HELLENIC

Connect | Educate | Inspire | Secure

Balancing cyber risks and profits; ways to tip the scale.

John ILIADIS
President of (ISC)^2 Hellenic Chapter

60 seconds about $(ISC)^2$ and the Hellenic Chapter

Start counting!

HELLENIC

Who is (ISC)²?

- **Largest** nonprofit membership association of certified security professionals
- Provider of lifelong professional **security education**
- **Global advocate** for the growth and success of the security profession
- 500.000 members, associates and candidates
- 170 Countries

(ISC)² Hellenic Chapter

past few months…

What we 've been up to (past 6 months)

- 4 Members-only events
- Vendor-based training in the works?
- 2x Gold CyberSecurity Awards (again…)
- Thought leadership in 5 Conferences
- Two TV appearances
- NIST CSF translation
- Two security awareness events delivered onsite, upon request
- New sheriff in town (BoD elections)

Without further ado…

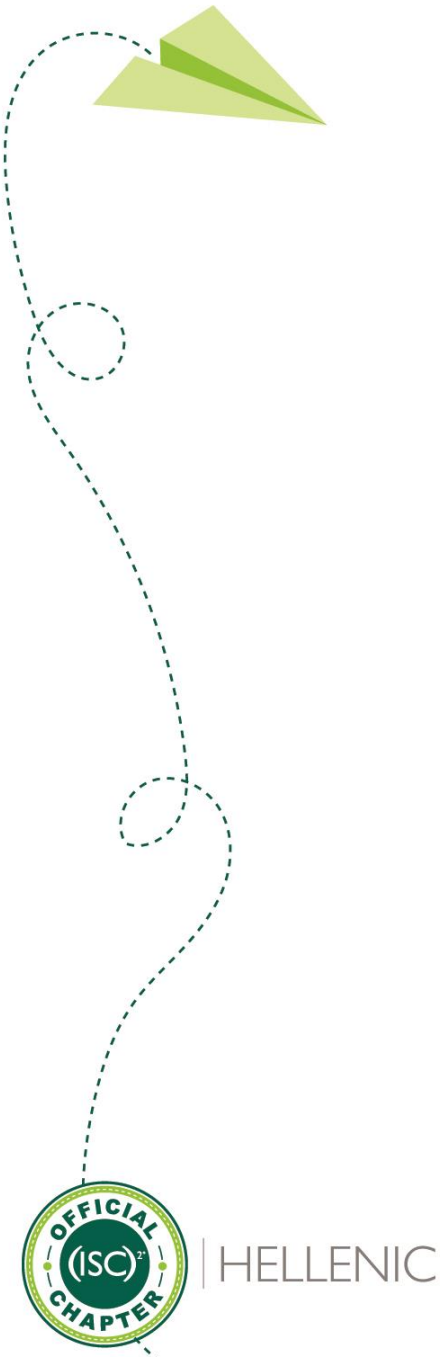
jot down your questions;
plenty of time for them, today ☺

OFFICIAL (ISC)² CHAPTER | HELLENIC

The Agenda

- Three kinds of CISO
- Three ways to talk to the people upstairs
- Three steps towards becoming the perfect CISO
- One way to CISO's sudden death

THREE KINDS OF CISO



CISO - THE DEFENDER

- Defending organization's information assets
- Maintain a strong cybersecurity posture
- Managing Security Operations

OFFICIAL (ISC)² CHAPTER | HELLENIC

CISO - THE BUSINESS-ENABLER

- Ensures security measures don't hinder growth
- Integrates InfoSec into:
  - Strategy building
  - Product development
  - Other decision-making processes

- Delivers informed risk choices towards profitable outcomes

OFFICIAL (ISC)² CHAPTER | HELLENIC

CISO – IN PRISON

- Wells notice* served to Solarwinds CISO
- Uber CISO convicted
- Who's next?
- Get out of jail free card?

* *"notification issued by regulators to inform individuals or companies of completed investigations where infractions have been discovered… the nature of the enforcement proceedings to be initiated against the recipient"*

OFFICIAL (ISC)² CHAPTER | HELLENIC

Get out of Jail Free Card ?

