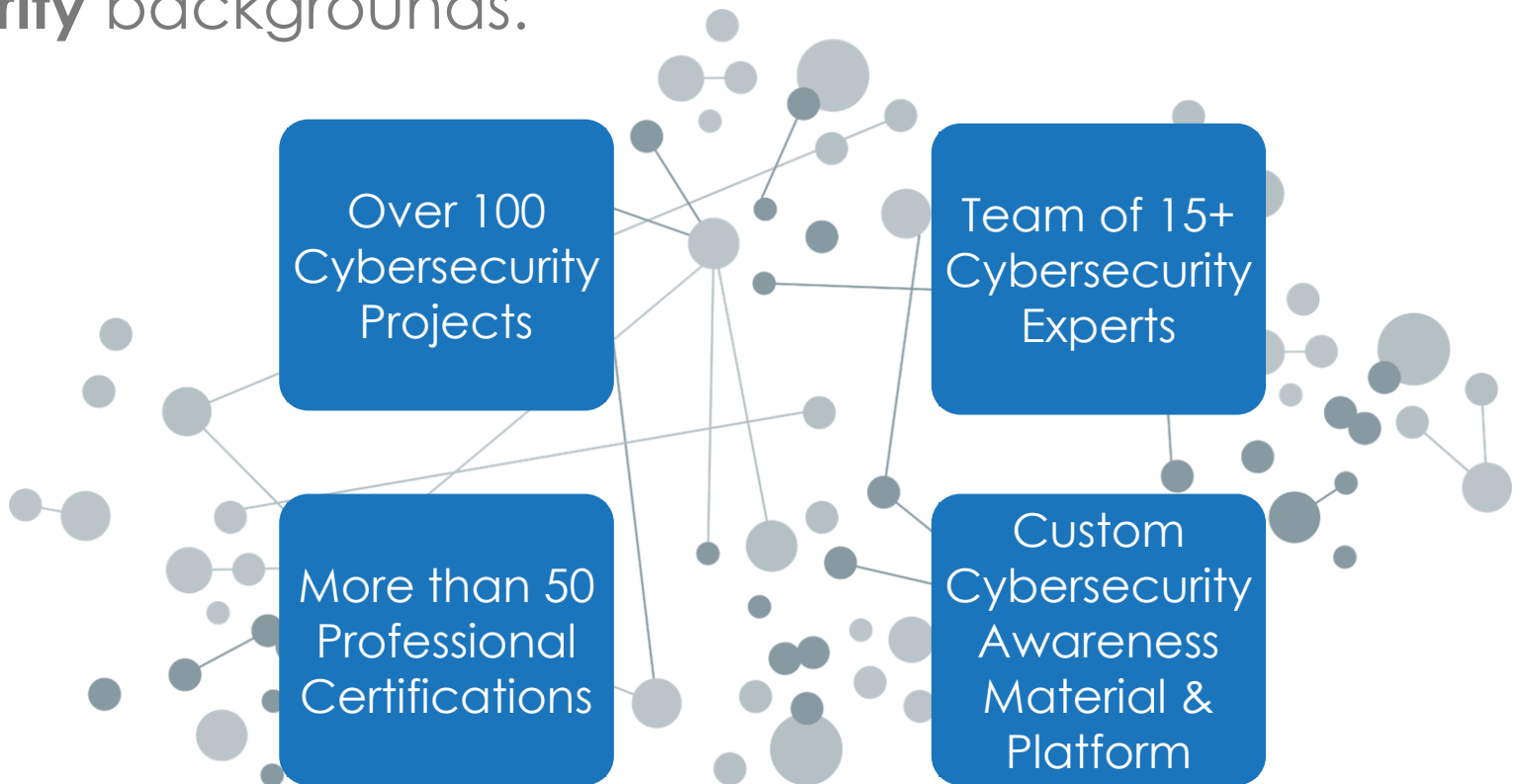
100 years  
collective  
Cybersecurity  
experience

Recognized  
Project  
Management  
methodologies

More than 50  
Professional  
Certifications

Custom  
Cybersecurity  
Awareness  
Material &  
Platform

Advanced  
LMS content  
development  
Tools



# isAWARE Platform (Information Security AWAREness)



  
Cyber Noesis

  
Cyber Noesis  
Group of Experts

 Set  
Objectives

 Update  
Material

 Customized  
Platform

## Phishing Campaign Management System



Vast Pool of  
Phishing Templates

Customized Phishing  
Templates

Comprehensive Phishing  
Campaign Dashboard

## Learning Management System




Customized Content  
Development




Security Training  
Courses

Security Training Games  
& Assessments

### Learning Booster

-  Digital Library
-  Assessment  
Methods
-  Participation  
Management
-  Gamified  
Learning
-  Grades
-  Certification of  
Achievement

