A Roadmap to Cyber Resilience

Why ?, How ?

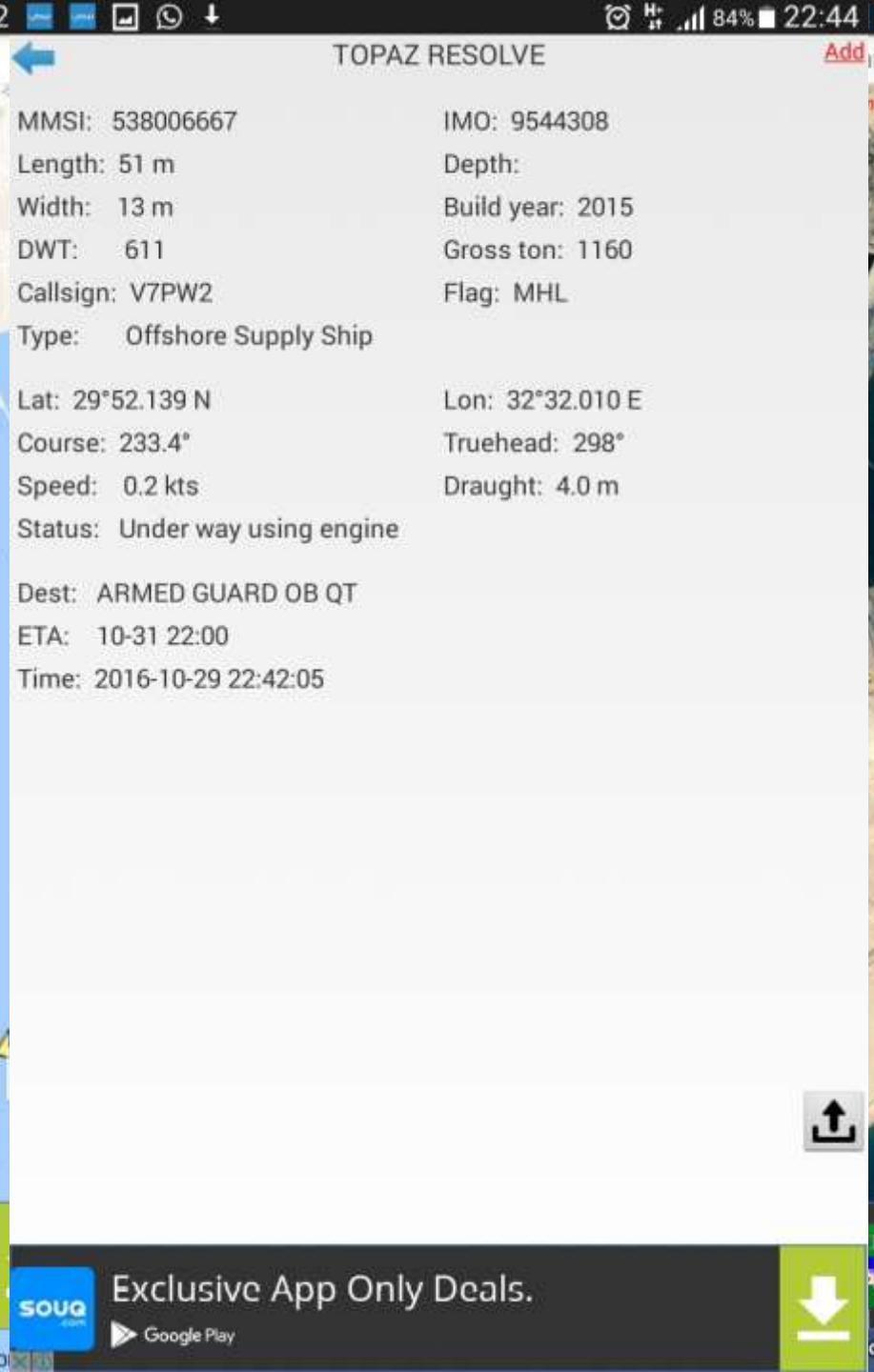
Dr. Emadeldin Helmy
Cyber Risk & Resilience – Bus. Continuity
Exec. Director, NTRA

The 5th Regional Cyber security Summit
27 October 2016 , Egypt

Agenda

- Why…?
- Threats
- Cyber war ….?
- Traditional security ?
- How…..?
- Objectives, approach
- Building resilience
- Evaluating resilience
- Governance Tools


Name/Callsign/MMSI/IMO or Port Name
Current vessels in this area: 28
LILY J
2016-10-29 22:24:27
Adabiya
Solitaire
Google Play
Google
©2016 Google - Map data ©2016 Google


TOPAZ RESOLVE
Add
MMSI: 538006667
IMO: 9544308
Length: 51 m
Depth:
Width: 13 m
Build year: 2015
DWT: 611
Gross ton: 1160
Callsign: V7PW2
Flag: MHL
Type: Offshore Supply Ship
Lat: 29°52.139 N
Lon: 32°32.010 E
Course: 233.4°
Truehead: 298°
Speed: 0.2 kts
Draught: 4.0 m
Status: Under way using engine
Dest: ARMED GUARD OB QT
ETA: 10-31 22:00
Time: 2016-10-29 22:42:05
souq.com
Exclusive App Only Deals.
Google Play


Name/Callsign/MMSI/IMO or Port Name
TOPAZ RESOLVE
2016-10-29 22:42:05
Solitaire
FREE ★★★★☆ (323,808)
©2016 Google - Map data ©2016 Google, ORION-ME, Mapa GIS

Zero-Day Vulnerabilities

EN English (United States) Help

In 2009 there were

2,361,414

new piece of malware created.

In 2015 that number was

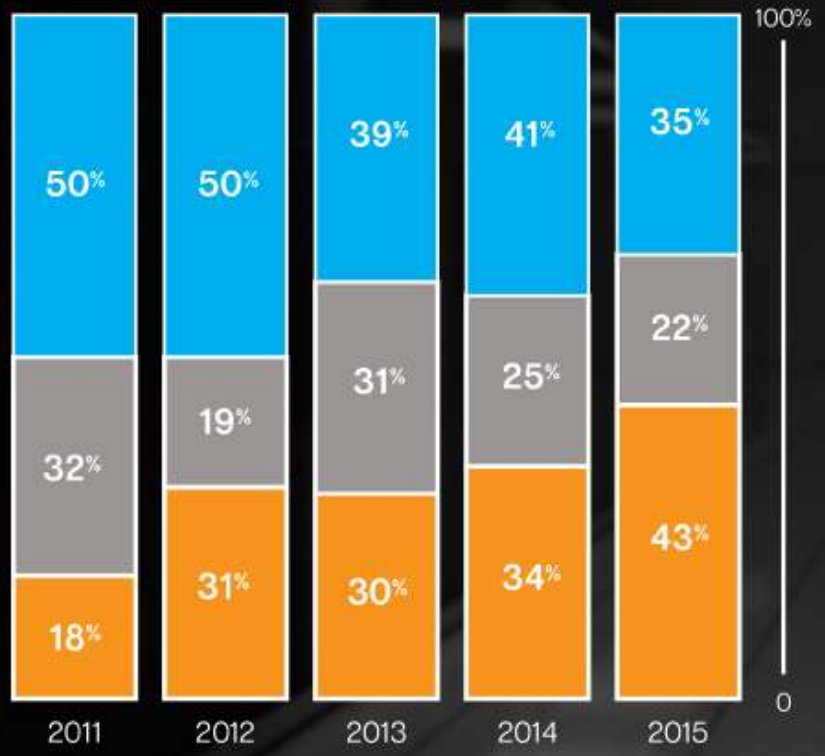
430,555,582

That's

1 Million 179 Thousand

a day.

