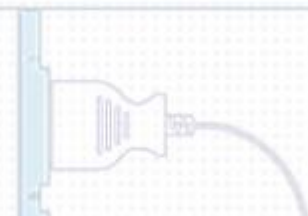# Cyber@Mekorot

Udi Roth – CISO, Mekorot Water Co.

Mekorot - Facts And Numbers

Supply 70%
Of all water

Supply 80%
Of drinking water

1,070
drillings

km12,000
of pipes

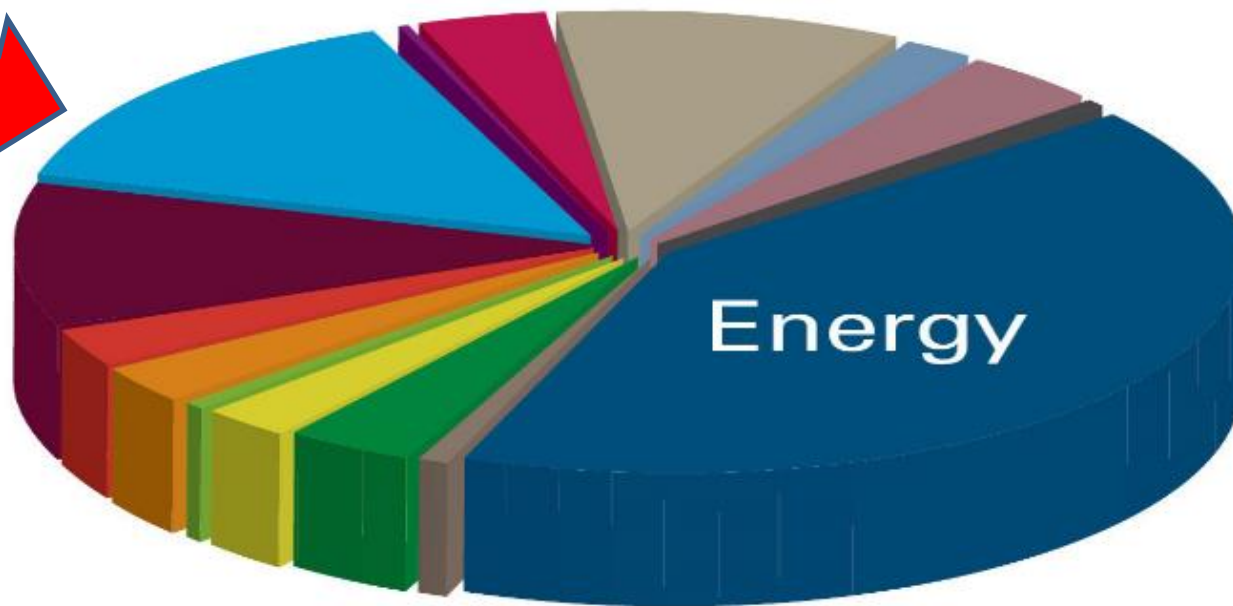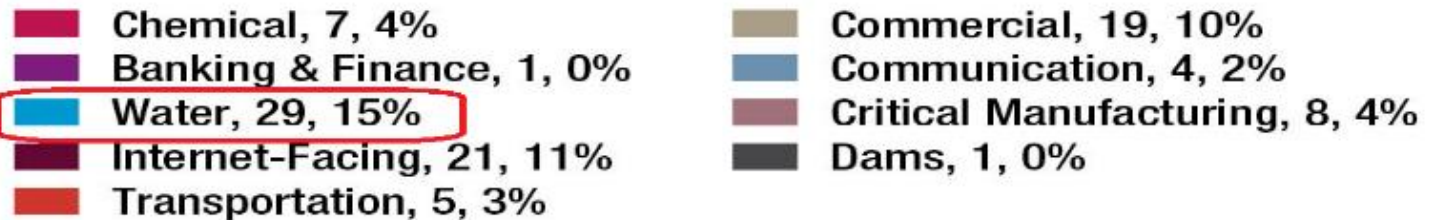**3,100**
Facilities
Nation wide

