ESI European Software Institute Center Eastern Europe

CERT

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?]**

PLOVDIV UNIVERSITY „PAISII HILENDARSKI"
FACULTY OF MATHEMATICS AND INFORMATICS

ФМИ, ПУ – 4 курс, СИ

Dr. George Sharkov gesha@esicenter.bg (ESI CEE), gsharkov@uni-plovdiv.bg
Dr. Maya Stoeva mstoeva@uni-plovdiv.bg
Christina Todorova tina@esicenter.bg (ESI CEE CyResLab)

SEMP SOFTWARE ENGINEERING MANAGEMENT PROGRAM

http://SEMP.esicenter.bg

Carnegie Mellon University
ISR 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.	2	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	4

Съдържание (cont.)

№	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	6	4
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	4
6	Изготвяне и представяне на доклад (презентация) за заплахи, слабости, кибер атаки. Оценка на щетите. Превенция и реакция.	2	6

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

ESI CEE - European Software Institute Center Eastern Europe

Cyber Security and Resilience Lab

ESI CEE founded in 2003 as part of European Software Institute

Cyber Resilience Laboratory (CyResLab.org) - in 2013, supported by CERT @ Software Engineering Institute, Carnegie Mellon University

co-founded Cyber Security Lab @ Sofia Tech Park, public-private-partnership

https://sofiatech.bg/en/laboratory-complex/laboratories/cyber-security-lab-2/

2018 we've joined forces – CySec/ResLab - Security & Resilience – Two Sides of A (Winning) Coin

Holistic approach

Research **weaknesses** of the **digital dependency** in both the **public** and the **private sector**, development of **models** and **platforms** for **simulation**, **detection** and **prevention**

Research and development of **methods** and **solutions** to ensure **security**, **sustainability** and **resilience** for CIP and CIIP

Design and elaboration of **secure and sustainable models** as well as **informational solutions** for both the **public** (e-government) and the **private** (business) sectors on national and international level

Development and provision of a center for **trainings** and **testing** in the sphere of **informational security** and **cyber resilience**, prevention and defense against cyber threats – pen testing, white/black/grey box testing, red-team testing

www.cryptobg.org

CERT | Software Engineering Institute | Carnegie Mellon

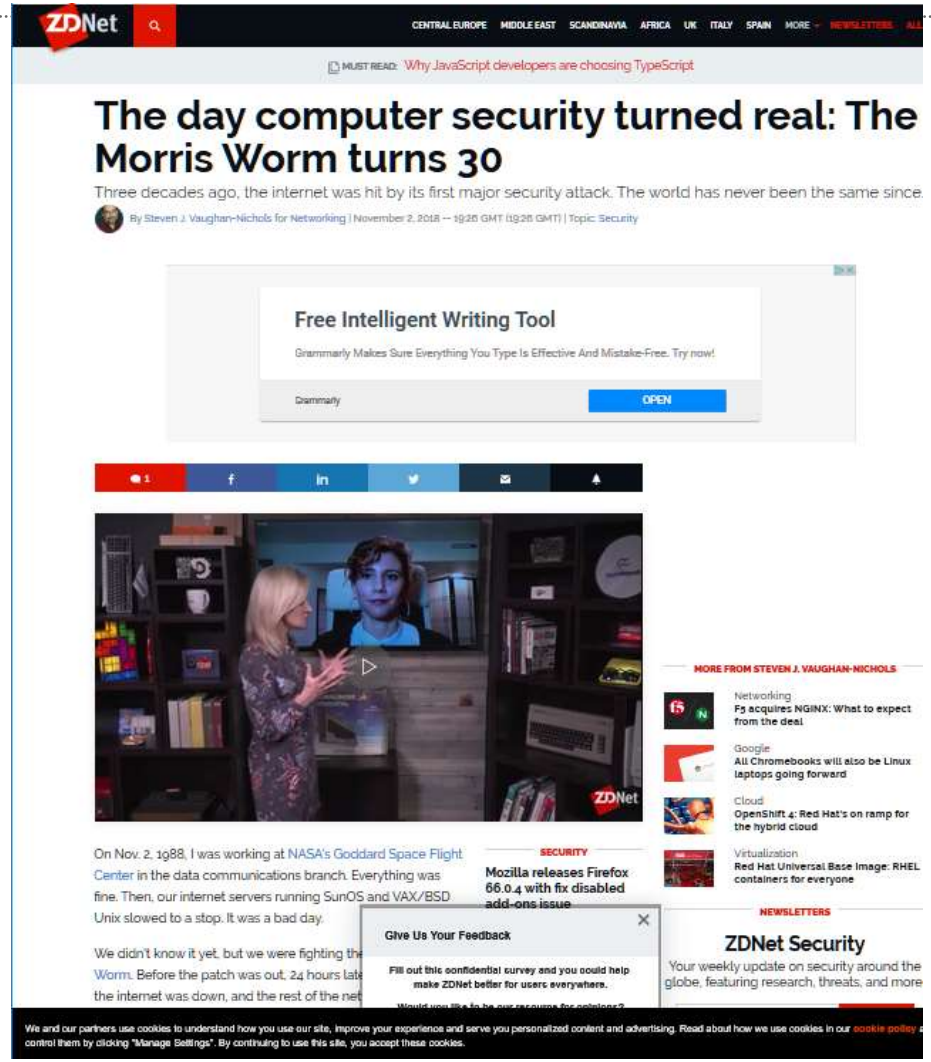
Carnegie Mellon University

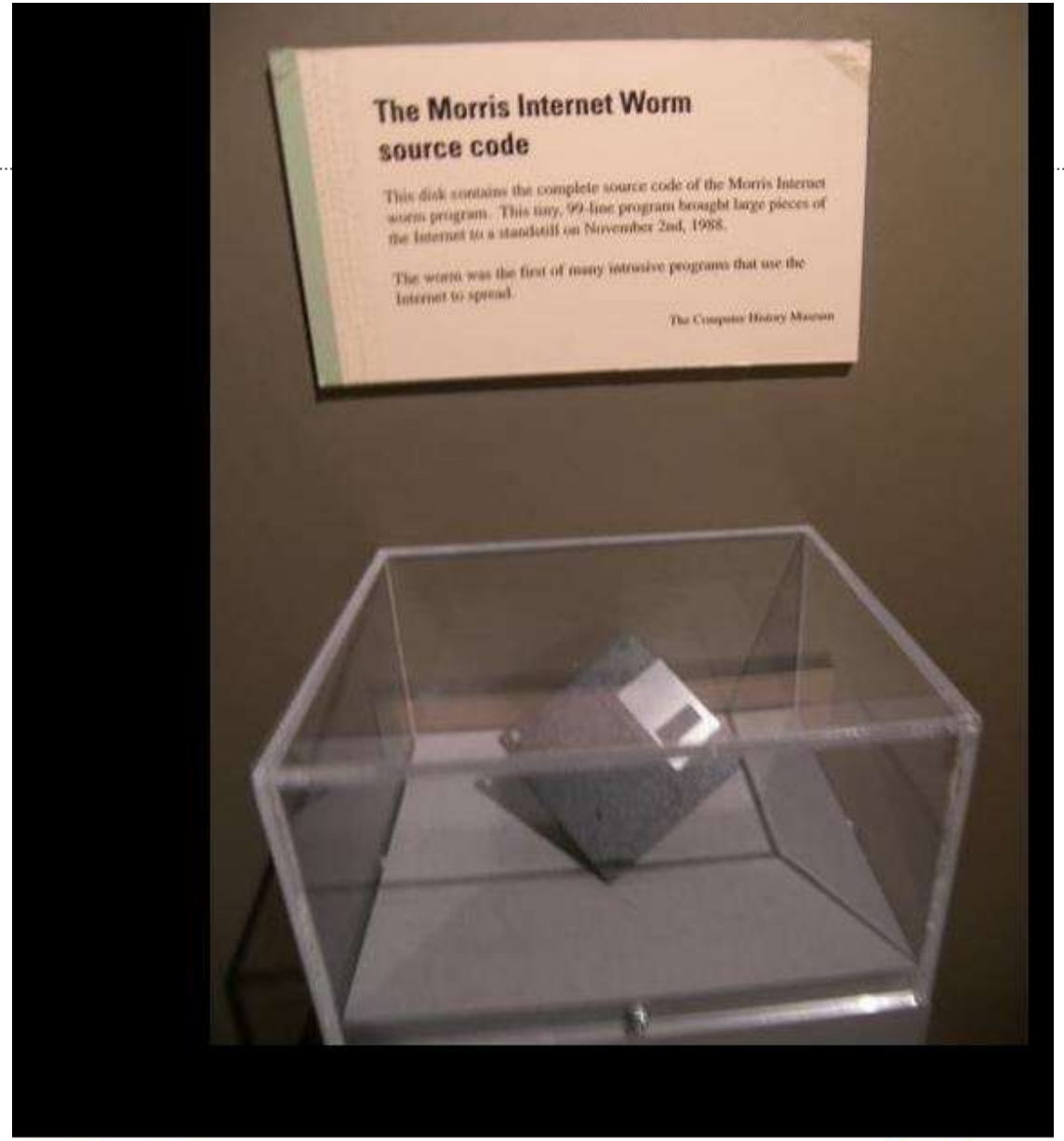
Software Engineering Institute (SEI)

- 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





Floppy Diskette containing the source code for the Morris Worm held at the Computer History Museum.

Go Card USA from Boston, USA - Museum of Science - Morris

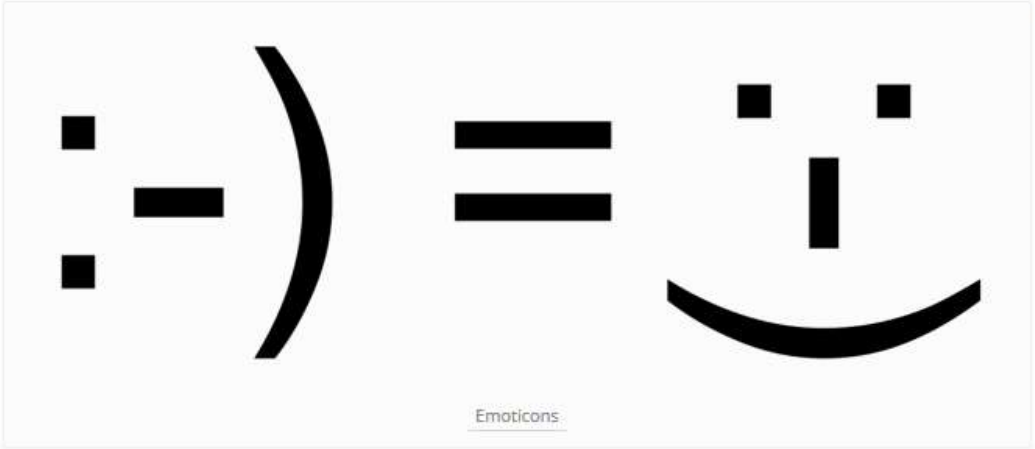
Morris worm - Wikipedia | The day computer security t | Scott Fahlman and the (

scihi.org/scott-fahlman-emoticons/

You are here: Home › computer science › Scott Fahlman and the Origin of the Emoticons :-)

Scott Fahlman and the Origin of the Emoticons :-)

computer science 19. September 2018 0 Harald Sack



Emoticons

On September 19 , 1982 , **Scott Fahlman** posted the first documented emoticons 🙂 and 😕 on the Carnegie Mellon University Bulletin Board System . As SMS and the Internet became widespread in the late 1990s , emoticons became increasingly popular and were commonly used on text messages , internet forums and e-mails . Emoticons have played a significant role in communication through technology .

> *"I often think there should exist a special typographical sign for a smile — some sort of concave mark, a supine round bracket."*
> *— Vladimir Nabokov, NYT interview in 1969*

SEARCH

Search...

FOLLOW US

Tweets by @SciHiBlog

SciHi
@SciHiBlog

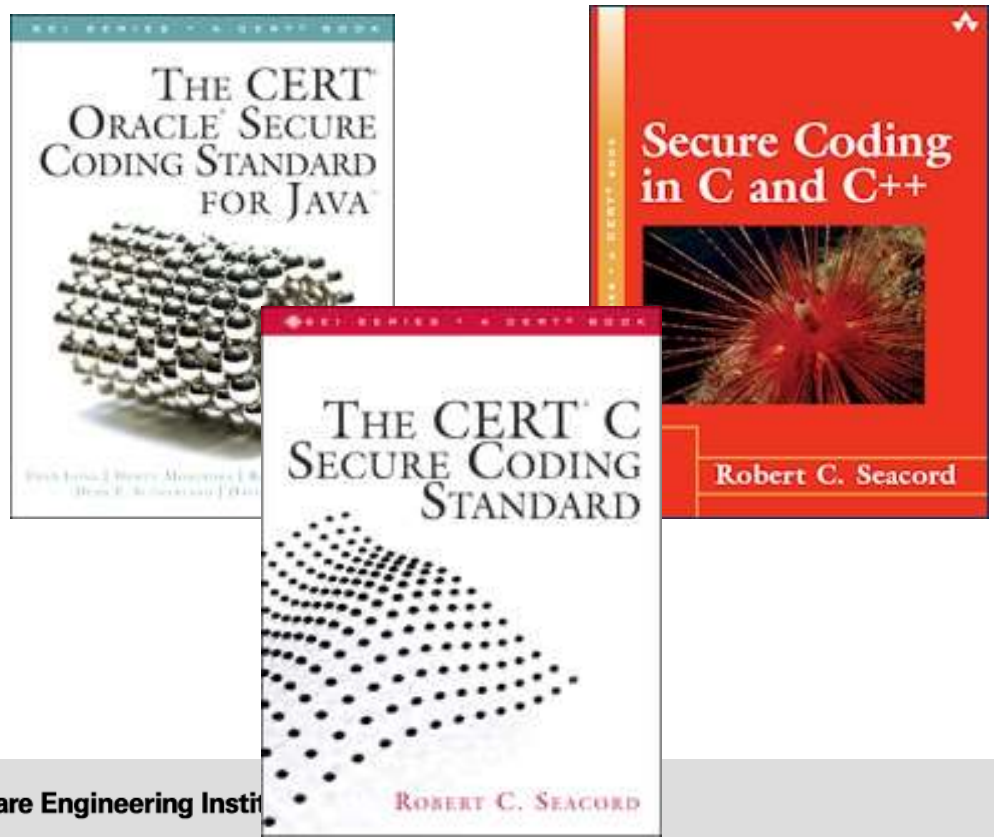
Chess playing automata have a long tradition, as e.g. The famous Turk, by Wolfgang von Kempelenscihi.org/deepblue-vs-ga…

Computer Emergency Response Team

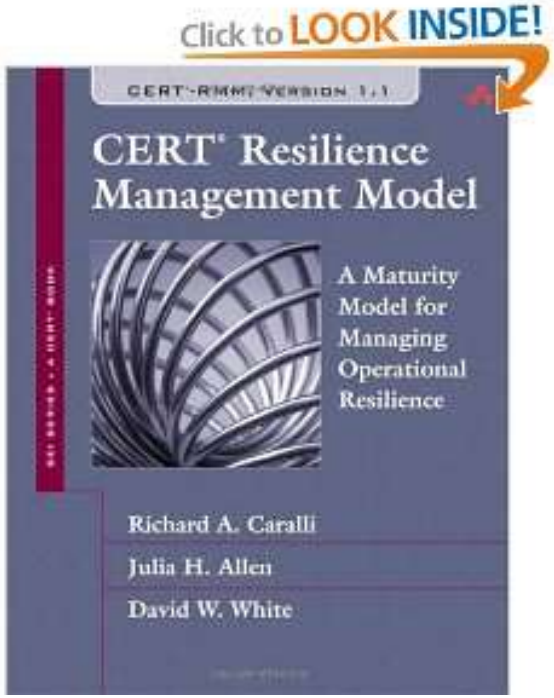
Software Engineering Institute | Carnegie Mellon

CERT

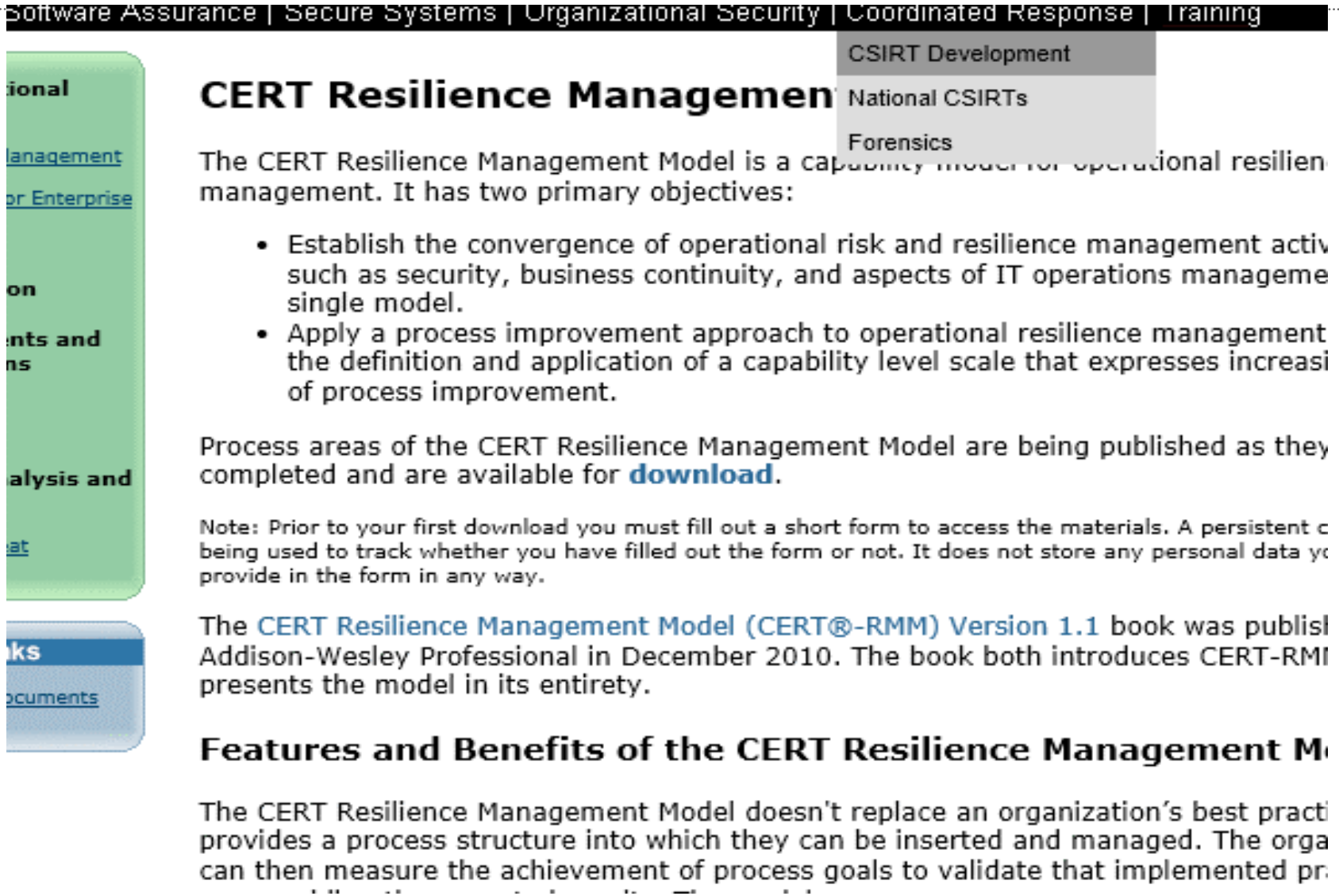
Closing gaps & develop good code:
Secure Coding Standards
[languages + compilers]



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



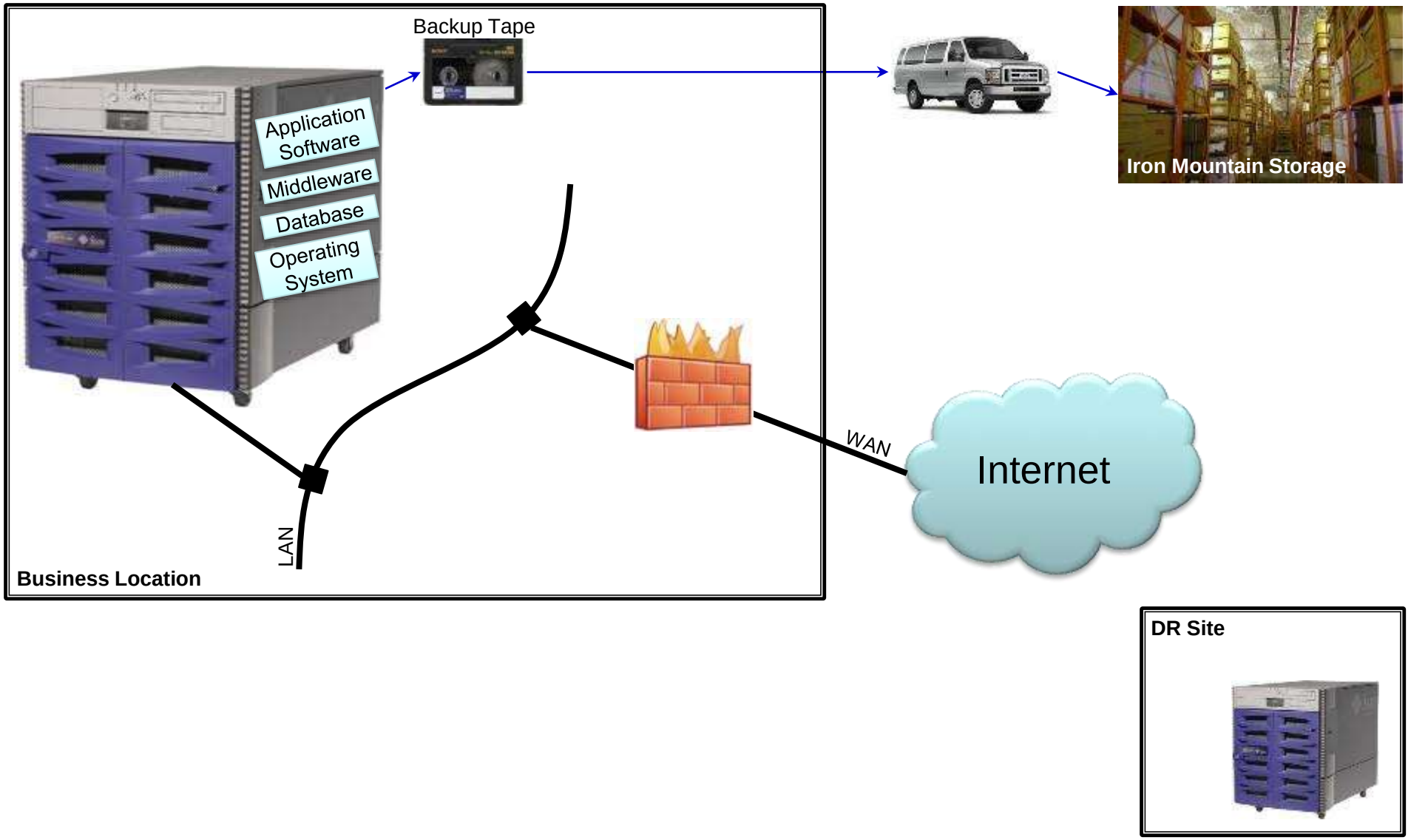
http://www.cert.org/resilience/rmm.html



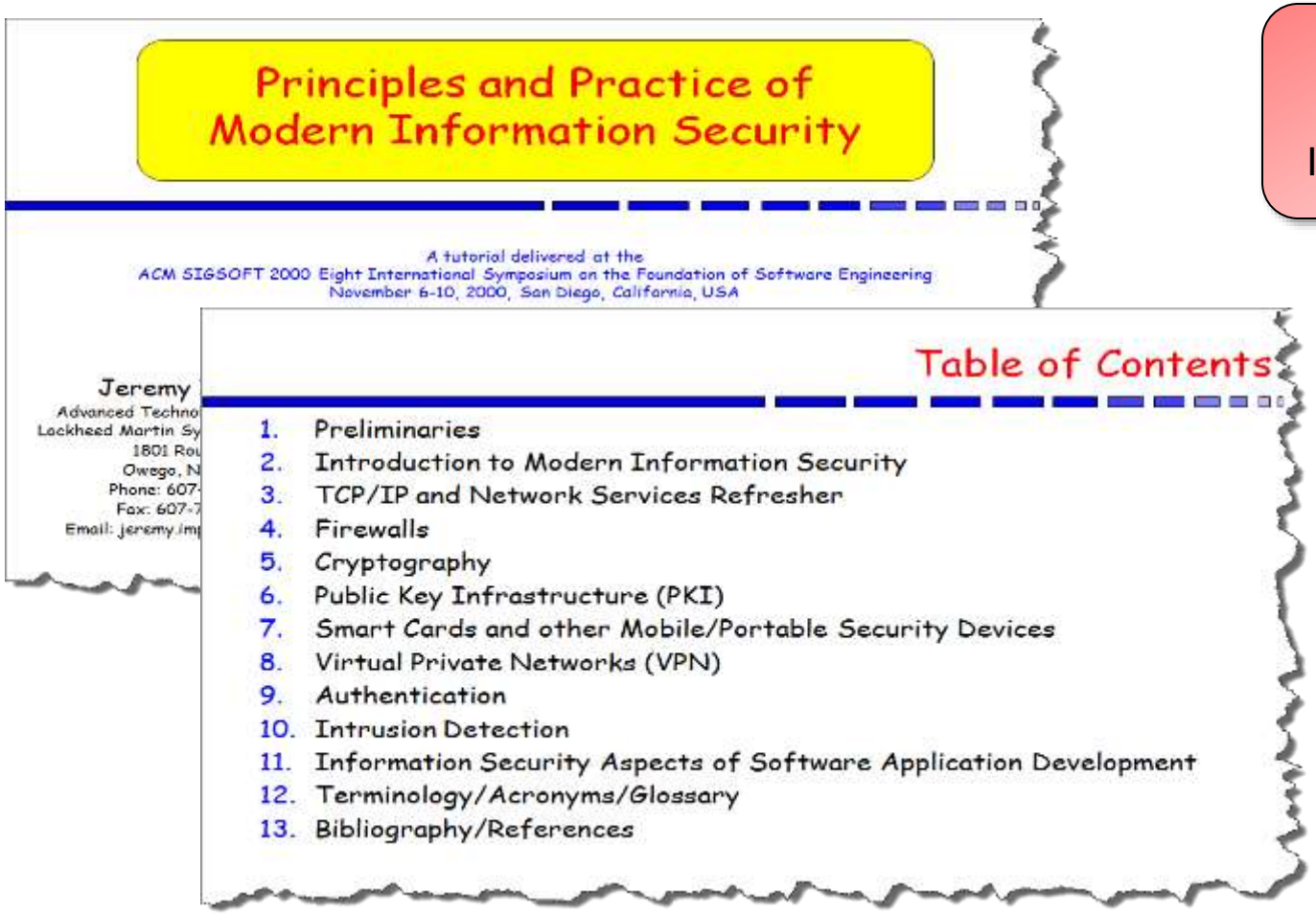
КИБЕРСИГУРНОСТ И ВЪЗМОЖНОСТИ ЗА ПРИЛОЖЕНИЕ НА ИНОВАТИВНИ ТЕХНОЛОГИИ В РАБОТАТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ В БЪЛГАРИЯ

https://www.ipa.government.bg/bg/publications#cbp=/bg/kibersigurnost-i-vzmozhnosti-za-prilozhenie-na-inovativni-tehnologii-v-rabotata-na-drzhavnata

