The Israel Export
& International Cooperation Institute

ISRAEL CYBER ALLIANCE

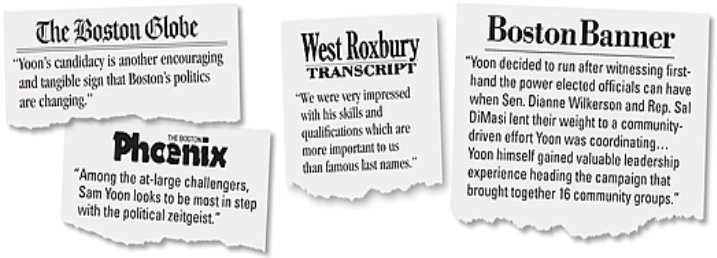
Rethink Challenge™

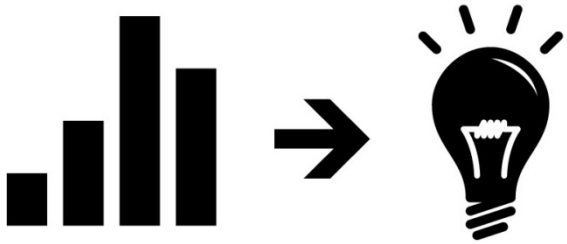
Where Are We Headed ?
Trends, insights and possible solutions for National Cyber Defense

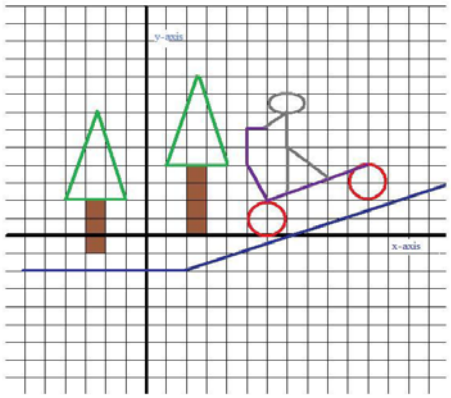
Presented by:
Zori Kor

2 February, 2017

Agenda


The Boston Globe
"Yoon's candidacy is another encouraging and tangible sign that Boston's politics are changing."
Phoenix
"Among the at-large challengers, Sam Yoon looks to be most in step with the political zeitgeist."
West Roxbury TRANSCRIPT
"We were very impressed with his skills and qualifications which are more important to us than famous last names."
Boston Banner
"Yoon decided to run after witnessing first-hand the power elected officials can have when Sen. Dianne Wilkerson and Rep. Sal DiMasi lent their weight to a community-driven effort Yoon was coordinating… Yoon himself gained valuable leadership experience heading the campaign that brought together 16 community groups."




y-axis
x-axis


Energy, Water, Communication…

Australia - Maroochy Shire Attack (April 2000)

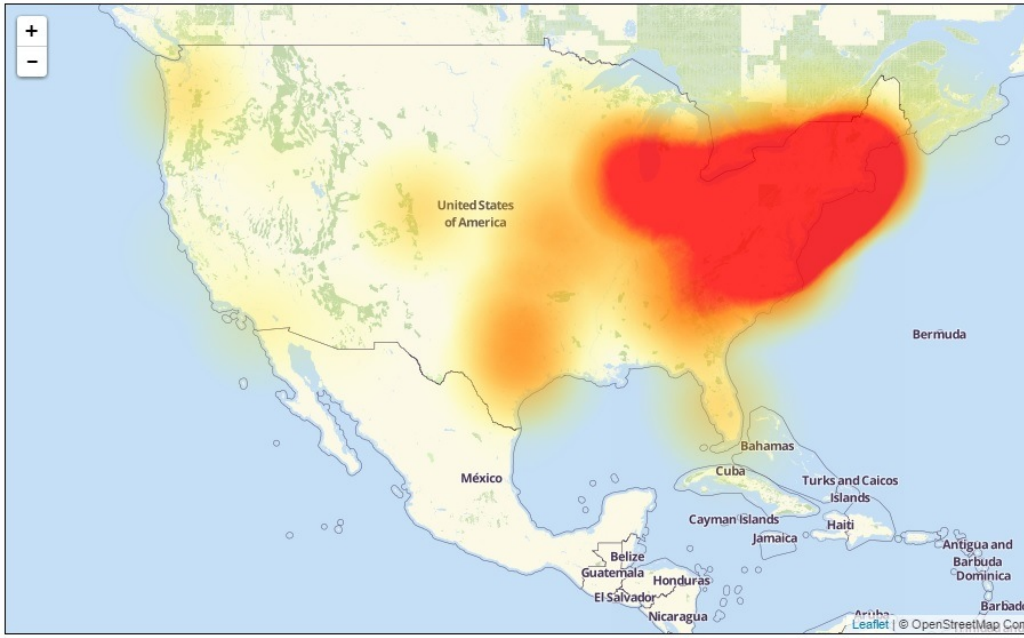
- On several occasions Boden used radio equipment to issue radio commands to sewage equipment in use.

- 800,000 liters of raw sewage to leaked into parks, rivers and the nearby Hyatt Regency hotel.

DDoS Attack on DNS provider Dyn

Background

- On Friday October 21, 2016, a large DDoS attacked DNS servers infrastructure in the Eastern United States resulting in outages on popular websites like Twitter, Spotify, Amazon, Reddit, Yelp, Netflix, The New York Times, among others.



