The New Era CISO – Fantasy Unicorn or Superhero?
A first 120 Days Roadmap

Panagiotis Kalantzis
MScIS, CISSP, CISM, CISO, ISO27001 LA
Cyber Security & Data Privacy Expert

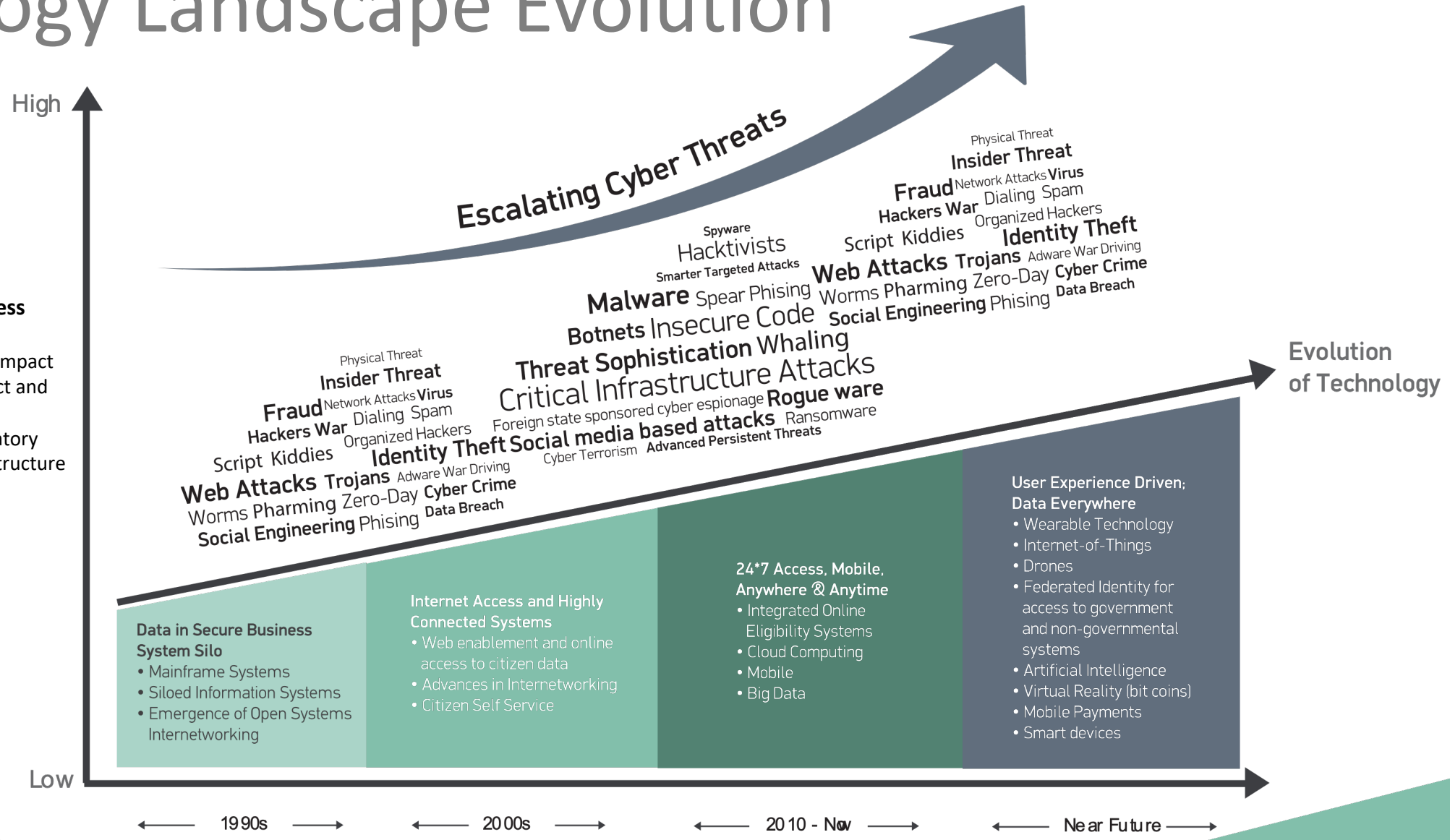
Agenda

- Modern Threats & Traditional Information Security
- Expectations of a Modern CISO
- Modern CISO Life
- Tools in the Armory of the Modern CISO
- Summary

