ESI European Software Institute
Center Eastern Europe

SEI Partner | Carnegie Mellon

CERT® Resilience Management Model

Cyber Security & Business Resilience

[CERT-RMM: How to make our **business resilient** with the new technologies & dependencies?]

Dr. George Sharkov **(ESI CEE)**
Yavor Papazov **(ESI CEE CyResLab)**

SEMP SOFTWARE ENGINEERING MANAGEMENT PROGRAM

http://SEMP.esicenter.bg

Carnegie Mellon University
institute for SOFTWARE RESEARCH

Software Engineering Institute
Carnegie Mellon

ESI European Software Institute
Center Eastern Europe

NEW BULGARIAN UNIVERSITY • НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ •

SEMP: SOFTWARE ENGINEERING MANAGEMENT PROGRAM

The course is developed (and compiled) jointly by ESI Center (Eastern Europe) and CMU from the main lines and materials for SEMP, in partnership with SEI/CMU.

It introduces students to process improvement as a main factor for the quality of products and services.

Based on process-oriented models - CMMI, the "industrial" standard developed by SEI/CMU, project management (PMI/PM BOK), personal/team management (PSP/TSP BOK), strategic planning (Balanced ScoreCards), information security.

Augmented by modern methods and techniques – Agile CMMI, Six Sigma, etc. Mapping between main industrial models and standards. Implementation. Models for quality improvement in small settings and SMEs. Business aspects – cost of quality, what is "the right model for my company", why invest in PI, what is the return, who can help.

USAID FROM THE AMERICAN PEOPLE

AMERICA FOR BULGARIA FOUNDATION
Фондация Америка за България

Notices

General disclaimer (European Software Institute – Center Eastern Europe, ESI CEE)
www.esicenter.bg

STATEMENT FOR LIMITED USE OF TRAINING AND PRESENTATION MATERIALS

All training and presentation materials by ESI CEE (or under a license of a third party), in a printed or electronic form, are intended for attendee's personal use or for limited internal use for their organization awareness and educational purposes. Neither the training attendee, nor their organization shall use all or part of these materials for commercial purposes.

These materials SHALL NOT be reproduced or used in any other manner without obtaining a formal permission from ESI CEE at office@esicenter.bg.

All, or part of the materials, might be a subject to additional restrictions or copyrights, as duly indicated, and shall be respected.

For all materials ***Copyrighted by SEI (Software Engineering Institute, Carnegie Mellon University, USA), SEI-CERT:***
© 2009-2012 Carnegie Mellon University

"This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study." All materials are marked on the slide, or as a SEI/CERT-Carnegie Mellon background (layout)

Съдържание на курса

№	ТЕМА	Лекции	Упраж-нения
1	Оперативни рискове и управление на устойчивостта и надеждността на ИТ-базирани (дигитализирани) системи и услуги. Преглед на моделите и стандартите за информационна сигурност и надеждност на ИТ (компютърни и мрежови) ресурси.	2	
2	Модел CERT-RMM. Източници, предназначение и внедряващи организации. Обща структура. Основни категории процеси, базови активи (assets), класификация на слабостите и заплахите.	4	2
3	Детайлно описание на активите и ресурсите, свързани с технологични (компютърни и мрежови) и информационни ресурси. Одит (оценка) на заплахите и слабостите, отговорности и устойчивостта на ресурсите. Стратегии и планове за Protect и Sustain. Удовлетворяване на принципите за CIA (Confidentiality, Integrity, Availability).	4	2

Съдържание (2)

№	ТЕМА	Лекции	Упраж-нения
4	Избрано от процесни области: Engineering category, Operations category. Детайлно представяне и упражнения за: ADM - Asset Definition and Management RRD - Resilience Requirements Development RTSE - Resilient Technical Solution Engineering SC – Service Continuity AM – Access Management ID – Identity Management IMC – Incident Management and Control PM – People Management TM – Technology Management VAR – Vulnerability Analysis and Resolution	12	6
5	• Анатомия на модерните атаки (уеб, мобилни). Примери. • Разглеждане на log-файлове за трафик, средства (WireShark, др.) • Оценка на риска (слабости, уязвимости, exploits), дизайн и интеграция с cloud-базирани услуги (информация, защита, криптиране). • Рискове и специфични политики при използване на лични устройства в организацията (BYOD = Bring Your Own Device)	4	2
6	Изготвяне и представяне на доклад (презентация) за заплахи, слабости, кибер атаки. Оценка на щетите. Превенция и реакция.	4	3

Who are we?

ESI European Software Institute tecnalia

Since 1993

partner of:

Software Engineering Institute | Carnegie Mellon

ESI European Software Institute Center Eastern Europe

Since 2003

ESI Center Eastern Europe

PPP: SW Industry(BASSCOM), ESI & State ICT agency, supported by: USAID, UNDP

SEI Partner | Carnegie Mellon

CMMI

CERT RMM

it mark

Affordable "BIG" standards for "small" companies

ESICenters • ESI@net Partners

Good practices, achievements…

www.cryptobg.org

https://dnbl.ncia.nato.int

MCSC Collaboration model

ISACs (Information Sharing and Analysis Centers)

CERT | Software Engineering Institute | Carnegie Mellon

Carnegie Mellon University

Software Engineering Institute (SEI)

- Federally funded research and development center based at Carnegie Mellon University
- Basic and applied research in partnership with government and private organizations
- Helps organizations improve development, operation, and management of software-intensive and networked systems

CERT – *Anticipating and solving our nation's cybersecurity challenges*

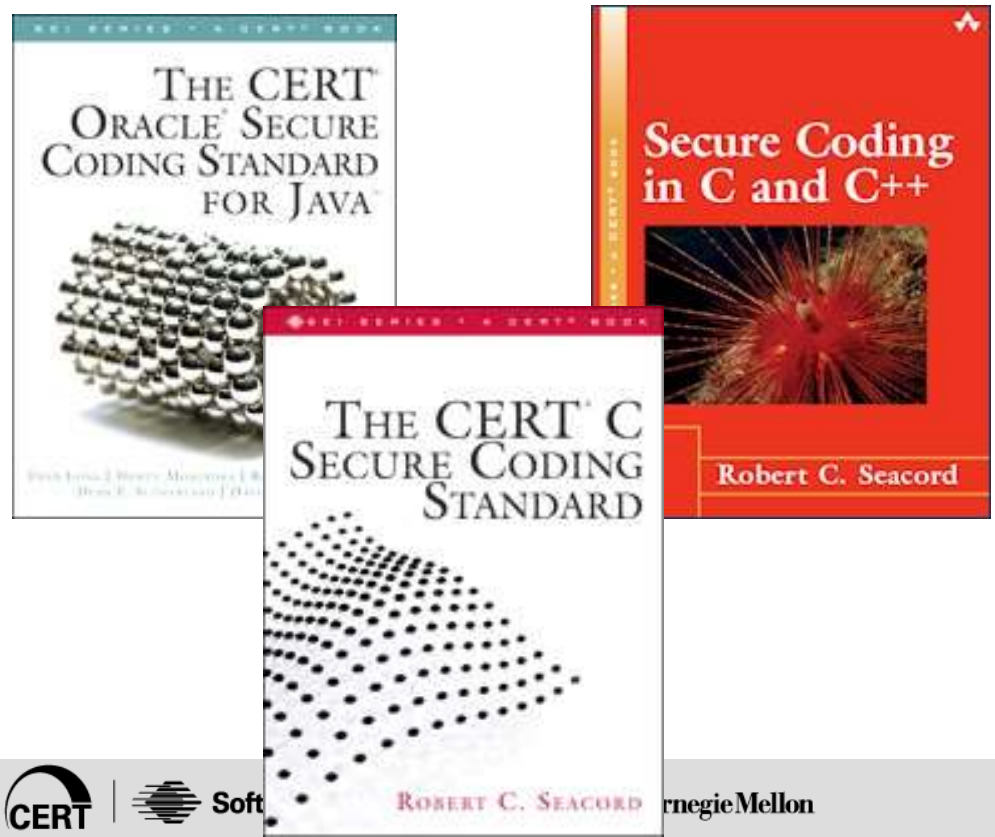
- Largest technical program at SEI
- Focused on internet security, digital investigation, secure systems, insider threat, operational resilience, vulnerability analysis, network situational awareness, and coordinated response

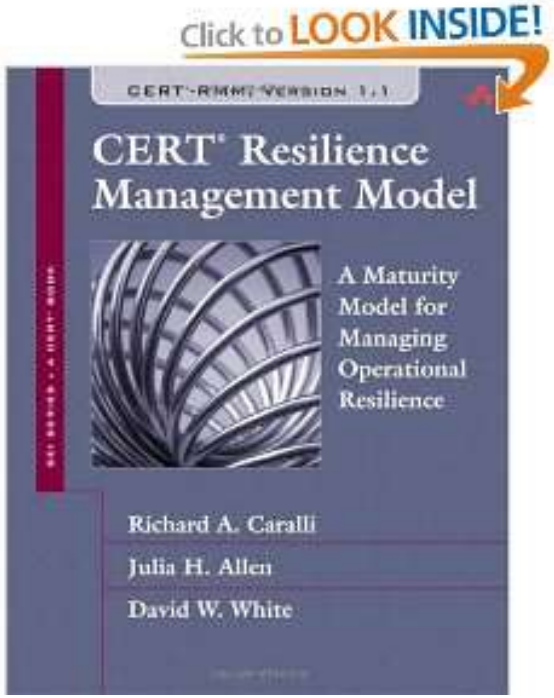
Computer Emergency Response Team (the origin 1988, and now)

CERT | Software Engineering Institute | Carnegie Mellon

Closing gaps & develop good code:
Secure Coding Standards
[languages + compilers]

Generic Model to Manage and Assess the Operational Resilience
[Information Security, Security Business Continuity]





Resources

Training

Introduction to the CERT Resilience Management Model (3-day course)

- Public courses (Pittsburgh and DC)
- Private onsite courses

Appraiser and instructor training in development

CERT-RMM User Group Annual Series

- Quarterly 2-day workshops
- Focus on CERT-RMM implementation
- CERT-RMM Coach Certification option

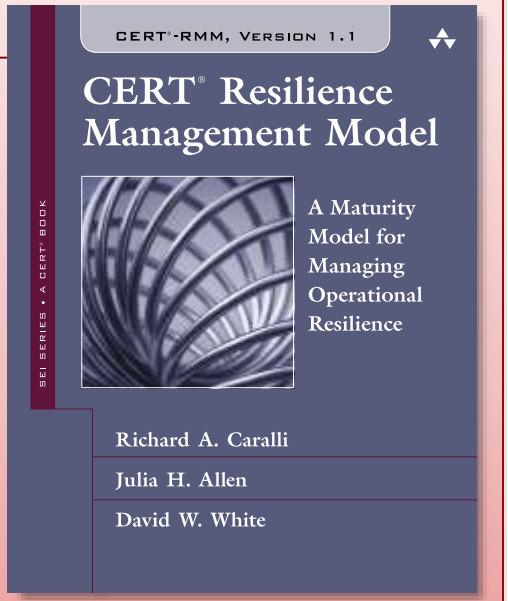
Website

www.cert.org/resilience

Book

Includes full model (v1.1) plus adoption guidance and perspectives of real-world use of the model

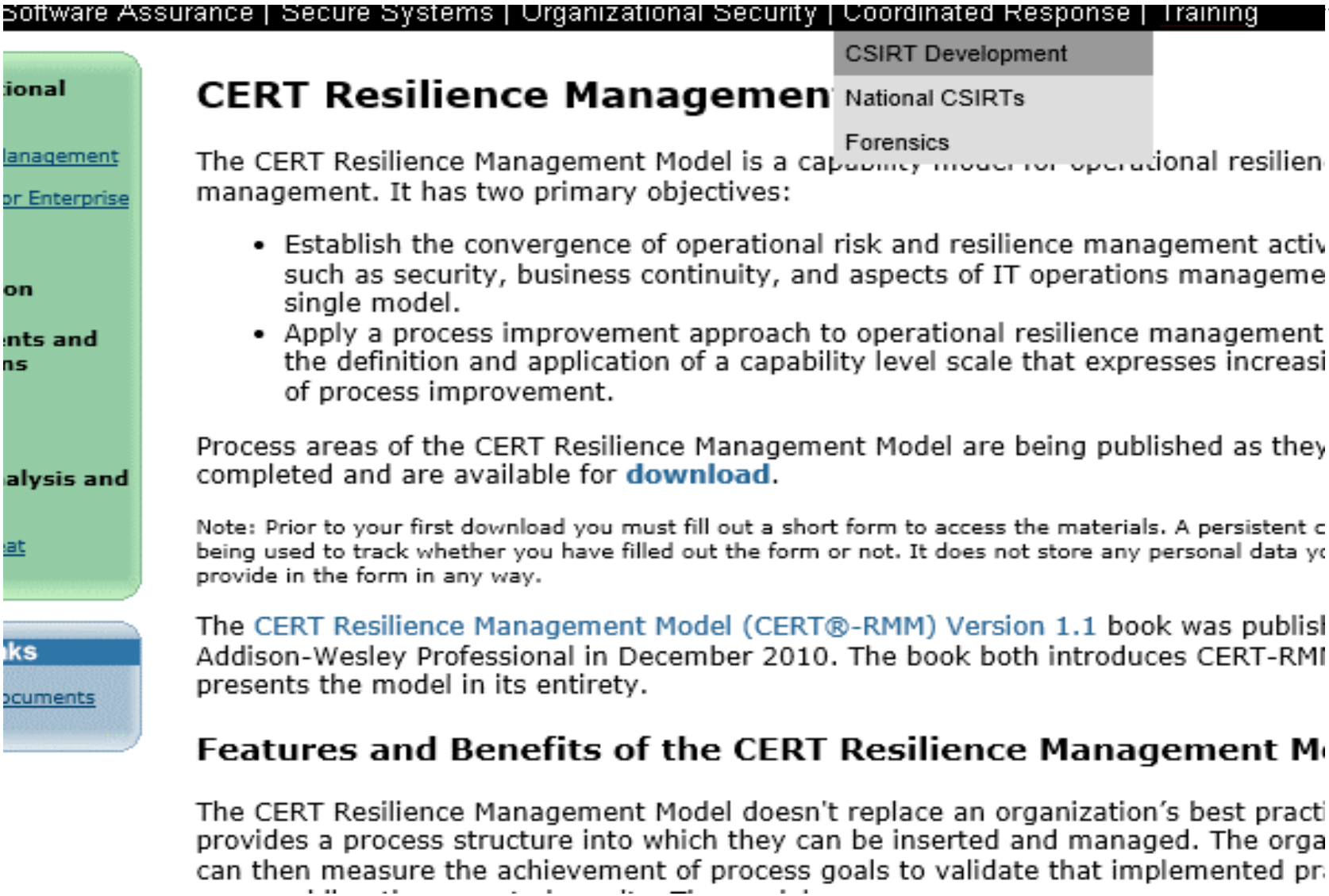
www.amazon.com/CERT-Resilience-Management-Model-RMM/dp/0321712439



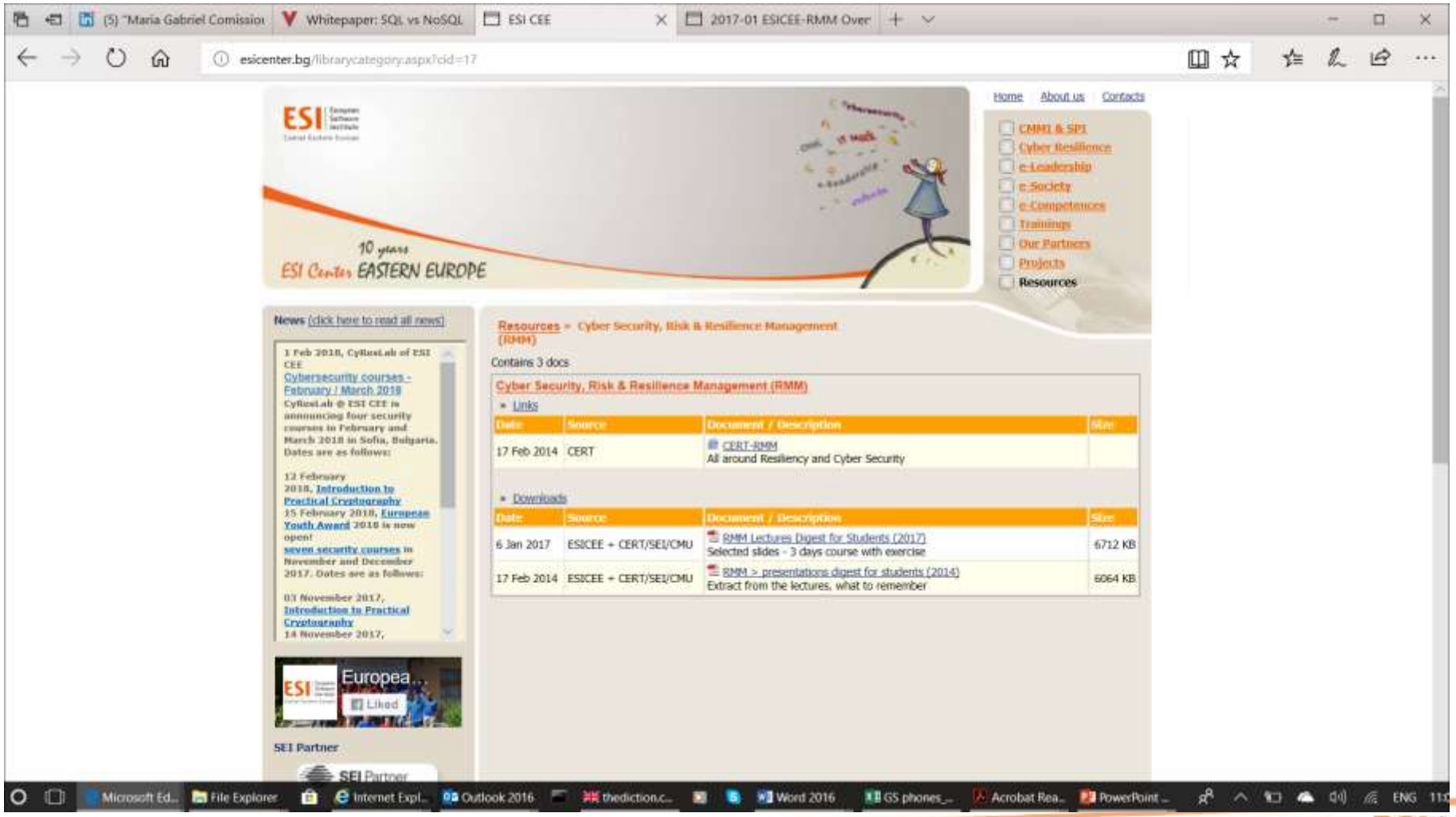
Support

Engage CERT-RMM team to lead appraisals, provide implementation coaching, pilot CERT-RMM Compass, or deliver custom training

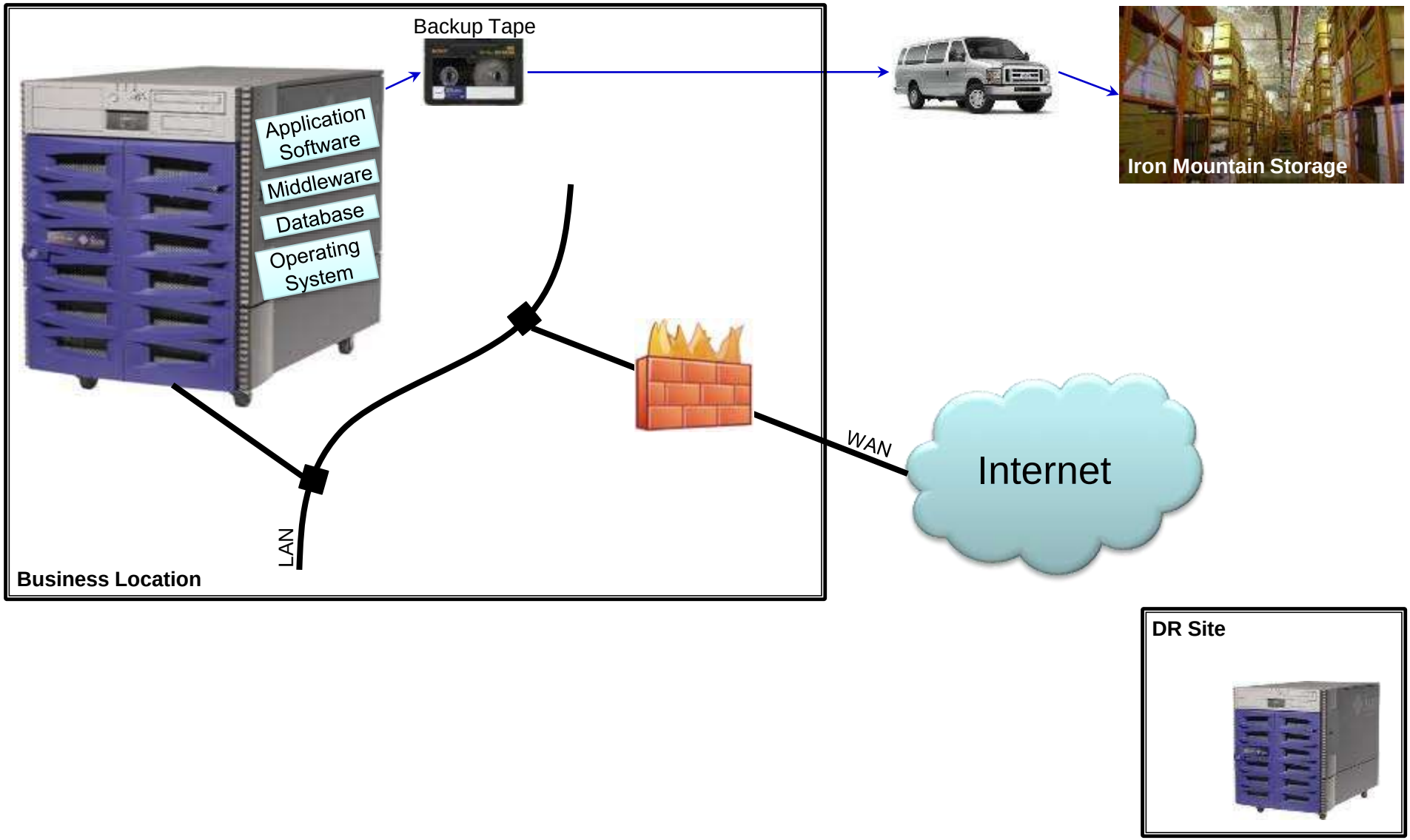
http://www.cert.org/resilience/rmm.html



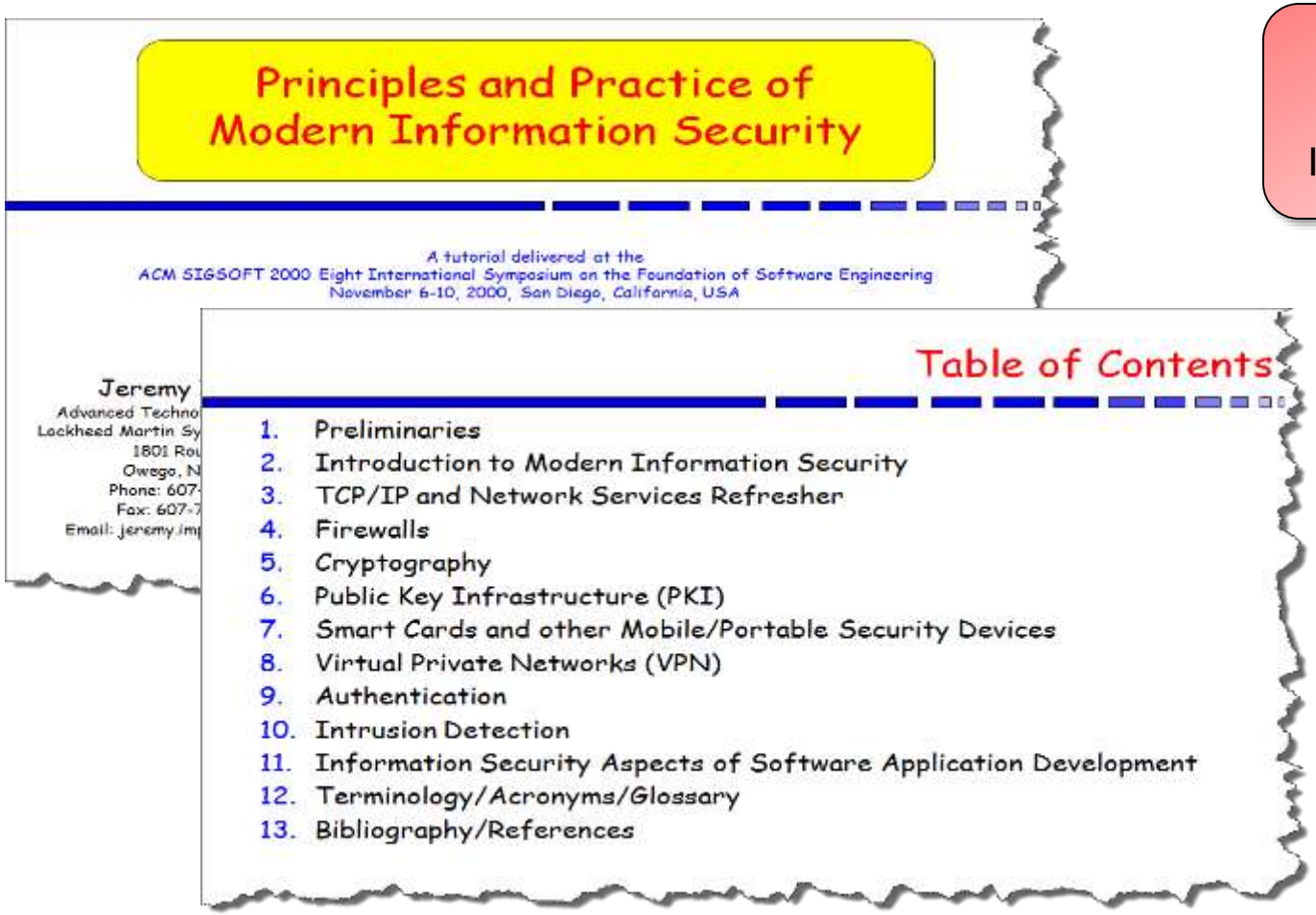
www.esicenter.bg >Resources (Educaiton)
www.cyreslab.org



Yesterday it would have been about…

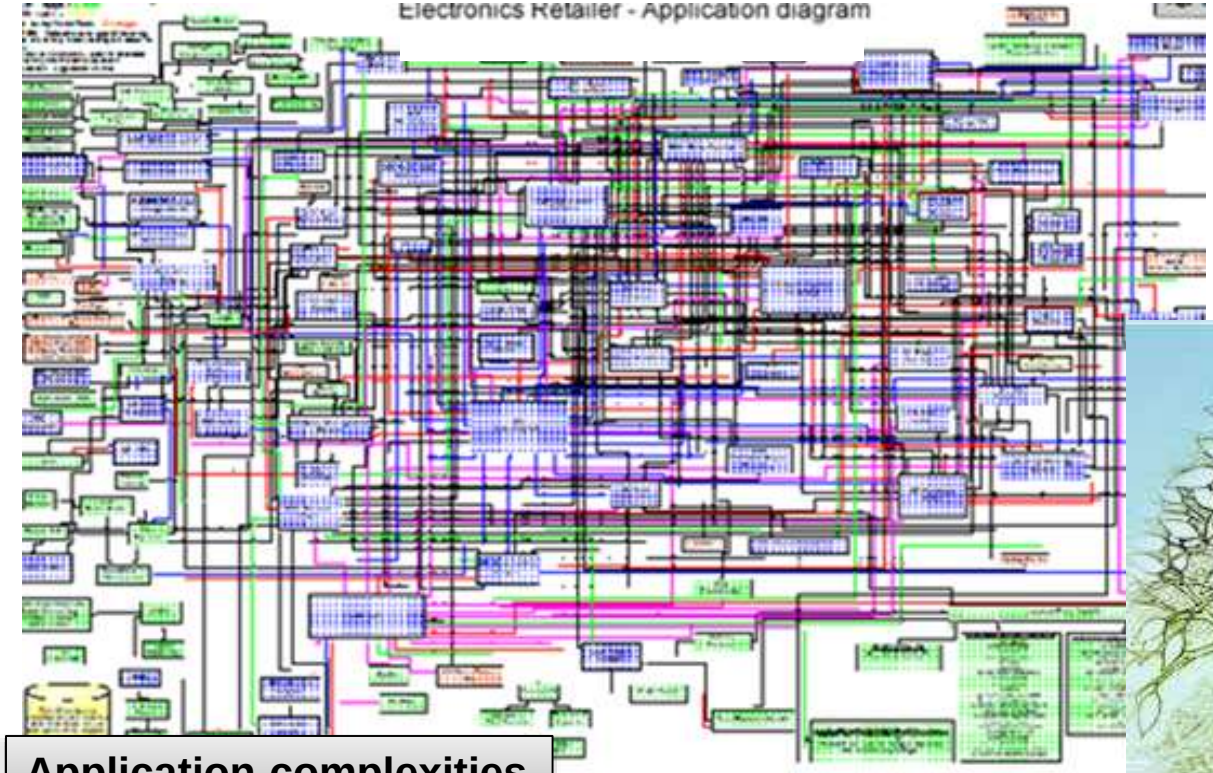


Yesterday it would have looked like…



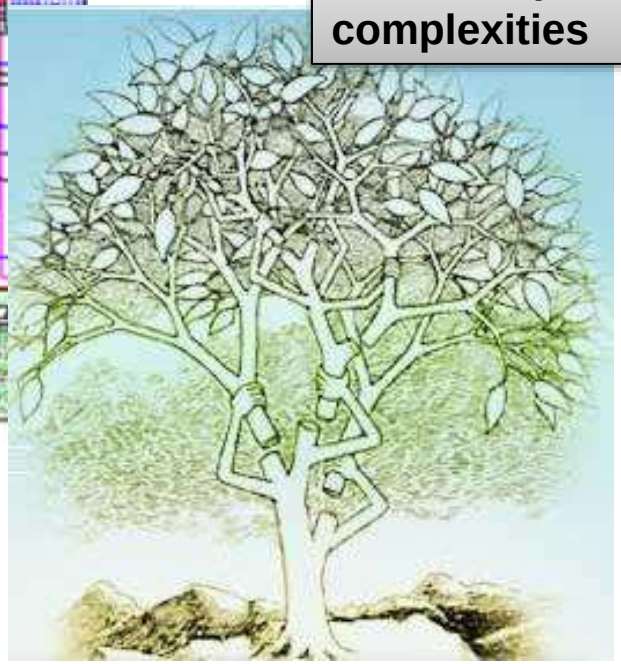
It would have been all about IT and Controls

Today it has to deal with…



Application complexities

Business process complexities



and more…

Today it has to be about…

Sample definition of IA:

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Sample definition of IA:

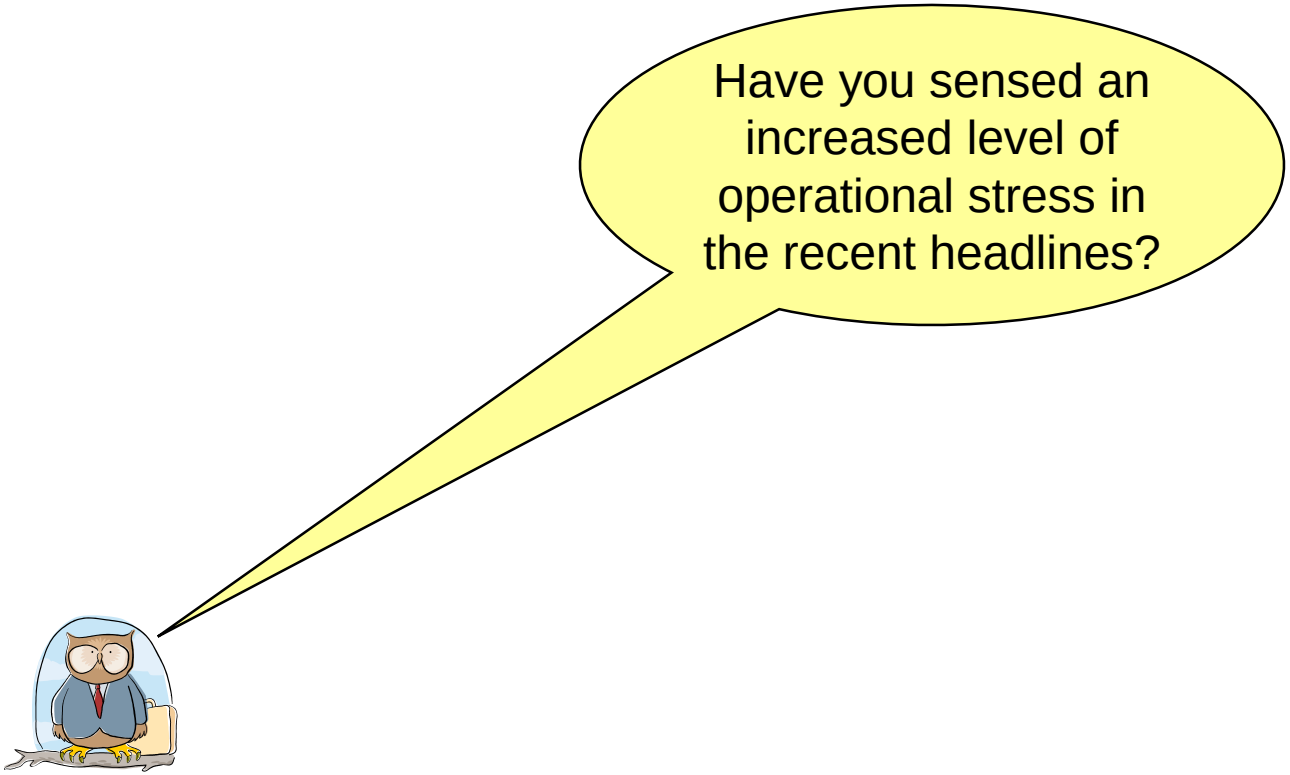
Information assurance is related to the field of information security, in that it is primarily concerned with the protection of information systems and their contents. Generally considered the more broadly-focused of these two fields, IA consists more of the strategic risk management of information systems rather than the creation and application of security controls. In addition to defending against malicious hackers and code (e.g., viruses), IA practitioners consider corporate governance issues such as privacy, regulatory and standards compliance, auditing, business continuity, and disaster recovery as they relate to information systems. Further, while information security draws primarily from computer science, IA is an interdisciplinary field requiring expertise in accounting, fraud examination, forensic science, management science, systems engineering, security engineering, and criminology, in addition to

and more…

What do you see here?

Look closer …

Look Again!


Have you sensed an increased level of operational stress in the recent headlines?

March 30, 2012

Friday, March 30, 2012 As of 5:16 PM EDT New York 89°|74°

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Community

World | U.S. | New York | Business | Markets | Tech | Personal Finance | Life & Cul

Asia | Europe | Earnings | Economy | Health | Law | Autos | Management | Media & Marketin

BUSINESS | March 30, 2012, 5:16 p.m. ET

Data Breach Sparks Worry

Hack Attack at Card Processor Compromises Potentially Thousands of Account

Article | Video | Stock Quotes | Comments (82)

By ROBIN SIDEL and ANDREW R. JOHNSON

Concerns about credit-card security heightened Friday after a little-known Atlant company disclosed it had been hit by hackers, potentially exposing hundreds of thousands of account holders to fraud.

Credit and debit card processor Global Payments has been hit by a security breach that has put some 50,000 cardholders at risk, Andrew Johnson reports on Lunch Break. Photo: Bloomberg News.

The breach at Global Payments In GPN +1.68% is the latest in a wav data attacks that have heightened consumer concerns about identity The card industry has been partic vulnerable to those concerns amic of big breaches in recent years as Americans choose to pay with plas rather than cash.

The exten

July 14, 2012

HUFF POST BUSINES

THE INTERNET NEWSPAPER: NEWS BLOGS VIDE

FRONT PAGE | POLITICS | ENTERTAINMENT | WORLD | TECH | MEDIA | GREEN

Business | Small Business | Money | The Watchdog | Occupy Wall Street

Global Payments Security Breach: Firm Dropped By Visa After 1.5 Million Credit Card Numbers Possibly Exposed

April 16, 2012

Monday, April 16, 2012 As of 8:21 PM EDT New York 89°|74°

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Comm

World | U.S. | New York | Business | Markets | Tech | Personal Finance | Life &

Small Business

Asia | Europe | Earnings | Economy | Health | Law | Autos | Management | Media & Marketin

BUSINESS | Updated April 16, 2012, 8:21 p.m. ET

Tornadoes Hamper Boeing Supplier

Spirit Says Output Suspended 'At Least' Through Tuesday, Deliveries Could Res of Week

Article | Stock Quotes | Comments

By JON OSTROWER

WICHITA, Kan.—A key Boeing Co. BA +2.51% supplier said it aims to resur deliveries by the end of the week after tornadoes battered its factories here, highlighting the fragility and resilience of the aerospace giant's global supply it works to sharply increase production.

The storms late Saturday caused significant-to-major damage to 10 buildings flagship campus of Spirit AeroSystems Inc., which makes fuselages and oth for Boeing's hot-selling 737, 777 and 787 Dreamliner passenger jets. Spirit ex said production—which normally runs seven days a week—would be suspen least" through Tuesday, and that it expects "near-term production disruptions including delivery impacts" to customers.

Spirit spokesman Ken Evans sa assessments found most of its machinery and inventory intact. believe we can use the facilities got," he said in an interview here in Wichita, a major manufacturing hub for the aerospace industry. "We don't

June 10, 2012

Sunday, June 10, 2012 As of 6:32 PM EDT New York 89°|74°

Nader Mehravari

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

Factiva Smar

Search only W

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Community | See What's New in

World | U.S. | New York | Business | Markets | Tech | Personal Finance | Life & Culture | Opinion

Digits | Personal Technology | What They Know | All Things Digital

TECHNOLOGY | Updated June 10, 2012, 6:32 p.m. ET

LinkedIn Defends Reaction in Wake of Password Theft

Service Says It Doesn't Think Any Accounts Were Hacked After Password Theft

Article | Stock Quotes | Comments (9)

By SHAYNDI RAICE And BEN WORTHEN

A A

LinkedIn Corp. LNKD +0.91% moved to reassure customers about the security of their data, following a password theft that caused a black eye for the social-networking service.

LinkedIn said in a blog post over the weekend that it had received no reports that member accounts were breached as a result

View, Calif., company has come under fire sin

and published on an unauthorized website W

Some security experts questioned the adequacy of LinkedIn's procedures for protecting passwords, and some users complained about delays in receiving information about the incident.

Vincente Silveira, a LinkedIn director, defended company said in a blog

In This Art

ORGANIZATIONS

LinkedIn Corporati

SUBJECTS

INDUSTRIES

Internet/Online Se

Social Media

More like this

FROM NYTIMES.

LinkedIn Breach

FROM THE NEW Z

LinkedIn co

LinkedIn Says It Spent $1 Million Trying To Solve Its Password Theft

LinkedIn

June 12, 2012

Tuesday, June 12, 2012 New York 89°|74°

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Community

World | U.S. | New York | Business | Markets | Tech | Personal Finance | Life & Cul

Election 2012 | Washington Wire | The Obama Budget | Capital Journal | Economy | San Francisco Bay

U.S. NEWS | Updated June 12, 2012, 12:35 a.m. ET

Brain-Bank Freezer Glitch Hits Research on Autism

A freezer malfunction extensively damaged one of the world's largest collections of brain samples for autism research, a hospital affiliated with Harvard Medical School said.

The Harvard Brain Tissue Resource Center at McLean Hospital in Belmont, Mass., said Monday it is investigating what caused the temperature in a freezer to rise without sounding two backup alarm systems.

The freezer had stored 150 brain specimens, including 53 earmarked for research into causes and treatments of autism, a condition characterized by poor social skills and difficulties with communication.

The brain specimens are part of a collection of 168 brains belonging to Autism Speaks Inc., a New York advocacy gr
center. The brains were dona

Francine Benes, director of th
research. "The question is by

Freezer Glitch at Autism Brain Bank Sets Back Research

The world's largest collection of autism brains at Harvard-affiliated McLean Hospital is badly damaged because of a freezer failure, dealing what could be a 10-year setback to autism research.

July 12, 2012

Thursday, July 12, 2012 As of 4:43 PM EDT New York 89°|74°

THE WALL STREET JOURNAL.
PROFESSIONAL WITH FACTIVA

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Community

World | U.S. | New York | Business | Markets | Tech | Personal Finance | Life & Culture

Digits | Personal Technology | What They Know | All

TECHNOLOGY | Updated July 12, 2012, 4:43 p.m. ET

Yahoo Passwords Stolen in Latest Data Breach

Article | Video | Stock Quotes | Comments (12)

By DREW FITZGERALD

Yahoo Inc. YHOO +0.32% said it is investigating a data breach that allowed a hacker group to download about 453,000 unencrypted user names and passwords in another black eye for the Internet company.

The Sunnyvale, Calif., company said
belongs to Yahoo Voices, a self-publ
A hacking organization called D33Ds
appended a note describing the download "as a wake-up call and not as a threat." The
group said it aims to expose Yahoo's

Yahoo hacked, 450,000 passwords posted online

Yahoo sued over stolen usernames and passwords

Some people registered for the Yahoo
using email addres

July 27, 2012

Friday, July 27, 2012 New York 81°|71°

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Community

World | U.S. | New York | Business | Markets | Tech | Personal Finance | Life & Cul

Digits | Personal Technology | What They Know

TECHNOLOGY | July 27, 2012

Data-Center Failures Hit Twitter Users

By SHIRA OVIDE

Twitter Inc. said that failures in its computer-data centers were the cause of an outage on Thursday that prevented some users from accessing the short-messaging service.

The Twitter blackout lasted up to t
restored about 1:30 p.m. Eastern
president of engineering, said an
He wrote that a system in Twitter's
well. "What was noteworthy about
parallel systems at nearly the sam
aggressively in our systems to avo

The timing of the outage came as Twitter has bee[illegible]g up for a big push with the Olympics, which kick off Friday. Twitter has devoted resources to encouraging Olympic athletes to post messages, and the company also struck a partnership with Comcast Corp.'s CMCSA +1.20% NBCUniversal to launch a website showing Twitter posts from

Twitter apologizes, blames data center failures for outage

The company said that a coincidental failure of two parallel data center system left people without the micro-blogging service.

July 31, 2012

Tuesday, July 31, 2012 As of 12:30 PM EDT New York 81°|71°

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Community

World | U.S. | New York | Business | Markets | Tech | Personal Finance | Life & Cult

Asia | Europe | Earnings | Economy | Health | Law | Autos | Management | Media & Marketing

BUSINESS | Updated July 31, 2012, 12:30 p.m. ET

India's Power Grid Collapses Again

Article | Slideshow | Stock Quotes | Comments (120)

By SAURABH CHATURVEDI And SANTANU CHOUDHURY

NEW DELHI--Much of India's electricity supply network collapsed Tuesday in the country's second major outage in two days, affecting more than 680 million people —double the population of the U.S.—and causing business losses estimated to run into the hundreds of millions of dollars.

Thousands of offices and factories had to switch to generators or shut shop, more than 200 trains were brought to a standstill while hospitals had to ask nurses to manually work critical equipment such as ventilators as 21 provinces experienced a near-total

India electricity grids fail leaves 620 million people without power

August 3, 2012

Friday, August 3, 2012 As of 3:05 PM EDT New York 93°|74°

THE WALL STREET JOURNAL.
PROFESSIONAL WITH FACTIVA

U.S. Edition Home | CFO Journal | CIO Journal | Today's Paper | Video | Blogs | Journal Community

World | U.S. | New York | Business | Markets | Tech | Personal Finance | Life & Cult

TECHNOLOGY | August 3, 2012, 3:05 p.m. ET

Reuters News Site Hacked

Article | Comments (7)

By SHALINI RAMACHANDRAN

Thomson Reuters Corp. said Friday that its blogging platform for Reuters News hacked, resulting in multiple false posts to its website, including a fake interview Syrian rebel army leader.

"Reuters did not carry out such an interview and the posting has been deleted international news service posted Friday on Twitter.

Reuters didn't release any details about who was responsible for the attack. "W working to address the problem," a spokeswoman said in a statement.

According to Reuters, a false blog post attributed to one of its reporters, conta interview with the Free Syrian Army leader Riad al-Asaad, saying that his force going to retreat from Aleppo, a northern Syrian province, after encountering th army. For months, the Free Syrian Army has been fighting the Syrian governm control of the country.

Reuters said the Free Syrian Army released a statement saying that the intervi took place and blamed Syrian President Bashar al-Assad's government for the

Reuters said its journ

REUTERS EDITION: U.S. Regis

Home | Business | Markets | World | Politics | Tech | Opinion | Breakingvie

Reuters Twitter account hacked, false tweets about Syria sent

Recommend 74 recommendations. Sign Up to see what your friends recommend.

Sun Aug 5, 2012 8:19pm EDT

(Reuters) - Reuters News said one of its Twitter accounts was hacked on Sunday and false tweets were posted, mainly related to the current armed struggle in Syria.

"Earlier today @ReutersTech was hacked and changed to @ReutersME," said a spokesperson for Reuters, which is owned by Thomson Reuters CorpTO>. "The account has been suspended and is currently under investigation."

The incident follows the company's disclosure that the blogging platform of the Reuters News website was compromised on Friday and a false posting purporting to carry an interview with a Syrian rebel leader was illegally posted on a Reuters' journalist's blog.

In the latest incident a series of 22 false tweets were sent purporting to be from Reuters News. Some of the tweets also carried false reports about Syrian rebel losses suffered in battles with Syrian government forces.

Tweet 542 | Share | Share this | +1 3 | Email | Print

Related News

Syrian leader Assad's plant pound vital p Aleppo
Sat, Aug 4 2012

Syrian army on rebels in Al Damascus
Fri, Aug 3 2012

Reuters blo

REUTERS

U.S. Power Plant Hit by USB-Based Malware

January 16, 2013

By Chloe Albanesius | January 16, 2013 03:14pm EST | 21 Comments

A U.S.-based power plant was hit with a malware attack thanks to an infected USB stick used for software updates.

The incident was revealed in a new report from th U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The power plant contacted CERT after discovering a virus in a turbine control system that impacted about 10 computers on its control system network, and affected operations for about three weeks.

The USB drive in question was used to back up control system configurations. However, when th technician - who was not aware of the malware - inserted the USB stick into a computer with antivirus software, it picked up on at least three incidents of malware.

"Initial analysis caused particular concern when one sample was linked to known sophisticated malware," according to CERT, which deployed a team in October for an on-site inspection.

That team found the malware on two engineering workstations that were "critical to the operation of the control environment." Compounding the problem was the fact that there

What do they all point to?

The Washington Post

No timetable set for return of Va. DMV licensing service

By Derek Kravitz
Washington Post Staff Writer
Wednesday, September 1, 2010

A computer outage that has wreaked havoc on Virginia state agencies entered its seventh day Wednesday, and officials acknowledged that the failure was more complicated than they originally thought.

Disruptive Events

BBC Mobile | News | Sport | Weather | Travel

NEWS BUSINESS

28 November 2011 Last updated at 14:44 ET

Thailand factory output slumps on severe flooding

Thailand's factory output fell by 36.8% in October after the country's worst flooding for 60 years.

The floods hit seven of the country's largest industrial estates, which are a hub for component makers for the car and electronics industries.

Output of hard disk drives fell 50.4% in October, while production of electronics fell 45.5%.

Car production, which is based in eastern Thailand away from the floods, fell 61.3% due to parts shortages.

Related

Thailand's flooding killed more than 100

COMPUTERWORLD

Subscribe to a Newsletter

Sony cuts off Sony Online Entertainment service after hack

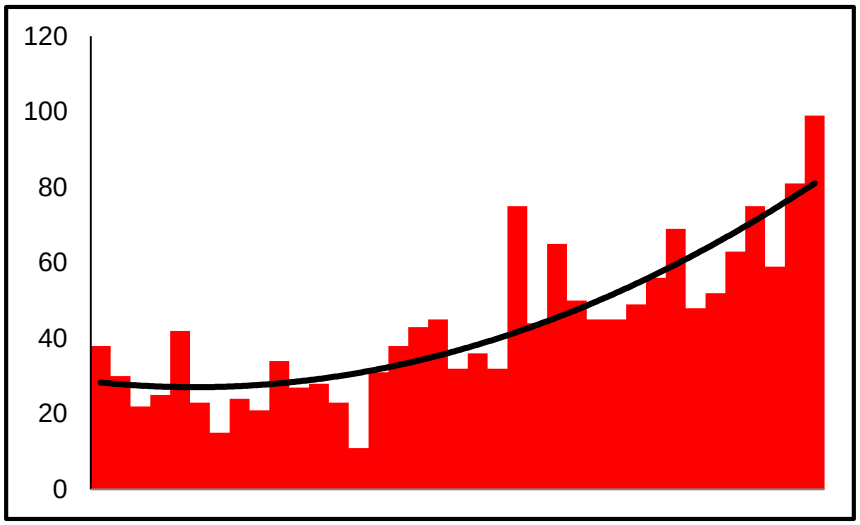
By Robert McMillan
May 2, 2011 09:17 PM ET

Comments (5) Recommended (45) Like 144

IDG News Service - The widely publicized hack of Sony's computer networks is worse than previously thought, also affecting 24.6 million Sony Online Entertainment network accounts.

Sony -- which has kept its Sony PlayStation Network offline for nearly two weeks as it investigates a computer intrusion -- took a second gaming

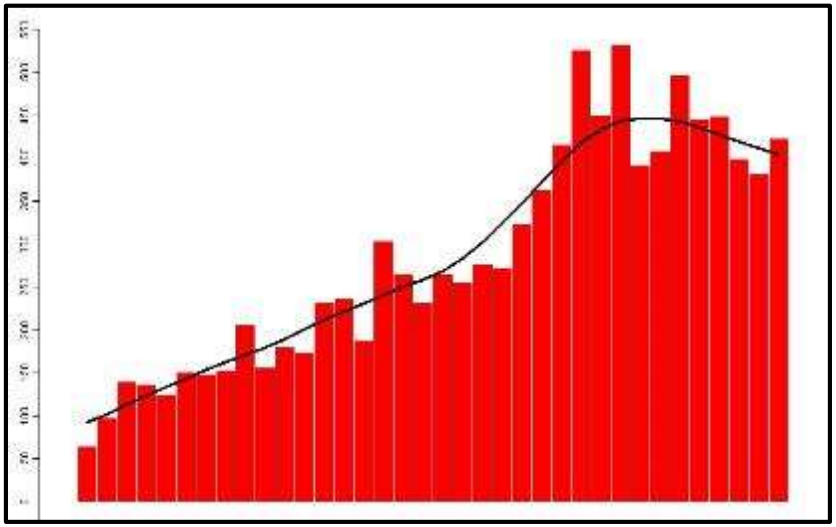
Are there more disruptive events?