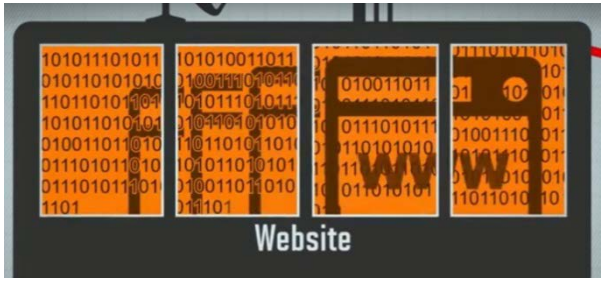
- **This DDoS was the biggest cyber attack the world has ever seen.**

How Did It Happen?

Hackers assembled a botnet army of ordinary internet-enabled devices using publicly available source code, Mirai malware.

Hackers are then able to direct those devices to send massive waves of junk requests to a DNS provider.

The DNS provider could not carry out its job of acting as a switchboard for the internet and consumers could no longer reach popular websites.



amazon

reddit

NETFLIX

Spotify

Russian Banks Targeted in DDoS Attack

Background

- In November 2016, at least five Russian banks were targeted as part of an attack powered by compromised IoT devices, including state-owned Sberbank.
- More than a half of the IoT botnet devices were situated in India, Taiwan, and other countries.
- To gain control over the devices, the hackers took advantage of smart devices that use easy to guess passwords.

Why are these attacks so dangerous?

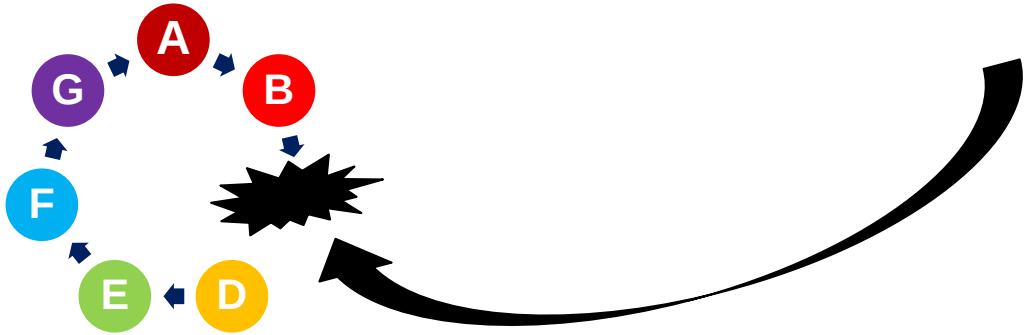
- The compromised devices, which make up the bot-net army, are still out there and unpatched, which means that we can expect additional attacks.
- Hackers can use the DDoS as a diversion to break into other databases or accounts and access private information.

Where do the cyber threats come from?

- Outside

- Inside

- Supply Chain



The National Challenge

- Which Infrastructures Are Critical?
- Which Components Are Critical in the Critical Infrastructures and other organizations?
- Education
- Protection, prevention, response, recovery

The Cyber Security Evolution in Isarel

1996: Right after P.M. Rabin assassination – Brainstorming: What else might go wrong?

2002: Israeli government resolution to promote cyber security of critical infrastructure. Establishment of NISA

2010-2012: P.M.'s Cyber initiative, establishment of the Israeli National Cyber Bureau.

2015: Establishment of the Israeli Cyber Security Authority.

Establish National Defence Strategy (The Israeli Experience)

- Broad cooperation: Gov-Private sector
  - Early warning,
  - Public-private collaboration
- “Soft” and guiding regulation (3-tier protection priority, detailed recommendations/instructions, education, audit mechanism, awareness and more)
- National and sectorial CERT

ISRAEL CYBER ALLIANCE

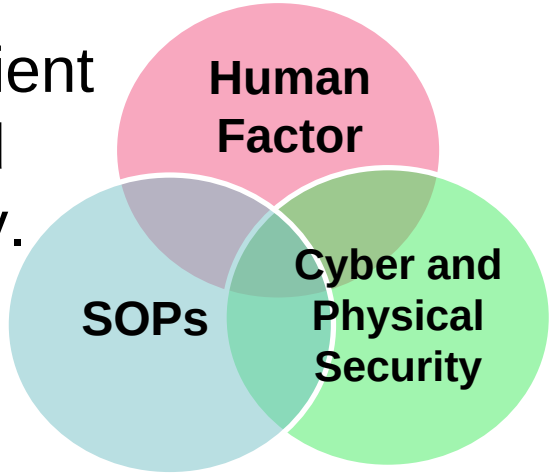
Rethink Challenge™

Public awareness

1. Cyber security is everybody’s business.
2. Campaign.
3. Talk about it

The Modern Approach

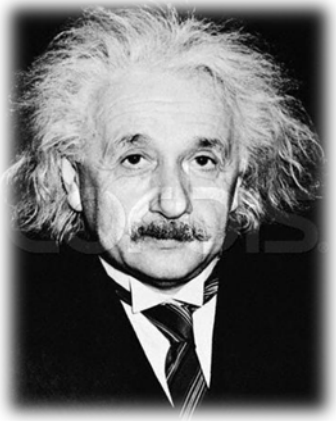
- Efficiently incorporating three components – SOPs, human factor training and technology.
- Threat-oriented with prioritization among threats.
- Holistic.
- Utilizes all available resources in an efficient manner – break up of individual silos and combines physical and IT/Cyber security.



The Solution Vectors

- Customer designed solutions
  (NO “one size fits all”).
- Implementation of IT/Cyber security measur
  Not “by the book” only!
- Awareness seminars, training sessions, education, knowledge transfer and specialized courses.

Formula



$$E = M * C^2$$

$$Cybersecurity = (Risk\ Assessment * Training)^{Audit}$$

Thank you

Zori Kor

zkor@asero.com