Spear-Phishing Attacks by Size of Targeted Organization



Org Size	2015 Risk Ratio	2015 Risk Ratio as Percentage	Attacks per Org
Large Enterprises 2,500+ Employees	1 in 2.7	38%	3.6
Medium Business 251–2,500 Employees	1 in 6.8	15%	2.2
Small Business (SMB) 1–250 Employees	1 in 40.5	3%	2.1

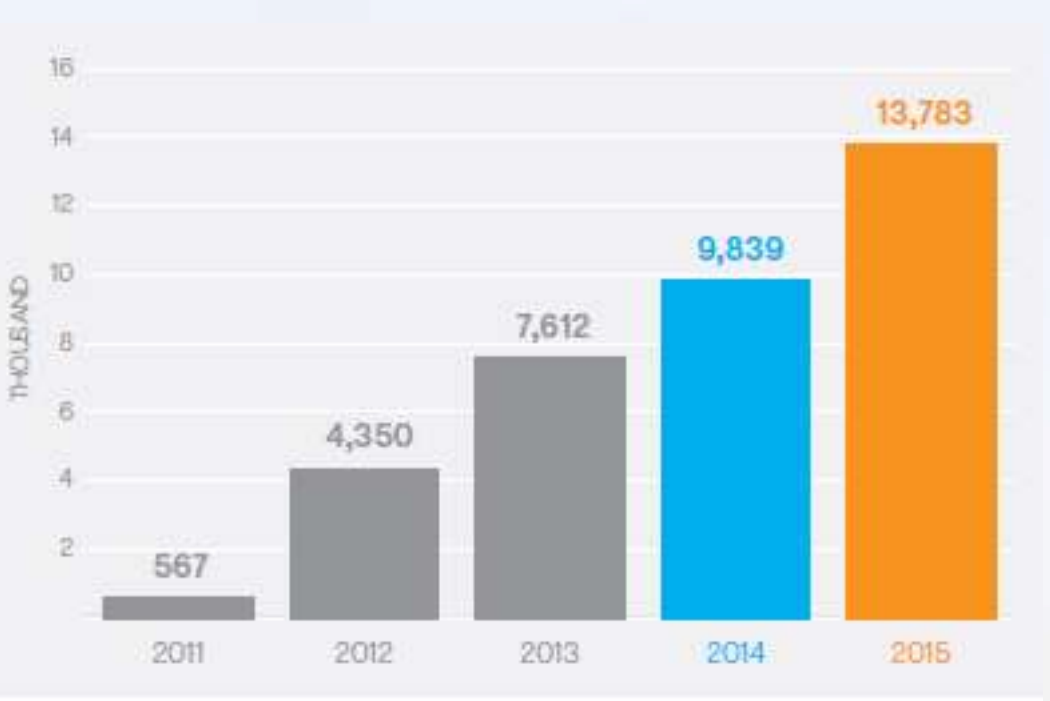
NTRA
EGYPT
الجهاز القومي لتنظيم الاتصالات
NATIONAL TELECOM REGULATORY AUTHORITY

Small businesses experience most of the data breach incidents because they:

- Are less aware of their exposures
- Have fewer resources to provide appropriate data protection and/or security awareness training for employees
- Are less likely to have strong cyber risk management controls in place
- Typically do not have a dedicated risk management professional
- Serve as a training ground for cyber thieves who are honing their skills to prepare for bigger attacks
- Are less likely to discover data breach

Forms of data breach your business can potentially be exposed to:

- Hacking
- Theft or release of funds due to unauthorized access (such as by former employees or vendors)
- Stolen or lost paper and electronic files
- Stolen or lost laptop, smartphone, tablet or computer disks
- Stolen credit card information
- Employee error or oversight



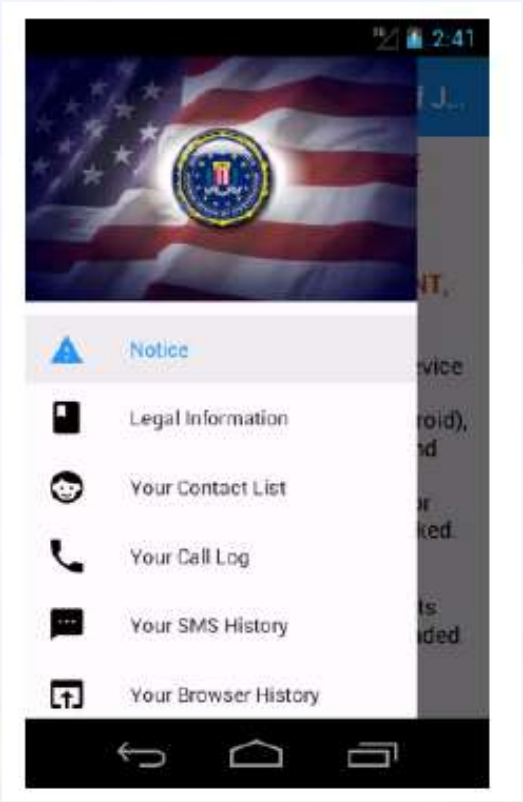
The world bought more than 1.4 billion smartphones in 2015, up 10 percent from the 1.3 billion units sold in the previous year, according to IDC's Worldwide Quarterly Mobile Phone Tracker (January 27, 2016).

The volume of Android variants increased by 40 percent in 2015, compared with 29 percent growth in the previous year.

Cross-Over Threats stolen cookies (essentially the users' credentials), impersonating the user to remotely install apps onto the victims' phones and tablets without their knowledge

Android Attacks Become More Stealthy

Ransomware Goes Mobile



Distinguishing Madware

Symantec analyzed 71 percent more apps in 2015 and more than three times as many (230 percent) more were classified as malicious. A 30 percent rise in grayware was owing in large part to a 77 percent rise in apps containing unwanted madware.

	2013	2014	2015
Total Apps Analyzed	6.1 Million	6.3 Million	10.8 Million
Total Apps Classified as Malware	0.7 Million	1.1 Million	3.3 Million
Total Apps Classified as Grayware	2.2 Million	2.3 Million	3.0 Million
Total Grayware Further Classified as Madware	1.2 Million	1.3 Million	2.3 Million
Malware Definition	Programs and files that are created to do harm. Malware includes computer viruses, worms, and Trojan horses.		
Grayware Definition	Programs that do not contain viruses and that are not obviously malicious, but that can be annoying or even harmful to the user, (for example, hacking tools, accessware, spyware, adware, dialers, and joke programs).		
Madware Definition	Aggressive techniques to place advertising in your mobile device's photo albums and calendar entries and to push messages to your notification bar. Madware can even go so far as to replace a ringtone with an ad.		

Dangers of Mobile Banking

Mobile devices are small computers that can face big problems

Shared devices could share problems.

Some devices are safer than others.