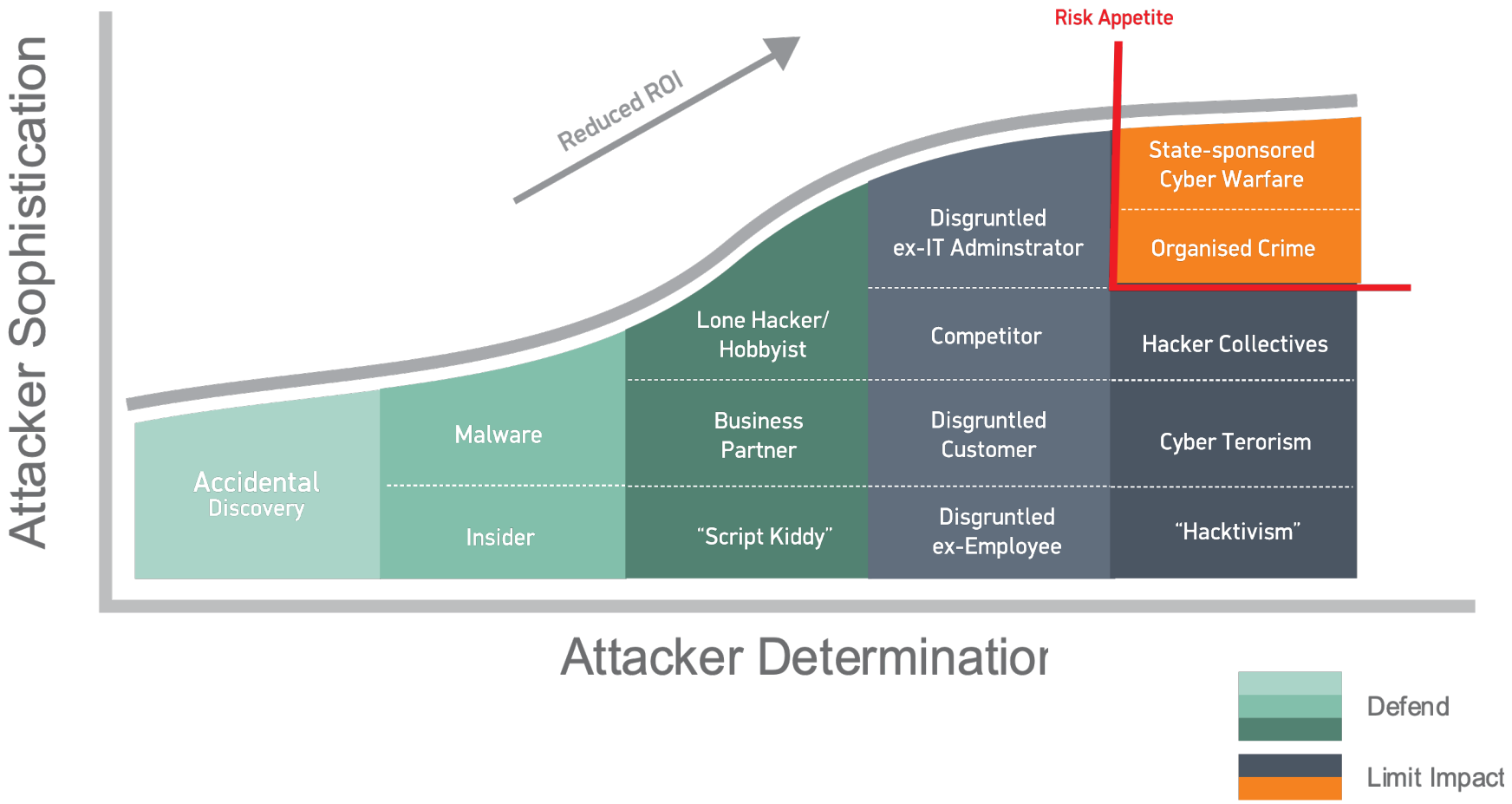
Traditional Information Security Function