Federal Emergency Management Agency

US Declared Disasters

1975-2011



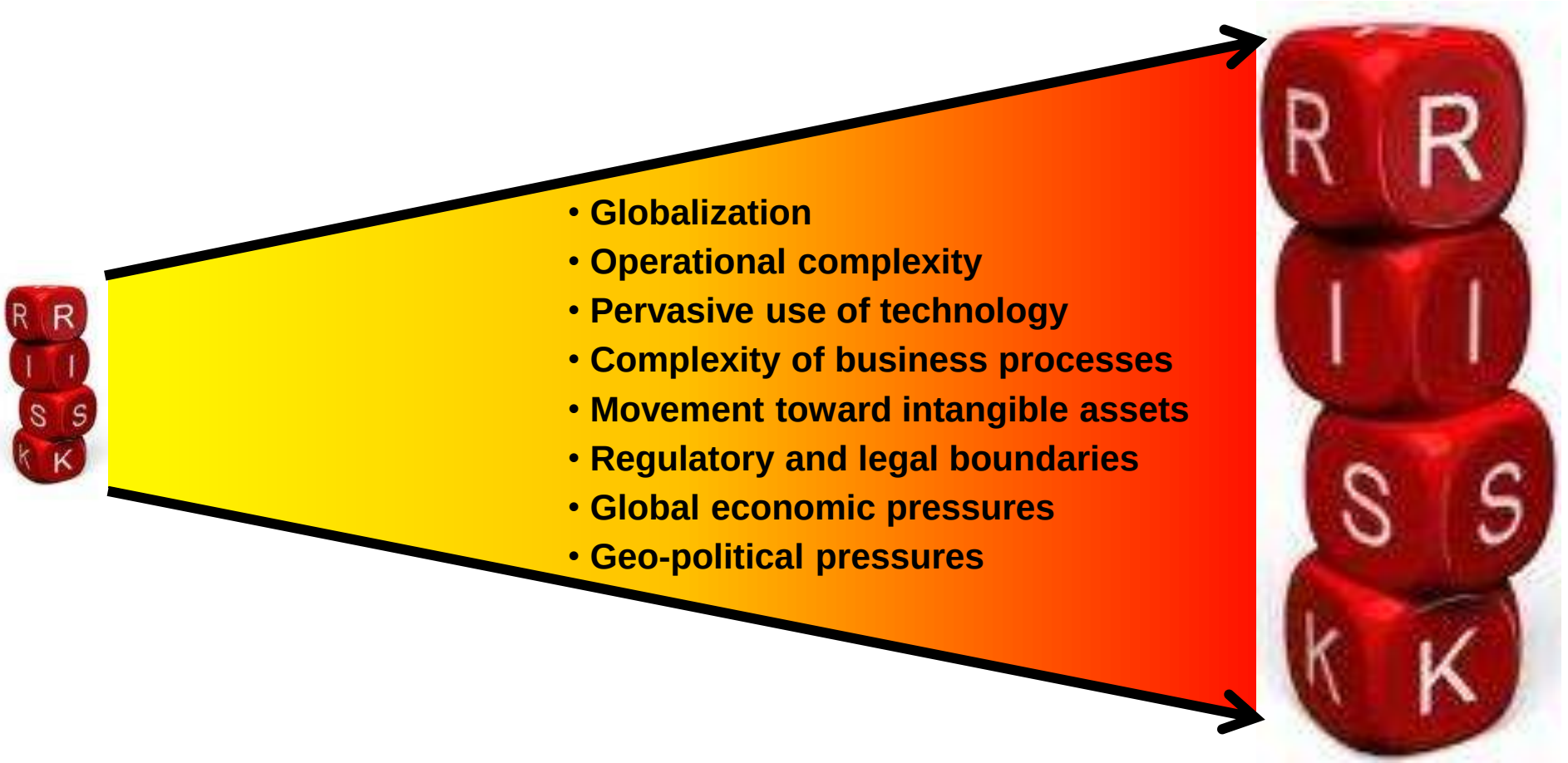
The International Disaster Database

Worldwide Disasters

1975-2010

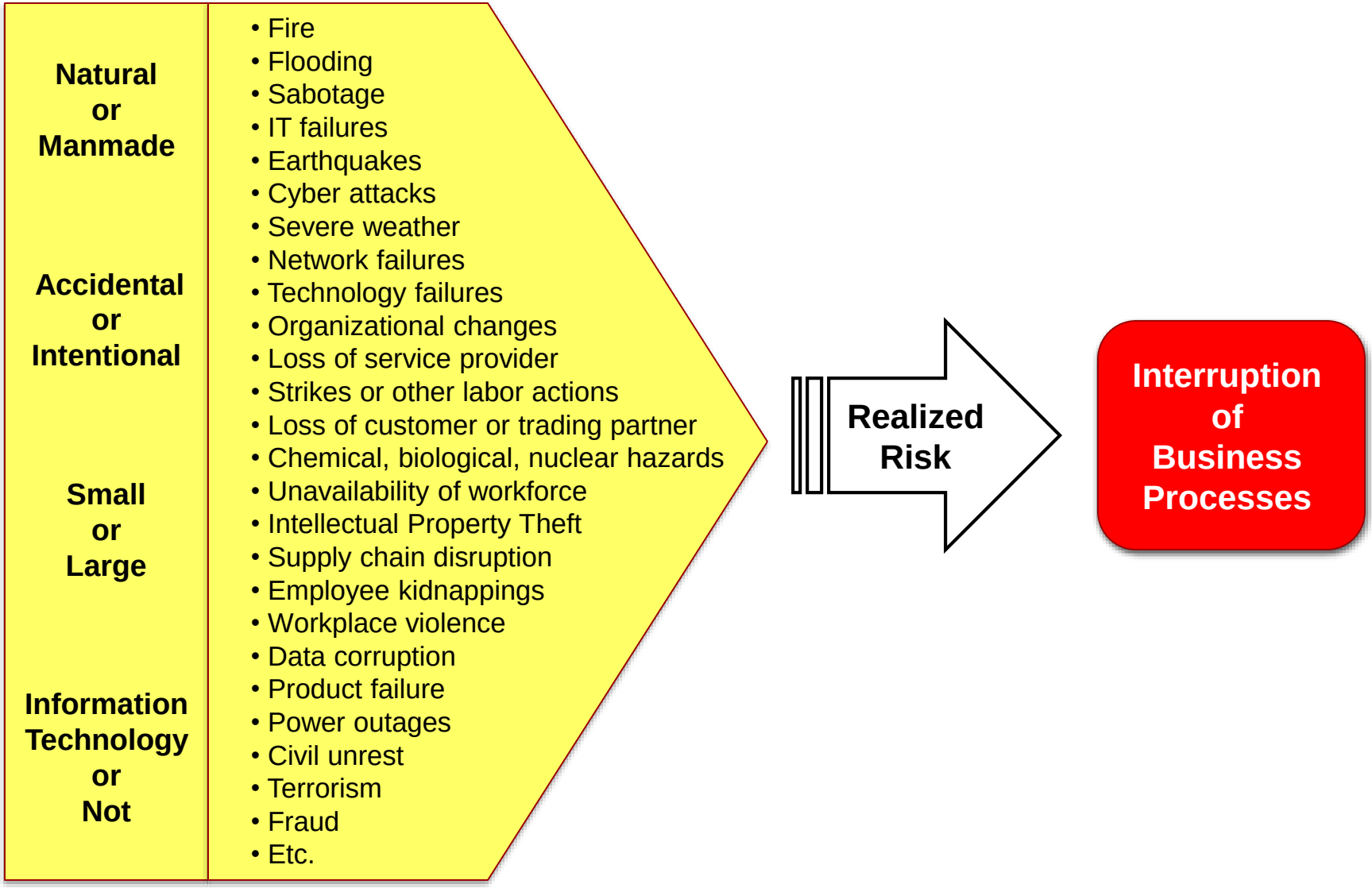
There **appears** to be; But, is that right question to ask?

What is the Right Question to Ask?

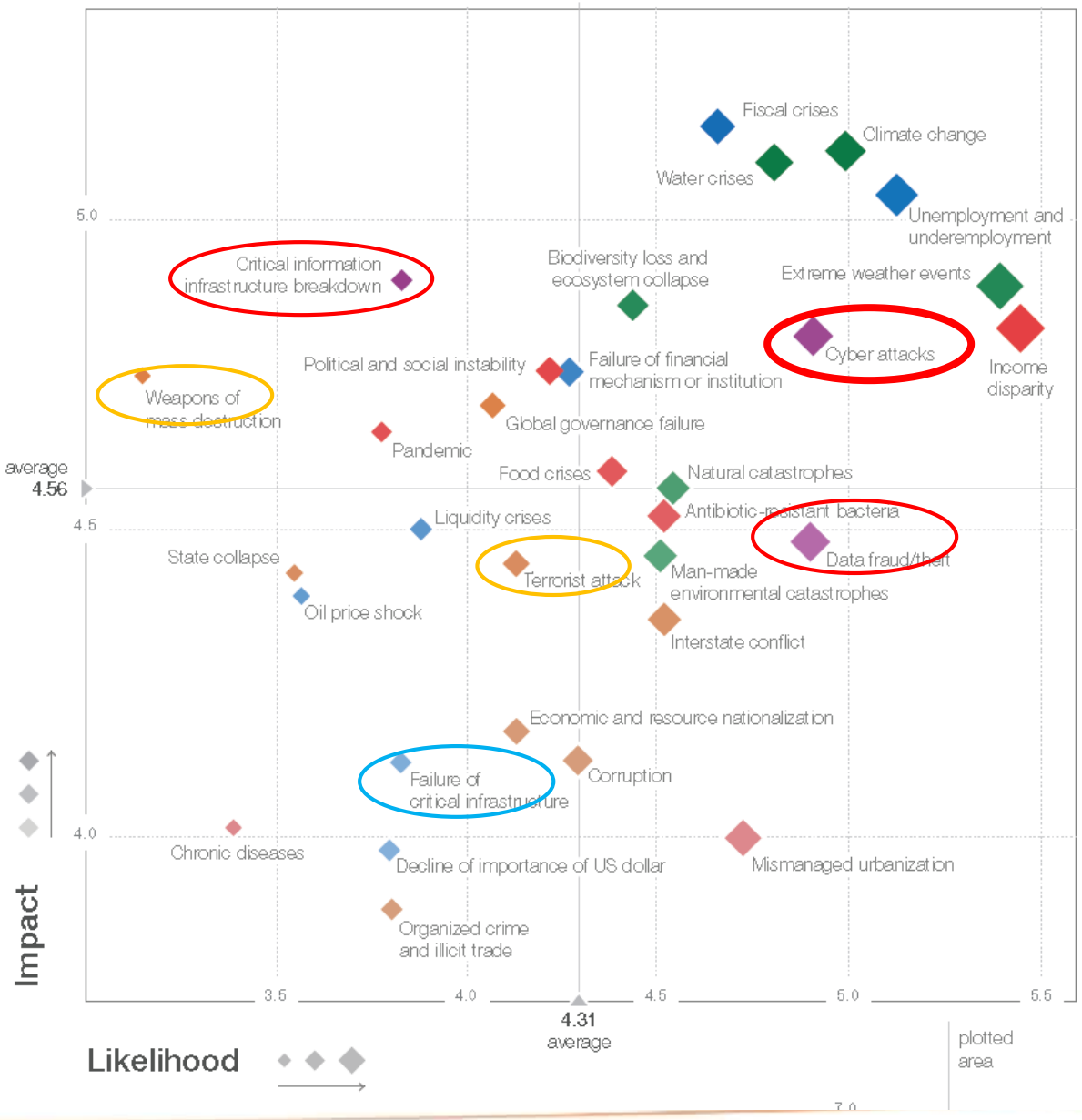


Is the Risk Environment Expanding?

Disruptive Events

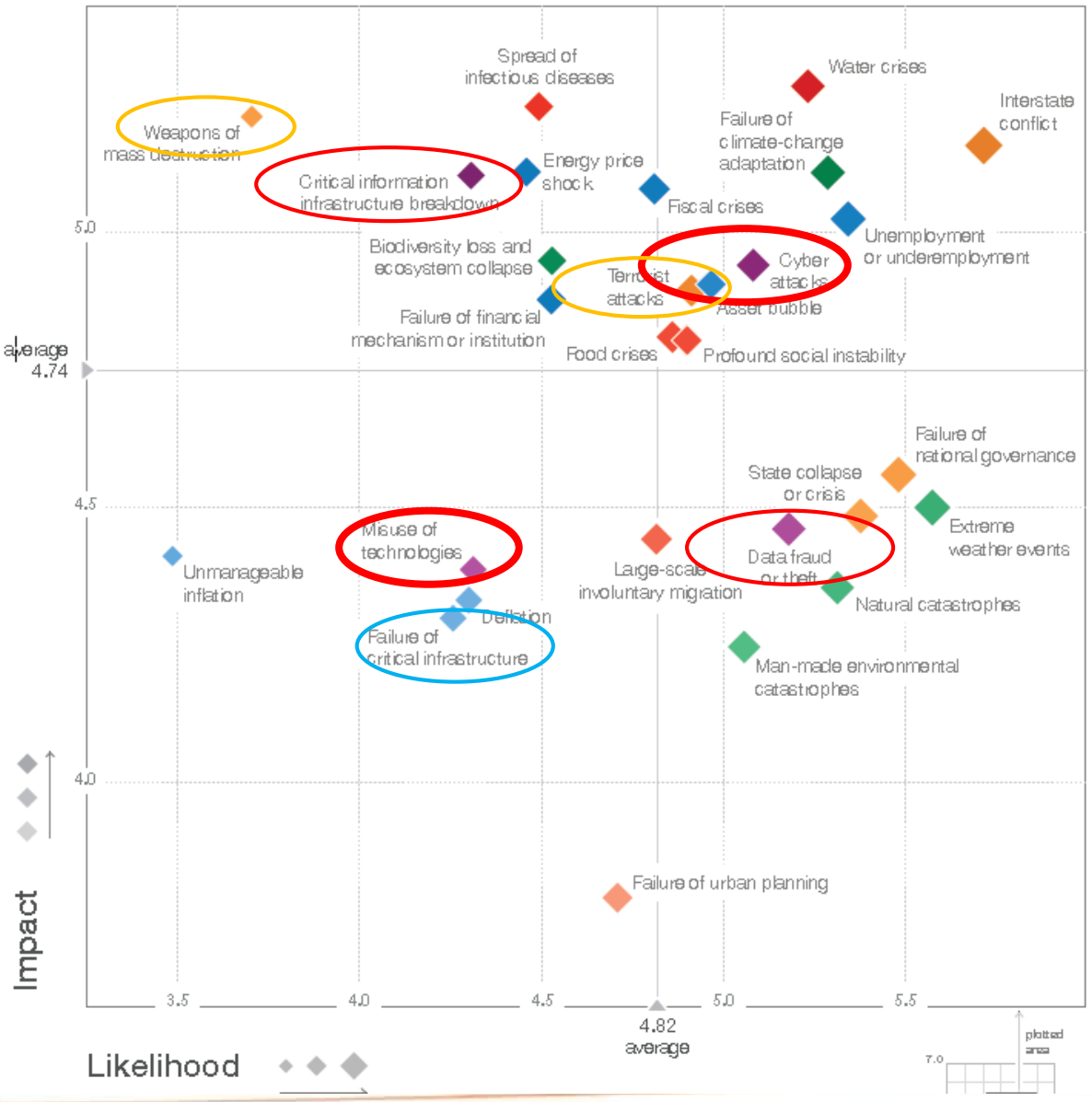


The Global Risk Landscape - 2014



Source: World Economic Forum, "Global Risks 2014, 9th Edition

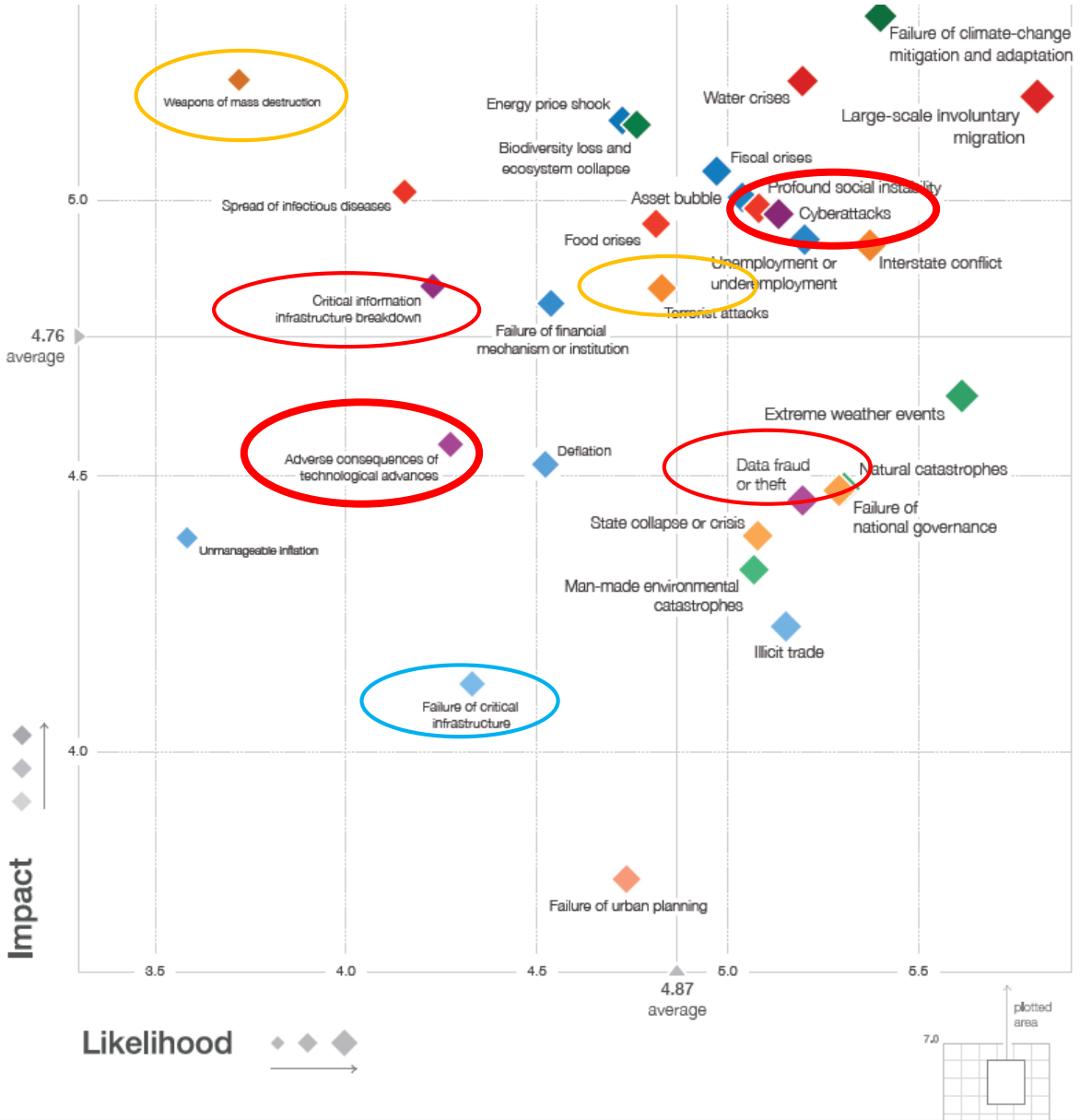
The Global Risk Landscape - 2015



Source: World Economic Forum, "Global Risks 2015, 10th Edition

The Global Risk Landscape - 2016

WORLD ECONOMIC FORUM



Source: World Economic Forum, "Global Risks 2015, 10th Edition

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Global Agenda Council on Risk & Resilience

Resilience Insights

1. Building Resilience to Water Crises

2. Building Resilience to Large- Scale Involuntary Migration

3. Building Resilience to Large- Scale Cyberattacks

NEW

Building Resilience to Large-Scale Cyberattacks

Background

As the Fourth Industrial Revolution [illegible], the pace of technological [illegible] also brings with it new [illegible]ilities (see the Global Risks [illegible] for a detailed discussion). [illegible] these vulnerabilities are [illegible]d with increasing global digital [illegible], cyber systems and [illegible] the data they hold

Internet, automation of knowledge work, the Internet of Things and cloud technology will be the most disruptive".[50] While this innovation will result in new efficiencies and capabilities, it will also introduce new vulnerabilities, allowing attackers to quickly evolve their tactics and exploit unaddressed system and network weaknesses.

Further compounding the risk is today's hyperconnected global environment, where people and things, critical infrastructures and economies are increasingly digitally connected – anytime and anywhere. According to this year's Global Risks Report 2016, *"As the Internet of Things leads to more connections between people and machines, cyber dependency due to increasing digital interconnection of people, things and organizations – considered by survey respondents as the third most important global trend – will increase."*[51] This hyperconnectivity ties the risk of one entity to all entities with which it shares a connection, thereby multiplying the ways through which an attacker could gain access to systems and data. Similarly, it increases the potential for cascading consequences resulting from a cyberattack or cyber disruption.

Although many entities are poised to reap the benefits of technological

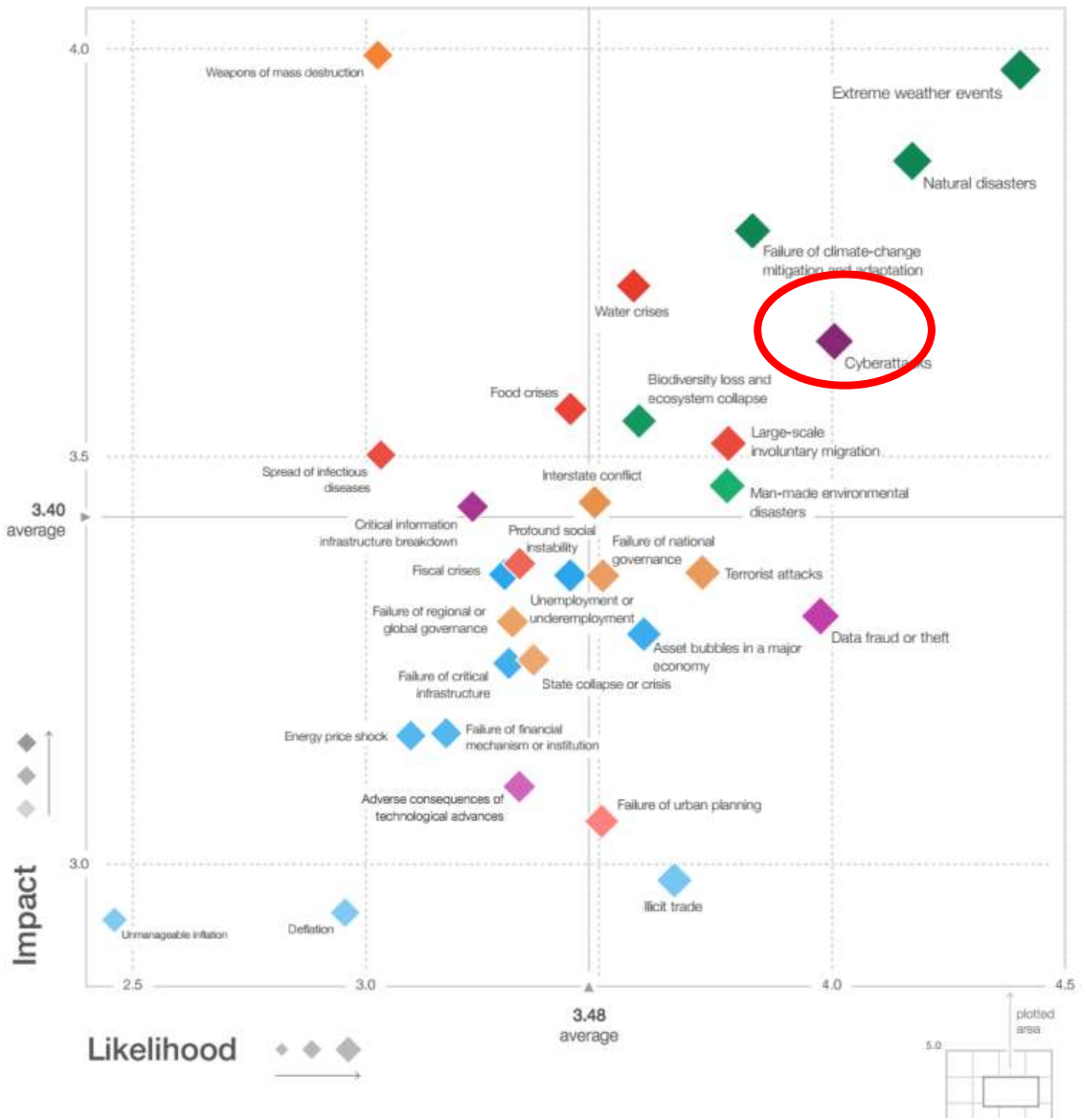
and capabilities for readiness, respo… reconstitution and reinvention. Building resilience to large-scale cyberattacks requires a concerted effort towards advancing the understanding of and the disciplines that contribute to cyber resilience. This section posits a number of suggestions on how to improve the cyber resilience of organizations. Some require action by governments and some can be taken by all entities – public or private/big or small.

Recommendations

A. Increase Understanding of Risk of Large-Scale Cyberattacks and other Cyber Threats

As described above, it is clear that the dramatic pace of technological innovation today, coupled with widespread global connectivity and vast amounts of data creation, have resulted in increasing risk to cyber assets and online networks. The risk of large-scale cyberattacks continues to feature as a high impact/high likelihood risk in the Global Risks Landscape 2016 (Figure 1) – although overshadowed by environmental and societal risks. However, it is worth noting that the overall perception of the significance of large-scale cyberattacks and a closely connected risk, the **breakdown of**

Figure I: The Global Risks Landscape 2018



January 25, 2018
WEF, Davos

To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity

enisa
European Network and Information Security Agency

New dependencies: new vulnerabilities

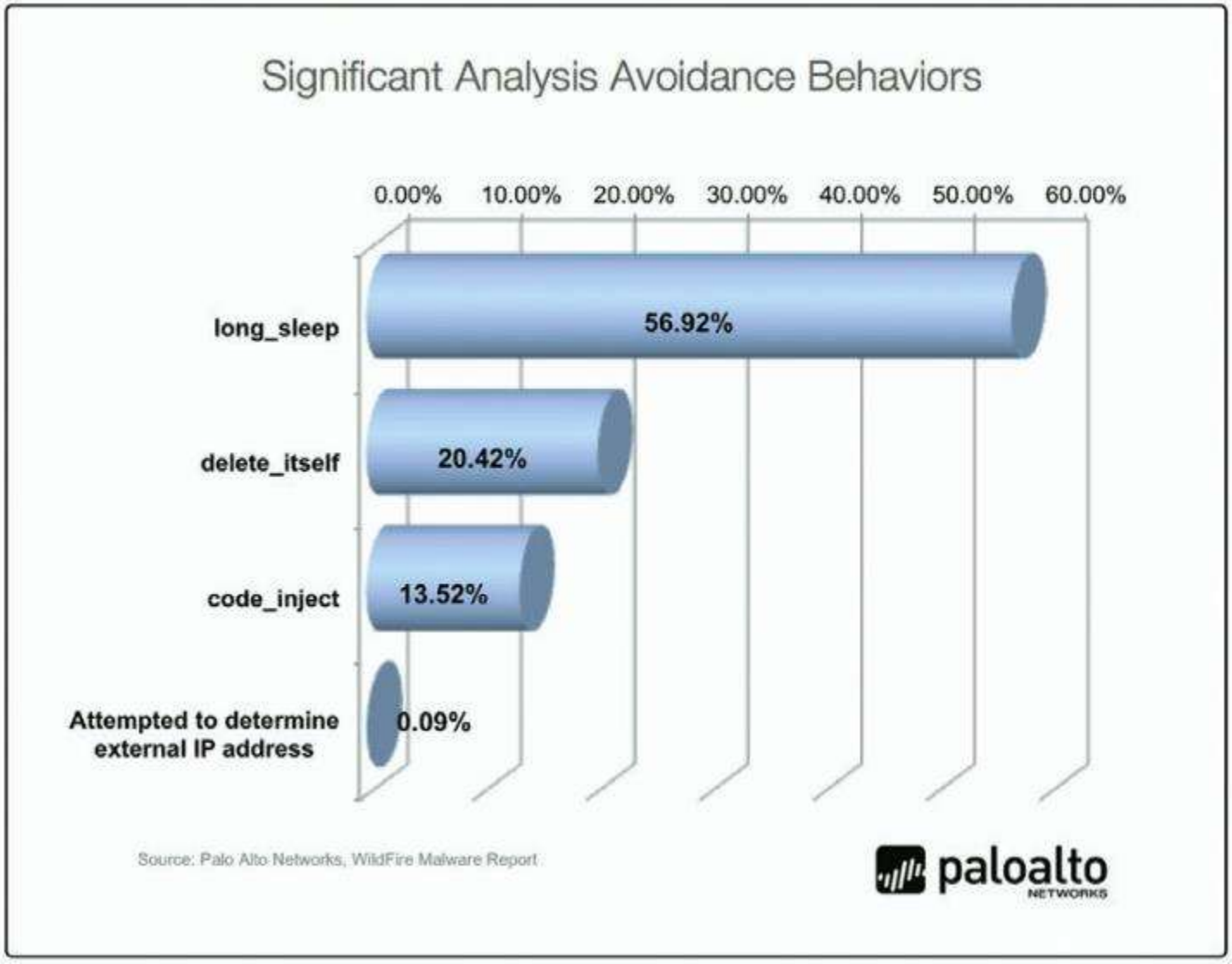
Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Computing	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtualisation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑
11. Insider threat	→	↑		↑		↑	↑	↑
12. Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13. Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14. Cyber espionage	↑	↑		↑	↑	↑		↑
15. Ransomware/ Rogueware/ Scareware	↓		↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⊃	1. Malware	⊃	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	⊃	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	⊃	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	⊃	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	⊃	10. Physical manipulation/ damage/ theft/loss	⊃	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Modern malware – behavior on the host



May 29, 2012 "hiding" or "stealth" – for how long?

Flame virus went undetected for **two years !**

lated items

er computer virus let
e to 'wage cyber war
an and Russia'

ebook investigates
displaying hardcore
on users' newsfe

gle TV fi
ita
set to
ory with new
ent editing tab

ne 5 release: Anger at
rts new connector will
e accessories
lete

test blog posts

Terror bytes: The Flame virus is part of a new type of malware software

Operation "Red October"

Victims of advanced cyber-espionage network

5 years !

KASPERSKY lab

An Amazon Echo may be the key to solving a murder case

November, 2015

Posted Dec 27, 2016 by Sarah Buhr (@sarahbuhr)

Next Story

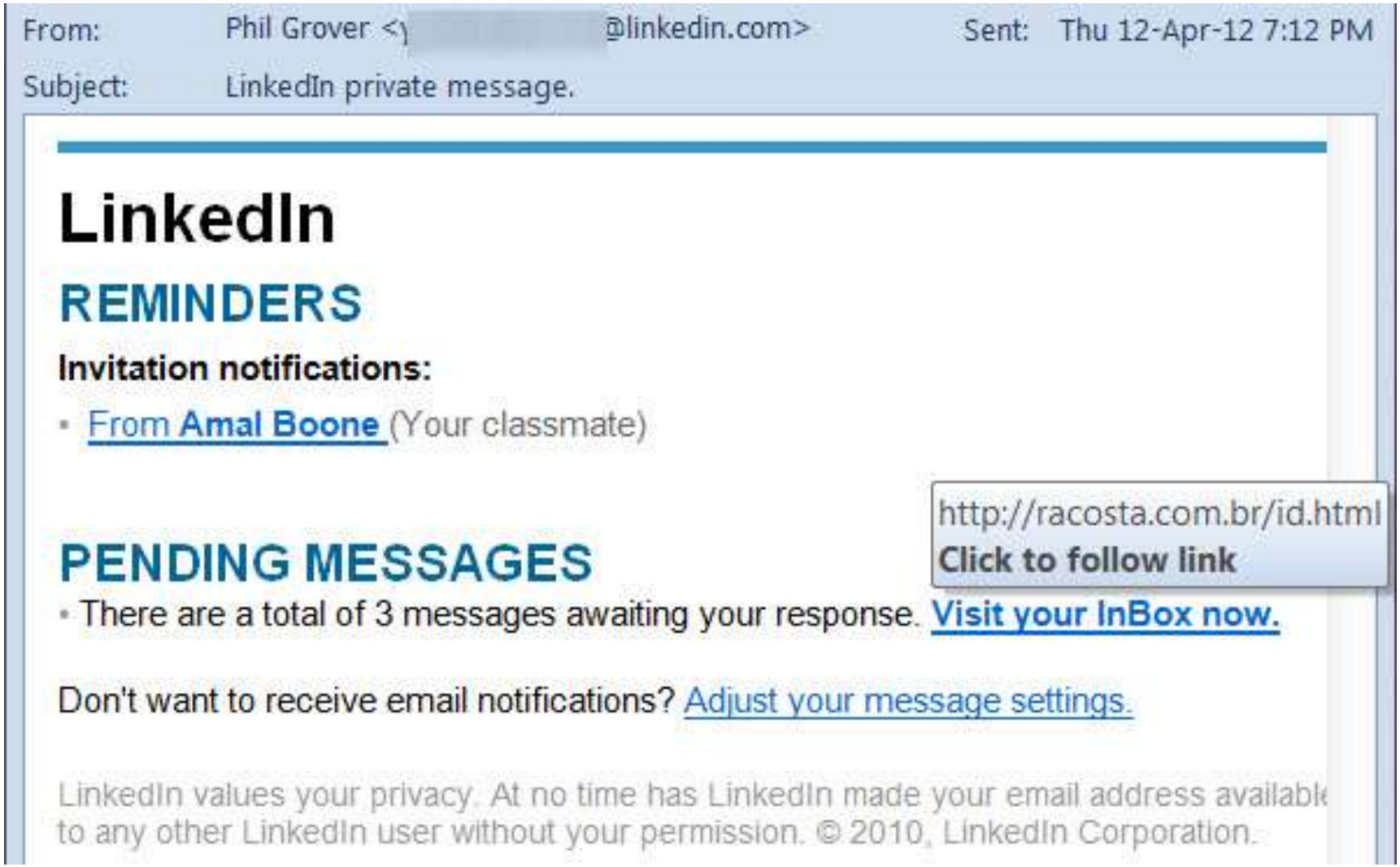
Internet-connected devices may start helping in criminal cases. As first reported in The Information, police in Bentonville, Arkansas have issued a warrant to Amazon, asking the company to hand over data from an Echo device to help prosecute a suspected murderer.

James Andrew Bates, the suspect in the case, was charged with first-degree murder in November of 2015 after authorities found victim Victor Collins strangled and drowned in Mr. Bates' hot tub.

Mr. Bates told police he'd invited Collins and two other friends, Owen McDonald and Sean Henry, over to watch a football game and said he decided to go to bed about 1 a.m., leaving the victim

https://techcrunch.com/2016/12/27/an-amazon-echo-may-be-the-key-to-solving-a-murder-case/

It looks so usual …



From: Phil Grover <[redacted]@linkedin.com> Sent: Thu 12-Apr-12 7:12 PM

Subject: LinkedIn private message.

LinkedIn

REMINDERS

Invitation notifications:

- From **Amal Boone** (Your classmate)

http://racosta.com.br/id.html
Click to follow link

PENDING MESSAGES

- There are a total of 3 messages awaiting your response. **Visit your InBox now.**

Don't want to receive email notifications? Adjust your message settings.

LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. © 2010, LinkedIn Corporation.

racosta.com.br/id.html

NOTIFICATIONS

Invitation notifications: • From Baker Barry (Your Colleague)

In the background, several scripts seek out software with vulnerabilities that can be exploited including:

- Adobe reader and Acrobat: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188
- Microsoft Windows Help and Support Center in Windows XP: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1885

From: messages-noreply@bounce.linkedin.com on behalf of

To: Avi Turiel

Cc:

Subject: Invitation to connect on LinkedIn

LinkedIn

From Translations

Project Manager at

I'd like to add you to my professional network on LinkedIn.

- Globus

Confirm that you know

You are receiving Invitation to Connect emails. Unsubscribe

© 2012, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, US

"You can use this system to modify approximately everything related to the navigation of the plane, That includes a lot of nasty things."

April 12, 2013

Hacker says phone app could hijack plane

By Doug Gross , CNN
updated 8:27 AM EDT, Fri April 12, 2013 | Filed under: Mobile

CNN.com

Hugo Teso, a security analyst and licensed pilot, says he's developed software that could steal control of an airplane.

(CNN) -- Could this be the deadliest smartphone app ever?

A German security consultant, who's also a commercial pilot, has demonstrated tools he says could be used to hijack an airplane remotely, using just an Android phone.

Speaking at the Hack in the Box security summit in Amsterdam, Netherlands, Hugo Teso said Wednesday that he spent three years developing SIMON, a framework of malicious code that could be used to attack and exploit airline security software, and an Android app to run it that he calls PlaneSploit.

http://www.cnn.com/2013/04/11/tech/mobile/phone-hijack-plane/

Using a flight simulator, Teso showed off the ability to change the speed, altitude and direction of a virtual airplane by sending radio signals to its flight-management system. Current security systems don't have strong enough authentication methods to make sure the commands are coming from a legitimate source, he said.

IDC: There will be more than – 60 billion connected devices in the world by 2020

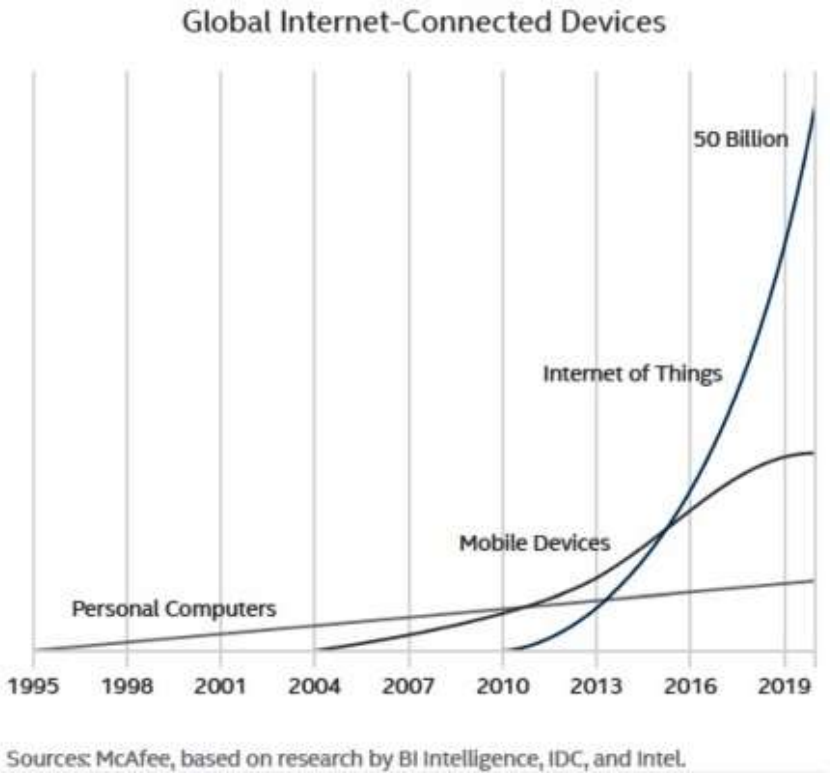
January 17, 2014

t the International Consumer Electronics S

(CNN) -- It's bad enough that
ck trying to scam us with malicio

We now must worry about be
appliances, as well.

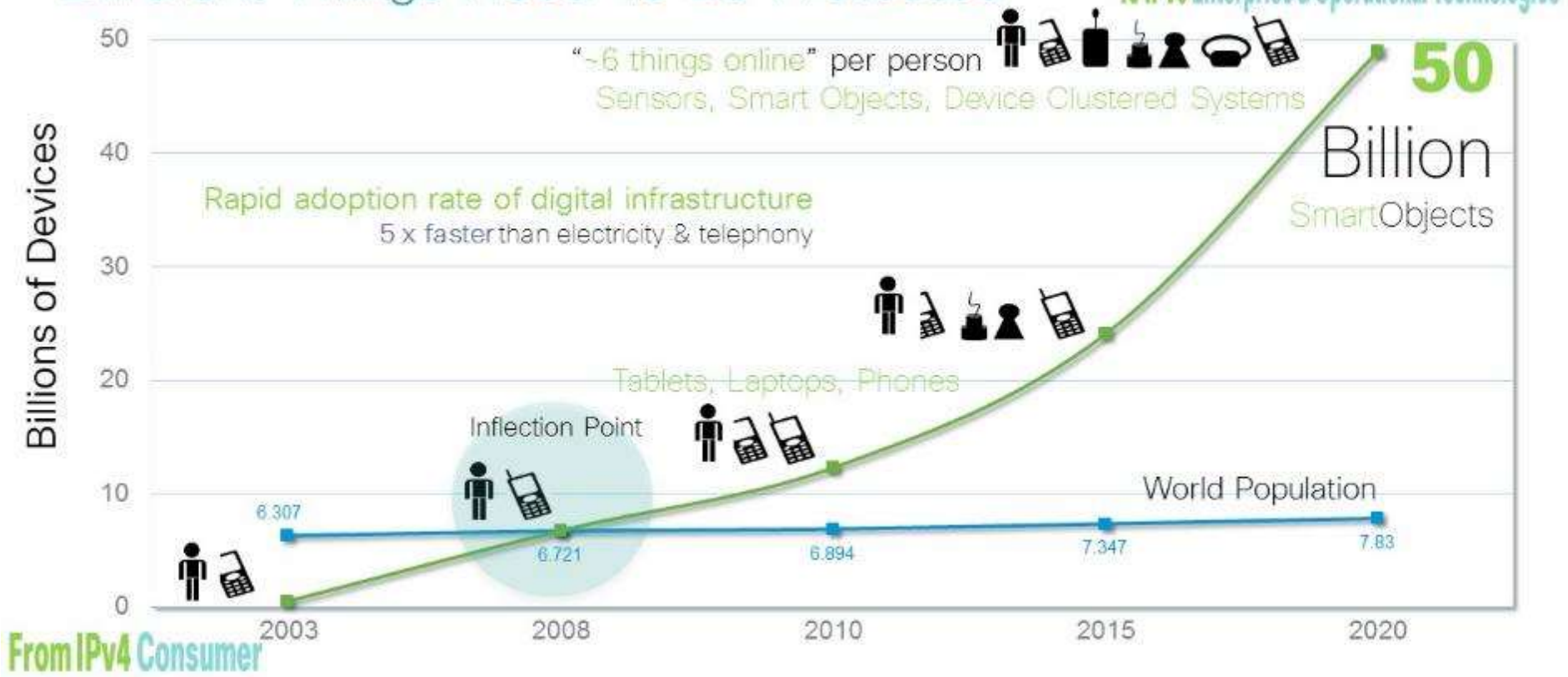
An Internet-security firm has
global cyberattack launched f


Global Internet-Connected Devices
50 Billion
Internet of Things
Mobile Devices
Personal Computers
1995
1998
2001
2004
2007
2010
2013
2016
2019
Sources: McAfee, based on research by BI Intelligence, IDC, and Intel.

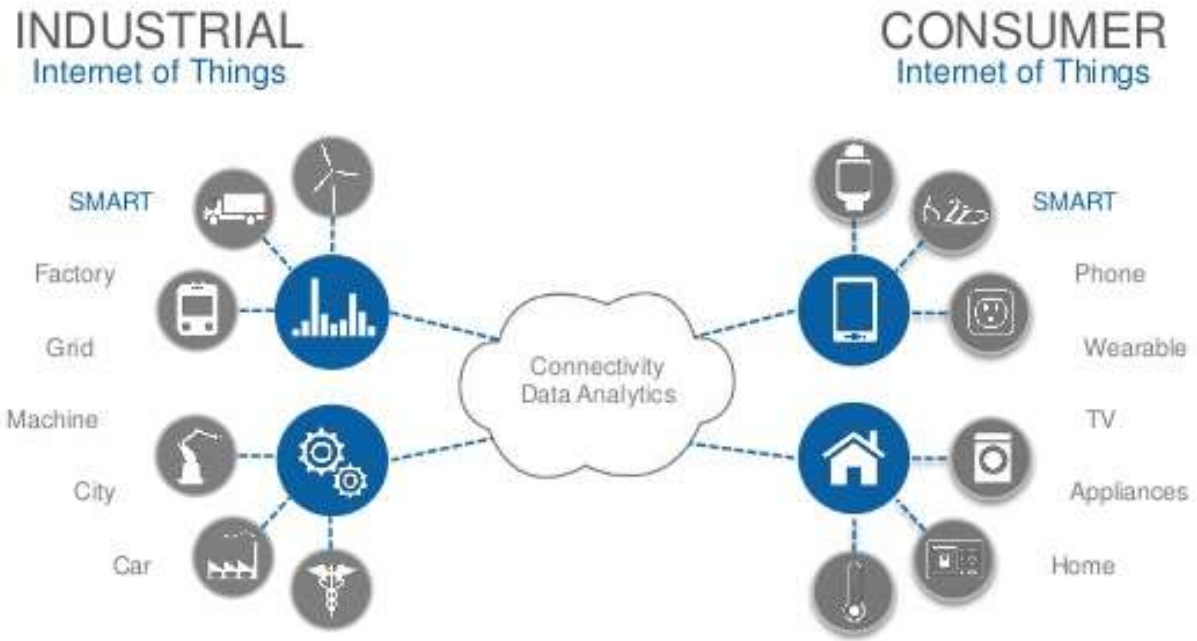

CCTV Botnet in Our Own Back Yard


HUMAN
ORGAN

Different Things Need To Be Protected

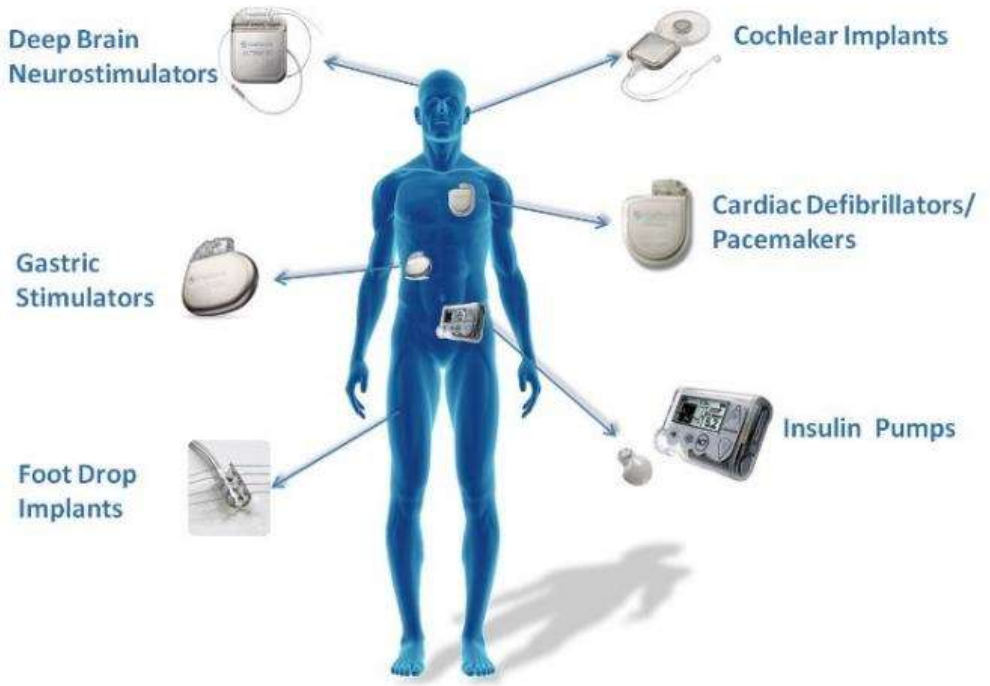


Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf



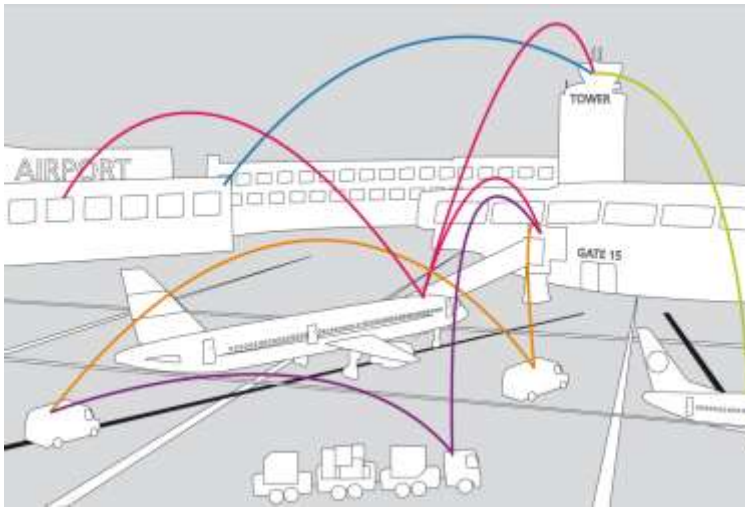
Based on Moor Insights & Strategy's report *Segmenting the Internet of Things (IoT)*

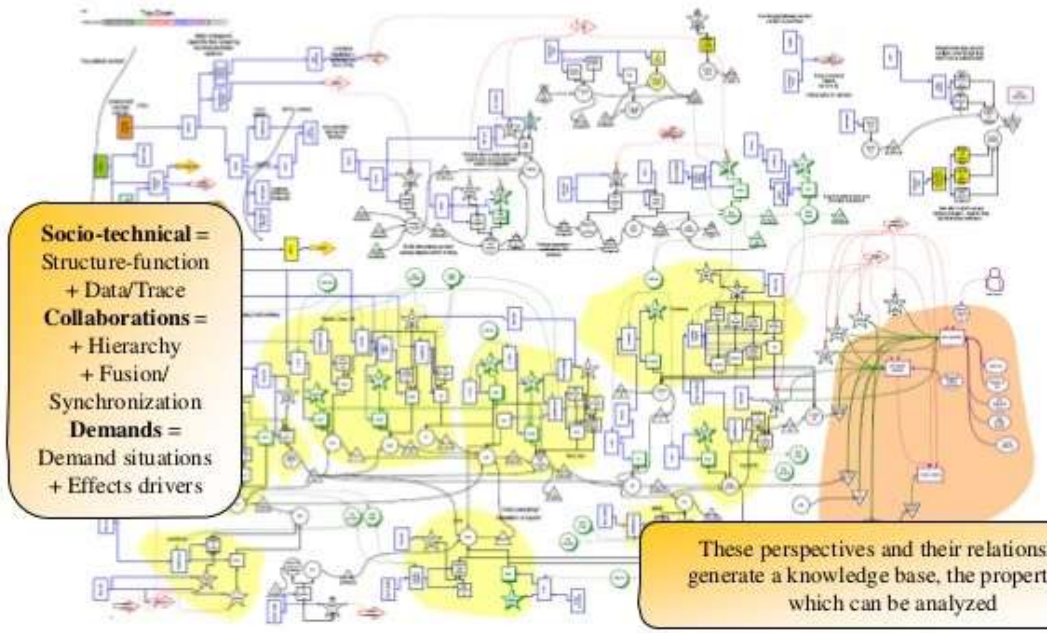
WIRELESS IMPLANTABLE MEDICAL DEVICES




CHEROKEE

Digitized Society (the “fifth domain”) = digital “ecosystem” of
1) Cyber-Physical Systems
2) Complex Systems-of-Systems with emergent behavior





21Oct2015

https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html

https://ipvm.com/reports/hik-backdoor

5Mar2017

Hikvision Backdoor Confirmed

Author: Brian Karas, Published on May 08, 2017

The US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has issued an advisory for vulnerabilities to Hikvision cameras, crediting and confirming the work of researcher Montecrypto who originally disclosed the backdoor in Hikvision cameras.

Backdoor Disclosure

On March 5, 2017, Montecrypto declared:

> I would like to confirm that there is a backdoor in many popular Hikvision products that makes it possible to gain full admin access to the device.

Confirming one week later that:

> One can remotely escalate their privileges from anonymous web surfer to admin.

/advisories/ICSA-17-124-01

IPVM

The world's leading video surveillance information source, IPVM provides the best reporting, testing and training for 10,000+ members globally. Dedicated to independent and objective information, we uniquely refuse any and all advertisements, sponsorship and consulting from manufacturers.

About | FAQ | Contact

MEMBER LOGIN

Login

Password

Login

Air-IT

Sales +44 (0)115 880 0044 Su

IT Support | Managed IT | Cloud | IT Consultancy | Telephony | Connectivity | Con

Air-IT / News / Company News / Cryptolocker Ransomware threats on the rise again

Cryptolocker Ransomware threats on

Friday 18th March 2016

Many businesses are losing critical documents and information through renewed attacks on their computers by new strains of the Cryptolocker Ransomware virus. Find out what you need to know and do to protect yourself.

Cryptolocker attacks are increasingly on the rise. While most have obvious-sounding names like "Paycrypt", "CrypVault" and "Cryptowall" others might sound less harmful such as "Locky".

There are steps you should take to protect yourself since the latest version is more virulent than ever and even more destructive.

How the current types differ from older ones

The Cryptolocker threat first hit the headlines back in 2014, you can find out more about this in our original post – GameOverZeus / Cryptolocker Threat Explained.

How the current types differ from older ones

The Cryptolocker threat first hit the headlines back in 2014, you can find out more about this in our original post – GameOverZeus / Cryptolocker Threat Explained.

The current, so-called 3rd generation, Cryptolocker virus has the following new and threatening features:

Extended scope of attack

- Previously an attack was restricted to common file types such as your Office documents. The new version has extended its scope significantly, so it will make more of your files and information inaccessible. It will also attack files that will affect the computer itself.
- In some cases it can even attack files that have been backed-up to local drives and shared storage on servers.

New Apple Mac versions of Ransomware

- Those of you with Apple Macs have enjoyed a degree of immunity from attacks. This is no longer the case, and there are recently documented cases where Macs have been hit. In this case the ransomware is known as "KeRanger" – these attacks started in early March.

Potential threat to smart phones and tablets

- Industry pundits think it may just be a matter of time before our smartphones and tablets are also vulnerable – read more here.

