

Methodology and Implementation Strategy for the Israeli Market

Aviram Atzaba
Executive Director
Strategy & International Cooperation
Israel National Cyber Directorate
atzaba@cyber.gov.il



סייבר ישראל
מערך הסייבר הלאומי

INCD Mission

Defense

Ensure a safe and durable cyber sphere



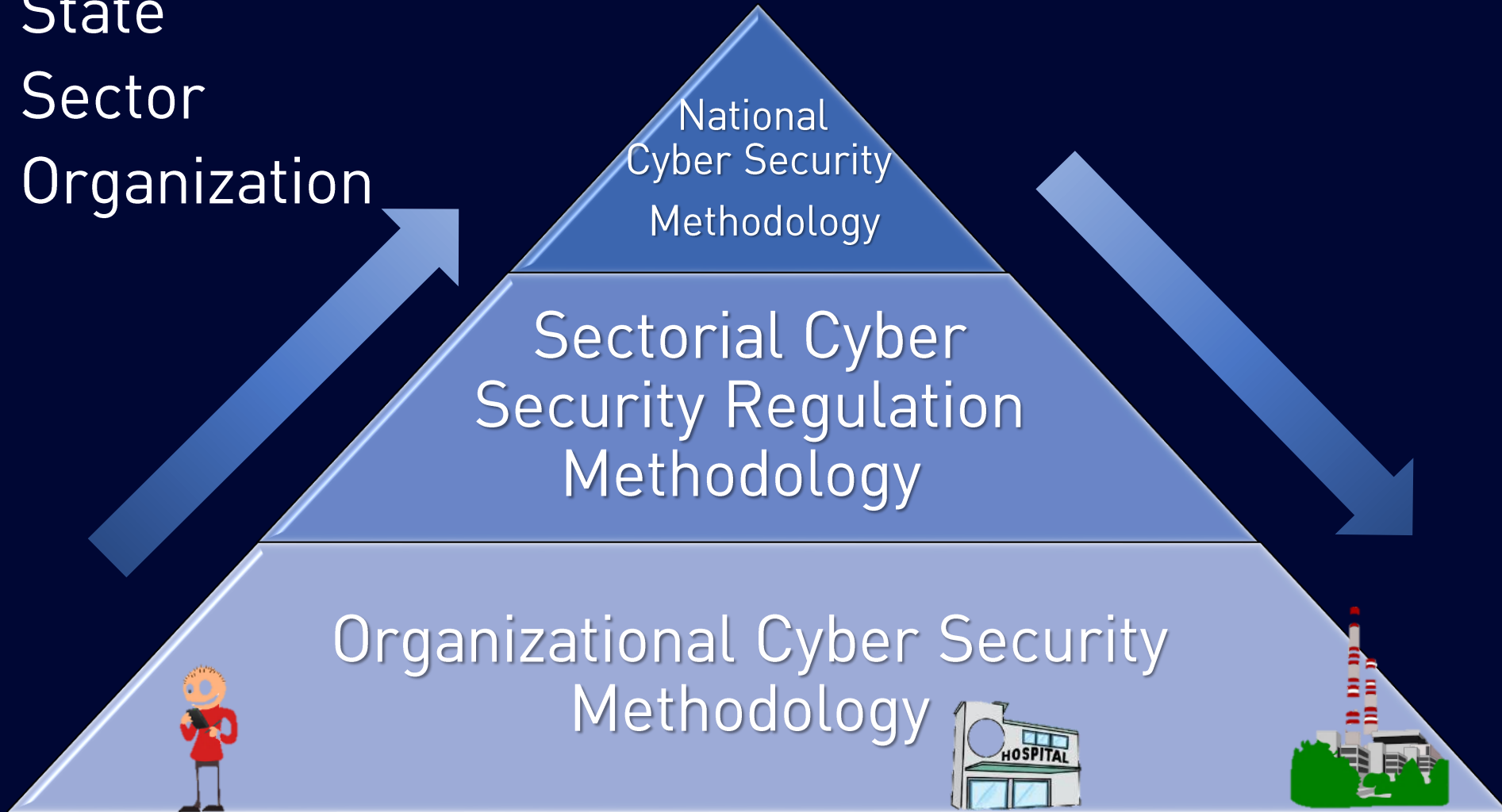
Leadership

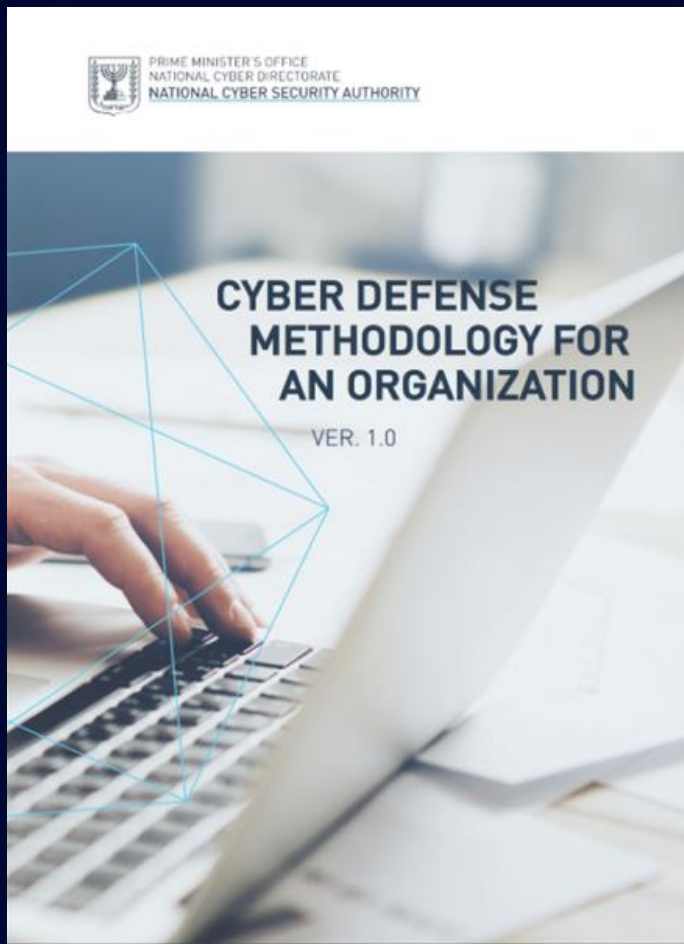
Promote Israel posture as a Cyber world leader



Market Cyber Security Framework

- State
- Sector
- Organization





Cyber Defense Methodology for an organization 1.0

2017



סייבר ישראל
מערך הסייבר הלאומי

מערך הסייבר הלאומי

4

Recent Attacks



Shirbit hack serves as a wakeup call to every financial company

What's next for Shirbit and the insurance sector after company released client data
Irit Avissar and

PAY2KEY

HELLO [REDACTED] USERS!

Congratulations!
Your entire network and all your informations such as computers/ employees information/ users folders/ servers/ file-servers/ applications/ databases/etc... in your network has been successfully encrypted!
Some of your important information dumped and ready to leak, in case we can't make a good deal!
Don't modify encrypted files or you can damage them and decryption will be impossible!
Don't try unofficial decryptors to recover your files or you can damage them and decryption will be impossible!
There is only ONE possible way to get back your files! Pay and contact to receive your special decryptor!
You should pay 7 BTC to receive official decryptor and easily recover your files. [REDACTED] special decryptor is now ready and waiting for your payment, let's do it!
You can send 4 random files from any computers and receive decrypted data, just as a proof that works!
Your UserID IS: [REDACTED]
Your Network ID [REDACTED]
| NOTICE |
Offer available until 11/08/2020. If you do not pay on time, price will be doubled!
Wallet: [REDACTED]

Cyber attacks again hit Israel's water system, shutting agricultural pumps

Incident follows more serious April attack attributed to Iran that officials said could have poisoned hundreds with chlorine