Protect – Shield – Defend - Prevent

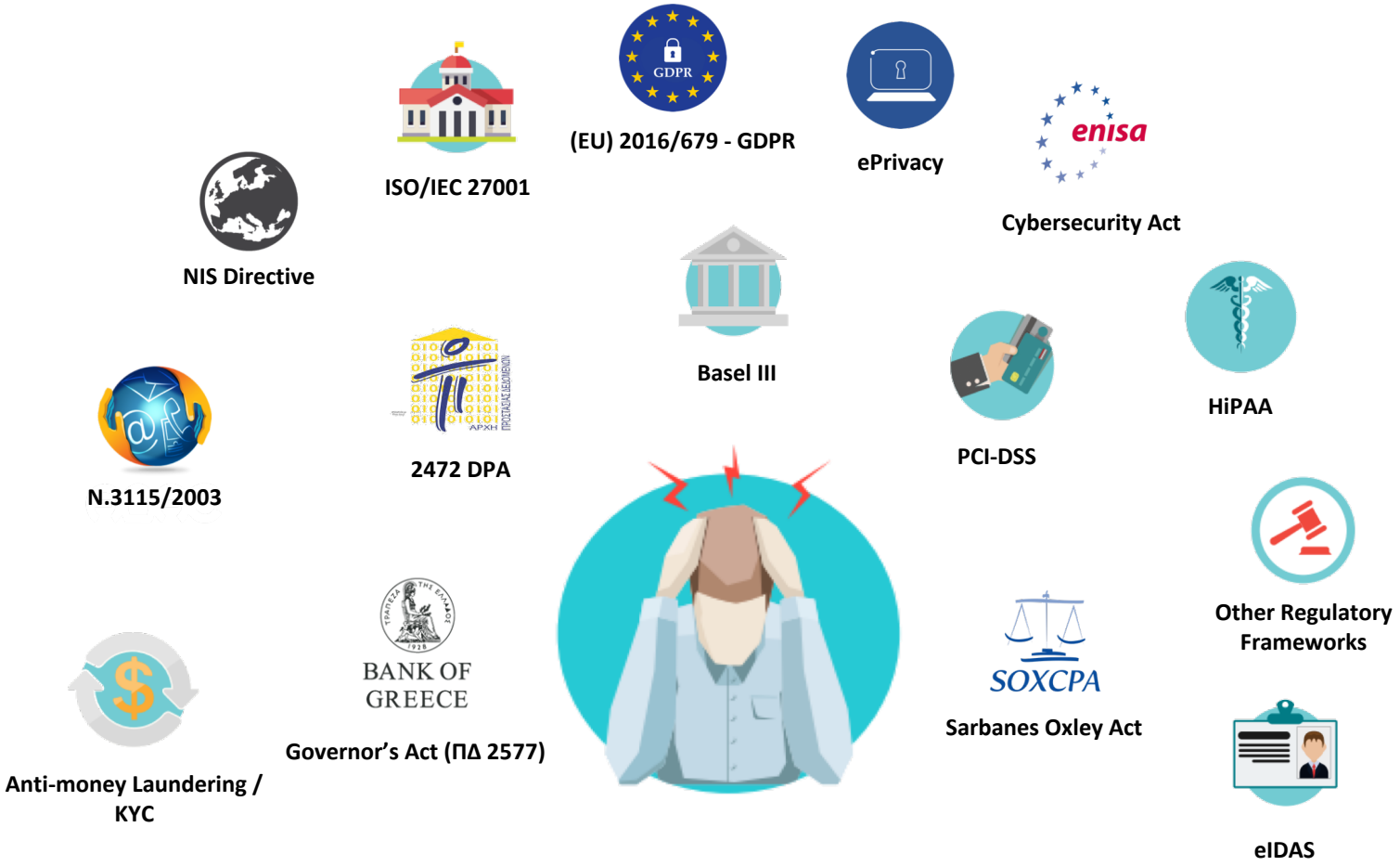
Technology Landscape Evolution



Attacker Profile



Multitude of Requirements



Traditional Information Security Function

Protect – Shield – Defend - Prevent

- ✓ Is Necessary
- ✓ Is Not Sufficient
- ✓ **Fails too Frequently**

Towards a Modern Information Security Function

1. Protect – Shield – Defend – Prevent
2. Monitor – Detect – Hunt
3. Respond – Recover – Sustain

Information Security in the Boardroom

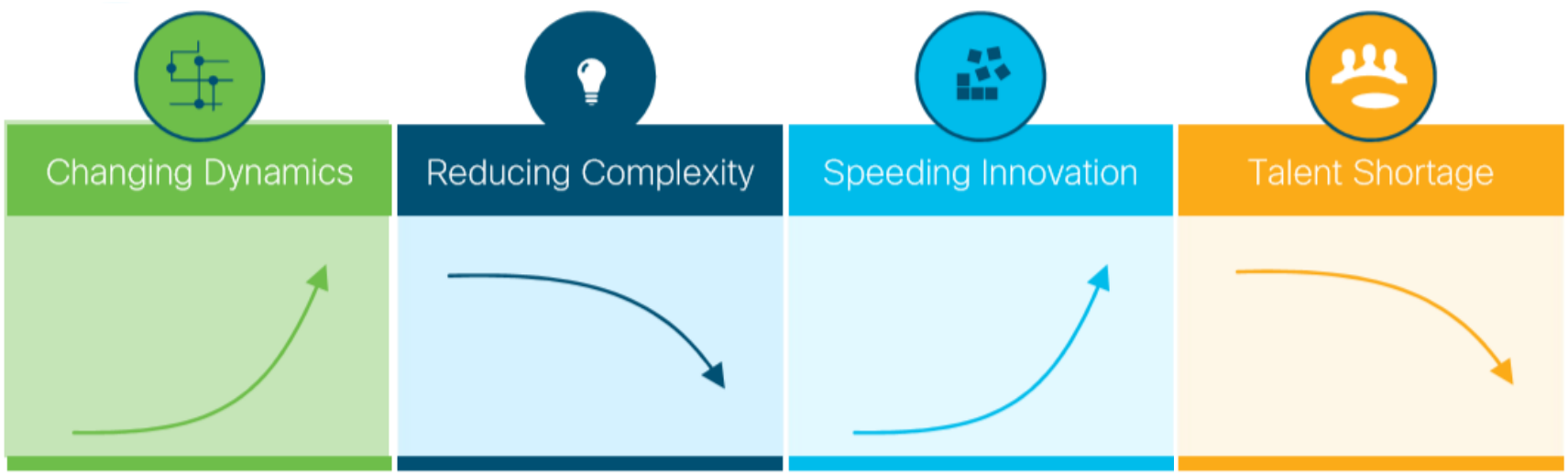
Modern CISO Life NOT Simple

Modern CISO Expectations

Strategic security	Technical security
Security framework	Hardware hardening
Policy development	Incident response
Awareness campaigns (ISTAP)	Firewalls
Security procedures	Anti-virus software
Regulatory compliance	Intrusion detection and prevention
IS management systems	Vulnerability scans
Risk analysis	Penetration testing
Best practices	Data-loss prevention tools
Data privacy (GDPR)	Access control
Crisis management	System security
Organisational view	Network security
Security regardless of technology	System monitoring
Government models (Cyber Essentials)	IT disaster recovery