Protect with a password, or risk passing along your bank account

Instant might not always be "instant."

Old, unused phones still store your information

Poor reception can lead to poor security.

Auto-saved passwords are not secure protection.

Beware of 'rogue apps.'

Outdated apps often mean out-of-date security

The Insecurity of Things

Cars

Fiat Chrysler recalled 1.4 million vehicles

Smart home devices

Millions of homes are vulnerable to cyber attacks

Medical devices

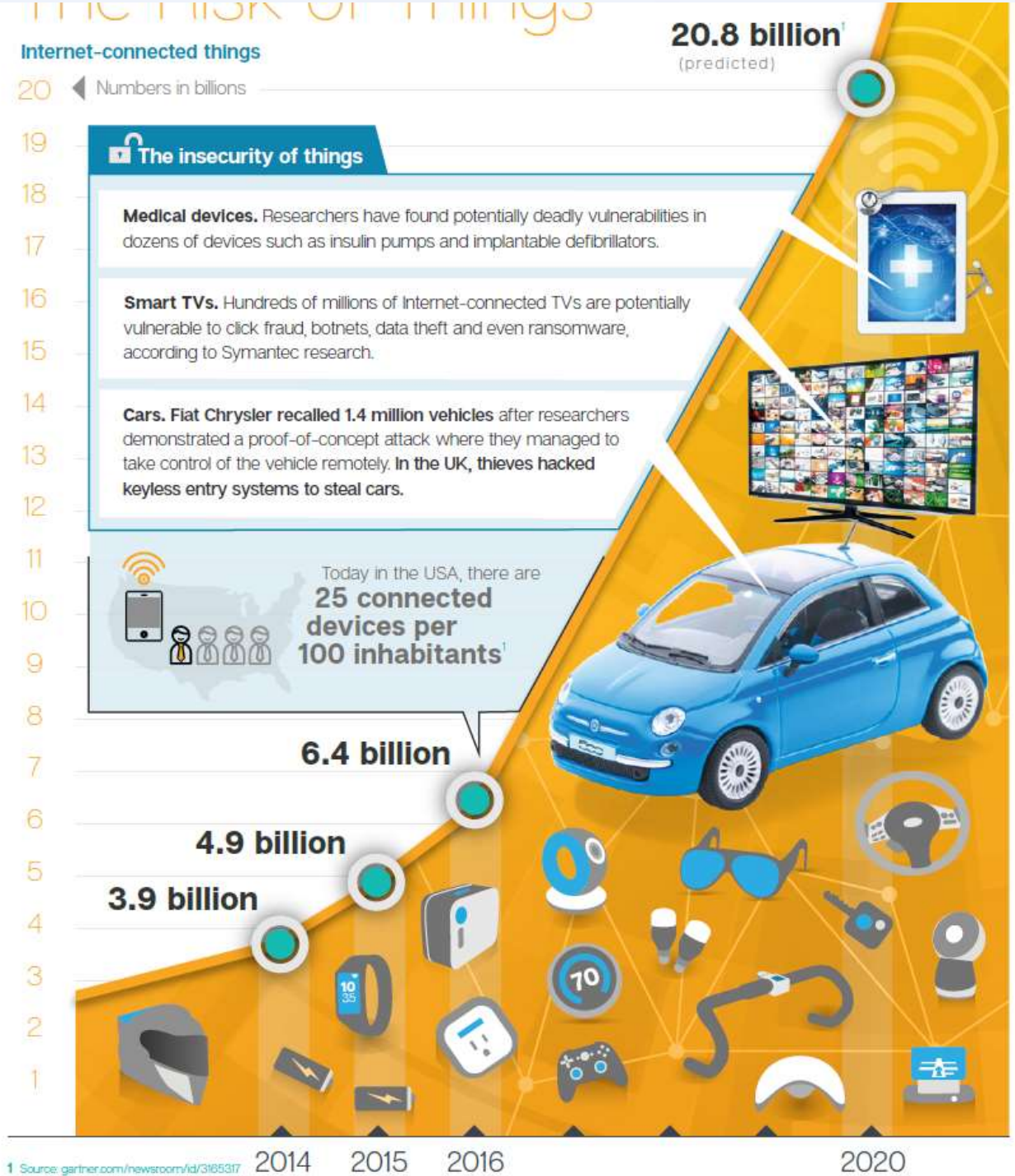
Researchers have found potentially deadly vulnerabilities in dozens of devices such as insulin pumps, x-ray systems, CT-scanners, medical refrigerators, and implantable defibrillators.

Smart TVs

Hundreds of millions of Internet-connected TVs are potentially vulnerable .

Embedded devices

Thousands of everyday devices, including routers, webcams, and Internet phones, share the same hard-coded SSH and HTTPS server certificates,



2016 Data Breach Investigations Report

Breaches with a financial motive dominate everything else , including espionage and fun.

89% of breaches had a
financial or espionage motive

Victim demographics

IoT is coming to kill us all

Mobile attacks bring us to our knees

Figures

2014

An average day in an enterprise, every:

- **1 min a host accesses a malicious website**
- **3 mins a bot is communicating with its C2 center**
- **9 mins High Risk Application is used**
- **10 minsa known malware is being downloaded**
- **27 minsan unknown malware is being downloaded**
- **49 mins sensitive data is sent outside the organization**

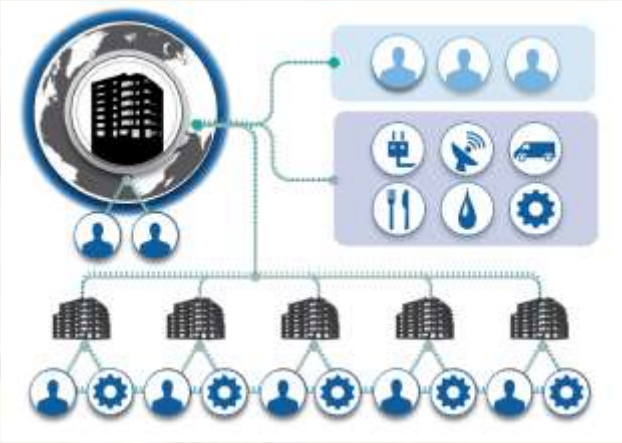
2015

An average day in an enterprise, every:

- **24 secs a host accesses a malicious website**
- **1 min a bot is communicating with its C2 center**
- **5 mins High Risk Application is used**
- **6 mins a known malware is being downloaded**
- **34 secs an unknown malware is being downloaded**
- **36 mins sensitive data is sent outside the organization**