Yesterday it would have been about…



Yesterday it would have looked like…



Principles and Practice of Modern Information Security

A tutorial delivered at the
ACM SIGSOFT 2000 Eight International Symposium on the Foundation of Software Engineering
November 6-10, 2000, San Diego, California, USA

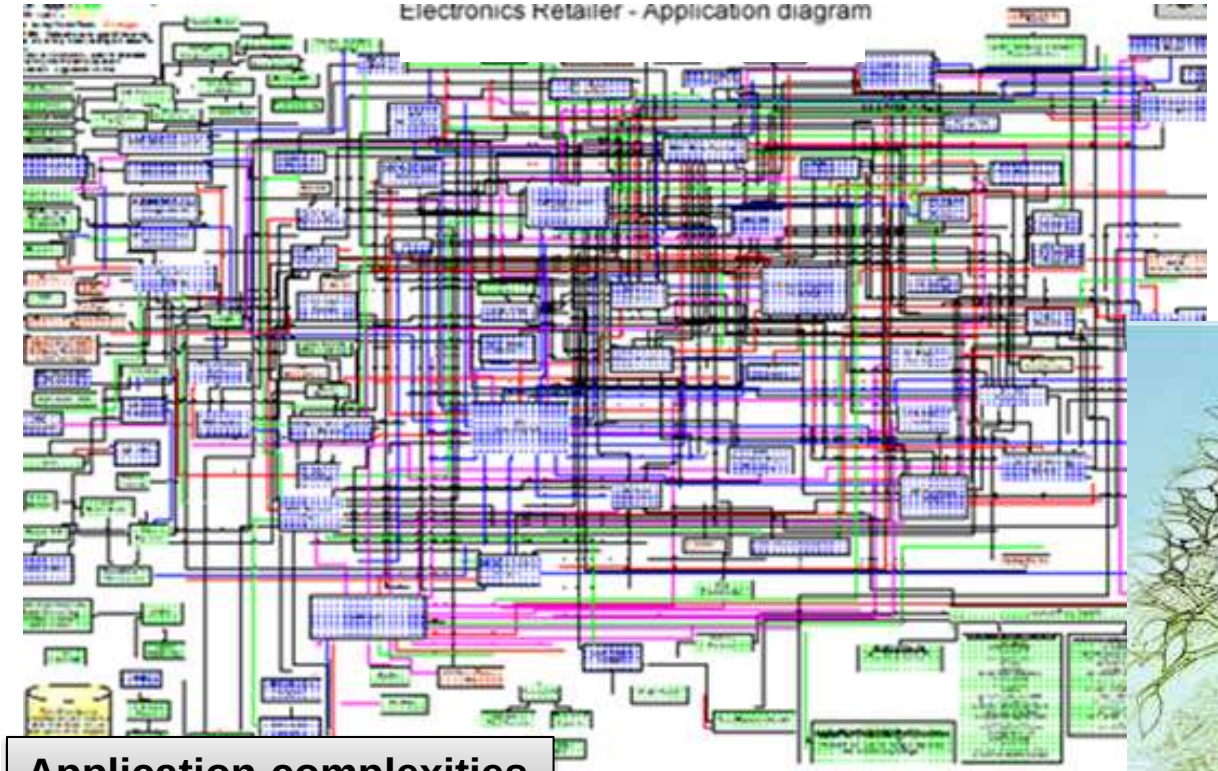
Jeremy
Advanced Techno
Lockheed Martin Sy
1801 Rou
Owego, N
Phone: 607-
Fax: 607-7
Email: jeremy.m

Table of Contents

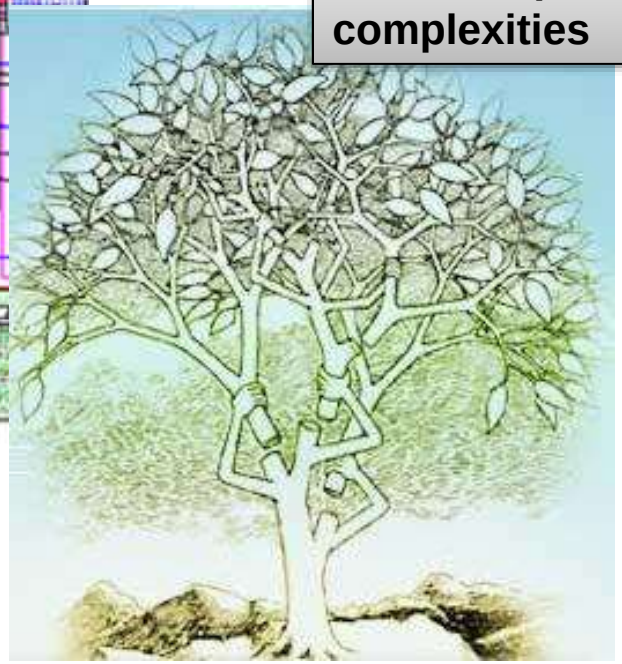
1. Preliminaries
2. Introduction to Modern Information Security
3. TCP/IP and Network Services Refresher
4. Firewalls
5. Cryptography
6. Public Key Infrastructure (PKI)
7. Smart Cards and other Mobile/Portable Security Devices
8. Virtual Private Networks (VPN)
9. Authentication
10. Intrusion Detection
11. Information Security Aspects of Software Application Development
12. Terminology/Acronyms/Glossary
13. Bibliography/References

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…

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 Accoun

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 19, 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

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 resume some 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 chain a it works to sharply increase production.

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

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

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 group that was storing part center. The brains were donated by families of people

Francine Benes, director of the Harvard brain center, research. "The question is by how much," she said.

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 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

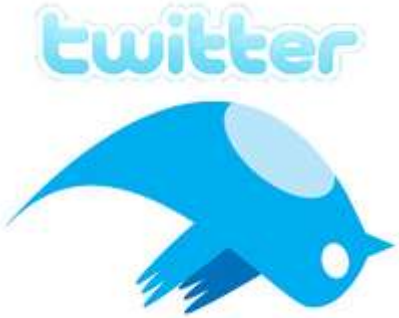
Data-Center Failures Hit Twitter Users

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]ming 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

A A

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.

Enlarge Image

Prakash Singh/Agence Fr

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 blackout that raised questions about the

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 was hacked, resulting in multiple false posts to its website, including a fake interview with a Syrian rebel army leader.

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

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

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

Reuters said the Free Syrian Army released a statement saying that the interview never took place and blamed Syrian President Bashar al-Assad's government for the false

REUTERS

REUTERS EDITION: U.S.

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

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 plane pound vital p Aleppo
Sat, Aug 4 2012

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

Reuters blo

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

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.

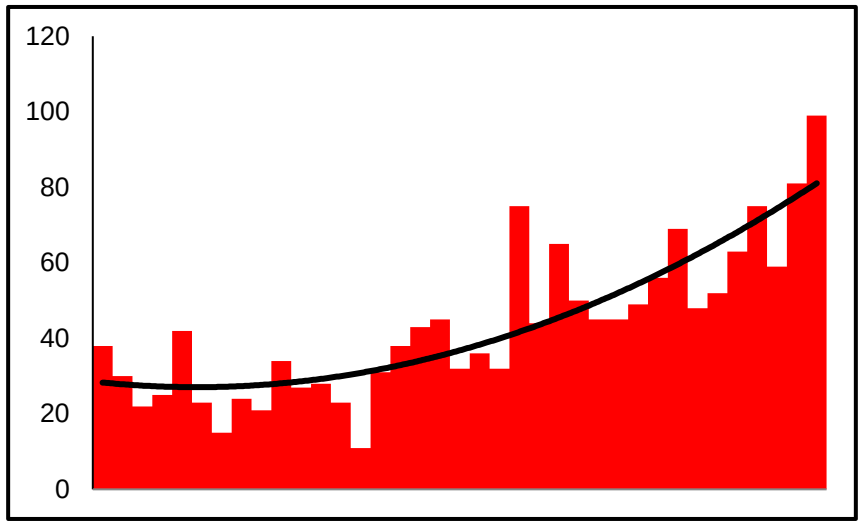
"Initial analysis caused particular concern when one sample was linked to known sophisticated malware," according to CERT, which deployed a team in October for an on-site inspection.

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

January 16, 2013

What do they all point to?

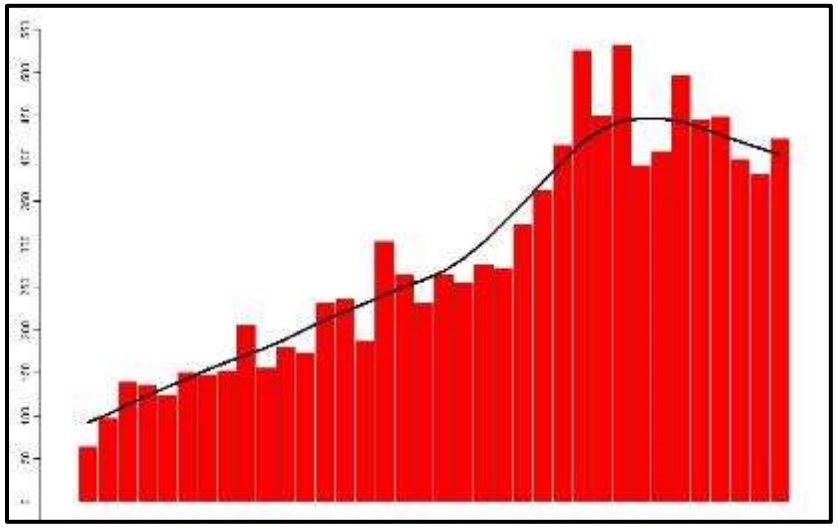
Are there more disruptive events?



Federal Emergency Management Agency

US Declared Disasters

1975-2011

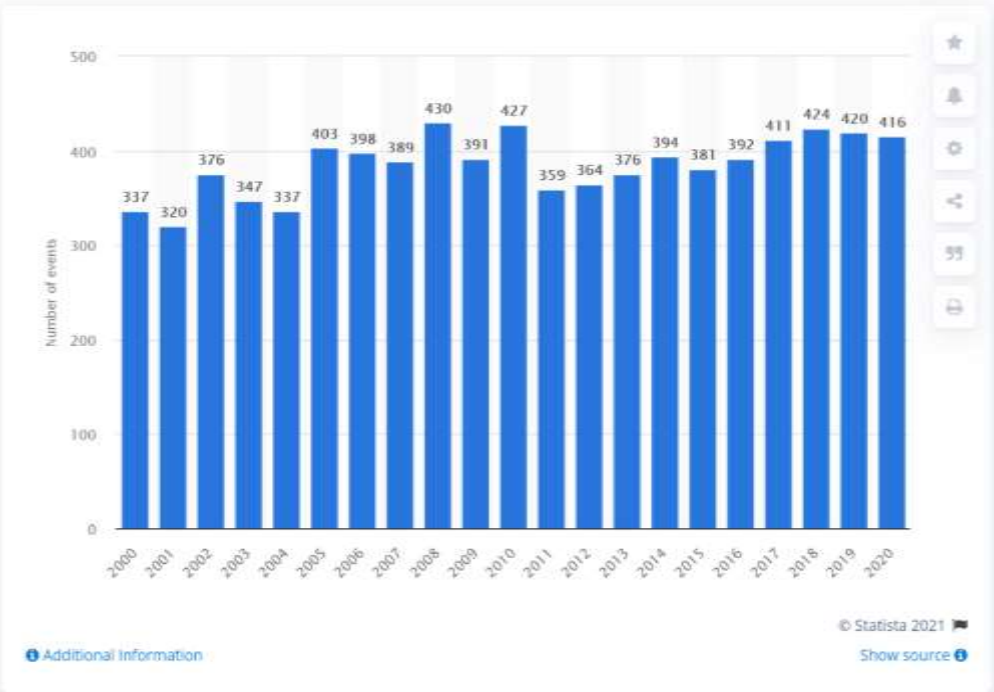


The International Disaster Database

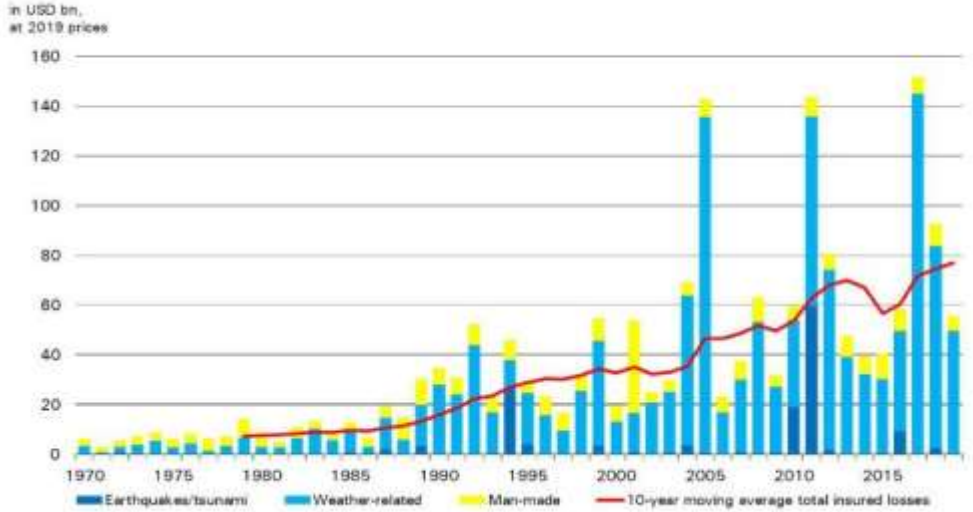
Worldwide Disasters

1975-2010

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



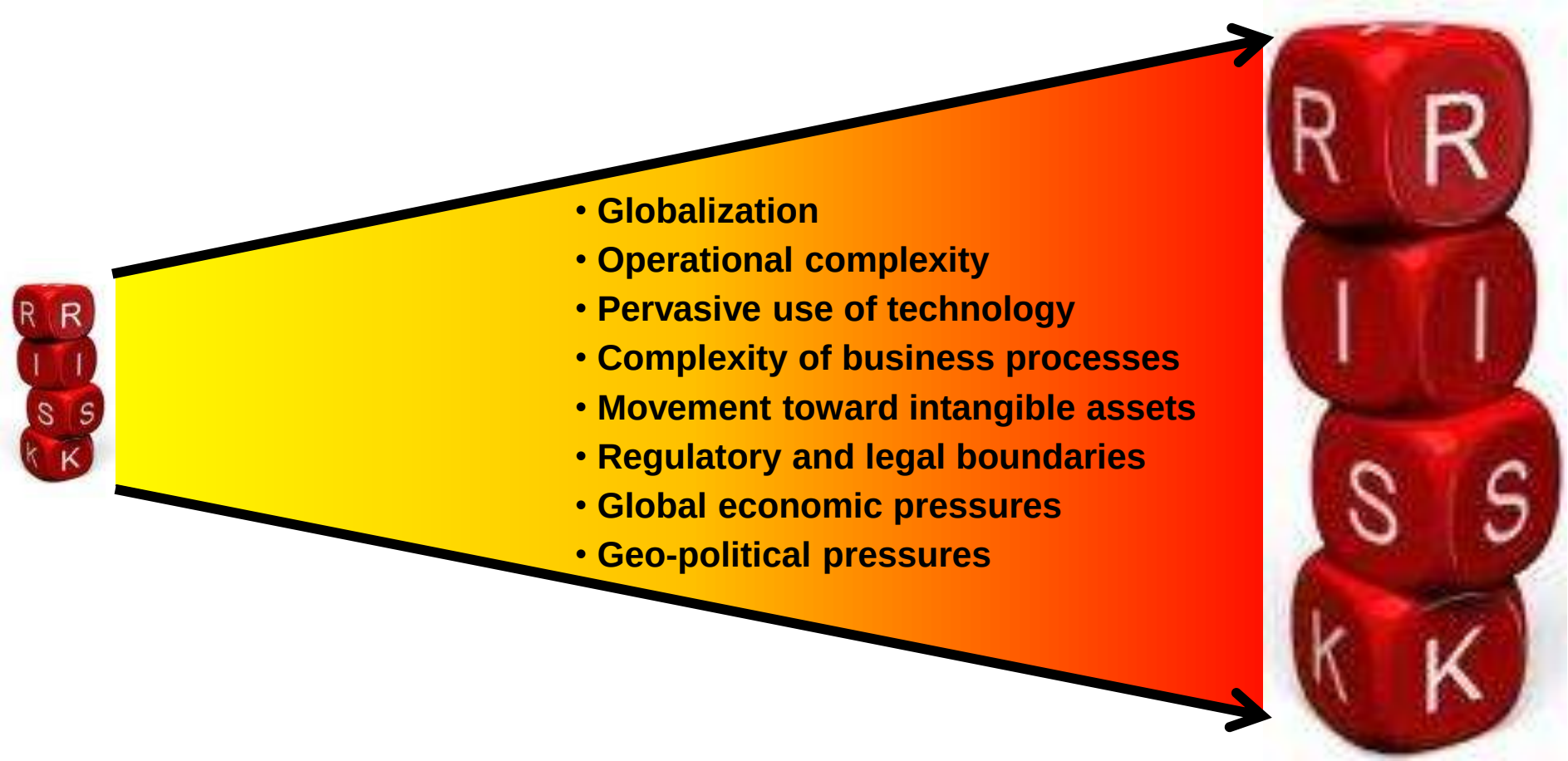
Annual number of natural disaster events globally from 2000 to 2020



Global catastrophes caused USD 56 billion insured losses in 2019, estimates Swiss Re Institute

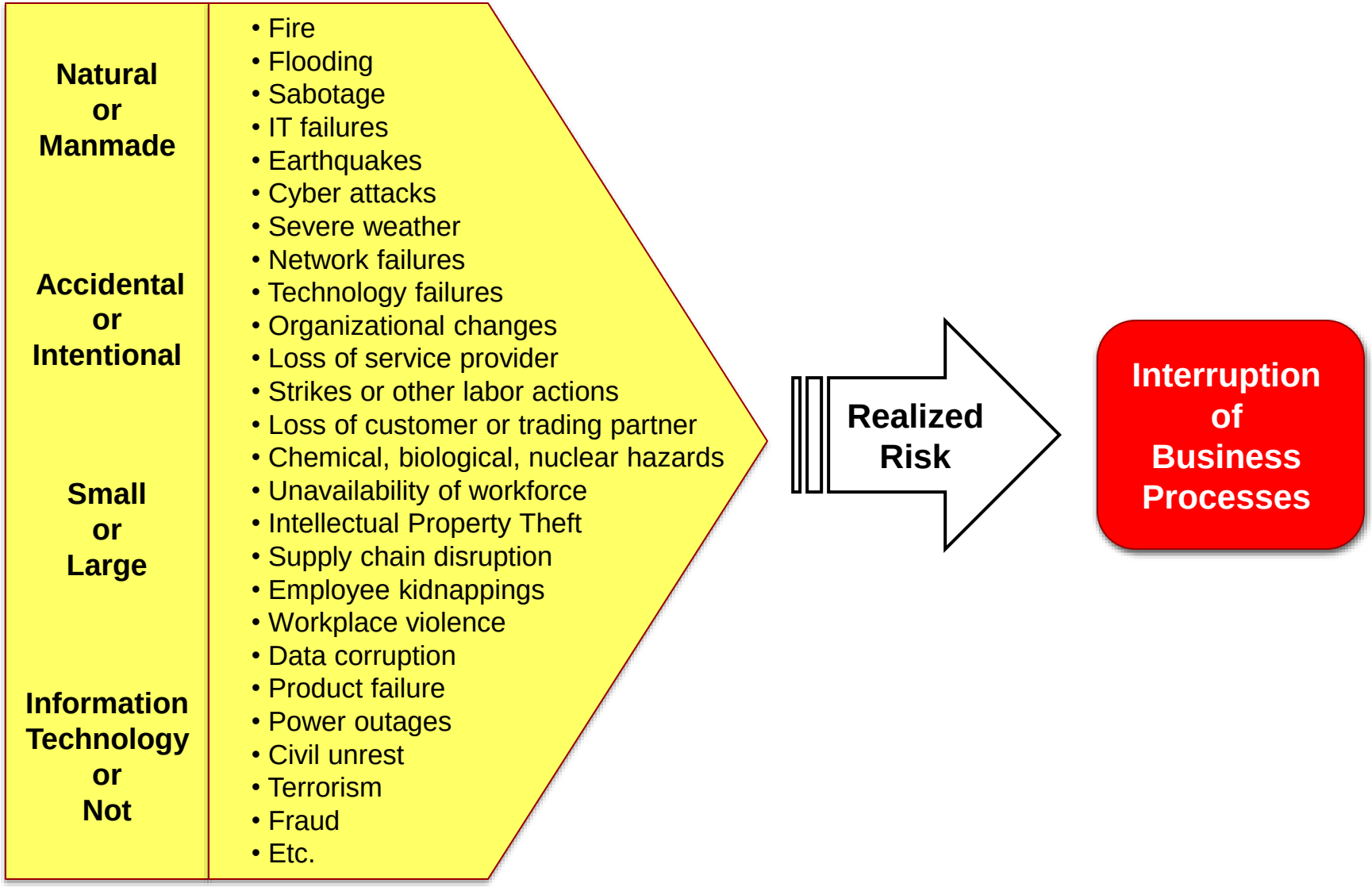
https://www.swissre.com/media/news-releases/nr-20191219-global-catastrophes-estimate.html

What is the Right Question to Ask?

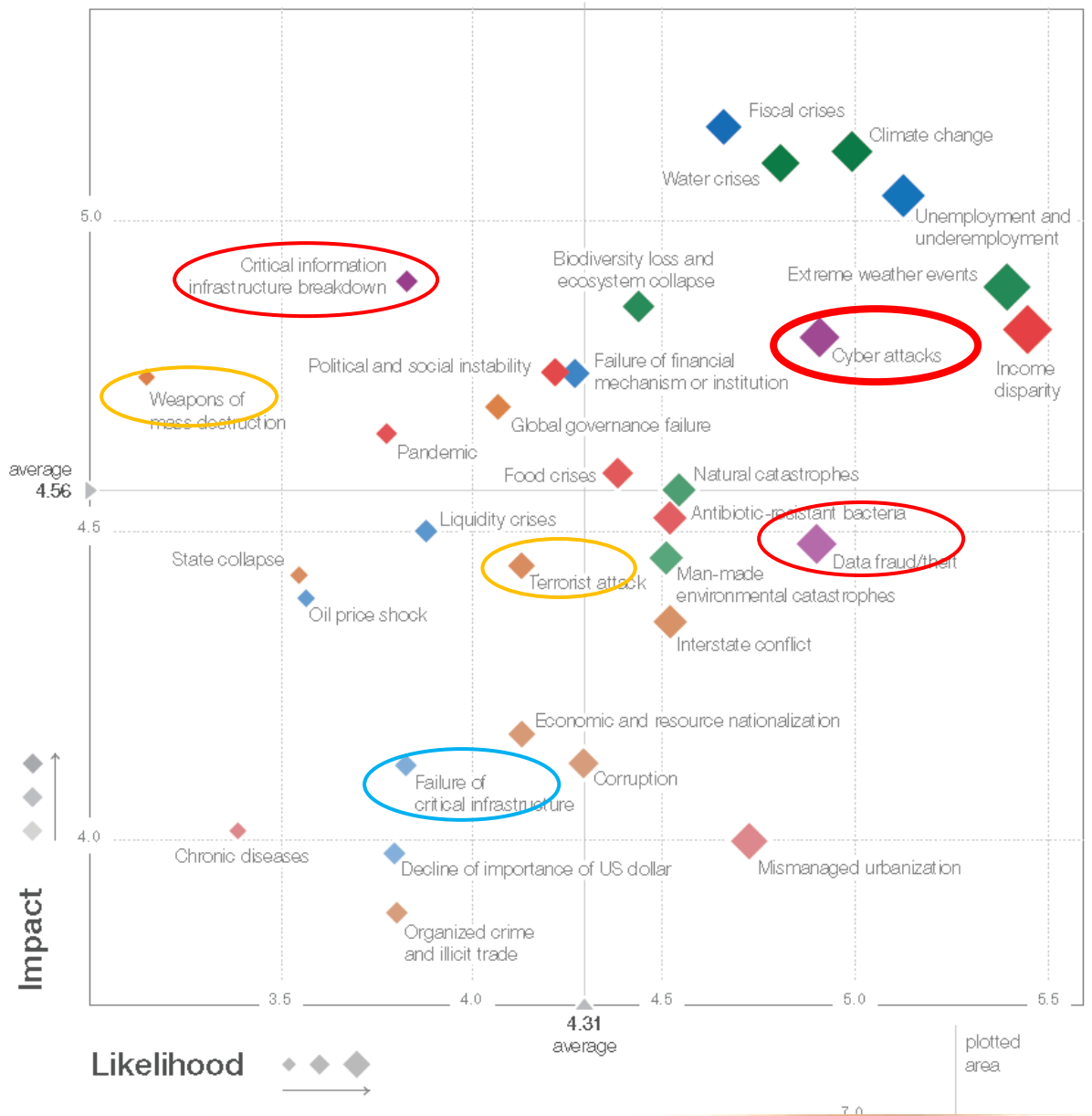


Is the Risk Environment Expanding?

