

Information Security Strategy

Dr. Noam Weinblatt
2Bsecure



Overview



- > Is your organization going in right directions in terms of Cyber security?
- > Are you investing in right or wrong security domains (security technologies, processes and controls)?
- > Do you have a cyber security agenda?
- > Are you navigating according to a work plan for cyber security, or are you reacting only?

Do you implement reactive or proactive security?

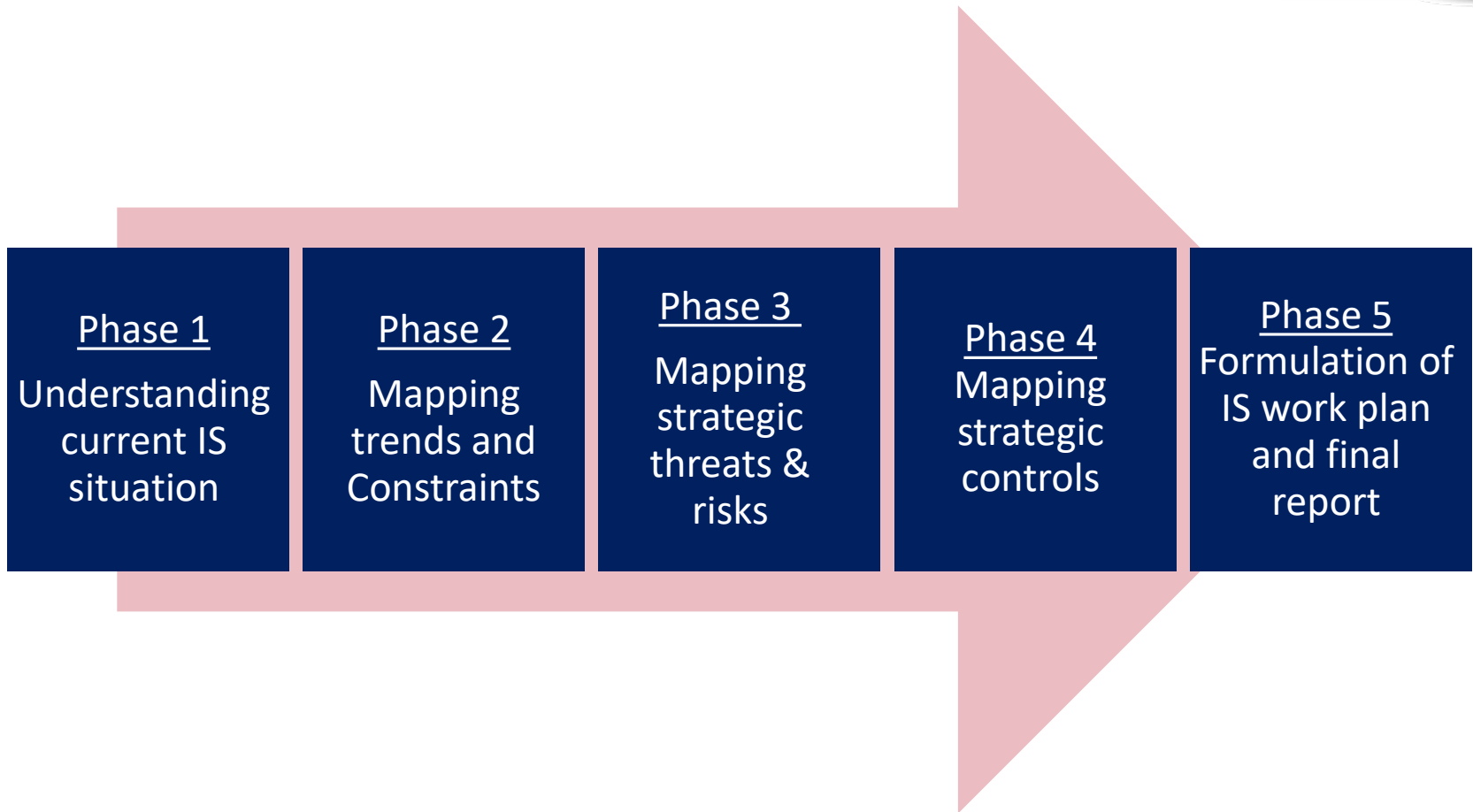


Overview



- > In cyber security, it pays to look ahead!
- > Large organizations today realize that periodical security testing or dealing with pinpointed Information Security incidents is neither the most professional nor the most cost-efficient way of dealing with Information Security.
- > An Information Security Strategy is a multi-year plan to mitigate strategic risks while complying with legal and statutory requirements, as well as the company's business and technological strategy!