By TOI STAFF

17 July 2020, 1:18 am | 5



1,425 shares



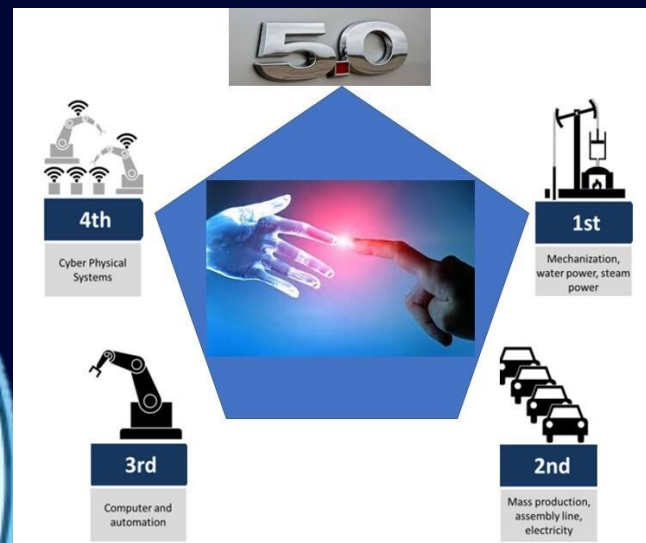
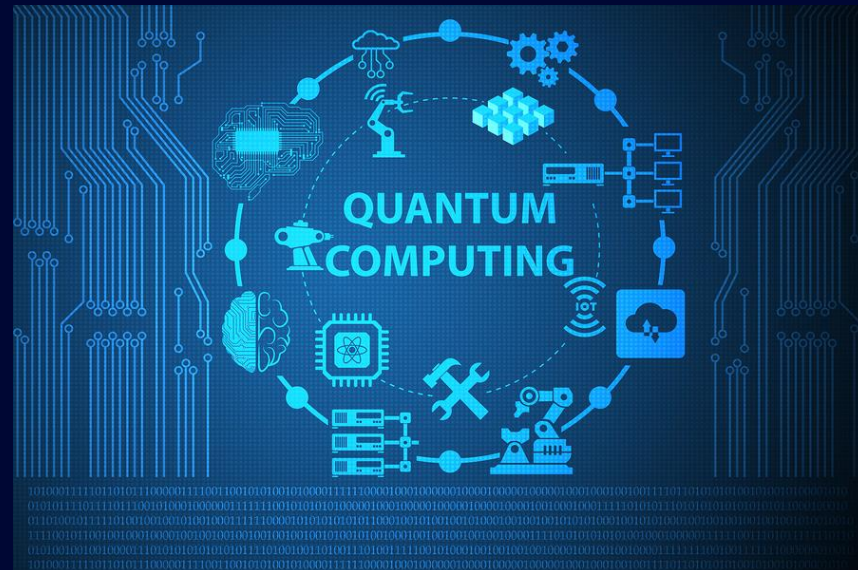
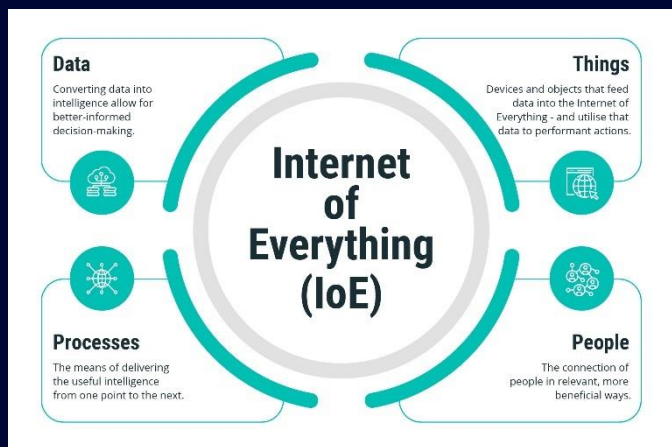
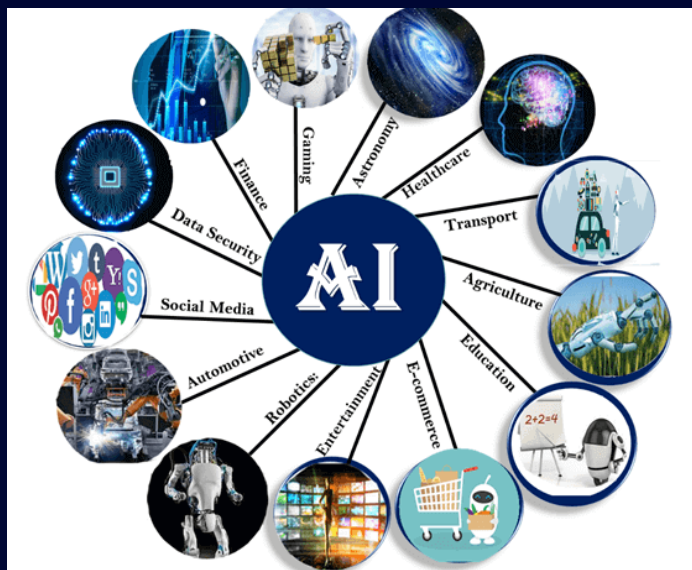
סייבר ישראל