The Digital Person

The Digital Enterprise



The Digital Challenge

Source: The Check Point 2015

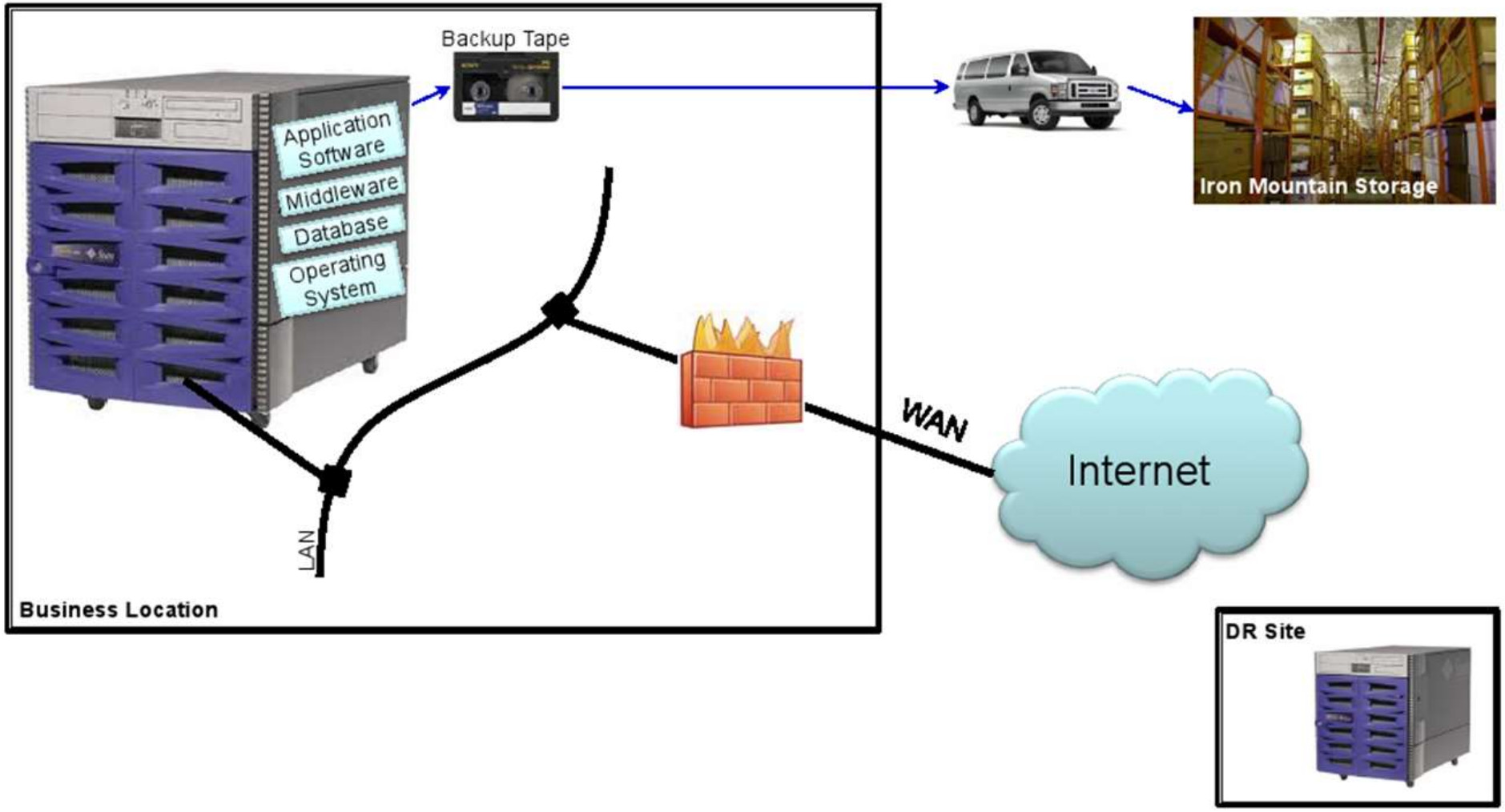
It is Cyber War

It is Cyber War

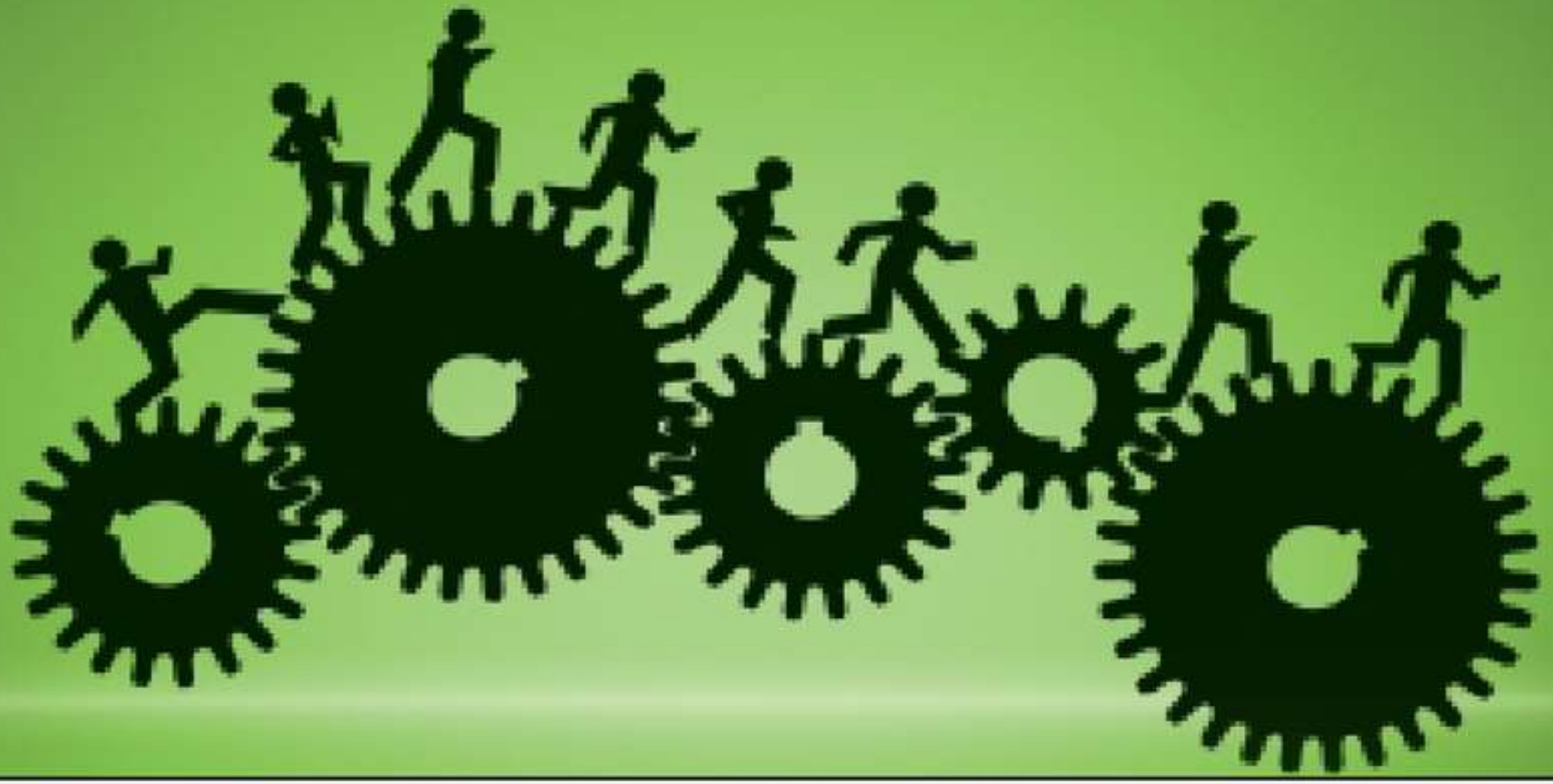
It is Cyber War

Yesterday's mission success would have been…

Why ?