Disruptive Events

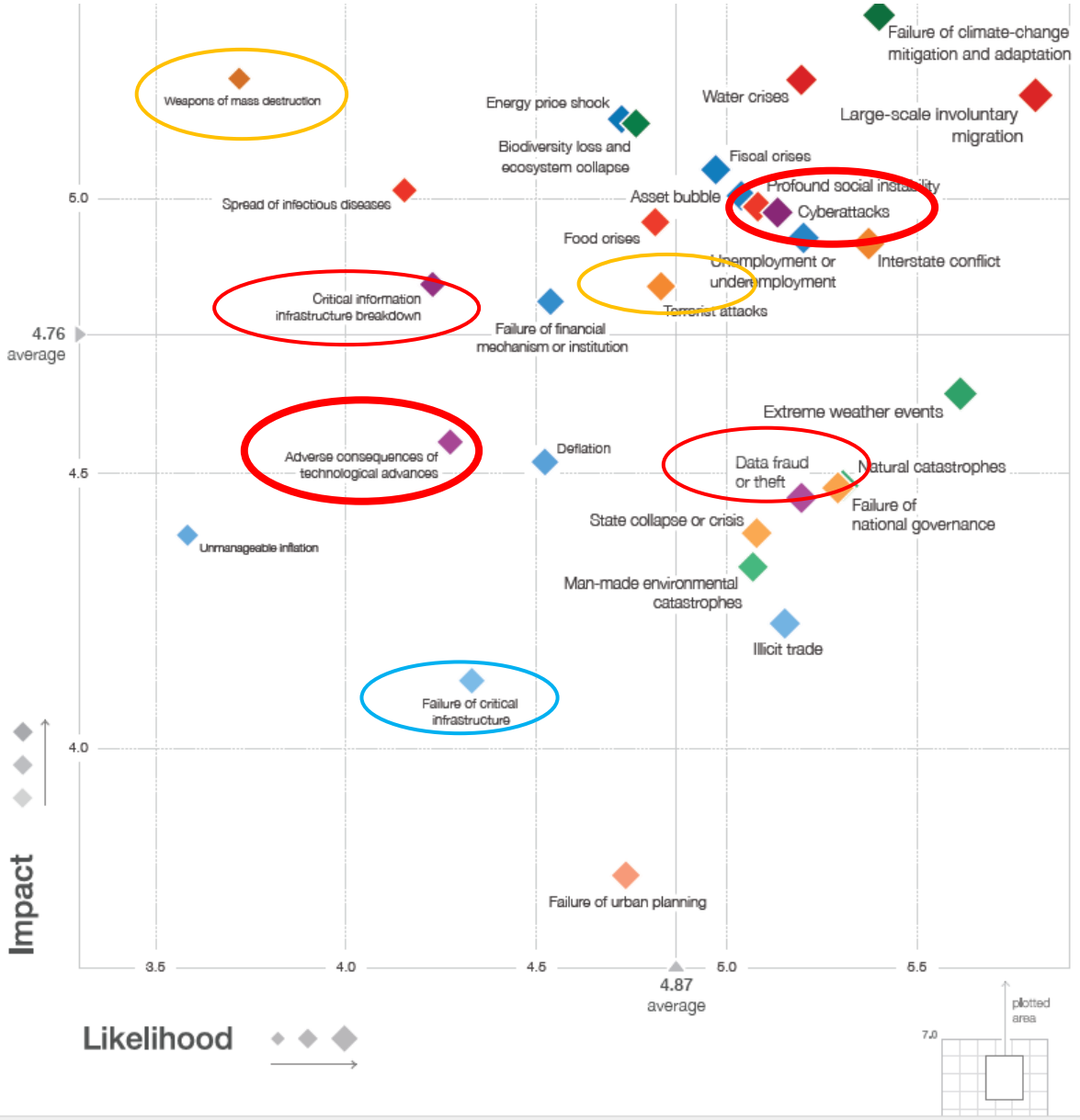


The Global Risk Landscape - 2014



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

The Global Risk Landscape - 2016



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]bilities (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".[80] 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."*[81] 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

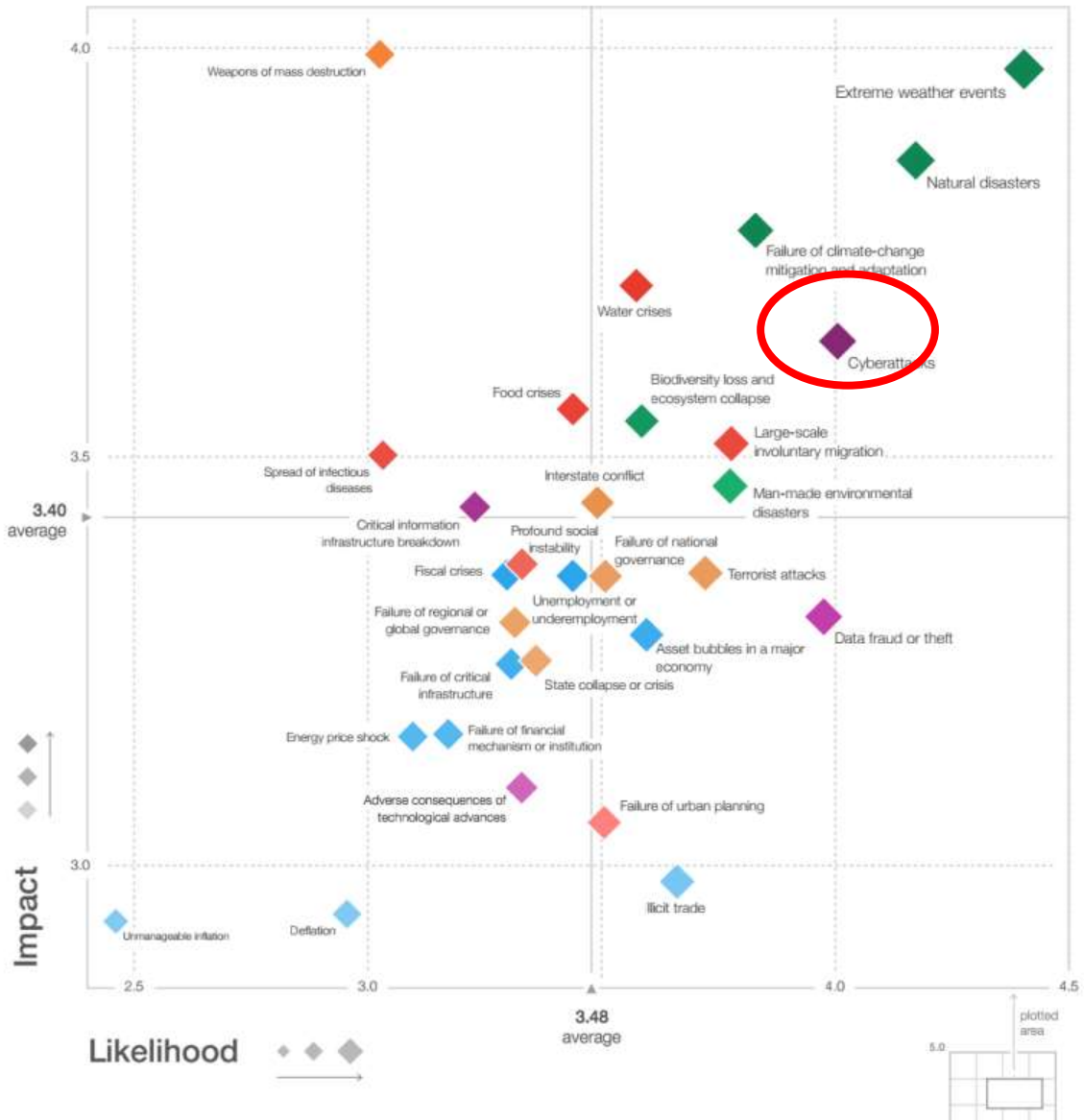
and capabilities for readiness, respo… reconstitution and reinvention. Building resilience to large-scale cyberattacks requires a concerted effort towards advancing the understanding of and the disciplines that contribute to cyber resilience. This section posits a number of suggestions on how to improve 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

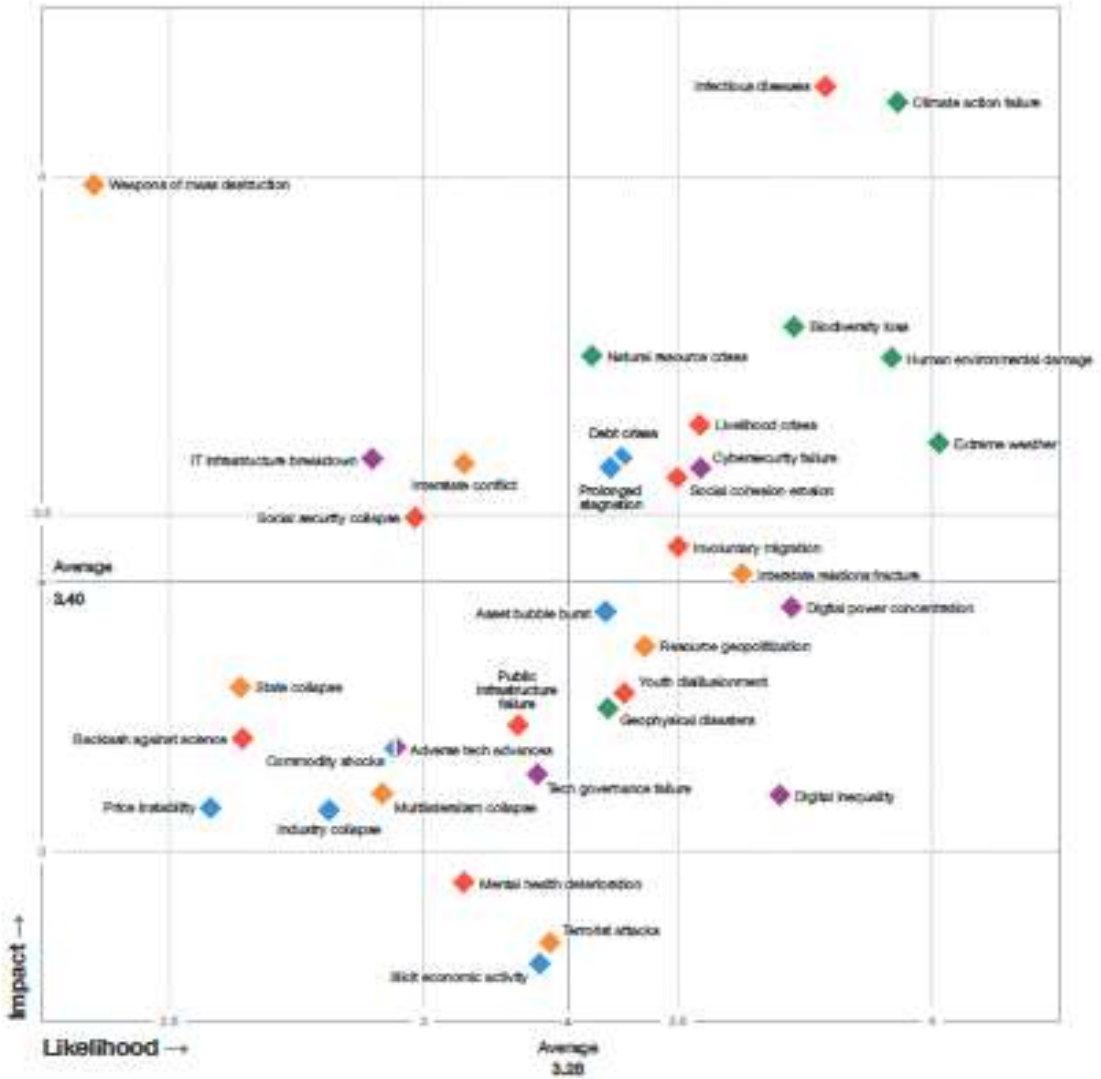
To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity

FIGURE II

Global Risks Landscape

2021

How do respondents perceive the impact ↑ and likelihood → of global risks?

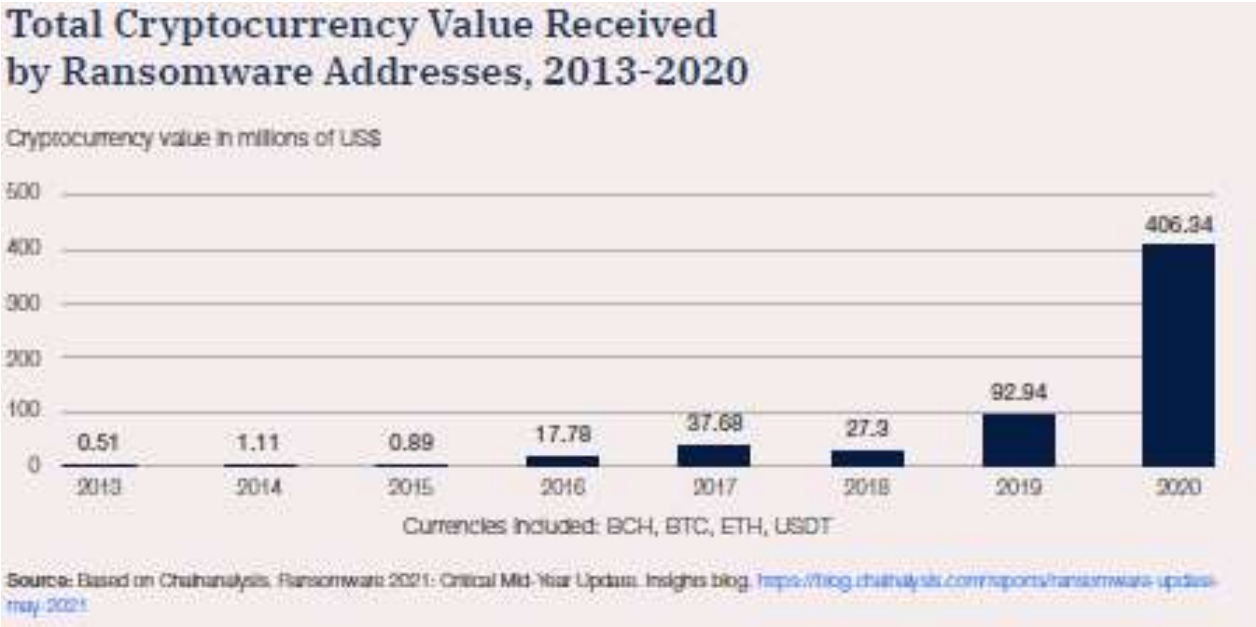


Evolving Risks Landscape

Top Global Risks by Likelihood

	1st	2nd	3rd	4th	5th	6th	7th
2021	Extreme weather	Climate action failure	Human environmental damage	Infectious diseases	Biodiversity loss	Digital power concentration	Digital inequality

	1st	2nd	3rd	4th	5th
2020	Extreme weather	Climate action failure	Natural disasters	Biodiversity loss	Human-made environmental disasters
2019	Extreme weather	Climate action failure	Natural disasters	Data fraud or theft	Cyberattacks
2018	Extreme weather	Natural disasters	Cyberattacks	Data fraud or theft	Climate action failure
2017	Extreme weather	Involuntary migration	Natural disasters	Terrorist attacks	Data fraud or theft
2016	Involuntary migration	Extreme weather	Climate action failure	Interstate conflict	Natural catastrophes
2015	Interstate conflict	Extreme weather	Failure of national governance	State collapse or crisis	Unemployment
2014	Income disparity	Extreme weather	Unemployment	Climate action failure	Cyberattacks
2013	Income disparity	Fiscal imbalances	Greenhouse gas emissions	Water crises	Population ageing
2012	Income disparity	Fiscal imbalances	Greenhouse gas emissions	Cyberattacks	Water crises



"Cybersecurity failure" is one of the risks that worsened the most through COVID-19

enisa
European Network and Information Security Agency

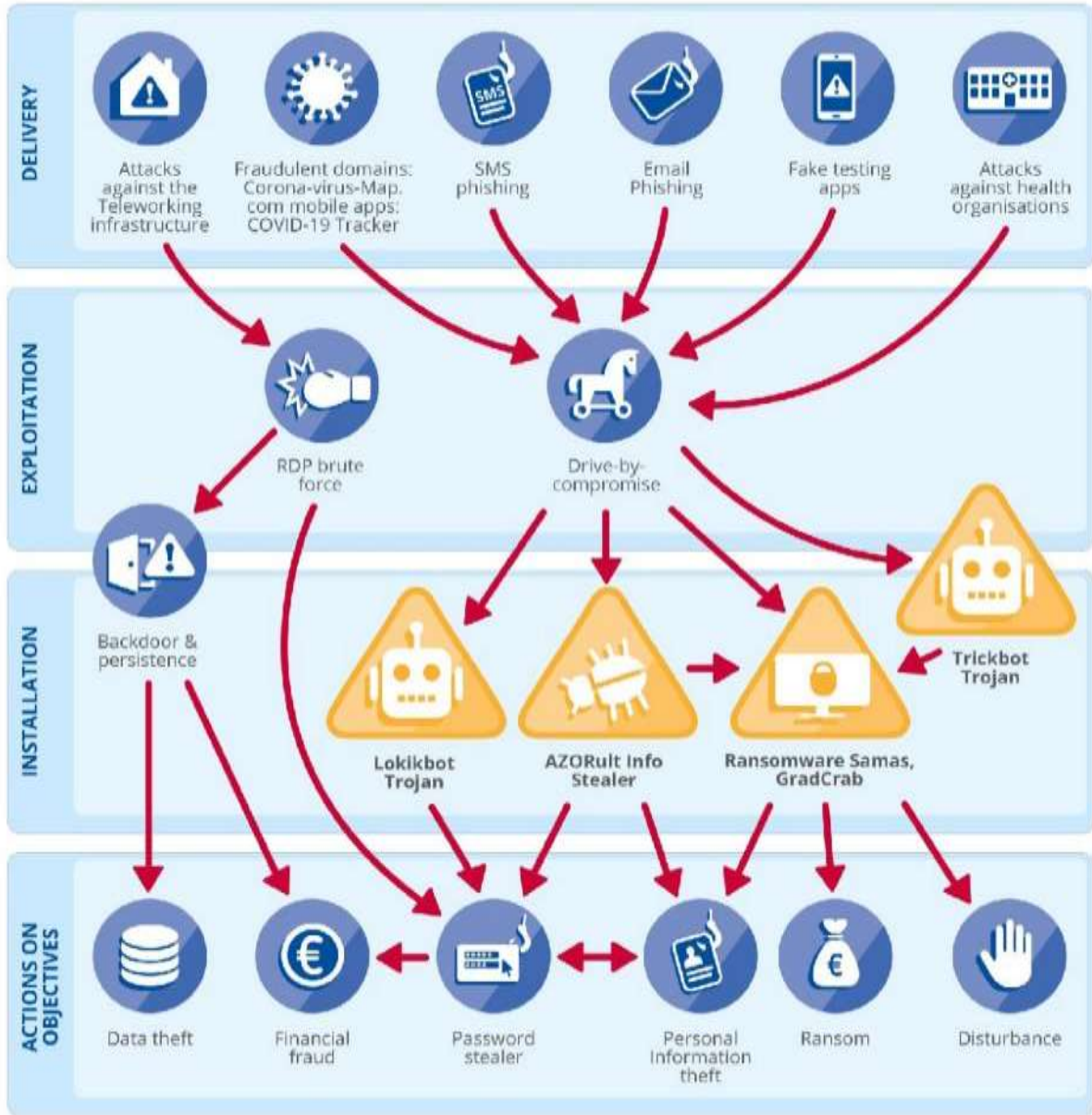
Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial 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

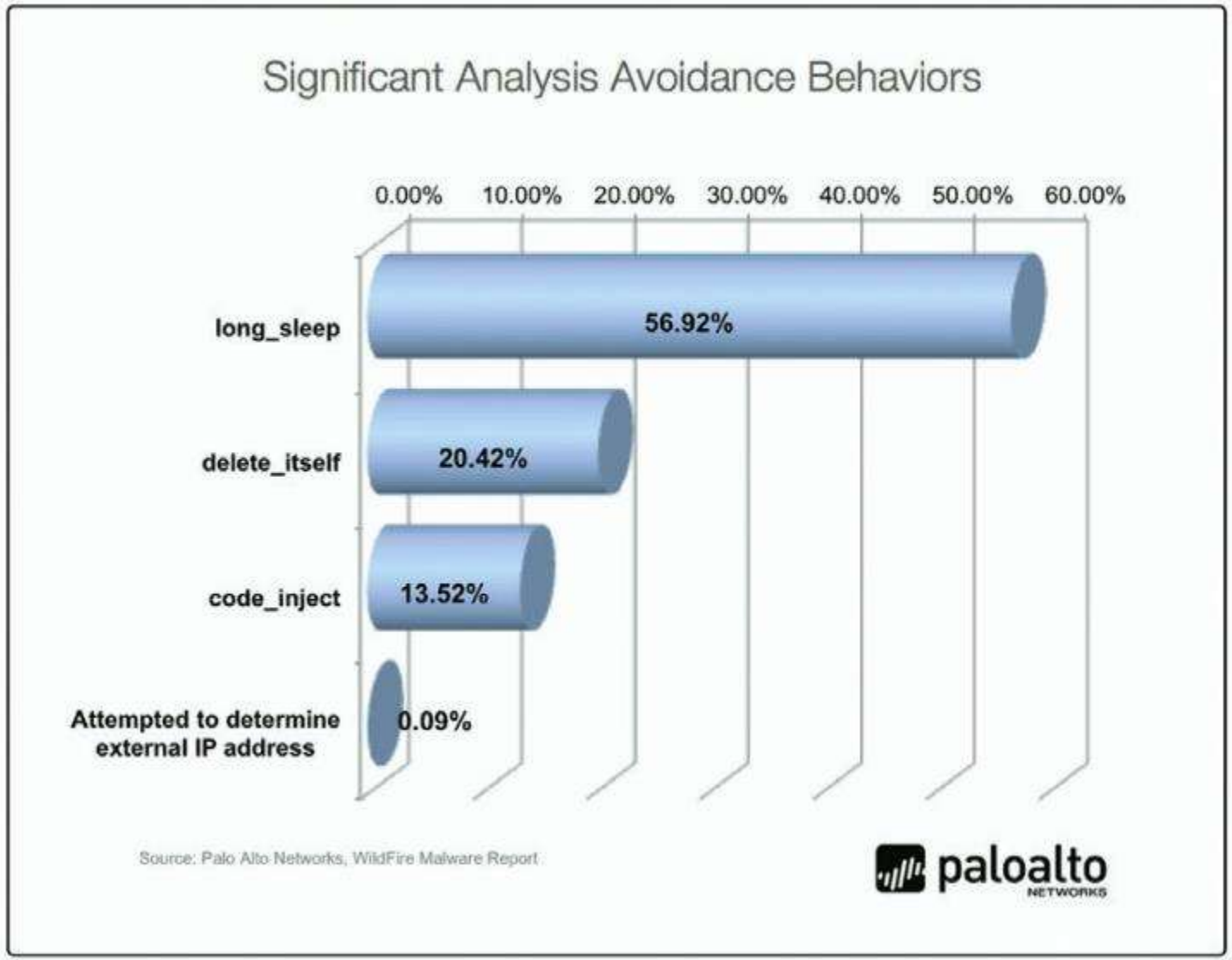
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

THREAT LANDSCAPE MAPPING

Exploitation by cybercriminals and advanced persistent threat (APT) groups of the current coronavirus (COVID-19) global pandemic.



Modern malware – behavior on the host



"hiding" or "stealth" – for how long?