- Include CISOs in D&O contracts! It's a must-have.
- Proactively maintain incident response plans
  - Technical response
  - Coordinate with legal (inform authorities)
  - Crisis management

- Clarity
  - Clear lines of reporting with executive leadership
  - Share responsibility for cybersecurity decisions

OFFICIAL (ISC)² CHAPTER | HELLENIC

Three Ways to Talk About Security to the People Upstairs

HELLENIC

1 - Security – a fad?

Chasing after those constantly emerging buzzwords towards the elusive Holy Grail?

Undermines essence of Security

Stakeholders may dismiss Security as irrelevant

2 - Security – FUD ?

Fear, Uncertainty and Doubt

Risk owners can never be certain they ‘ve got the controls they need

Always look on the dark side of life

Leads to negative atmosphere and hinders collaboration

OFFICIAL (ISC)² CHAPTER | HELLENIC

3 - Security – an Investment Center!

Framing it as an enabler of business growth, innovation and competitive advantage

Helps align security initiatives with business goals

Highlights the ROI associated with security measures

Encourages stakeholders to view security as a critical component of their strategic decision-making

OFFICIAL (ISC)² CHAPTER | HELLENIC

THREE STEPS TOWARDS BECOMING THE PERFECT CISO

OFFICIAL (ISC)² CHAPTER | HELLENIC

The perfect CISO: *mythical unicorn?*

The Perfect CISO; a step-by-step guide

- Step 1: Be an InfoSec leader
- Step 2: Treat Security as an Investment Center
- Step 3: Excel in Communication

let's do this, one step at a time…

Step 1: Be an InfoSec Leader

Be an InfoSec Leader

Executive Committee to CISO:
"Talk to us, Bob; how are we doing with respect to Security?"

OFFICIAL (ISC)² CHAPTER | HELLENIC

Be an InfoSec Leader

CyberSecurity Posture					
Identify	Governance	↗	**Detect**	Log and Event Management	↗
	Asset Management	■		Incident Monitoring	↘
	Risk Assessment	■	**Respond**	Incident Response Planning	↗
	TPRM	↘		Crisis Management	↗
Protect	Identity Management	↗		Mitigation	■
	Service Segmentation	■	**Recover**	Planning	↗
	Data Classification	↗		Testing	↗
	Protecting Data at Rest	↘		Improving	↘
	Protecting Data in Transit	↗			
	Protecting Data in Use	■			

↗ Trending positively ■ No change ↘ Trending negatively

OFFICIAL (ISC)² CHAPTER | HELLENIC

Be an InfoSec Leader

CyberSecurity Posture					
Identify	Governance	↗	**Detect**	Log and Event Management	↗
	Asset Management	■		Incident Monitoring	↘
	Risk Assessment	■	**Respond**	Incident Response Planning	↗
	TPRM	↘		Crisis Management	↗
Protect	Identity Management	↗		Mitigation	■
	Service Segmentation	■	**Re**	Planning	↗
	Data Classification	↗			↗
	Protecting Data at Rest	↘			↘
	Protecting Data in Transit	↗			
	Protecting Data in Use	■			

↗ Trending positively ■ No change ↘ Trending negatively

OFFICIAL (ISC)² CHAPTER | HELLENIC

Be an InfoSec Leader

- Accompanying your 1-pager with KPIs
  - Prevents “you are pulling my leg” situations
  - Highlights the ROI associated with security controls
  - Encourages stakeholders to view security as a critical component of their strategic decision-making

Be an InfoSec Leader

CyberSecurity Posture					
Identify	Governance	↗	**Detect**	Log and Event Management	↗
	Asset Management	■		Incident Monitoring	↘
	Risk Assessment	■	**Respond**	Incident Response Planning	↗
	TPRM	↘		Crisis Management	↗
Protect	Identity Management	↗		Mitigation	■
	Service Segmentation	■	**Recover**	Planning	↗
	Data Classification	↗		Testing	↗
	Protecting Data at Rest	↘		Improving	↘
	Protecting Data in Transit	↗			
	Protecting Data in Use	■			