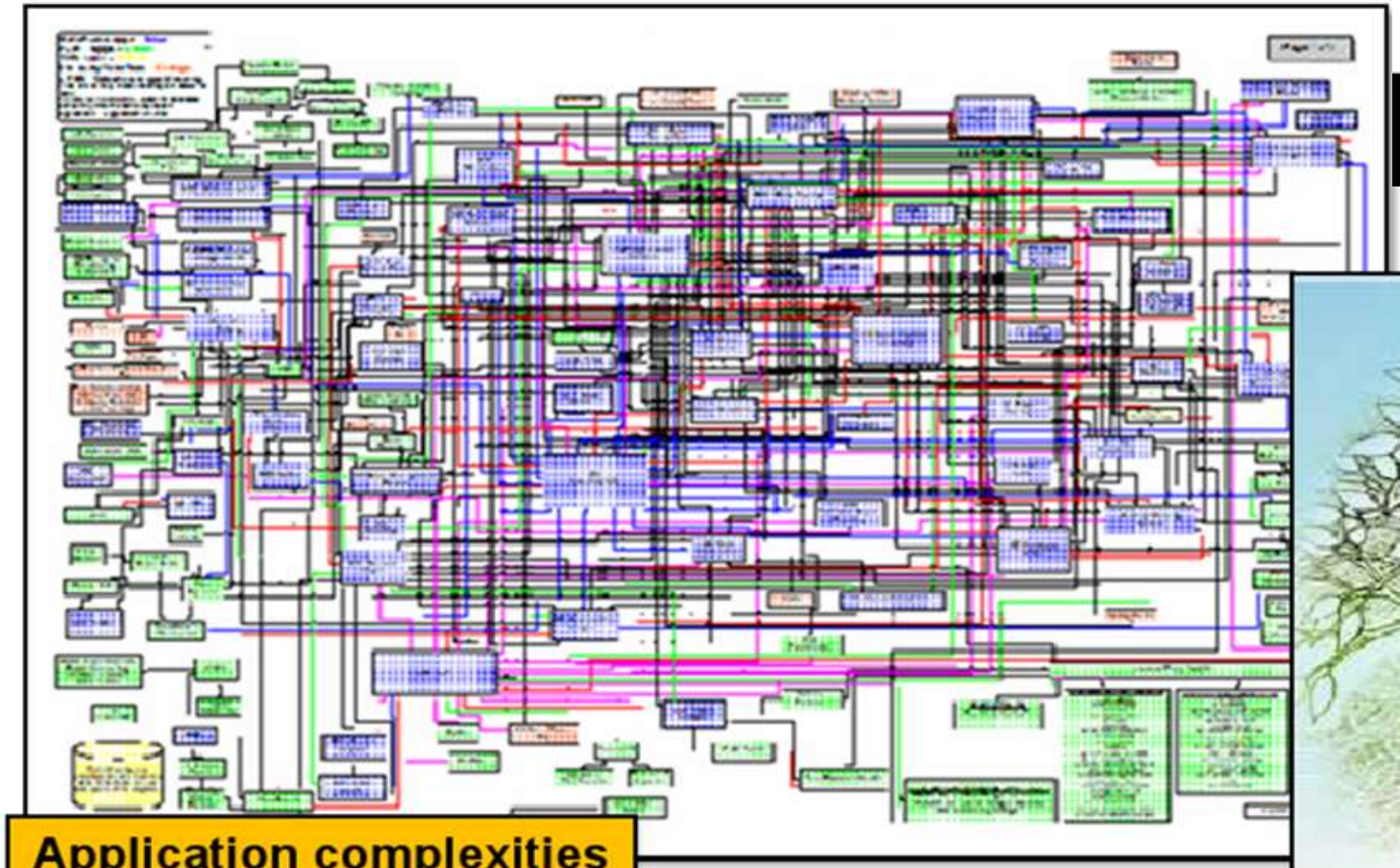
Organizational Mission



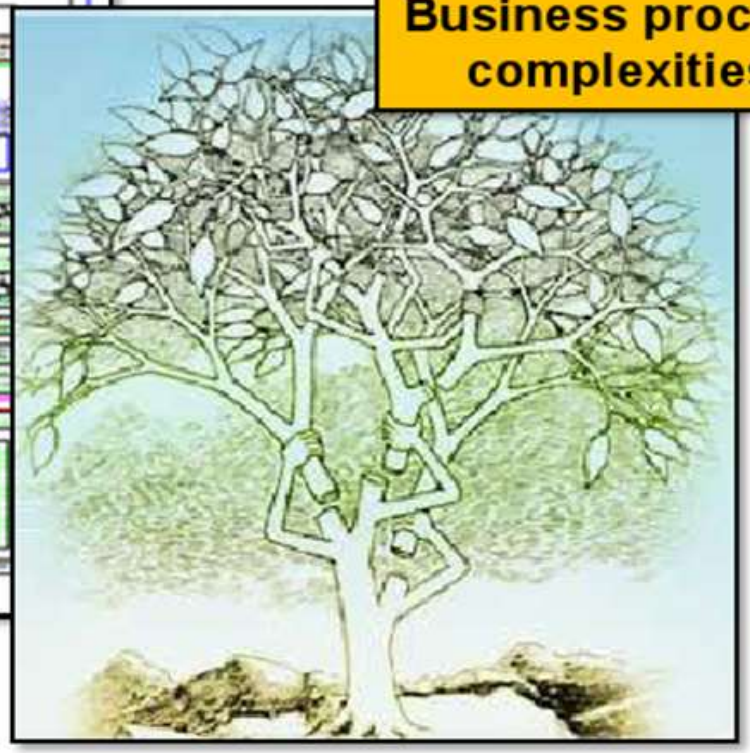
Organizational Mission - Revisited

Today's Mission Protection

Today mission success is about ..



Application complexities



Business process complexities

and more…

Worried yet?