May 29, 2012

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

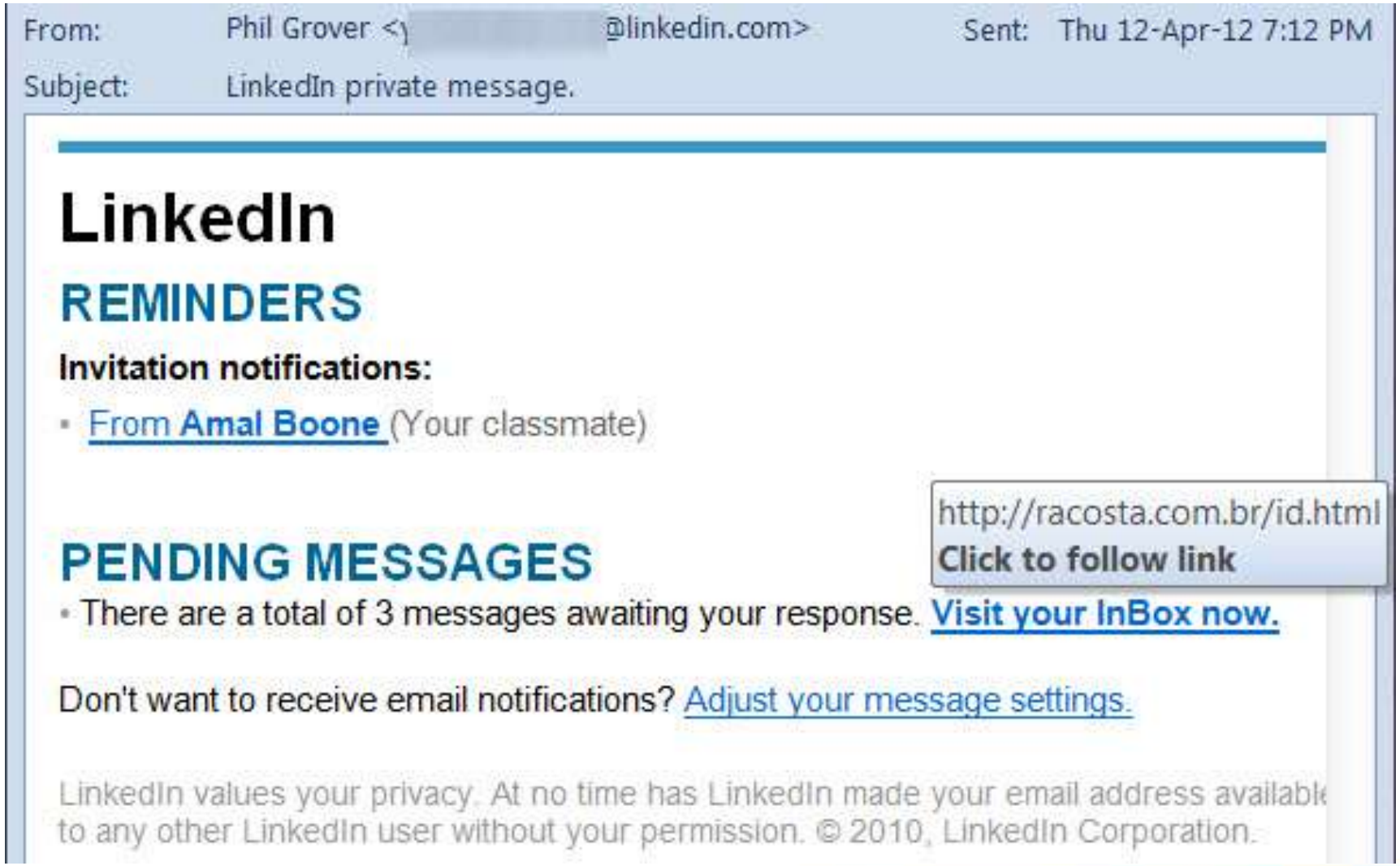
test blog posts

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

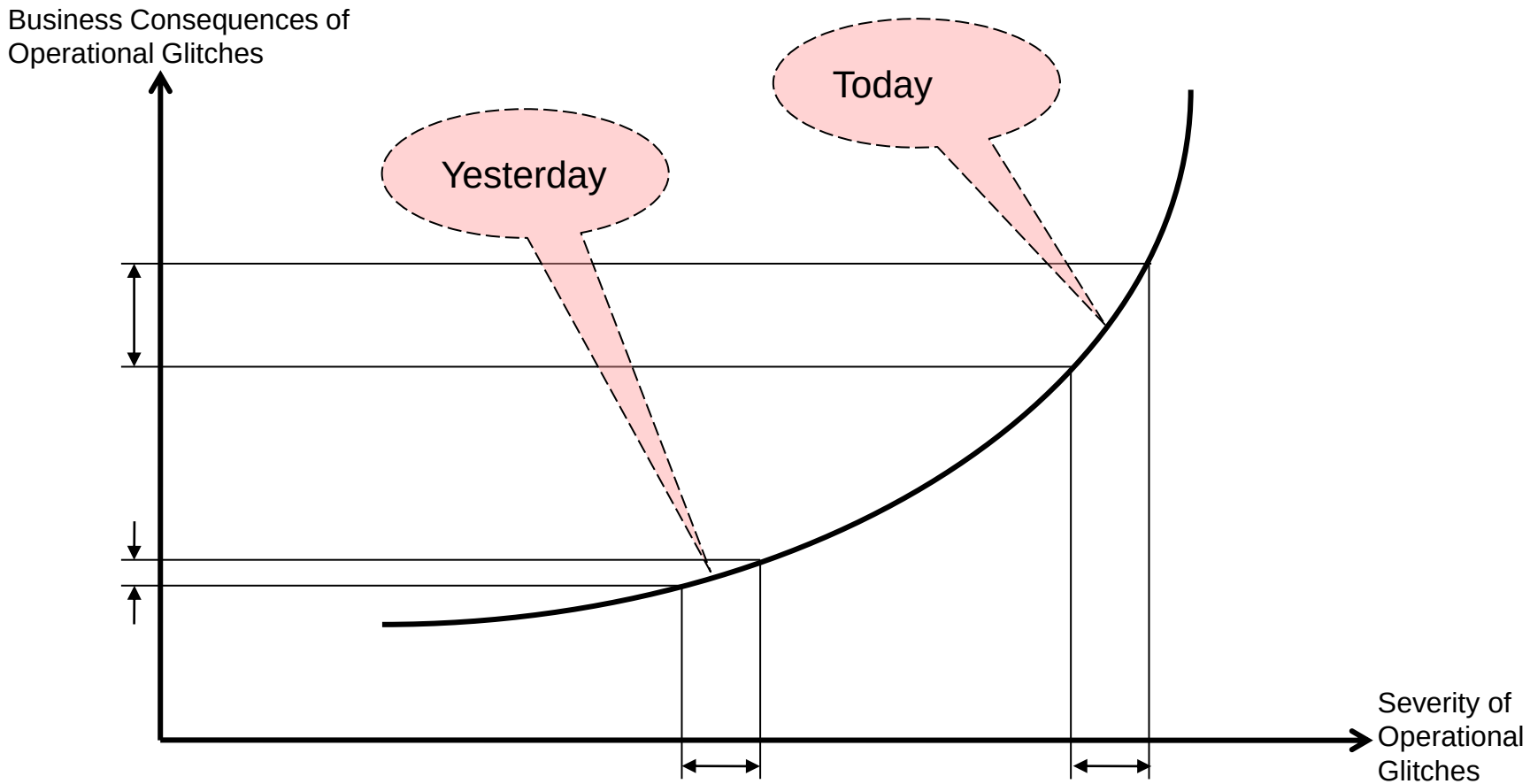
Operation "Red October"

Victims of advanced cyber-espionage network

It looks so usual …

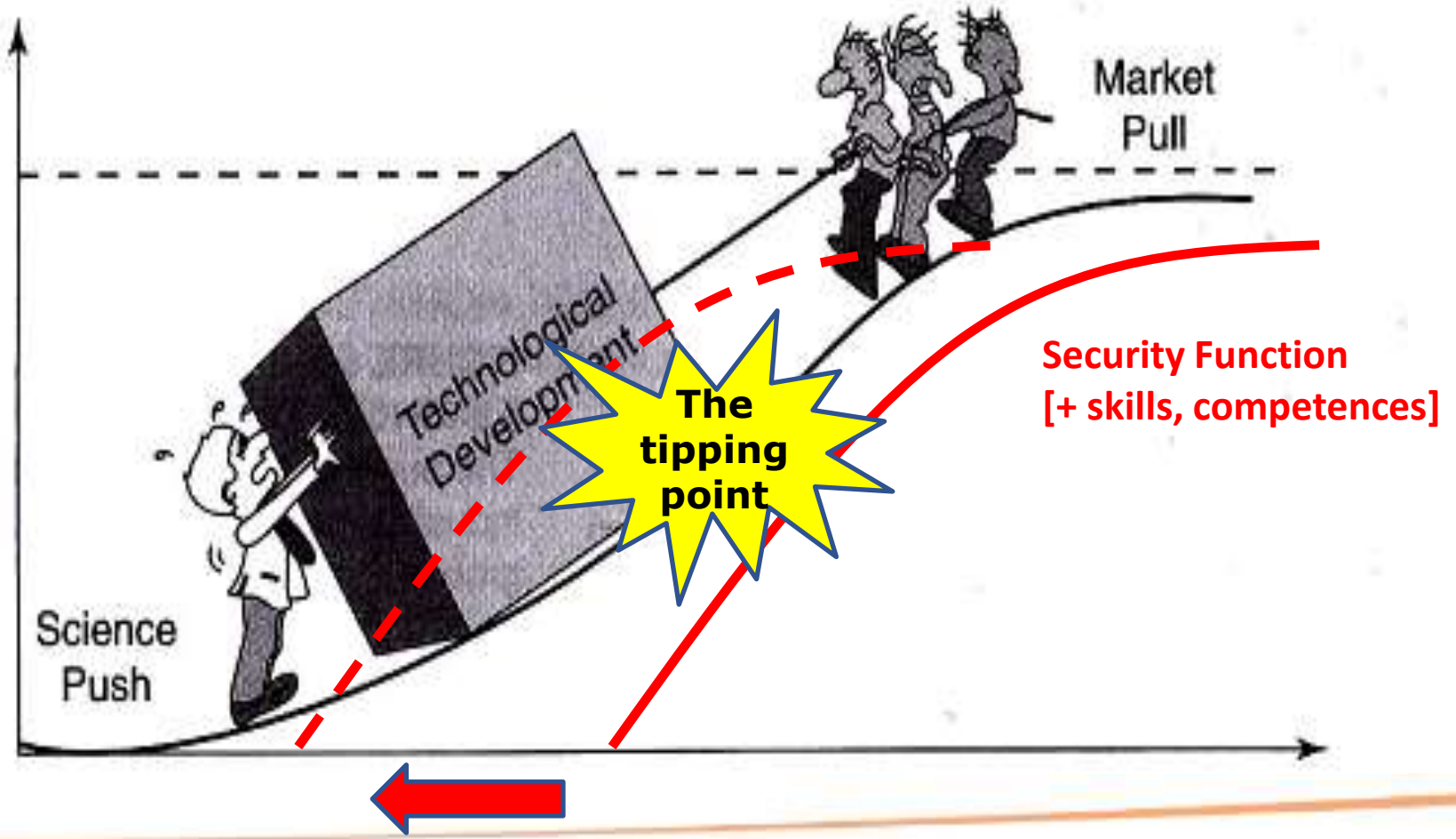


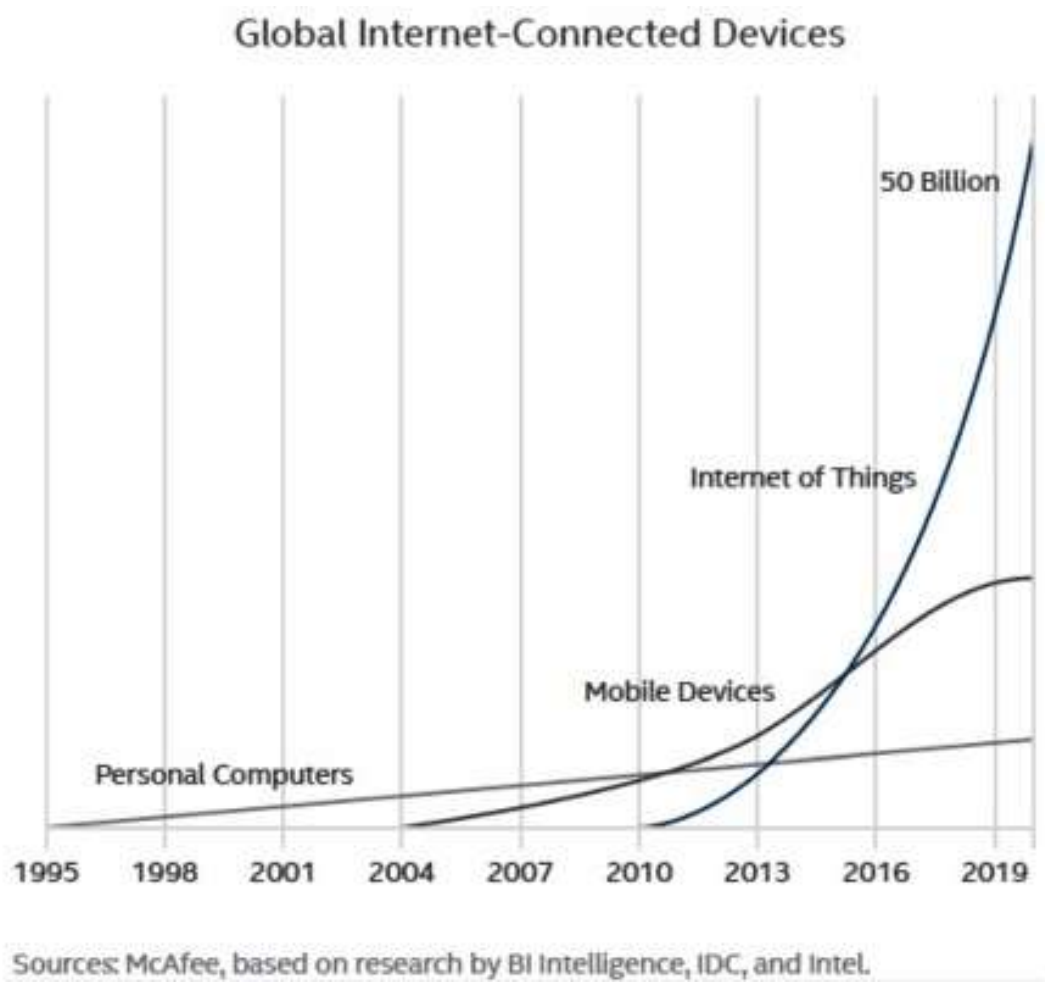
Today's Business Environment



Today's Business Environment is Much Less Forgiving

Digital society/ecosystem: Ready for the Digital Dependency?

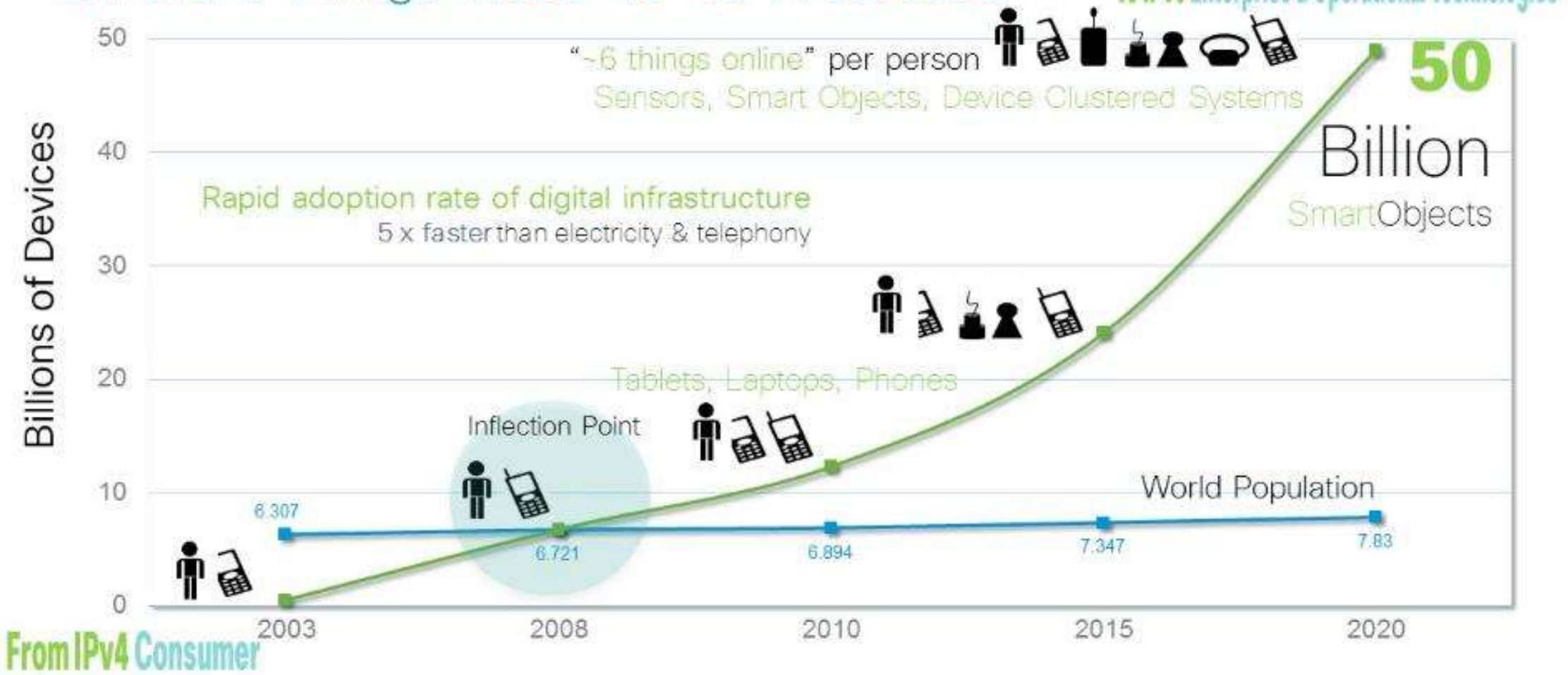



Global Internet-Connected Devices
50 Billion
Internet of Things
Mobile Devices
Personal Computers
1995
1998
2001
2004
2007
2010
2013
2016
2019
Sources: McAfee, based on research by BI Intelligence, IDC, and Intel.

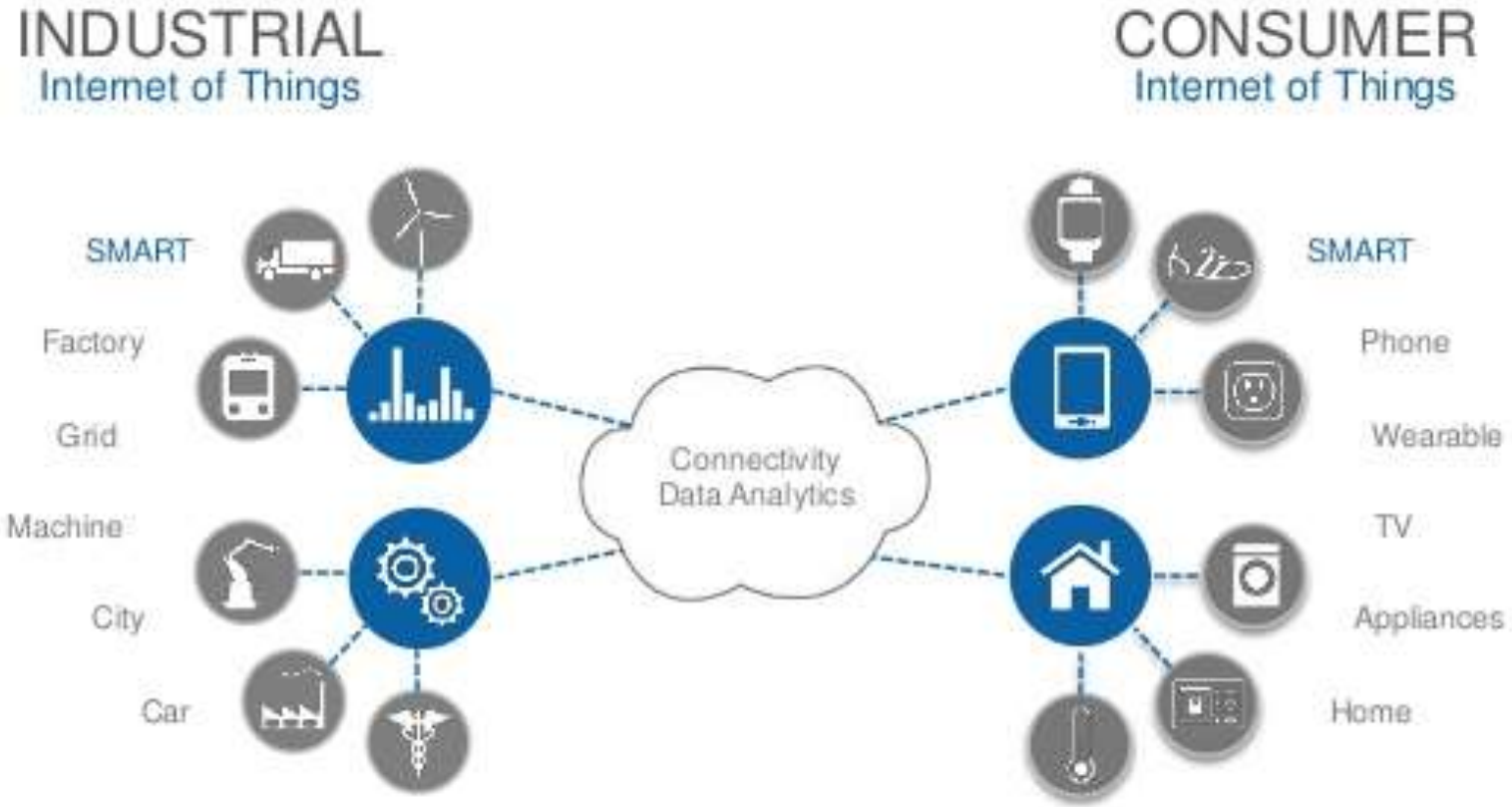

CCTV Botnet in Our Own Back Yard


HUMAN
ORGAN

Different Things Need To Be Protected



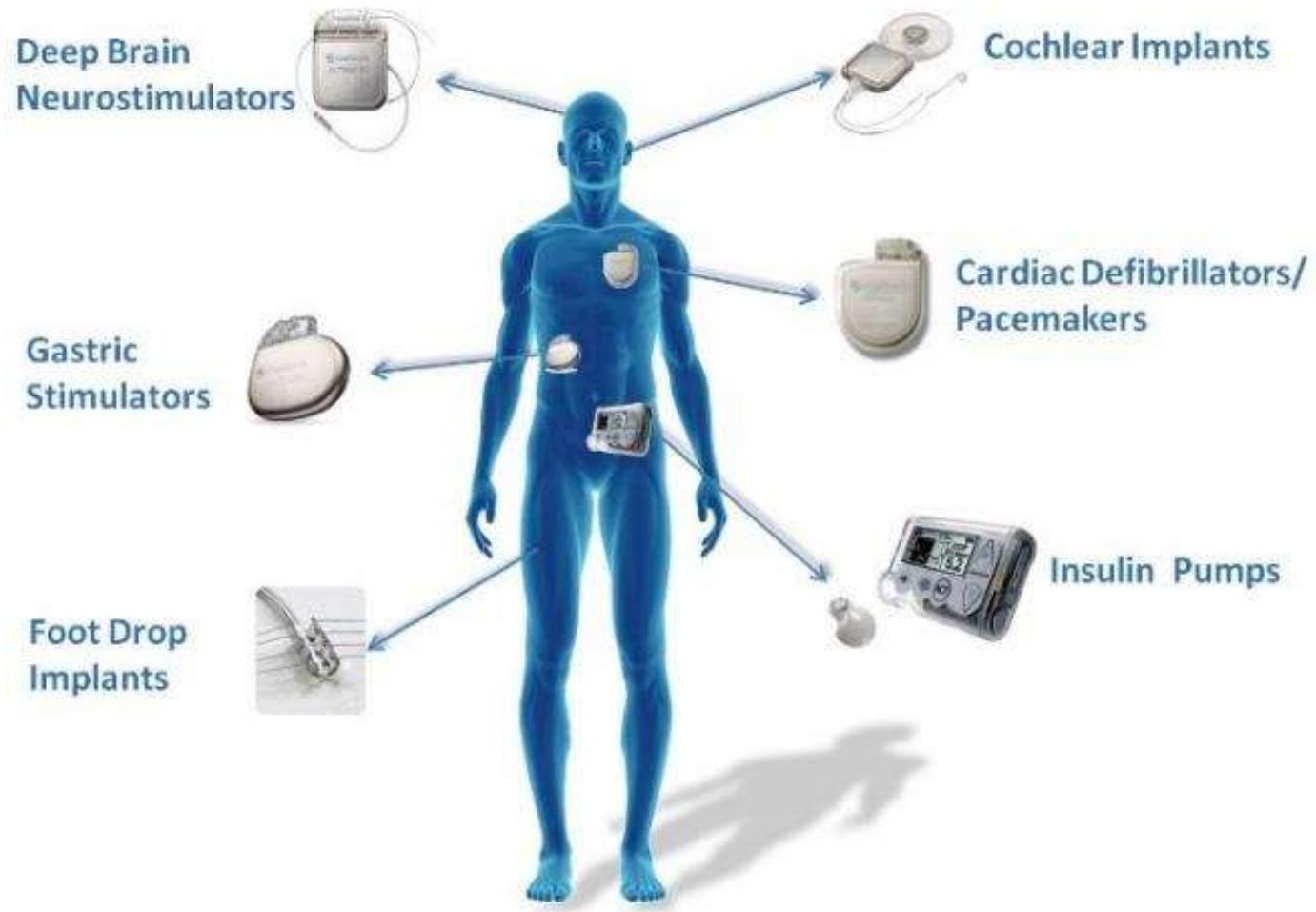
Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

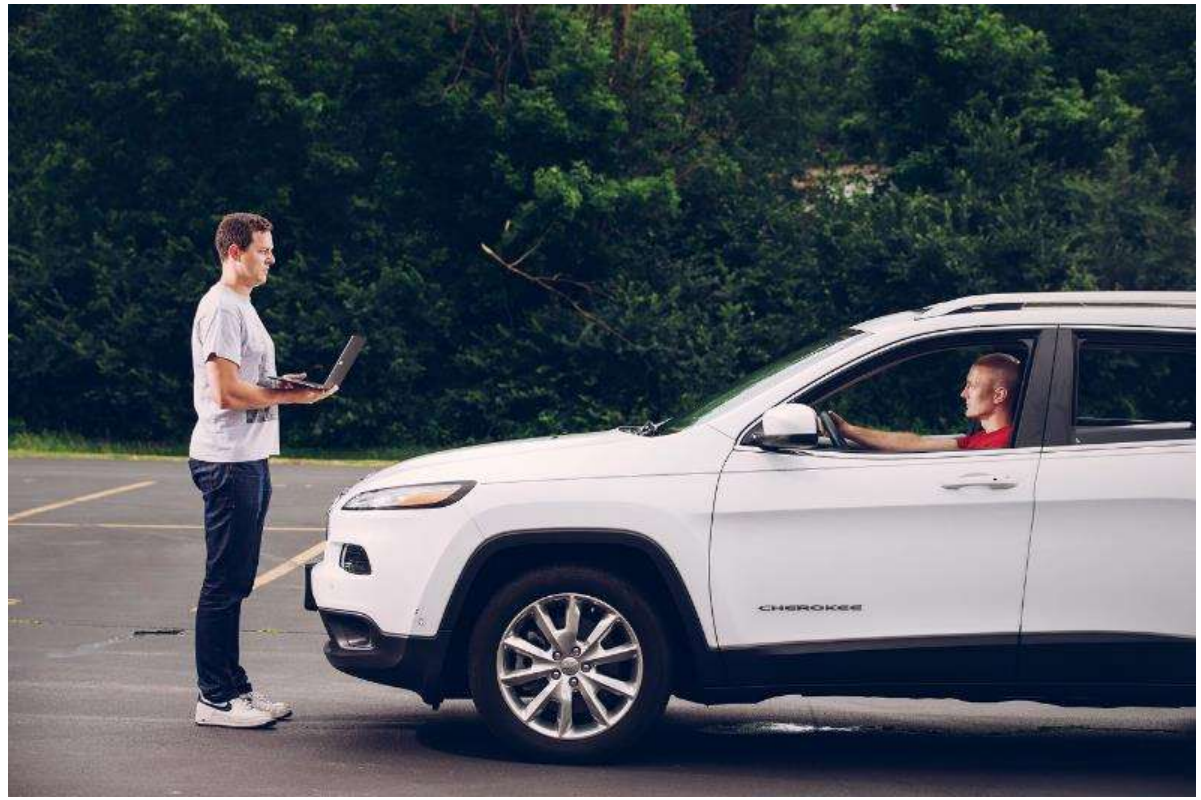


Based on Moor Insights & Strategy's report *Segmenting the Internet of Things (IoT)*