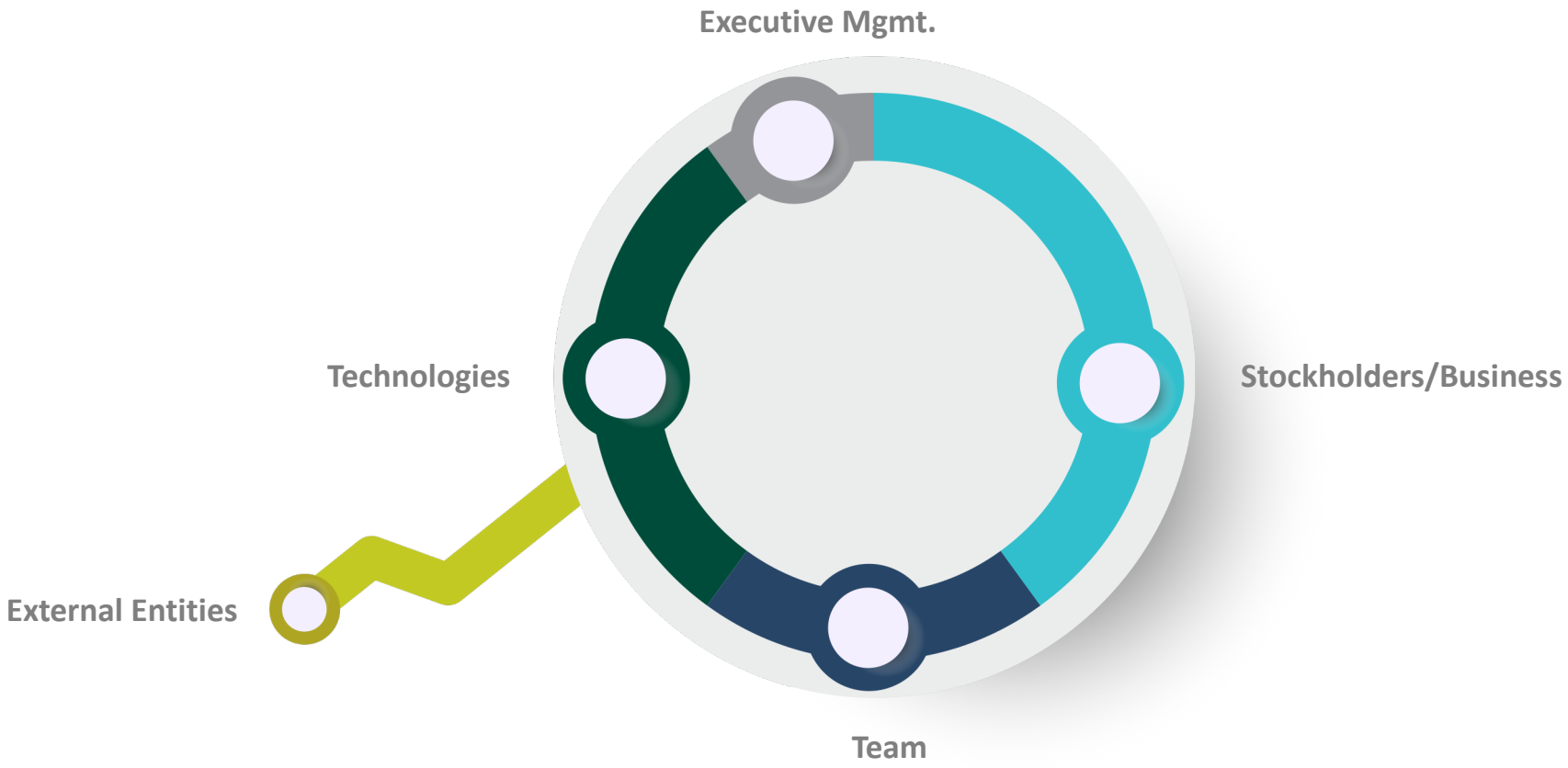

Network Security
Network Firewall
Network Monitoring/Forensics
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Web Security
Messaging Security
Risk & Compliance
Security Operations & Incident Response
SIEM
Security Incident Response
Momentum
CYBERscape · 1Q17
Threat Intelligence
Specialized Threat Analysis & Protection
Data Security
Mobile Security
Industrial / IoT Security
Fraud Prevention / Transaction Security
Identity & Access Management
Cloud Security