Security By Design - % of risks detected after deployment

Third-Party Risk Exposure - Percentage of third-party vendors assessed for risk, along with their risk ratings

Risk Mitigation Rate - Percentage of identified risks that have been adequately mitigated to an acceptable level

Incident Monitoring - Average time taken to initiate incident response to address security incidents

OFFICIAL (ISC)² CHAPTER | HELLENIC

Step 2: Treat InfoSec as an Investment Center

Treat InfoSec as an Investment Center

- **Executive Committee to CISO:**
- "Why should we invest in this latest series of security controls?"

OFFICIAL (ISC)² CHAPTER | HELLENIC

Treat InfoSec as an Investment Center

InfoSec investing is a two-way business street

You give some resources (money, other resources?)	You get stg back (achieving business goals)

How can we present that to the people upstairs?

Treat InfoSec as an Investment Center

Business Goals[1]	Cyber Risks	Security Controls
Produce the most trustworthy weather forecasting service to the public (income: ads)	--Unable to finalise predictions in time --Unable to receive weather sensor readings in time --Third party injects (MitM) false weather sensor readings	--Elastic infrastructure to compensate for peaks --Multiple independent comms to the sensors --Strong and continuous sensor authentication and encryption
Deliver the fastest and always-available weather forecasting service	--Delays in response to specific parts in the world --Delays in presenting the info to the public (DDoS, lack of infra resources)	--Elastic infrastructure to compensate for high demand --High availability infrastructure to reduce downtime risk --CDN service to ensure low response time and fight-off DDoS

[1]Two ways a CISO is made aware of business goals:

- **Proactively**. CISO is part of the Executive Committee, planning controls proactively.
- **Reactively**. CISO fills-in the first table column based on what officials said to the press, financial markets rumors, business goals in the website; unorthodox, but what if it happens?

OFFICIAL (ISC)² CHAPTER | HELLENIC

Treat InfoSec as an Investment Center

- Leading the InfoSec investment discussion about a new product or service, during design time

OFFICIAL (ISC)² CHAPTER | HELLENIC

Treat InfoSec as an Investment Center

Business Goals[1]	Cyber Risks	Security Controls
Produce the most trustworthy weather forecasting service to the public (income: ads)	--Unable to finalise predictions in time --Unable to receive weather sensor readings in time --Third party injects (MitM) false weather sensor readings	--Elastic infrastructure to compensate for peaks --Multiple independent comms to the sensors --Strong and continuous sensor authentication and encryption
Deliver the fastest and always-available weather forecasting service	--Delays in response to specific parts in the world --Delays in presenting the info to the public (DDoS, lack of infra resources)	--Elastic infrastructure to compensate for high demand --High availability infrastructure to reduce downtime risk --CDN service to ensure low response time and fight-off DDoS

BoD: How much Security is enough?
Don't we have enough already?

CISO: Next slide, please ☺

OFFICIAL (ISC)² CHAPTER | HELLENIC

Treat InfoSec as an Investment Center

- How much security is enough to make an omelet?
- Secret omelet ingredients!
  - **Risk governance; how?**

  - **Risk Appetite; what is it?**

OFFICIAL (ISC)² CHAPTER | HELLENIC

Treat InfoSec as an Investment Center

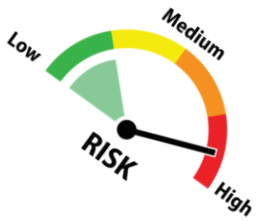
- Risk Governance
  - Product/Risk Owners?
  - Materiality of Cyber Risk (SEC) and disclosure?
  - Documented risk management process? Tool?
  - Residual risk acceptance?
  - Risk informed decisions towards **profitable** outcomes

OFFICIAL (ISC)² CHAPTER | HELLENIC

Treat InfoSec as an Investment Center

Risk Appetite *(an example)*

- Risks A, B: intolerable → mitigate
- Risks C: tolerable → closely monitor
- Risks D: no special attention



		Impact		
		High	Medium	Low
Likelihood	High	A	B	C
	Medium	B	C	D
	Low	C	D	D

Risk Matrix

OFFICIAL (ISC)² CHAPTER | HELLENIC

Step 3: Excel in Communication

Excel in Communication

You are NOT talking to them! “SHA256” or “Steganography” means nothing to most people.