### Communication Methods

-  Diary
-  Forums  
& Chat
-  Notifications

# Contents



About Cyber Noesis



**CyberSecurity Awareness Mistakes**



Putting all Pieces Together





# Indicative Real Attacks

Toyota Boshoku Corporation, an auto parts supplier, was the victim of a social engineering attack in 2019. The money lost amounts to **USD 37 million**. Using persuasion, **attackers persuaded a finance executive** to change recipient's bank account information in a wire transfer.

In March 2019, **the CEO of a UK energy provider** received a phone call from someone who sounded exactly like his boss. The call was so convincing that the CEO ended up transferring **\$243,000** to a “Hungarian supplier” — a bank account that actually belonged to a scammer.

## **\$75 Million Belgian Bank Whaling Attack**

Perhaps the most successful social engineering attack of all time was conducted against Belgian bank, Crelan. While Crelan **discovered its CEO had been “whaled”** after conducting a routine internal audit, the perpetrators got away with \$75 million and have never been brought to justice.



# There is NO specific victim profile!



Regardless of age, gender, academic background, professional experience, job position, and IQ,  
**everyone is likely to become a victim of cyberattacks...**



# Why Security Awareness Programs Fail?

- ✗ End-users simply **not knowing what the right course of action**
- ✗ Staff **not emotionally** involved.
- ✗ Objectives **not aligned with the strategic goals**.
- ✗ **Bland and generic content** fails to help the audience.
- ✗ **Settling for one-time**, compliance-driven approach.
- ✗ Content **not aligned** with local **culture, paradigms** and ... **language!**



# what do think about fast /canned food?

- ✓ Tasty...?
- ✓ Nutritious ...?
- ✓ Somehow Healthy ...?

**For how long can you  
be fed only with this?**



# Imagine a Security Awareness Video ...

- ✓ Strong Plot
- ✓ Storytelling
- ✓ Well-Made
- ✓ Film
- ✓ Hollywood Like Production







**What a funny video and  
a great production!**





**"Strong Password as  
defined in our Corporate  
Policy"?**

**Which policy?**






**Where can I find the policy?**

**I remember a document  
about 80 pages long...**


**Maybe our CISO will inform  
me later ...**





A woman with dark hair, wearing a dark blue blazer, is talking on a black mobile phone. She is standing in an office with orange and wood-paneled walls. A silver laptop is in the foreground, partially obscuring her lower body.

Be careful Paul, the  
“Fisherman” has sent  
us a new email for  
submitting credentials.

A man with dark hair and a beard, wearing a blue suit, white shirt, and dark tie, is talking on a black mobile phone. He has a questioning expression on his face and is gesturing with his left hand. He is in an office with large windows overlooking a city.

Really? This is the 2nd  
within this month... Is  
this again regarding  
MS 365 or Netflix?



Its about PayPal  
Service ... I never used  
this service, so it was  
easy to identify...



Thank you, Maria! I will  
also inform John and  
Kathy...







# What should we make differently ?

- Custom material
  - Based on organization needs...
  - Adapted to user's daily routine...
  - Adapted to local culture & user experience.

# We have to start thinking differently...



How would you educate your children about the negative effects of drug addiction?

Would you do so by asking them to watch just a, maybe well-made, impersonal video?





## What should we make differently ?

- Deploy various educational techniques.
- Reinforce the security message.
- Be patient and ready to explain multiple times.
- Treat communication like a game.
- Aim the effective understanding of an average user.

# Who are these guys?



Is it crucial for our end-users to know them?

Is their paradigm related with our culture?



# What should we make differently ?

- Use common language to align business objectives.
- Use elements of novelty.
- Use local language.
- Use easily understood paradigms aligned with users' culture.