Malvertising on websites

- The most recent IT industry news has confirmed that computers can be infected through adverts that appear on web sites – known as malvertising.
- Some of these sites belong to large and reputable organisations like the BBC and the New York Times where adverts were hijacked with ransomware that demanded payment in bitcoin to unlock infected computers – read more here.

The Hacker News
Security in a serious way

Android Ransomware now targets your Smart TV, Too!

Tuesday, June 14, 2016 Swati Khandelwal

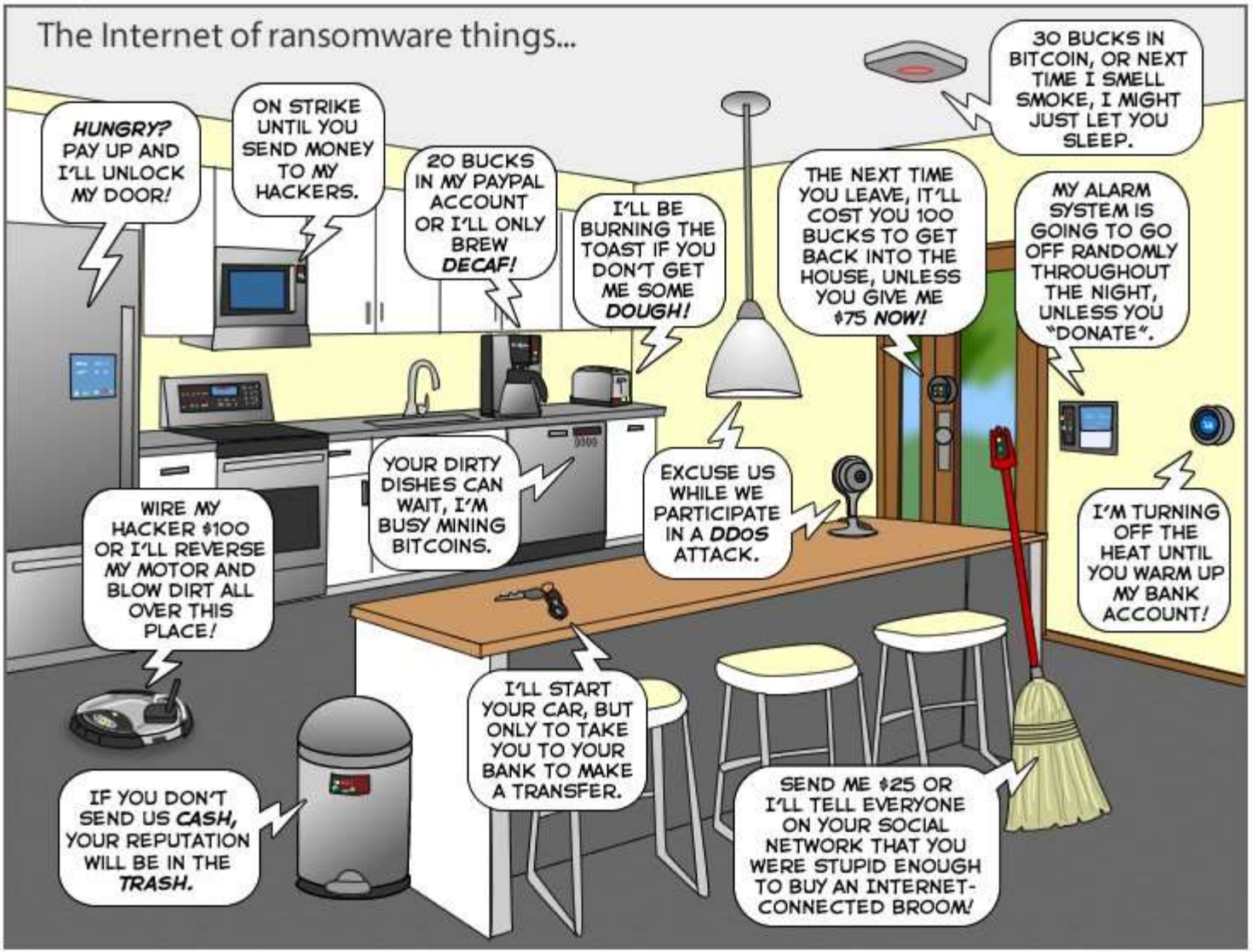
Do you own a Smartwatch, Smart TV, Smart fridge, or any Internet-connected smart device?

If your answer is yes, then you need to know the latest interest of the cyber criminals in the field of Internet of Things.

Ransomware!

After targeting hospitals, universities, and businesses, Ransomware has started popping up on Smart TV screens.

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

June 5, 2013

FACEBOOK
Notorious Zeus banking Trojan is gaining speed on Facebook

Notorious Zeus banking Trojan is gaining speed on Facebook

Suzanne Choney, NBC News

June 5, 2013 at 6:58 PM ET

Malware known as Zeus that can land on a user's computer and steal that user's bank account information is "re-merging with a vengeance" and finding its way onto Facebook. One security firm believes Zeus' reemergence "peaked in May," but is still quite active.

Reuters file

VIDEO GAMES
Valve isn't making one gaming console, but multiple 'Steam machines'

INTERNET
15 percent of adult Americans just say no to Internet use

SOCIAL MEDIA
This is not a test: Twitter

February 17, 2012

News

Crypto researcher Arjen Lenstra shares thoughts on paper blasting RSA cryptosystem

Lenstra: 'If the environment cannot provide enough entropy during key set-up, then RSA becomes a tricky choice'

By Ellen Messmer, Network World
February 17, 2012 01:43 PM ET

Network World - What a week for the RSA cryptosystem! A group of prominent researchers published a paper blasting it as woefully insecure, RSA said there's nothing wrong with the RSA algorithm, it's an implementation issue mainly with random-number key generation, and now the cryptography researcher behind the paper, Arjen Lenstra, signs off the week with a few thoughts about it all.

BACKGROUND: RSA brushes off crypto research findings that RSA algorithm is flawed

"If properly implemented, RSA is fine," said Lenstra, the well-known crypto researcher who worked with James Hughes, Maxime Augier, Joppe Bos, Thorsten Kleinjung and Christophe Wachter on the remarkable project that included examining millions of X.509 public-key certificates that are publicly available over the Web.

That study (explained in the "Ron is wrong, Whit is right" paper) had the researchers examining 6.4 million distinct X.509 certificates and PGP keys containing RSA moduli, and "we stumbled upon 12,720 different 1024-bit RSA moduli that offer no security." They said that "their secret keys are accessible to anyone who takes the trouble to redo our work."

Latest News

- Blackstone proposes counterbid
- Juniper to unveil programmable defined networking
- US senate passes Internet sales
- iPhone 6 rumor rollup for the wee
- FCC chairman announces his res

View more Latest News

Security White Papers

DDoS and Downtime: Consider Management
This paper draws on Verisign's DDo examine the threat of DDoS in the...

http://eprint.iacr.org/2012/064.pdf

Financial Crime Risk

Financial Crime Risk, Fraud and Security

Discussions | Promotions | Jobs | Members | Search

+Follow Doug

Is cybersecurity the next banking crisis in the making? Read the DavidReilly article in the wallstreetjournal to see

Doug Parr
Senior Vice President- North America at ENTERSEKT

WSJ

Hacking into tomorrow's banking crisis online.wsj.com
Any student of history knows that defensive bulwarks are too often built with the last war in mind. A risk for banks is that they and regulators focus too much on problems that led to the last financial crisis.

Like (1) • Comment (4) • Follow • Reply Privately • 4 months ago

Comments

Adrian Donţu likes this

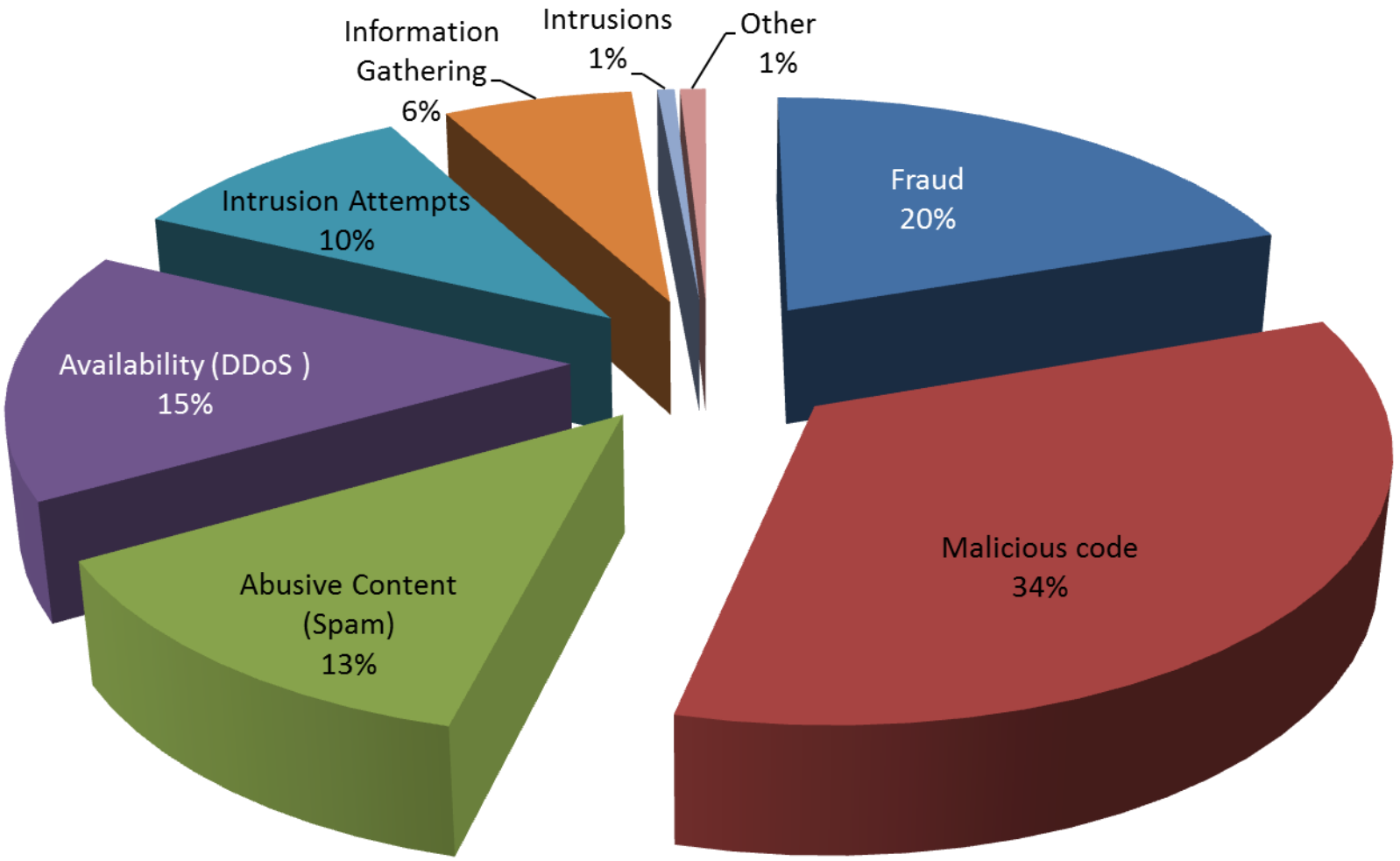
4 comments

Lynn

Lynn Wheeler
virtualization since Jan68, online at home since Mar70

Note at financial conferences in the mid-90s, there were presentations from the consumer dial-up banking groups about moving to the internet ... primary motivation was the enormous support costs for their proprietary dialup banking operations which would be offloaded to ISPs (including they had dozens of different drivers for different dialup modems and each driver had dozens of versions for each version of different operating systems). However, the cash management/commercial dialup banking operations said that they would *NEVER* move to the internet (although most eventually did) because of a long list of (cybersecurity) vulnerabilities (most of which continue to exist to this day).

Bulgaria under “attack”:
Type of incidents to 30th June 2018 (GOV CERT BG)



Ministry of education website defaced (XSS)

February, 2016

Public, private organizations, SMEs as targets
The raise of Cryptolocker/Ransomware

2015-2016

Cryptolocker attacks are increasingly on the rise. While most have obvious-sounding names like "Paycrypt", "CryptVault" and "Cryptowall" others might sound less harmful such as "Locky".

There are steps you should take to protect yourself since the latest version is more virulent than ever and even more destructive.

How the current types differ from older ones

The Cryptolocker threat first hit the headlines back in 2014, you can find out more about this in our original post – GameOverZeus / Cryptolocker Threat Explained.

How the current types differ from older ones

The Cryptolocker threat first hit the headlines back in 2014, you can find out more about this in our original post – GameOverZeus / Cryptolocker Threat Explained.

The current, so-called 3rd generation, Cryptolocker virus has the following new and threatening features:

Extended scope of attack

- Previously an attack was restricted to common file types such as your Office documents. The new version has extended its scope significantly, so it will make more of your files and information inaccessible. It will also attack files that will affect the computer itself.
- In some cases it can even attack files that have been backed-up to local drives and shared storage on servers.

New Apple Mac versions of Ransomware

- Those of you with Apple Macs have enjoyed a degree of immunity from attacks. This is no longer the case, and there are recently documented cases where Macs have been hit. In this case the ransomware is known as "KeRanger" – these attacks started in early March.

Potential threat to smart phones and tablets

- Industry pundits think it may just be a matter of time before our smartphones and tablets are also vulnerable – read more here.

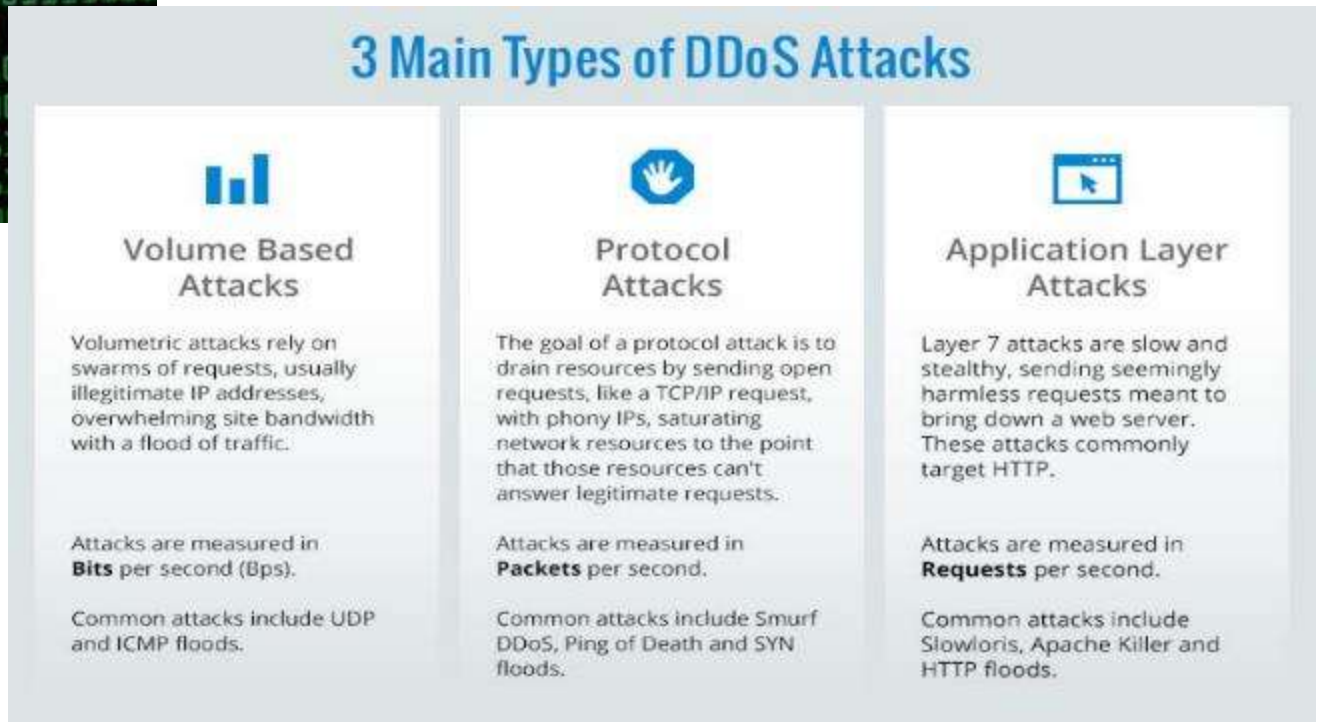
Malvertising on websites

- The most recent IT industry news has confirmed that computers can be infected through adverts that appear on web sites – known as malvertising.
- Some of these sites belong to large and reputable organisations like the BBC and the New York Times where adverts were hijacked with ransomware that demanded payment in bitcoin to unlock infected computers – read more here.

Largest ever DDoS: Elections Oct/Nov 2015

Targets: Election Committee, President, Parliament, Government & Ministries, public and business websites
(> 20 websites, 5-10 days campaign, > 2 bln hits/24h, incl. DNS flooding)

http://ddos-protection-services-review.toptenreviews.com/



ICANN & IDN:
Bulgarian new Cyrillic TLD .бг (.bg)
>>> IDN homograph attack

wikipedia.org

The internationalized domain name (IDN) homograph attack is a way a malicious party may deceive computer users about what remote system they are communicating with, by exploiting the fact that many different characters look alike, (i.e., they are homographs, hence the term for the attack). For example, a person frequenting citibank.com may be lured to click a link in which the Latin C is replaced with the Cyrillic C.

An example of an IDN homograph attack; the "e" and "a" are replaced with Cyrilic letters rather than Latin ones.

This kind of spoofing attack is also known as script spoofing. Unicode incorporates numerous writing systems, and, for a number of reasons, similar-looking characters such as Greek O, Latin O, and Cyrillic O were not assigned the same code. Their incorrect or malicious usage is a possibility for security attacks.[1]

http://en.wikipedia.org/wiki/IDN_homograph_attack

ICANN IDN – домейни на кирилица (.бг)

МВР.бг **МВР.br**

МОН.бг **МОН.br**

Но да не забравяме и …

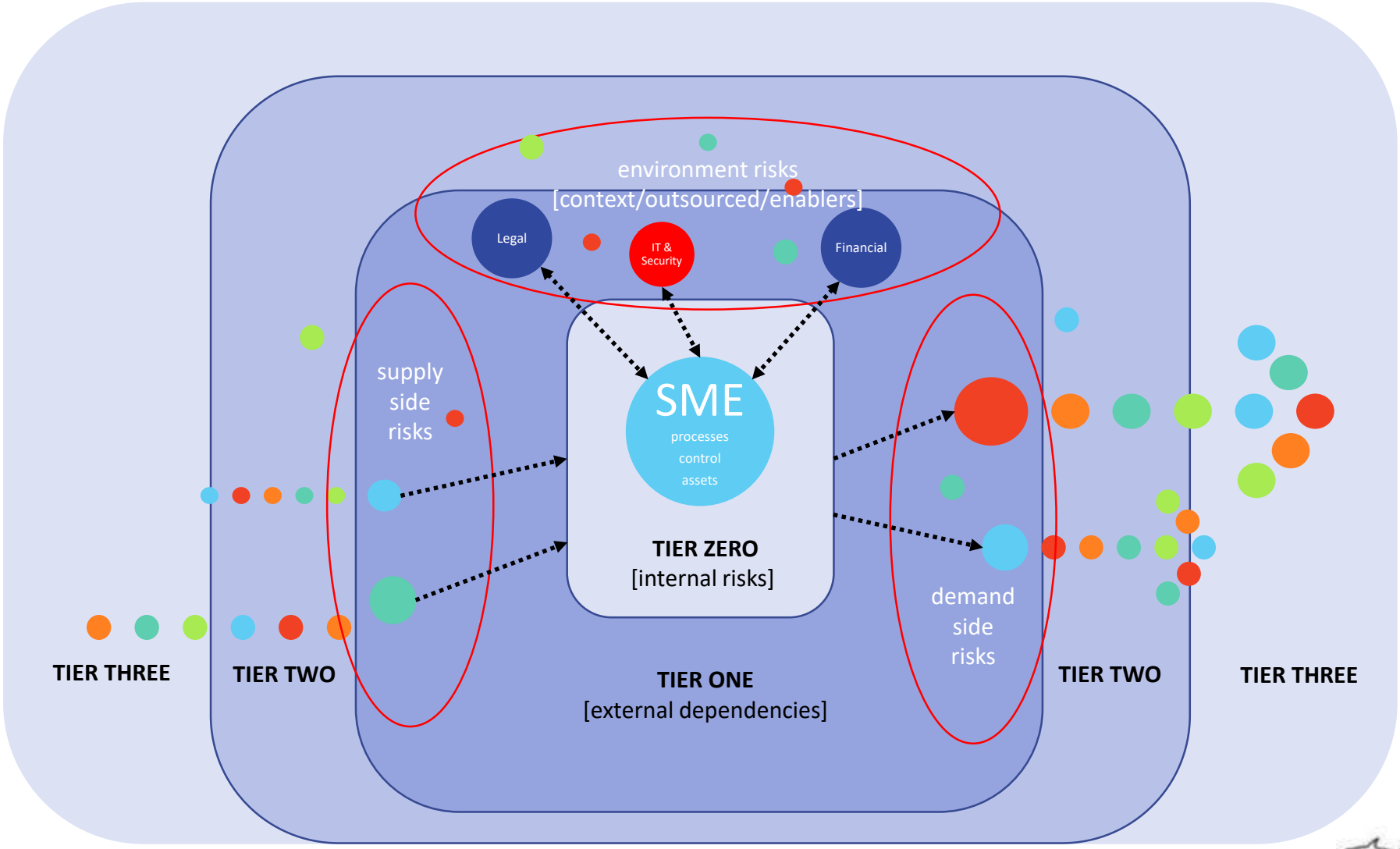
www.parlament.bg www.parliament.bg

www.dsk.bg www.dskbank.bg

WWW = „вай-вай-вай“ ???

Supply/Value Chains as PPP

GOV & SMEs in the business lifecycle: shared cyber risk

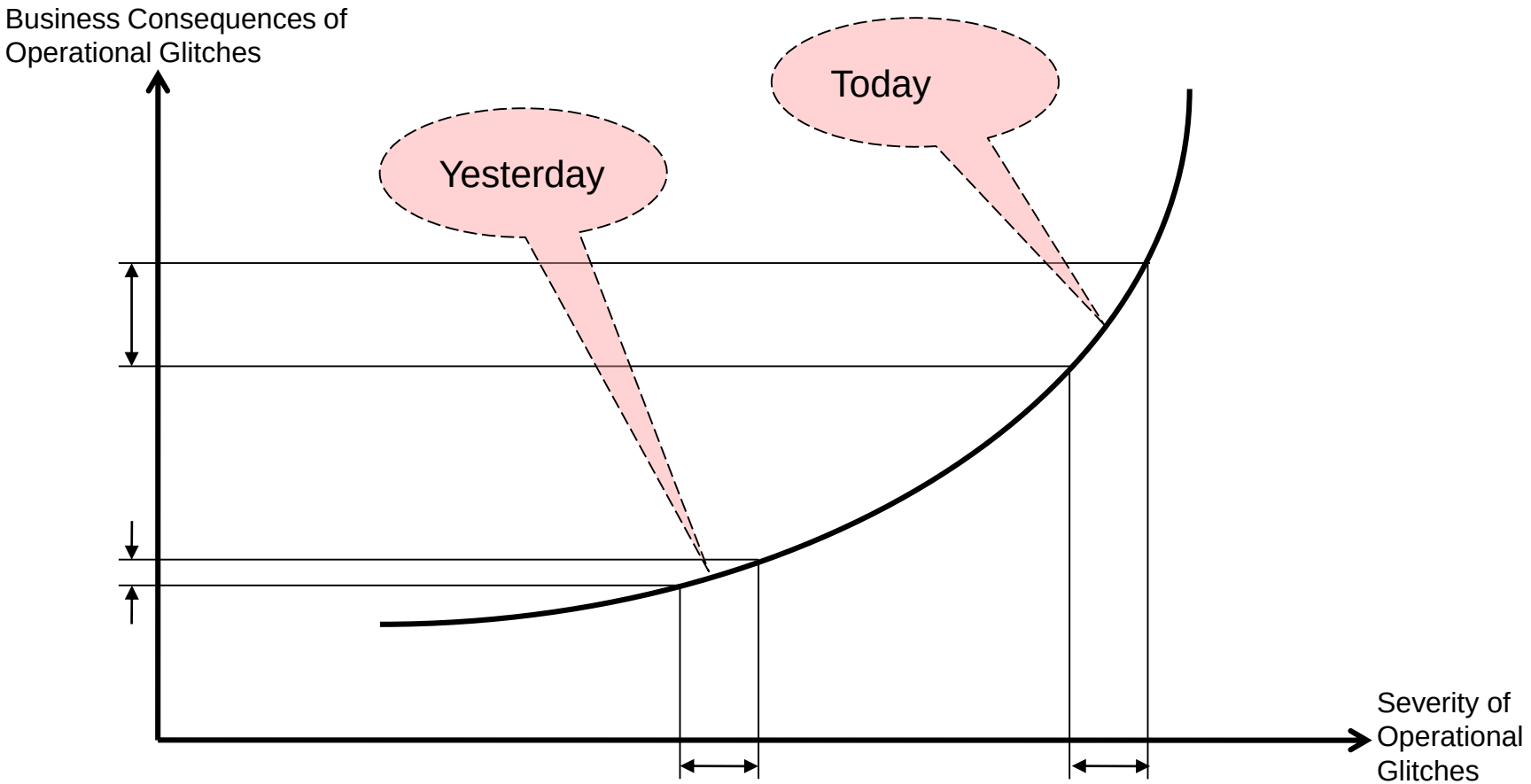



About Your Tesla
CONNECTIVITY
MODEL S
Tesla Model S firmware update 5.0 brings the Wifi and better sleep, creep and towing modes
tesla-update-firmware-5.0
Tesla owners should be receiving a pretty huge over the air update in the coming days which will enable a bunch of new functionality in the car.


HUMAN
ORGAN
FOR TRANSPLANT

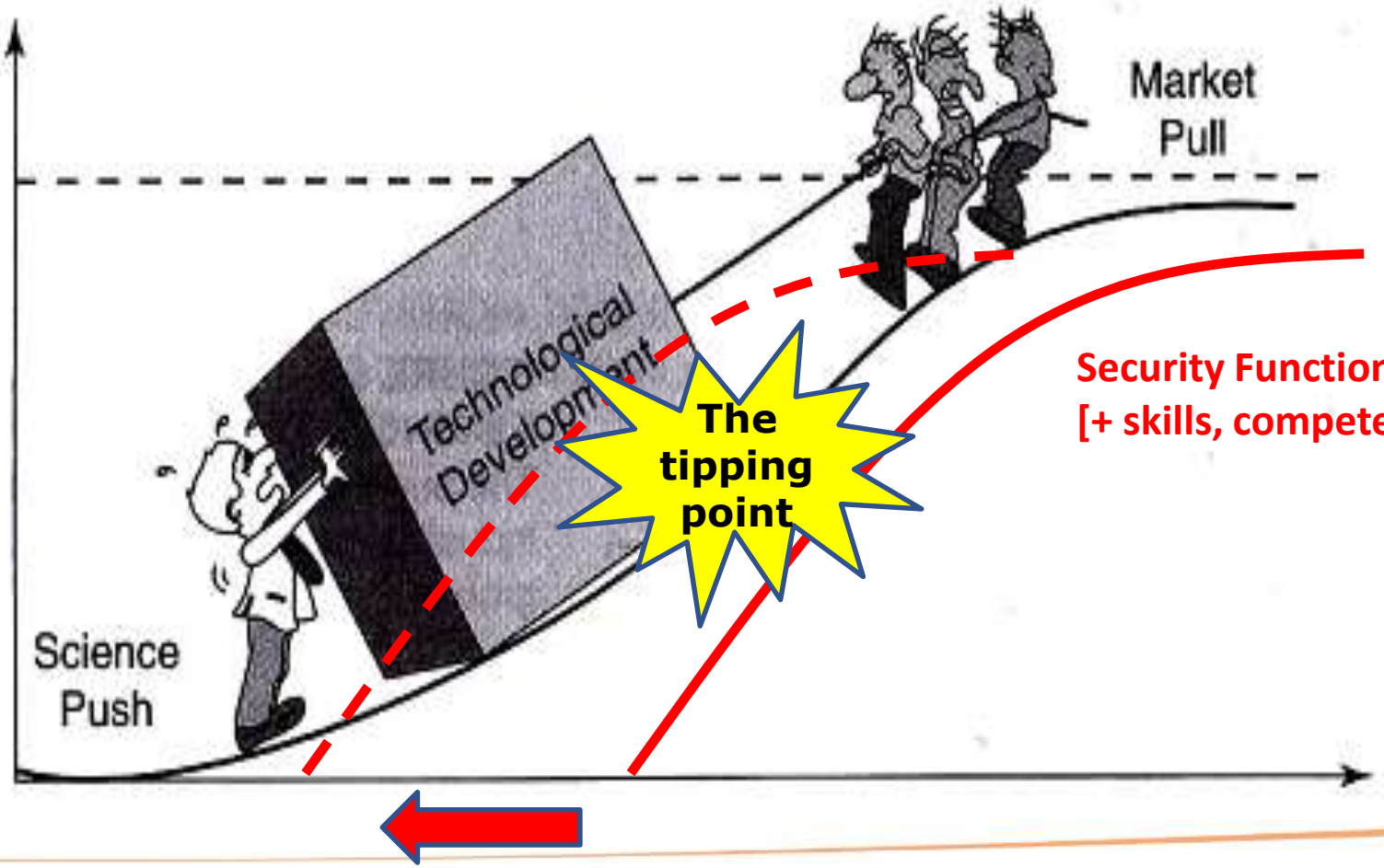
Digital Currency
[Inter]National Treasury

Today's Business Environment

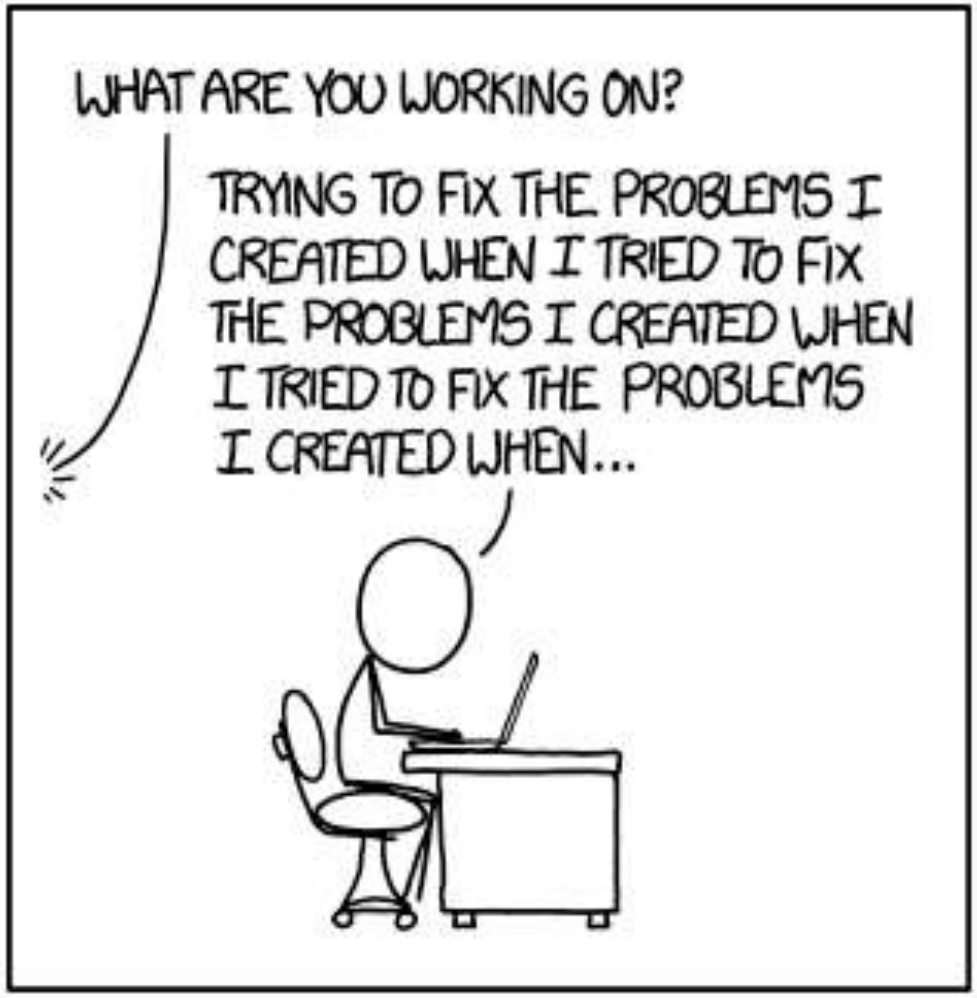


Today's Business Environment is Much Less Forgiving

Digital society/ecosystem: Ready for the Digital Dependency?



SW/ICT services quality: Ready for the Digital Dependency?



http://xkcd.com/1739/

Digital dependency:
If Software is eating the world,
are we safe ?

THE WALL STREET JOURNAL.

Tory Burch's New Store Is Her Clubhouse

When You Really Need to Attend That Conference

ADVENTURE & TRAVEL
The Ski Vacation That Should Be on Your ...

ESSAY

Why Software Is Eating The World

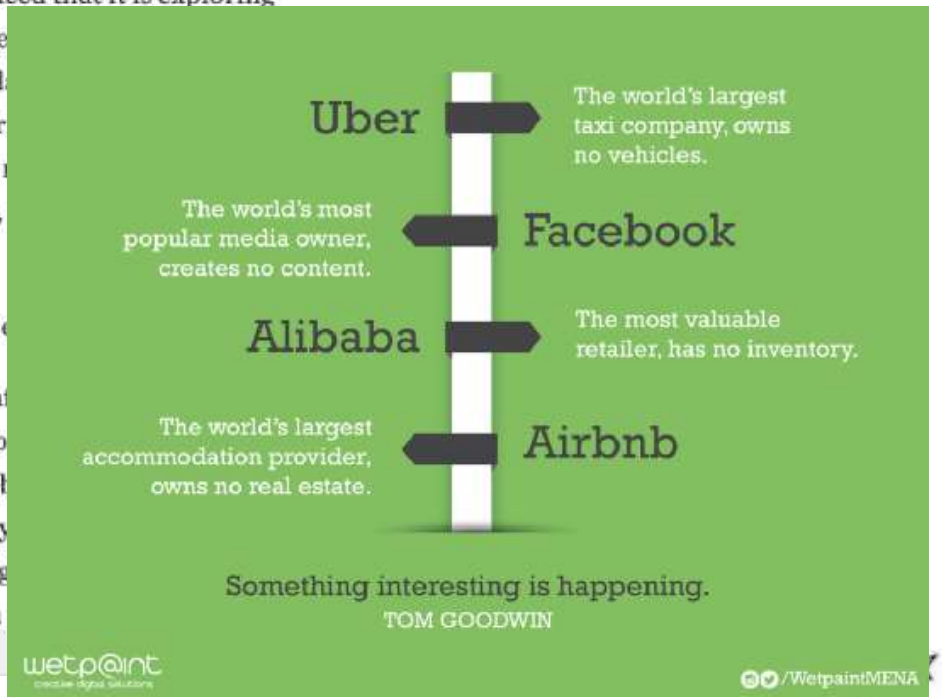
By MARC ANDREESSEN
August 20, 2011

This week, Hewlett-Packard (where I am on the board) announced that it is exploring jettisoning its struggling PC business in favor of investing more
where it sees better potential for growth. Meanwhile, Google pl
cellphone handset maker Motorola Mobility. Both moves surpr
both moves are also in line with a trend I've observed, one that
about the future growth of the American and world economies,
turmoil in the stock market.

In an interview with WSJ's Kevin Delaney, Groupon and LinkedIn investor Marc

In short, software is

More than 10 years a
dot-com bubble, a do
companies like Faceb
sparking controversy
their rapidly growing
valuations, and even



THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Lif

2011

ESSAY

Why Software Is Eating The World

By MARC ANDREESSEN

August 20, 2011

This week, Hewlett-Packard (where I am on the board) announced that it is exploring jettisoning its struggling PC business in favor of investing more heavily in software, where it sees better potential for growth. Meanwhile, Google plans to buy up the cellphone handset maker Motorola Mobility. Both moves surprised the tech world. But both moves are also in line with a trend I've observed, one that makes me optimistic about the future growth of the American and world economies, despite the recent turmoil in the stock market.

In an interview with WSJ's Kevin Delaney, Groupon and LinkedIn investor Marc

In short, software is eating t

More than 10 years after the dot-com bubble, a dozen or s companies like Facebook an sparking controversy in Silic their rapidly growing private valuations, and even the occ

2016

ANDREESSEN HOROWITZ

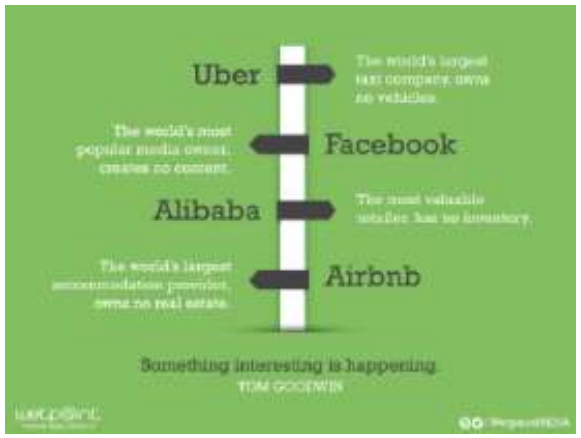
Software Is Eating the World

MACHINE & DEEP LEARNING

a16z Podcast: Software Programs the World

with Marc Andreessen, Ben Horowitz, Scott Kupor, and Sonal Chokshi

"All of a sudden you can program the world" — it's the continuation of the software eating the world thesis we put out over five years ago, and of the trajectory of past and current technology shifts. So what are those shifts? What tech trends and platforms do we find most interesting on the heels of raising our fifth fund? Are we just building on and extending existing platforms though, or will there be new platforms; and if so, what will they be? Well, distributed systems for one...



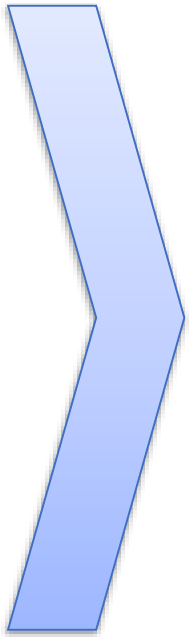
… distributed systems — encompassing cloud and SaaS; A.I., machine learning, deep learning; and quantum computing — to the role of hardware; future interfaces; and data, big and small.

… why simulations matter… and what do we make of our current reality if we are all really living in a simulation as Elon Musk believes?

Why Cyber? What "security"?

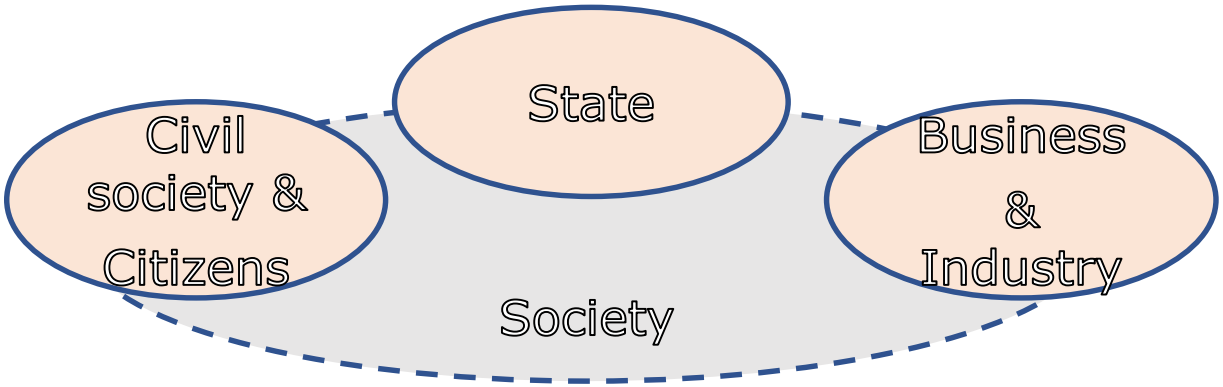
Cyber security
Cyber defense
Critical Infrastructure Protection
Cyber crime and protection
Cyber law & regulations
Crisis Management & Disaster Recovery
Risk Analysis & Management
Research & Innovations
Cyber/Digital Awareness
Education & Trainings
Digital industry
Digital ecosystems …

Digital dependency



Cyber
Resilient
Society

Why multi stakeholder model?



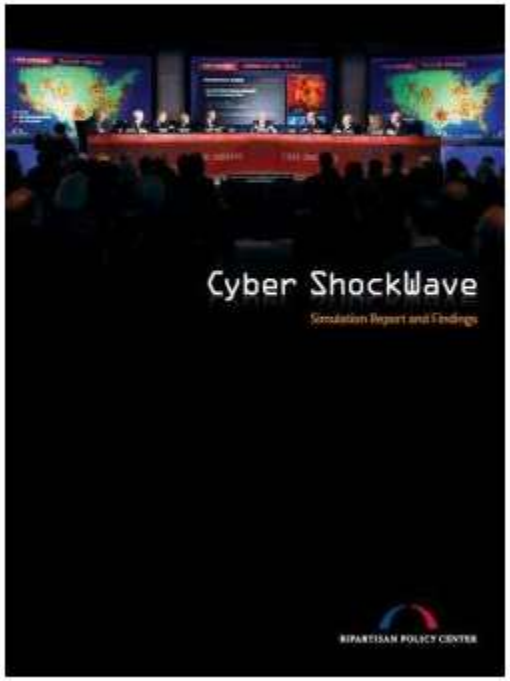
Cyber ShockWave, February 2010

"Cyber ShockWave" Exercise Shakes Up the Capital: How Would Our Leaders Respond to an All-Out Cyber Crisis?

by STEVE.KOVSKY *on* JUNE 29, 2011

A report was released yesterday detailing the fallout of an extraordinary simulated cyber attack scenario, which was orchestrated in Washington DC on February 16, 2010, by a bipartisan group of former senior administration and national security officials.

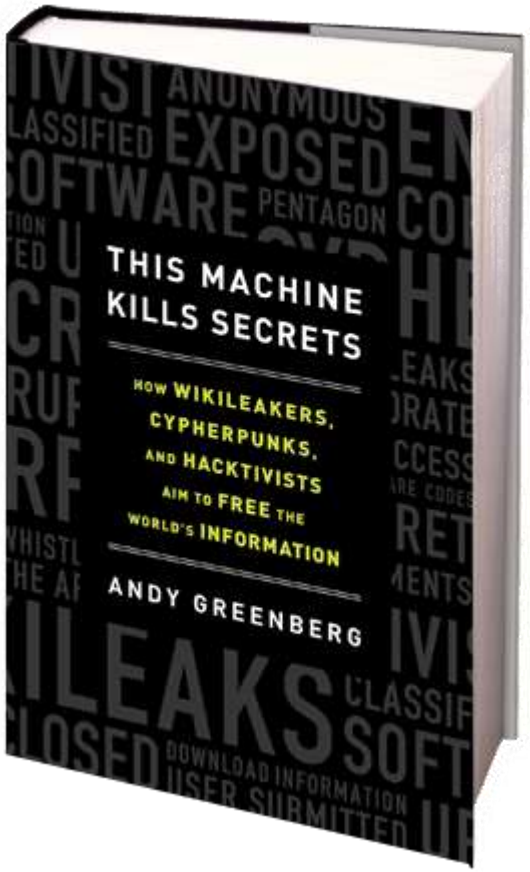
CNN's Wolf Blitzer moderated and broadcast a special news program on the "Cyber ShockWave" simulation. The purpose of the exercise was to gain insight into how government officials would respond in the event of a large-scale cyber crisis affecting much of the nation.



WORLD ECONOMIC FORUM

The annual cost of global cybercrime is estimated to be between $375 billion and $575 billion. In 2013 alone, there were 253 large-scale cybersecurity breaches in which the personal information of more than 600 million people was compromised – an increase of 62% on the previous year.

Our ShockWave?



http://www.thismachinekillssecrets.com/

You wouldn’t like to see this for your organization?

Hello internet!

Today let me pre

[redacted]

Let' take a look a

[redacted]

Not so much info

So! Let's start!

[redacted]

It look's greate fo

'[redacted]

And here are the

Table: Lotteries

id	participantsNumber	winnersNumber	IP	operatorName	date
[redacted]					
128	98	20	192.168.1.60 [redacted]	Петров	2012-09-11 10:02:11
145	498	14	192.168.1.60 [redacted]	Петров	2012-10-15 03:27:42
147	51	5	192.168.1.60 [redacted]	Петров	2012-10-16 03:02:41
150	51	5	192.168.1.60 [redacted]	Петров	2012-10-16 03:10:48
148	140	20	192.168.1.60 [redacted]	Петров	2012-10-16 03:03:17
149	140	20	192.168.1.60 [redacted]	Петров	2012-10-16 03:10:10
151	498	14	192.168.1.60 [redacted]	Петров	2012-10-17 09:42:26
156	526	13	10.168.100.60 [redacted]	Петров	2012-12-12 05:31:06
152	498	13	192.168.1.60 [redacted]	Петров	2012-10-17 09:44:12
154	293	30	10.168.100.60 [redacted]	Петров	2012-12-12 09:32:49
153	526	20	10.168.100.60 [redacted]	Петров	2012-12-11 02:53:03
155	293	20	10.168.100.60 [redacted]	Петров	2012-12-12 05:08:12
158	629	13	10.168.100.60 [redacted]	Петров	2013-01-08 09:22:38
157	629	30	10.168.100.60 [redacted]	Петров	2013-01-08 09:01:54

Ohhh!!! Mr. [redacted] Петров is so lucky!!!

Let's check something else...

Ok, It looks g

Vulnerabilities (OWASP + CyResLab)	%
DoS	50 %
Reflected XSS (injection)	18 %
Site reveals **sensitive information**	35 %
The site uses **old versions** with implausible attack scenarios	35 %
Arbitrary Code Execution/Injection	10+ %
Site allows for retrieval and **edit** of confidential information	5+ %
Possible stripping HTTPS for sensitive information	18 %
XSS and/or SQL attacks	5+ %

Organizational certainties

Risk environment will not contract—number of risks and complexity will increase.

Organizations must get better at "surviving" in uncertainty.

Knowledge and awareness of risk issues must be pervasive throughout the organization.

Traditional tools, techniques, and methods may not work in this environment.

Existing organizational structures may not be agile enough to adapt.

“Digital” society:

If we lost the battle,
could we still win the war?

The Economist

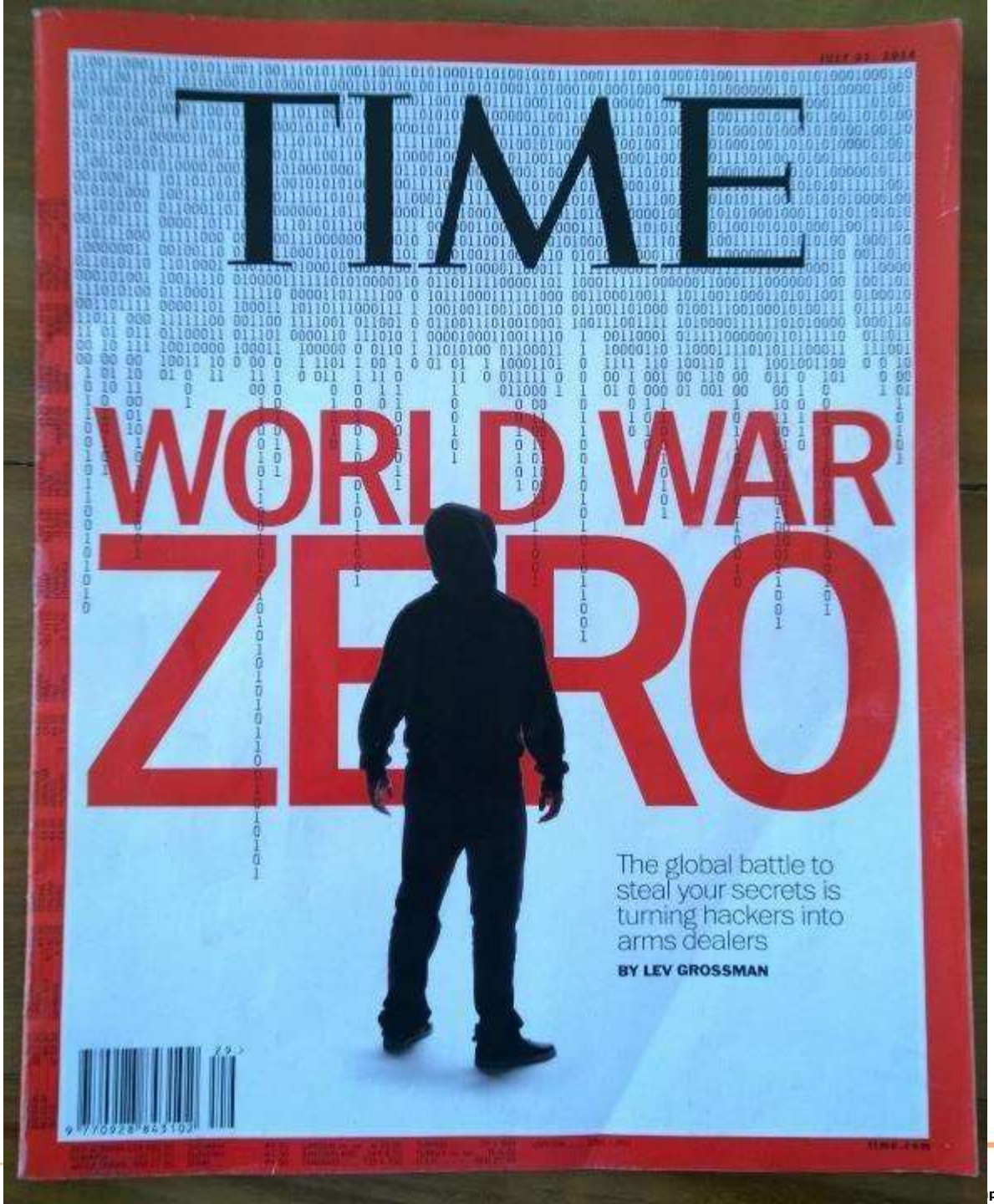
Cyberwar

War in the fifth domain

Are the mouse and keyboard the new weapons of conflict?

Jul 1st 2010 | from the print edition

http://www.economist.com/node/16478792


TIME
WORLD WAR ZERO
The global battle to steal your secrets is turning hackers into arms dealers
BY LEV GROSSMAN

NATO to form rapid reaction force to secure eastern Europe, US forms 'core coalition' against Islamic State

By ABC and wires

Updated 6 Sep 2014, 1:27am

NATO leaders have agreed to set up a rapid reaction force as part of efforts to reassure allies rattled by the Ukraine crisis and rising Islamic extremism, alliance head Anders Fogh Rasmussen says.

Speaking at a summit of NATO members in Wales, Mr Rasmussen said the force would send a clear message.

"Protect all allies at all times ... and it sends a clear message to any potential aggressor. Should you even think of attacking one, you will be facing the whole allies," he said.

PHOTO: NATO secretary-general Anders Fogh Rasmussen has announced a rapid reaction force to have a presence in Europe (Reuters: Yves Herman)

Cyber defence core task

The NATO leaders agreed on that a large-scale cyber attack on a member country could be considered an attack on the entire alliance, potentially triggering a military response.

The decision marks an expansion of the organisation's remit, reflecting new threats that can disable critical infrastructure, financial systems and the government without firing a shot.

"Today we declare that cyber defence is part of NATO's core task of collective defence," Mr Rasmussen said.

GOVINFOSECURITY

Cloud | Compliance | Continuous Monitoring | Cybersecurity | Mobil

News | Blogs | Interviews | Webinars | White Papers | Memberships | Resources | Events

Home > Articles

Syrian Rebels Hacked Via Skype

'Flirtatious Women' Tricked Fighters Into Installing Malware

By Mathew J. Schwartz, February 2, 2015

Paul Cornish, a professor at the Strategy and Security Institute at the U.K.'s University of Exeter. Both of those traits would likely apply to any rebel troops on the frontlines of a civil war.

"It all just goes to show that social engineering comes in all sorts of forms, and it doesn't matter how good-looking the apparent sender," Woodward says. "You should practice your **ABCs: Assume nothing, believe no one, check everything**. On the Internet a little paranoia goes a long way."

http://www.govinfosecurity.com/syrian-rebels-hacked-via-skype-a-7863/p-2

The files sent to targets included a multi-stage, self-extracting dropper file stored in the RAR format; Blackstar, which is a custom-built dropper for a well-known remote access Trojan called **Dark Comet**; the Onesize keylogger; and a malicious, encrypted Python script - named "Facebook-Account.exe" - that runs shell code, giving attackers remote access to a system.