CISO in Digital Transformation

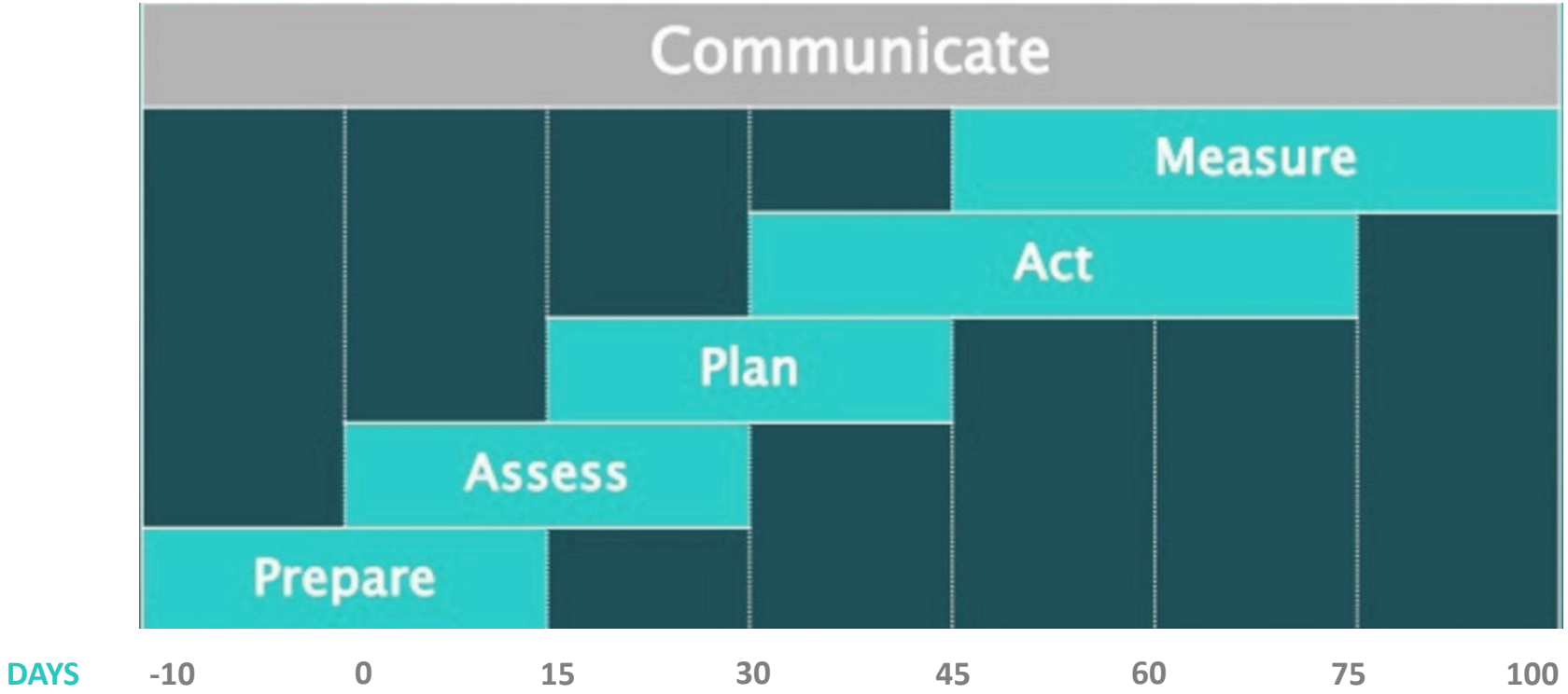


Does Modern CISO Exist?