מערך הסייבר הלאומי

מערך הסייבר הלאומי

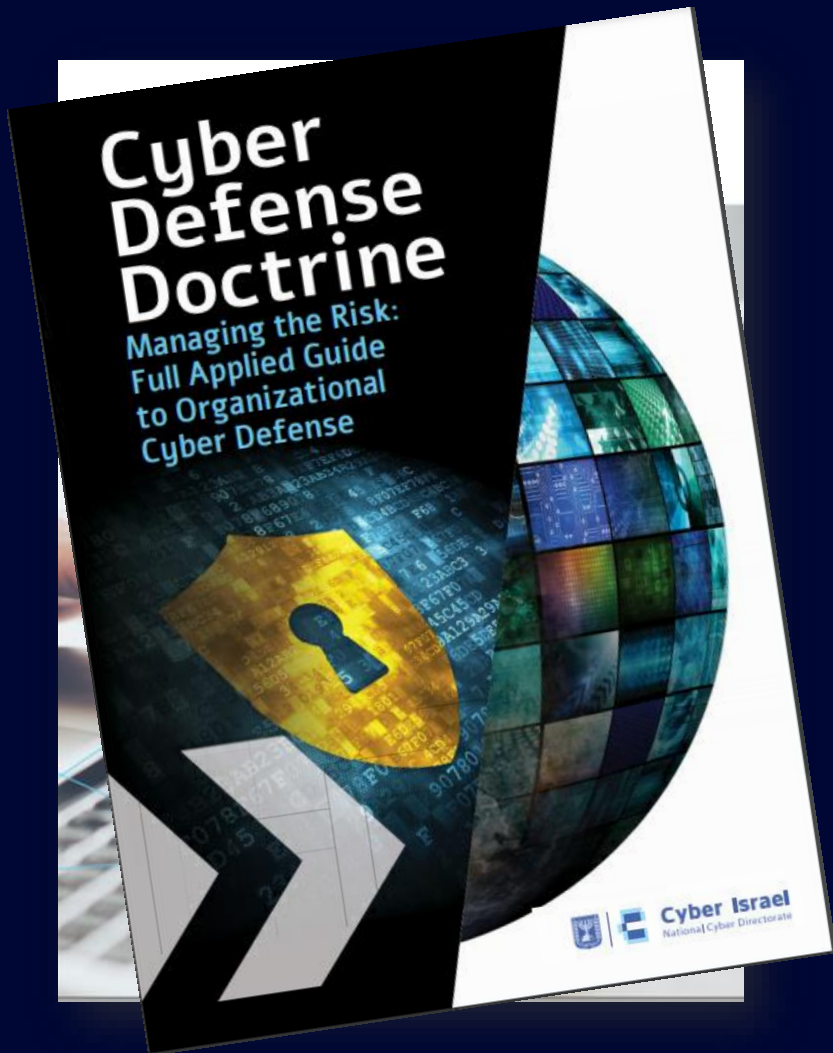
5

Winter is coming



סייבר ישראל
מערך הסייבר הלאומי

מערך הסייבר הלאומי



Cyber Defense Doctrine for an organization 2.0

2021



סייבר ישראל
מערך הסייבר הלאומי

מערך הסייבר הלאומי

7



El secreto de una
obra es 10% de
inspiracion y 90% de
transpiracion.