FireEye's report also details one sample it recovered of a downloader called Yabrod, which presents the target with a password-protected PDF that serves as a decoy. Behind the scenes, meanwhile, Yabrod attempts to install and execute a file called Cablecar, which attempts to inject shell code - drawn from the **Metasploit** open source vulnerability testing framework - into the system, giving attackers remote access. Yabrod connects to a command-and-control server, and can also store files stolen from the machine on a Dropbox account, FireEye says.

"This is classic traditional spy 'tradecraft'; the honeytrap has been around a lot longer than the Internet," Europol cybersecurity adviser **Alan Woodward**

7.7 GB of data that appears to have been stolen from forces that oppose President Bashar al-Assad of Syria in the country's ongoing and bloody civil war. The information "shed valuable insight into military operations planned against President Assad's forces,"

SECURITY sony, security

Hacked again? Russian hackers still inside Sony Pictures' network, security firm says

Lucian Constantin

Feb 4, 2015 12:23 PM

Sony Pictures Entertainment (SPE) might have a second security breach on its hands, or maybe the hackers from November's scandalous attack are still inside the company systems, according to a security firm that claims to have seen evidence of Russian hackers having access to SPE internal data.

The hackers accessed SPE's Culver City, California network in late 2014 by sending spear phishing emails to Sony employees in Russia, India and other parts of Asia, U.S. security intelligence firm Taia Global said Wednesday in a report.

s-sprout-an-imaging-powerhouse-built-into-a-very-touch-friendly-pc.h

The original Sony Pictures hack was blamed on North Korea, which was apparently upset depiction of country leader Kim Jong-un

The U.S. government blamed the North Korean government for the attack, with bot officials saying they're confident about the attribution. Some security firms and exp including Taia Global, which based on a linguistic analysis of the English statemen Guardians of Peace members following the attack concluded that they're most likel speakers.

Now Taia Global, given the evidence it has in its possession, thinks one of these tw closer to reality than the assessment from Sony and the U.S. government:

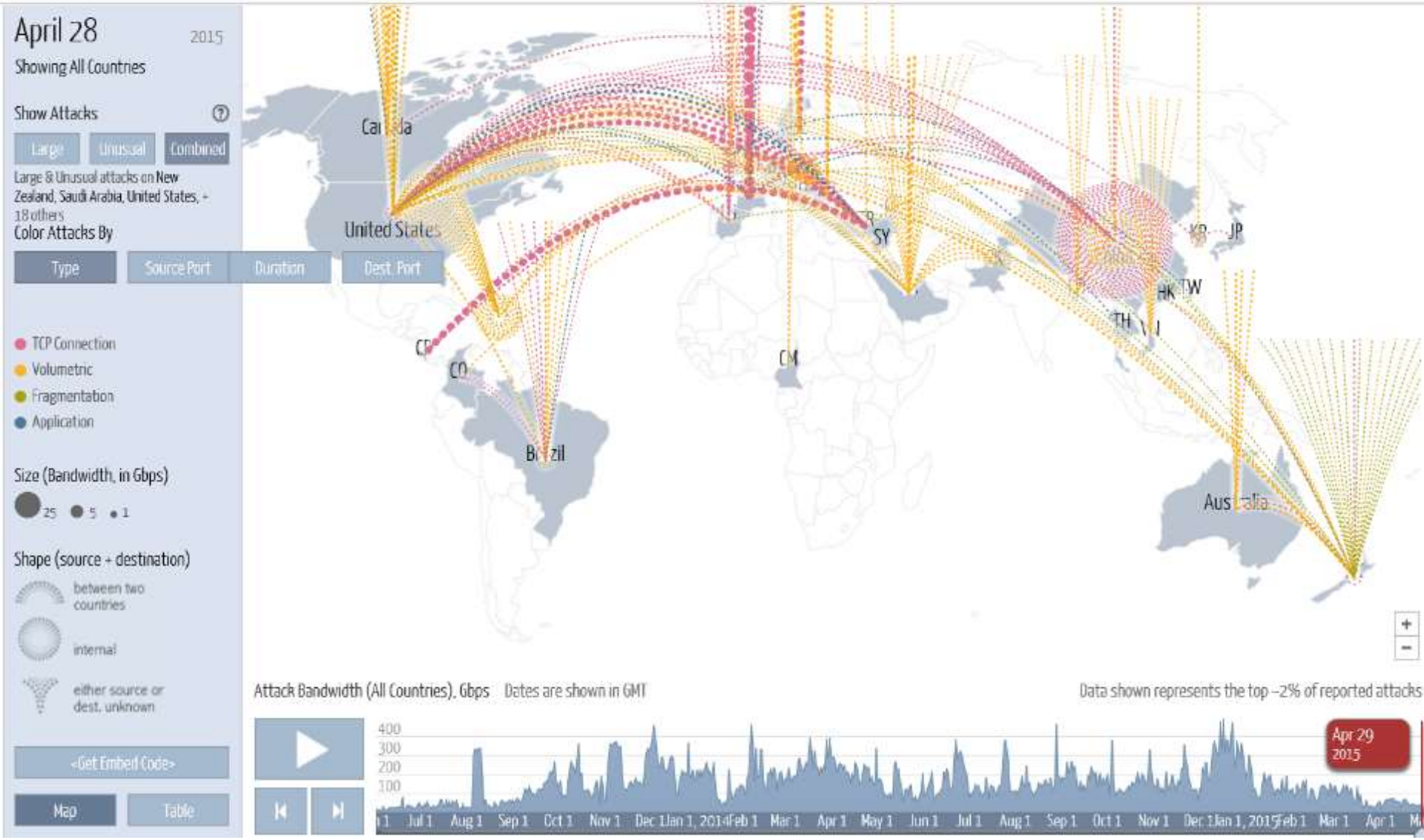
www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=2&time=16553&view=map

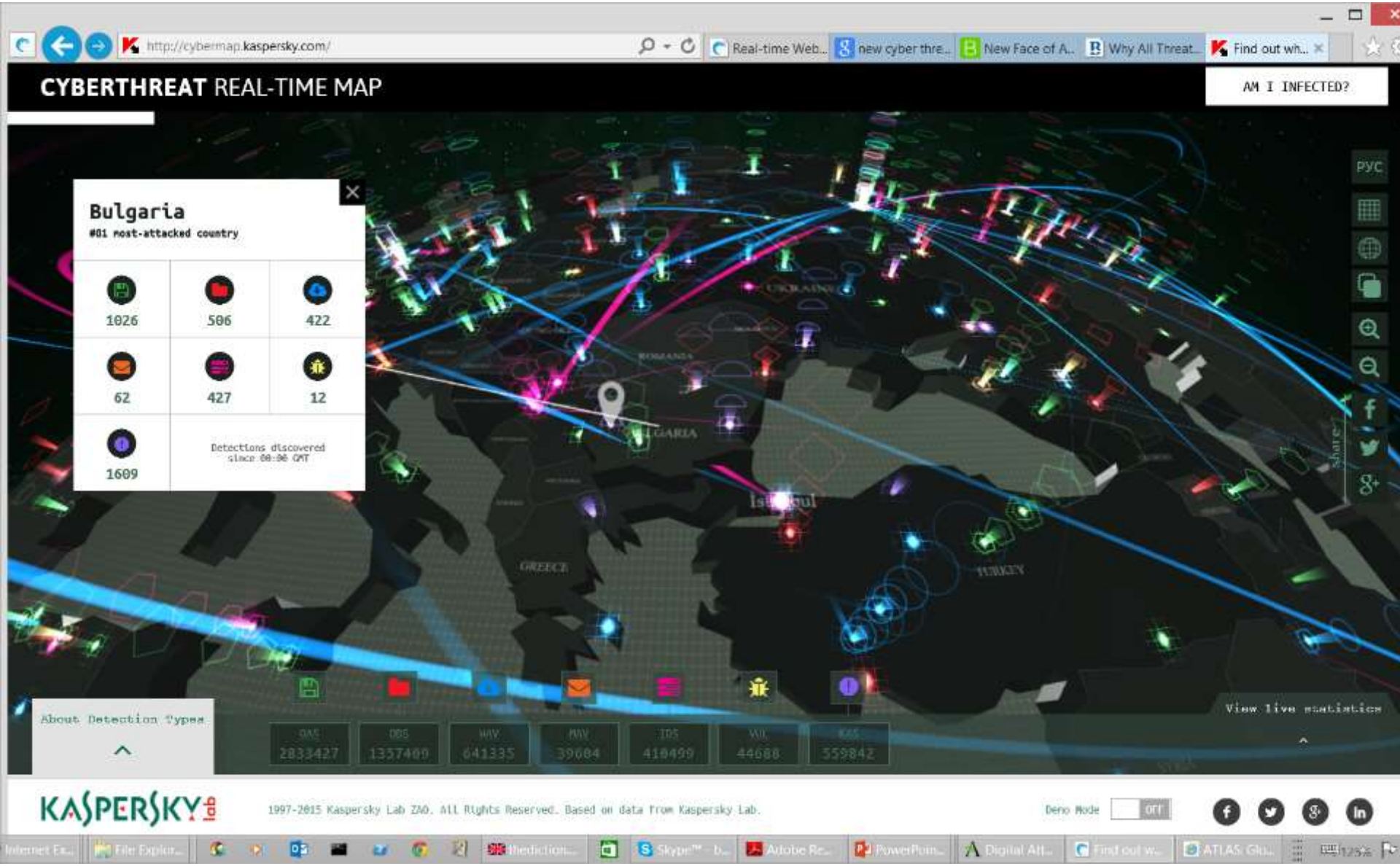
Advanced Threat Hub | Digital Attack Map

Digital Attack Map

Top daily DDoS attacks worldwide

Map · Gallery · Understanding DDoS · FAQ · About




http://cybermap.kaspersky.com/
Real-time Web...
new cyber thre...
New Face of A...
Why All Threat...
Find out wh...
CYBERTHREAT REAL-TIME MAP
AM I INFECTED?
РУС
Bulgaria
#01 most-attacked country
1026
506
422
62
427
12
1609
Detections discovered since 00:00 GMT
About Detection Types
View live statistics
2833427
1357409
641335
39084
410499
44688
359842
KASPERSKY lab
1997-2015 Kaspersky Lab ZAO. All Rights Reserved. Based on data from Kaspersky Lab.
Demo Mode
OFF

New Critical Infrastructure: Social Networks

Bulgarian PM in top 10 most active politicians on global internet, but …which one?

The new face of defense …

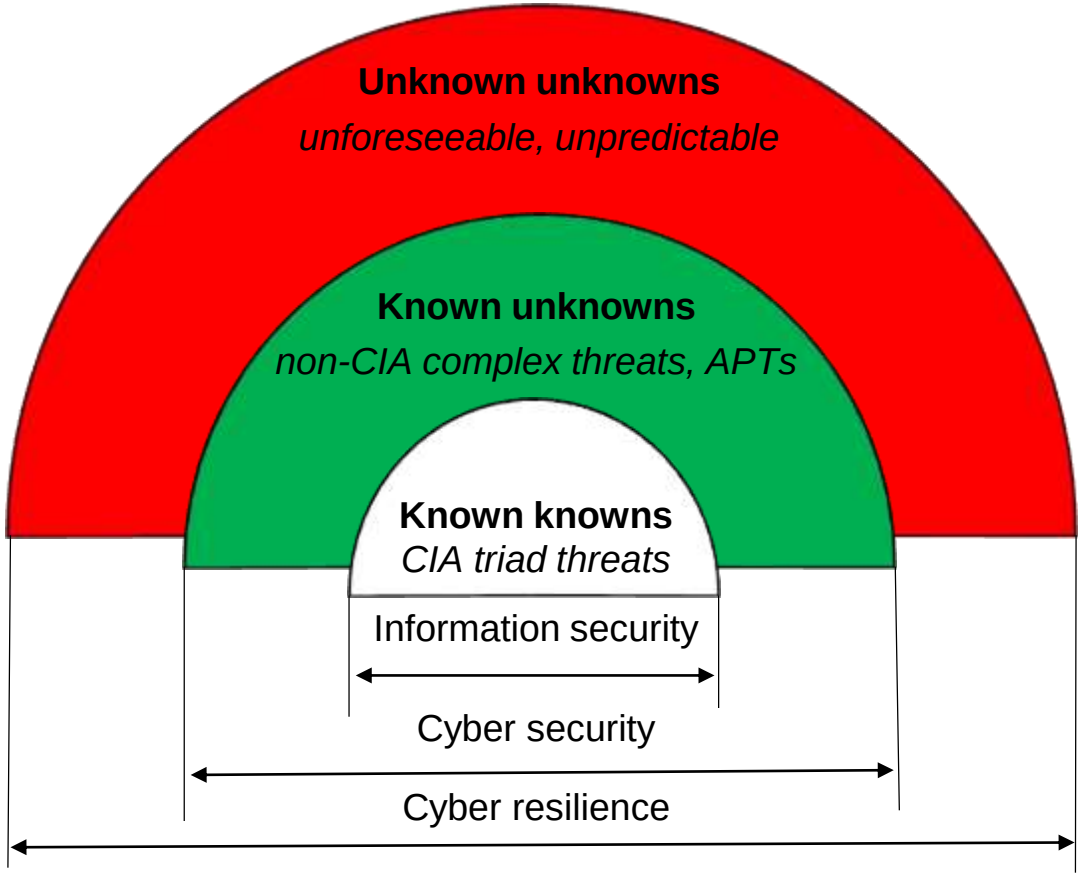
Awareness test:

Could we protect against …

the unknown ?

https://www.youtube.com/watch?v=Ahg6qcgoay4

Cyber Resilience Context



Cyber resilience context.

CIA: Confidentiality, Integrity, Availability

Credits: Eurocontrol: Manual for National ATM Security Oversight & Nassim Taleb "Black Swan"

Република България

Национална стратегия за киберсигурност

„Киберустойчива България 2020"

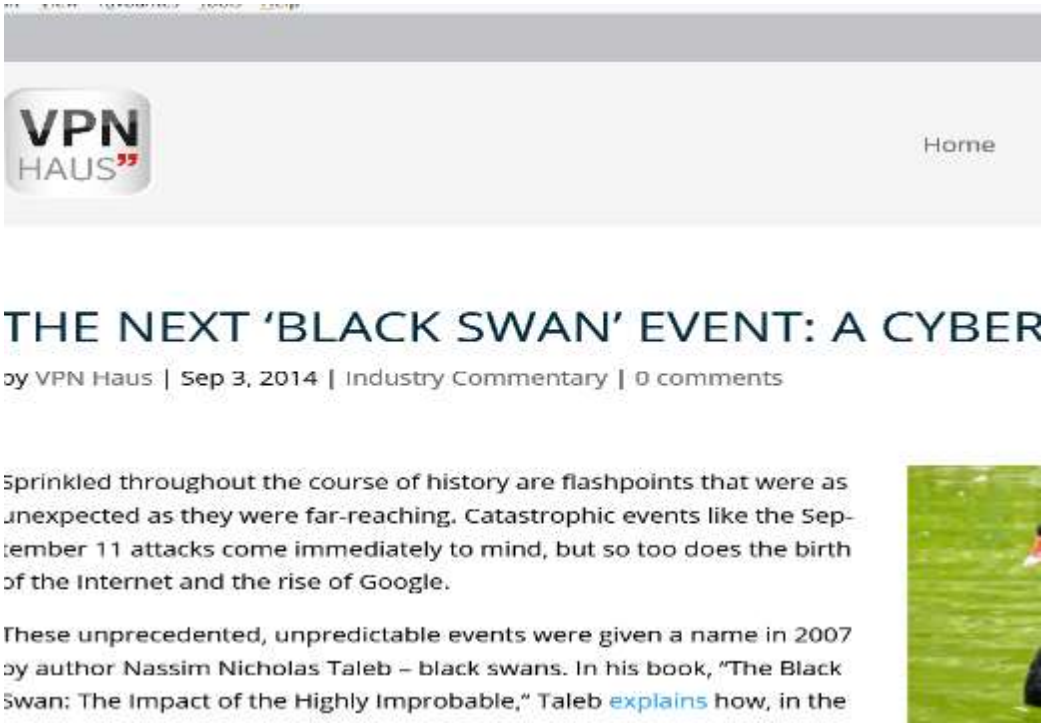
Министерски съвет

София, 2016

www.cyberbg.eu

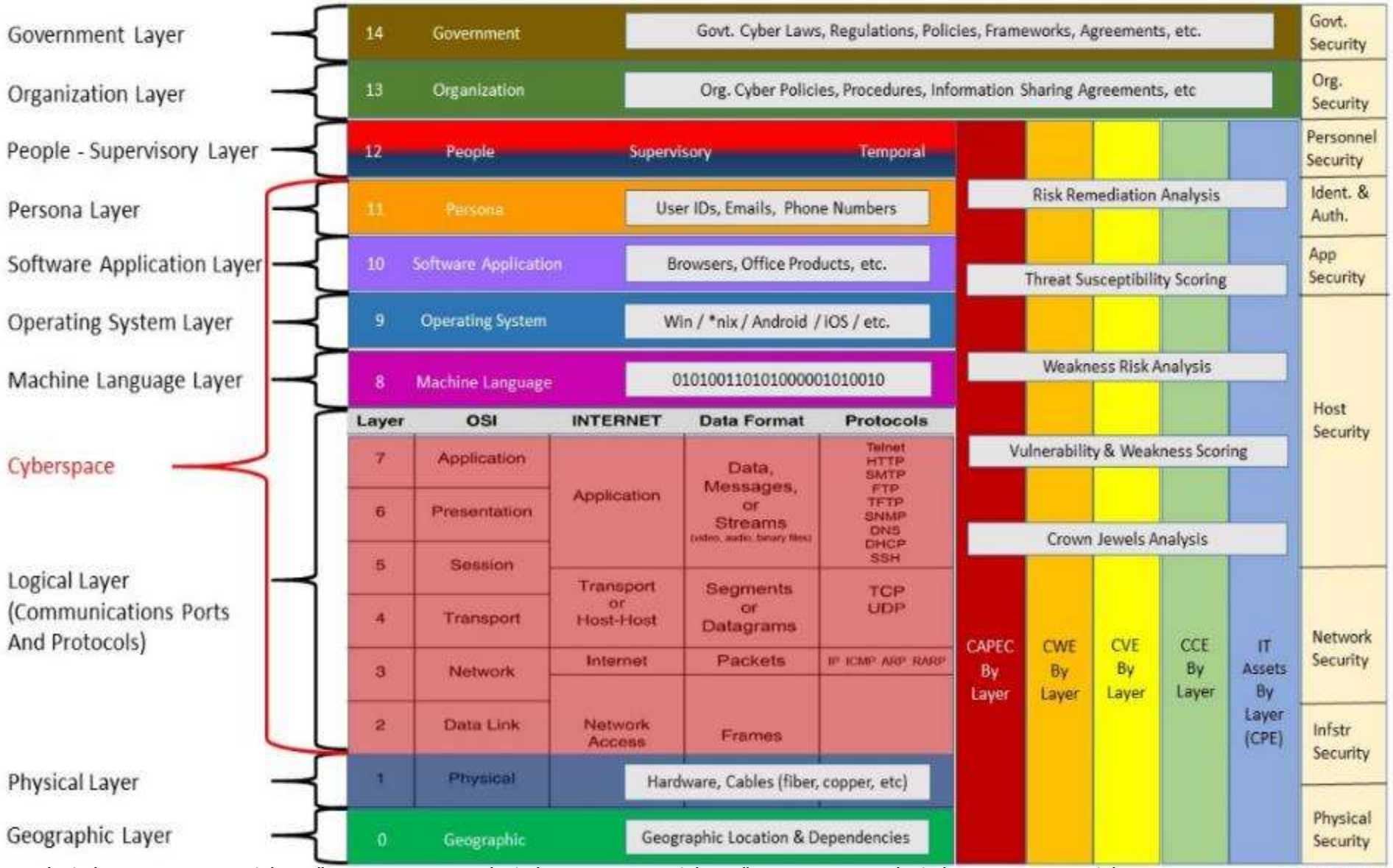
ВЕРСИЯ: 2016-07 CyberBG Strategy Approved - 16ch583pr.docx

Unknown unknowns = ontological uncertainties



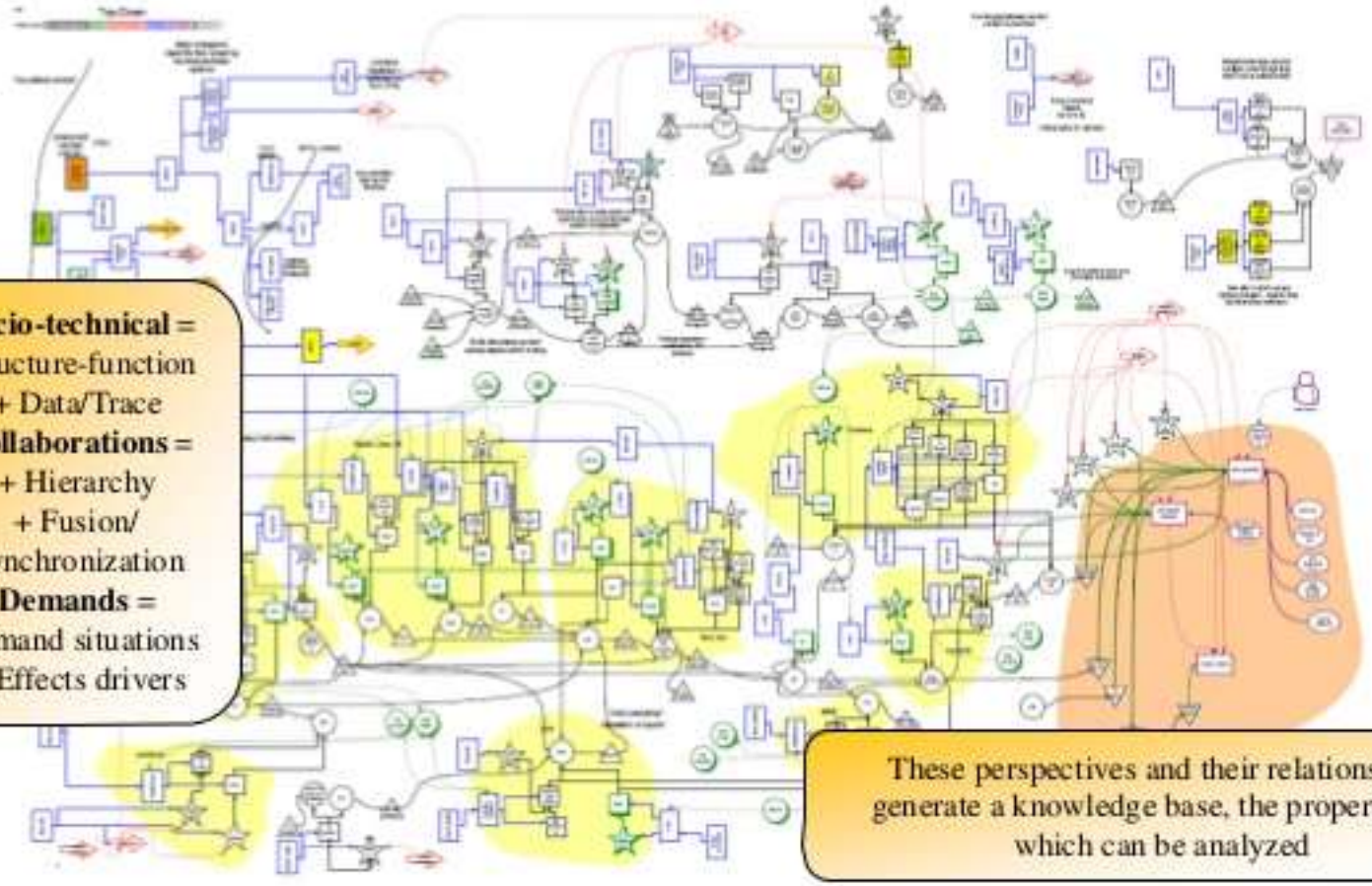
Need: Prepare Organizations and Nations for "Unknown Unknowns"

Beyond Layer 7: the real Cyberspace and Cyber "terrain" ("Defense in depth" – DoD; Cyber Physical Systems)



Complex systems of systems:

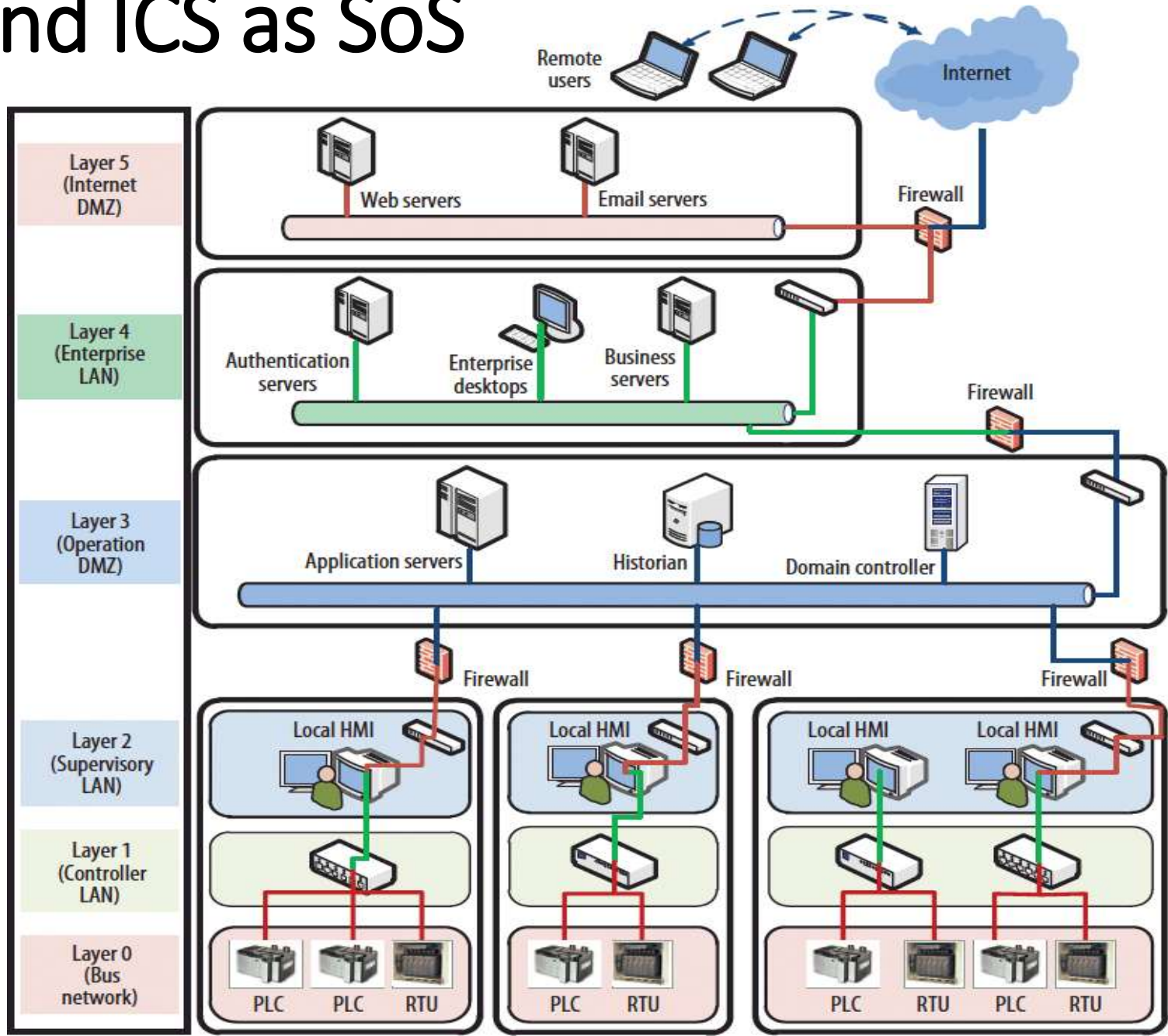
all three modeling perspectives become necessary



Socio-technical =
Structure-function
+ Data/Trace
Collaborations =
+ Hierarchy
+ Fusion/
Synchronization
Demands =
Demand situations
+ Effects drivers

These perspectives and their relationships generate a knowledge base, the properties of which can be analyzed

SCADA and ICS as SoS



Operational Risk Management

A form of risk affecting day-to-day business operations

A very broad risk category

- From high-frequency low-impact to low-frequency high-impact

Exacerbated by

- Actions of people
- Systems and technology failures
- Failed internal processes
- External events
- Bad decisions

Operational resilience emerges from effective management of operational risk.

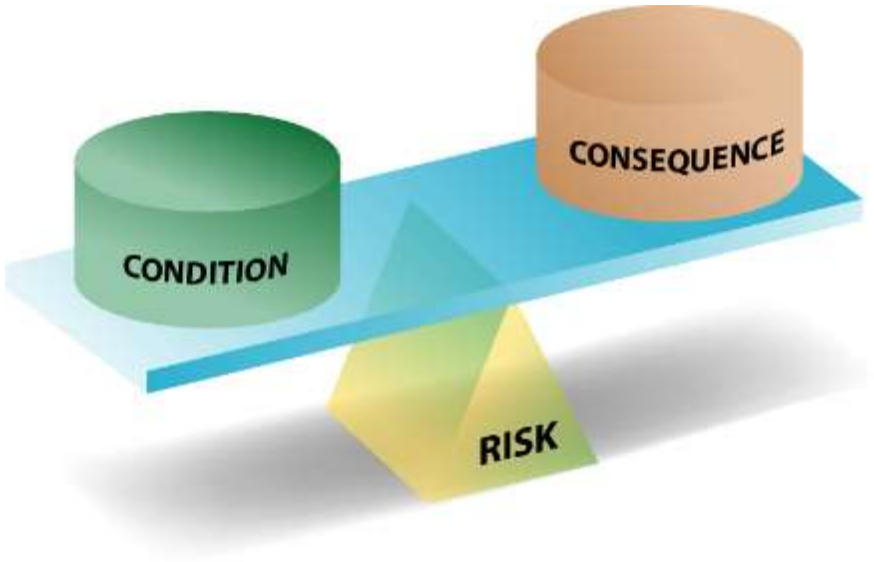
Security is an Op Risk Management activity

Managing firewall rule-sets

Access controls to systems and facilities

Limiting access to intellectual property or confidential information

Confirming identity and privileges



The aim of these "security" activities is ultimately to manage operational risk.

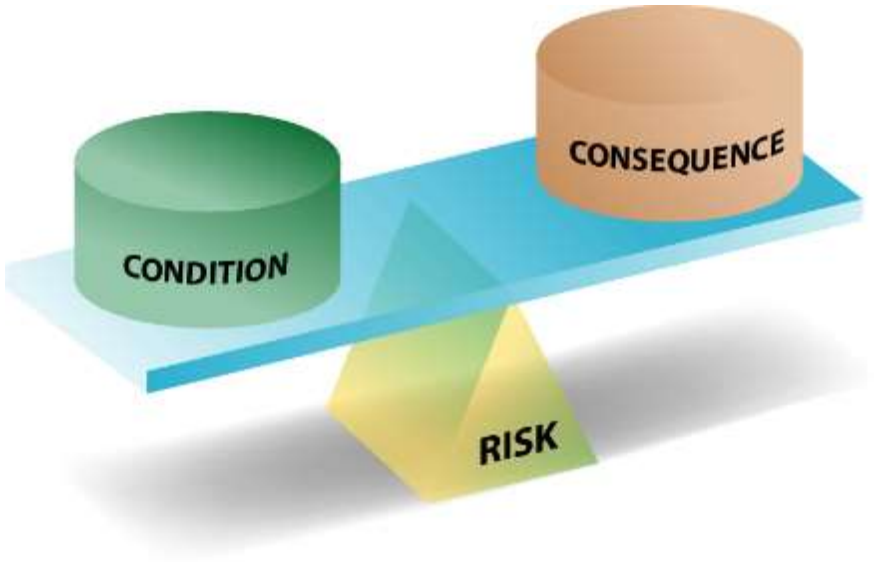
Business Continuity and Disaster Recovery are Op Risk Management activities

Limit unwanted effects of realized risk

Ensure availability and recoverability

Developing business continuity and disaster recovery plans

Manage impact from realized risk



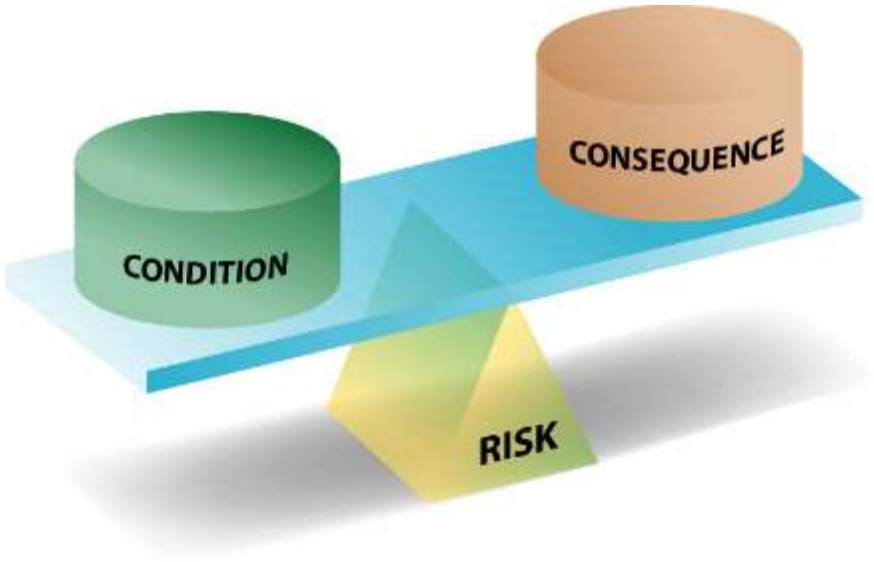
The aim of these "continuity" activities is also to manage operational risk.

IT Operations is an Op Risk Mgmt. activity

Limit vulnerabilities and threats that originate in the technical infrastructure

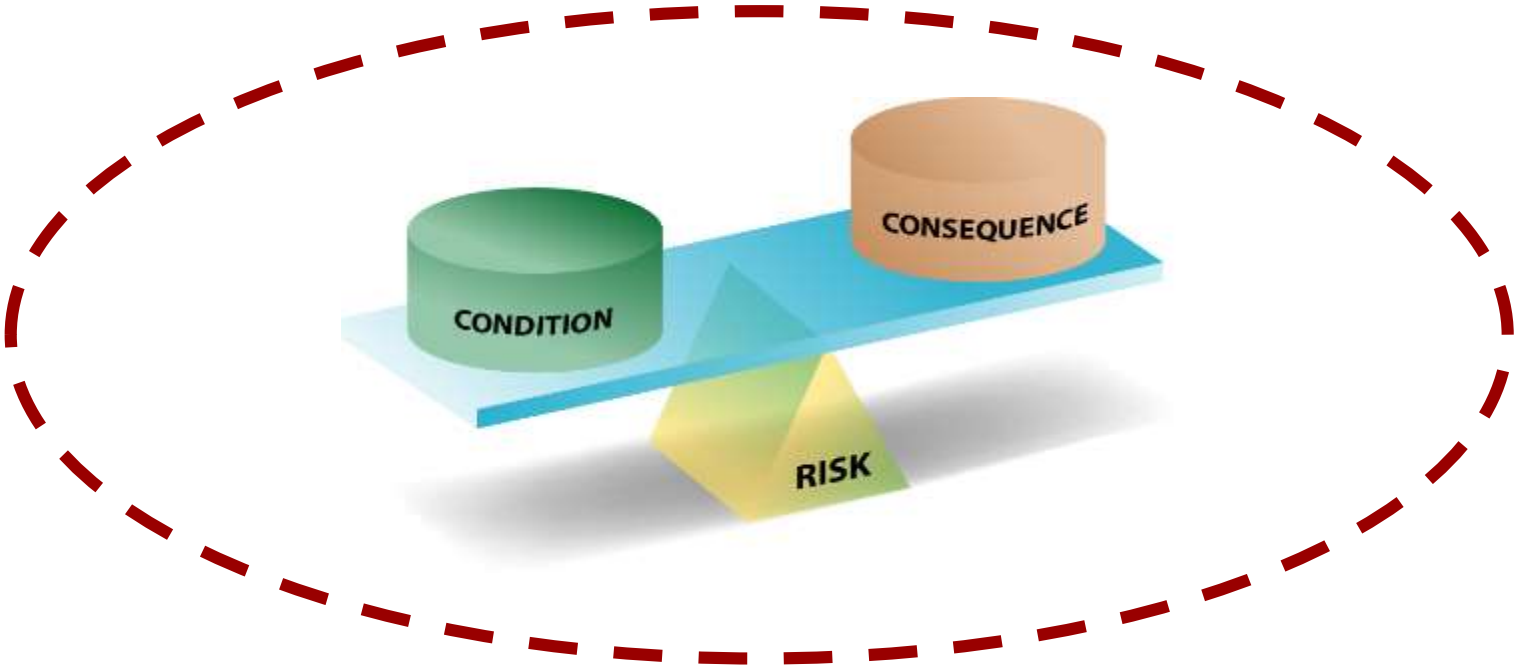
Providing appropriate access to systems & applications for staff and external entities

Ensure availability and recoverability of systems and technology



The aim of these "operations" activities is to manage operational risk.

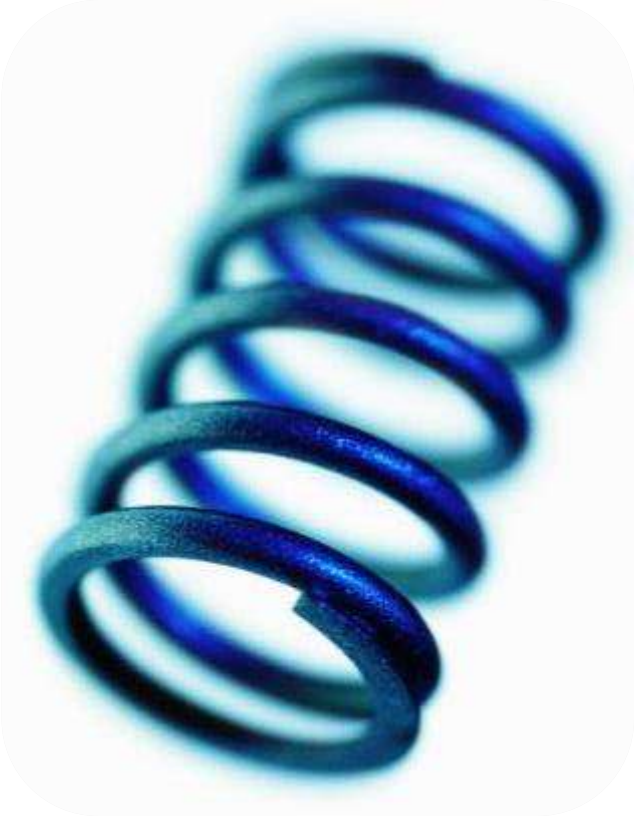
Managing Operational Risk requires a holistic approach



Managing both sides of the risk equation in alignment with business drivers and full knowledge of costs increases the risk management capability of the organization.

Operational resilience defined

Resilience: The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit [wordnet.princeton.edu]



Operational Resilience: The ***emergent*** property of an organization that can continue to carry out its mission in the presence of ***operational stress*** and ***disruption*** that does not exceed its operational limit [CERT-RMM]

Where does the ***disruption*** come from? Realized risk.

Security Risk Management

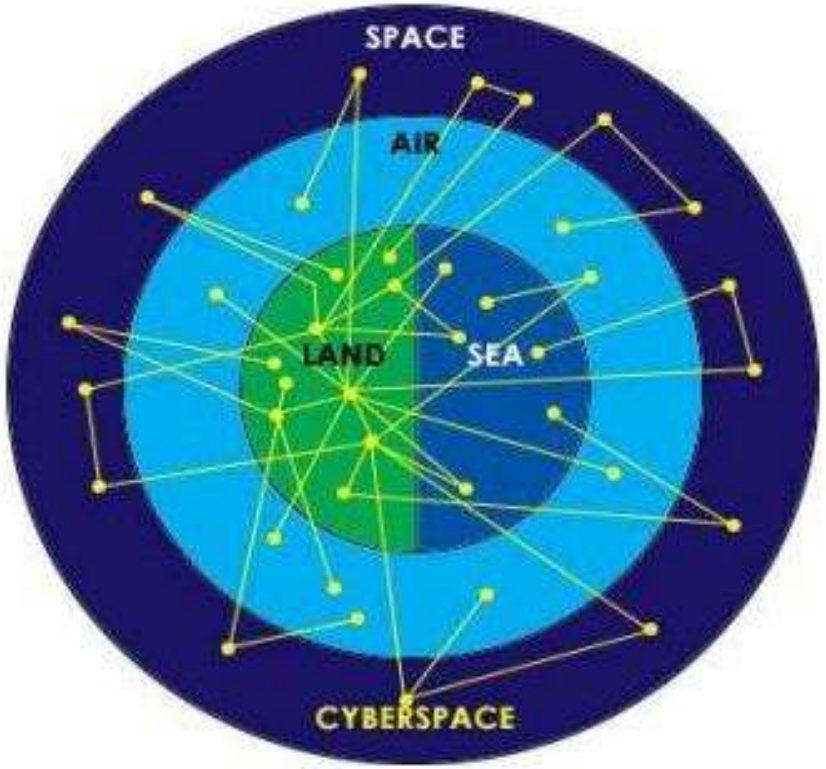
=

Resilience Management

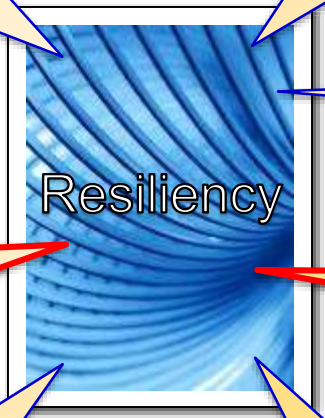
to resilience

from defense

Cyber Defense: Cyberspace as the 5th Domain: From "defense" to "resilience"



re·sil·ience *noun* [ri-ˈzil-yəns]



power or ability to return to the original form, position, etc., after being bent, compressed, or stretched

ability of an ecosystem to return to its original state after being disturbed

ability to recover from or adjust easily to misfortune or change

physical property of a material that can return to its original shape or position after deformation that does not exceed its elastic limit

ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation

ability to recover readily from illness, depression, adversity, or the like

capability of a strained body to recover its size and shape after deformation

An Analogy: Health

Is there a place that you can purchase health?

Is there a place where health is manufactured?

How do you become healthy?

Health & Resilience: They are both emergent properties.


Why we are NOT resilient?
How things generally work today?

Example

2011 Japan Earthquake & Tsunami

Example

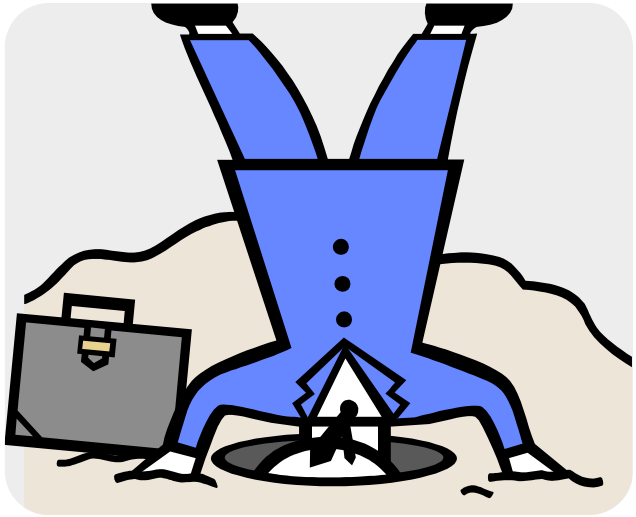

Monday, May 2, 2011 New York 60° | 46°
THE WALL STREET JOURNAL. | TECHNOLOGY
Hackers Breach Second Sony Service
Article
Stock Quotes
Comments (24)
Like 1K
+ More
Text
Information Security
Cyber Protection
COMPUTERWORLD
Sony cuts off Sony Online Entertainment service after hack
Robert McMillan
Comments (5)
Recommended (45)
Like 144
affecting 24.6 million Sony
Network offline for nearly two
weeks as it investigates a computer intrusion -- took a second gaming
Crisis Communications
PLAYSTATION® Network

Example


The Washington Post
Statewide computer meltdown in Virgi , other government business
By Derek Kravitz
Washington Post Sta
Saturday, August 28,
For a third straight
Department of M
issue driver's
computer
The Washington Post
t for return of Va. DMV licensing service
Wednesday, September 1, 2
A computer outage that ha
state agencies entered its
officials acknowledged tha
complicated than they origi
IT Operations
IT Disaster Recovery
s in
Monday, September 13, 2010; 8:31 PM
Northrop to pay for review of Va. failures
Government contractor Northrop Grumman will pay $250,000 for an independent review of the massive computer failure that cut off some state services for days in Virginia last month, and the company could be pressed to pay more if the review finds its negligence

Head-in-the-Sand

Bank Info Security – 2008 State of Banking Information Security Survey [www.bankinfosecurity.com/survey]



"Security leaders express confidence in contradictions"

64% rate their ability to counter threats as "very good" or "excellent" BUT:

- 21% have either suffered a security breach or **"don't know"**
- 66% outsource their Internet banking systems, but have only **moderate confidence in vendor security controls**
- 73% rate themselves as **"average"** in security awareness activities with customers

Lack of awareness, attention, and oversight amplifies the challenge

56% of employees still receive no security awareness training

Posted on 09 April 2014.

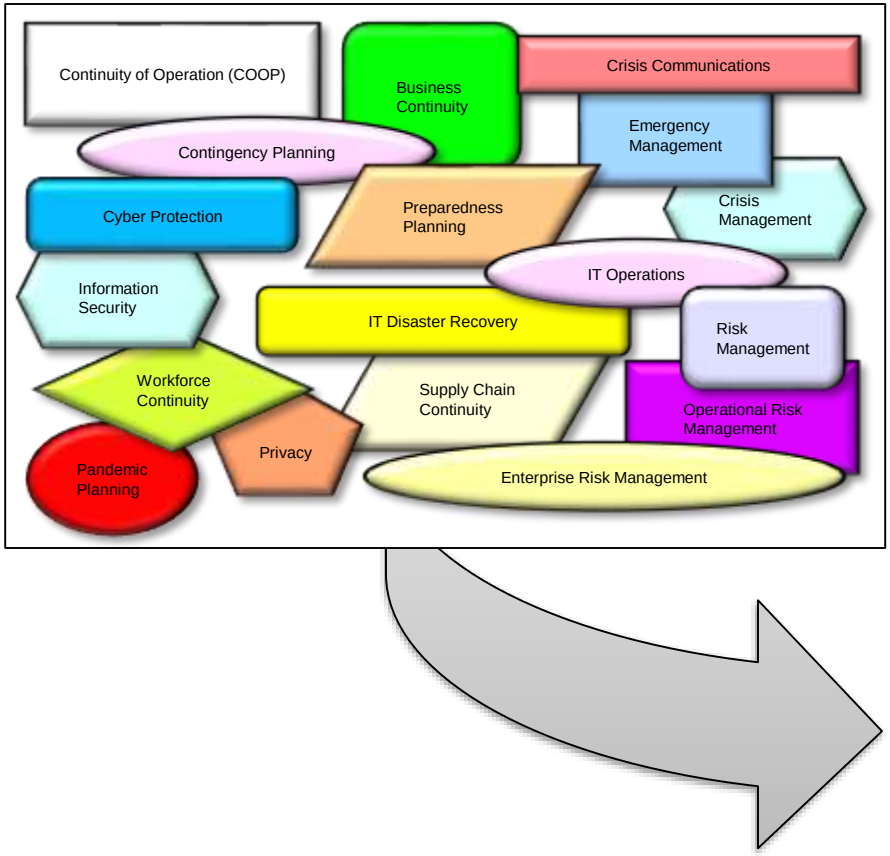
A new research survey by EMA takes you inside today's organizations to reveal how employee decisions related to information security can significantly increase organizational risk. The report examines the implementation of security awareness training in government, public and private companies and non-profit groups.

According to employee responses in the survey report:

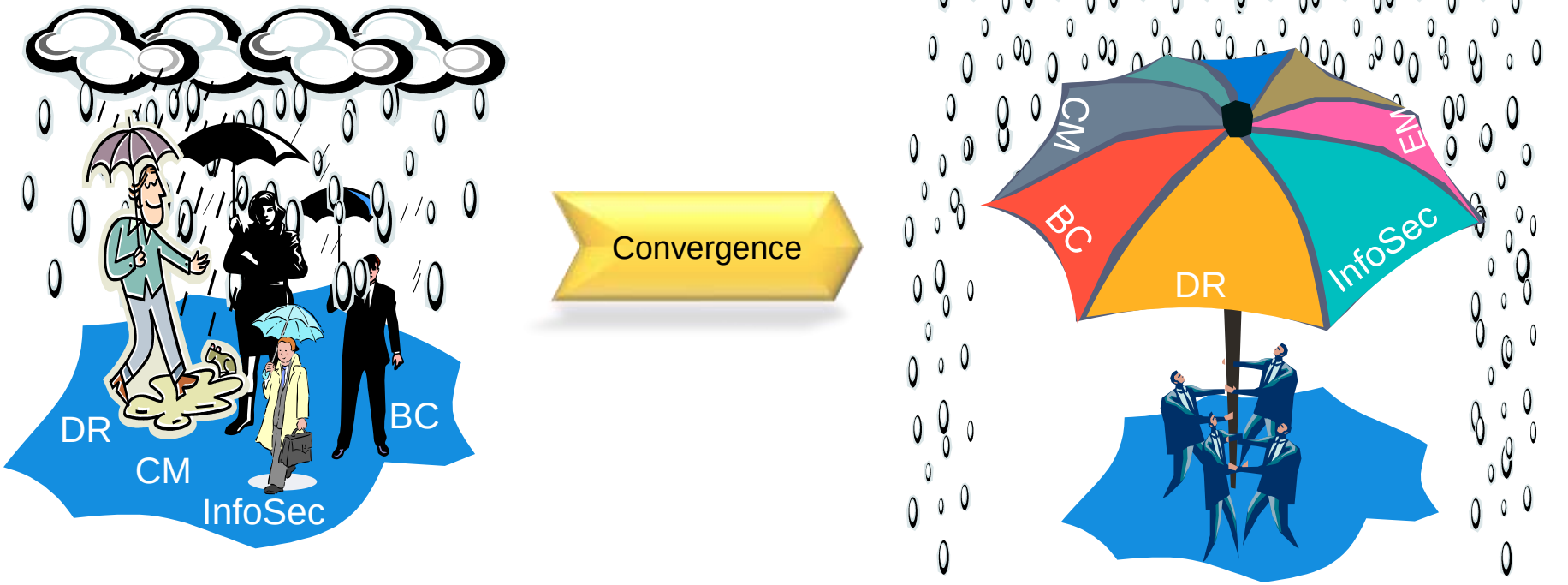
- 30% leave mobile devices unattended in their vehicle
- 33% use the same password for both work and personal devices
- 35% have clicked on a link in an email from an unknown sender
- 58% have sensitive information on their mobile devices
- 59% store work information in the cloud.

Some of the reported behaviors present inherent risks, while others depend on contributory factors like the failure to use device or data encryption.