Property–
12.5 Bi NIS

2,200
employees

Cyber Attacks on OT BY SECTORE

Cyber Incidents by Sector

- Chemical, 7, 4%
- Banking & Finance, 1, 0%
- Water, 29, 15%
- Internet-Facing, 21, 11%
- Transportation, 5, 3%
- Commercial, 19, 10%
- Communication, 4, 2%
- Critical Manufacturing, 8, 4%
- Dams, 1, 0%

- Nuclear, 6, 3%
- IT, 1, 0%
- Health Care, 5, 2%
- Government, 7, 4%
- Food & Agriculture, 2, 1%
- Energy, 82, 41%

Image source: DHS Industrial Control Systems Cyber Emergency Response Team, ICS-CERT Monitor

HACKING Menu

ASK YOUR SERVER ABOUT OUR SPECIALS!

Hack Group

	Bitcoin	USD
Hacking Web Server (VPS or hosting)	0.43	$266.52
Setting up Keylogger	0.25	$154.95
Device Tracking (smartphone/PC)	0.32	$198.34
Hacking Personal Computer	0.23	$142.56
Spyware Creation	0.35	$216.93
Intelligence Report – Background Check	0.23	$142.56
Setting Up Your Own Botnet	0.93	$567.42
Logs from Zeus Malware, 10 GB (Stolen CCs, PayPal, Bank Accounts)	1.24	$768.56

Russia Hackers

	Bitcoin	USD
Custom Ransomware (CTB-Locker)	2	$1,239.62

The Real Deal (TOR eBay-clone)

	Bitcoin	USD
24 Hour DDoS	0.743	$460.52
Social Media Hacking, Per Account	0.104	$64.46
Apple Enterprise Certificate Private Key	14.8569	$9,208.46

Cell Phone Hacking/ Phreaking

	Bitcoin	USD
SS7 API Access (1 Month)	0.32	$200.00
SMS / Call Spoofing (1 Month)	0.03	$20.00

Rent-A-Hacker

	Bitcoin	USD
Small Jobs	0.35	$221.14
Medium-Large Jobs	0.89	$552.85

Prices of 06-2015

Who Are The Attackers?

The attacker

- Home attacker
- organized group
- Organization (terror or crime)
- **State**
- **Power**

The Motivation

- **Ego**
- **Reputation**
- **Blackmail**
- **Ideology**
- **Competition**
- **Strategy**
- **Money**

The Attack tools

- **Social Engineering**
- **Hardware Hide-in**
- **Deception**
- **Espionage**
- **Psychological Manip.**
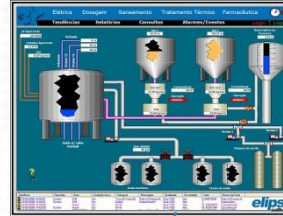- **Malware**
- **Software Attack Tools**

What do we protect?

12,000 Automatic Metering devices

3100 Facilities

9 Control Centers

2000 Users

1000 Servers

1500 users browsing the Internet

MEKOROT Israel National Water Co.

150 Tb Data

1000 Smartphones

500 Remote access users and service providers

Personal Data

Business Data

OT network Challenges

 Facilities are connected to the control centers
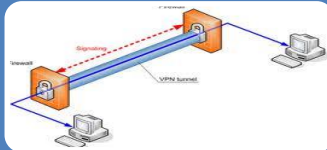
 Wireless Communication