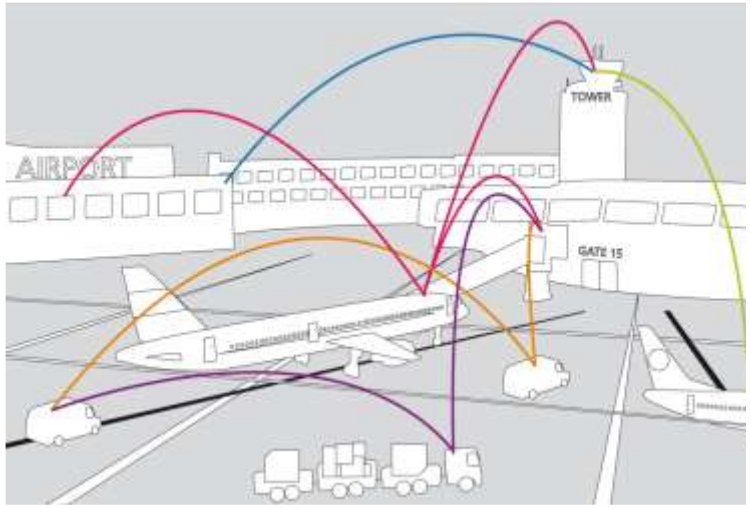
NATIONAL INSTRUMENTS

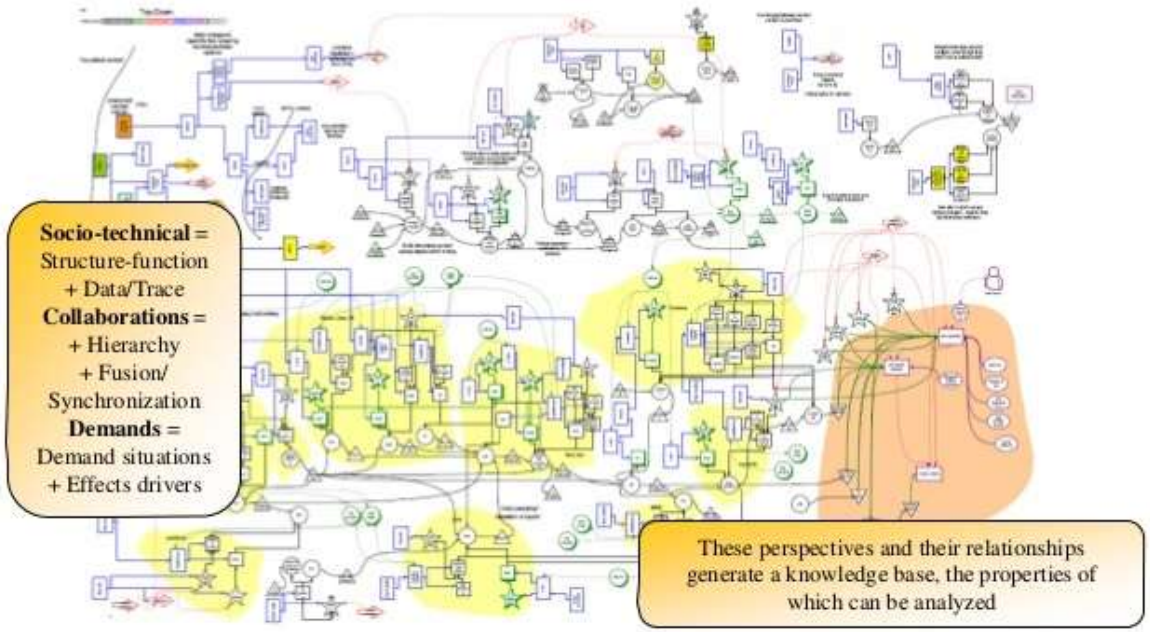
WIRELESS IMPLANTABLE MEDICAL DEVICES




CHEROKEE

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

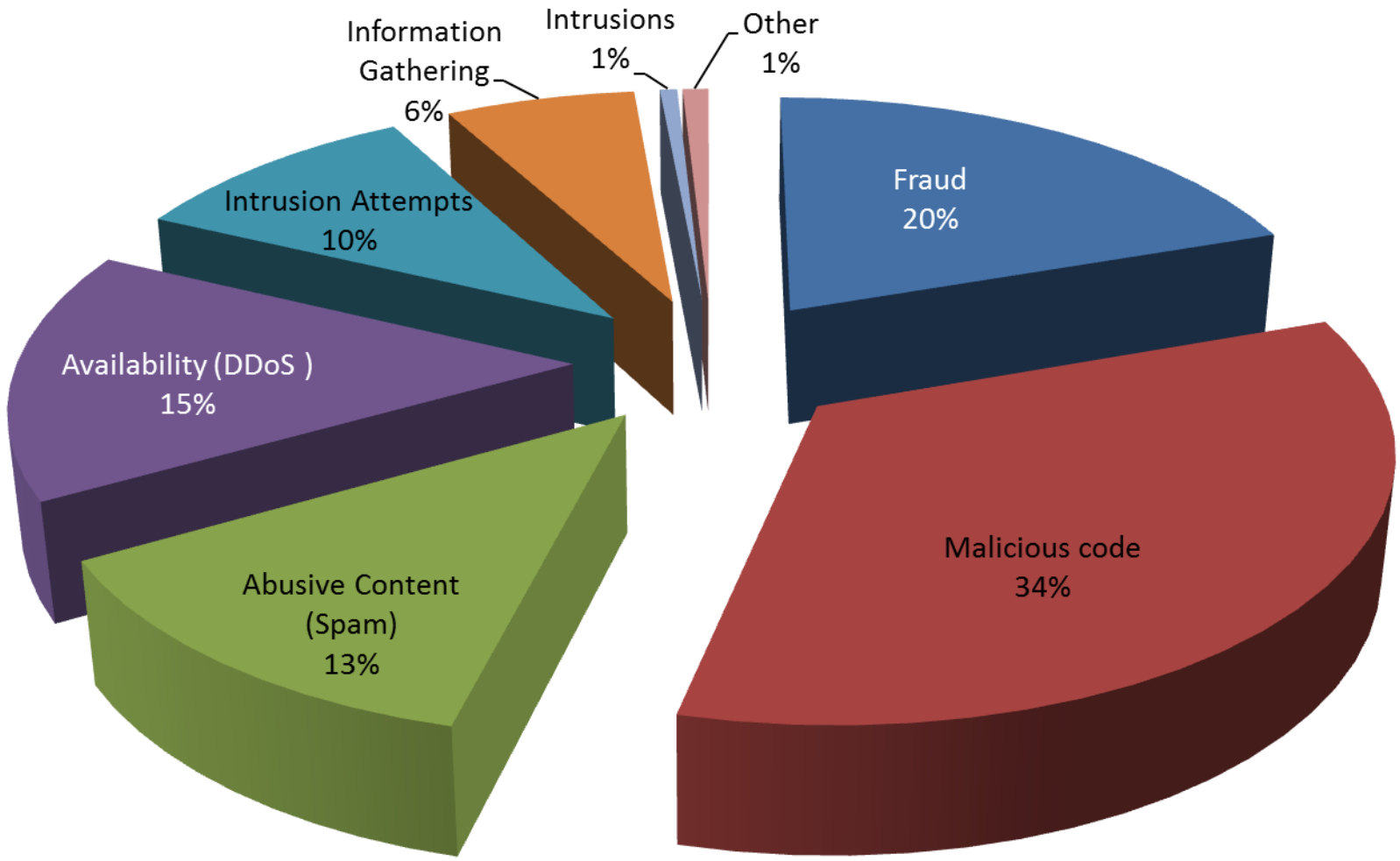




21Oct2015

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

Bulgaria under “attack”:
Type of incidents to 30th June 2020 (GOV CERT BG)



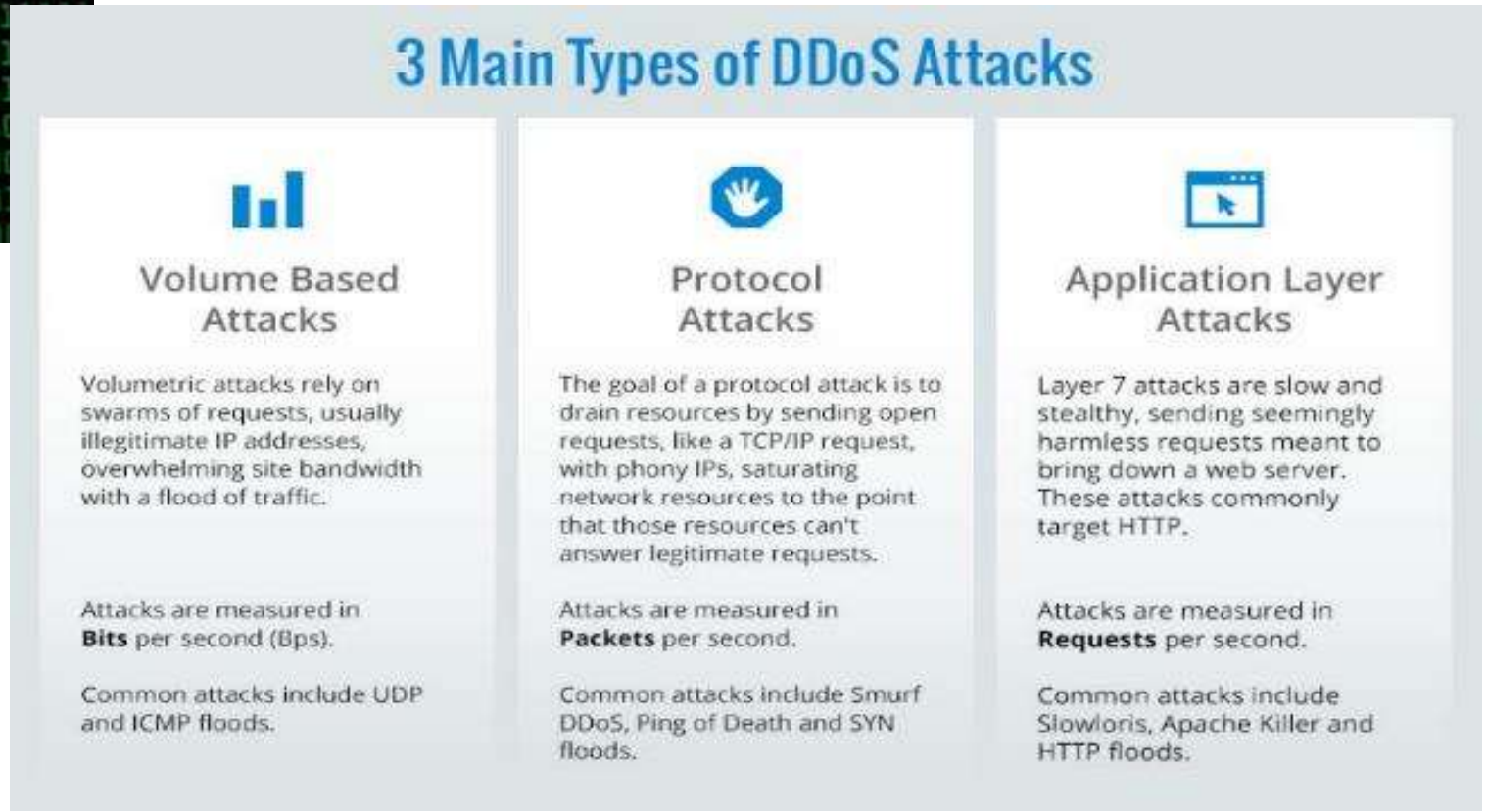
Ministry of education website defaced (XSS)

February, 2016

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/



Latest – evolving adversaries TTP (Tactics, Techniques and Procedures)

May 2017

The **WannaCry ransomware attack** was a worldwide cyberattack in May 2017 by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.[5] It propagated through EternalBlue, an exploit discovered by the United States National Security Agency (NSA) for older Windows systems. EternalBlue was stolen and leaked by a group called The Shadow Brokers at least a year prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life. These patches are imperative to an organization's cyber-security but many were not applied because of needing 24/7 operation, risking having applications that used to work break, inconvenience, or other reasons.

information monitor at a German train station displays the ransomware message CREDIT: ICHENTATEN/TWITTER

Follow

By **Chris Graham**
13 MAY 2017 • 1:20AM

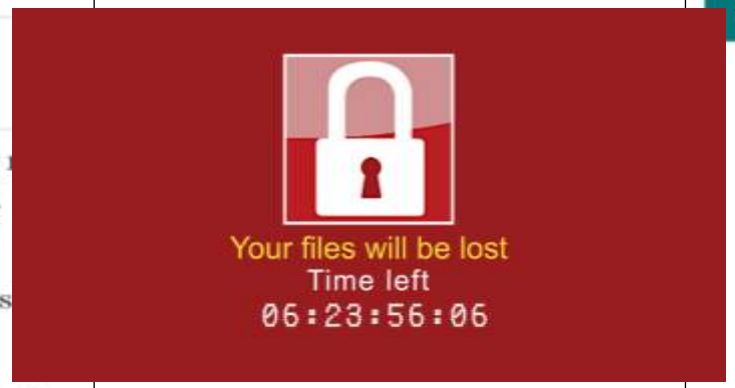
ermany's rail network was thrown into chaos on Friday when it fell victim to the cyber attack roiling the world.

ours after NHS hospitals were left crippled by the attack, Deuts hn became the hackers' latest high profile victim.

sing tools widely believed to have been developed by the US Nationa

The Telegraph

13 May 2017



A mysterious cyber gang - called Shadow Brokers- said last month it had stolen a 'cyber weapon' from the National Security Agency (NSA), America's powerful military intelligence unit.

NHS cyber attack | Organisations affected

NHS organisations across the country reported IT failures as a result of a major cyber attack. Those affected are believed to include:

ENGLAND

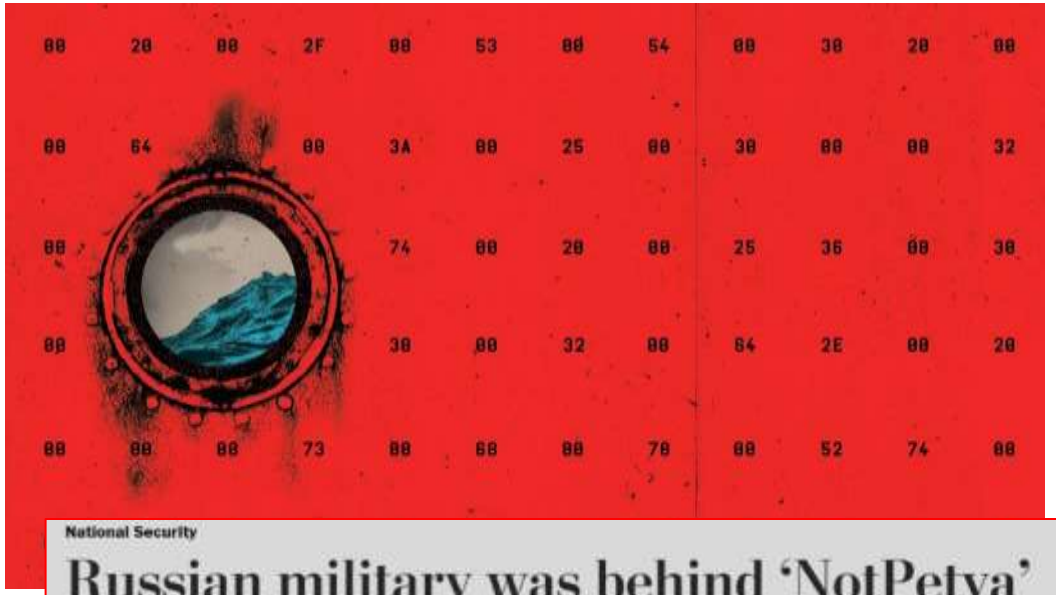
Barts Health Trust	Burton Hospitals NHS Foundation Trust
Blackpool Teaching Hospitals NHS Trust	Colchester General Hospital
Cheshire and Wirral Partnership NHS Foundation Trust	East Lancashire Hospitals NHS Trust
Derbyshire Community Health Services Trust	George Eliot Hospital NHS Trust, Warwickshire
East and North Hertfordshire NHS Trust	Nottinghamshire Healthcare NHS Trust
Hampshire Hospitals Trust	Northern Lincolnshire and Goole NHS Foundation Trust
North Cumbria University Hospitals NHS Trust	Nottinghamshire Healthcare NHS Foundation Trust
North Staffordshire Combined Healthcare	Sherwood Forest NHS Trust

Show more

The hacking tool, called 'Eternal Blue', gives unprecedented access to all computers using Microsoft Windows, the world's most popular computer operating system. It had been developed by the NSA to gain access to computers used by terrorists and enemy states.

The gang in turn 'dumped' the computer bug on an obscure website on April 14 and it is believed to have been picked up by a separate crime gang which has used it to gain remote access to computers around the world.

The hackers, who have not come forward to claim responsibility or



National Security

Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes

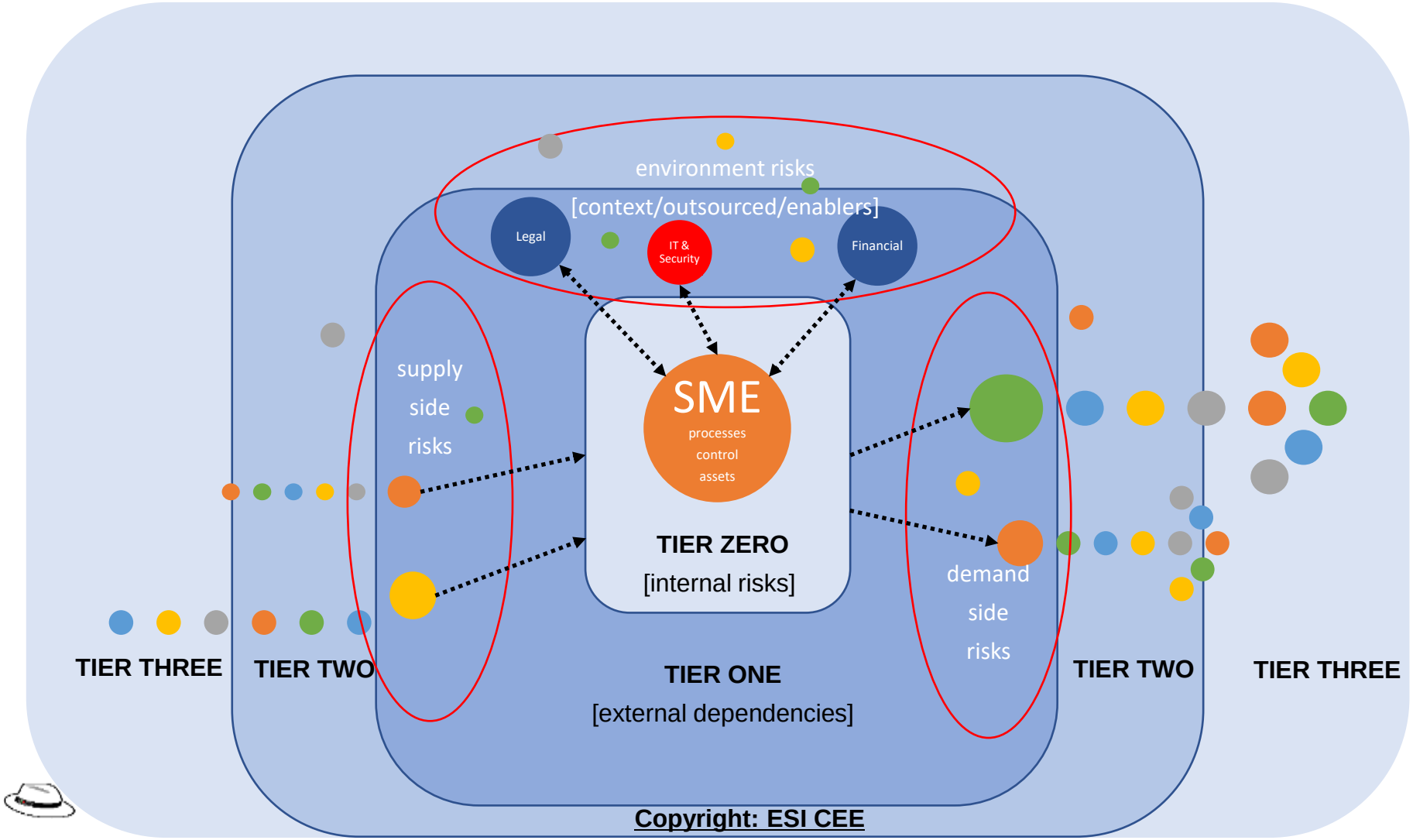
June 27, 2017

NotPetya

NotPetya is malware that was first seen in a worldwide attack starting on June 27, 2017. The main purpose of the malware appeared to be to effectively destroy data and disk structures on compromised systems. Though NotPetya presents itself as a form of ransomware, it appears likely that the attackers never intended to make the encrypted data recoverable. As such, NotPetya may be more appropriately thought of as a form of wiper malware. NotPetya contains worm-like features to spread itself across a computer network using the SMBv1 exploits EternalBlue and EternalRomance.[1][1][2][3]

Solution: Implementation schemes & **engagement**
Supply/value chains as **Blockchains**

Example > NotPetya spread over Supply Chains and affected other countries !!!



1) **TRUST** = **Need standards** applicable and affordable for ALL players **(SMEs!!)**

but also

2) Provide a **natural engagement** and propagation mechanism

(shared risk requires shared responsibility)

3 October 2020 (covid-19 pandemic)

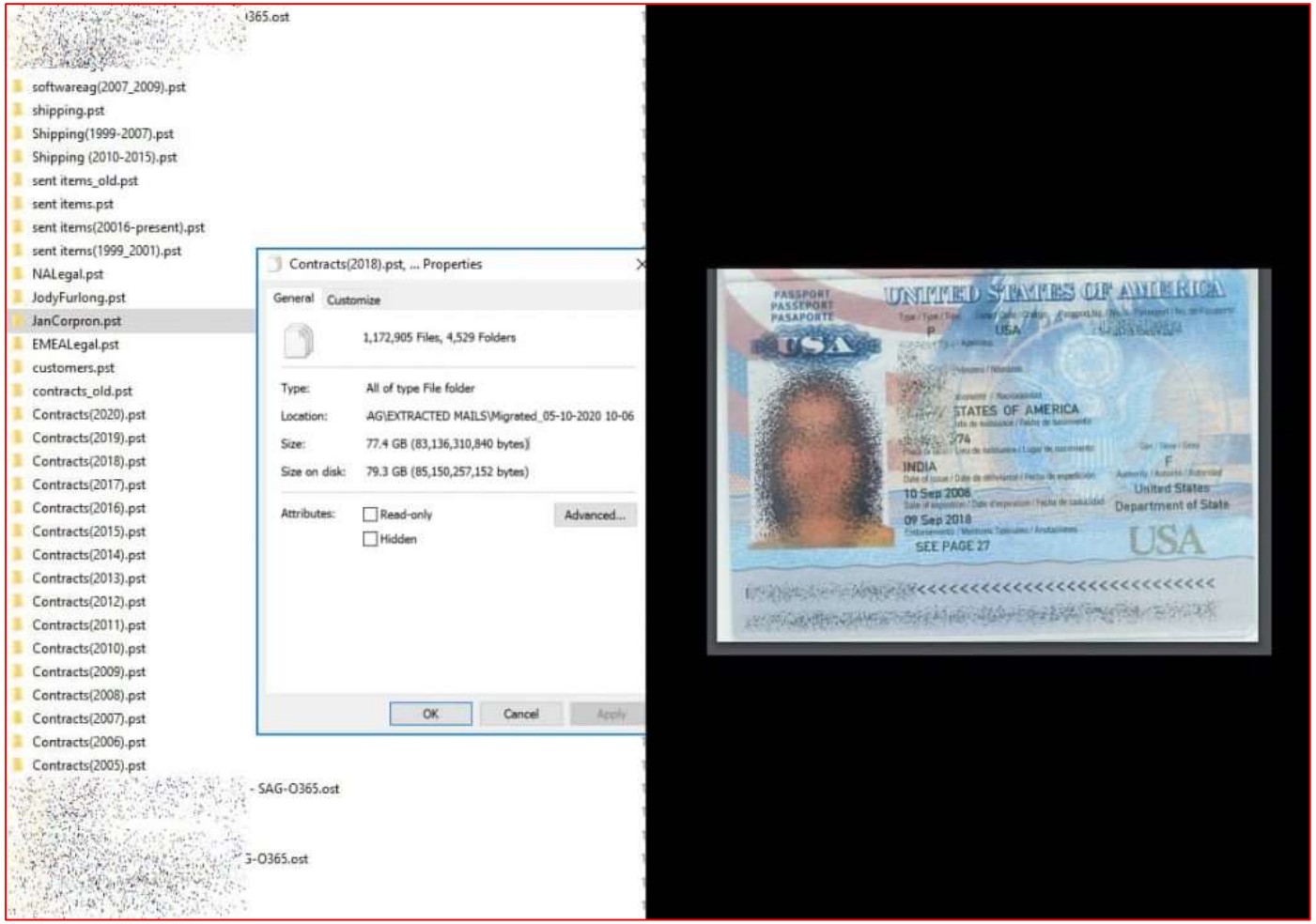
Clop ransomware hits Software AG, demands $20 million+ ransom

Software AG, a German tech giant had its helpdesk and internal communication systems disrupted after the Clop ransomware attack.

Over the weekend, Germany's second-largest tech firm Software AG suffered a ransomware attack. The company had to shut down many of its internal systems. Allegedly, the attackers took company data and demanded over $20 million (€17 million) in ransom.