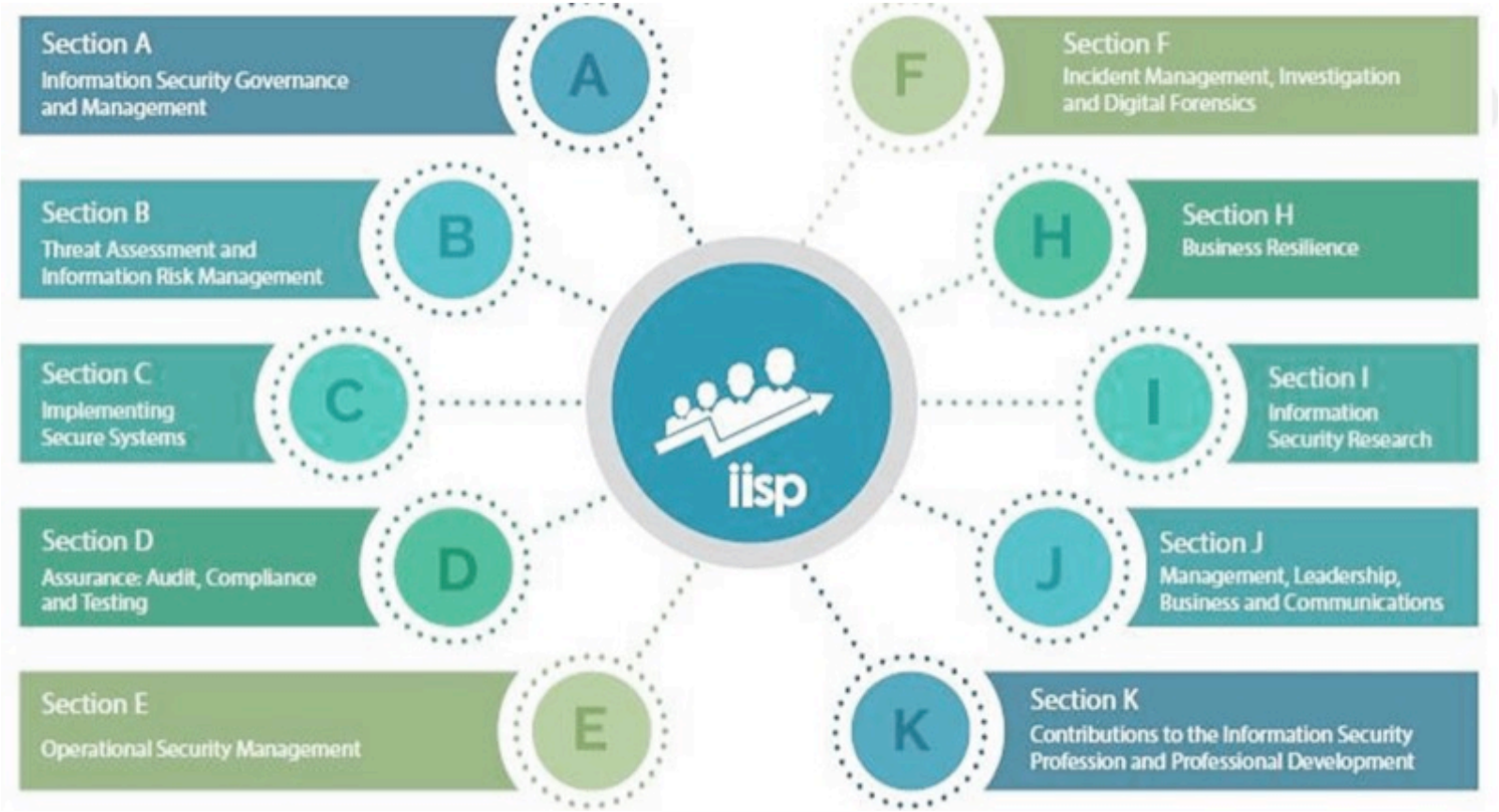
CISO 360 Role



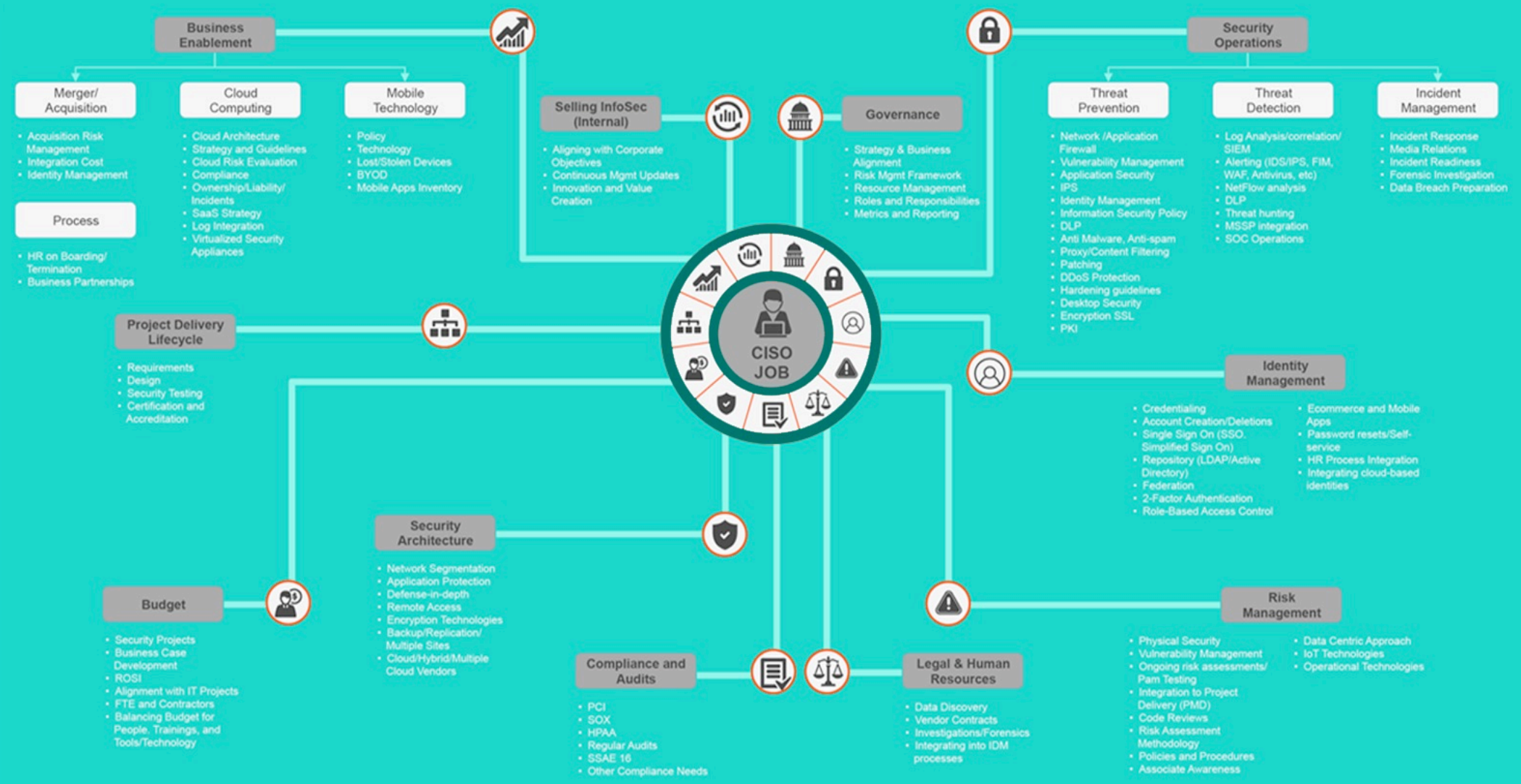
100 First Days of Everything



IISP Skills Framework



CISO Mind Map



CISO PERIODIC TABLE

Dx Digital Transformation									
Go Governance	Am Asset Management	Ns Network Security				Cs Cloud Security	Bd Big Data	Mi Malicious Insiders	Ra Role and Responsibility
Rm Risk Management	Cm Change Management	Es Endpoint Security	Tm Threat Management	Pt Penetration Testing	Ics Identity Centric Security	Dr Detection and Response	Ml Machine Learning	Ni Negligent Insiders	Bu Budget
Co Compliance	Pm Patch Management	Vm Vulnerability Management	As Application Security	SM Security Info & Event Mgmt (SIEM)	Dso DevSecOps	Sr Security Orchestration & Automation	IoT Internet of Things	Ha Hactivism	St Staffing
Gdp GDPR	Cfg Configuration Management	Es Email Security	Dp Data Protection	Ir Incident Response	Trm Third Party Risk Management	Th Threat Hunting	Bc Block Chain	Nt Nation State	Te Technology