 Employees using Laptops and cellular

 PLC's/RTU's in every site

 Data transfer to/from IT network

 Remote VIEW of HMI

IT network Challenges

Users browsing the web, downloading files

Laptops connected to other networks

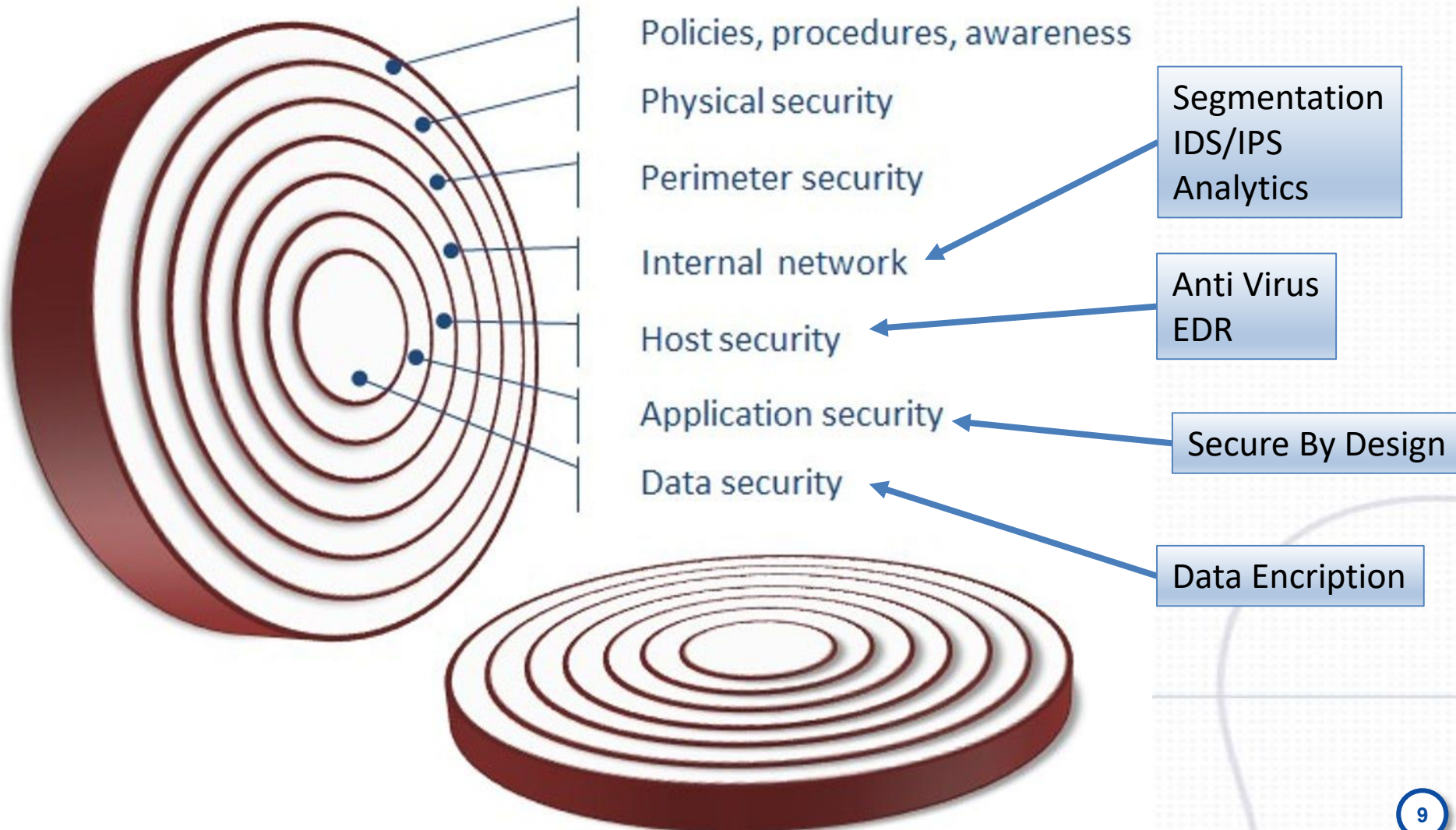Business Mobile Apps

Inbound DATA (D.O.K/DVD)
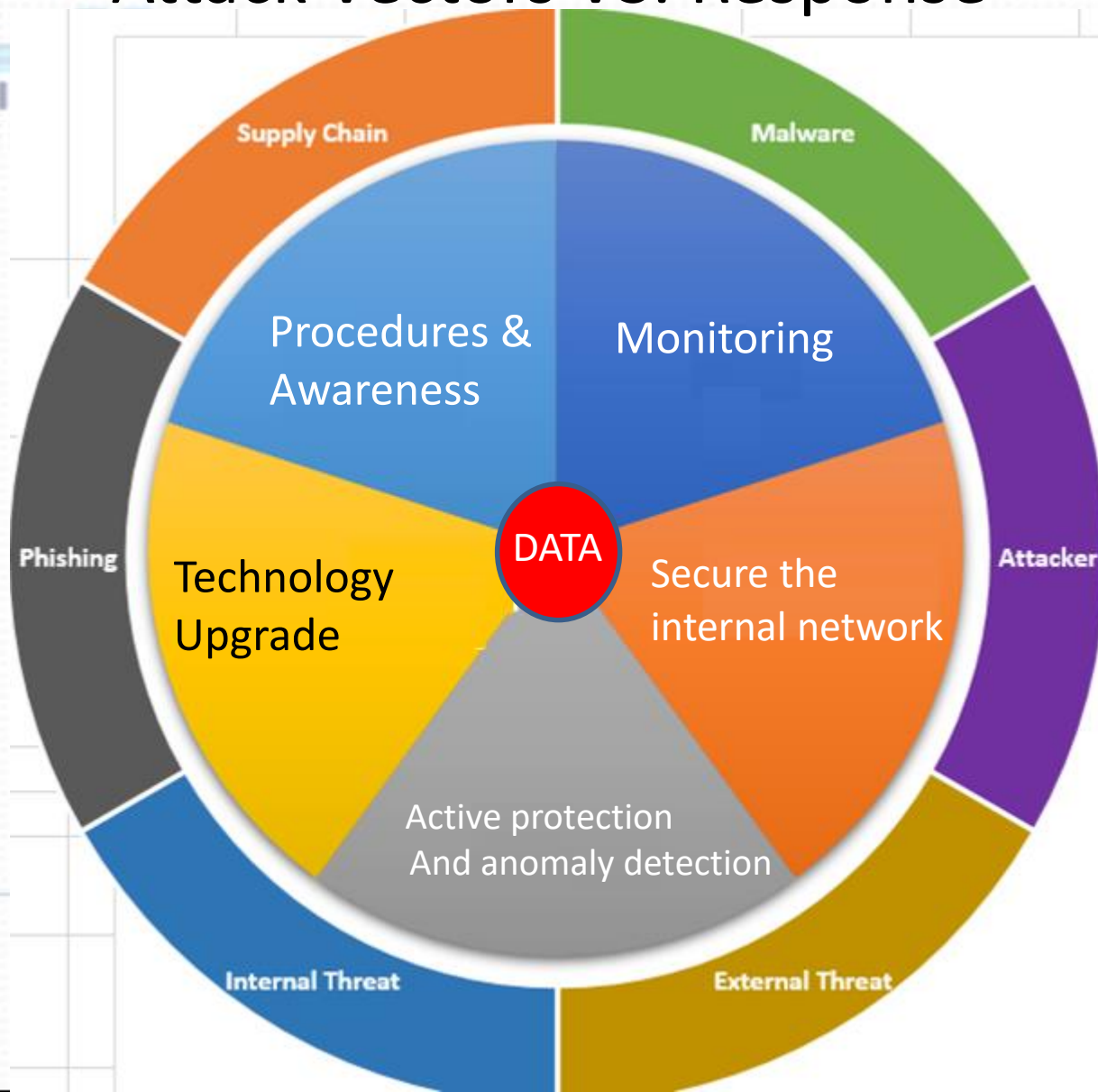
Remote Access by Service Providers