2Bsecure's Strategy Project



Phase 1

Understanding current IS situation

Phase 2

Mapping trends and Constraints

Phase 3

Mapping strategic threats & risks

Phase 4

Mapping strategic controls

Phase 5

Formulation of IS work plan and final report

1) Current Security Situation














- > Identifying current capabilities (strengths and weaknesses) in various security domains
- > Based on known security standards (e.g., ISO 27001, or NIST)
 - > Risk management
 - > Security policies and procedures
 - > Organizational security
 - > Security awareness
 - > Asset management & classification
 - > BYOD protection
 - > User & authorization management
 - > Cryptography
 - > Physical and environmental security
 - > Malware protection
 - > Data leakage protection
 - > Security monitoring
 - > Network segmentation
 - > Perimeter security
 - > Application security
 - > Third party & Cloud security
 - > Cyber Incident response
 - > BCP
 - > compliance



1) Current Security Situation

> For each component we provide *Industry review/benchmark compared to peers*:

Topic	Peers	Poor	-	-	Excellent
Data leakage Prevention	   				
Security Monitoring	   				

Industry Variability 

Focal Organization 

2) Mapping Trends & Constraints



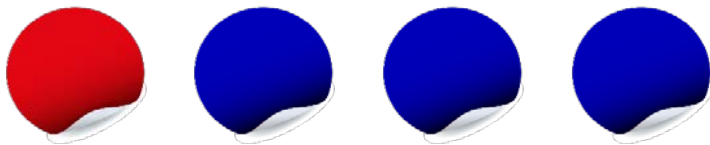
- > Mapping of trends and constraints that should be considered in the information security strategic road map. These include:
 - > **Business directions** of the organization
 - > **Technological directions**
 - > Information **security trends** that are expected to influence the information security field in coming years.



3) Mapping Strategic Risks



- > Identify top strategic risks/strategic vulnerabilities. For example:
 - Weak security monitoring capabilities
 - Weak control on third parties
 - Weak segmentation in network
 - Weak protections against advanced cyber threats (e.g., ransomware, APT)
- > *Methodology: workshop with senior information security, IT, and business representatives.*



4) Strategic Controls



Mapping of strategic controls that are most attractive in terms of:

- a. Strategic risk mitigation
- b. Estimated costs
- c. Implementation complexity
- d. Implementation time

	Strategic Information Security Risks					Aggregated Risk Mitigation		Implementation Time		Complexity	Annual Cost Estimation		Final Prioritization
	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Score	Value	Months	Value	Value	Comments	Cost (US\$)	
Risk weights	1	1	2	1	3								
Security awareness - phishing awareness software for employees	2	2	0	1	0	5	L	≤3	H	L	7 \$ per employee per year (quarterly training for each employee).	50,000	H
Implement secure file transfer: Secure channels for file transfer (e.g., Safe-T, Cyberark)	3	0	0	1	0	4	L	3-6	M	M	Costs for solution and implementation	150,000	M
Implement a WAF	1	0	0	0	3	10	M	≤3	H	M	Solution- 60,000\$ Implementation- 40,000\$	100,000	H













5) Final Report & IS Work Plan



- > **Final strategy report** – a comprehensive report describing all strategy activities.
- > **Multi-year work plan for Information security** - The work plan will be presented in an Excel.
- > **Presentation of security strategy to management**

5) Final Report & IS Work Plan



Topic	Peers	Poor	-	-	Excellent
Data leakage Prevention	   				 
Security Monitoring	   				

Industry Variability 

Focal organization - beginning of Project 

Focal organization - after completion of strategic plan 

Summary



- > Organizations find high value in strategic work.
- > Strategy helps increase management commitment and involvement in cyber security.
- > Security benchmark is a strong tool for managers to better understand their relative professional position, compared to peers.
- > Excellent decision making support tool (decisions not taken based on “gut feeling”).

Thank You!

Dr. Noam Weinblatt

noamwei@2bsecure.co.il

+972-3-6492007