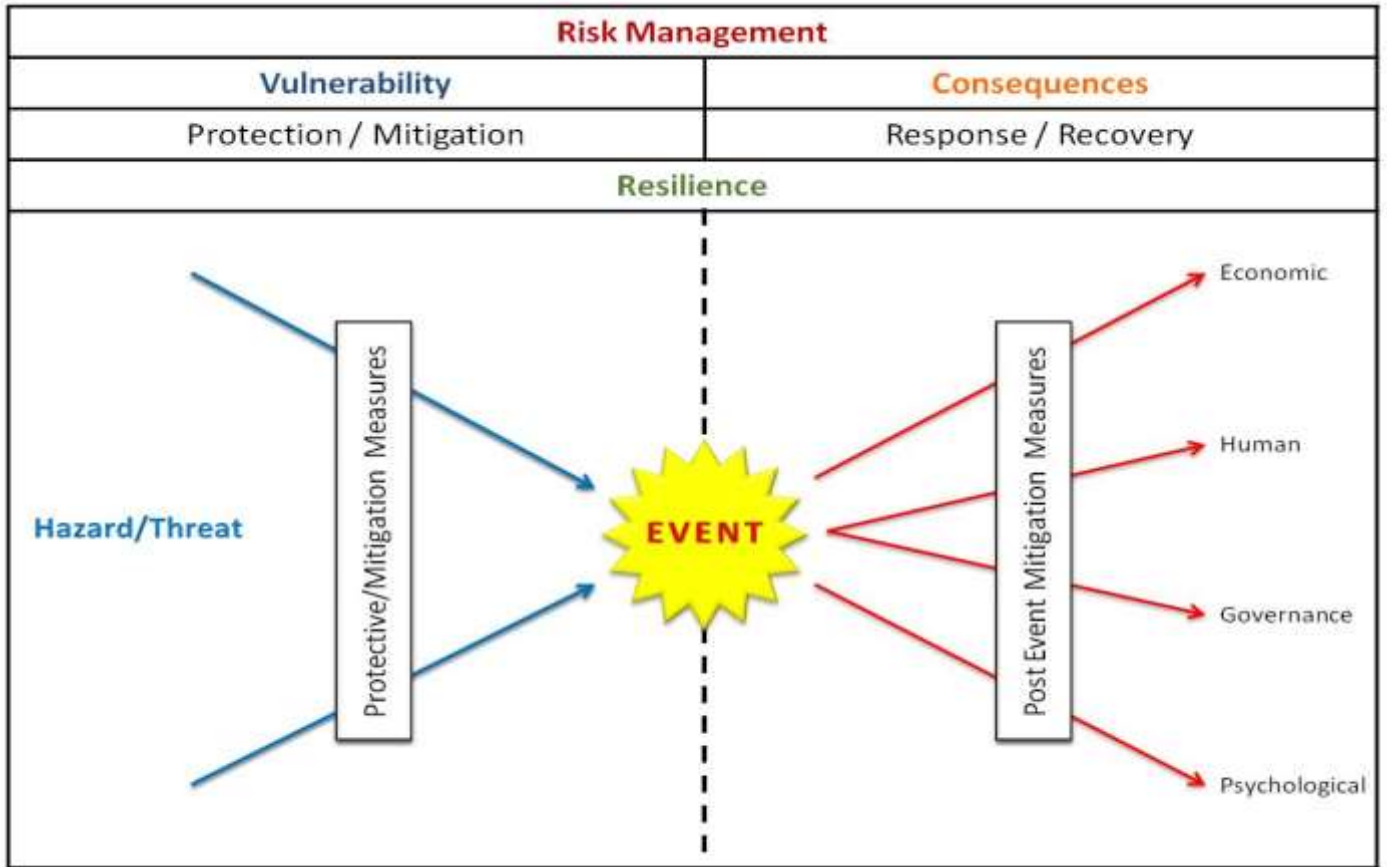
Cyber Security isn't going far enough.

Enter Cyber Resilience

We have to move to the next step: implementing a Cyber Resilience (CR).

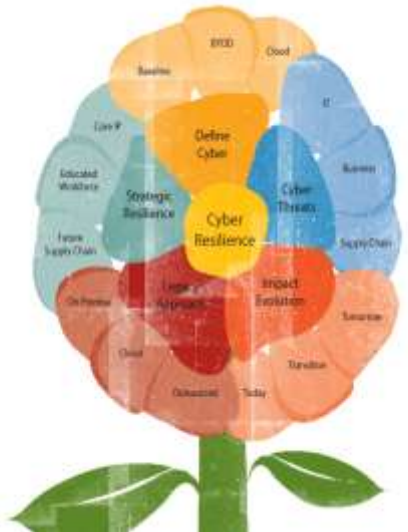
Challenge:

- Plan
- Develop
- Execute
- Govern



Building Cyber Resilience

National Telecommunications Regulatory Authority



Objectives:

Strengthen

Cyber Security Capabilities

÷ = x +

Enable consistent evaluation and benchmarking

Strategy Initiatives

- **Enable prioritized actions**

1. Share
2. Create
3. Partner
4. Identify
5. Raise

Proposed Approach

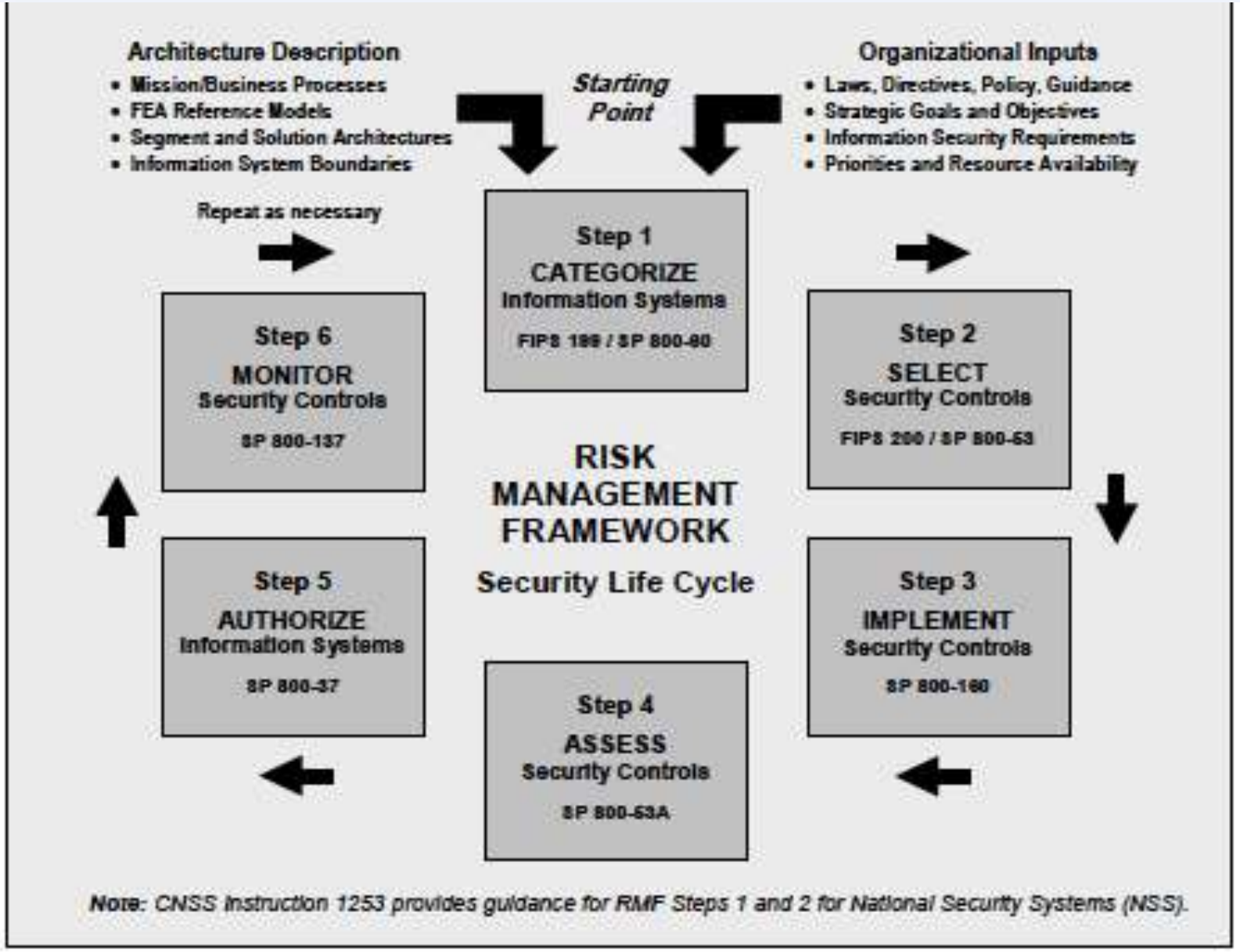


FIGURE 2: RISK MANAGEMENT FRAMEWORK

Problems of Measuring Risk

Businesses normally wish to measure in money, but

- Many of the entities do not allow this
  - Valuation of assets
    - Value of data and in-house software - no market value
    - Value of goodwill and customer confidence
  - Likelihood of threats
    - How relevant is past data to the calculation of future probabilities?
      - The nature of future attacks is unpredictable
      - The actions of future attackers are unpredictable
  - Measurement of benefit from security measures
    - Problems with the difference of two approximate quantities
      - How does an extra security measure affect a ~10^{-5} probability of attack?