Cybersecurity is Like An Onion layers

Policies, procedures, awareness

Physical security

Perimeter security

Internal network

Host security

Application security

Data security

Segmentation
IDS/IPS
Analytics

Anti Virus
EDR

Secure By Design

Data Encription

9

Protecting the network
Attack Vectors VS. Response

Cyber Regulation on Mekorot

State of Israel

- Israel National Cyber Authority
- Ministry of Energy
- Water Authority
- Privacy Protection Authority
- Securities Authority
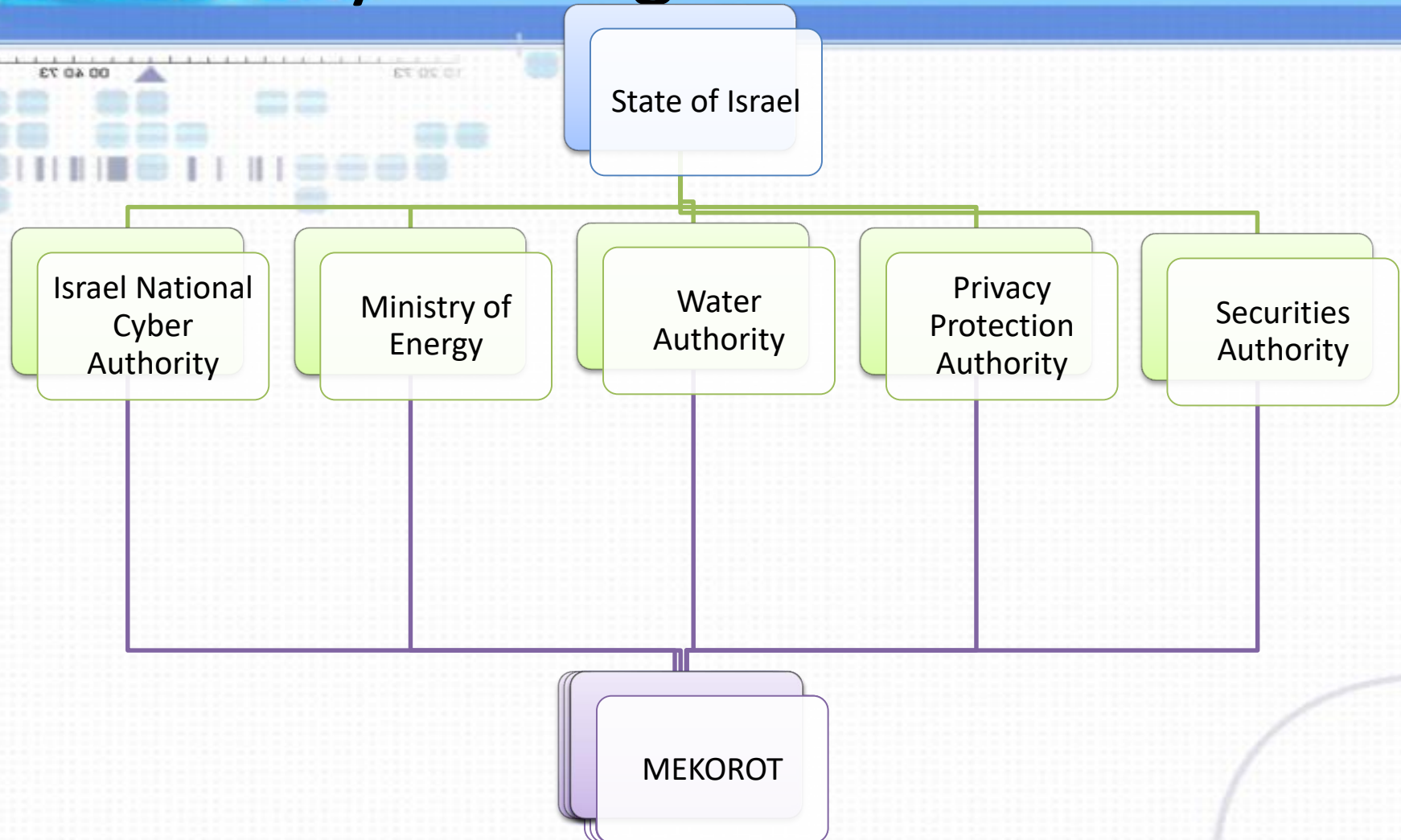
MEKOROT