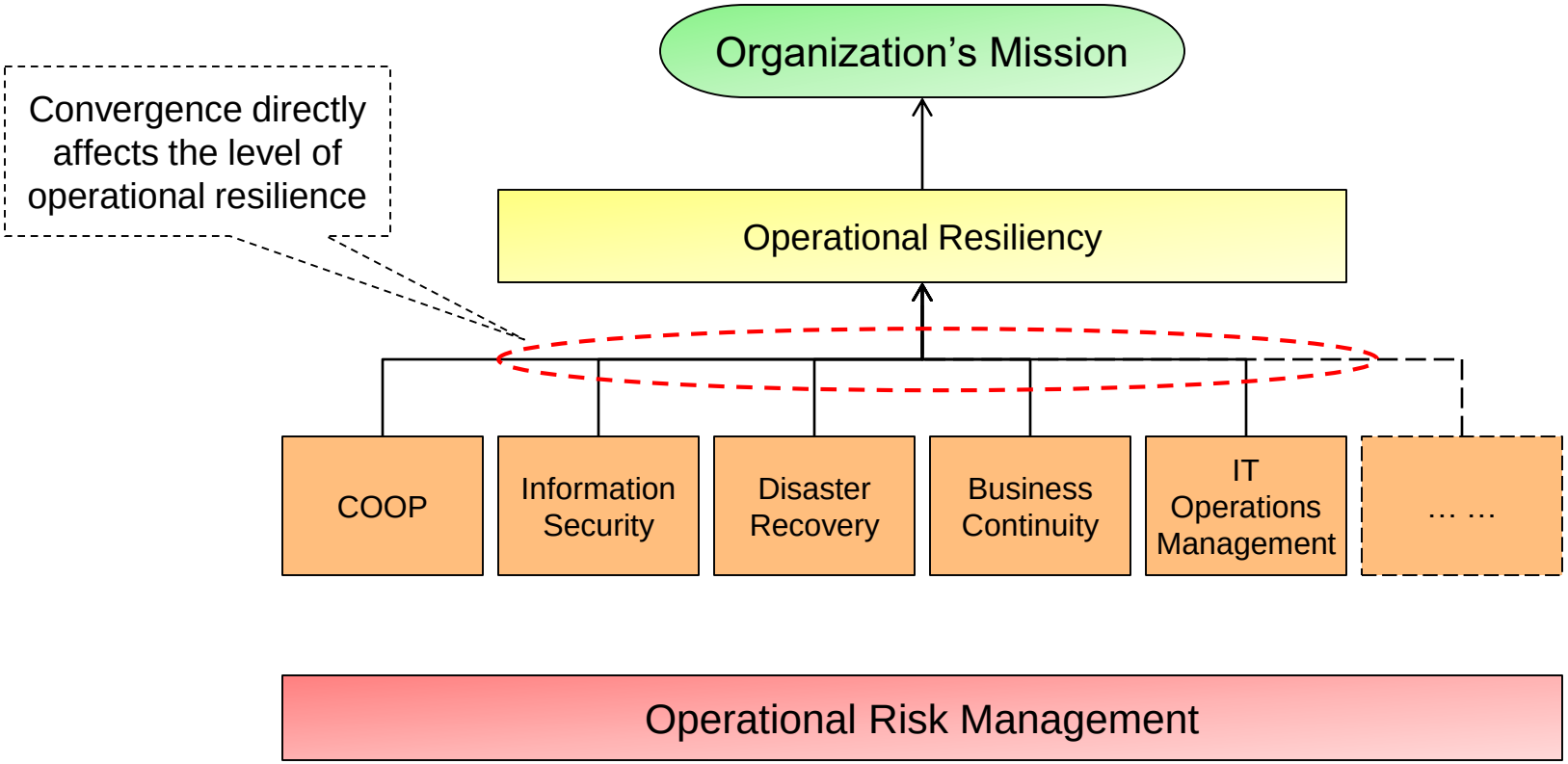
Convergence: An Analogy



Convergence: Another Analogy

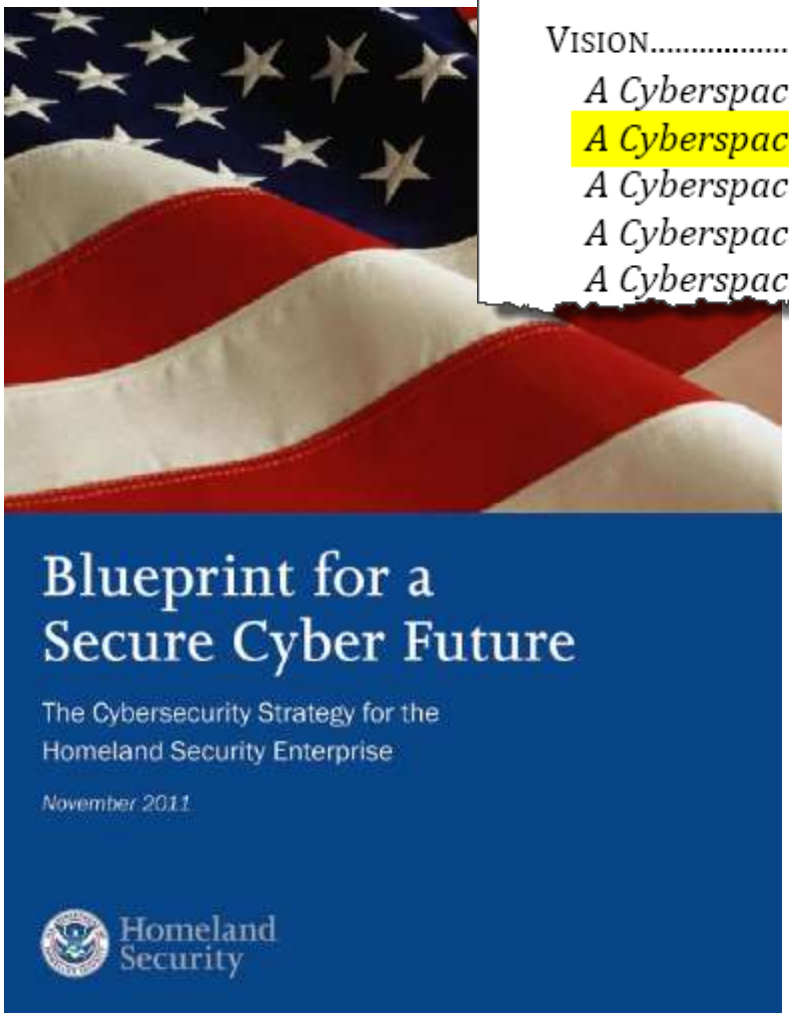


Convergence



Enterprise Risk Management

US DHS Blueprint for a Secure Cyber Future



THE FUTURE WE SEEK

VISION

A Cyberspace that is Secure

A Cyberspace that is Resilient

A Cyberspace that Enables Innovation

A Cyberspace that Protects Public Health and Safety

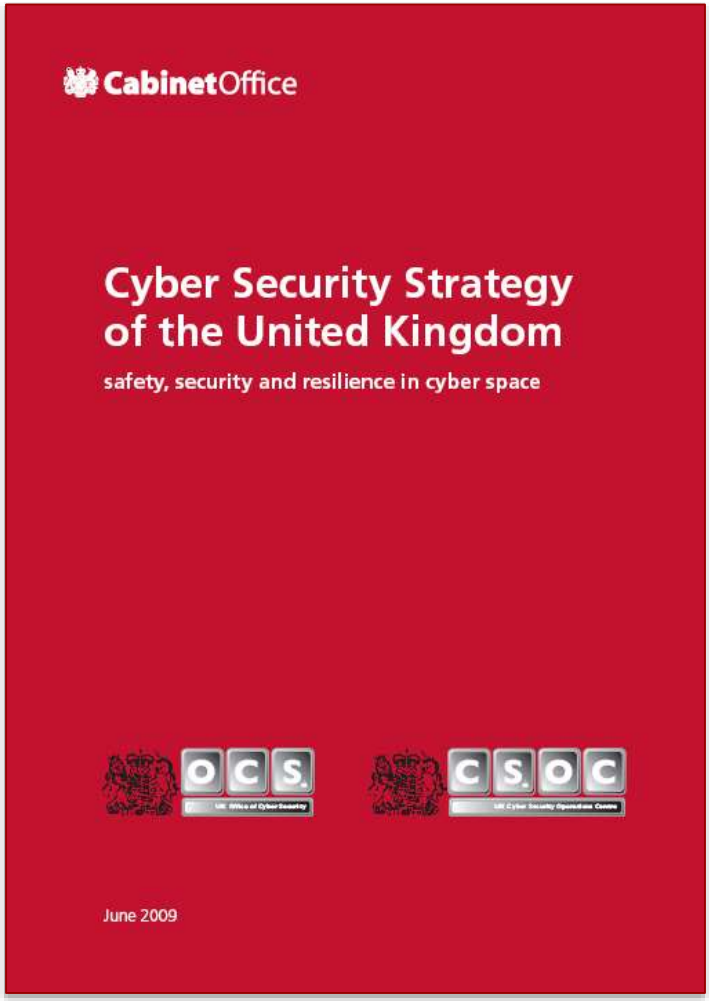
A Cyberspace that Advances Economic Interests and National Security

Executive Summary:

The Blueprint lists four goals for protecting critical information infrastructure:

- Reduce Exposure to Cyber Risk
- Ensure Priority Response and Recovery
- Maintain Shared Situational Awareness
- Increase Resilience

Cyber Security Strategy of UK



Workstream 1: Safe, Secure and Resilient Systems

3.11 This workstream will focus on enhancing the preparation for and protection from cyber attack in all sectors, to provide the greatest practicable resilience. This will require an improved understanding of potential vulnerabilities and the impacts were they to be exploited, as well as the establishment of appropriate mitigation measures. This will bring together ongoing work on redundancy and resilience in the telecommunications sector, for example, and feed into the business continuity arrangements for government and other critical sectors. It will need to consider, amongst other things, the encouragement of standards, and the need to refine procurement requirements.

New EU Cybersecurity strategy & Directive announced

NIS Public-Private Platform:

WG1 on risk management, including information assurance, risks metrics and awareness raising;

WG2 on information exchange and incident coordination, including incident reporting and risks metrics for the purpose of information exchange;

WG3 on secure ICT research and innovation.

Feb 07, 2013

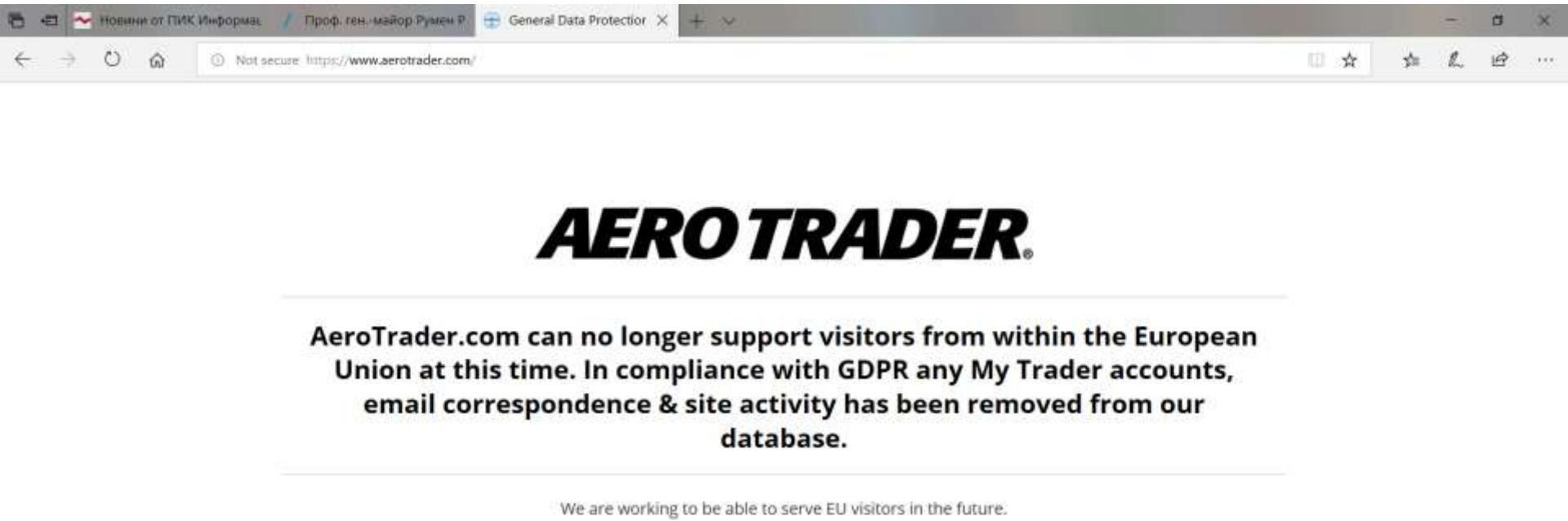
Today, Thursday, 7th of February the European Commission and the High Representative of the Euro
Security Policy announced the EU's Cybersecurity Strategy, and a complementary proposal for a Dire
common level of cyber security across the EU.

- **EU's Cyber Security strategy**
- **Proposal for a Directive on Network and Information Security**
- **Frequently Asked Questions; re the Directive proposal**
- **Commission press release; re EU Cybersecurity plan to protect open internet and online freedom and opportunity**

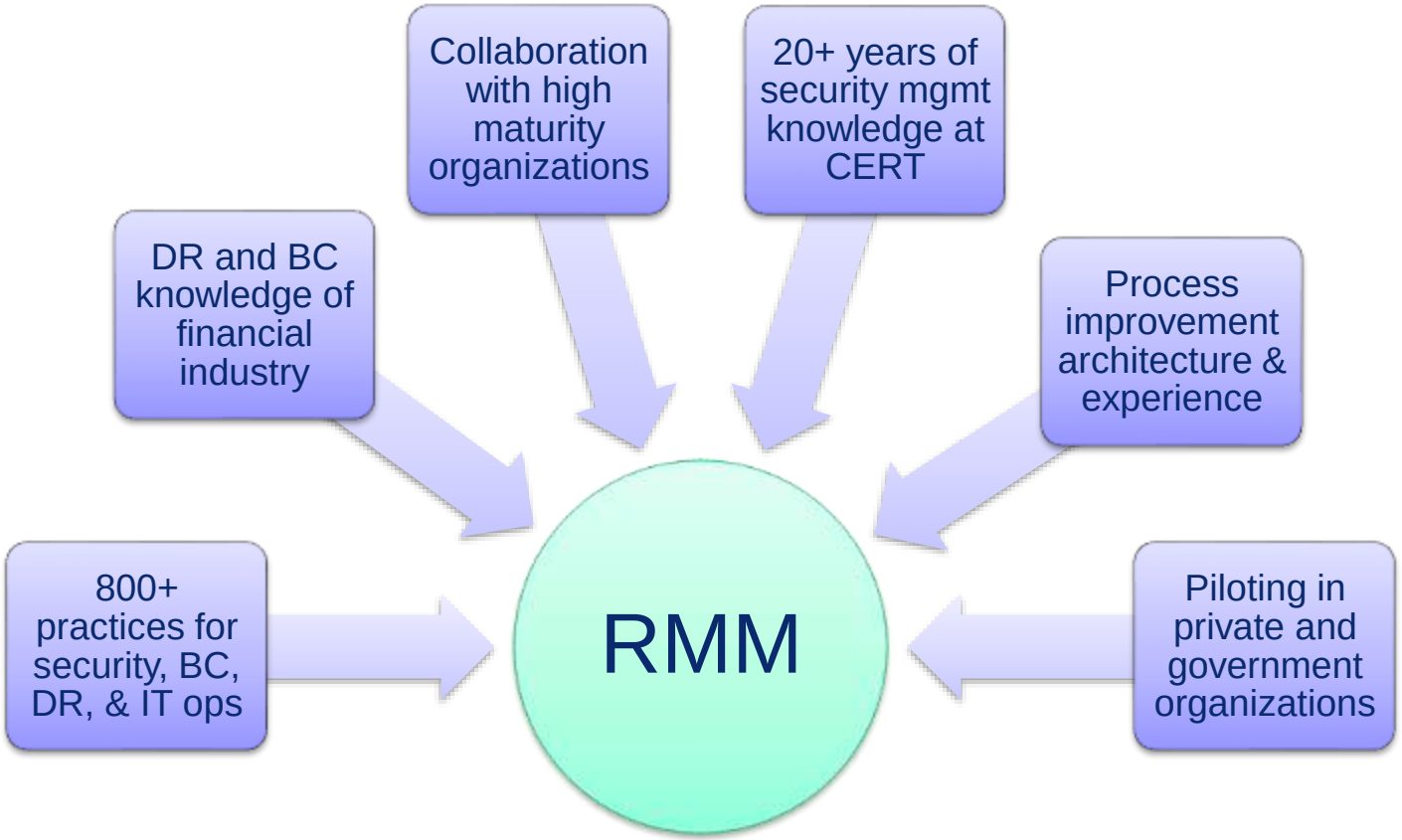
ENISA welcomes the initiative of the European Commission, and congratulates the High Representative Catherine Ashton, Vice-President Neelie Kroes and Commissioner Cecilia Malmström on their joint achievement.

The Executive Director of ENISA, Udo Helmbrecht, made a brief comment; "We are impressed by the comprehensiveness and ambitious scope of the Strategy. By successfully taking a broad approach from different sectors, notably also the European External Action Service, the Commission has provid the EU, which will also be of guidance for the Member States when formulating national policies. This interdependence of networks, and the importance of cybersecurity being at the top of the political age economy, society, business and citizens alike. The elements relating to ENISA in this communication are also a natural extension of the work of the Agency to date. We will analyse the Strategy and Directive further. Finally, we note that it is particularly timely and welcome in relation to the on-going ENISA mandate process."

Neelie Kroes, Catherine Ashton and Cecilia Malmström (from left to right)

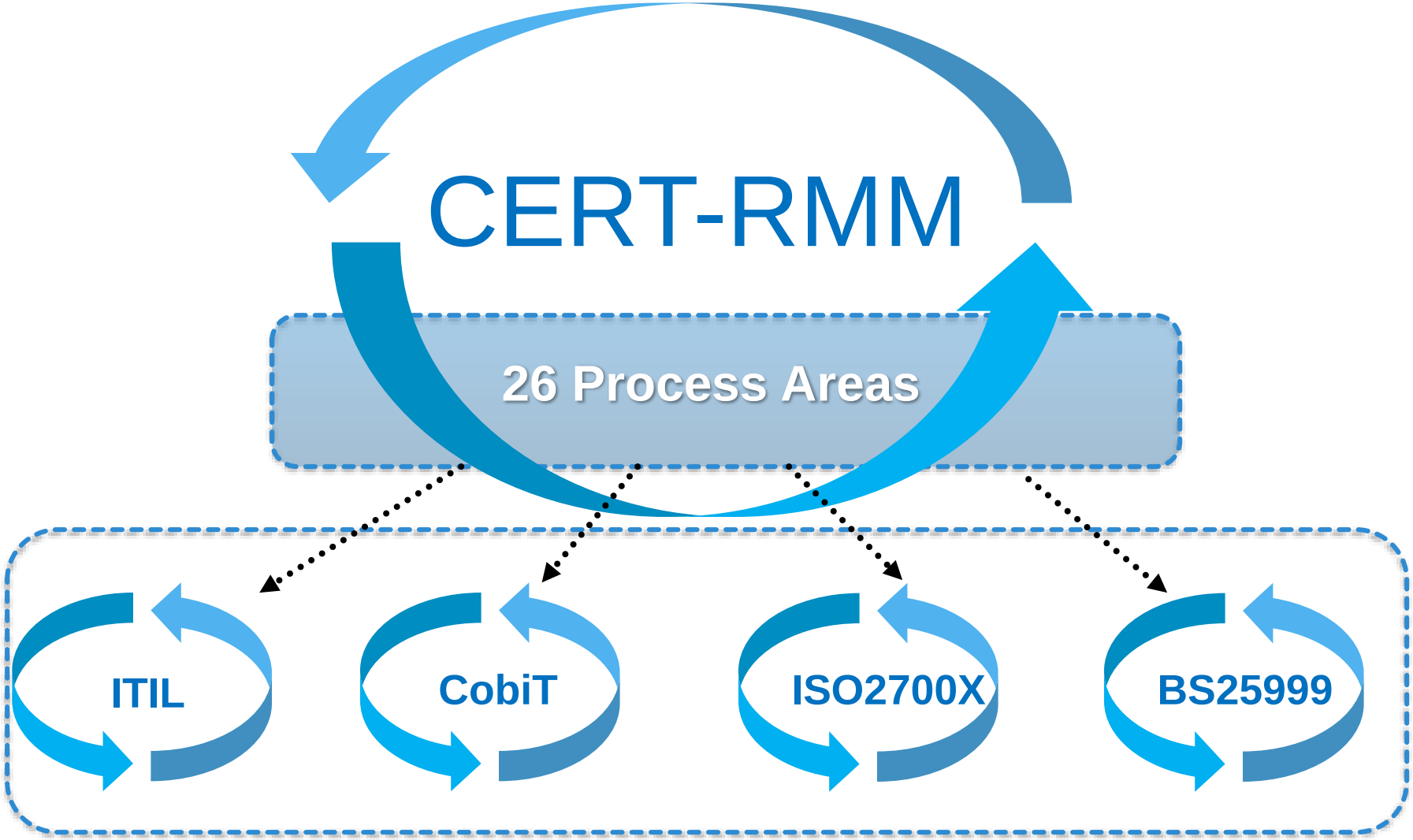

Новини от ПИК Информац
Проф. ген.-майор Румен Р
General Data Protectior
Not secure https://www.aerotrader.com/
AERO TRADER.
AeroTrader.com can no longer support visitors from within the European Union at this time. In compliance with GDPR any My Trader accounts, email correspondence & site activity has been removed from our database.
We are working to be able to serve EU visitors in the future.

How was RMM developed?



RMM codifies best practices for Info. Sec., IT DR, and BC from world leading organizations and numerous standards and codes of practice.

CERT-RMM as an Organizing/Integrating Structure



RMM – The Model

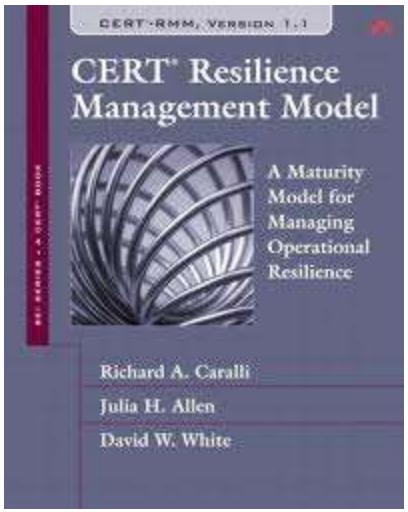
Guidelines and practices for

- Converging of security, business continuity, disaster recovery, and IT ops
- Implementing, managing, and sustaining operational resilience activities
- Managing operational risk through process
- Measuring and institutionalizing the resiliency process

Common vernacular and basis for planning, communicating, and evaluating improvements

Focuses on “what” not “how”

Organized into 26 process areas



Внимание: сигурността може да „хапе“

“Можете да направите една система сигурна като я направите или толкова проста, че просто знаете, че е сигурна, или толкова сложна, че никой не може да открие как да я използва.”

[Dan Geer, CISO In-Q-Tel; автор на Cyber*In*Security, 2003]

CERT-RMM: 26 process areas in 4 categories

Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management	
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training & Awareness
RISK	Risk Management

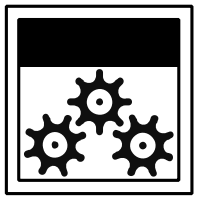
Operations	
AM	Access Management
EC	Environmental Control
EXD	External Dependencies Management
ID	Identity Management
IMC	Incident Management & Control
KIM	Knowledge & Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis & Resolution

Process Management	
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus

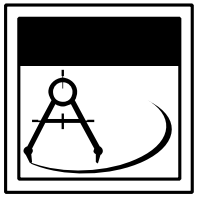
Model architecture

Composed of 26 process areas across four categories

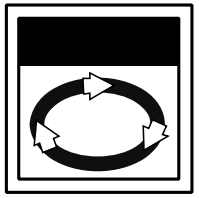
Enterprise Management



Operations Management

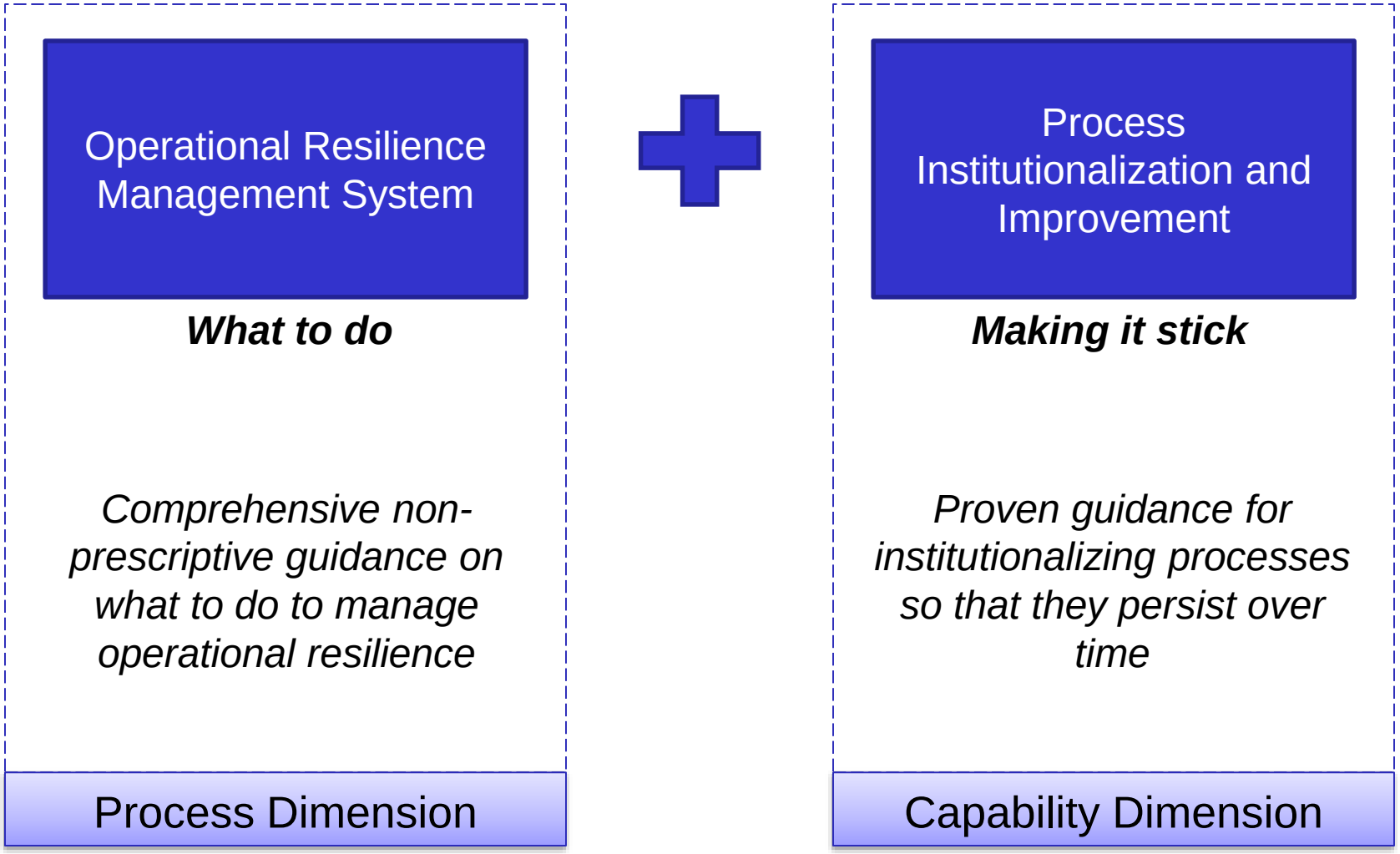


Engineering

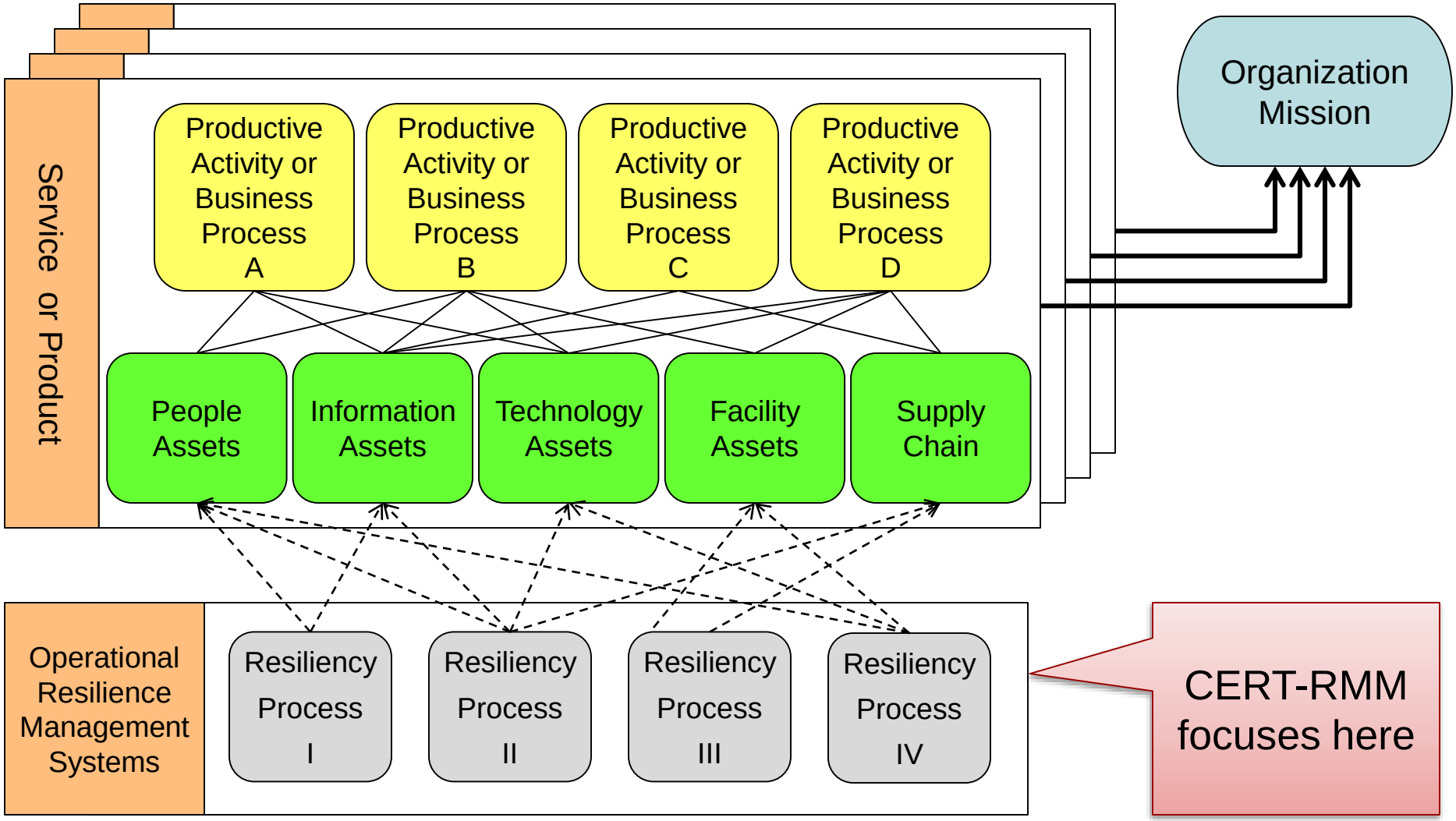


Process Management

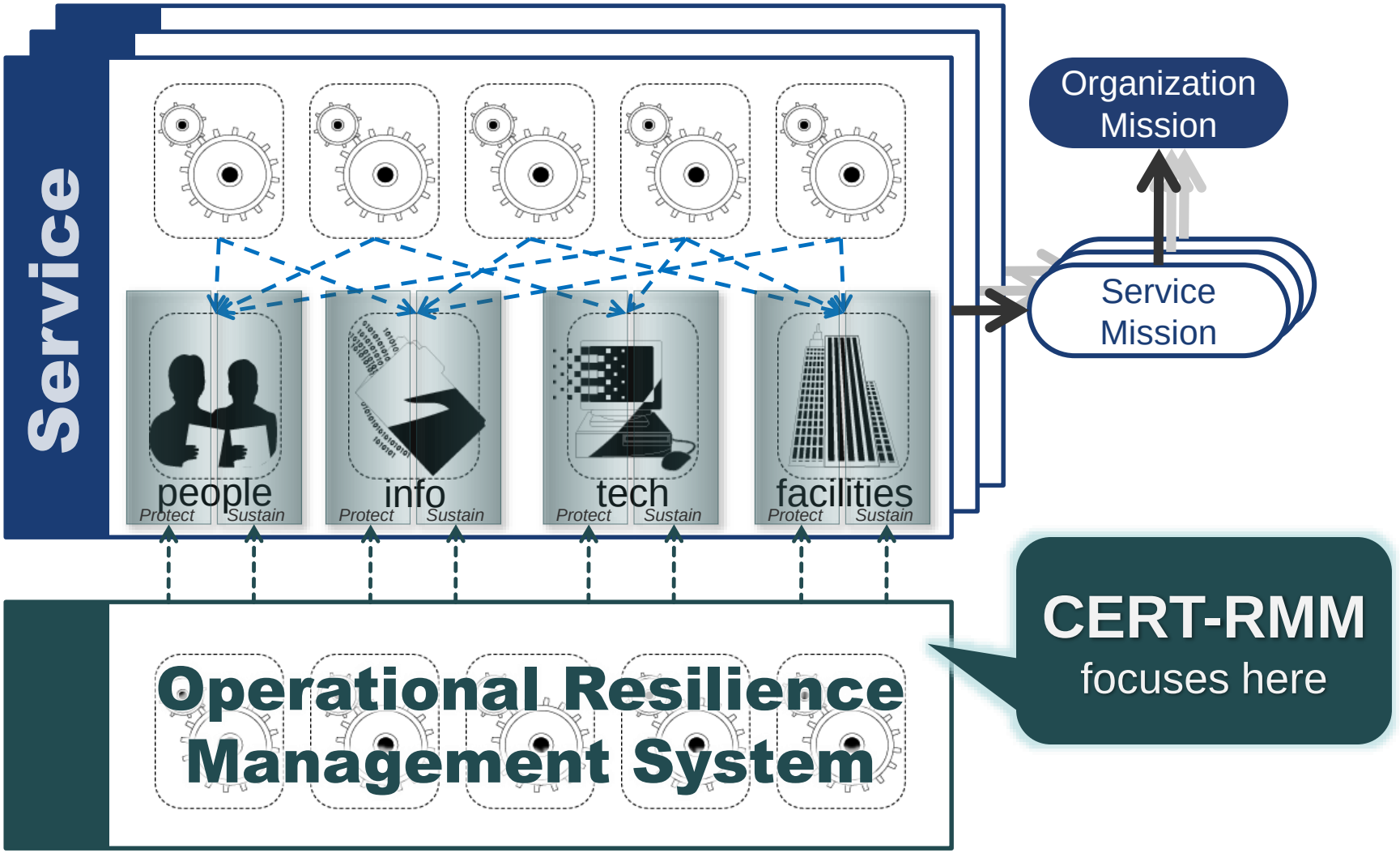
CERT-RMM Approach



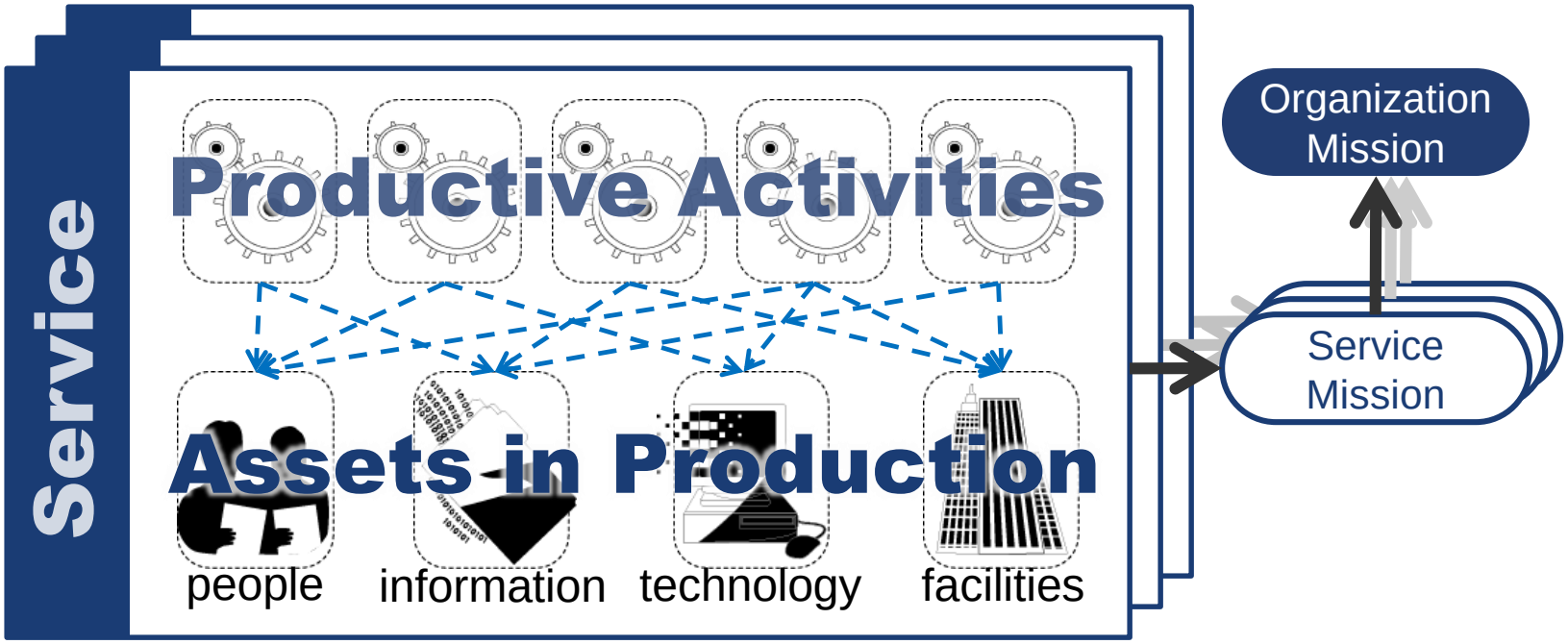
Organizational Context for Resiliency Activities



Organizational context



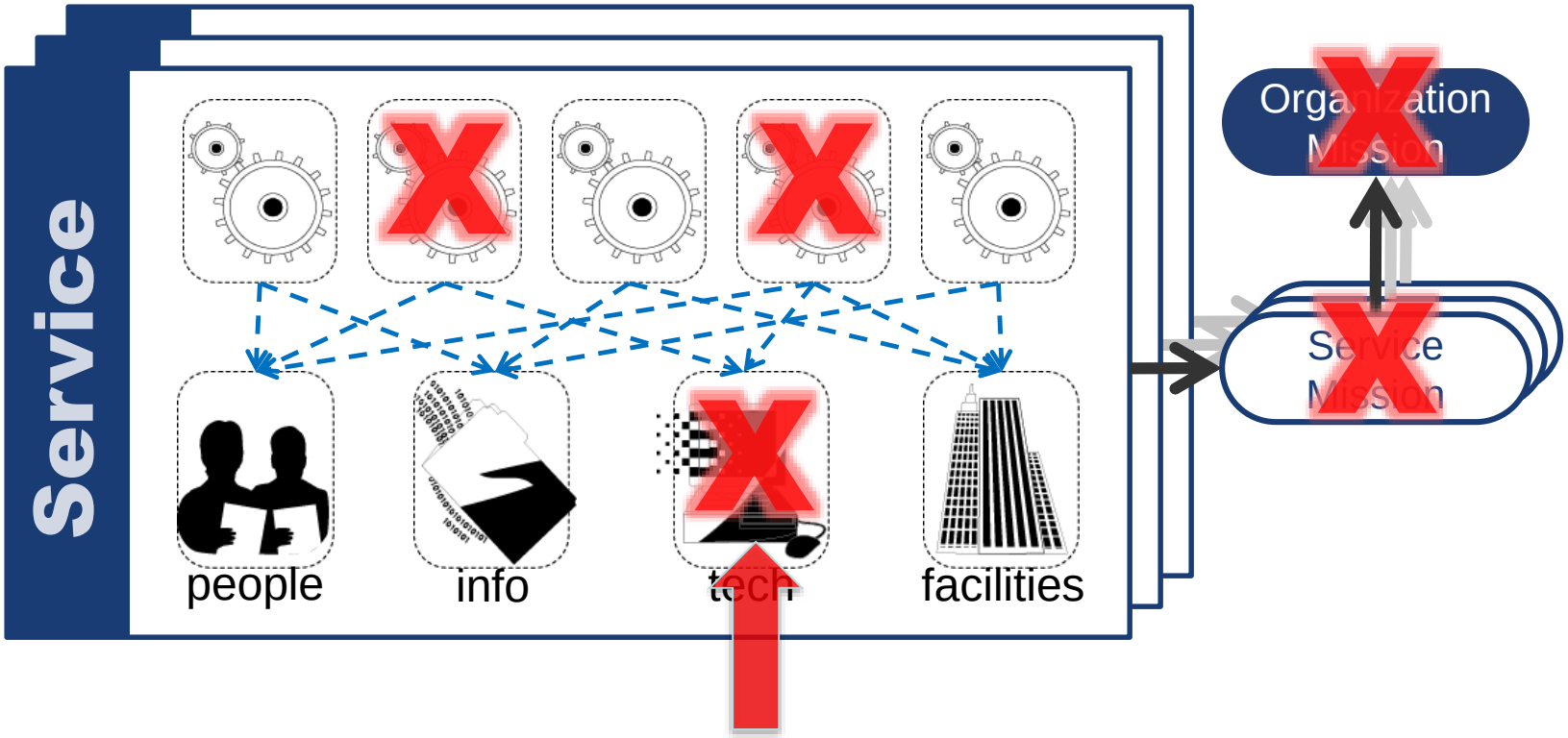
Organizational context



Four asset types:

- **People** – the human capital of the organization
- **Information** – data, records, knowledge in physical or digital form
- **Technology** – software, systems, hardware, network
- **Facilities** – offices, data centers, labs – the physical places

Organizational context - disruption



Operational risk can disrupt an asset

And lead to organizational disruption

☹ Anecdotal Evidence

Impact of top down risk decisions

Event declaration (NYC snow em

Supply chain resilience (NASDAQ after 9/11)

People resilience (two banks afte

Changes in operational environm

Technology resilience (Egypt inte

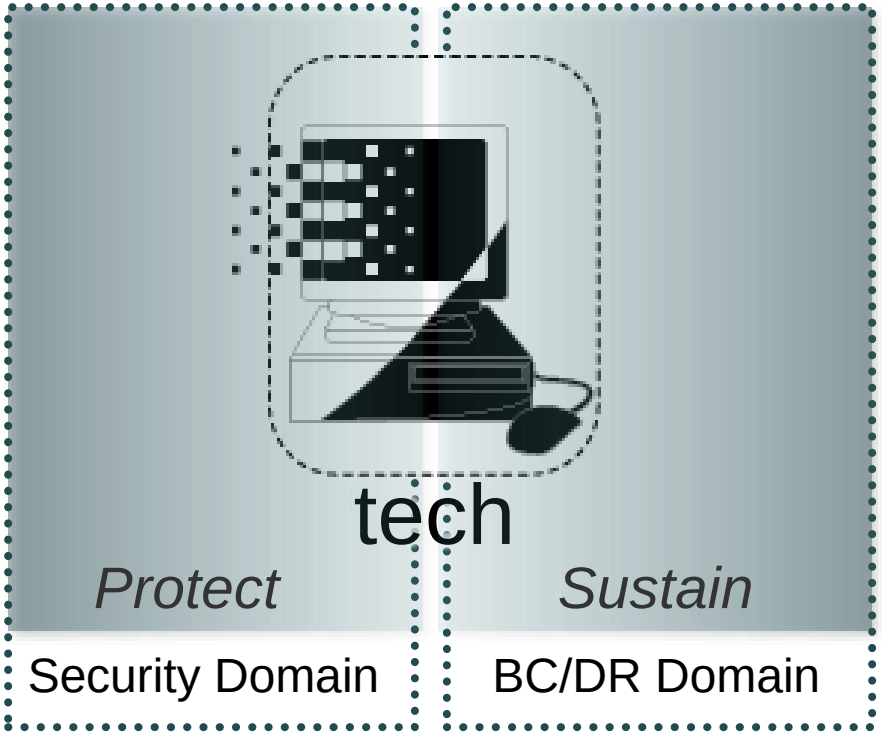
Prioritizing external relationships

Determining critical assets (netwo

Supply chain resilience: NASDAQ 9/11; fully ready to operate within 24 hours; no trading partners; need to manage your supply chain both upstream and downstream

USPIS dealing with white powder; never an issue until 9/11; they have white powder all of the time (coating on magazines etc.); after 9/11 white powder took on a totally different meeting; could close down a postal sorting facility for weeks; hazmat team; analyze white power; eradicate/remediate; then reopen; implemented a **white powder incident management process in all sorting facilities;**

Building resilience at the asset level



Protection strategies

Keep assets from exposure to disruption

Typically implemented as "security" activities

Sustainment strategies

Keep assets productive during adversity

Typically implemented as "business continuity" activities

Types of requirements

Confidentiality – Ensuring that only authorized people, processes, or devices have access to an information asset

Integrity – Ensuring that an asset remains in the condition intended and so continues to be useful for the purposes intended

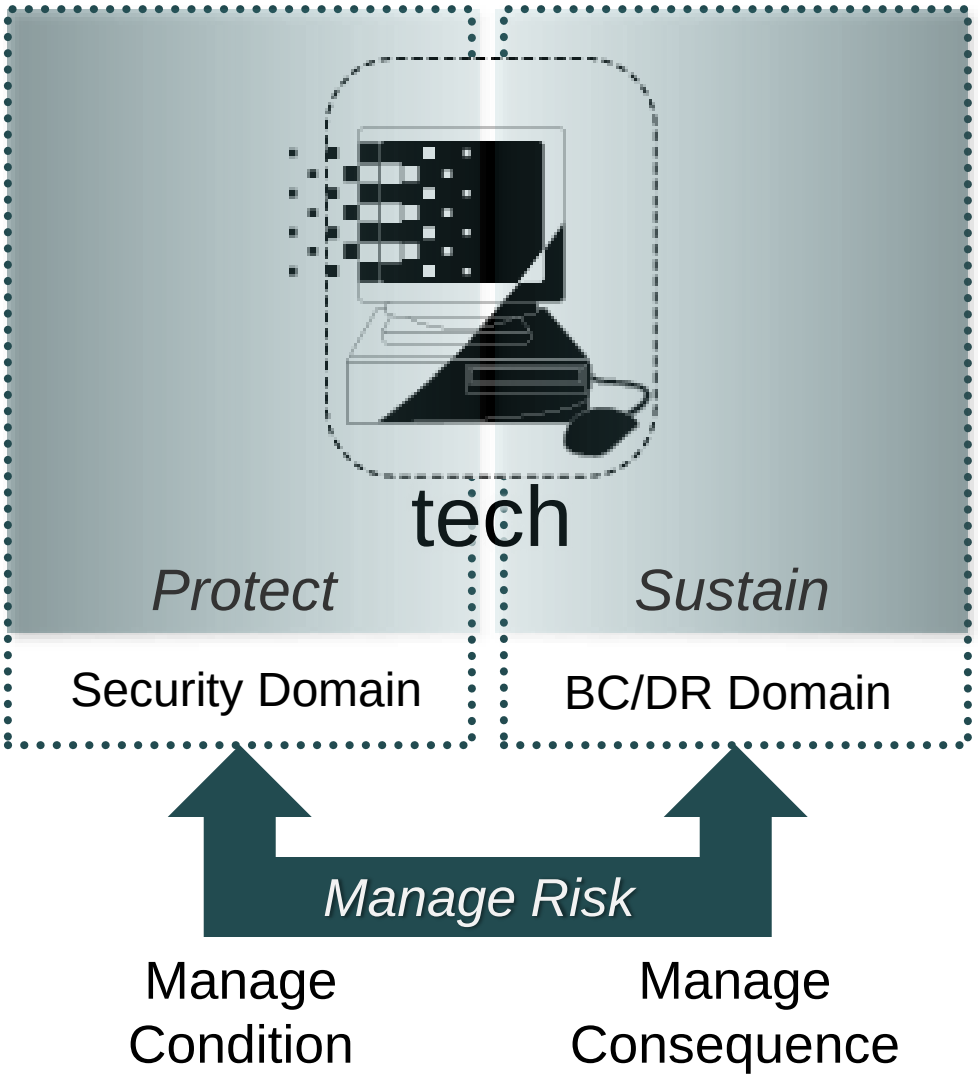
Availability – Ensuring that an asset remains accessible to authorized users (people, processes, or devices) whenever it is needed

Applicability of requirements

Not all resilience requirement types apply to all asset types.