Characteristics of Resilience

- **Survivability**
- **Disruption Tolerance**
- Being **resilient** may mean:
  - Remaining accessible
  - Degrading gracefully
  - Ensuring correctness of operation
  - Recovering from degradation
  - knowing the plan of action and what to do and can respond beyond their designated roles if necessary
  - Resilience is much more than fault-tolerance

Cyber Resilience Barriers

- Organizations may find it challenging to maintain cyber security operations in times of stress
  - Practices are not easily repeatable across the organization
  - Performance requirements are likely to fail
  - Key stakeholders are likely to lack situational awareness
- Organizations may not be resilient if key personnel…
  - …are absent
  - …fail to understand the cause, scope, and scale of the threat, event, or incident
  - …fail to apply the appropriate tools, knowledge, and skills as to how to best prepare, respond, and recover
- During times of stress, organizations are likely to:
  - Rely upon a high amount of interpersonal, yet informal, communication
  - Depend on skills, expertise, experience, and abilities of one or few people
- As employees vary over time, organizations may find it challenging to maintain fidelity and institutional knowledge

No suit Fits all

					
CERT-RMM	**OCTAVE**	**ES-C2M2**	**SGMM**	**3rd party Risk**	**Cybersecurity Assurance**
the foundation for a process improvement to operational resilience management. It defines the essential practices necessary to manage operational resilience.	is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning.	is a derivative that helps organizations evaluate, prioritize, and improve cybersecurity capabilities in the electricity subsector.	is a framework for guiding electricity generation, transmission, and distribution companies in planning their transformation, prioritize their actions, and measure their progress	Supply chain help organizations manage their external dependency risks focusing primarily on their relationships involving (ICT),	Cyber Resilience Review, Risk and Vulnerability Assessment, and External Dependencies Management Assessment Working with the stakeholders,

Cybersecurity Assurance Solutions

.Cyber Resilience Review (CRR)

Created by the CERT Division for the U.S. Department of Homeland Security (DHS), the CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains (based on CERT-RMM) including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.

Risk and Vulnerability Assessment (RVA)

An RVA identifies vulnerabilities and ensures that security implementation actually provides the protection that organizations require and expect. An RVA is conducted collaboratively by CERT subject matter experts and DHS using open source and commercial security tools to conduct vulnerability scanning and manual penetration testing. These scans and tests determine whether, and by what methods, an adversary can defeat security controls on a live or simulated network. The main goals of the RVA are to help secure against known vulnerabilities and threats by providing mitigation strategies to reduce risk, and aggregate vulnerability data so executives can make informed decisions regarding the security and safety of information systems.

External Dependencies Management (EDM) Assessment

The EDM Assessment evaluates an organization's risk management when forming relationships with external entities, ongoing management of third-party relationships, and the ability to sustain services when external entities fail to meet the terms of service or are otherwise disrupted. The EDM Assessment, offered by the DHS Cyber Security Evaluation Program, is a no-cost, voluntary, non-technical assessment to evaluate and communicate the EDM capability of critical infrastructure organizations.

Evaluating Cyber Resilience

Cyber Resilience Review

National Telecommunications Regulatory Authority

Cyber Resilience Review Evaluation Tool

CRR-self-assessment-package

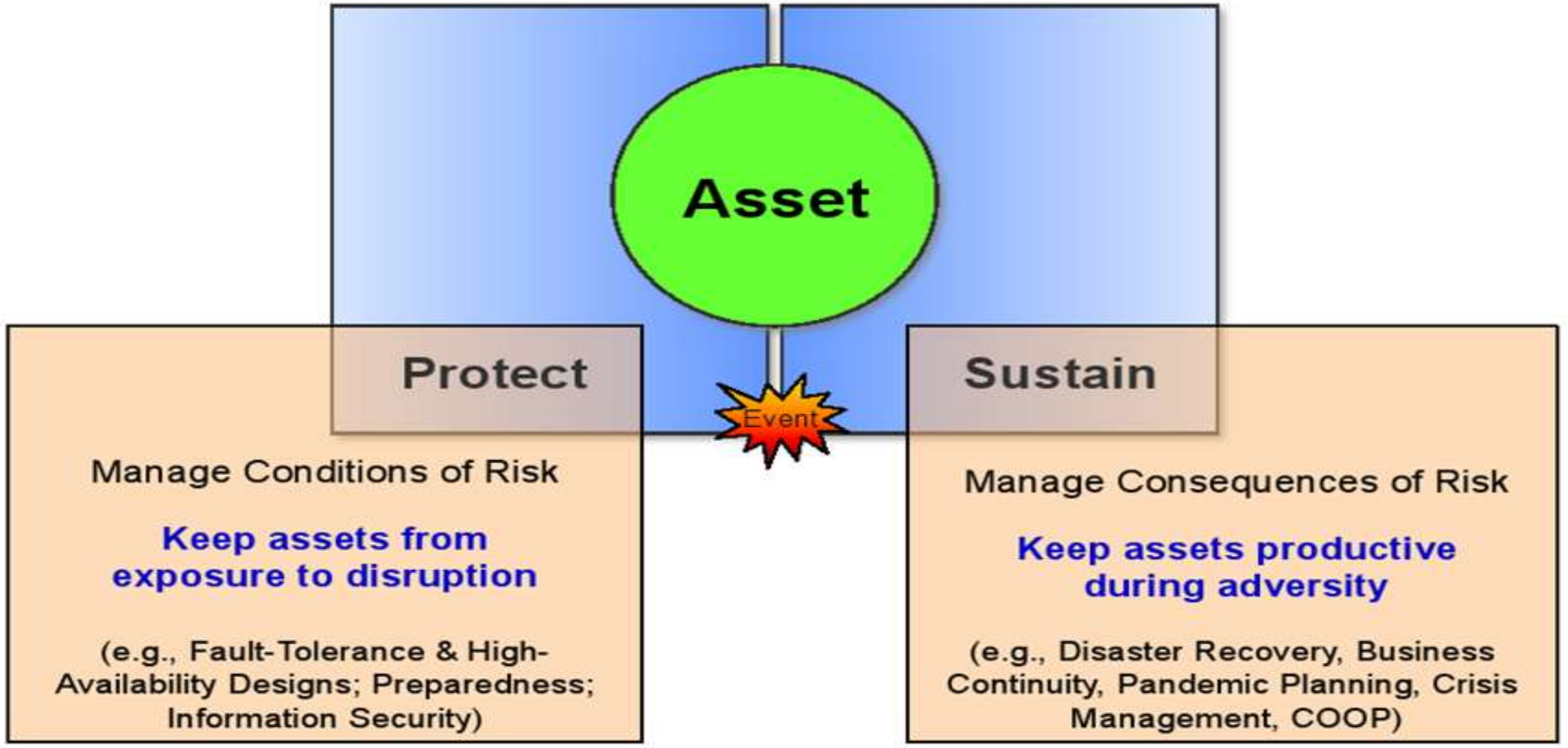
The CRR is a no-cost, non-technical assessment to evaluate operational resilience and cybersecurity capabilities of an organization. The CRR is based on the CERT Resilience Management Model a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience