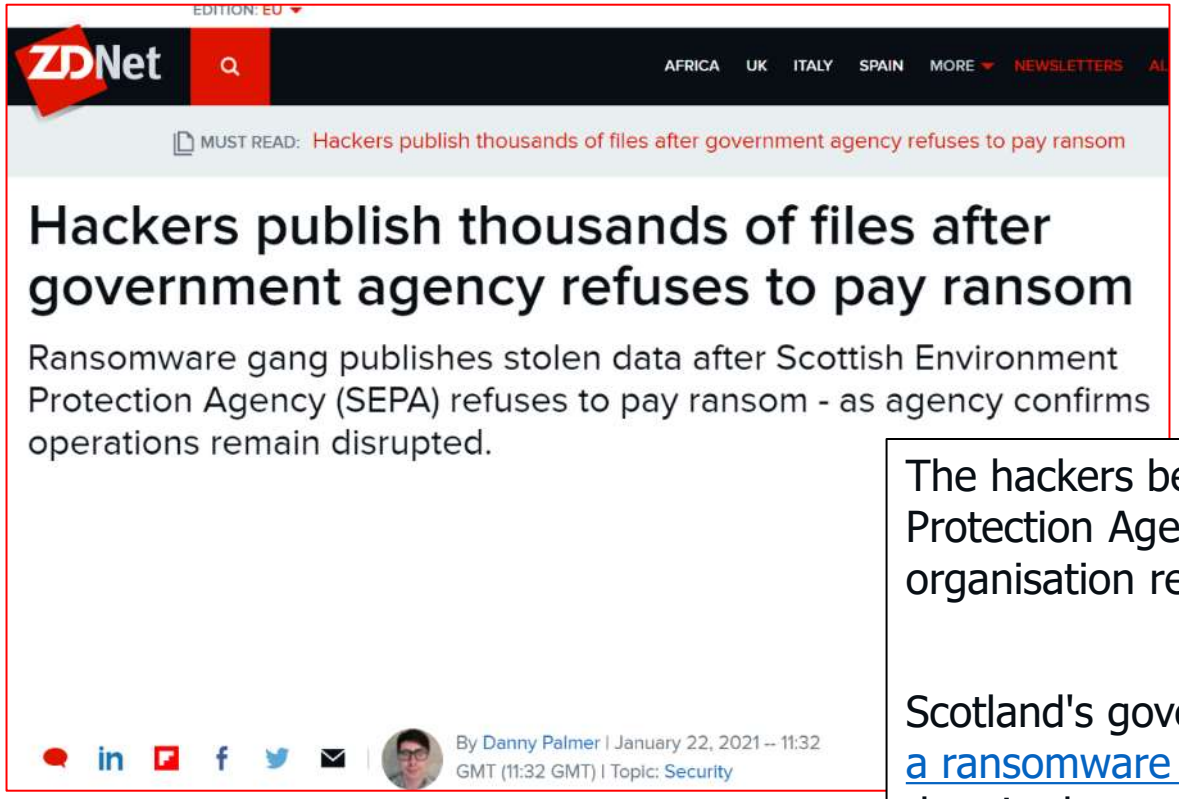
According to the company, its cloud offerings weren't affected; however, its internal communications and helpdesk went offline and haven't recovered fully as yet.

```
 HELLO DEAR SOFTWARE AG
YOUR NETWORK IS ENCRYPTED!
ALL YOUR FILES ARE ENCRYPTED!
Also a lot of sensitive data has been downloaded from your network.
For example:

\\[redacted]

This is a small part, about 10%.
If you refuse to cooperate, all data will be published for free download on our portal:
http://[redacted].onion/ (use TOR browser)
mirror http://[redacted].onion.dog/
To get access to your files back, contact us by email:
unlock@goldenbay.su
or
unlock@graylegion.su
AND
[redacted]
or write to the chat at:
[redacted](use TOR browser)

!!! DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM !!!
CIOp-_^
```



https://www.hackread.com/clop-ransomware-software-ag-20-million-ransom/

22 January 2021



EDITION: EU

ZDNet

AFRICA UK ITALY SPAIN MORE NEWSLETTERS

MUST READ: Hackers publish thousands of files after government agency refuses to pay ransom

Hackers publish thousands of files after government agency refuses to pay ransom

Ransomware gang publishes stolen data after Scottish Environment Protection Agency (SEPA) refuses to pay ransom - as agency confirms operations remain disrupted.

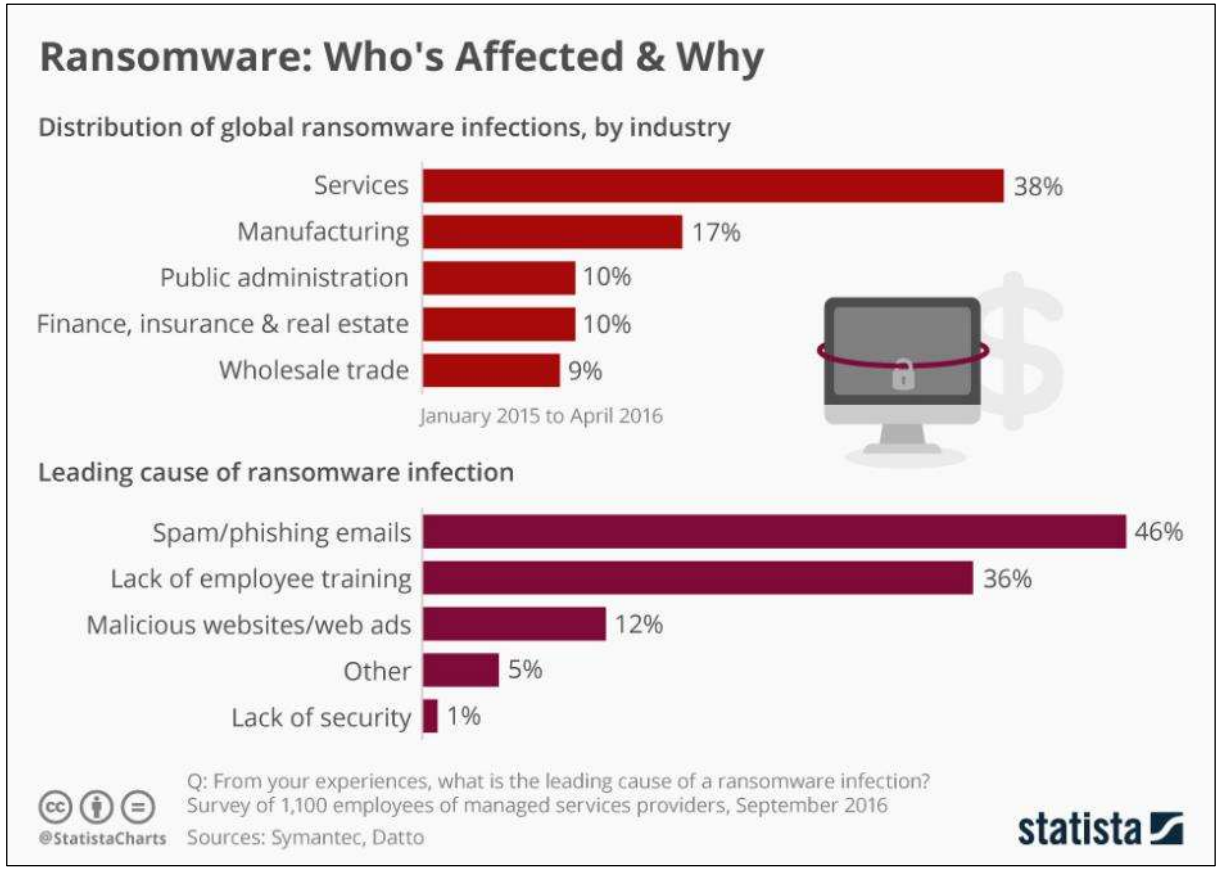
By Danny Palmer | January 22, 2021 -- 11:32 GMT (11:32 GMT) | Topic: Security

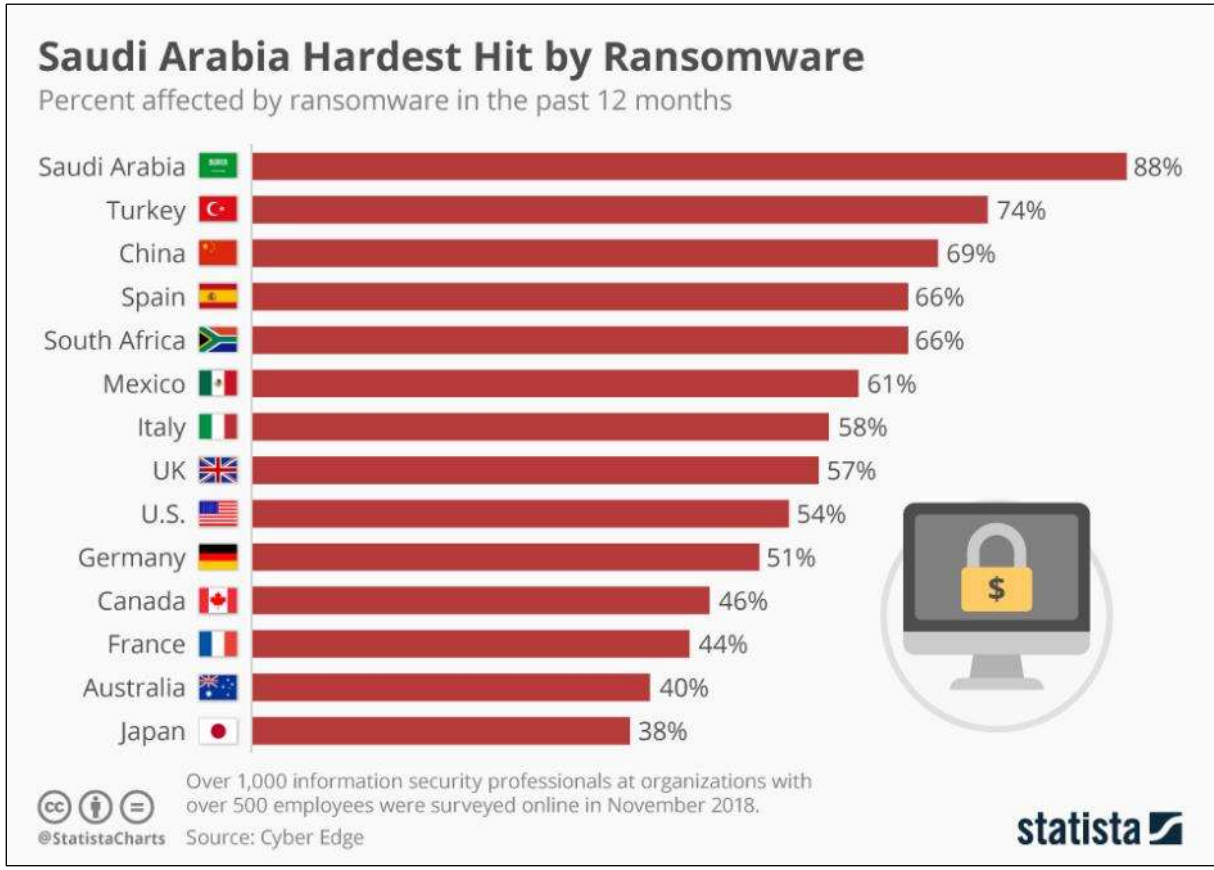
The hackers behind the ransomware attack on the Scottish Environment Protection Agency (SEPA) have published thousands of stolen files after the organisation refused to pay the ransom.

Scotland's government regulator for protecting the environment was hit with a ransomware attack on Christmas Eve, with cybercriminals stealing 1.2 GB of data in the process. Almost a month on from the attack, SEPA services remain disrupted – but despite this, the agency has made it clear it won't engage with those behind the attack.

SEPA hasn't confirmed what form of ransomware it has fallen victim to, but the Conti ransomware gang claimed responsibility for the attack.

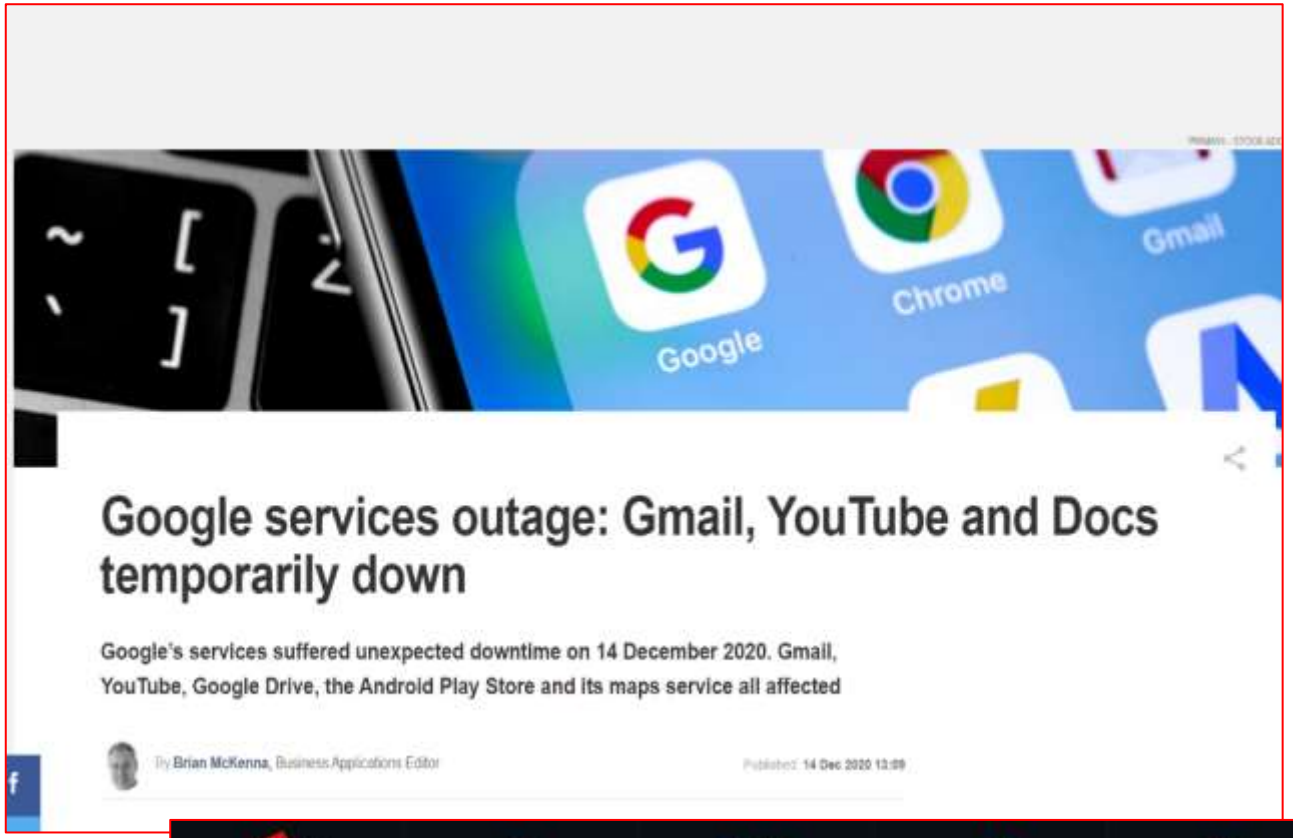
As a **result of the non-payment**, Conti has published all of the stolen data on its website, posting over 4,000 documents and databases related to contracts, commercial services and strategy. The latest update from SEPA confirms that at least 4,000 files have been stolen and published.





https://www.statista.com/chart/9378/distribution-of-global-ransomware-infections-and-leading-causes/

https://www.computerweekly.com/news/252493590/Google-services-outage-Gmail-YouTube-and-Docs-down



14 December 2020

https://www.zdnet.com/article/google-heres-what-caused-our-big-global-outage/

The company reveals that the crux of the issue, now tagged as **'Google Cloud Infrastructure Components incident 20013',** was reduced capacity for Google's central identity-management system, blocking any service that required users to log in.

However, the root cause was an issue in Google's automated storage quota management system, which in turn reduced the capacity of the authentication system.

The two main services impacted were Google Cloud Platform, which means Cloud Console, Cloud Storage, BigQuery, and the Google Kubernetes Engine. All users would have experienced an authentication error during the 50-minute outage.

Google Workspace, formerly G Suite, services affected included Gmail, Calendar, Meet, Docs and Drive. Again, all users globally were experiencing authentication errors.

It's the **third worldwide outage at a public cloud provider in the past two months**. Google's service disruption wasn't as long as the **five-hour Amazon Web Services outage last month, but the broad impact of both incidents affected each company's technical support and their engineers' ability to communicate with external customers.**

20 November 2020 (covid-19 panemic)

A reporter hacked an EU Council meeting

Using login information shared on one of the defense ministers' Twitter accounts, the Dutch 31-year-old reporter gatecrashed their meeting on Friday, creating a moment of comic relief — combined with a security alert — at a meeting where a classified document on threats facing the EU was on the agenda.

In Friday's incident, a member of Dutch Defense Minister Ank Bijleveld's staff tweeted a picture containing the **web address** of the meeting. The URL **displayed the meeting ID and five of the six digits** needed to access the meeting.

ZDNet | SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

MUST READ: US, China or Europe? Here's who is really winning the global race for AI

Third malware strain discovered in SolarWinds supply chain attack

CrowdStrike, one of the two security firms formally investigating the hack, sheds some light on how hackers compromised the SolarWinds Orion app build process.

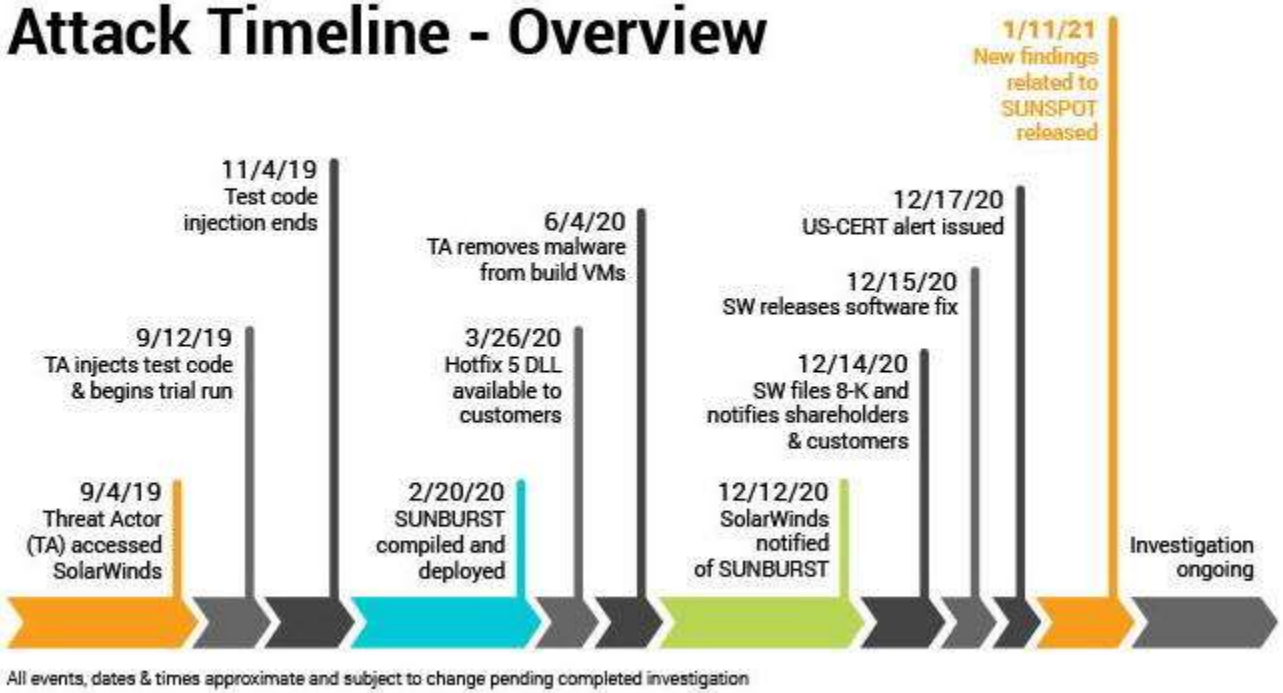
17 December 2020

[Third malware strain discovered in SolarWinds supply chain attack | ZDNet]

CODE OVERLAP WITH TURLA MALWARE

On top of this, security firm Kaspersky also published its own findings earlier in the day in a separate report.

Kaspersky, which was not part of the formal investigation of the SolarWinds attack but still analyzed the malware, said that it looked into the Sunburst malware source code and found code overlaps between Sunburst and Kazuar, a strain of malware linked to the Turla group, Russia's most sophisticated state-sponsored cyber-espionage outfit.



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

2011

THE WALL STREET JOURNAL.

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

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

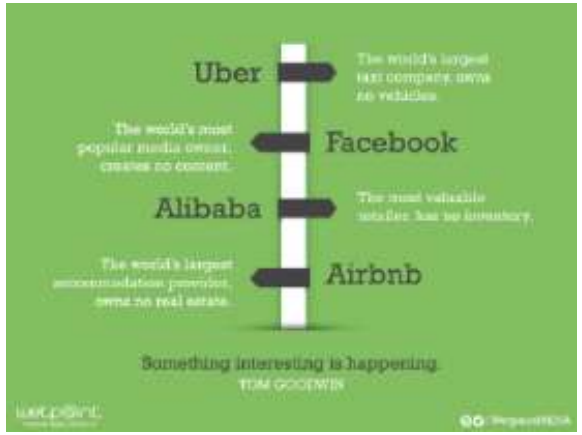
Software Is Eating the World

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...



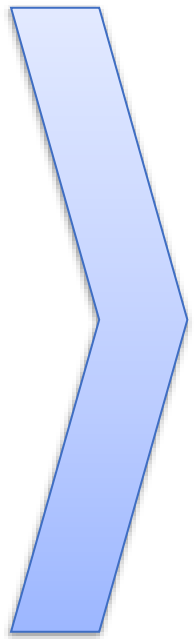
… distributed systems — encompassing cloud and SaaS; A.I., machine learning, deep learning; and quantum computing — to the role of hardware; future interfaces; and data, big and small.

… 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"? Focus on Resilient Society

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

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+ %

Digital (internet) society:

If we've lost many battles,
could we still win the Cyber War?

The Cyber/Hybrid 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

PCWorld

Work. Life. Productivity.

NEWS | REVIEWS | HOW-TO | VIDEO | BUSINESS | LAPTOPS | TABLETS | PHONES | HARD

Antivirus | Privacy | Encryption

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.

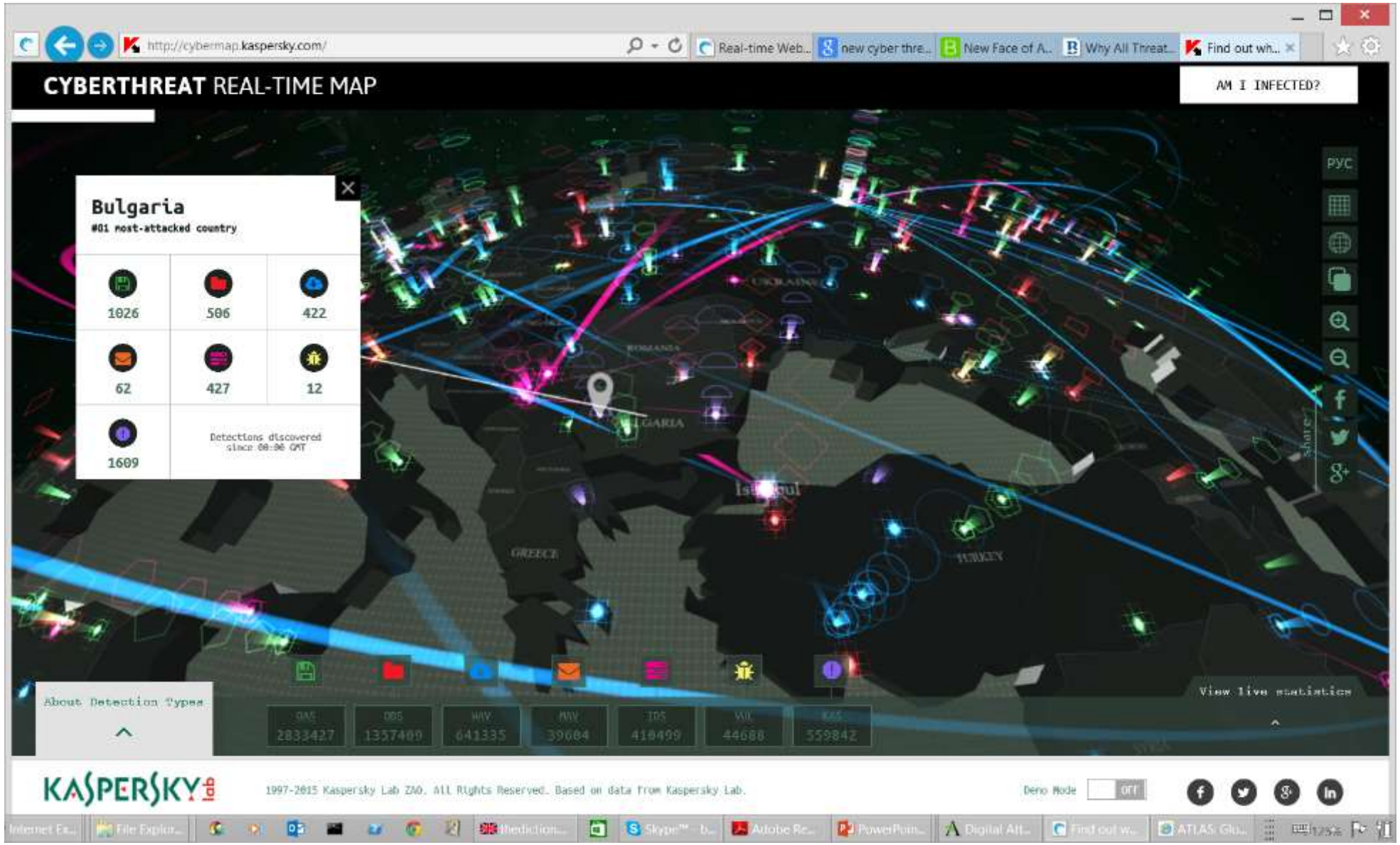
The hackers accessed SPE's Culver City, California network in late 2014 by sending spear phishing emails to Sony employees in Russia, India and other parts of Asia, U.S. security intelligence firm Taia Global said Wednesday in a report.