Resilience Requirement	Asset Type			
	People	Information	Technology	Facilities
Confidentiality	--	X	--	--
Integrity	X*	X	X	X
Availability	X	X	X	X

Resilience strategy



The optimal “mix” of protection and sustainment strategies

Depends on the **value of the asset to the service** and the **cost of deploying and maintaining the strategy**

BC, security, & IT operations collaborating to manage risk

Engineering process areas

Establishing resilience for organizational assets and services

ADM – Asset Definition and Management

RRD – Resilience Requirements Development

RRM – Resilience Requirements Management

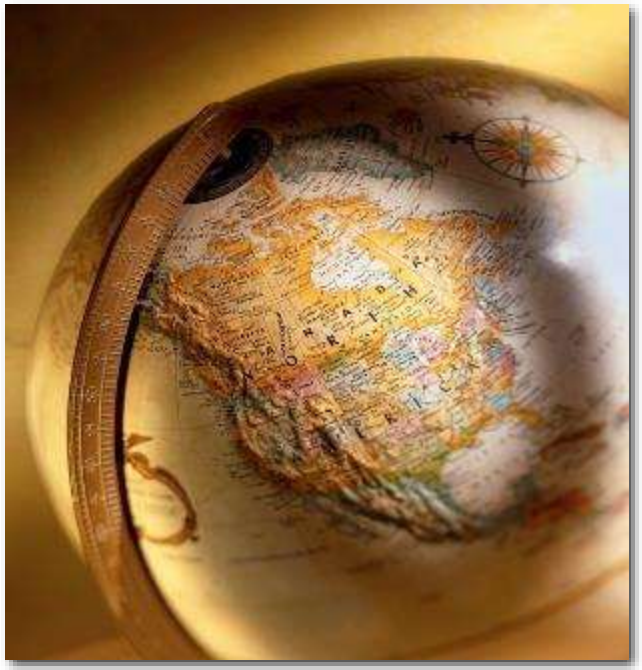
SC – Service Continuity

CTRL – Controls Management

RTSE – Resilient Technical Solution Engineering

Enterprise management process areas

Supporting the resilience process



EF – Enterprise Focus

COMP – Compliance

FRM – Financial Resource Management

HRM – Human Resource Management

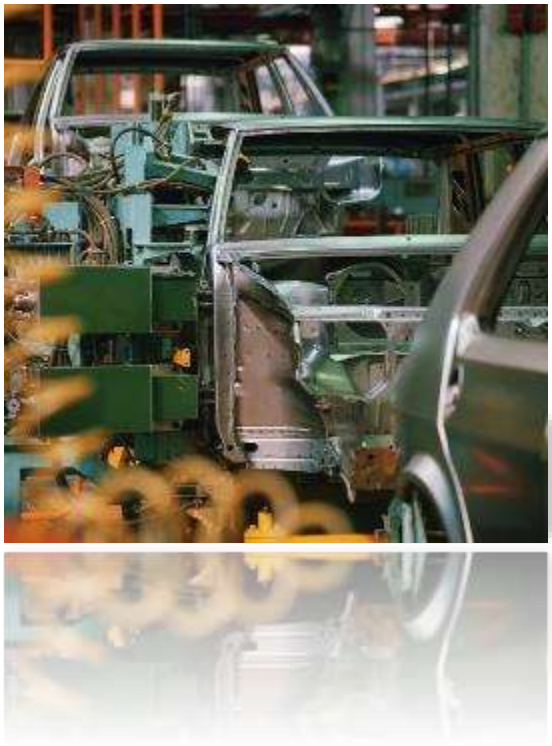
RISK – Risk Management

COMM – Communications

OTA – Organizational Training and Awareness

Operations process areas

Managing the operational aspects of resilience



PM – People Management

KIM – Knowledge and Information Management

TM – Technology Management

EC – Environmental Control

AM – Access Management

ID – Identity Management

IMC – Incident Management and Control

VAR – Vulnerability Analysis and Resolution

EXD – External Dependencies Management

Process management process areas

Defining, planning, deploying, implementing, monitoring, controlling, appraising, measuring, and improving processes

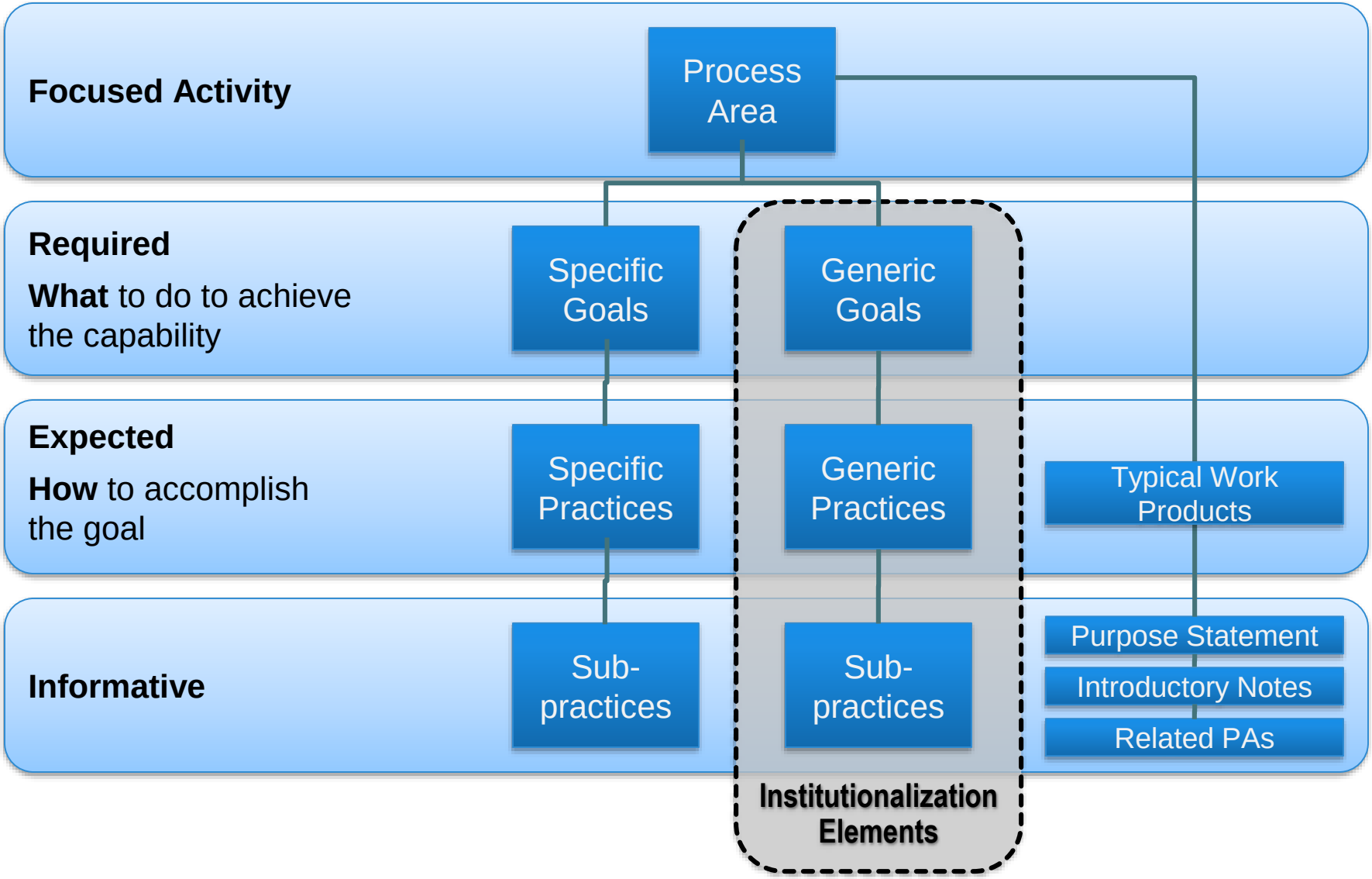
MON – Monitoring

MA – Measurement and Analysis

OPD – Organizational Process Definition

OPF – Organizational Process Focus

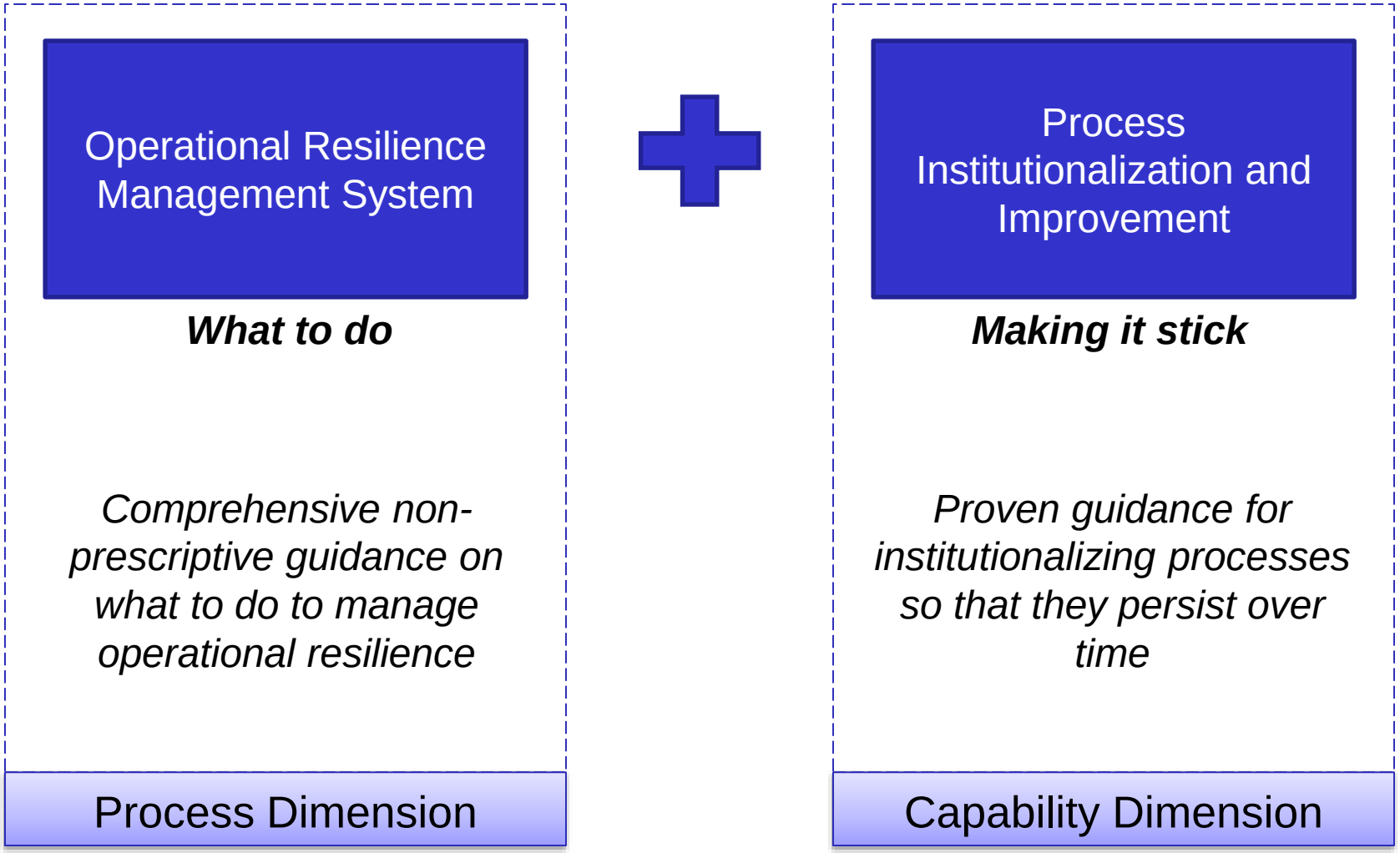
CERT-RMM process area architecture



CERT-RMM numbers

Process institutionalization in CERT-RMM

CERT-RMM Approach



What do these organizations have in common?

What do these organizations have in common?

Customer Happiness

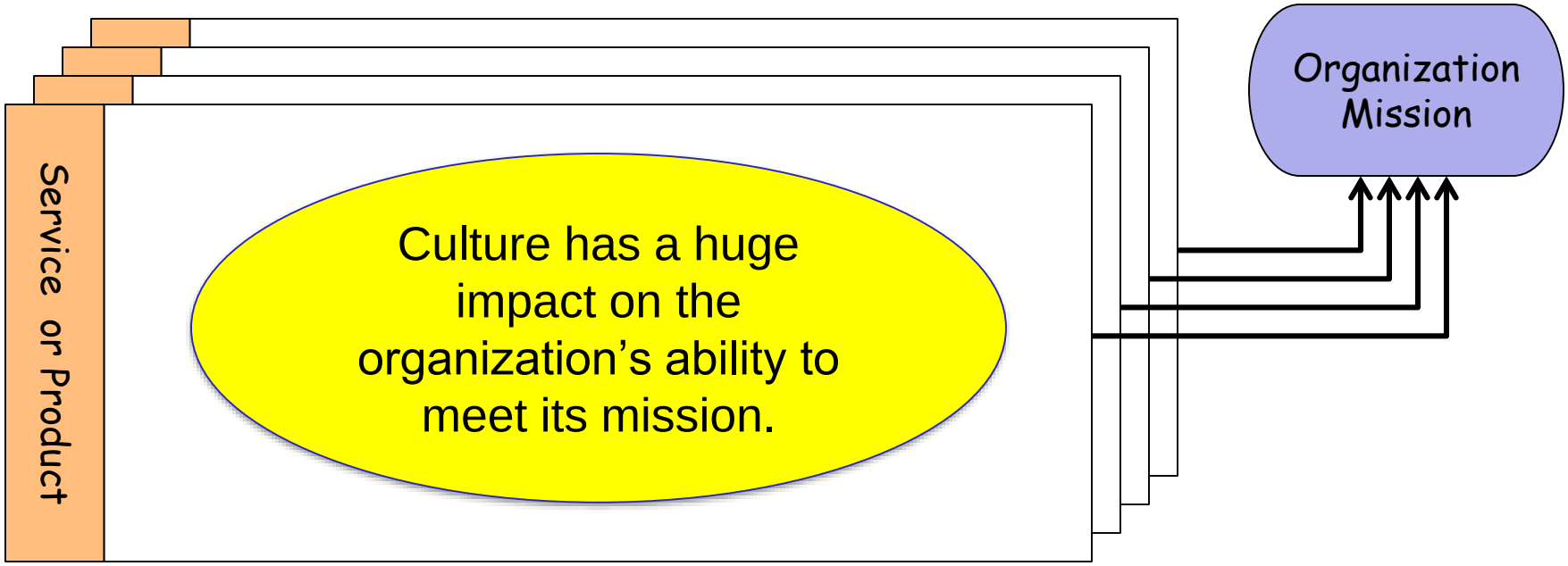
Chain of Command
Unit Cohesion
Regulations

Strong Culture

Customer Service

Tradition
Protection

Institutionalizing a Culture of Resiliency



Institutionalizing a Culture of Resiliency

institutionalize *verb* (CUSTOM) (UK USUALLY **institutionalise**) UK US /ɪnˌtɪ.stɪˈtjuː.ʃᵊn.ə.laɪz/ (US) /-ˈtuː-/ [T]

to make something become part of a particular society, system, or organization

What was once an informal event has now become institutionalized.

Organizations must provide explicit guidance for institutionalizing resilience activities so that they persist over time

Ask not how well am I performing today?

Ask do I have what it takes to sustain high performance beyond today?

Process

A set of practices performed to achieve a given purpose

Utilizes people and technology

Defined at many levels

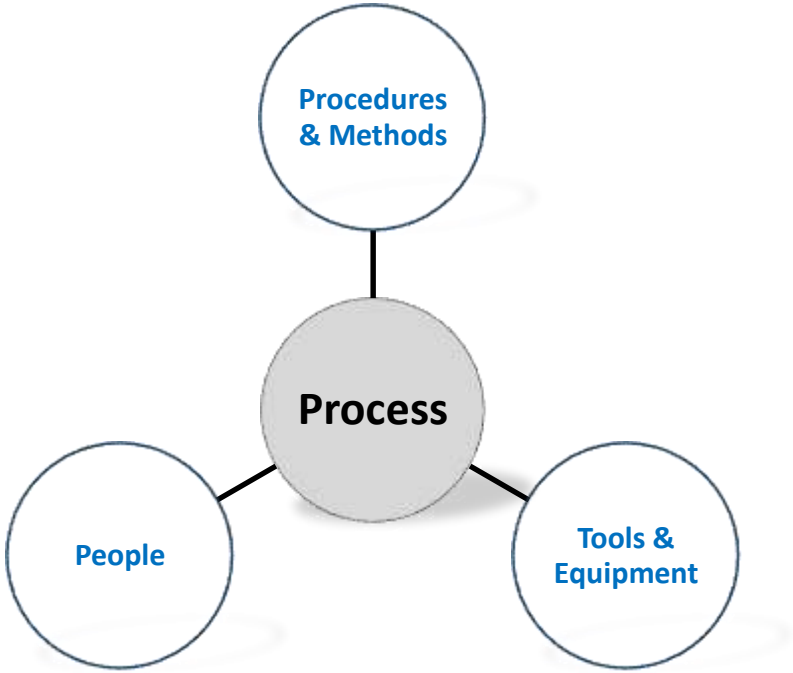
- Higher order “process” such as the “software engineering process” or the “resilience management process”
- Lower order “process” such as the invoicing process or the check cashing process

Regardless of level, all have the same basic attributes—**an ordered way to achieve something**

The value of process

Organizational improvement requires a focus on three critical dimensions: people, procedures and methods, and tools and equipment.

Process is what unifies these critical dimensions toward organizational objectives.



The quality of a system or product is highly influenced by the quality of the process used to acquire, develop, and maintain it. *

*Source: *CMMI® for Development, Version 1.2*, CMU/SEI-2006-TR-008, Software Engineering Institute, Carnegie Mellon University, August 2006

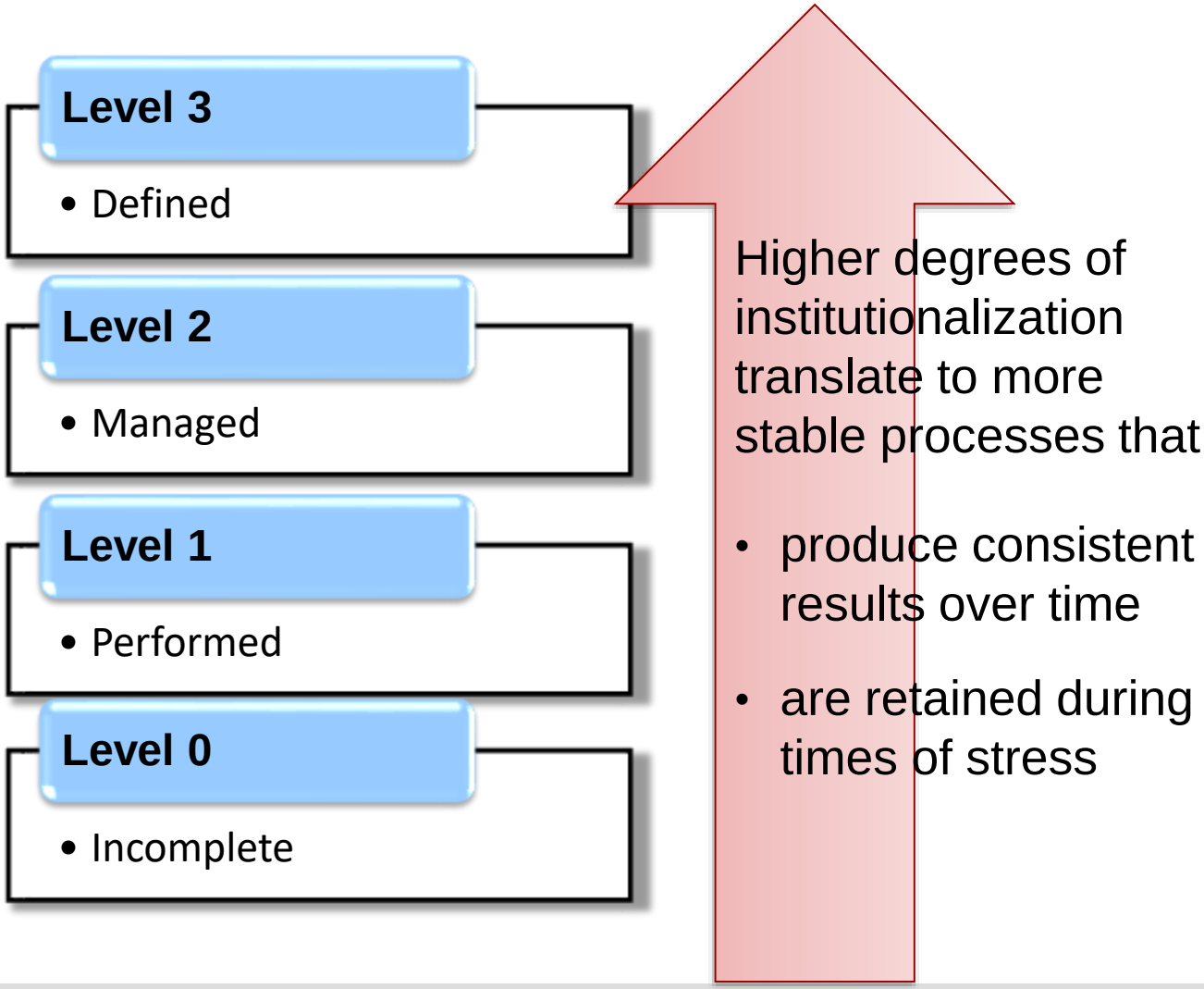
Process institutionalization in CERT-RMM

Capability levels are used in CERT-RMM to measure process institutionalization

Processes are acculturated, defined, measured, and governed

Practices are performed

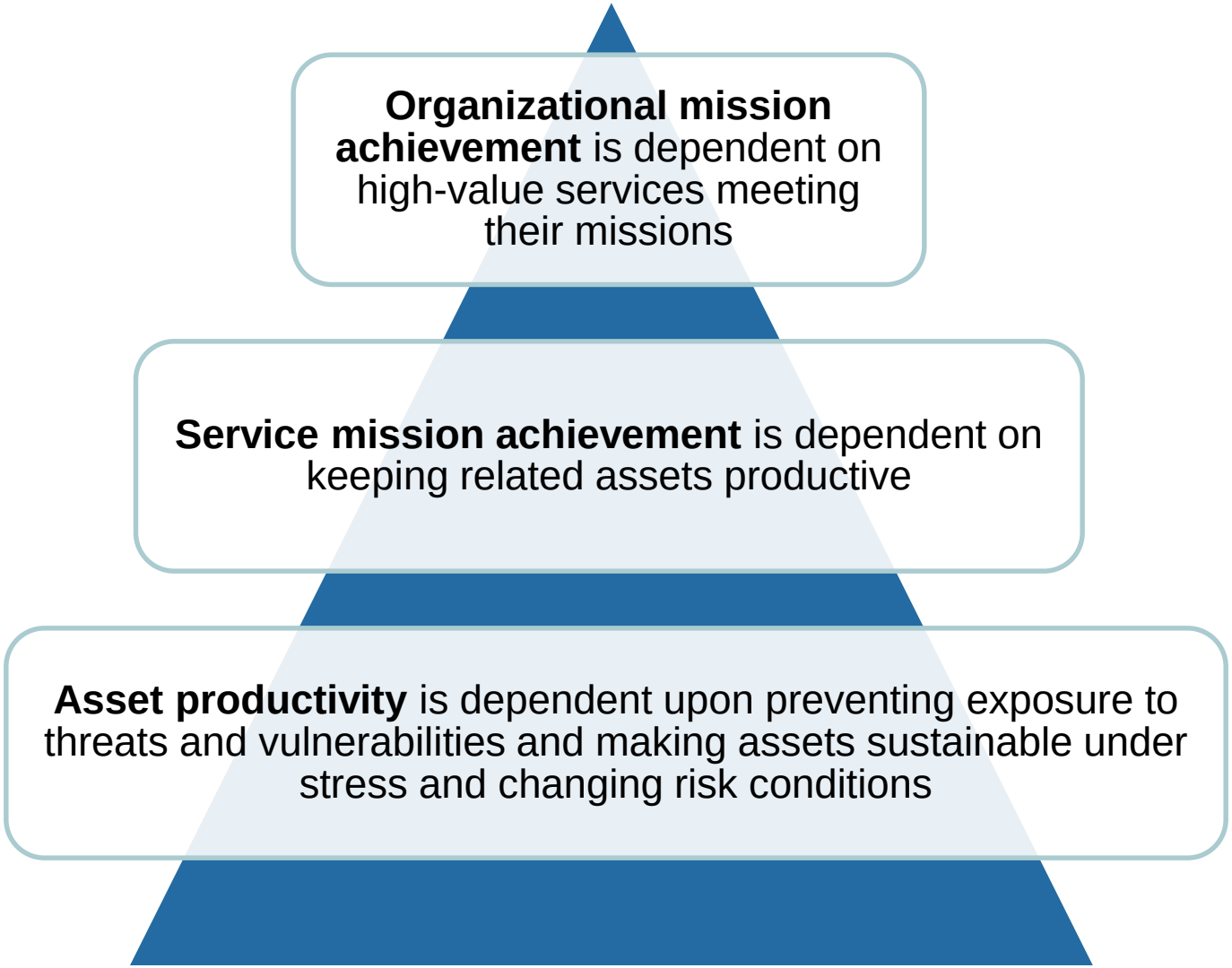
Practices are incomplete



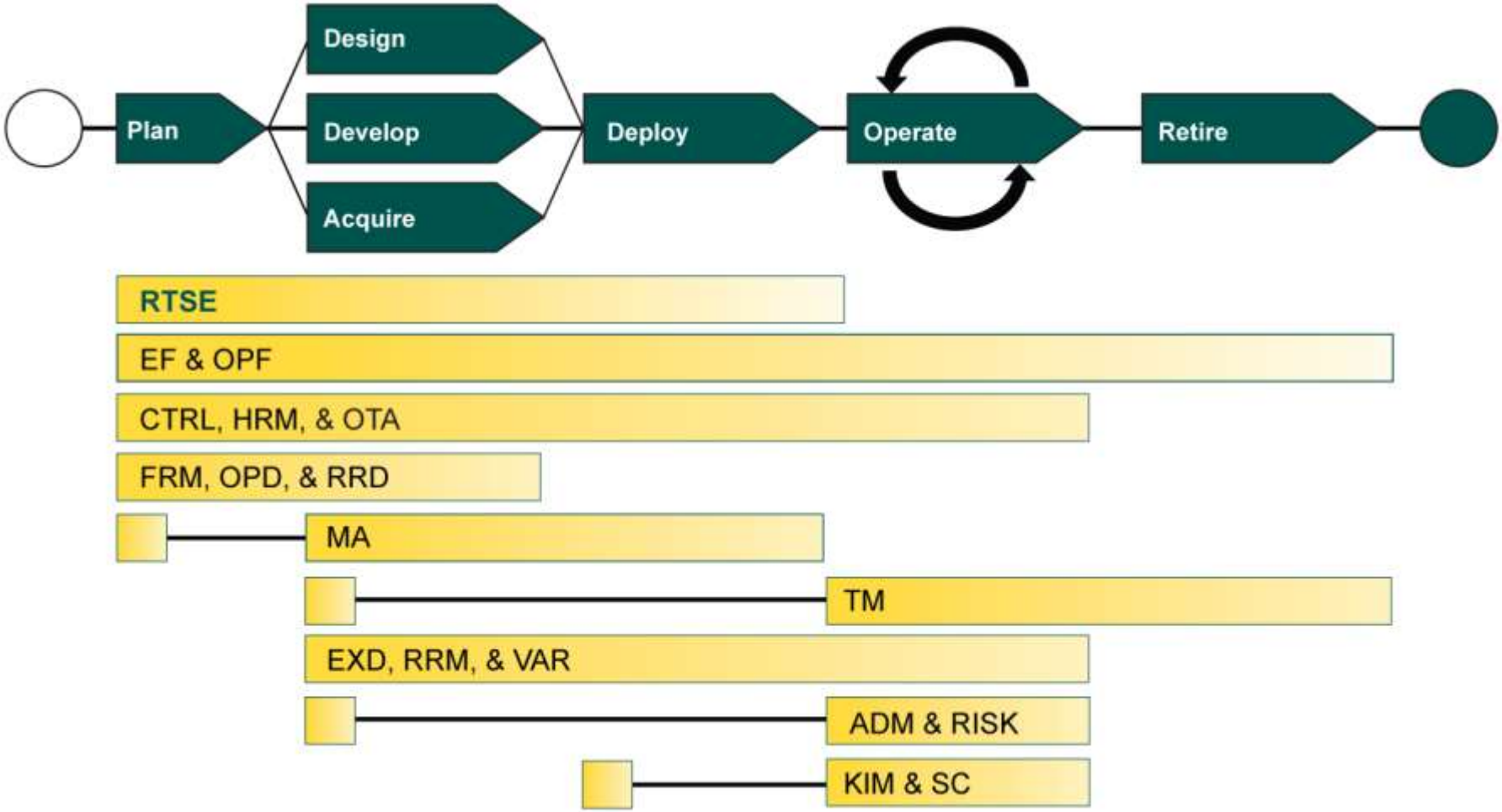
Higher degrees of institutionalization translate to more stable processes that

- produce consistent results over time
- are retained during times of stress

The Success Pyramid



CERT-RMM for software assurance



For Software Assurance

Access Management
Asset Definition and Management
Communications
Compliance
Controls Management
Enterprise Focus
Environmental Control
External Dependencies
Financial Resource Management
Human Resource Management
Identity Management
Incident Management & Control
Knowledge & Information Mgmt

Measurement and Analysis
Monitoring
Organizational Process Focus
Organizational Process Definition
Organizational Training & Awareness
People Management
Resiliency Requirements Development
Resiliency Requirements Management
Resilient Technical Solution Engr.
Risk Management
Service Continuity
Technology Management
Vulnerability Analysis & Resolution

For Managing Cloud Computing

Access Management
Asset Definition and Management
Communications
Compliance
Controls Management
Enterprise Focus
Environmental Control
External Dependencies
Financial Resource Management
Human Resource Management
Identity Management
Incident Management & Control
Knowledge & Information Mgmt

Measurement and Analysis
Monitoring
Organizational Process Focus
Organizational Process Definition
Organizational Training & Awareness
People Management
Resiliency Requirements Development
Resiliency Requirements Management
Resilient Technical Solution Engr.
Risk Management
Service Continuity
Technology Management
Vulnerability Analysis & Resolution

Sample scoping:
For Managing the Insider Threat Challenge

Access Management
Asset Definition and Management
Communications
Compliance
Controls Management
Enterprise Focus
Environmental Control
External Dependencies
Financial Resource Management
Human Resource Management
Identity Management
Incident Management & Control
Knowledge & Information Mgmt

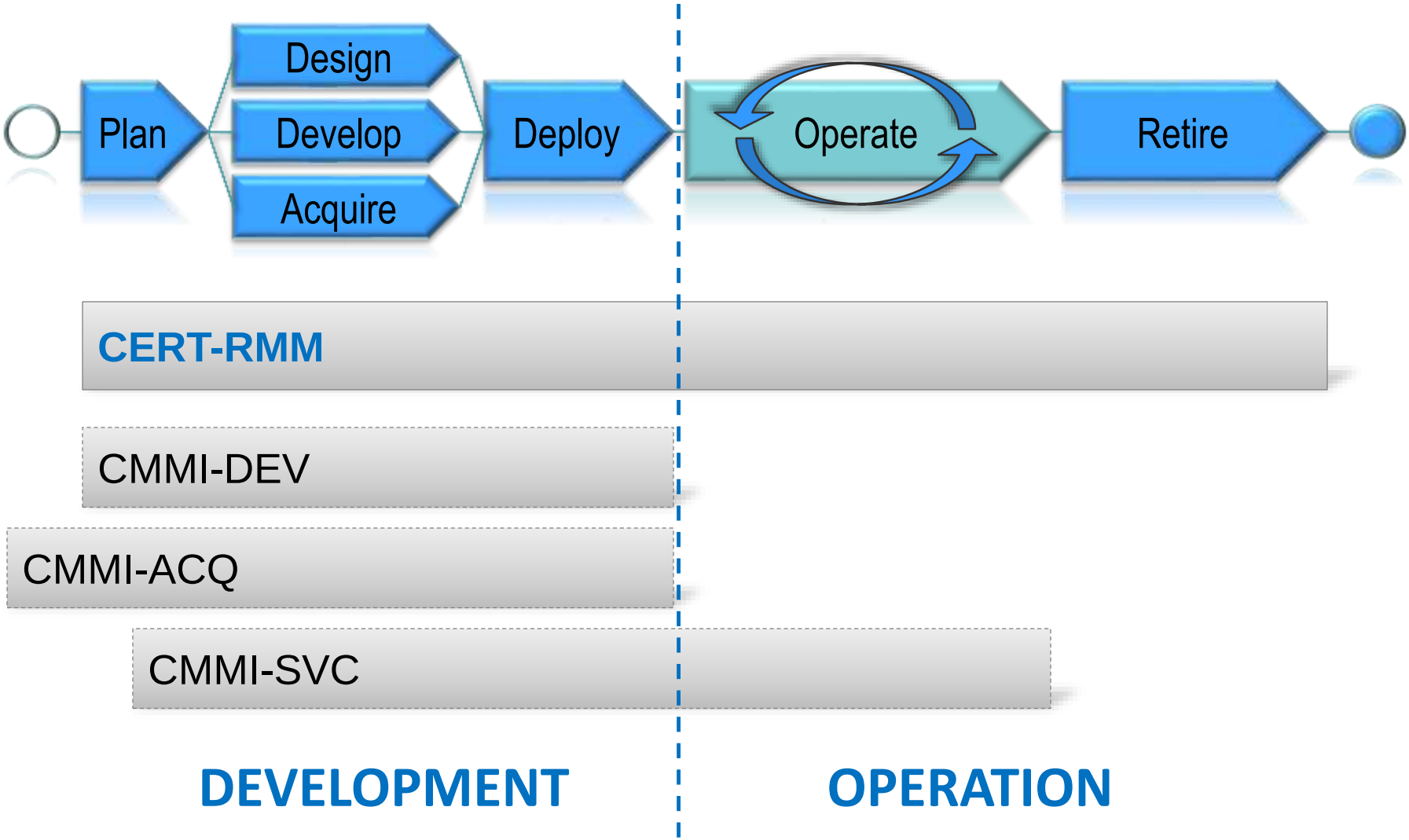
Measurement and Analysis
Monitoring
Organizational Process Focus
Organizational Process Definition
Organizational Training & Awareness
People Management
Resiliency Requirements Development
Resiliency Requirements Management
Resilient Technical Solution Engr.
Risk Management
Service Continuity
Technology Management
Vulnerability Analysis & Resolution

For Managing Disaster Recovery, COOP, Business Continuity Policies

Access Management
Asset Definition and Management
Communications
Compliance
Controls Management
Enterprise Focus
Environmental Control
External Dependencies
Financial Resource Management
Human Resource Management
Identity Management
Incident Management & Control
Knowledge & Information Mgmt

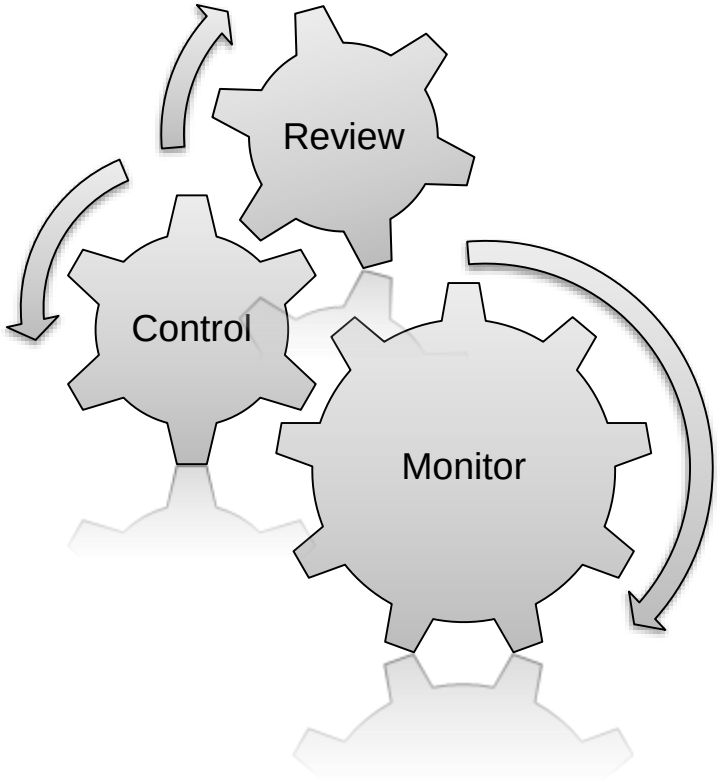
Measurement and Analysis
Monitoring
Organizational Process Focus
Organizational Process Definition
Organizational Training & Awareness
People Management
Resiliency Requirements Development
Resiliency Requirements Management
Resilient Technical Solution Engr.
Risk Management
Service Continuity
Technology Management
Vulnerability Analysis & Resolution

CERT-RMM position in life cycle



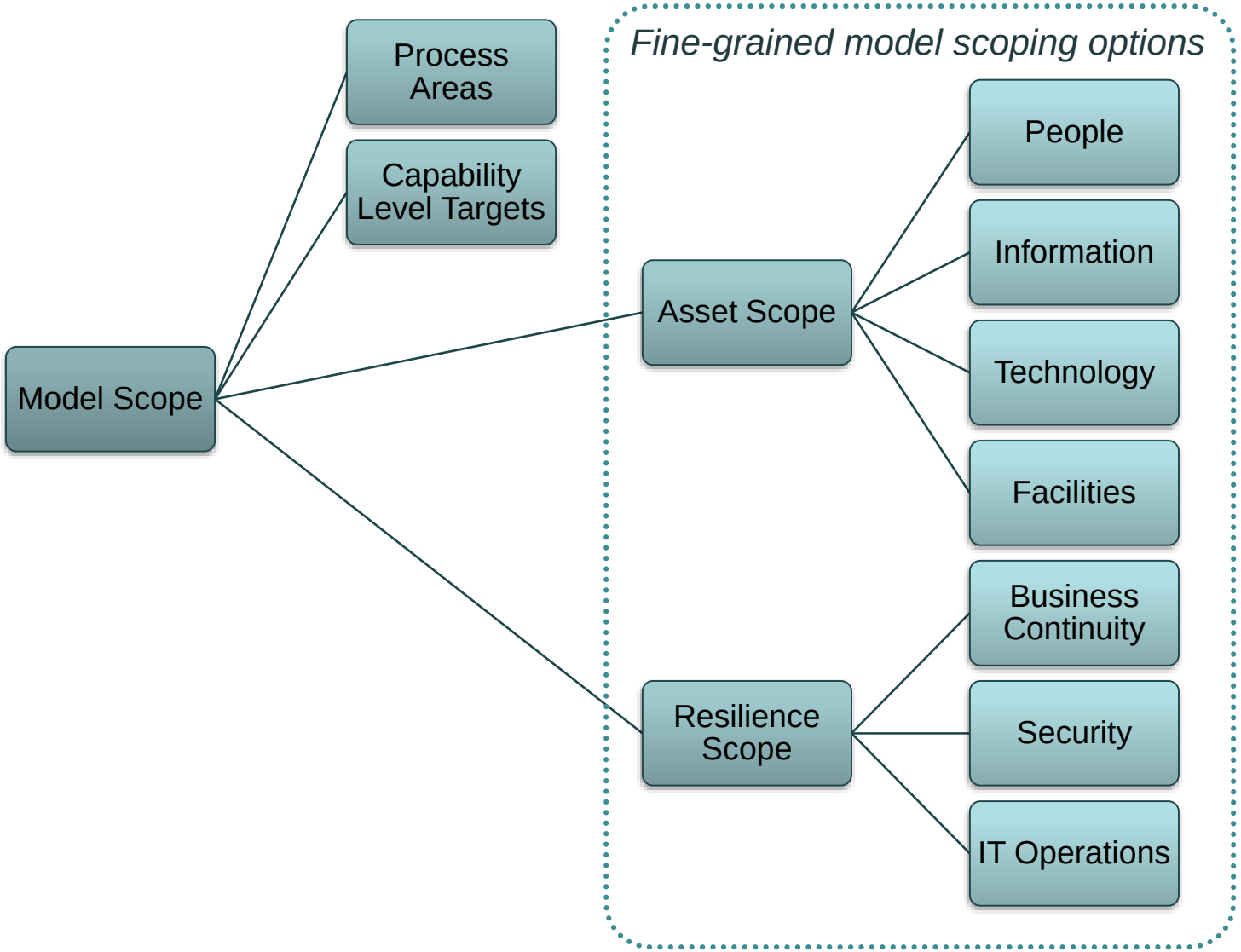
Level 2 generic goals and practices

Generic Goal 2
Institutionalize a Managed Process

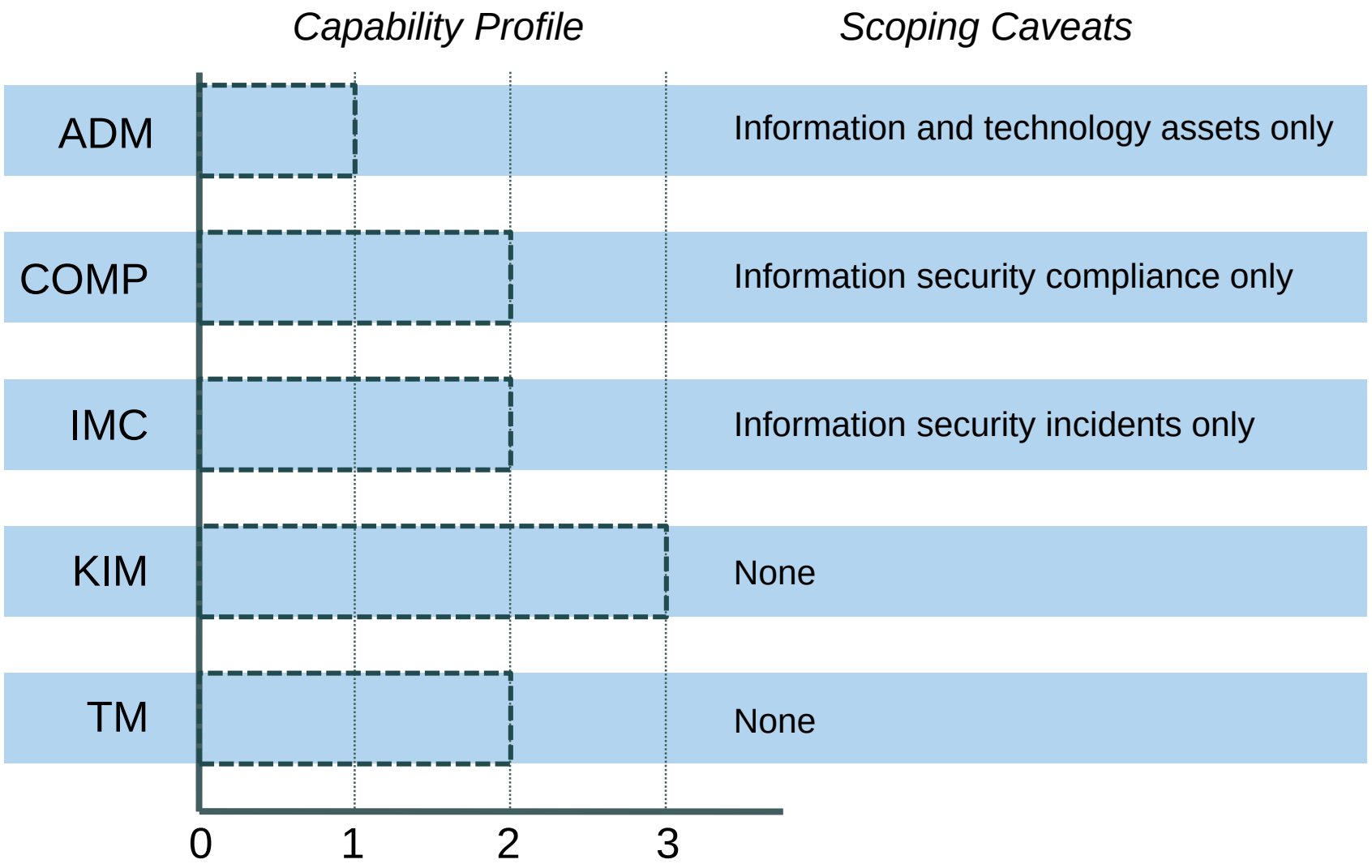


Number	Generic Practice
GG2.GP1	Establish Process Governance
GG2.GP2	Plan the Process
GG2.GP3	Provide Resources
GG2.GP4	Assign Responsibility
GG2.GP5	Train People
GG2.GP6	Manage Work Product Configurations
GG2.GP7	Identify and Involve Relevant Stakeholders
GG2.GP8	Monitor and Control the Process
GG2.GP9	Objectively Evaluate Adherence
GG2.GP10	Review Status with Higher-Level Management

CERT-RMM model scope in detail -2



CERT-RMM model scope example



Foundational process areas in CERT-RMM

PA	Foundational Elements
ADM	▪ Connects directly to practices in asset-based process areas KIM, TM, EC, and PM ▪ Strong relationship with EF (on asset-service connection)
AM	▪ Connects directly to practices in asset-based process areas KIM, TM, and EC ▪ Strong relationship with ID (ID and AM should be considered together)
CTRL	▪ Connects directly to practices in asset-based process areas KIM, TM, EC, and PM
EF	▪ Elements of EF appear in capability level 2 generic goals and practices ▪ Elements of EF relate to RISK, COMP, and FRM
FRM	▪ Elements of FRM appear in capability level 2 generic goals and practices
HRM	▪ Elements of HRM appear in capability level 2 generic goals and practices ▪ Strong relationship with OTA and PM
MON	▪ Strong relationship with several PAs, including COMP, RRM, IMC, EF, MA, and VAR
OTA	▪ Elements of OTA appear in capability level 2 generic goals and practices
RISK	▪ Connects directly to practices in asset-based process areas KIM, TM, EC, and PM ▪ Elements of RISK appear in capability level 2 generic goals and practices ▪ Strong relationship with EF, VAR, and IMC
RRD	▪ Connects to ADM to establish assets and their resilience requirements
SC	▪ Connects directly to practices in asset-based process areas KIM, TM, EC, and PM

Sample class A appraisal output -1

SC: Service Continuity

S	**SG1**	**Prepare for service continuity**
LI	SG1.SP1	Plan for service continuity
LI	SG1.SP2	Establish standards and guidelines for service continuity
NS	**SG2**	**Identify and prioritize high-value services**
FI	SG2.SP1	Identify the organization's high-value services
PI	SG2.SP2	Identify internal and external dependencies and interdependencies
LI	SG2.SP3	Identify vital organizational records and databases
S	**SG3**	**Develop service continuity plans**
FI	SG3.SP1	Identify plans to be developed
FI	SG3.SP2	Develop and document service continuity plans
FI	SG3.SP3	Assign staff to service continuity plans
LI	SG3.SP4	Store and secure service continuity plans
LI	SG3.SP5	Develop service continuity plan training
NS	**SG4**	**Validate service continuity plans**
LI	SG4.SP1	Validate plans to requirements and standards
PI	SG4.SP2	Identify and resolve plan conflicts
S	**SG5**	**Exercise service continuity plans**
FI	SG5.SP1	Develop testing program and standards
FI	SG5.SP2	Develop and document test plans
FI	SG5.SP3	Exercise plans
FI	SG5.SP4	Evaluate plan test results
NS	**SG6**	**Execute service continuity plans**
FI	SG6.SP1	Execute plans
NI	SG6.SP2	Measure the effectiveness of the plans in operation
S	**SG7**	**Maintain service continuity plans**
LI	SG7.SP1	Establish change criteria
LI	SG7.SP2	Maintain changes to plans
NS	**GG2**	**Institutionalize a managed process**
PI	GG2.GP1	Establish process governance
LI	GG2.GP2	Plan the process
LI	GG2.GP3	Provide resources
FI	GG2.GP4	Assign responsibility
LI	GG2.GP5	Train people
LI	GG2.GP6	Manage work product configurations
PI	GG2.GP7	Identify and involve relevant stakeholders
FI	GG2.GP8	Monitor and control the process
PI	GG2.GP9	Objectively evlauate adherence
FI	GG2.GP10	Review status with higher-level managers
NS	**GG3**	**Institutionalize a defined process**
PI	GG3.GP1	Establish a defined process
NI	GG3.GP2	Collect improvement information

Key:

Goal Ratings

S	Satisfied
NS	Not Satisfied

Practice Characterizations

FI	Fully Implemented
LI	Largely Implemented
PI	Partially Implemented
NI	Not Implemented
NY	Not Yet

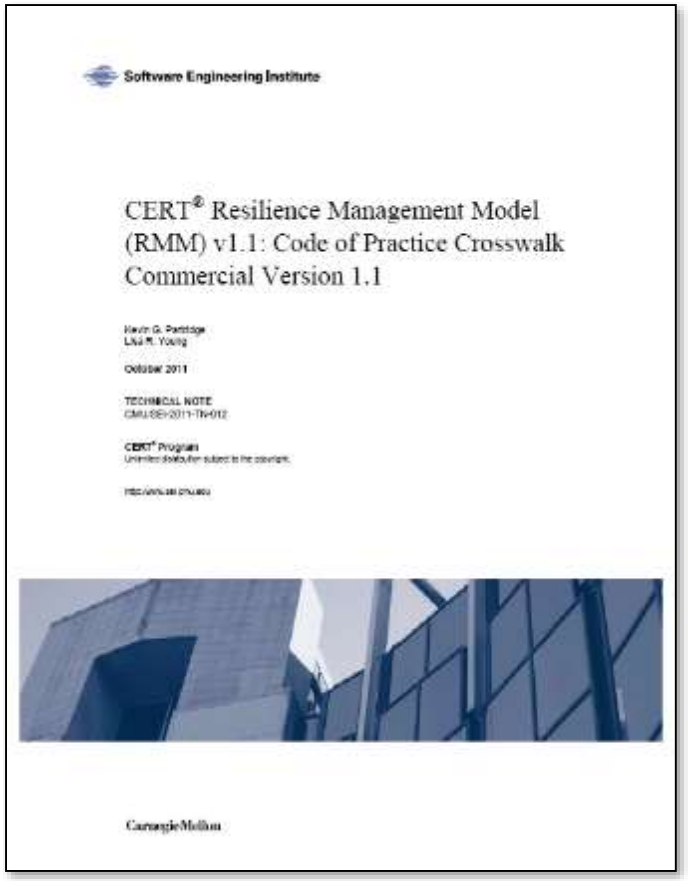
RMM Code of Practice Crosswalk

Links RMM practices to common codes of practice and standards

Including:

- ANSI/ASIS SPC.1-2009
- BS25999
- COBIT 4.1
- COSO ERM Framework
- CMMI
- FFIEC BCP Handbook
- ISO 20000-2
- ISO/IEC 24762
- ISO/IEC 24762
- ISO/IEC 27005
- ISO/IEC 31000
- NFPA 1600
- PCI DSS
- Etc…

A version of the crosswalk to common NIST standards is available.



RMM Code of Practice Crosswalk

Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG5.SP4 Evaluate Plan Test Results Subpractices 1. Compare actual test results with expected test results and test objectives. 2. Document areas of improvement for service continuity plans. 3. Document areas of improvement for testing service continuity plans	4.5.3	5.4.1 9.3.2		SCON:SP3.3	DS4.5	Board and Senior Manage-ment Re-sponsibility Risk As-sessment Risk Man-agement Risk Moni-toring and Testing Appendix H: Testing Program	6.3.4	5.10 6.15.4	14.1.5			7.5	

Extensive Tabular Crosswalk between RMM's 26 Process Areas and 251 Specific Practices and Key Industry Standards

RMM NIST Crosswalk

CERT® RESILIENCE MANAGEMENT MODEL V1.1	NIST SPECIAL PUBLICATIONS											
PROCESS AREA GOALS AND PRACTICES	800-18 REV.1	800-30	800-34 REV. 1	800-37	800-39	800-53	800-53A	800-55 REV. 1	800-60 VOL. 1 REV.1	800-61 REV. 1	800-70 REV. 2	800
KIM – KNOWLEDGE AND INFORMATION MANAGEMENT												
KIM:SG1 Establish and Prioritize Information Assets				2.1		AC-22			3.1.1, 4			
KIM:SG2 Protect Information Assets			3.4.1, 3.4.2			AC-16, AC-21, PE-5, SC-2, SI-12	3.1		3.1.2, 4			
KIM:SG3 Manage Information Asset Risk		3, 4, 5				PM-4, PM-7	PM-7					3.1
KIM:SG4 Manage Information Asset Confidentiality and Privacy						AU-13, IA-1, MP-2, MP-3, MP-4, MP-5, MP-6, PL-5, SC-8, SC-9, SC-11, SC-12, SC-13, SC-14, SC-17, SI-12						
KIM:SG5 Manage Information Asset Integrity						SC-8, SC-14, SC-20, SC-21						2.1
KIM:SG6 Manage Information Asset Availability						CP-9				3.4.3		
MA – MEASUREMENT AND ANALYSIS												
MA:SG1 Align Measurement and Analysis Activities						PM-6	3.1, 3.2.1, 3.2.2, Appendix D, Appendix F	3.4.3, 3.4.4, 5.2, 5.5, 5.7, 6.1		3.2.4, 3.4.3, 4.3, 5.3, 6.3, 7.3, 8.2		2.1.2, 3.1.1, 3.2
MA:SG2 Provide Measurement Results							3.3, Appendix G	3.4.3, 6.2				2.1.3
MON – MONITORING												
MON:SG1 Establish and Maintain a Monitoring Program						CA-7, PM-6, SI-4		5.1, 5.2			3	2.1, 2.3, 3

Distinguishing Features of RMM

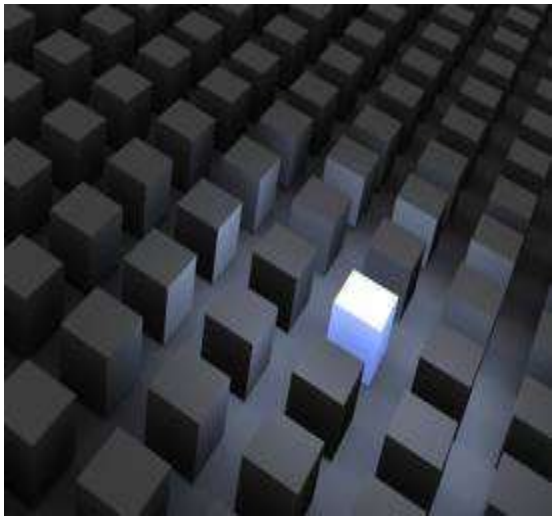
Converges key operational risk management activities: security, BC/DR, and IT operations

Guides **implementation and management** of operational resilience activities

Descriptive rather than prescriptive - focuses on the “what” not the “how”

Provides an organizing convention for effective selection and deployment of codes of practice and standards

Guide for improvement in areas where an organization’s capability does not equal its desired state



Distinguishing Features of RMM (Cont.)