More Regulations:
- Health And Water Quality
- Finance (SOX)
- Environment

Cyber Regulation on Mekorot
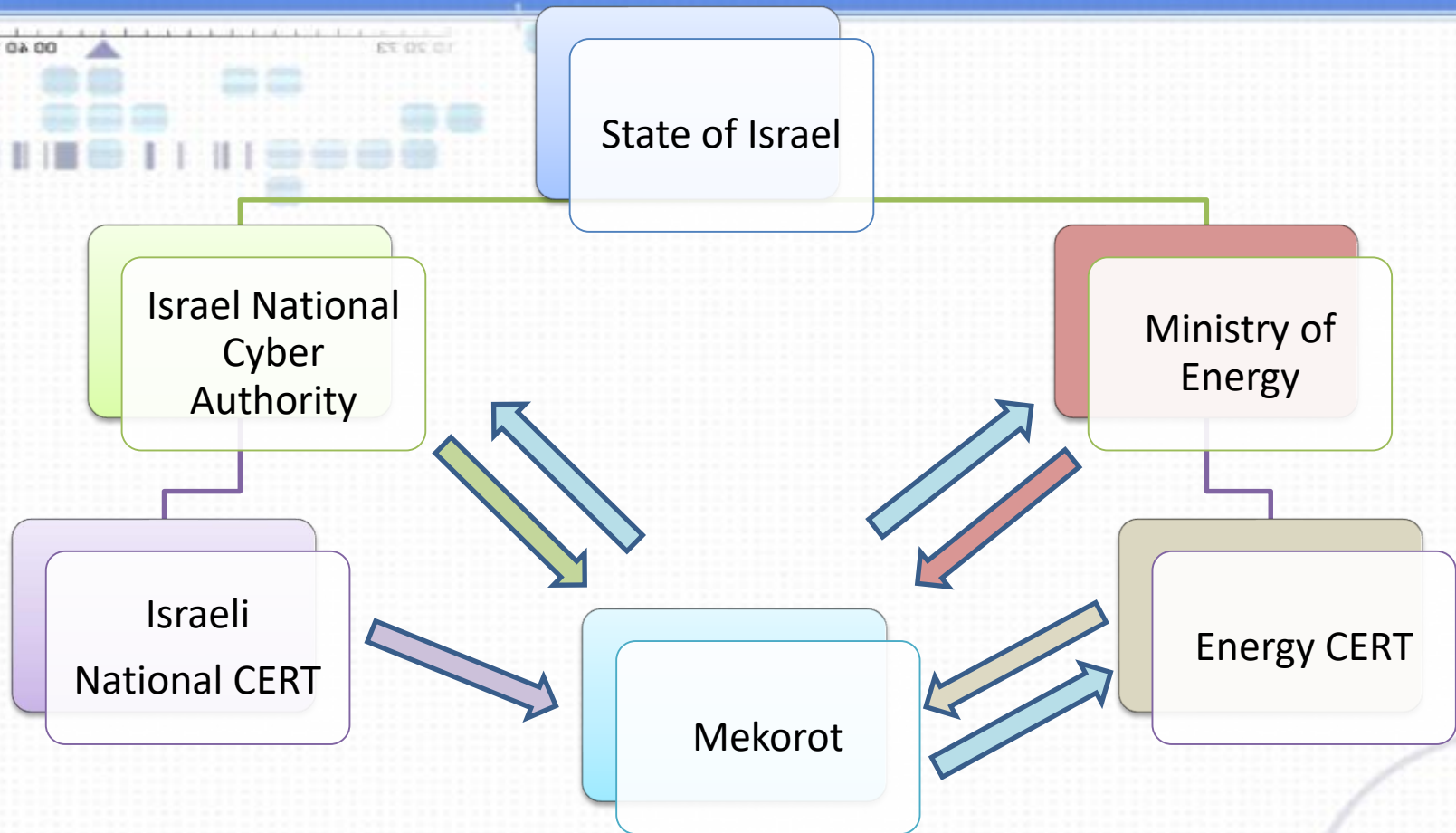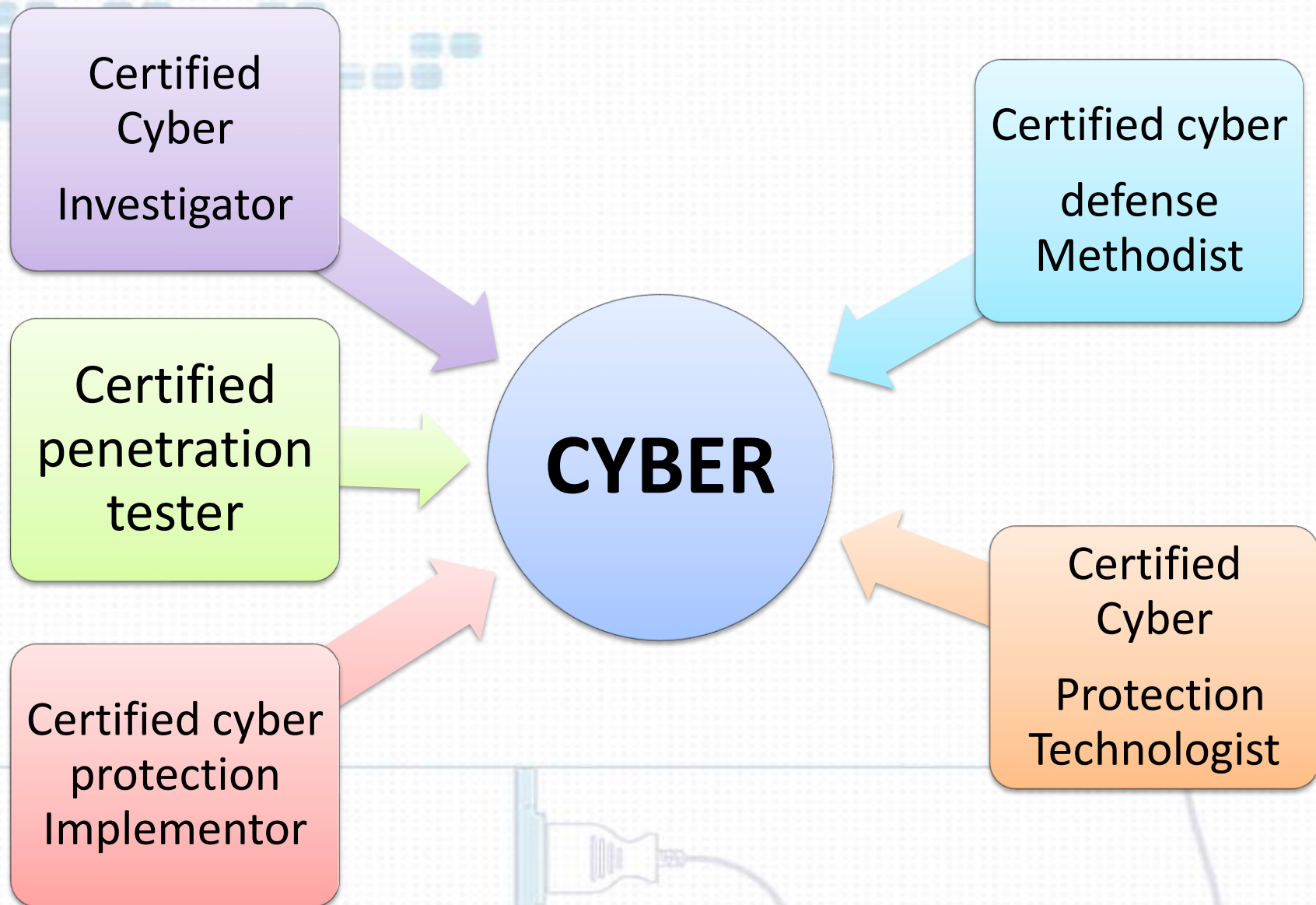
State of Israel