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

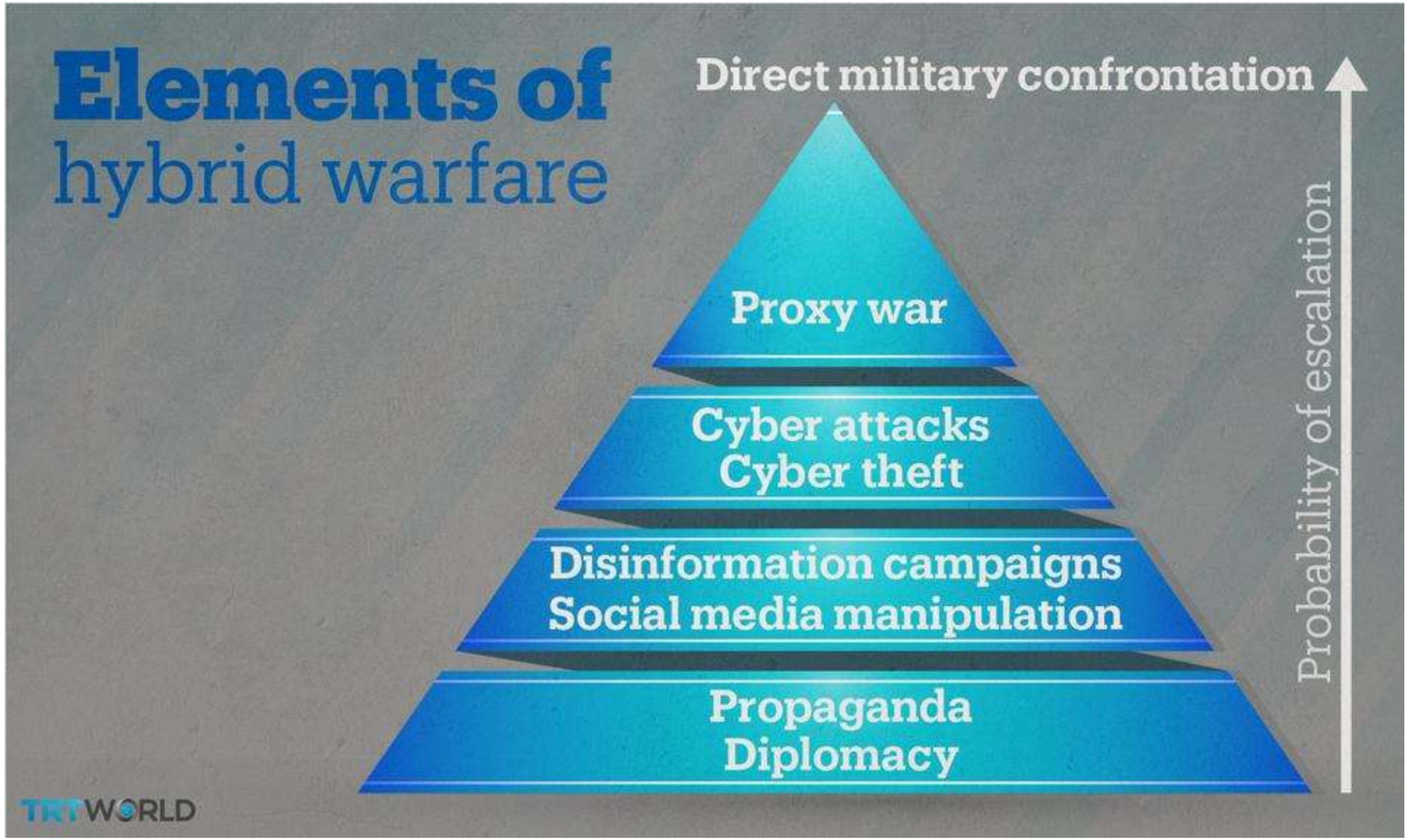
The U.S. government blamed the North Korean government for the attack, with bot officials saying they're confident about the attribution. Some security firms and exp including Taia Global, which based on a linguistic analysis of the English statemen Guardians of Peace members following the attack concluded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

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


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
416499
44688
559842
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?


Elements of
hybrid warfare
Direct military confrontation
Probability of escalation
Proxy war
Cyber attacks
Cyber theft
Disinformation campaigns
Social media manipulation
Propaganda
Diplomacy
TRT WORLD

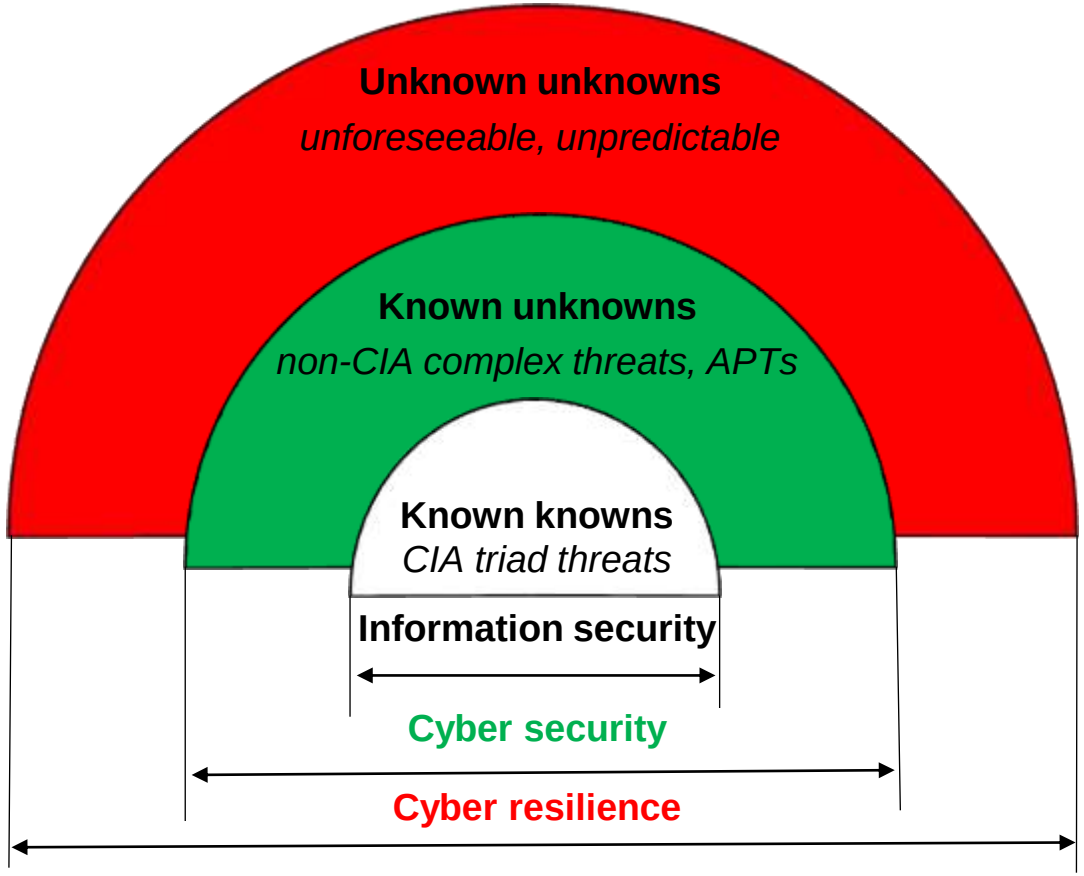
Awareness test:

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" for the "unknown unknowns"

Republic of Bulgaria

Council of Ministers

National Cyber Security Strategy
Cyber Resilient Bulgaria 2020

www.cyberBG.eu

Adopted on July 13, 2016

+ Cybersecurity Law (Act) – November, 2018
+ NATO/EU engagements
+ R&D and industry cooperation


Република България

Национална стратегия за киберсигурност

„Киберустойчива България 2020"

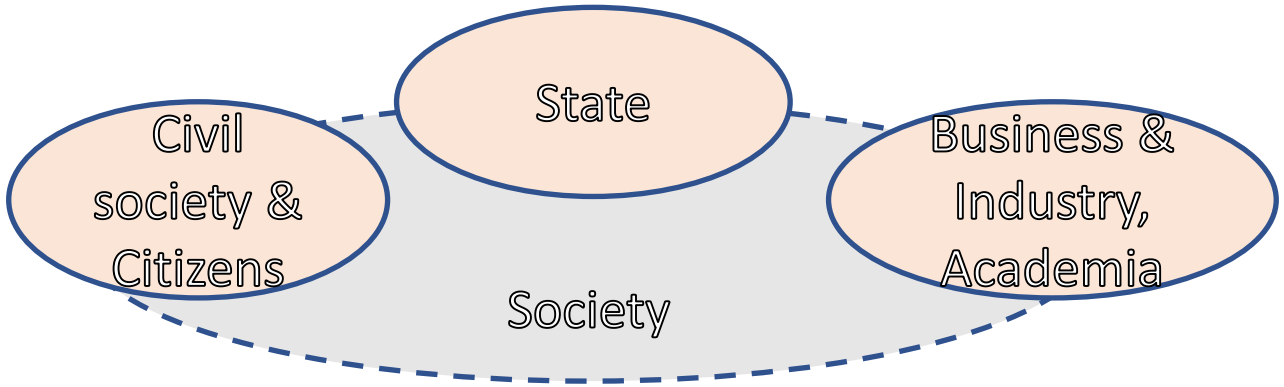
Министерски съвет

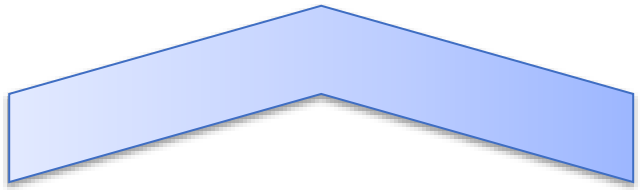
София, 2016

www.cyberbg.eu

National Cyber Security & Resilience: A multi stakeholder engagement

www.cyberBG.eu





National strategies
USA, UK, Netherlands , Austria, Germany, Finland, …

Bulgarian context:
How to protect against the unknown?

- 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 organizations
- Traditional tools, techniques, and methods may not work in this environment
- Existing organizational structures and governance model may not be agile enough to adapt

Cyber Picture = Situational awareness

Cybersecurity and resilience: Cyber Domain (Digitized Ecosystem) and Standardization

Digitized Europe fundamentals:

- DSM (Digital Single Market) – strategies, programs
- GDPR (General Data Protection Regulation) – May 2018
- NISD (Security of Network and Information Systems Directive) – May 2018
- EU Cyber Act (Package) – ENISA 2.0 Regulation + Cybersecurity Certification – June 2019
- EU Cybersecurity Strategy + NIS-d Directive (16 Dec 2020) - TBC
- others (like PSD2 for banks/payments)

All cybersecurity aspects are covered (no significant gaps), BUT:

- **too many standards**, and many are not actionable or particularly useful (entry barrier for SMEs)
- **need to converge** toward useful, interoperable sets of standards
- if **not freely available on-line**, constantly evolving, and well-versioned – low practical value and represent cybersecurity impediments
- need broad industry & society, public-private support and adoption **(multi-stakeholder holistic approach)**

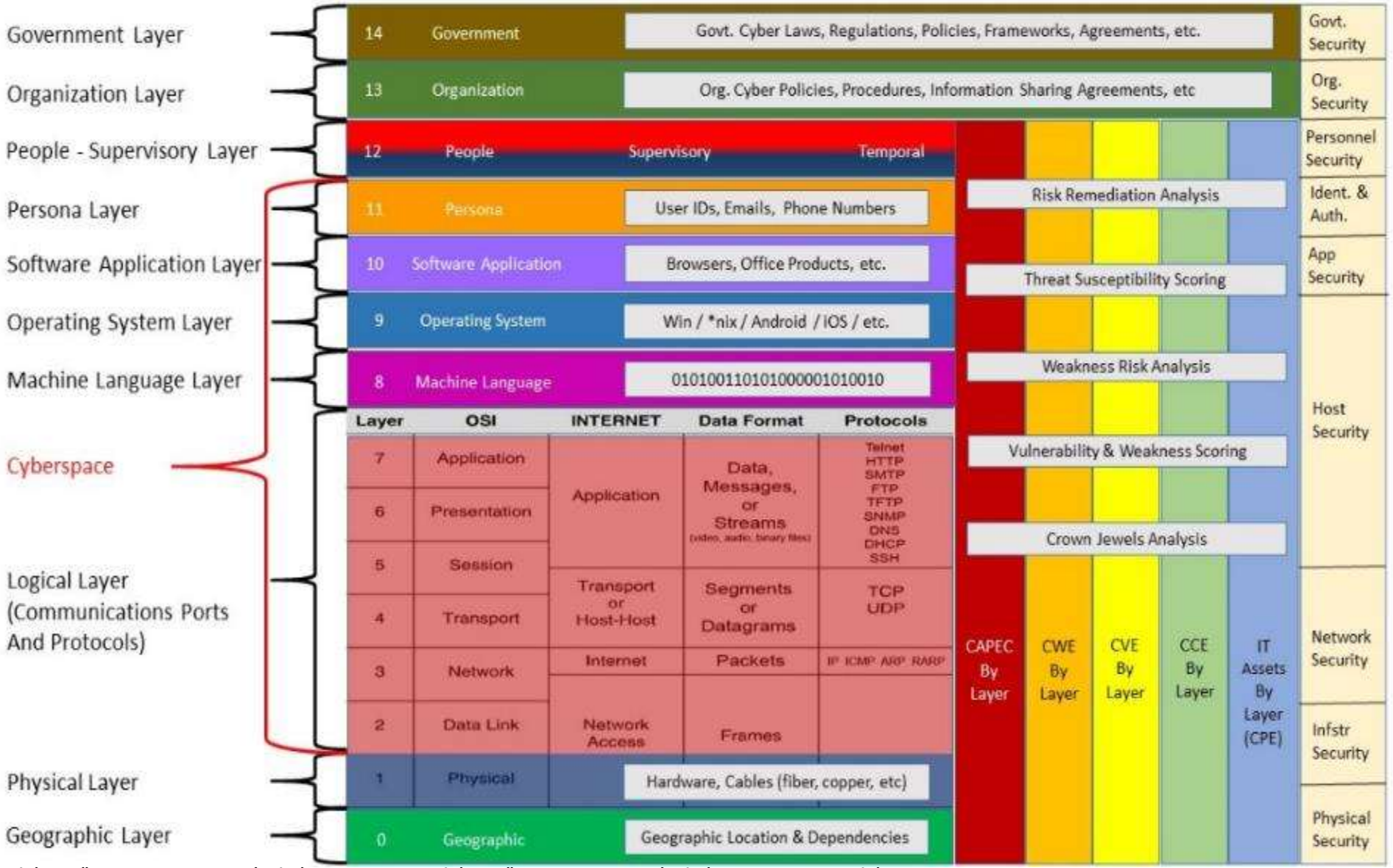
There are no simple or easy cyber security solutions

- 100% cybersecurity is not achievable – reduced risks (defense, threat exchange measures) and business resilience
- security measures may have privacy concerns (e.g. end-to-end-encryption)
- Rapidly evolving new industry platforms (NFV-SDN/5G, quantum computing…) need urgent "predictive" attention

Difficult to provide effective cyber security certification

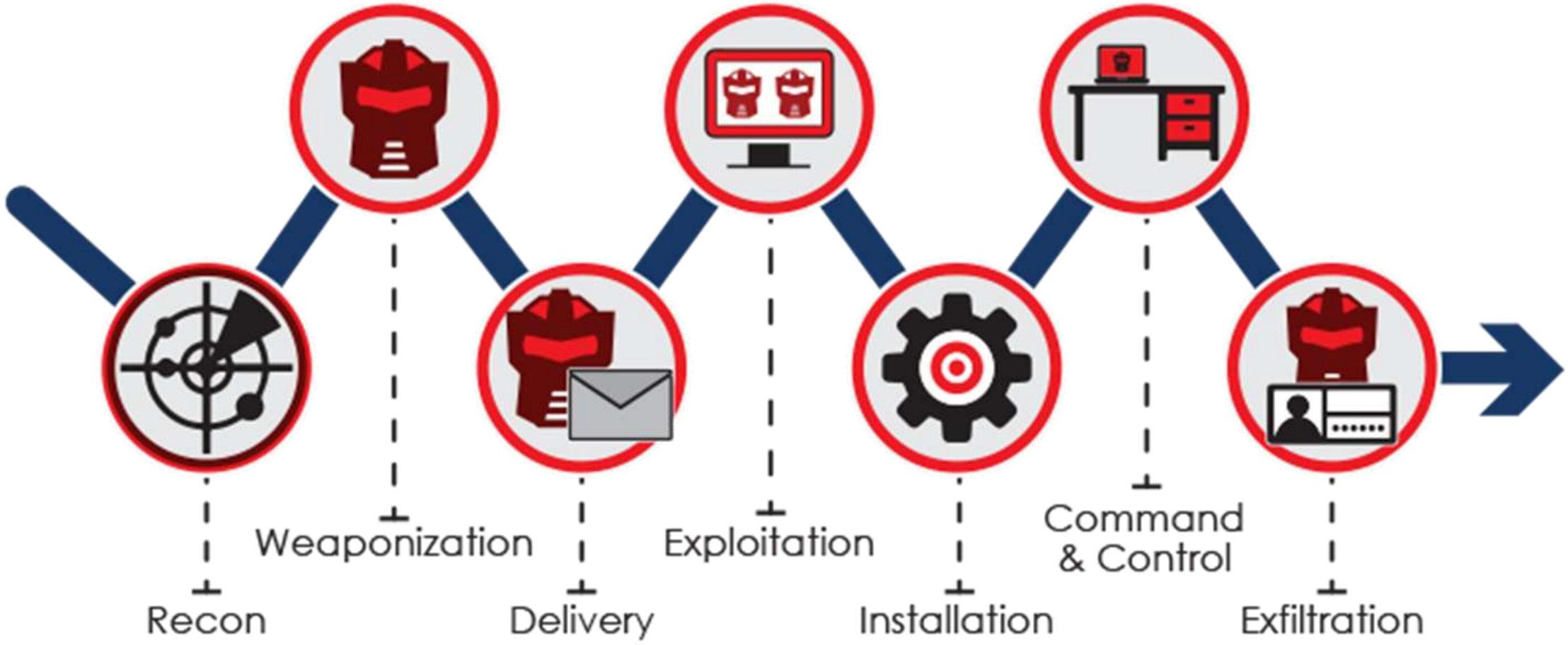
The anatomy of cyber attacks

Cyberspace and Cyber "terrain"
Beyond Layer 7



Cyber Kill Chain (simplified)

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

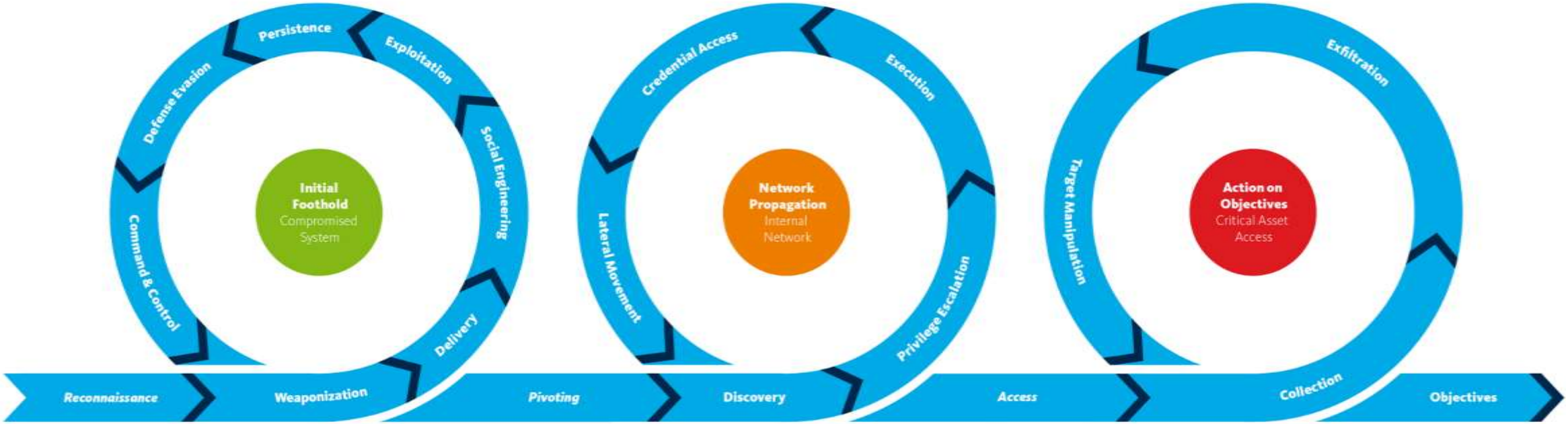


	Tactics	Clients	Networks	Servers
Stage 1 **Gather Info**	External reconn.	Social media, Email headers	Network scanning for Wifi AP, find physical network ports	Service & asset scanning OS fingerprinting Service enumeration
Stage 2 **Get in**	Deliver payload	Web, Email, portable Media	MITM	Upload paths, MITM Software updates
	Run payload	Bypass AWL/hardening	RCE on network equipment	SQL injections…
	External control	Remote shell/admin	Remote shell	Remote shell
	Gain privilege-access	Exploit bugs, OS loopholes	Default passwords	Exploit bugs, OS loopholes
	Install payload	files, shortcuts, registry	Network equipment backdoors	files, shortcuts, registry
Stage 3 **Stay in**	Internal reconn.	Scan for neighbors	Scan for zones	Scan for services
	Abuse credentials	Windows Credentials dump, rouge employees	VPNs, rouge network admins	Rouge admins
	Internal control	VPN, RDP, PSexec	Network admin take-overs	RDP, PSexec
Stage 4 **Execute mission**	Steal (Confidentiality)	Steal from endpoints, MITBrowser, OTP hijack	Steal on the wire	Dump database & files
	Tamper (Integrity)	Modification of documents	MITM	Change records
	Deny (Availability)	Wipe, encrypt-ransom	DDoS	DDoS, Wipe/Encrypt
	Damage (Safety)	Spoof commands	Replay commands	Spoof commands

Sample techniques & controls – non exhaustive. Take Mitre ATT&CK & CIS CSC

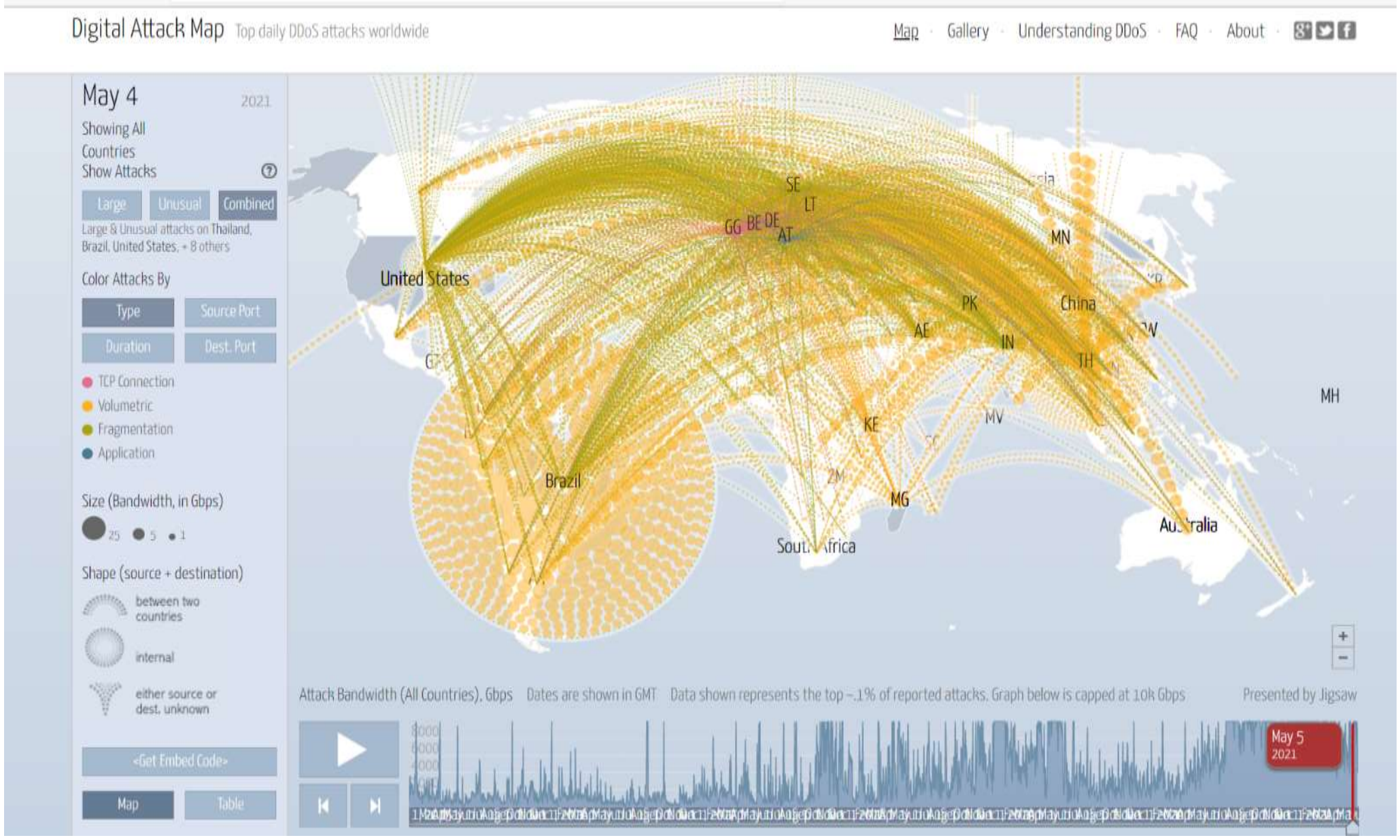
Kill Chain (unified)

A unified version of the kill chain was developed to overcome common critiques against the traditional cyber kill chain, by uniting and extending Lockheed Martin's kill chain and MITRE's ATT&CK framework. The unified kill chain is an **ordered arrangement of 18 unique attack phases** that may occur in end-to-end cyber attacks, which covers activities that occur outside and within the defended network. As such, the unified kill chain improves over the scope limitations of the traditional kill chain and the time-agnostic nature of tactics in MITRE's ATT&CK. The unified model can be used to analyze, compare and defend against end-to-end cyber attacks by advanced persistent threats (APTs).



DDoS Attacks Worldwide

https://digitalattackmap.com/

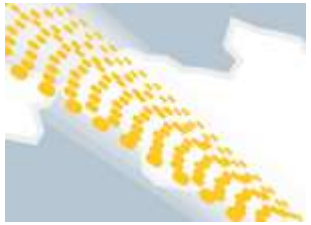


Attack Class: Four common categories of attacks

https://digitalattackmap.com/understanding-ddos/

TCP Connection Attacks - *Occupying connections*

These attempt to use up all the available connections to infrastructure devices such as load-balancers, firewalls and application servers. Even devices capable of maintaining state on millions of connections can be taken down by these attacks. Learn more...



Volumetric Attacks - *Using up bandwidth*

These attempt to consume the bandwidth either within the target network/service, or between the target network/service and the rest of the Internet. These attacks are simply about causing congestion. Learn more...

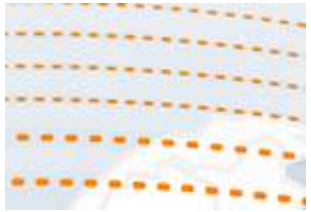
Fragmentation Attacks - *Pieces of packets*

These send a flood of TCP or UDP fragments to a victim, overwhelming the victim's ability to re-assemble the streams and severely reducing performance. Learn more...

Application Attacks - *Targeting applications*

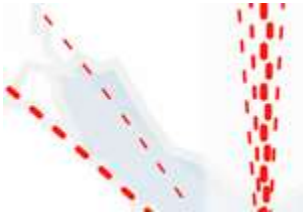
These attempt to overwhelm a specific aspect of an application or service and can be effective even with very few attacking machines generating a low traffic rate (making them difficult to detect and mitigate). Learn more...