Improves confidence in how an organization responds in times of operational stress

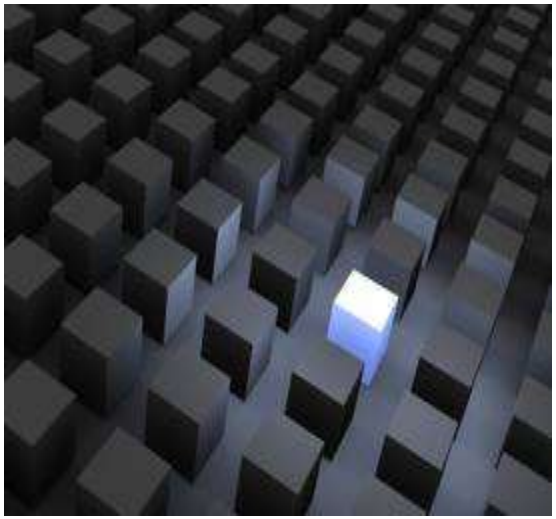
Baseline from which to perform an appraisal

Enables **measurements** of effectiveness

Process improvement model

Enables **institutionalization**

Not a proprietary model



Current Approaches to Security Management

Security by **compliance**

- FISMA
- HIPAA
- PCI

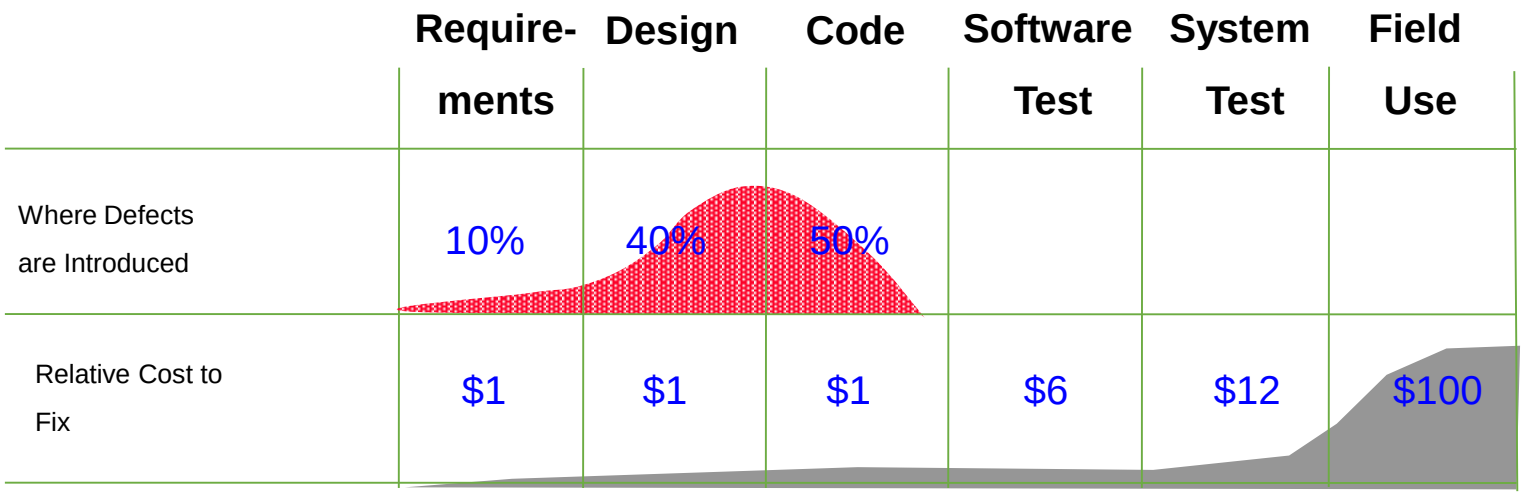
Security by adoption of **best practices**

- ISO 27000
- DISA STIGs, NIST
- Vendor guides

Result

- Uneven use of limited resources

Remember - Defects : Insertion Pattern & Cost of Removal

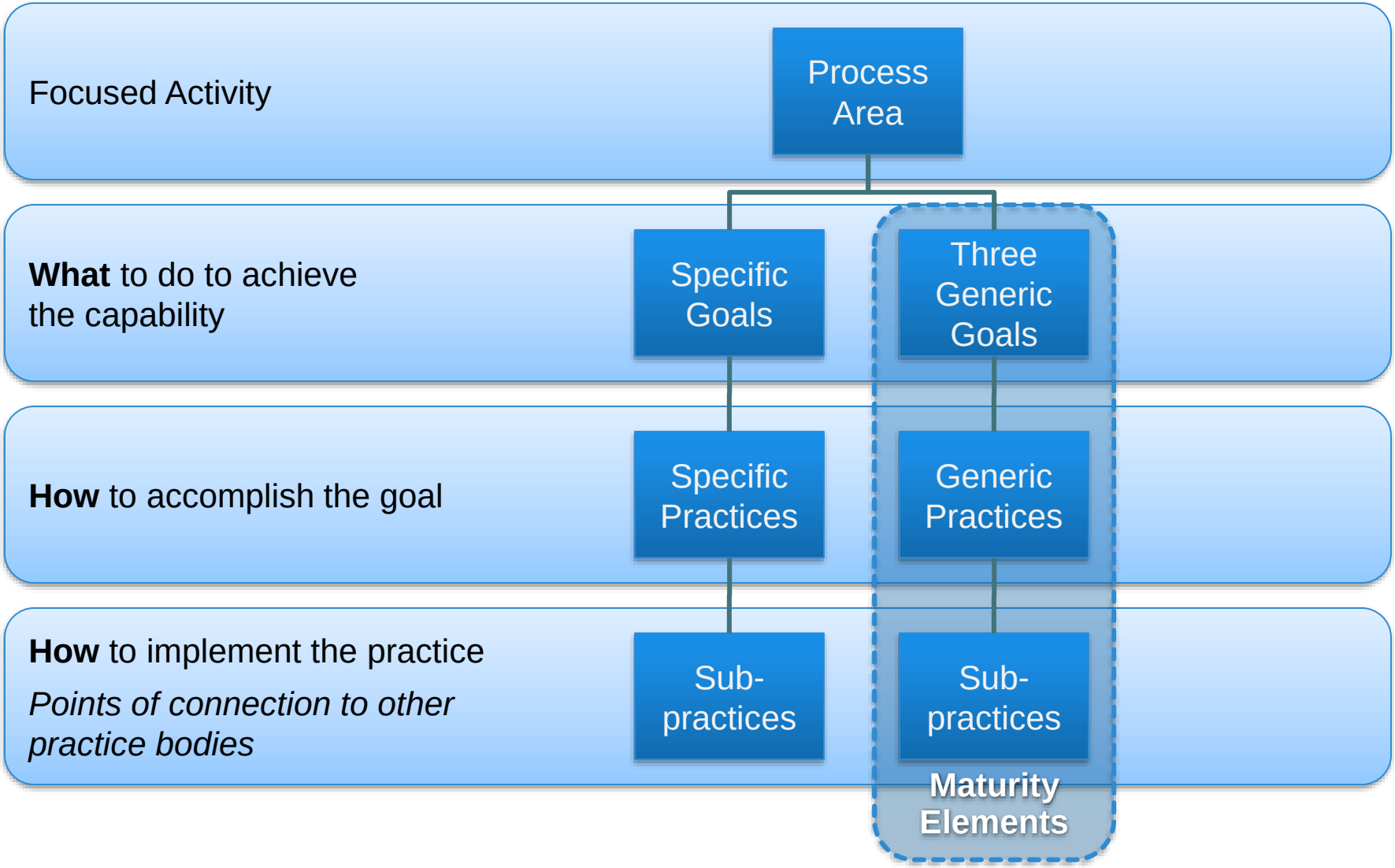


Source: SEPG Asia Pacific 2009
presented by Ravindra Nath, KUGLER MAAG CIE GmbH

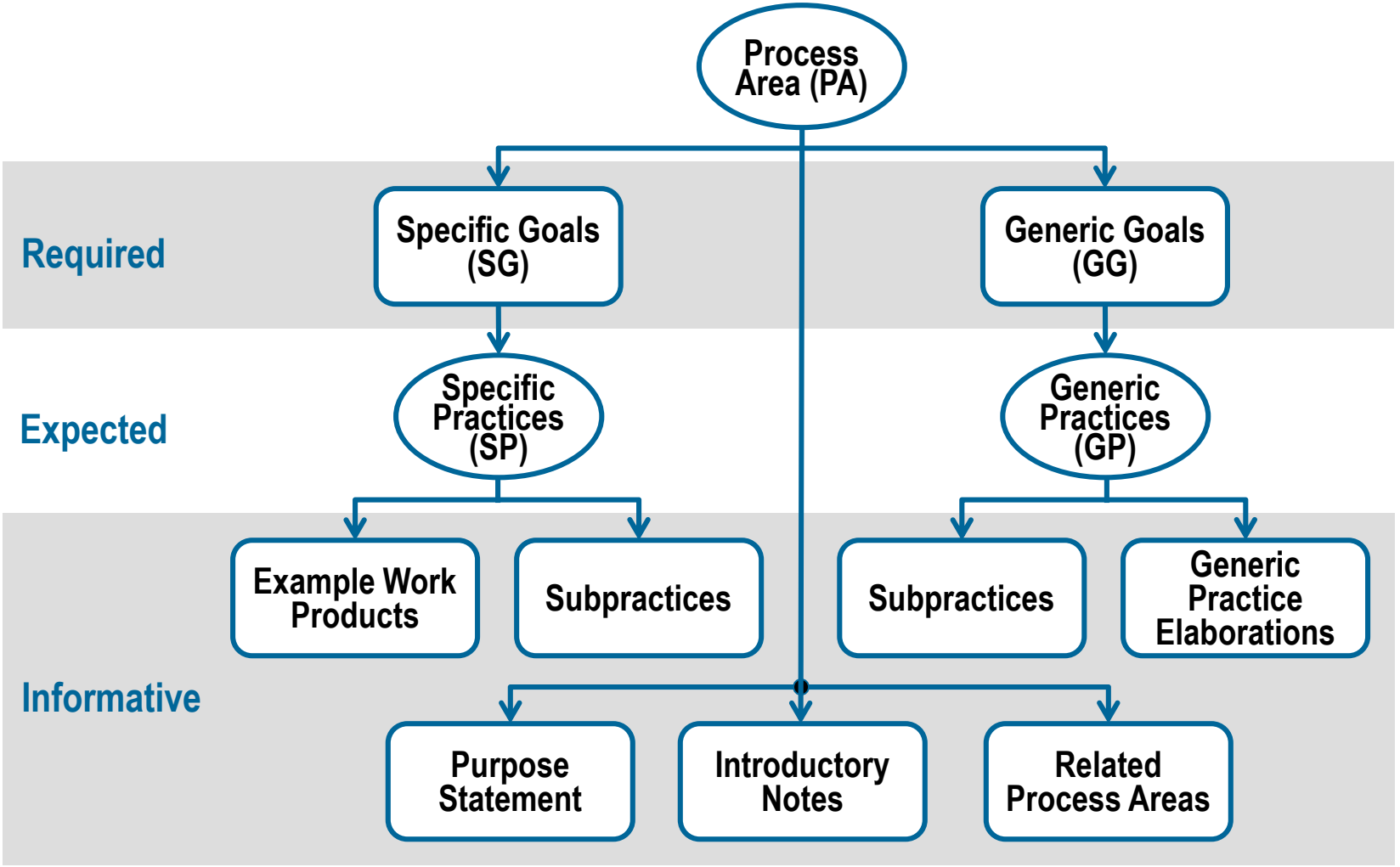
But this is also about SW Quality?

SELECT name FROM users WHERE name='' OR ''='' AND passwd= '' OR ''=''

CERT-RMM Process Area Architecture



Process Area Components (or how to read the book)

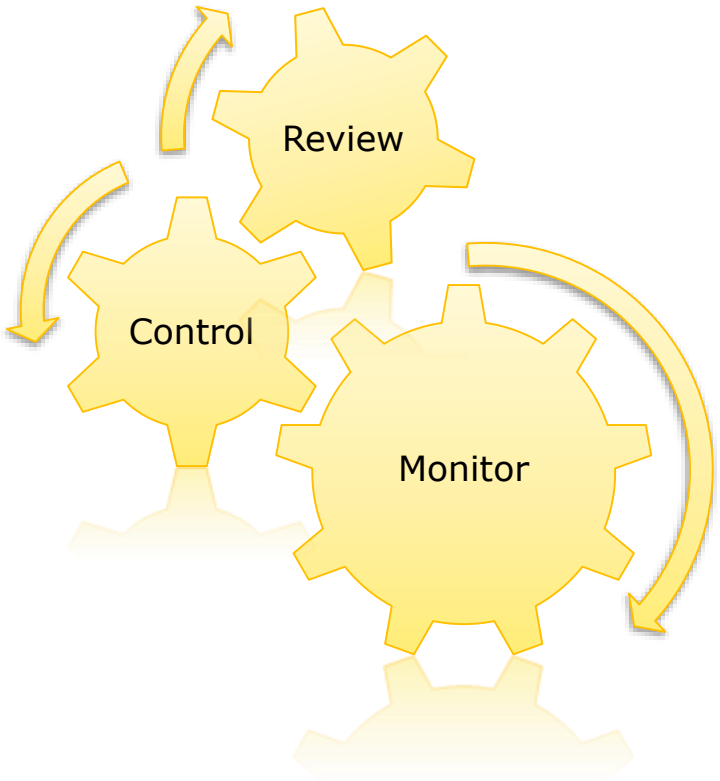


EXD similarity to asset cluster pattern

	PM	KIM	TM	EC	EXD
ADM	SG1	SG1	SG1	SG1	✔
RRD/CTRL	HRM	SG2	SG2	SG2	SG3.SP1 SG3.SP2
RISK	SG2	SG3	SG3	SG3	SG2
Confidentiality	--	SG4	--	--	Selection Formalization Management
Integrity	HRM	SG5	SG4	SG4	
Availability	SG3	SG6	SG5	SG4	

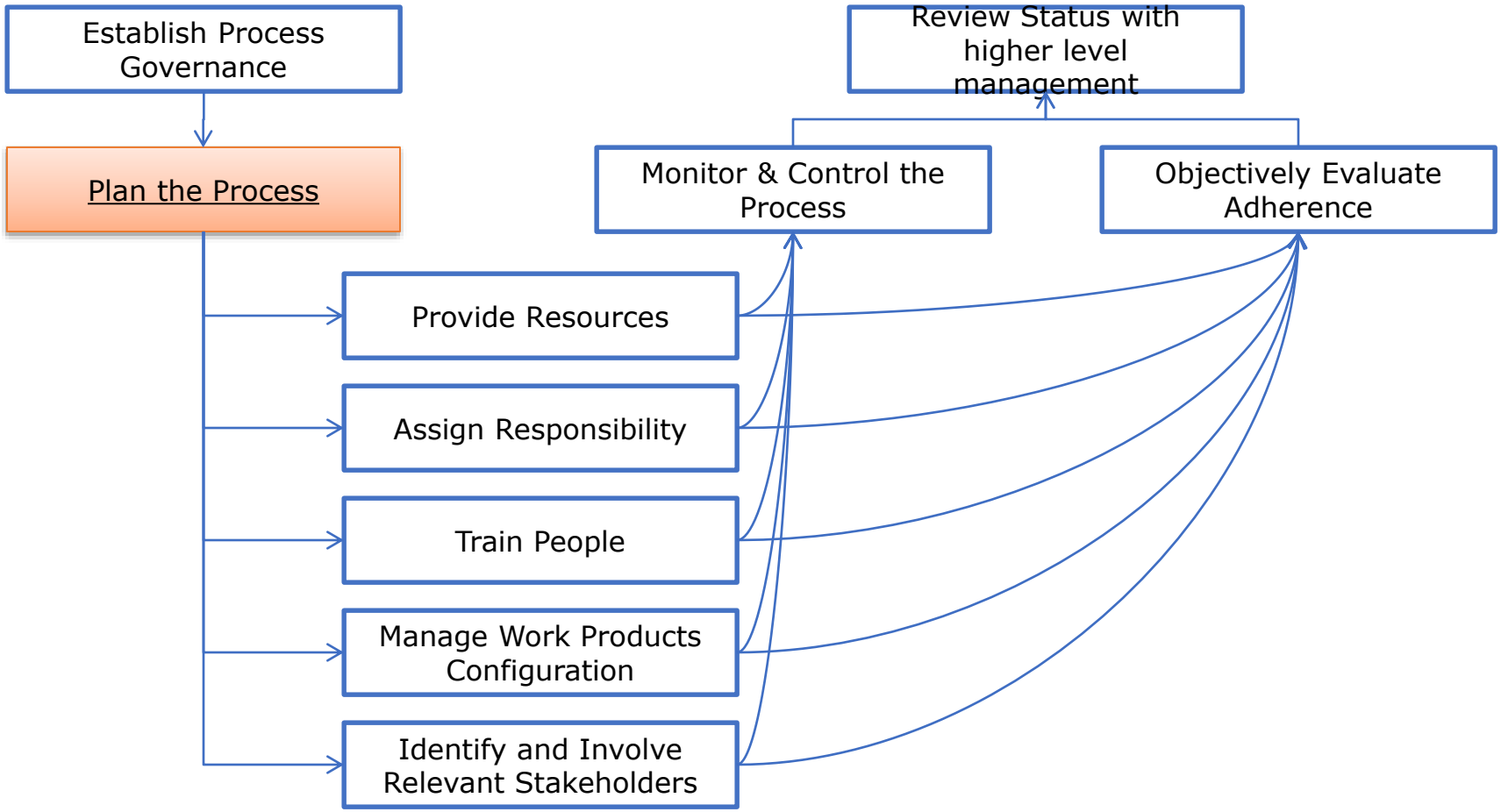
Generic goals and practices

Generic Goal 2
Institutionalize a Managed Process



Number	Generic Practice
GG2.GP1	Establish Process Governance
GG2.GP2	Plan the Process
GG2.GP3	Provide Resources
GG2.GP4	Assign Responsibility
GG2.GP5	Train People
GG2.GP6	Manage Work Product Configurations
GG2.GP7	Identify and Involve Relevant Stakeholders
GG2.GP8	Monitor and Control the Process
GG2.GP9	Objectively Evaluate Adherence
GG2.GP10	Review Status with Higher-Level Management

How PAs relate to Generic Practices?



Source: Kiril Karaatanasov, ESI Center Bulgaria

DO NOT FORGET!!!

Process ≠ Bureaucracy

Process = Work

Selected CERT-RMM process areas

Foundational process areas in CERT-RMM

PA	Foundational Elements
ADM	▪ Connects directly to practices in asset-based process areas KIM, TM, EC, and PM ▪ Strong relationship with EF (on asset-service connection)
AM	▪ Connects directly to practices in asset-based process areas KIM, TM, and EC ▪ Strong relationship with ID (ID and AM should be considered together)
CTRL	▪ Connects directly to practices in asset-based process areas KIM, TM, EC, and PM
EF	▪ Elements of EF appear in capability level 2 generic goals and practices ▪ Elements of EF relate to RISK, COMP, and FRM
FRM	▪ Elements of FRM appear in capability level 2 generic goals and practices
HRM	▪ Elements of HRM appear in capability level 2 generic goals and practices ▪ Strong relationship with OTA and PM
MON	▪ Strong relationship with several PAs, including COMP, RRM, IMC, EF, MA, and VAR
OTA	▪ Elements of OTA appear in capability level 2 generic goals and practices
RISK	▪ Connects directly to practices in asset-based process areas KIM, TM, EC, and PM ▪ Elements of RISK appear in capability level 2 generic goals and practices ▪ Strong relationship with EF, VAR, and IMC
RRD	▪ Connects to ADM to establish assets and their resilience requirements
SC	▪ Connects directly to practices in asset-based process areas KIM, TM, EC, and PM

RTSE – Resilient Technical Solution Engineering

Ensure that software and systems are developed to satisfy their resilience requirements

RTSE specific goals

Goal	Goal Title
RTSE:SG1	Establish guidelines for resilient technical solution development
RTSE:SG2	Develop resilient technical solution development plans
RTSE:SG3	Execute the plan

RTSE: Building in versus bolting on

Requires organizational intervention

Extends resilience requirements to assets that are **to be developed**

Creates requirements for quality attributes

Attempts to reduce the level of operational risk

Extends across the life cycle

RTSE: Designing and testing for resilience

- Performing resilience controls planning and design
- Incorporating resilience controls into architecture design
- Designing resilience-specific architecture
- Adopting secure coding practices
- Processes for detecting and removing defects
- Designing testing criteria to attest to asset resilience
- Testing resilience controls
- Designing service continuity plans during the development process

Secure coding: top 10 recommendations

1. **Validate input** - be suspicious of most external data sources
2. **Heed compiler warnings –** compile highest warning level available
3. **Architect and design for security policies –** e.g. divide the systems into intercommunicating subsystems, each with an appropriate privilege set
4. **Keep it simple –** complex design increase implementation, configuration, and use errors; assurance become dramatically complex
5. **Default deny -** base access decisions on permission rather than exclusion
6. **Adhere to the principle of least privilege**
7. **Sanitize data sent to other systems**
8. **Practice defense in depth** - multiple defensive strategies: if one layer of defense turns inadequate, another layer can prevent a security flaw
9. **Use effective quality assurance techniques -** identifying and eliminating vulnerabilities: penetration testing, fuzz testing, source code audits
10. **Adopt a secure coding standard**

+

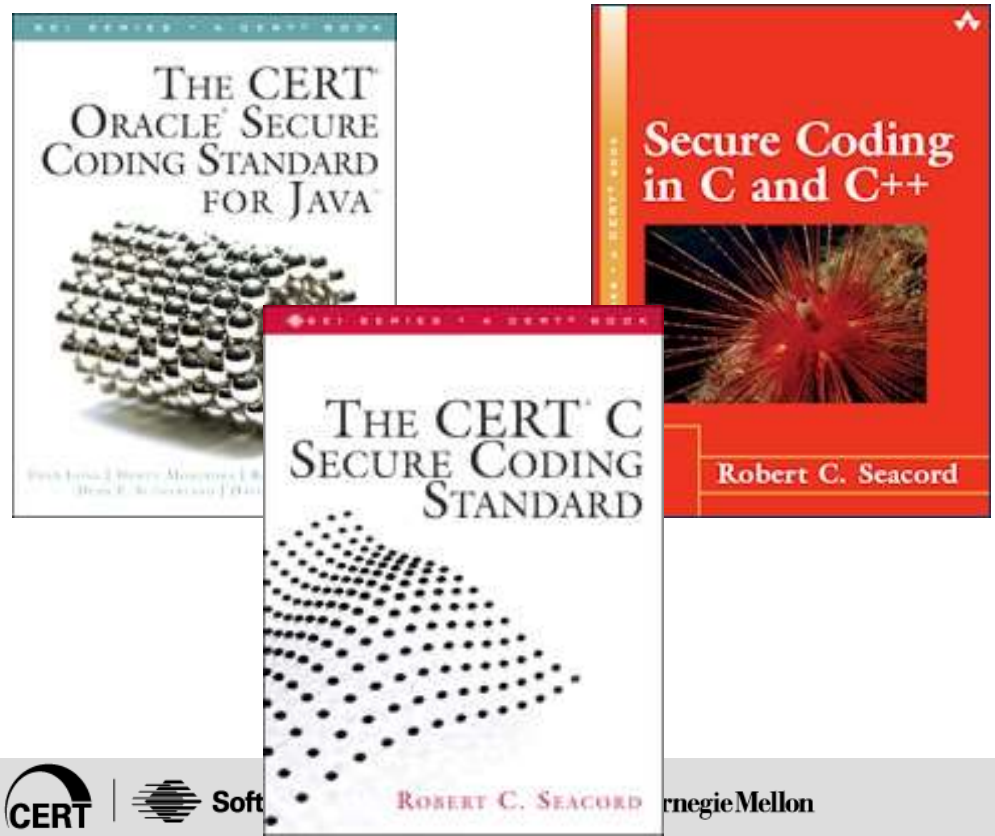
Define security requirements

Model threats

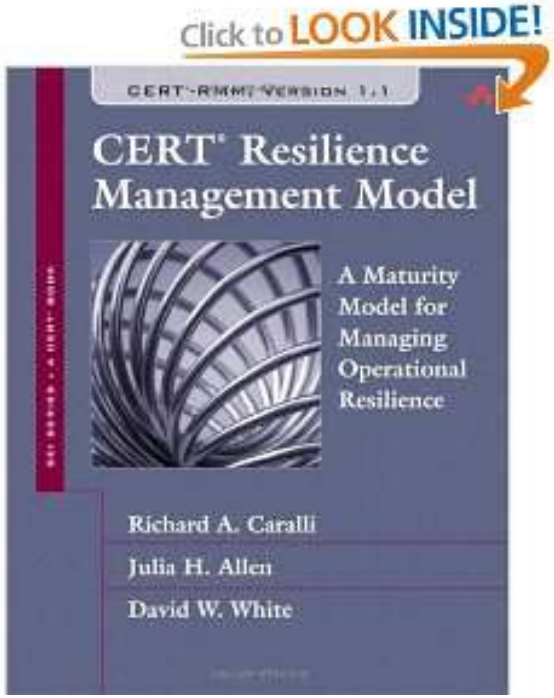
Computer Emergency Response Team

Software Engineering Institute | Carnegie Mellon

Closing gaps & develop good code:
Secure Coding Standards
[languages + compilers]



Generic Model to Manage and Assess the Operational Resilience
[Information Security, Security Business Continuity]



RTSE influences

BSIMM2

bsimm.com

The Building Security In Maturity Model (BSIMM, pronounced “bee simm”) is a study of existing software security initiatives. By quantifying the practices of many different organizations, we can describe the common ground shared by many as well as the variations that make each unique.

Open Web Applications Security Project (OWASP) **Software Assurance Maturity Model** www.owasp.org

Microsoft Security Development Life Cycle

www.microsoft.com/security/sdl/

DHS **Process Reference Model for Assurance Mapping to CMMI-DEV V1.2**

https://buildsecurityin.us-cert.gov/swa/procresrc.html

Incident Management and Control (IMC)

Event

Incident

Crisis

Incident Management and Control (IMC)

Summary of Specific Goals and Practices

IMC:SG1 Establish the Incident Management and Control Process

IMC:SG1.SP1 Plan for Incident Management
IMC:SG1.SP2 Assign Staff to the Incident Management Plan

IMC:SG2 Detect Events

IMC:SG2.SP1 Detect and Report Events
IMC:SG2.SP2 Log and Track Events
IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence
IMC:SG2.SP4 Analyze and Triage Events

IMC:SG3 Declare Incidents

IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria
IMC:SG3.SP2 Analyze Incidents

Incident Management and Control (IMC)

IMC:SG4 Respond to and Recover from Incidents

IMC:SG4.SP1 Escalate Incidents

IMC:SG4.SP2 Develop Incident Response

IMC:SG4.SP3 Communicate Incidents

IMC:SG4.SP4 Close Incidents

IMC:SG5 Establish Incident Learning

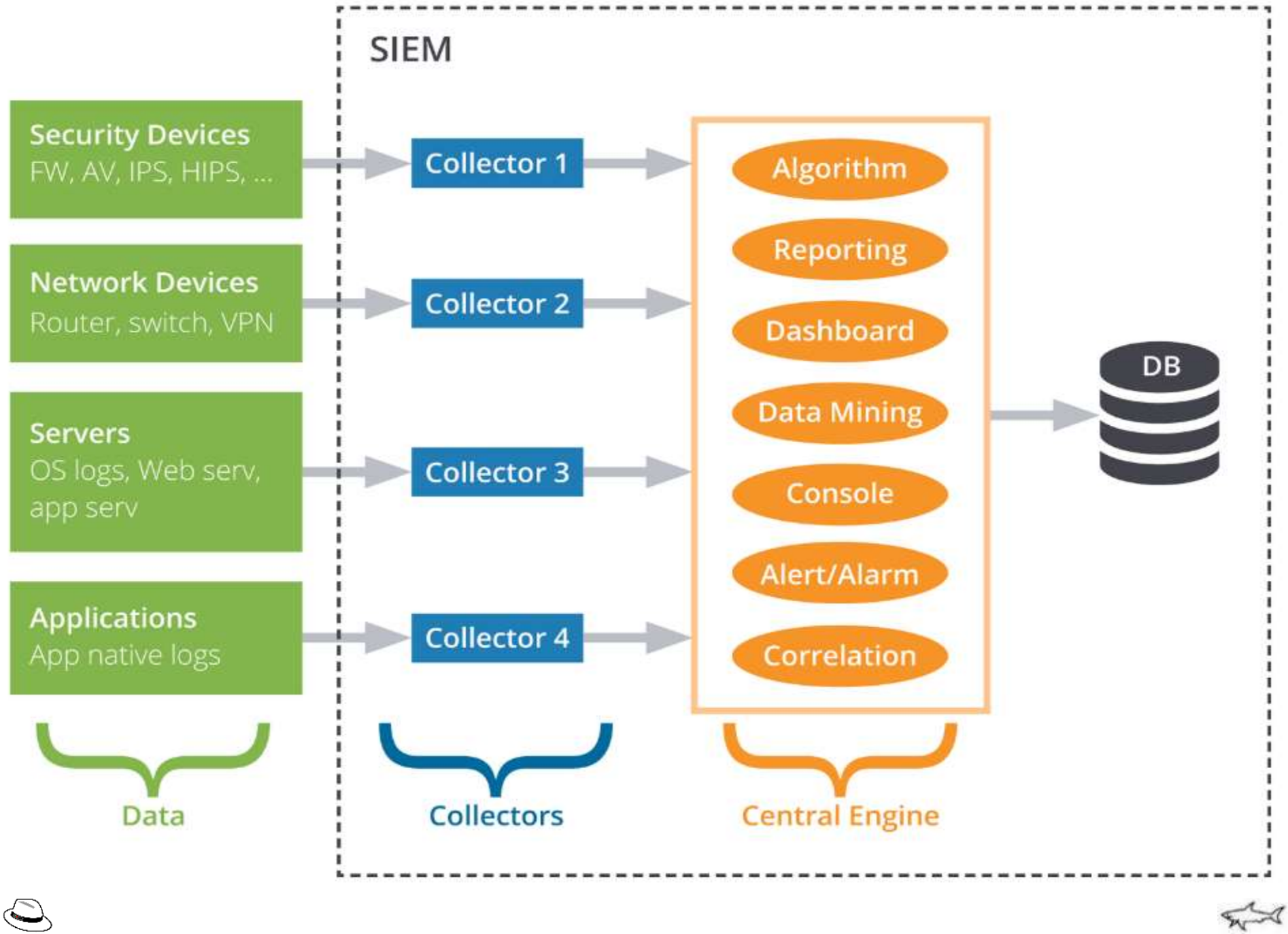
IMC:SG5.SP1 Perform Post-Incident Review

IMC:SG5.SP2 Integrate with the Problem Management Process

IMC:SG5.SP3 Translate Experience to Strategy

Security information and event management (SIEM) is a solution that provides a bird's eye view of an IT infrastructure. It fulfills two main objectives: (1) detecting in (near) real-time security incidents, and (2) efficiently managing logs. These objectives were respectively called security event management (SEM) and security information management (SIM), but nowadays these functions have been merged into a single capability known as SIEM. From a high-level point of view, a SIEM collects information (e.g., logs, events, flows) from various devices on a network, correlates and analyzes the data to detect incidents and abnormal patterns of activity, and, finally, stores the information for later use (reporting, behavior profiling, etc.). When successfully deployed and configured, a SIEM helps organizations:

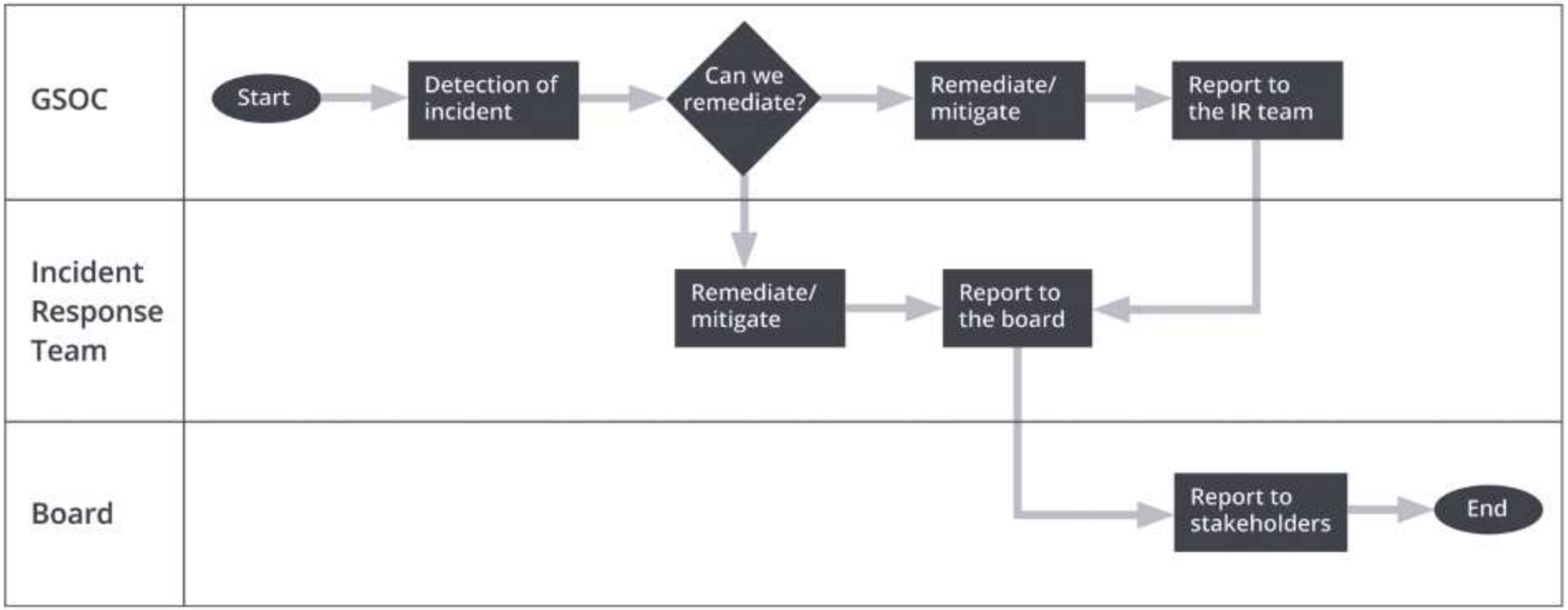
- Discover internal/external threats.
- Monitor (privileged) user activity and access to resources.
- Provide compliance reporting.
- Support incident response.


SIEM
Security Devices
FW, AV, IPS, HIPS, ...
Network Devices
Router, switch, VPN
Servers
OS logs, Web serv, app serv
Applications
App native logs
Collector 1
Collector 2
Collector 3
Collector 4
Algorithm
Reporting
Dashboard
Data Mining
Console
Alert/Alarm
Correlation
DB
Data
Collectors
Central Engine

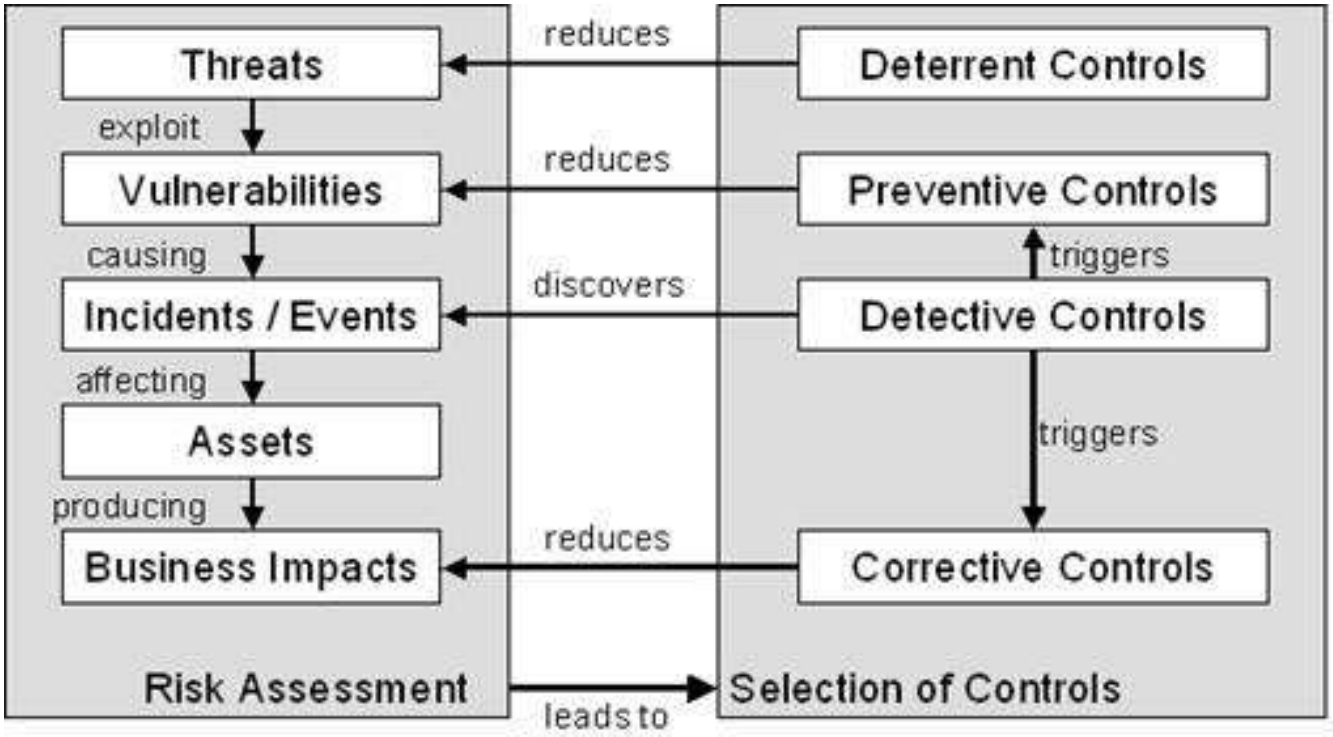
Functions of a SOC

monitor-and-respond strategy

Security Operation Center [SOC]

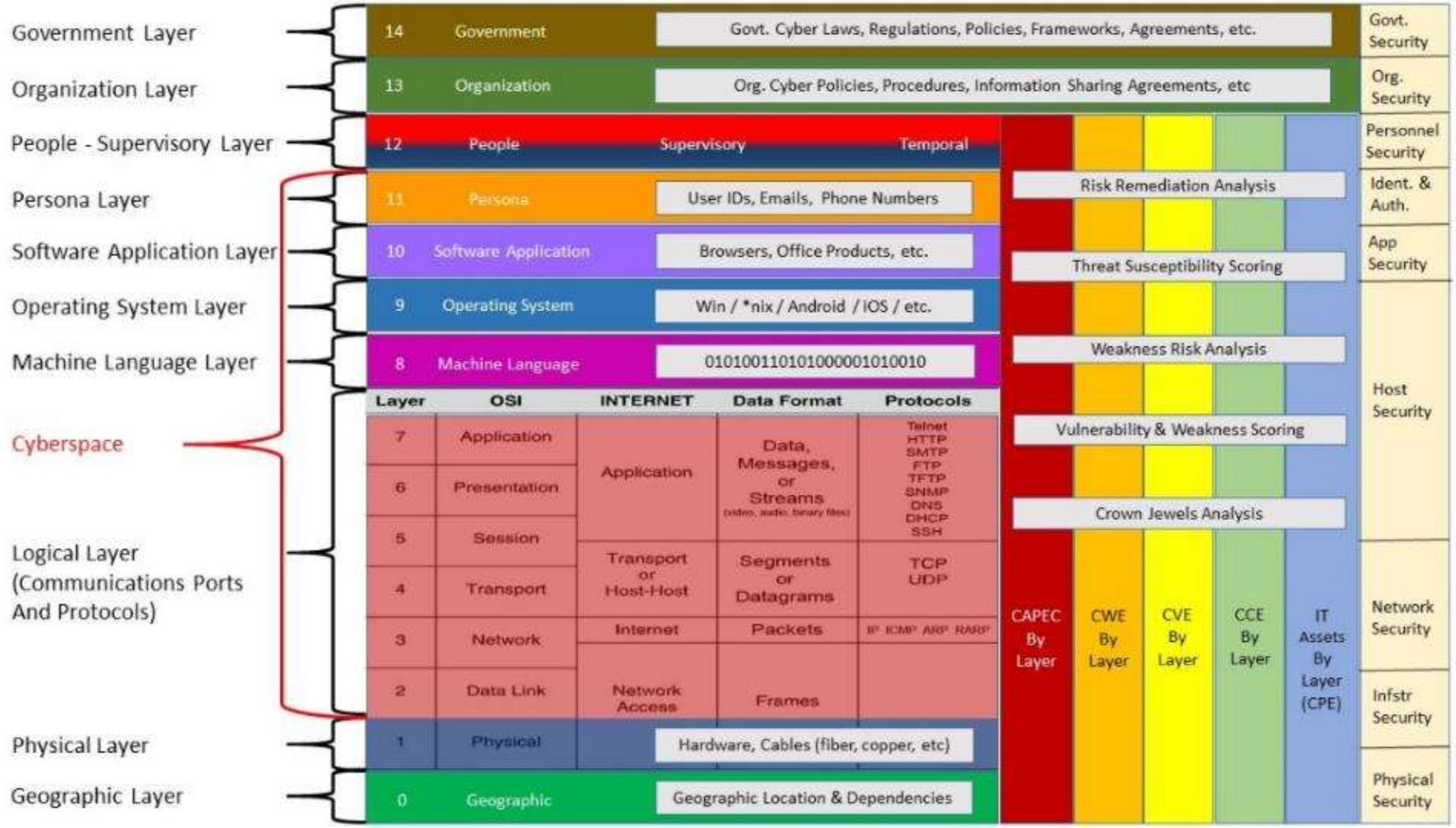


Reacting upon incident flow chart.



Source: http://security.globalpractitioner.org/introduction/infosec_5_5.htm

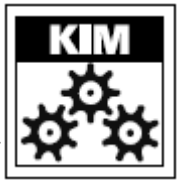
Cyber Terrain



More…related to technical How-to-s

COMP	Compliance
ID	Identity Management
RRD	Resilience Requirements Development
KIM	Knowledge and Information Management
TM	Technology Management
VAR	Vulnerability Analysis & Resolution
AM	Access Management

KIM: Knowledge and Information Management



Purpose:

The purpose of Knowledge and Information Management is to establish and manage an appropriate level of controls to support the confidentiality, integrity, and availability of the organization's information, vital records, and intellectual property.

KIM: Attributes of Information Assets

availability

accessible to authorized users (people, processes, or devices) **whenever it is needed**

confidentiality

accessible **only** to authorized people, processes, and devices

integrity

being in the **condition intended by the owner** and so continuing to be useful for the purposes intended by the owner

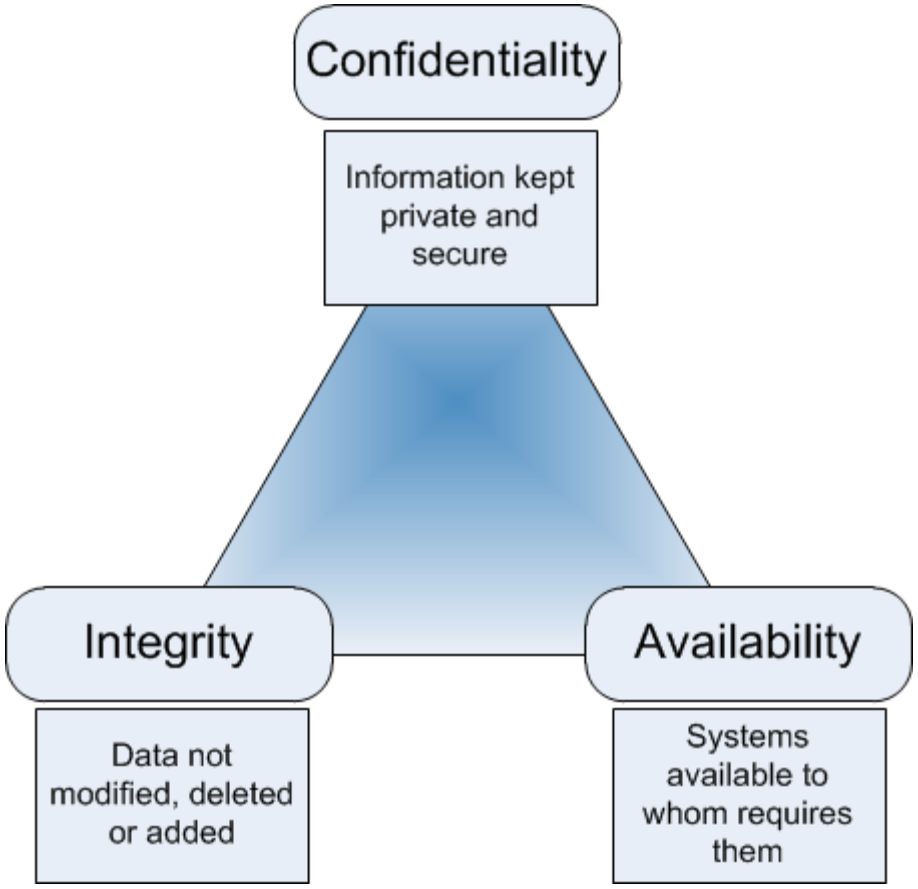
privacy

information about an individual **is disclosed only** to people, processes, and devices **authorized by that individual** or permitted **under privacy laws** and regulations.

sensitivity

degree to which an information asset must be protected based on the **consequences** of its unauthorized access, modification, or disclosure.

Beyond Confidentiality, Integrity & Availability



https://medium.com/@jym/beyond-confidentiality-integrity-availability-fbe4a64f69c4

KIM: Summary of Specific Goals and Practices

KIM:SG1 Establish and Prioritize Information Assets

KIM:SG1.SP1 Prioritize Information Assets

relative to their importance in supporting the delivery of high-value services

KIM:SG1.SP2 Categorize Information Assets

Examples:

SSP: develop sensitivity categorization scheme

• *unclassified, typically includes*

- *public or non-sensitive (information that is approved for public use)*
- *restricted or internal use only (memos, project plans, audit reports)*
- *confidential or proprietary (organizational intellectual property, product designs, customer information, employee records)*

• *classified, which may include levels such as*

- *secret*
- *top secret*

SSP: Assign responsibility for the assignment of sensitivity categorization levels to information assets

KIM:SG2 Protect Information Assets

KIM:SG2.SP1 Assign Resilience Requirements to Information Assets

KIM:SG2.SP2 Establish and Implement Controls

KIM:SG3 Manage Information Asset Risk

KIM:SG3.SP1 Identify and Assess Information Asset Risk

KIM:SG3.SP2 Mitigate Information Asset Risk

KIM: Summary of Specific Goals and Practices

KIM:SG4 Manage Information Asset Confidentiality and Privacy

KIM:SG4.SP1 Encrypt High-Value Information

Cryptographic controls are applied to information assets to ensure confidentiality and prevent accidental disclosure

Typical work products:

1. *Policy and guidelines for encryption application*
2. *Encryption methodologies and technologies*
3. *Cryptographic key management policies and procedures*
4. *Encrypted information assets*

KIM:SG4.SP2 Control Access to Information Assets

Example (compliances):

Laws and regulations concerning confidentiality and privacy include

- *Family Educational Rights and Privacy Act (FERPA)*
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Gramm-Leach-Bliley Act (GLB)*
- *Fair Credit Reporting Act (FCRA)*
- *Children's Online Privacy Protection Act (COPPA)*

KIM:SG4.SP3 Control Information Asset Disposition

Typical work products: Information asset disposition guidelines

Posts in category *Data Security*

The Correct Disposal of It Equipment Containing Sensitive Data

APR17 2012 WRITTEN BY BRENDAN PALMER LEAVE A COMMENT

You have moved to the cloud, Who looks after your old IT equipment? Is it secure?

Organisations need to be extremely careful when disposing of IT equipment that contains sensitive data. There are many reports of computers, with their hard drives intact, being found in open markets in Ireland and the third world, worldwide on eBay and other online auction sites, there is also a ready market for all types of used data tapes in these markets. Deleting files or even reformatting a hard drive does not remove the information, as this can be restored using readily available software. Even overwriting does not erase the information, with forensic software available to read drives down to many multiple levels of overwrite

There is a specific responsibility on ICT Data Controllers when disposing of any equipment or storage media containing personal information and problems associated

Possible Threat To Obama's Security Discovered

Tiversa employees found engineering and communications information about Marine One at an IP address in Tehran, Iran.

Bob Boback, CEO of Tiversa, said, ”We found a file containing entire blueprints and avionics package for Marine One, which is the president's helicopter."

Clark said, “Once it's out there, it's **hard to get it back**. I don't think the full ramifications of this have been understood by the watchdog agencies.”

KIM: Summary of Specific Goals and Practices

KIM:SG5 Manage Information Asset Integrity

KIM:SG5.SP1 Control Modification to Information Assets

Typical work products:

1. Information asset access control lists

2. List of staff members authorized to modify information assets

3. Information asset modification logs

4. Audit reports

KIM:SG5.SP2 Manage Information Asset Configuration

KIM:SG5.SP3 Verify Validity of Information

KIM:SG6 Manage Information Asset Availability

KIM:SG6.SP1 Perform Information Duplication and Retention

KIM:SG6.SP2 Manage Organizational Knowledge

GDPR + social networks

Trends and threats in the EU

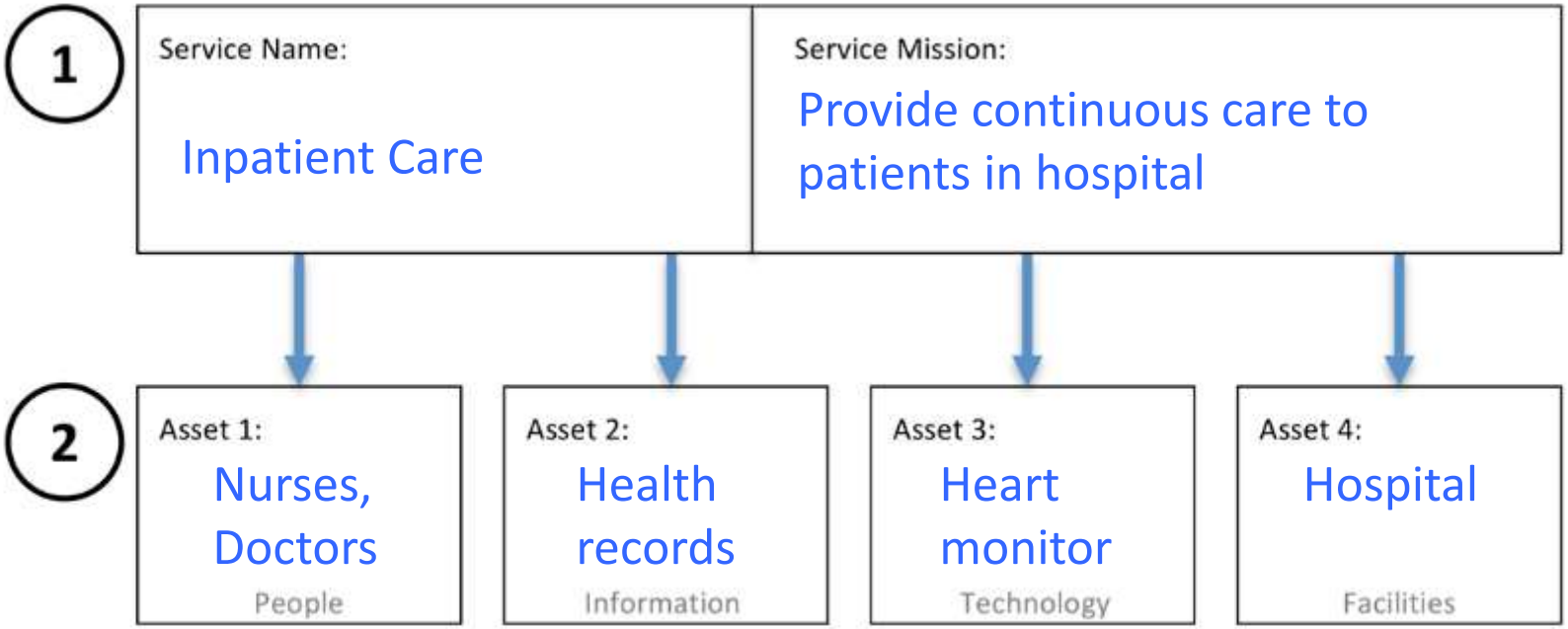
- Data theft represents the primary information security threat – more significant than either viruses or hacker infiltration
- Of all possible results of compromised information security, the threat of leakage of confidential information is keeping more members of the IT department (93%) awake at night than any other
- Europe's primary data leakage channels are identified as portable storage devices, e-mail, and Internet-based channels such as web-mail and forums
- Only 11% of those surveyed were confident their company's information security had not been breached over the last year
- The lack of industry standards is highlighted as the primary obstacle (42%) to wider implementation of anti-leakage technologies

Exercise:

Assets, mission, disruption, impact

CIA sampling (& KIM basics)

Exercise part 1, steps 1 & 2



Exercise part 1, step 3

3

A. What is the strategic importance of the service?

As a hospital, providing continuous care to in-patients is our top strategic objective

B. Which asset could be disrupted and how?

Health records could be lost or corrupted due to record system failure

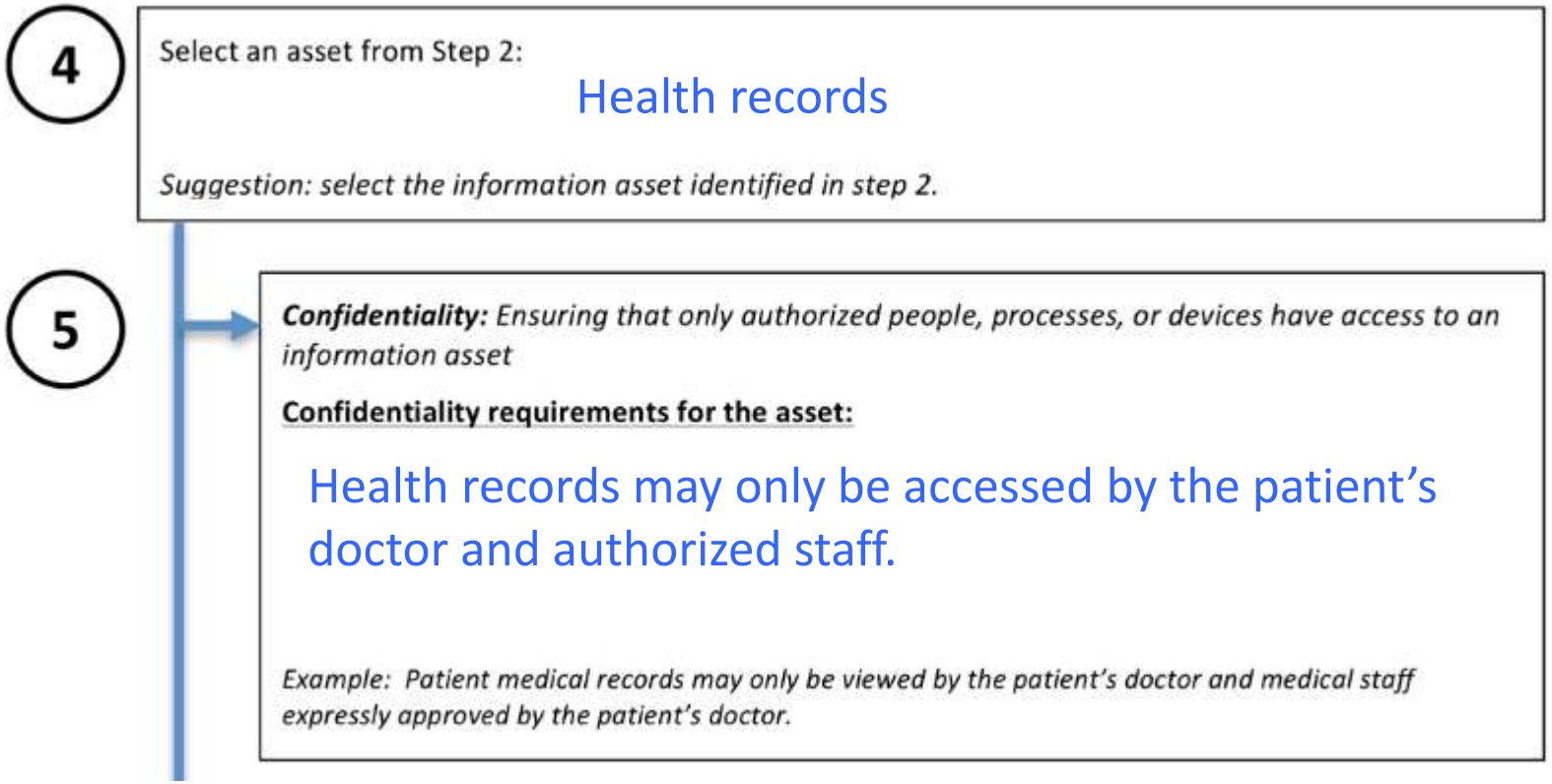
C. What would be the impact on the service mission if the asset were disrupted?