Mario Vargas Llosa



סייבר ישראל
מערך הסייבר הלאומי

מערך הסייבר הלאומי

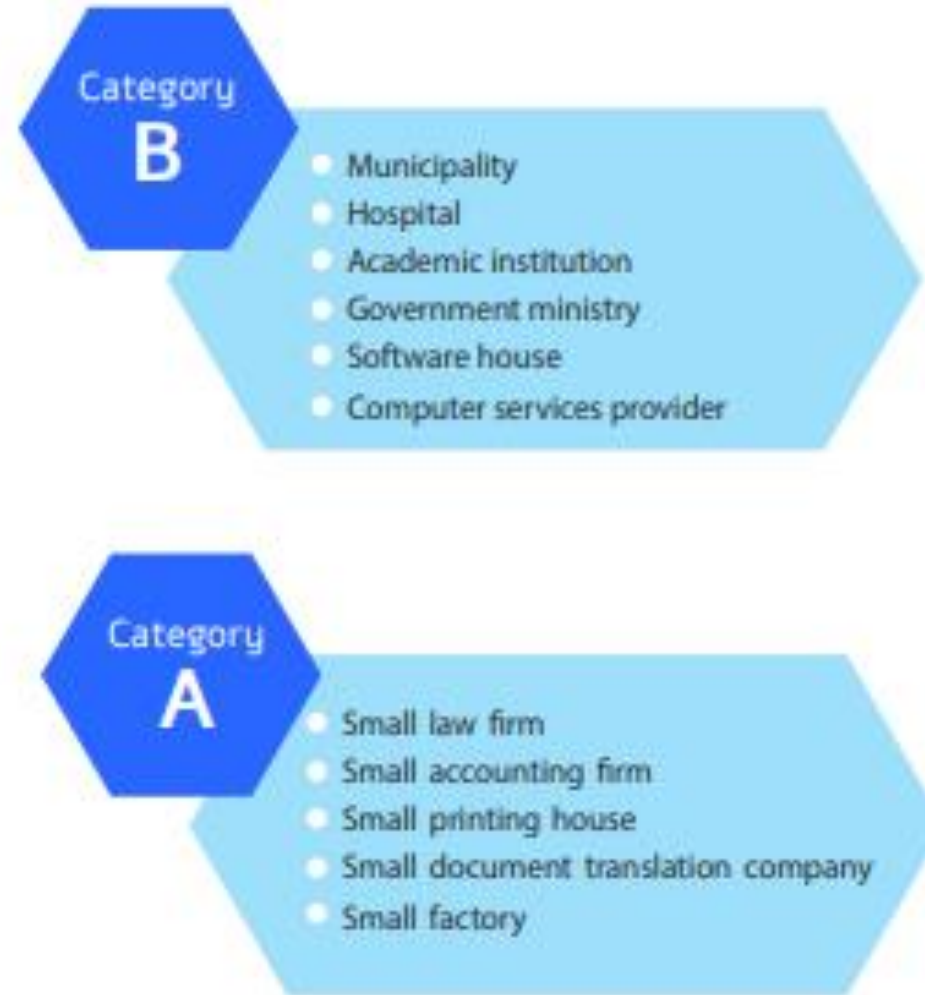
8

Organization Defense 2.0 - Principles

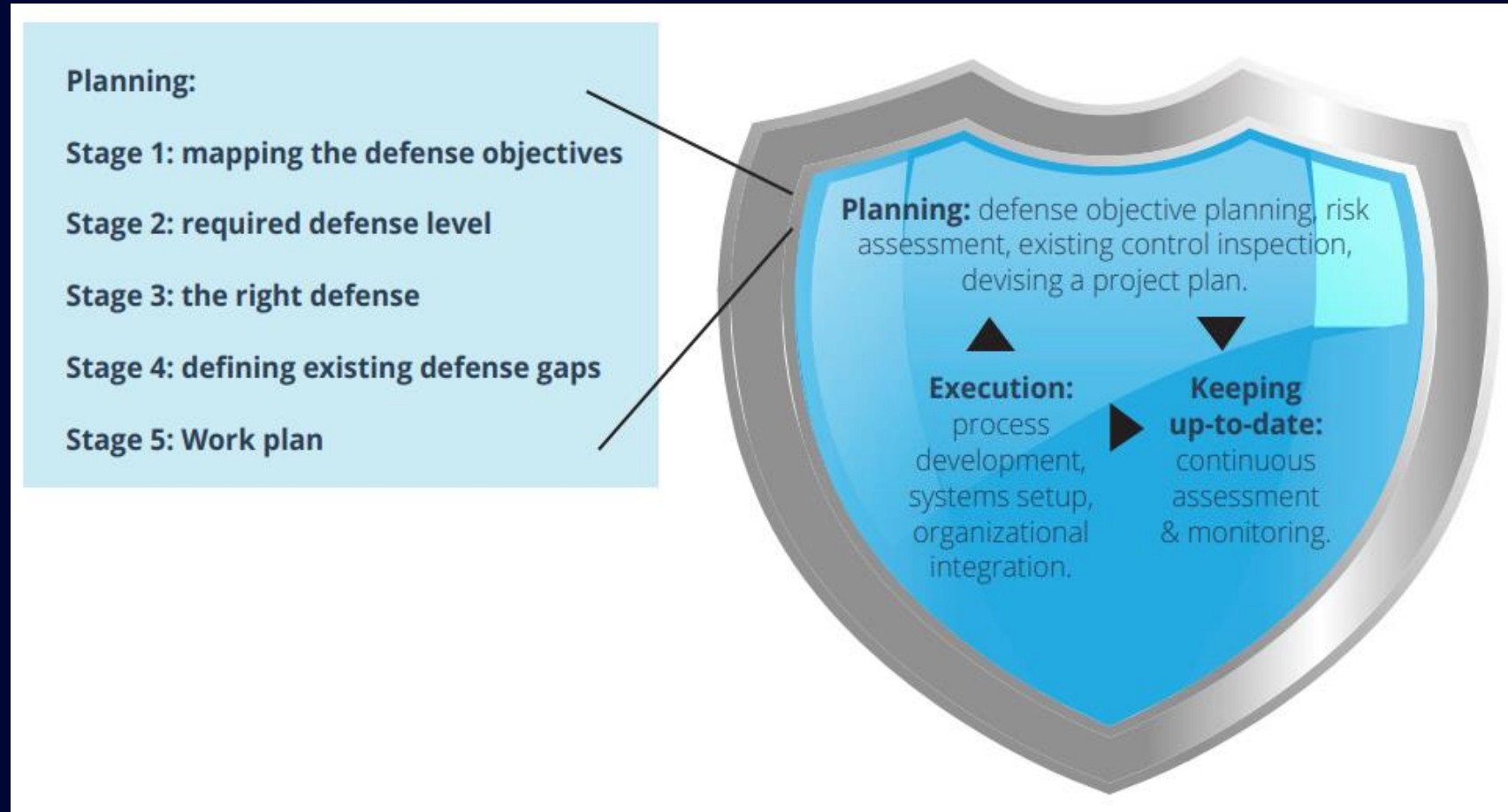
- Management's Responsibility.
- Defense from the Adversary's View.
- A defense based on Israeli knowledge and experience.
- Defense in accordance with the potential damage.
- Defense based on depth of implementation.