OFFICIAL (ISC)² CHAPTER | HELLENIC

Excel in Communication

Be like the Borg. Adapt, depending on the audience*

OFFICIAL (ISC)² CHAPTER | HELLENIC

**Star Trek reference to a group of cybernetic organisms that adapt quickly to unforeseen and adverse conditions*

Excel in Communication

- Adapt style depending on audience
  - What's in it for them?
  - Creating alliances
- Persuading ≠ deceiving; highlighting your points
- Let's take theory and put it to practice…

OFFICIAL (ISC)² CHAPTER | HELLENIC

Excel in Communication

putting theory to practice

» Loss aversion

- The biannual cost of this CyberSecurity service went up by 20% for new purchases after February 20th
- We are eligible for a 17% discount on the biannual cost of this new CyberSecurity service, until the 19th of February

» Sunk Cost Effect

- We ‘ve purchased this VPN solution. Invest in the 2FA add-on?
- This (bundle) VPN license has got 2FA capabilities; activate it?

OFFICIAL (ISC)² CHAPTER | HELLENIC

Excel in Communication

putting theory to practice

» Framing

- The biannual cost for this new CyberSecurity service will go up from 5.000€ to 8.000€, after February 20th
- The daily cost for this new CyberSecurity service will go up from 7€ to 10€, after February 20th

» Active Choice

- We should invest on the new XR534U71 CyberSecurity product to protect Service X
- Should we keep the Cyber Risk at high levels for Service X or bring it down with the new XR534U71 CyberSecurity product?

OFFICIAL (ISC)² CHAPTER | HELLENIC

Excel in Communication

putting theory to practice

» Enhanced Active Choice

- Should we keep the Cyber Risk at high levels for Service X and pay the increased (+1.000€) annual Cyber Insurance premium it carries along, or should we bring Cyber Risk down with the new XR534U71 CyberSecurity product? *(saliency of negative choice's cost)*

» Compromise Effect

- Which Cyber Insurance contract should we get?
  - 1.5mil premium, 5mil policy limit ?
  - 70K premium, 550K policy limit?
  - 8K premium, 25K policy limit?

(three options varying along two dimensions; option of choice: the middle one)

OFFICIAL (ISC)² CHAPTER | HELLENIC

Are we done????

- PERFECTION IN BALANCING PROFITS AND RISKS?
- ARROGANCE? ICARUS "SUDDEN DEATH"?
- MEMENTO MORI… *

*In some accounts of the Roman triumph, a companion or public slave would stand behind or near the triumphant general during the procession and remind him from time to time of his own mortality

OFFICIAL (ISC)² CHAPTER | HELLENIC

Saving CISOs from SUDDEN DEATH

Rule No1: It's all about *our infosec people*, …$#%id

Rule No2: Read again Rule No1!

It’s all about our infosec people, …$#%id Part 1

- Challenges
  - Overworked and stressed out
  - Understaffed

- We need to become better at:
  - Coaching our people
    - take a look at *Coaching with Compassion;* many more out there
  - Headhunting; we are 3.4mil short
    - think outside of the box; use CC or other novel tackling methods

OFFICIAL (ISC)² CHAPTER | HELLENIC

It's all about our infosec people, …$#%id Part 2

» We need to become better at:

- Developing our people

CFO: What if we train them and they leave?

CISO: What if we don't train them and they stay?

- Investing in diversity; groupthink ↓ confidence ↓

OFFICIAL (ISC)² CHAPTER | HELLENIC

Q&A

…our Members grow stronger, together!

j.iliadis@isc2-chapter.gr

OFFICIAL (ISC)² CHAPTER | HELLENIC