# Contents



About Cyber Noesis



CyberSecurity Awareness Mistakes



**Putting all Pieces Together**



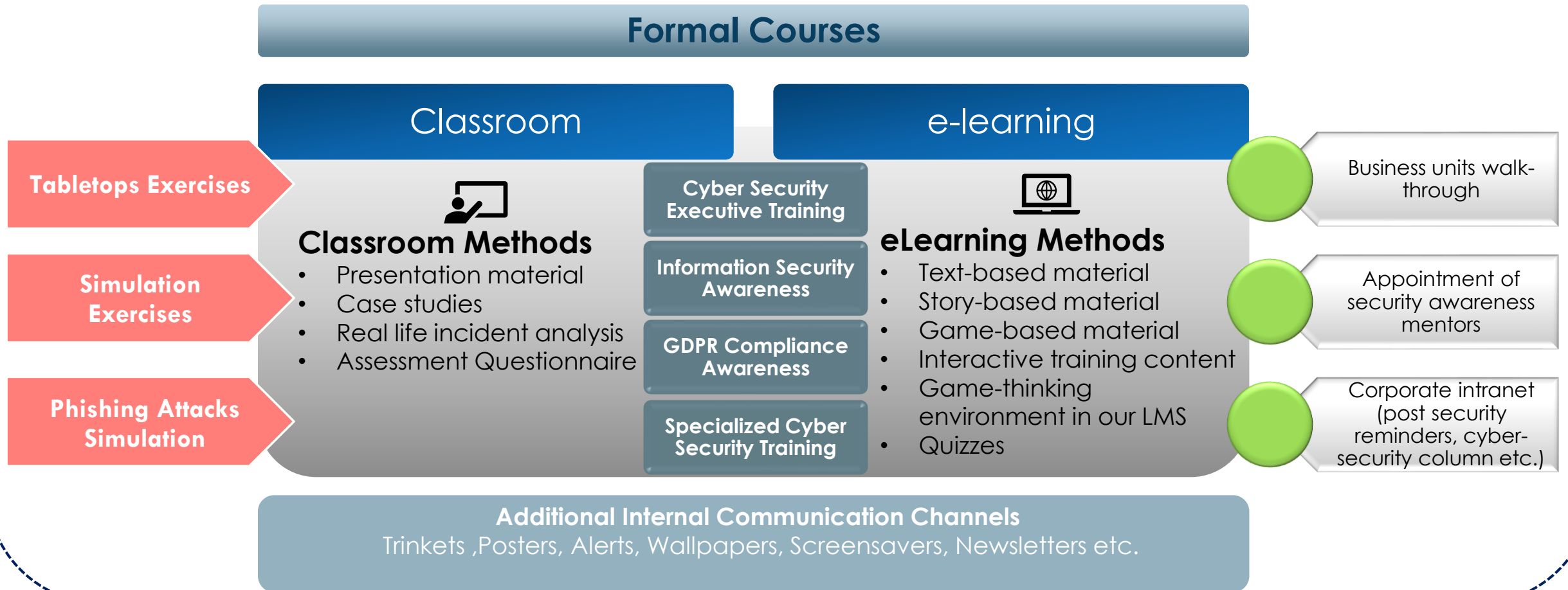


# Behavior change is an ambitious (and necessary) goal!

- ➡ Learning in the correct context.
- ➡ Repeating actions to embed knowledge.
- ➡ Continuous evaluation to adopt strategy.
- ➡ Rewarding staff to encourage new habits.

# Putting all pieces together...

## Information Security Education & Awareness Programme





# Our Courses' Customization Methodology



# Our Phishing Campaign Customization Methodology



# Cyber Noesis' Training Services & isAWARE Platform Awards

- © Cyber Security Awards 2022: Gold Award in Education and Training Services Category
- © Cyber Security Awards 2022: Silver Award in Cyber Awareness Category
- © Education Leaders Awards 2022: Bronze Award in Remote & Hybrid Training Services
- © BITE Awards 2021: Silver Award in IT Security for isAWARE Platform



# Cyber Security Awareness Program



Should be designed to change behavior and reinforce **good security practices**.



Should train individuals to **recognize Information Security concerns** and respond accordingly.



Should be focused on the organization's **entire employee population**.



Should aim **all levels of the organization** including senior and executive managers.



Should inform employees about their **roles**, and **expectations** surrounding their roles.



Should be designed in a way that can be deployed in **various ways, methods and techniques**.



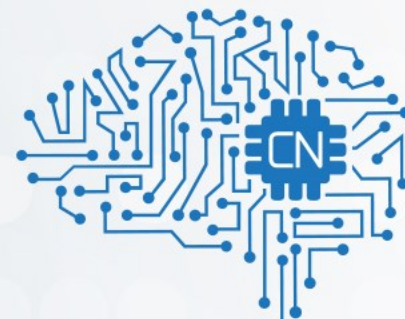
Cyber Noesis

***Lack of knowledge is not the  
users' fault!***

**Thank you!**

[www.cybernoesis.com](http://www.cybernoesis.com)





# Cyber Noesis

We position...  
**CYBER SECURITY FIRST!**



[www.cybernoesis.com](http://www.cybernoesis.com)