Structure

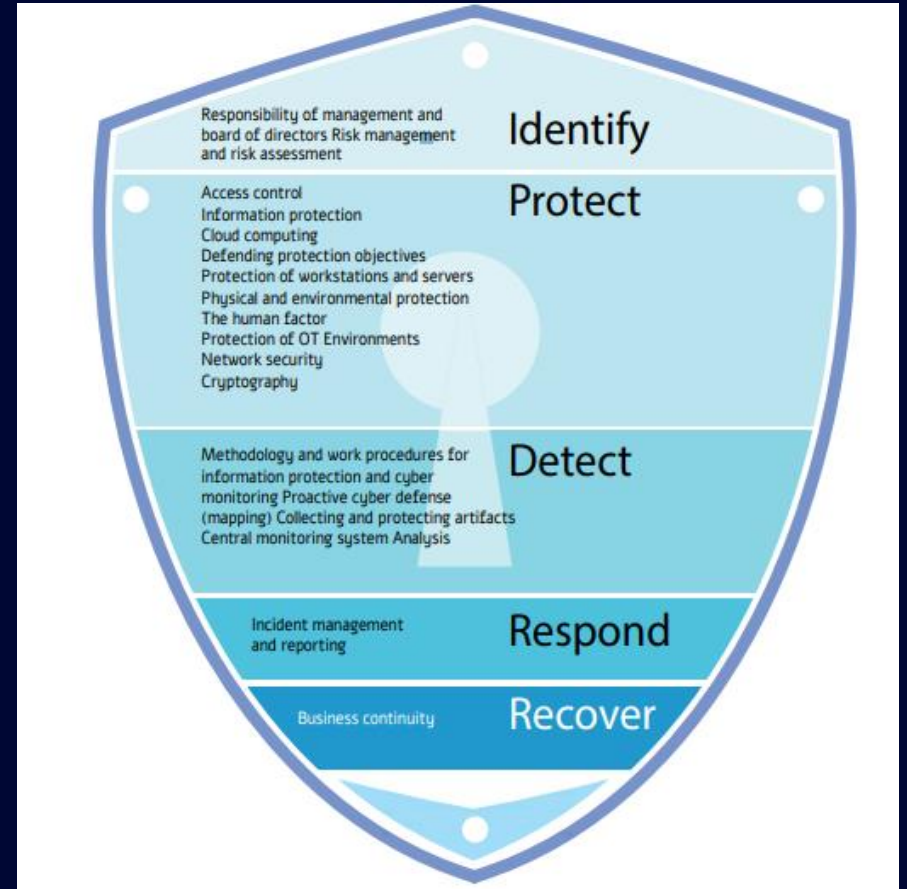


Organization Defense - Planning



Organization Defense – Control Families

- **NIST Framework**
- Tailored Control Families
- Specific controls, based on best international and Israeli experience and knowledge.