Additional supporting material relating to the Framework can be found on the NIST website at http://www.cert.org/resilience/rmm.html

CRR Domain Goals

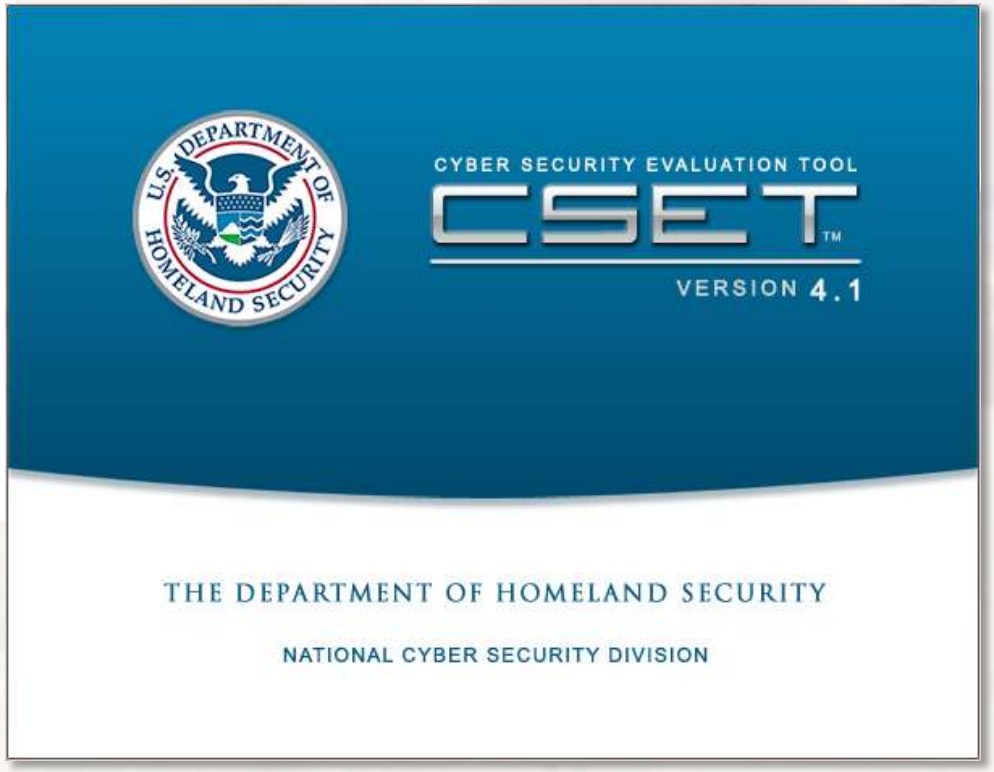
AM	**Asset Management** *identify, document, and manage assets during their life cycle*	IM	**Incident Management** *identify and analyze IT events, detect cyber security incidents, and determine an organizational response*
CCM	**Configuration and Change Management** *ensure the integrity of IT systems and networks*	SCM	**Service Continuity Management** *ensure the continuity of essential IT operations if a disruption occurs*
RISK	**Risk Management** *identify, analyze, and mitigate risks to critical service and IT assets*	EXD	**External Dependencies Management** *establish processes to manage an appropriate level of IT, security, contractual, and organizational controls that are dependent on the actions of external entities*
CNTL	**Controls Management** *identify, analyze, and manage IT and security controls*	TRNG	**Training and Awareness** *promote awareness and develop skills and knowledge of people*
VM	**Vulnerability Management** *identify, analyze, and manage vulnerabilities*	SA	**Situational Awareness** *actively discover and analyze information related to immediate operational stability and security*

Operational Resilience Starts at Asset Level



Cyber Security Evaluation Tool (CSET) ™

- Stand-alone software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy



CSET Download:

www.us-cert.gov/control_systems/csetdownload.html

CSET Standards

Requirements Derived from Widely Recognized Standards

NIST Special Publication 800-53	Recommended Security Controls for Federal Information Systems Rev 3 and with Appendix I, ICS Controls
ISO/IEC 15408	Common Criteria for Information Technology Security Evaluation, Revision 3.1
NERC Critical Infrastructure Protection (CIP)	Reliability Standards CIP-002 through CIP-009, Revisions 2 and 3
DoD Instruction 8500.2	Information Assurance Implementation, February 6, 2003
NIST Special Publication 800-82	Guide to Industrial Control Systems (ICS) Security, June, 2011
NRC Reg. Guide 5.71	Cyber Security Programs for Nuclear Facilities, January 2010
CFATS RBPS 8- Cyber	Chemical Facilities Anti-Terrorism Standard, Risk-Based Performance Standards Guidance 8 – Cyber, 6 CFR Part 27
DHS Catalog of Recommendations	DHS Catalog of Control Systems Security, Recommendations for Standards Developers, Versions 6 and 7

ITU Recommendations for resilience

- **Establish Governance -** Identify and organise key stakeholders
- **Governance, Risk and Compliance () -** Fulfil through policies and processes,
- **Service continuity** - **Protect information proactively**
- **Authenticate users** with Strong Authentication

- **Threat intelligence** - major trends in terms of potential attackers, through analysing trends on malware, security threats, and vulnerabilities
- **Managed security services** - Outsourcing security services to providers. The ICT leadership can in that way focus on their functional duties of running the systems
- Rely on their national Computer Emergency Response Teams (CERT), in order to be aligned with national coordination on cyber-incidents and security, and benefit from the international visibility this provides these entities provide.
- **Protect the infrastructure** by securing endpoints, messaging and web environments.
- **Ensure 24x7 availability of the critical infrastructure**
- **Develop an information management strategy**

Ref . Cyber-security, data protection and cyber-resilience in Smart Sustainable Cities, ITU-T SG17, April 2015

How to least Risk Management?

- Vendor Management
- Policies and Procedures
- Security Awareness/Education
- Risk Assessment
- Enforcement of Policies & Procedures
- Basic Data Security Good Practices

RESOURCES

Cybersecurity Framework and supporting materials:
http://www.nist.gov/itl/cyberframework.cfm
NIST Computer Security Resource Center: http://csrc.nist.gov/
C3 Voluntary Program: www.dhs.gov/ccubedvp
C2M2 Program: http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program
Cybersecurity Resilience Review : http://www.us-cert.gov/ccubedvp/self-service-crr

Questions

Dr. Emadeldin Helmy
Cyber Risk Ass. & Resilience
ehelmy@tra.gov.eg