Ba Business Alignment	Iam Identity Access Management	Ws Web Security	Soc Security Operations Center	Cti Cyber Threat Intelligence	Ca Cloud Access Security Broker	Ng Next Gen SOC	Ai Artificial Intelligence	Oc Organized Crime	Oz Organization

- Business Fundamentals
- IT Fundamentals
- Security Program Fundamentals
- Advanced Security Programs
- Emerging Technology
- Threat Actions
- CISO Constraints

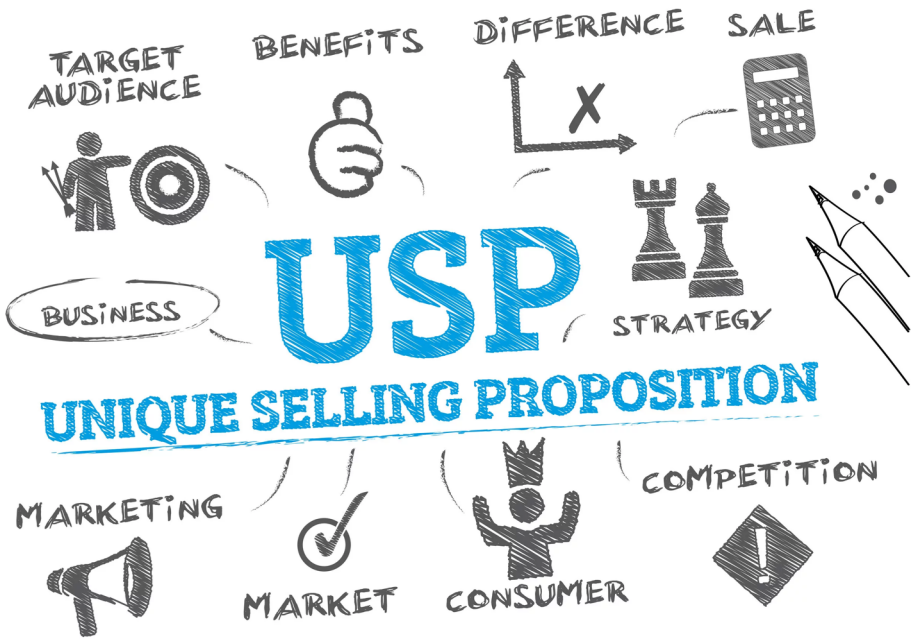
Unique Selling Proposition

Security can be a hard sell

- because it adds cost
- because our "clients" see our programs as adding inconvenience or cumbersome steps in business processes

Show the real value of Information Security

- provide services that allow the enterprise to meet business risk with its eyes wide open. Its value is in managing risk
- solid evidence that your security programs are contributing to the organization's productivity, its competitiveness and ultimately its bottom line
- demonstrate a direct contribution to the revenue stream and profit margin of the company



Executive Sponsorship

Do a quick determination of commitment of executives:

- **Committed or Involved?**
  Investment in resources?
  Willingness to hold people responsible?
- **Direction will be guided by the answer**

Make it or Break it

1. Change of management
2. Breach Detection
3. Audit / New Findings
4. Mergers & Acquisitions
5. Maturity Shift
6. Large Scale project(s)
7. Tech Replacement
8. Management briefing

Speak the language of business

1. Risk
2. Revenue
3. Employee efficiency
4. Strategic value
5. Cost
6. Customer satisfaction

Panagiotis Kalantzis

Information/Cyber Security & Data Privacy Expert

p.kalantzis@phiconsultancy.eu

+30 6980 335566 I +30 6987 323414

http://www.linkedin.com/in/pkalantzis