Israel National Cyber Authority

Ministry of Energy

Israeli National CERT

Mekorot

Energy CERT

NEW Regulation of cyber professions

Certified Cyber Investigator

Certified penetration tester

Certified cyber protection Implementor

CYBER

Certified cyber defense Methodist

Certified Cyber Protection Technologist

13

Regulation of cyber professions

- Each profession has two certification levels - a basic level and an advanced level
- The professions subjects to be regulated are:
  - Certified cyber protection Implementor - theoretical and hands-on.
  - Certified for penetration tester - high practical knowledge of weaknesses In cyber protection systems and intrusion testing
  - Certified Cyber Investigator - up-to-date and high practical knowledge of incident investigations (criminal)

  - Certified cyber defense Methodist - in-depth theoretical knowledge of a Cyber Defense Methodologies.
  - Certified Cyber Protection Technologist - A person with extensive theoretical knowledge and in-depth knowledge of the subject area of Cyber protection technologies.

Regulation of cyber professions

- Each profession has two certification levels
  a basic level and an advanced level

- Certification By An exam

- Qualification maintenance every 2-3 years

But .....
The Most Important thing in
our Bussiness IS !!!!!

Ehud (Udi) Roth

udi@mekorot.co.il

+972 50 72 400 58

Tel Aviv, Israel

Summery

- Cyber Security, Computer and software development expert with 35 years of experience in design and operate an enterprise Cyber security operation, secured communication networks ,secured data centers and Secured Software development.

Work experience

- CISO @ Mekorot Water Co. - 16 Years
- Network & infrastructure manager @ Mekorot Water Co. – 10 Years
- Application & System programming @ Mekorot Water Co. 9 Years.

Education

- Cissp, Cyber Security Certification
- BSc. , Computer Information technology
- Practical Engineer, Computer