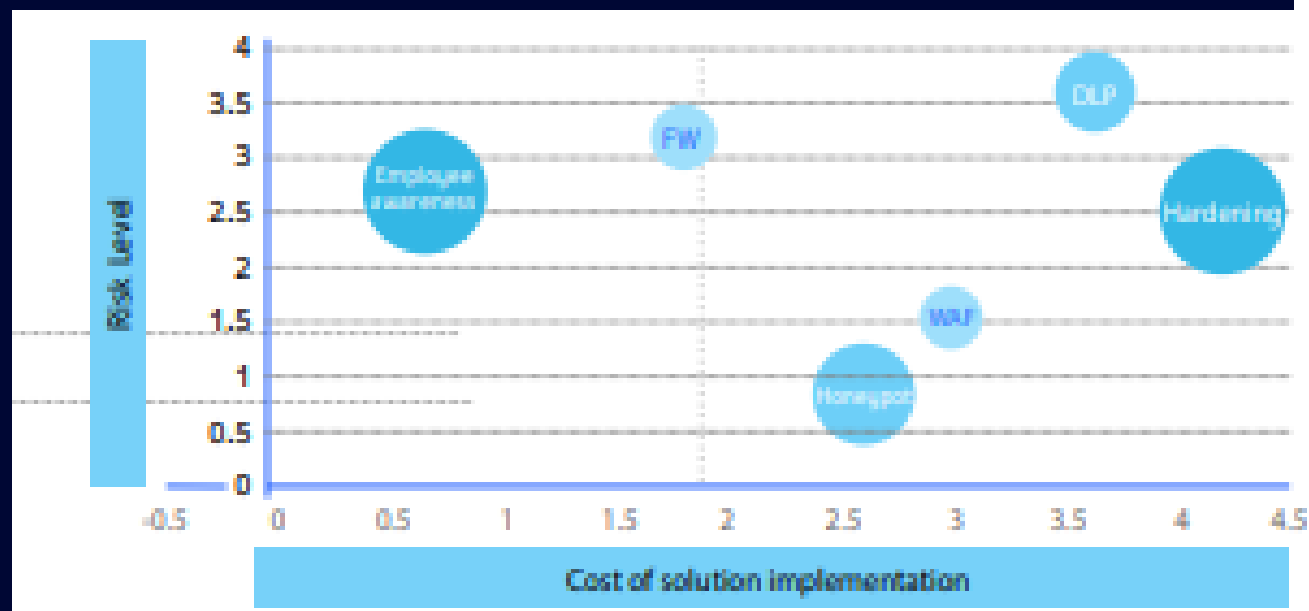


Organization Defense - Information Layers

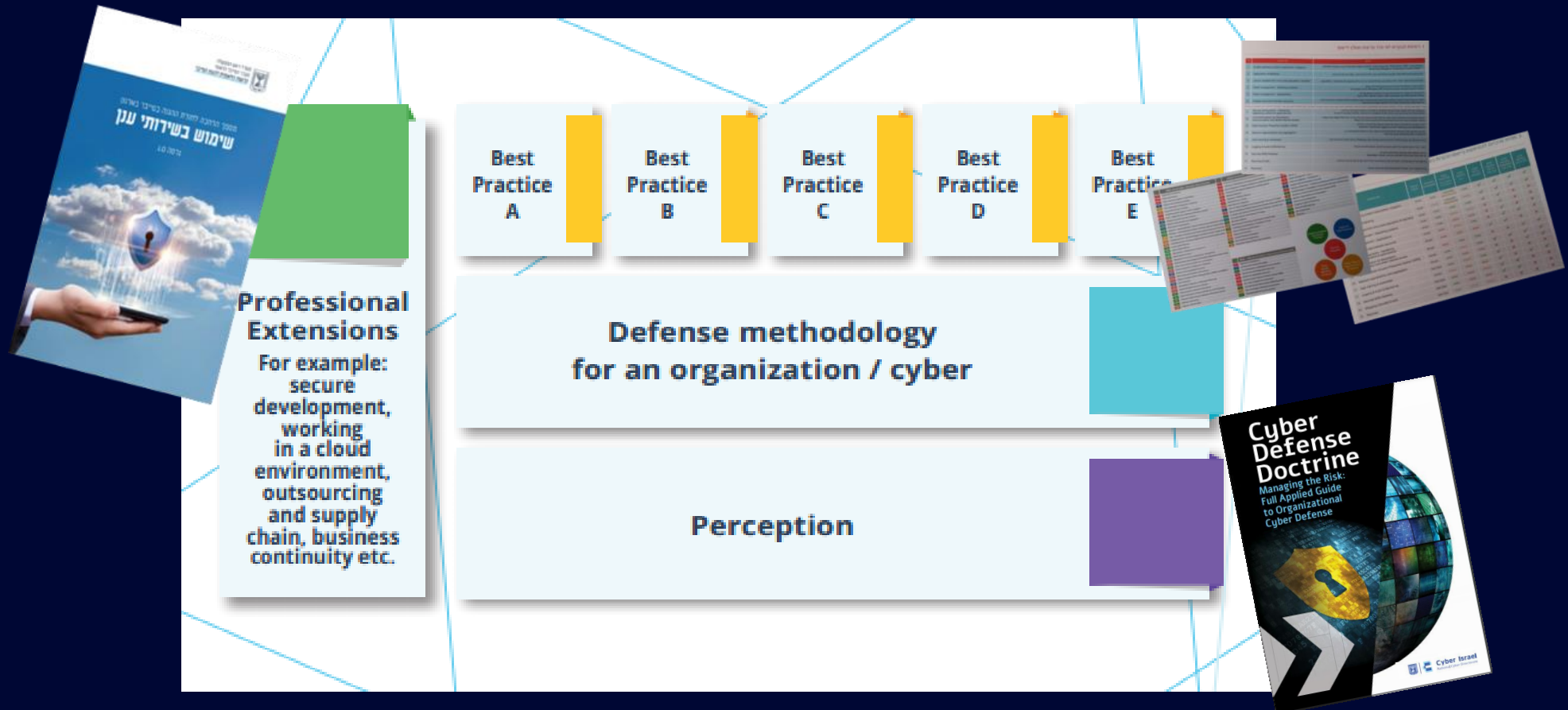
- **Multi-level Interpretations**
(C-Level Business Risk, CISO, IT).
- **Cyber Kill Chain** stage.
- **The level of risk** where the control should be applied
(Levels 1-4).
- **Link to INCD services**
(CERT, Guidance, Regulation, Intel etc...)



Organization Defense - Work Plan



Probability (P) / intensity (I)	4	3	2	1
4	16 System A	13	10 System C	7
3	15	12	9	6
2	14	11 System B System D	8	5 System E
	13	10	7	4



YUVAL Platform and certification scheme

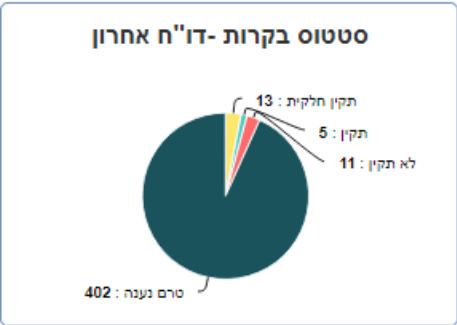
ת.ע.

פרויקט	תת פרויקט	סדר עדיפות מומלץ לטיפול
תהליכים ארגונים תומכים	Awareness Training Program	שלב א
אמצעי הגנה על עמדות קצה ושרתים	Hardening	שלב א
אמצעים להגנה על זכויות דיגיטליות	MFA	שלב א
תהליכים ארגונים תומכים	Human Resorces Information Security	שלב א
אמצעי ניסור ותגובה	Enable Logs	שלב א
ים בין רשתות	NGFW	שלב א
קה	Legal Aggrement (including SLA)	שלב א
ודירה	PT	שלב ב
ז על אחסון/עיבוד/שינוע מידע בארגון	Secure File Transfer	שלב ב
קה	INCD Supply Chain Compliance	שלב ב
י על אתר אינטרנט חיצוני	WAF	שלב ב
עסקית	Business Continuity Plan / Disaster Recovery Plan	שלב ג
יות דיגיטליות	IDM	שלב ג
י קצה ושרתים	MDM	שלב ג
קה	On Site Audit	שלב ג
	SIEM	שלב ג
ים בין רשתות	DLP Gateway	שלב ג