Patients might not receive appropriate or timely care

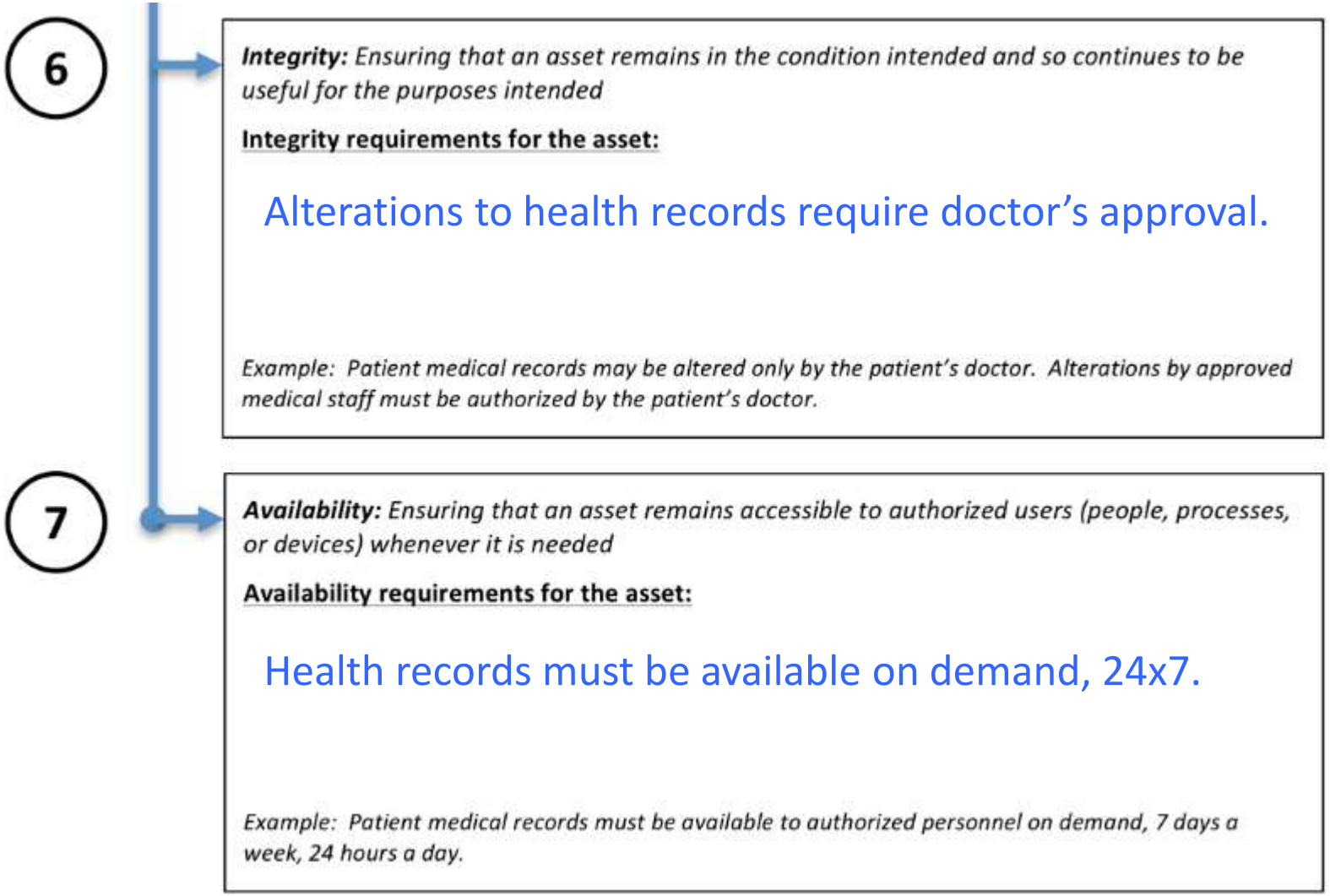
D. What consequences, if any, would the organization experience? Consider a) reputational harm, b) impacts to life, safety, and health of employees and customers, c) legal fines or penalties, and d) other financial losses.

Potential loss of life, serious reputational and financial harm

Exercise part 2, steps 4 & 5



Exercise part 2, steps 6 & 7



ID: Identity Management

Purpose:

The purpose of Identity Management is to create, maintain, and deactivate identities that may need some level of trusted access to organizational assets and to manage their associated attributes

ID: Identity Management

- disclosure of information (resulting in violations of privacy and confidentiality requirements)
- unauthorized use of systems and servers (to carry out fraudulent activities)
- unauthorized entry to secured facilities (which could affect the life, safety, and health of staff and customers)
- destruction or loss of vital information and systems that the organization relies upon day-to-day to carry out its strategic objectives

Because the operating environment is complex and the persons, objects, and entities that need access to organizational assets are ever-changing, the organization must actively manage the population of identities to ensure that it is valid.

ID: Identity Management

Goals/Practices

ID:SG1 Establish Identities

Identities are created to represent persons, objects, and entities that require access to organizational assets.

ID:SG1.SP1 Create Identities

- *Persons, objects, and entities that require access to organizational assets are registered and profiled.*

ID:SG1.SP2 Establish Identity Community

- *identity community can be defined as the collection of the organization's identity profiles. The identity community defines the baseline population of persons, objects, and entities—internal and external to the organization*

ID:SG1.SP3 Assign Roles to Identities

ID:SG2 Manage Identities

- *Identities are managed to ensure they reflect the current environment of associated persons, objects, and entities.*

ID:SG2.SP1 Monitor and Manage Identity Changes

ID:SG2.SP2 Periodically Review and Maintain Identities

- *to identify identities that are invalid*

ID:SG2.SP3 Correct Inconsistencies

- *Inconsistencies between the identity community and the persons, objects, and entities they represent are corrected.*

ID:SG2.SP4 Deprovision Identities

- *Identities for which need has expired or has been eliminated are deprovisioned*

Something You Know, Have, or Are

- All approaches for human authentication rely on at least one of the following:
- *Something you know* (eg. a password). This is the most common kind of authentication used for humans. We use passwords every day to access our systems. Unfortunately, something that you know can become something you just forgot. And if you write it down, then other people might find it.
- *Something you have* (eg. a smart card). This form of human authentication removes the problem of forgetting something you know, but some object now must be with you any time you want to be authenticated. And such an object might be stolen and then becomes something the attacker has.
- *Something you are* (eg. a fingerprint). Base authentication on something intrinsic to the principal being authenticated. It's much harder to lose a fingerprint than a wallet. Unfortunately, biometric sensors are fairly expensive and (at present) not very accurate.

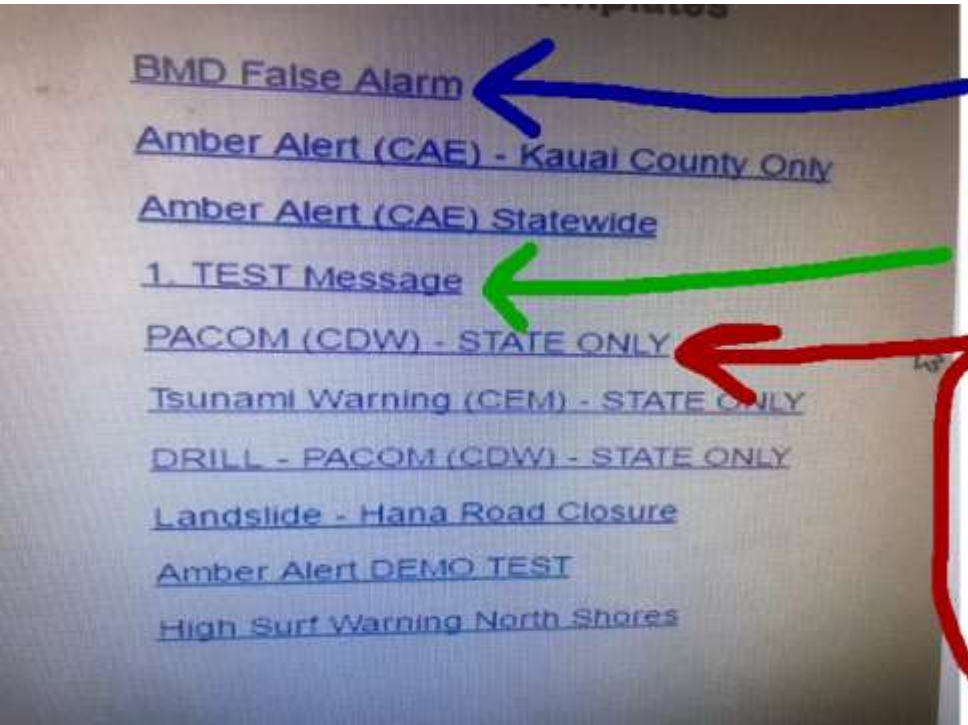
https://www.cs.cornell.edu/courses/cs513/2005fa/nnlauthpeople.html

8:08

Saturday, January 13

⚠ EMERGENCY ALERTS now

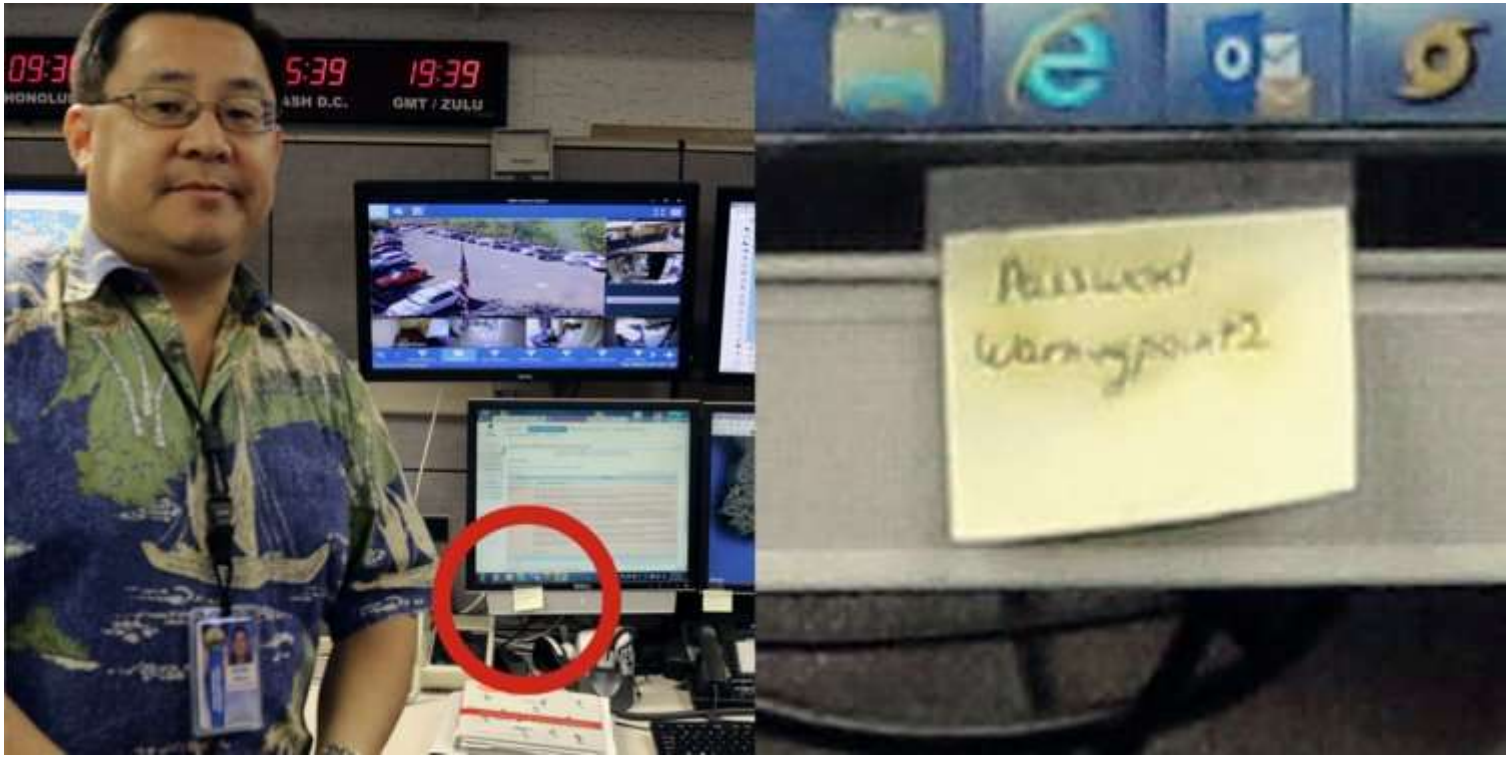
Emergency Alert
BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.



New false alarm option! :D

Press this every day to make sure the system actually works...

NEVER PRESS THIS UNLESS THERE'S AN ACTUAL INCOMING MISSILE OR ELSE YOU'LL CAUSE MASS PANIC AND FREAK EVERYONE OUT!!!!!!!!!1!


5:39
19:39
GMT / ZULU
Password

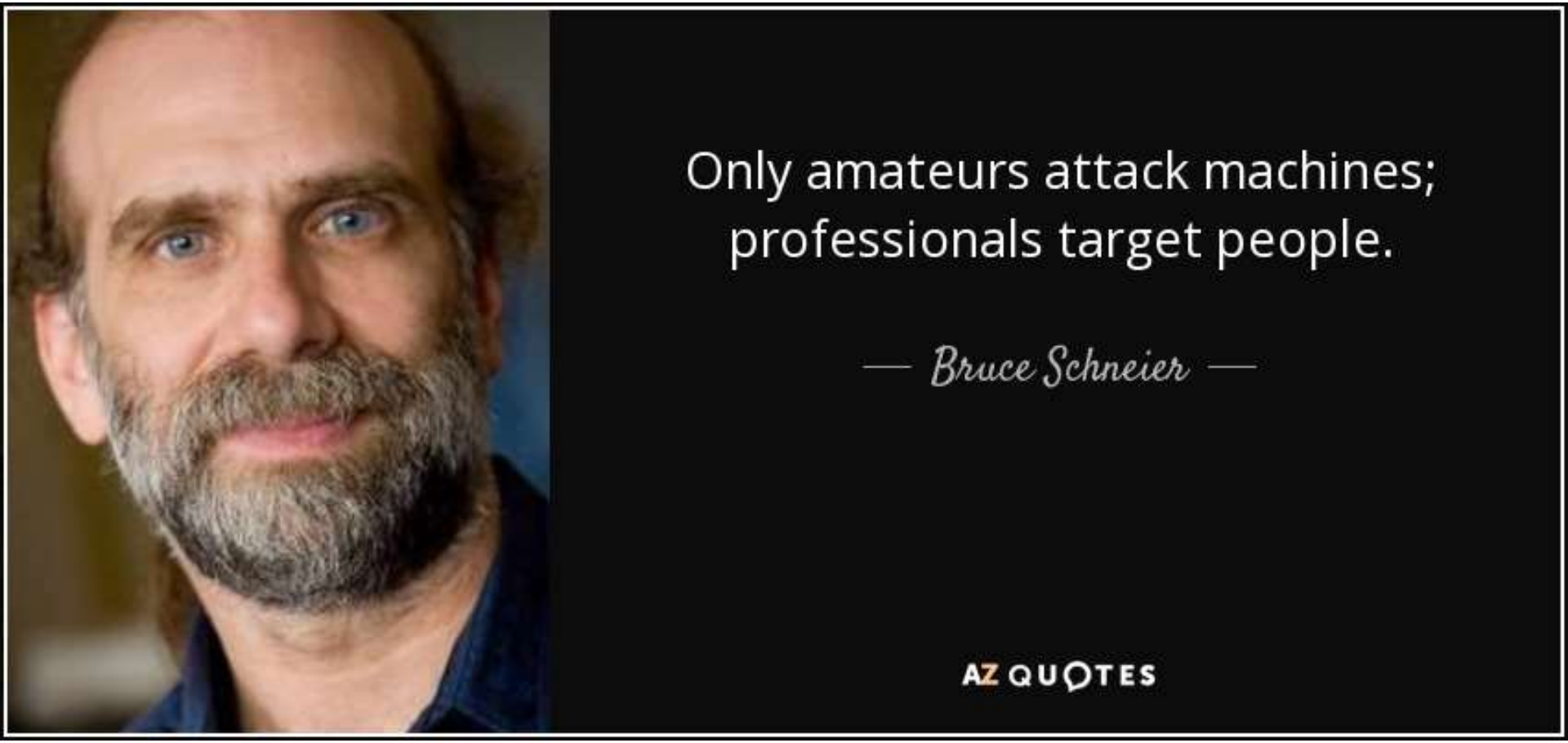
No “untouchables”: Barclays chairman’s identity stolen

Marcus Agius, chairman of the board at Barclays Bank was a victim of identity theft and fraud of 10,000 GBP. The amount was withdrawn from his account using a credit card trick.

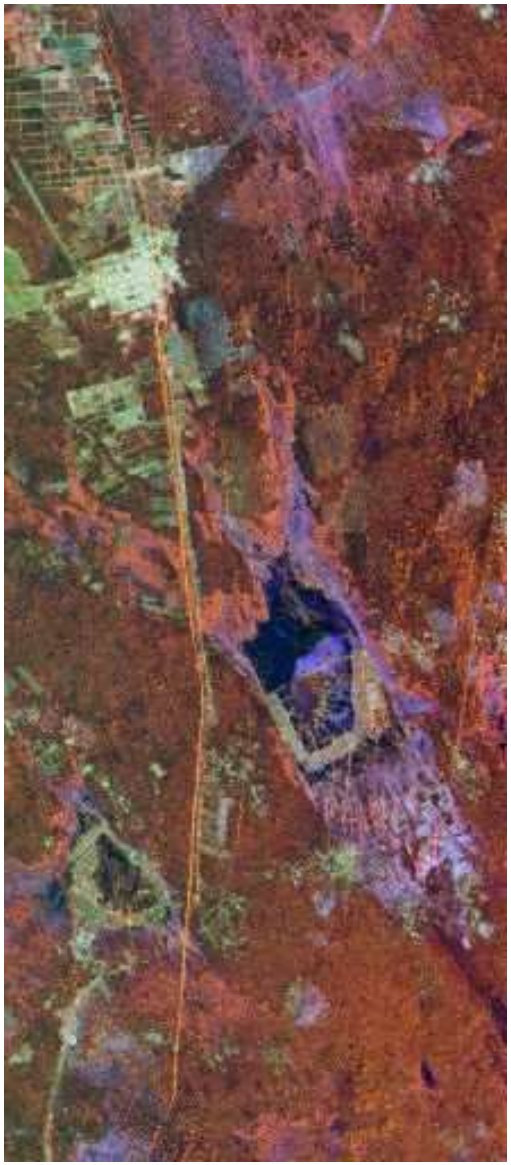
The thief collected personal data of Agius and used them to deceive a help desk operator to send him a new credit card as if he was Mr Agius himself. The guy took the card to a high street branch of Barclays and withdrew the amount.

"It was down to human error. Procedures were not followed fully and we have learned from it”

[By Iain Thomson, vnunet.com, 11 Jan 2008]


Only amateurs attack machines; professionals target people.
— Bruce Schneier —
AZ QUOTES

One of the most secure constructions?



Width: ~6 m

Height: ~7 m

Age: 2000 years

Length: 6.400 km

Weak point: the human

Wu Sangui general: the **most trusted, most faithful** strategist guarded the 1st gate.

There was a rebel among inhabitants.

Wu's "service" maid was kidnapped.

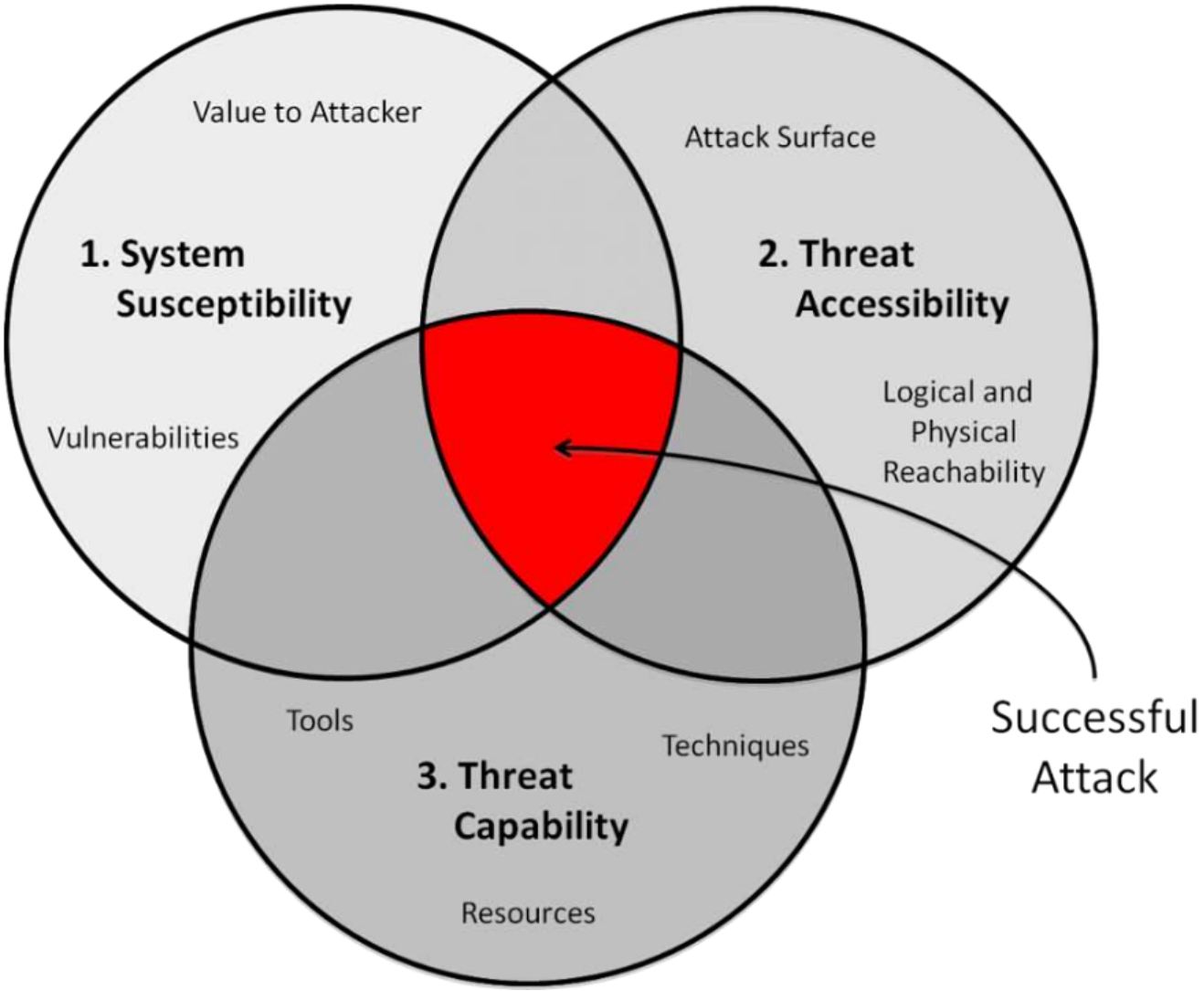
Wu, thinking he would get back his lady he willingly **opened the gate** for two thousand mandurian horsemen.

That put an end to the rule of the Ming dynasty.

Sample Targeted Attack Scenario Flow – Email Phishing

	Stage 1 - Gather Info	Stage 2 - Get In	Stage 3 – Stay In	Stage 4 – Execute Mission
Attacker	1. Gathers info of victim ↓ 2. Emails payload to victim (user)	4. Controls user machine & installs RAT ↓ 5. Scans intranet pages & victim's inbox to find IT support email ↓ 6. Fakes email to admin to seek help installing printer	8. Dumps admin hash ↓ 9. Runs OS commands to find server assets (eg. enumerate file shares) ↓ 10. Uses admin credentials to read files not accessible to victim on file shares	11. Copies files to drop servers via victim compromised machine ↓ 12. Pivots into Admin station with RDP into servers to clear selected audit log entries
User		3. Opens email attachment		
Admin		7. Responds to email & remotely log into victim PC		

Steps need further details of how it is carried out. Eg. powershell to find emails addresses or spoof email to admin. Should try to **reuse breach simulator's scenarios**...


Value to Attacker
1. System Susceptibility
Vulnerabilities
Attack Surface
2. Threat Accessibility
Logical and Physical Reachability
Tools
Techniques
3. Threat Capability
Resources
Successful Attack

AM: Access Management

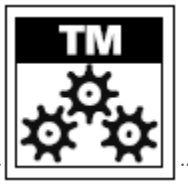
In order to support services, assets such as information, technology, and facilities must be made available (accessible) for use. This requires that persons (employees and contractors), objects (such as systems), and entities (such as business partners) have sufficient (but not excessive) levels of access to these assets.

TM: Technology Management

Purpose:

The purpose of Technology Management is to establish and manage an appropriate level of controls related to the integrity and availability of technology assets to support the resilient operations of organizational services.

TM: Technology Management



TM:SG1 Establish and Prioritize Technology Assets

TM:SG1.SP1 Prioritize Technology Assets

TM:SG1.SP2 Establish Resilience-Focused Technology Assets

TM:SG2 Protect Technology Assets

TM:SG2.SP1 Assign Resilience Requirements to Technology Assets

TM:SG2.SP2 Establish and Implement Controls

TM:SG3 Manage Technology Asset Risk

TM:SG3.SP1 Identify and Assess Technology Asset Risk

TM:SG3.SP2 Mitigate Technology Risk

TM:SG4 Manage Technology Asset Integrity

TM:SG4.SP1 Control Access to Technology Assets

TM:SG4.SP2 Perform Configuration Management

TM:SG4.SP3 Perform Change Control and Management

TM:SG4.SP4 Perform Release Management

TM:SG5 Manage Technology Asset Availability

TM:SG5.SP1 Perform Planning to Sustain Technology Assets

TM:SG5.SP2 Manage Technology Asset Maintenance

TM:SG5.SP3 Manage Technology Capacity

TM:SG5.SP4 Manage Technology Interoperability

EXD similarity to asset cluster pattern

	PM	KIM	TM	EC	EXD
ADM	SG1	SG1	SG1	SG1	✔
RRD/CTRL	HRM	SG2	SG2	SG2	SG3.SP1 SG3.SP2
RISK	SG2	SG3	SG3	SG3	SG2
Confidentiality	--	SG4	--	--	Selection Formalization Management
Integrity	HRM	SG5	SG4	SG4	
Availability	SG3	SG6	SG5	SG4	


ASSETS
IDENTITY THEFT
CYBER SUBVERSION
EMAIL SPAM
CYBER TERRORISM
SABOTAGE
CYBER SNOOPING
CYBER ESPIONAGE
CYBER WAR
DATA THEFT
CYBER HACKING
Vulnerabilities
TECH ISSUES
PROCESSES
PEOPLE
THREATS

COMP: **COMPLIANCE**

Related PAs: EF, RISK, MON

COMP:SG1 Prepare for Compliance Management

COMP:SG1.SP1 Establish a Compliance Plan
COMP:SG1.SP2 Establish a Compliance Program
COMP:SG1.SP3 Establish Compliance Guidelines and Standards

COMP:SG2 Establish Compliance Obligations

COMP:SG2.SP1 Identify Compliance Obligations
COMP:SG2.SP2 Analyze Obligations
COMP:SG2.SP3 Establish Ownership for Meeting Obligations

COMP:SG3 Demonstrate Satisfaction of Compliance Obligations

COMP:SG3.SP1 Collect and Validate Compliance Data
COMP:SG3.SP2 Demonstrate the Extent of Compliance Obligation Satisfaction
COMP:SG3.SP3 Remediate Areas of Non-Compliance

COMP:SG4 Monitor Compliance Activities

COMP:SG4.SP1 Evaluate Compliance Activities

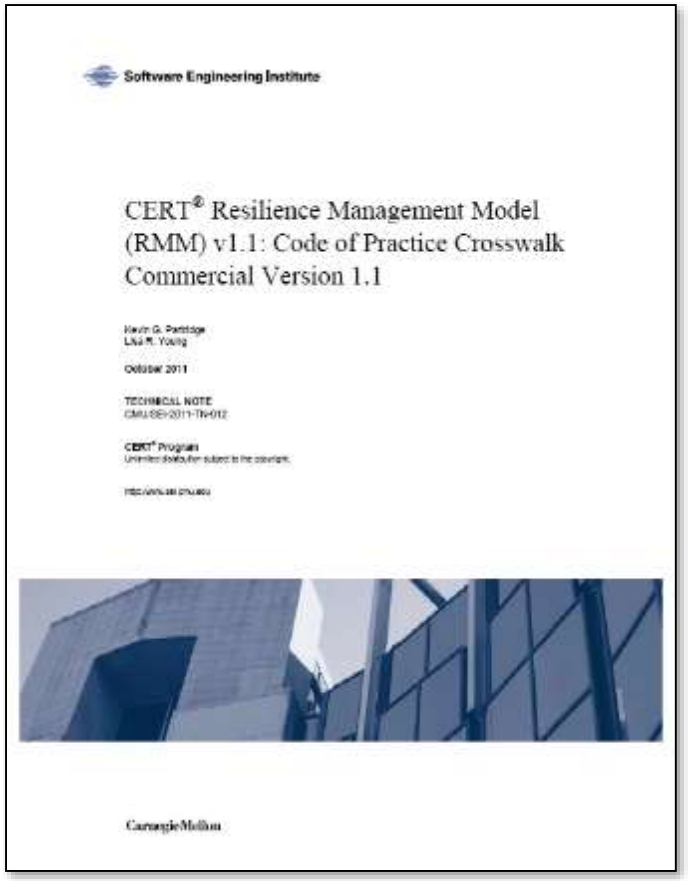
RMM Code of Practice Crosswalk

Links RMM practices to common codes of practice and standards

Including:

- ANSI/ASIS SPC.1-2009
- BS25999
- COBIT 4.1
- COSO ERM Framework
- CMMI
- FFIEC BCP Handbook
- ISO 20000-2
- ISO/IEC 24762
- ISO/IEC 24762
- ISO/IEC 27005
- ISO/IEC 31000
- NFPA 1600
- PCI DSS
- Etc…

A version of the crosswalk to common NIST standards is available.



RMM Code of Practice Crosswalk

Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG5.SP4 Evaluate Plan Test Results Subpractices 1. Compare actual test results with expected test results and test objectives. 2. Document areas of improvement for service continuity plans. 3. Document areas of improvement for testing service continuity plans	4.5.3	5.4.1 9.3.2		SCON:SP3.3	DS4.5	Board and Senior Manage-ment Re-sponsibility Risk As-sessment Risk Man-agement Risk Moni-toring and Testing Appendix H: Testing Program	6.3.4	5.10 6.15.4	14.1.5			7.5	

Extensive Tabular Crosswalk between RMM's 26 Process Areas and 251 Specific Practices and Key Industry Standards

RMM NIST Crosswalk

CERT® RESILIENCE MANAGEMENT MODEL V1.1	NIST SPECIAL PUBLICATIONS											
PROCESS AREA GOALS AND PRACTICES	800-18 REV.1	800-30	800-34 REV. 1	800-37	800-39	800-53	800-53A	800-55 REV. 1	800-60 VOL. 1 REV.1	800-61 REV. 1	800-70 REV. 2	800
KIM – KNOWLEDGE AND INFORMATION MANAGEMENT												
KIM:SG1 Establish and Prioritize Information Assets				2.1		AC-22			3.1.1, 4			
KIM:SG2 Protect Information Assets			3.4.1, 3.4.2			AC-16, AC-21, PE-5, SC-2, SI-12	3.1		3.1.2, 4			
KIM:SG3 Manage Information Asset Risk		3, 4, 5				PM-4, PM-7	PM-7					3.1
KIM:SG4 Manage Information Asset Confidentiality and Privacy						AU-13, IA-1, MP-2, MP-3, MP-4, MP-5, MP-6, PL-5, SC-8, SC-9, SC-11, SC-12, SC-13, SC-14, SC-17, SI-12						
KIM:SG5 Manage Information Asset Integrity						SC-8, SC-14, SC-20, SC-21						2.1
KIM:SG6 Manage Information Asset Availability						CP-9				3.4.3		
MA – MEASUREMENT AND ANALYSIS												
MA:SG1 Align Measurement and Analysis Activities						PM-6	3.1, 3.2.1, 3.2.2, Appendix D, Appendix F	3.4.3, 3.4.4, 5.2, 5.5, 5.7, 6.1		3.2.4, 3.4.3, 4.3, 5.3, 6.3, 7.3, 8.2		2.1.2, 3.1.1, 3.3
MA:SG2 Provide Measurement Results							3.3, Appendix G	3.4.3, 6.2				2.1.3
MON – MONITORING												
MON:SG1 Establish and Maintain a Monitoring Program						CA-7, PM-6, SI-4		5.1, 5.2			3	2.1, 2.3, 3

Additional requirements and compliances

NIS Directive (EU, EP)

EC Directive 2016/1148/EU – Network and Information Security

- Obligations for member states: adoption of a national strategy for NIS & identification of operators of essential services
- Obligations for operators of essential services and for digital service providers
- Implementation deadline: 9 May 2018

EU General Data Protection Regulation (G[illegible])

Deadlines: May 2018

PSD2 (Payment Services Directive – Advanced)

An important "tiny" amendment to the Cyber Act: The Blueprint EU CYBRID: Cyber crisis = Hybrid crisis

Recommendation (EU) 2017/1584 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises:

- importance for Member States to have **a mechanism in place that would allow for an effective handling and response to cybersecurity incidents of a large-scale and crises.**
- how to incorporate cyber security in **existing crisis management mechanisms**
- Fundamental for the cooperation and collaboration mechanisms to handle incident of a large scale (multi countries/sectors/players) – **automation in info exchange, but also in incident response**

- Recommendation Nr. 7

Member States, with the assistance of ENISA and building on previous work in this area, should cooperate in developing and adopting a common taxonomy and template for situational reports to describe the technical causes and impacts of cybersecurity incidents *to further enhance their technical and operational cooperation during crises. In this regard, Member States should take into account the ongoing work within the Cooperation Group on incident notification guidelines and in particular aspects related to the format of national notifications*

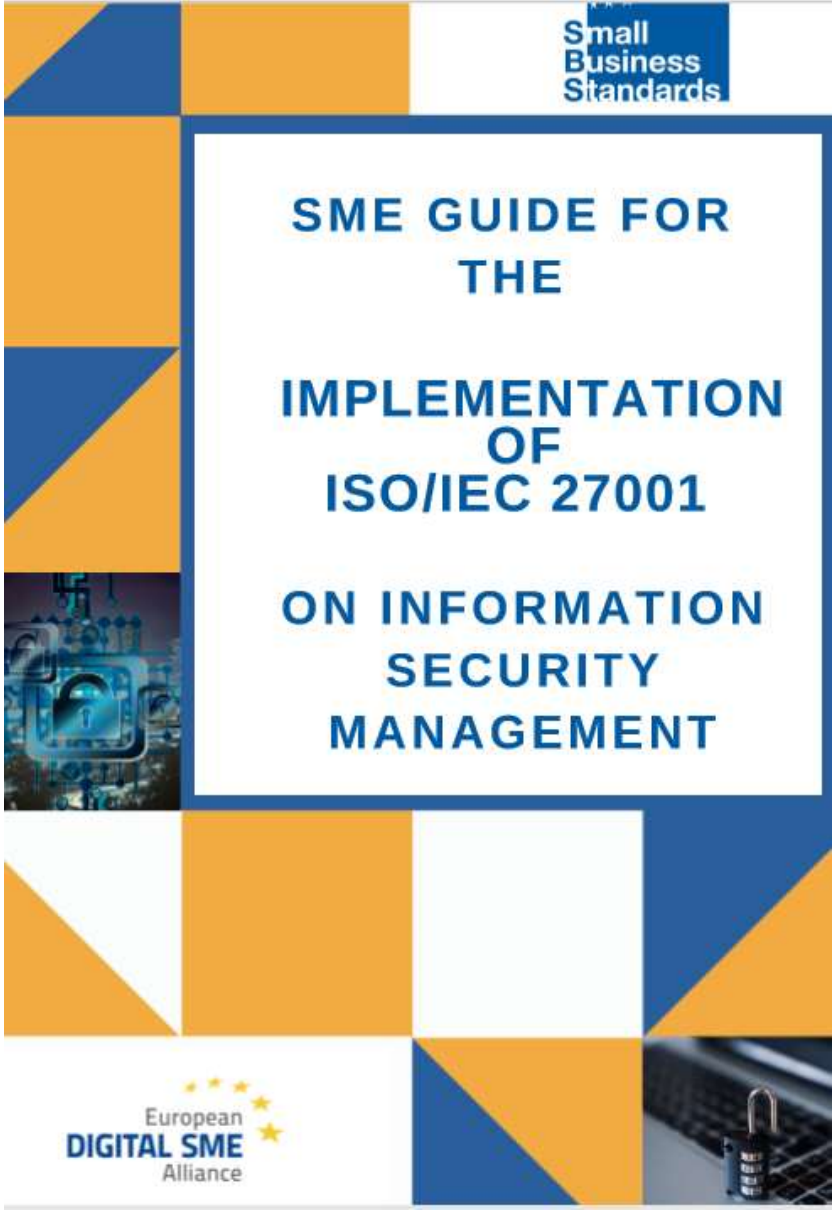
- Recital 20 (on Situational awareness)

Awareness and understanding of the real-time situation, risk posture, and threats gained through reporting, assessments, research, investigation, and analysis, is vital to enable well-informed decisions This 'situational awareness' - by all relevant stakeholders - is essential for an effective coordinated response. Situational awareness includes elements about the causes as well as the impact and origin of the incident.

Assessments: Cyber Resilience Review (CRR)

The Department of Homeland Security (DHS) partnered with the Computer Emergency Response Team (CERT) Division of Carnegie Mellon University's Software Engineering Institute to create the CRR. The CRR is a derivative of the CERT Resilience Management Model (RMM) (http://cert.org/resilience/rmm.html) tailored to the needs of critical infrastructure owners and operators.

https://www.us-cert.gov/ccubedvp/assessments



https://www.digitalsme.eu/new-sbs-guide-information-security-management-standard-iso27001-made-easy-smes/

eu2018bg.bg

VAR: VULNERABILITY ANALYSIS AND RESOLUTION

Related PAs: RISK, MON

VAR:SG1 Prepare for Vulnerability Analysis and Resolution

VAR:SG1.SP1 Establish Scope

VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy

VAR:SG2 Identify and Analyze Vulnerabilities

VAR:SG2.SP1 Identify Sources of Vulnerability Information

VAR:SG2.SP2 Discover Vulnerabilities

VAR:SG2.SP3 Analyze Vulnerabilities

VAR:SG3 Manage Exposure to Vulnerabilities

VAR:SG3.SP1 Manage Exposure to Vulnerabilities

VAR:SG4 Identify Root Causes

VAR:SG4.SP1 Perform Root-Cause Analysis

VAR:SG1.SP1 Establish Scope

The assets and operational environments that must be examined for vulnerabilities are identified

VAR:SG2 Identify and Analyze Vulnerabilities

VAR:SG2.SP1 Identify Sources of Vulnerability Information

These are examples of sources of vulnerability data:

• vendors of software, systems, and hardware technologies that provide warnings on vulnerabilities in their products

• common free catalogs, such as the US-CERT Vulnerability Notes Database and the MITRE Corporation's Common Vulnerabilities and Exposures list

• industry groups

• vulnerability newsgroups and mailing lists

• the results of executing automated tools, techniques, and methods

• internal processes such as service desk, problem management, incident management and control, and monitoring, where vulnerabilities may be detected

VAR:SG2.SP3 Analyze Vulnerabilities

Subpractices…: Prioritize and categorize vulnerabilities for disposition

Examples of categories for vulnerability resolution:

- *Take no action; ignore.*
- *Fix immediately (typically the case for vendor updates or changes).*
- *Develop and implement vulnerability resolution strategy (typically the case when the resolution is more extensive than simple actions such as vendor updates).*
- *Perform additional research and analysis.*
- *Refer the vulnerability to the risk management process for formal risk consideration.*

Референтен стандарт за уеб услуги

Предлага систематизиран преглед на изискванията за сигурност в web

Определя три нива на сигурност, като ниво 2 може да се счита за „нормално“

Ако бъде изискан още на ниво изисквания за web scистеми за държавната администрация би осигурил поне базови нива на сигурност

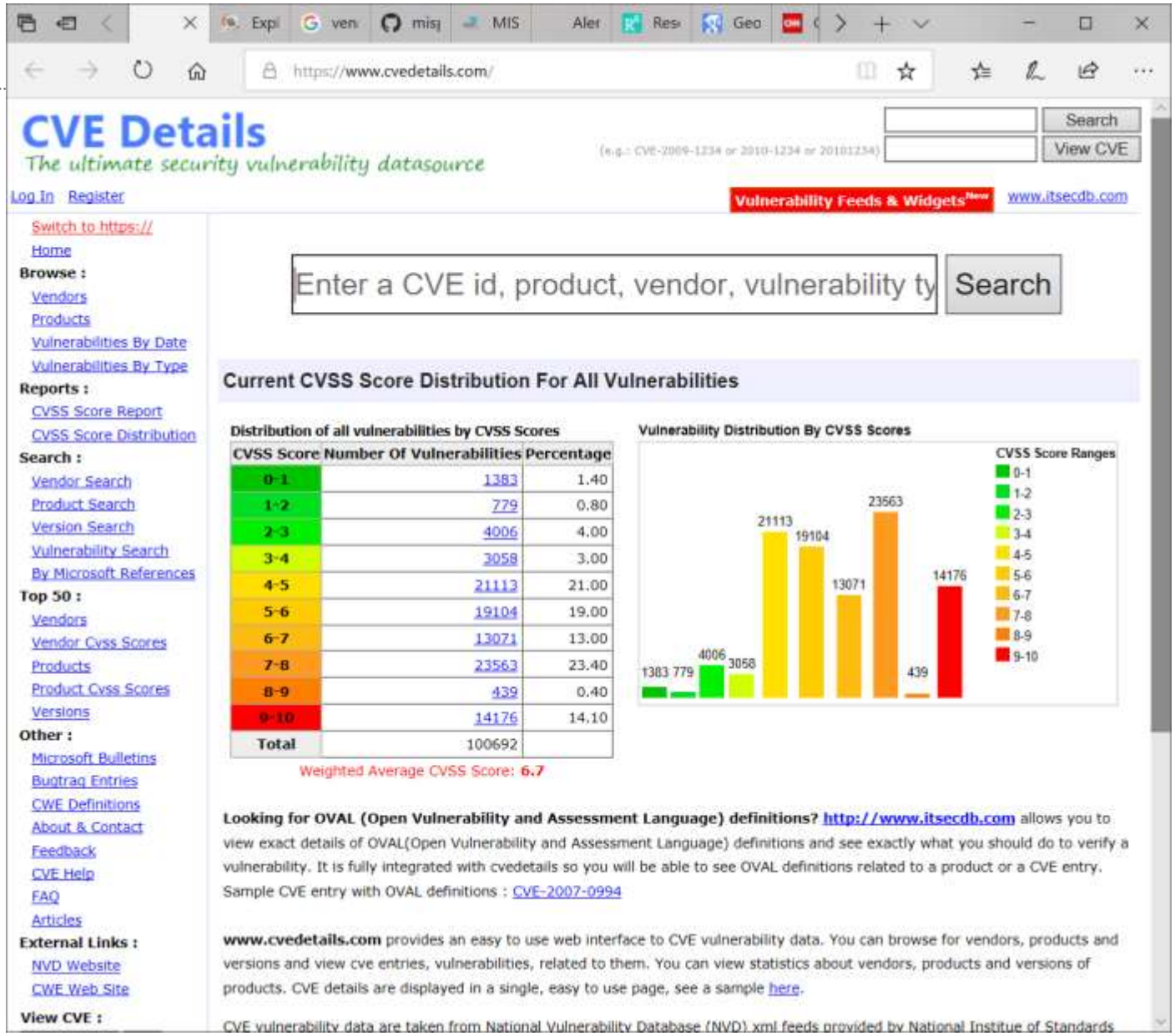
OWASP Application Security Verification Standard (ASVS) Project

Security Verification Requirements

#	Description	L1	L2	L3	Since
1.1	All app components are identified and known to be needed.	✓	✓	✓	1.0
1.2	Security controls are never enforced only on the client side, but on the respective remote endpoints.		✓	✓	1.0
1.3	A high-level architecture for the application and all connected remote services has been defined and security has been addressed in that architecture.		✓	✓	1.0
1.4	Data considered sensitive in the context of the application is clearly identified.			✓	1.0
1.5	All app components are defined in terms of the business functions and/or security functions they provide.			✓	1.0
1.6	A threat model for the application and the associated remote services has been produced that identifies potential threats and countermeasures.			✓	1.0
1.7	All security controls have a centralized implementation.		✓	✓	3.0
1.8	Components are segregated from each other via a defined security control, such as network segmentation, firewall rules, or cloud based security groups.		✓	✓	3.0
1.9	A mechanism for enforcing updates of the application exists.		✓	✓	3.0
1.10	Security is addressed within all parts of the software development lifecycle.		✓	✓	3.0
1.11	all application components, libraries, modules, frameworks, platform, and operating systems are free from known vulnerabilities		✓	✓	3.0.1
1.12	There is an explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow a key management standard such as NIST SP 800-57.		✓	✓	3.1

https://www.exploit-db.com/

https://www.cvedetails.com/



http://www.misp-project.org/datamodels/#misp-taxonomies

How the assess the (potential) impact / damage in unified way (based on unified taxonomy)?

Example of severity of impact scoring system in a multi-state model (MS ISAC, USA)

https://www.cisecurity.org/cybersecurity-threats/alert-level/

How Levels are Determined – using multi-state model (SEE THE LINK FOR DETAILS):

The Alert Level is determined using the following threat severity formula:

Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)

- **Lethality: How likely is it that the attack will do damage?**
  (Value = Potential Damage)
  - *5: Exploit exists. Attacker could gain root or administrator privileges. Attacker could commit denial of service.*
  - *4: Exploit exists. Attacker could gain user level access privileges. Attacker could commit denial of service.*
  - *3: No known exploit exists. Attacker could gain root or administrator privileges. Attacker could commit degradation of service.*
  - *2: No known exploit exists. Attacker could gain user level access privileges.*
  - *1: No known exploit exists. Attacker could not gain access.*
- **Criticality: What is the target of the attack?**
  (Value = Target)
- **System Countermeasures: What host-based preventive measures are in place?**
  (Value = Countermeasure)
- **Network Countermeasures: What network-based preventive measures are in place?**
  (Value = Countermeasure)

Using the result from the formula defined above, the Alert Level Indicator would generally reflect severity levels as follows:

Alert Level Indicator - Severity

- Green - Low : -8 to -5
- Blue - Guarded : -4 to -2
- Yellow - Elevated : -1 to +2
- Orange - High : +3 to +5
- Red - Severe : +6 to +8

COMM: Communications

COMM:SG1 Prepare for Resilience Communications

- COMM:SG1.SP1 Establish a Resilience Communications Plan
- COMM:SG1.SP2 Identify Communications Requirements
- COMM:SG1.SP3 Establish Communications Guidelines and Standards

COMM:SG2 Deliver Resilience Communications

- COMM:SG2.SP1 Identify Communications Methods and Channels
- COMM:SG2.SP2 Establish and Maintain Communications Infrastructure
- COMM:SG2.SP3 Provide Resilience Communications

COMM:SG3 Improve Communications

- COMM:SG3.SP1 Assess Communications Effectiveness
- COMM:SG3.SP2 Improve Communications

EF: Enterprise Focus

EF:SG1 Establish Strategic Objectives: The strategic objectives are established as the foundation for the operational resilience management system.

EF:SG1.SP1 Establish Strategic Objectives: Strategic objectives are identified and established as the basis for resilience activities.

EF:SG1.SP2 Establish Critical Success Factors: The critical success factors of the organization are identified and established.

EF:SG1.SP3 Establish Organizational Services: The high-value services that support the accomplishment of strategic objectives are established.

EF:SG2 Plan for Operational Resilience: Planning for the operational resilience system is performed.

EF:SG2.SP1 Establish an Operational Resilience Management Plan: A plan for managing operational resilience is established as the basis for the operational management program.

EF:SG2.SP2 Establish an Operational Resilience Management Program: A program is established to carry out the activities and practices of the operational resilience management plan.

EF:SG3 Establish Sponsorship: Visible sponsorship of higher level managers for the operational resilience management system is established.

EF:SG3.SP1 Commit Funding for Operational Resilience Management: A commitment by higher level managers to fund resilience activities is established.

EF:SG3.SP2 Promote a Resilience Aware Culture: A resilience-aware culture is promoted through goal setting and achievement.

EF:SG3:SP3 Sponsor Resilience Standards and Policies: The development, implementation, enforcement, and management of resilience standards and policies are sponsored.

EF:SG4 Provide Resilience Oversight: Governance over the operational resilience management system is established and performed.

EF:SG4.SP1 Establish Resilience as a Governance Focus Area: Governance activities are extended to the operational resilience management system and accomplishment of the process goals.

EF:SG4.SP2 Perform Resilience Oversight: Oversight is performed over the operational resilience management system for adherence to established procedures, policies, standards, guidelines, and regulations.

EF:SP4.SP3 Establish Corrective Actions: Corrective actions are identified to address performance issues.

Is this the new paranoia ?

"A paranoid is someone who knows a little of what's going on.

A psychotic is a guy who's just found out what's going on."
~ William S. Burroughs (1914-1997)

Remember: mind the bear!

http://www.youtube.com/watch?v=Qk2I69ZAV4Y

credits:

CERT-RMM LA Apprentice Program

Presentations: International Symposium "*Recent Developments in Cryptography and Information Security"* (Bulgaria, 2007, 2008)
EU/EC /CEN reports
SEI/CERT profile
public press and media, as indicated