תאימות לתקנים

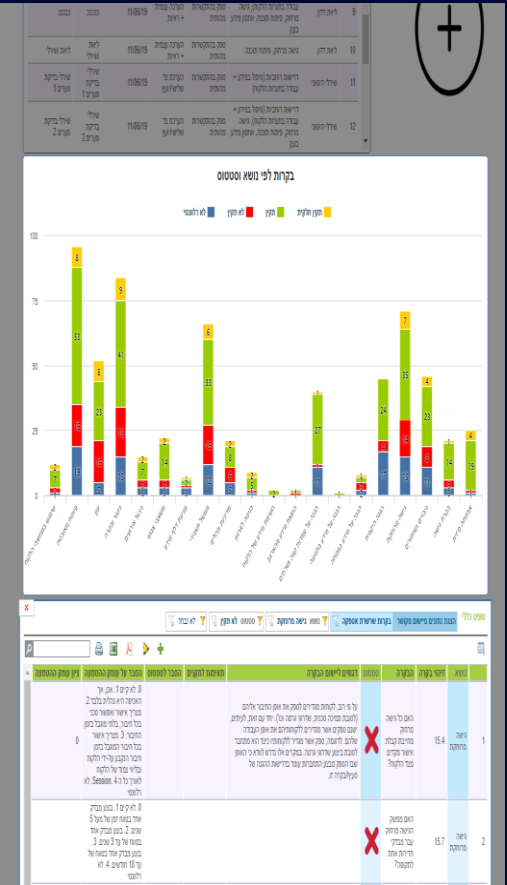
תורת ההגנה ב'

*פוטנציאל נזק מעל 500,000



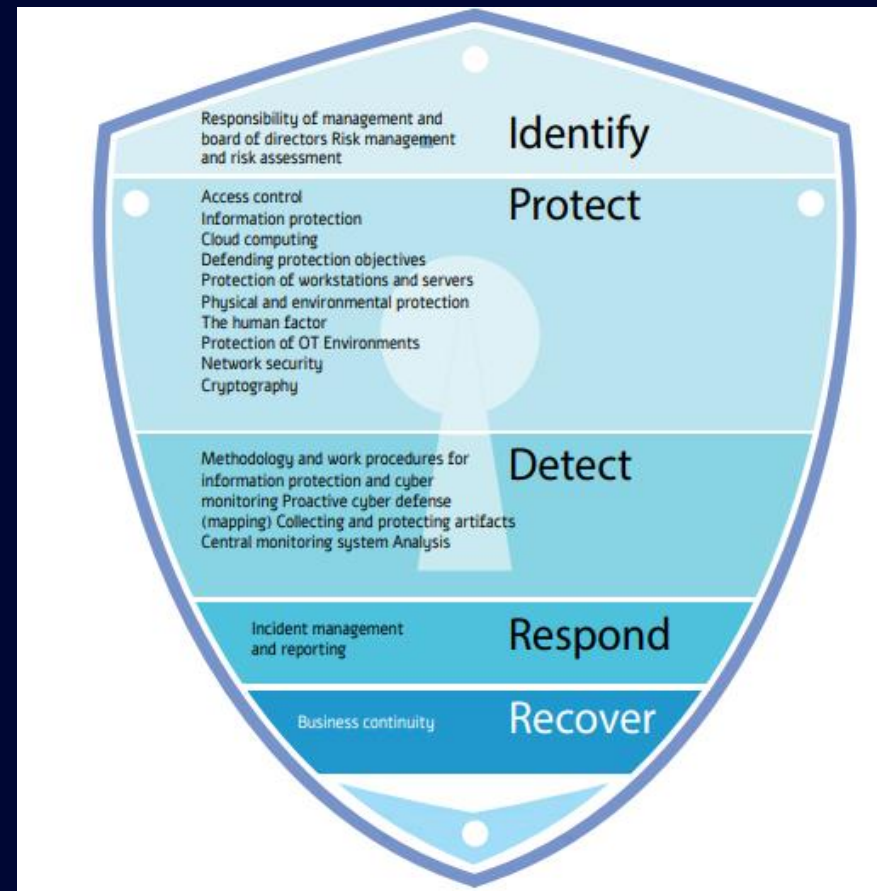
תורת ההגנה א'

יאל נזק מתחת 500,000



Why NIST CSF

- Common Language
 - Local
 - international
- Framework
 - Enables tailoring
 - Incorporated into methodology and regulation
- Balanced Focus
- Cybersecurity POV
 - Vs auditors POV



What's Next?

- International CSF-based certification
- NIST AI Framework
- Continuous BP and updates
 - In YUVAL system





Muchísimas gracias

Aviram Atzaba
Executive Director
Strategy & International Cooperation
Israel National Cyber Directorate
atzaba@cyber.gov.il



סייבר ישראל
מערך הסייבר הלאומי

מערך הסייבר הלאומי

19