Amplification: Two ways attacks can multiply traffic they can send. https://digitalattackmap.com/understanding-ddos/



DNS Reflection - *Small request, big reply.*

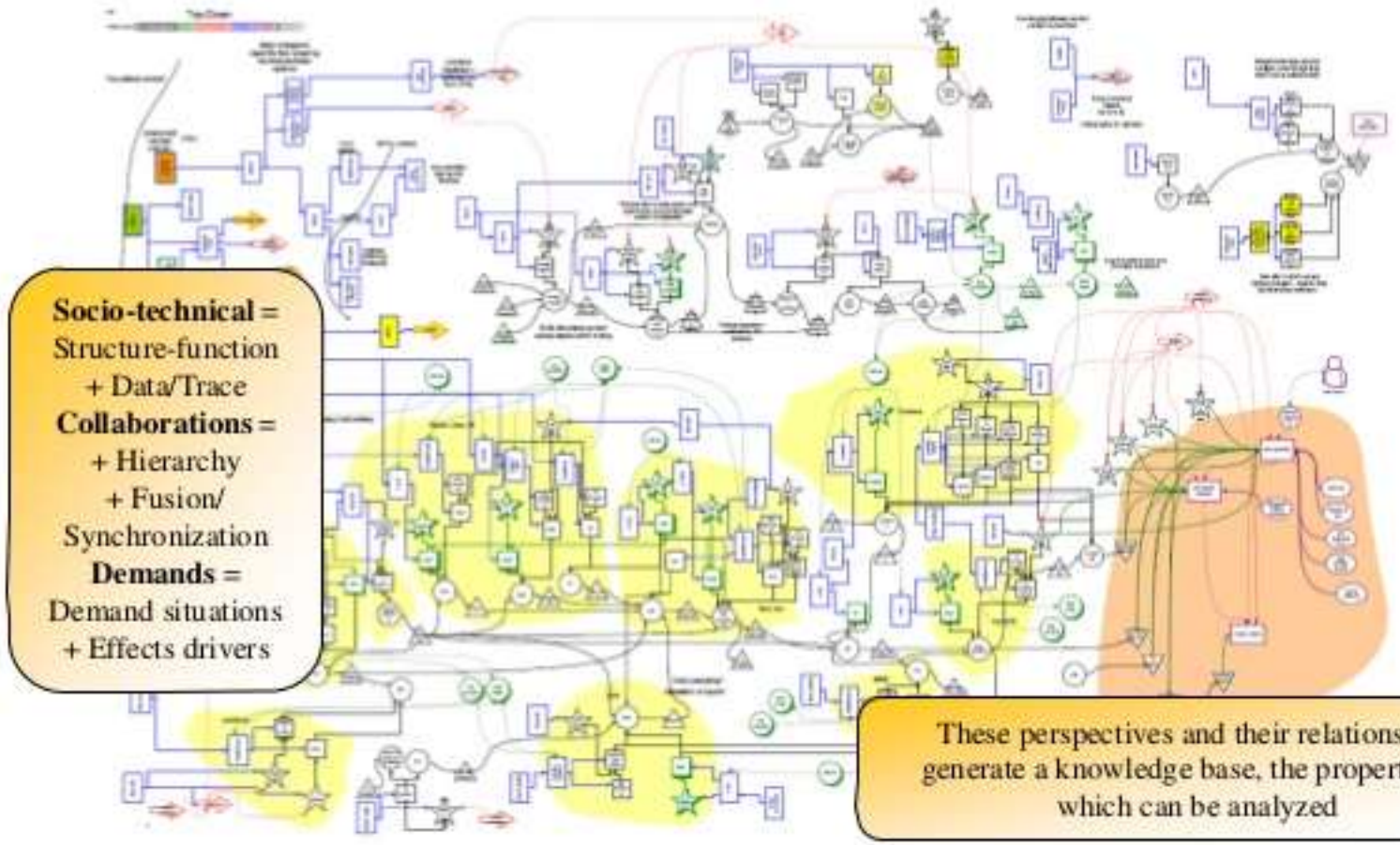
By forging a victim's IP address, an attacker can send small requests to a DNS server and ask it to send the victim a large reply. This allows the attacker to have every request from its botnet amplified as much as 70x in size, making it much easier to overwhelm the target. Learn more...



Chargen Reflection - *Steady streams of text*Most computers and internet connected printers support an outdated testing service called Chargen, which allows someone to ask a device to reply with a stream of random characters. Chargen can be used as a means for amplifying attacks similar to DNS attacks above Learn more...

Complex systems of systems:

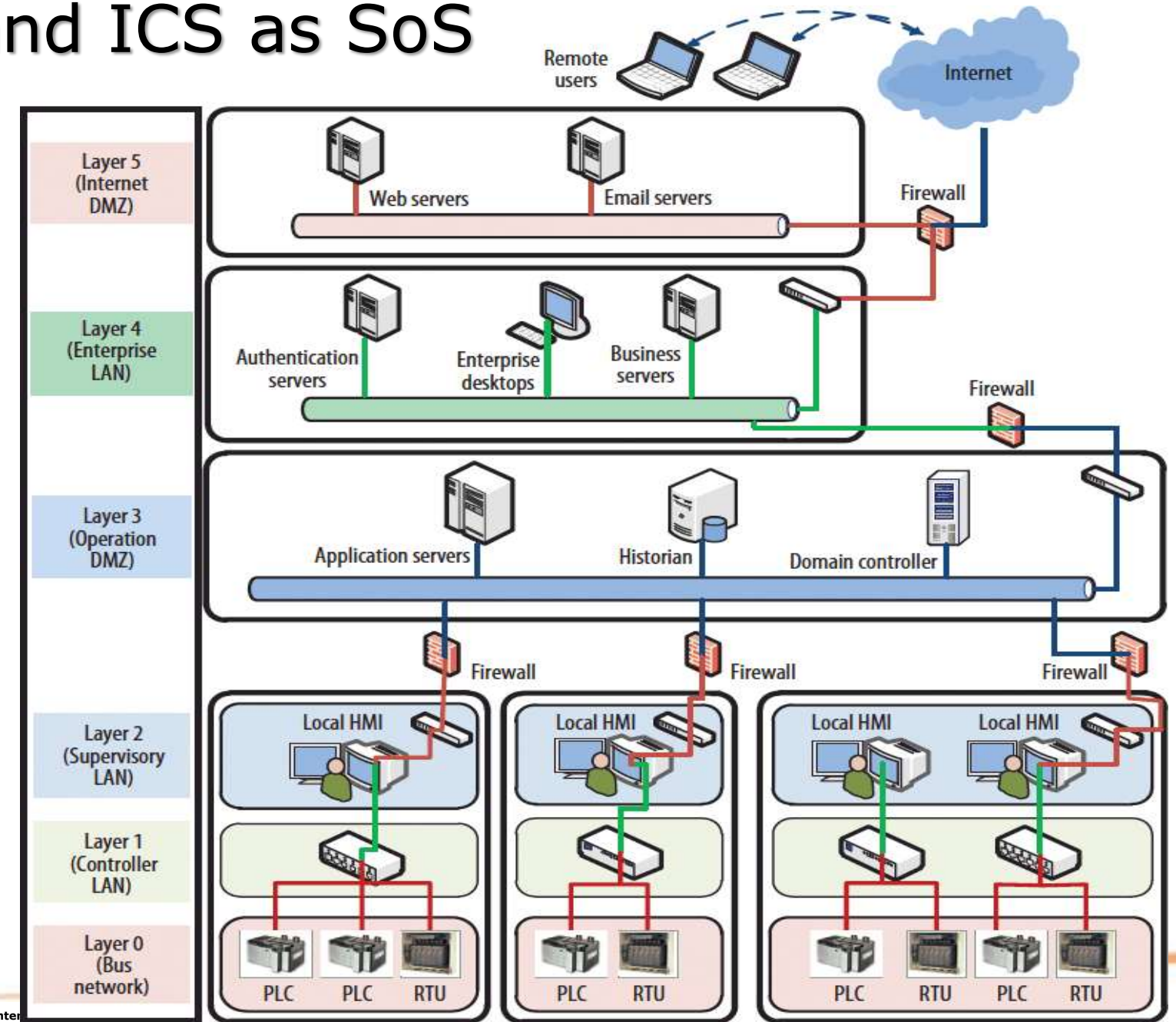
all three modeling perspectives become necessary



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

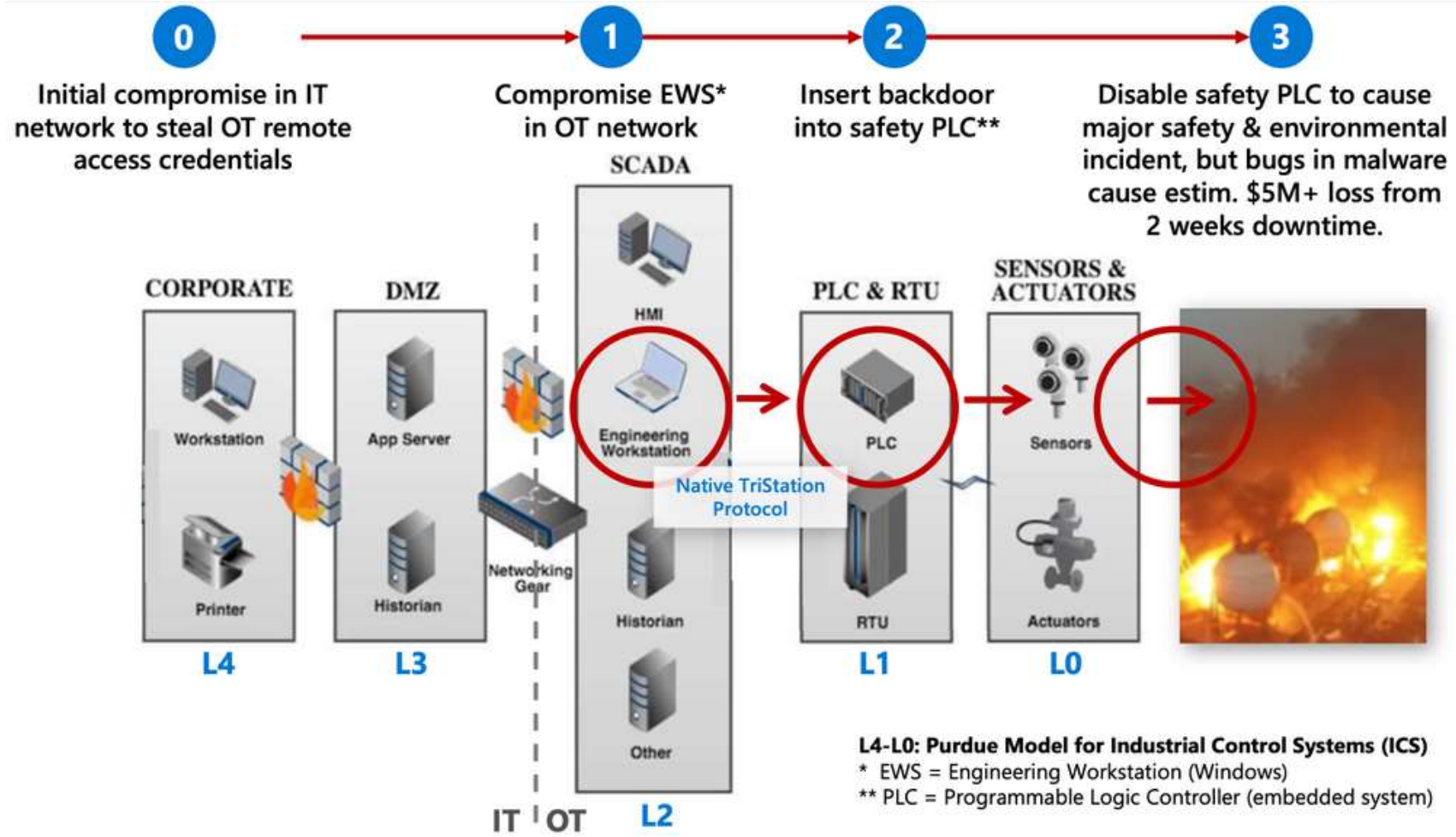
SCADA and ICS as SoS



Targeting Critical Infrastructure MITRE ATT&CK for ICS/SCADA

TRITON Deep Dive

https://techcommunity.microsoft.com/t5/microsoft-defender-for-iot-blog/microsoft-scores-highest-in-threat-visibility-coverage-for-mitre/ba-p/2577072



https://www.computerweekly.com/news/252461467/Triton-industrial-malware-group-still-active-researchers-warn

CERT® Resilience Management Model

Cyber resilient business, organizations, society

Operational Risk Management

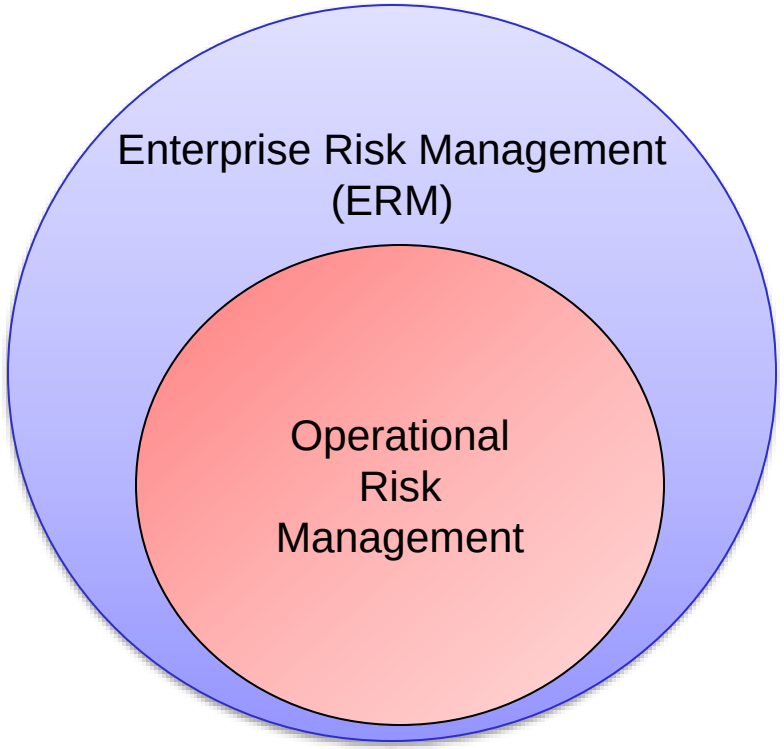
A form of risk affecting day-to-day business operations

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.

Organizational certainties

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

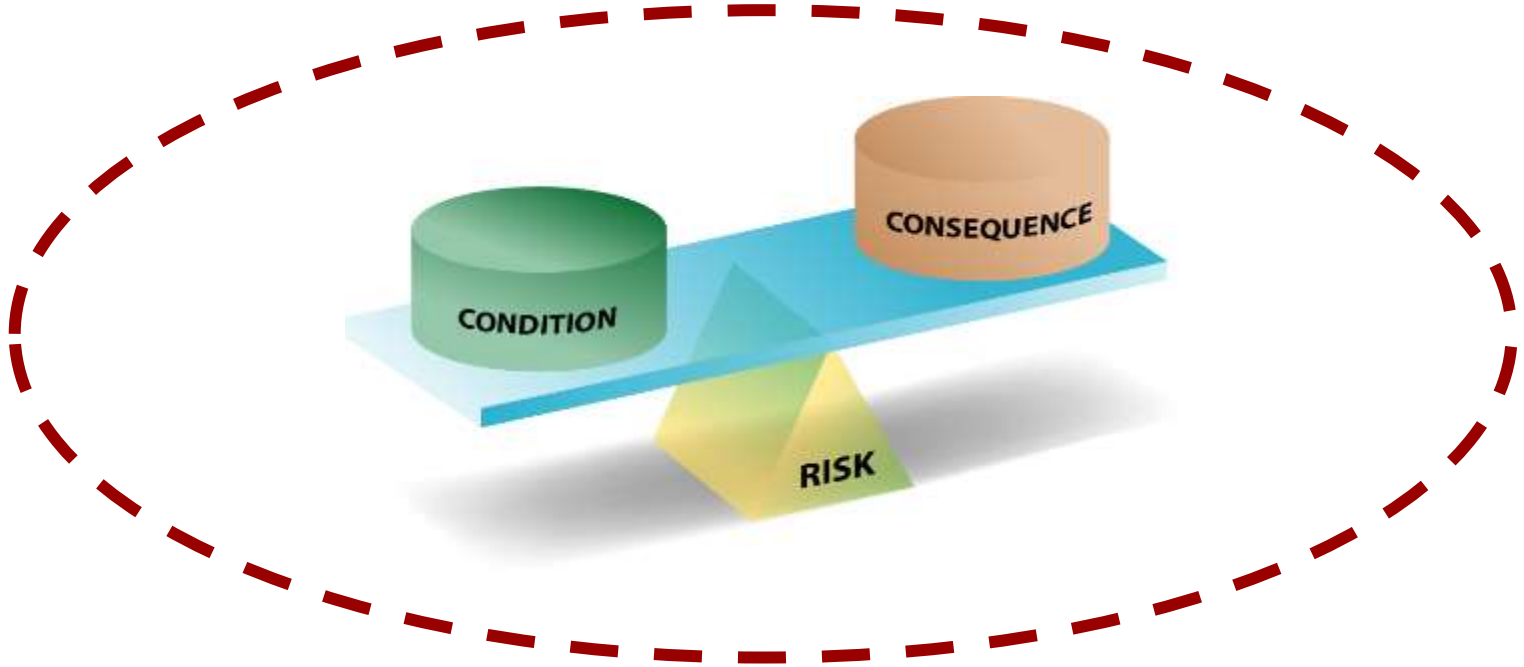
Organizations must get better at “surviving” in uncertainty.

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.

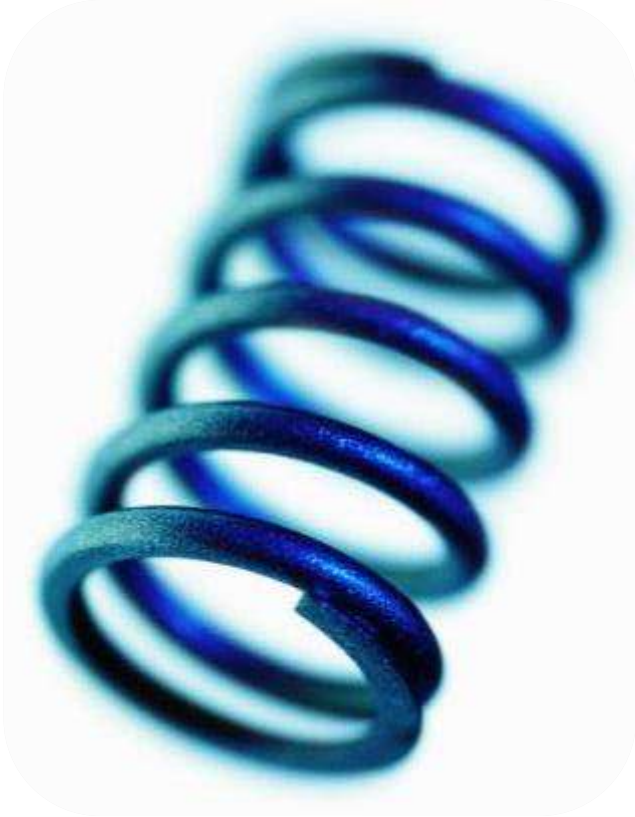
Managing Operational Risk requires a holistic approach



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.

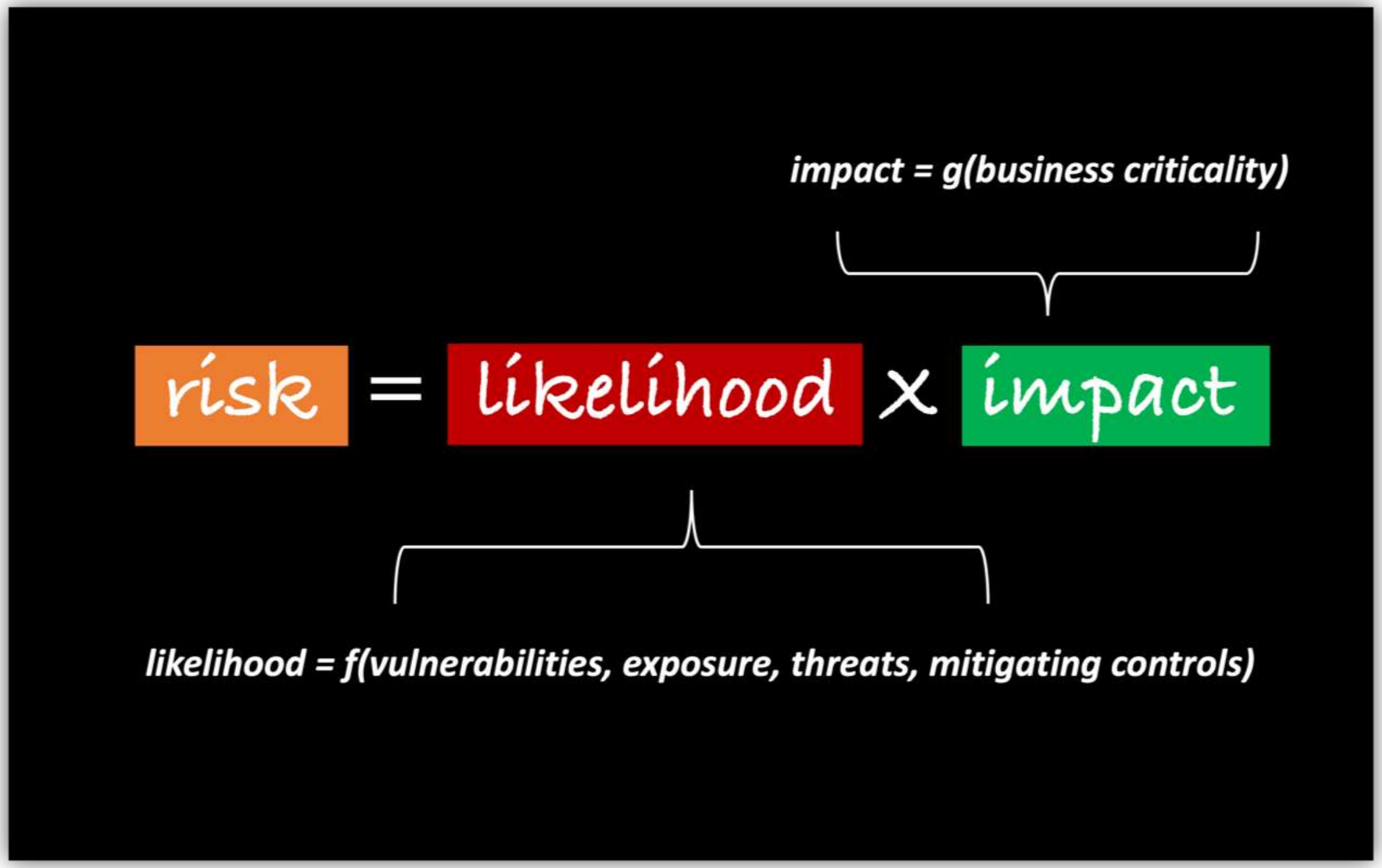
Operational resilience defined

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]

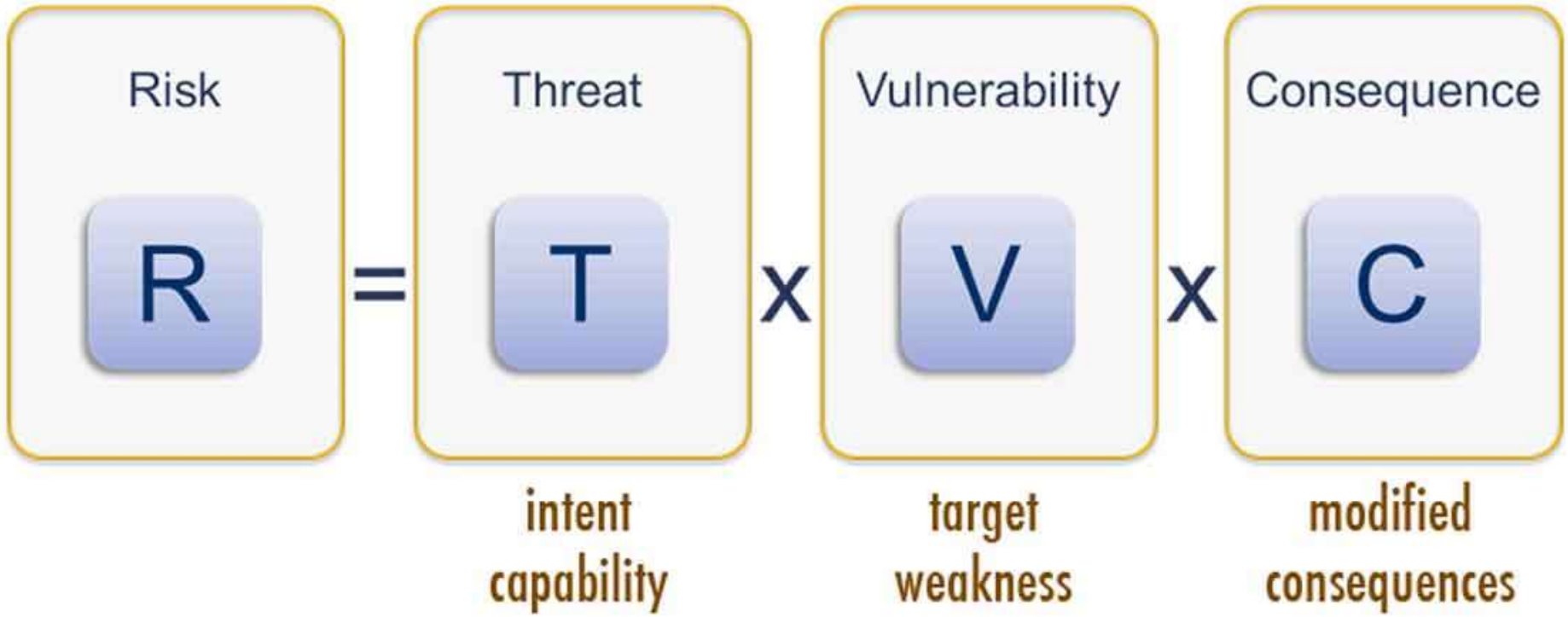


Operational Resilience: The ***emergent*** property of an organization that can continue to carry out its mission in the presence of ***operational stress*** and ***disruption*** that does not exceed its operational limit [CERT-RMM]

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


impact = g(business criticality)
risk = likelihood x impact
likelihood = f(vulnerabilities, exposure, threats, mitigating controls)

Risk = TVC

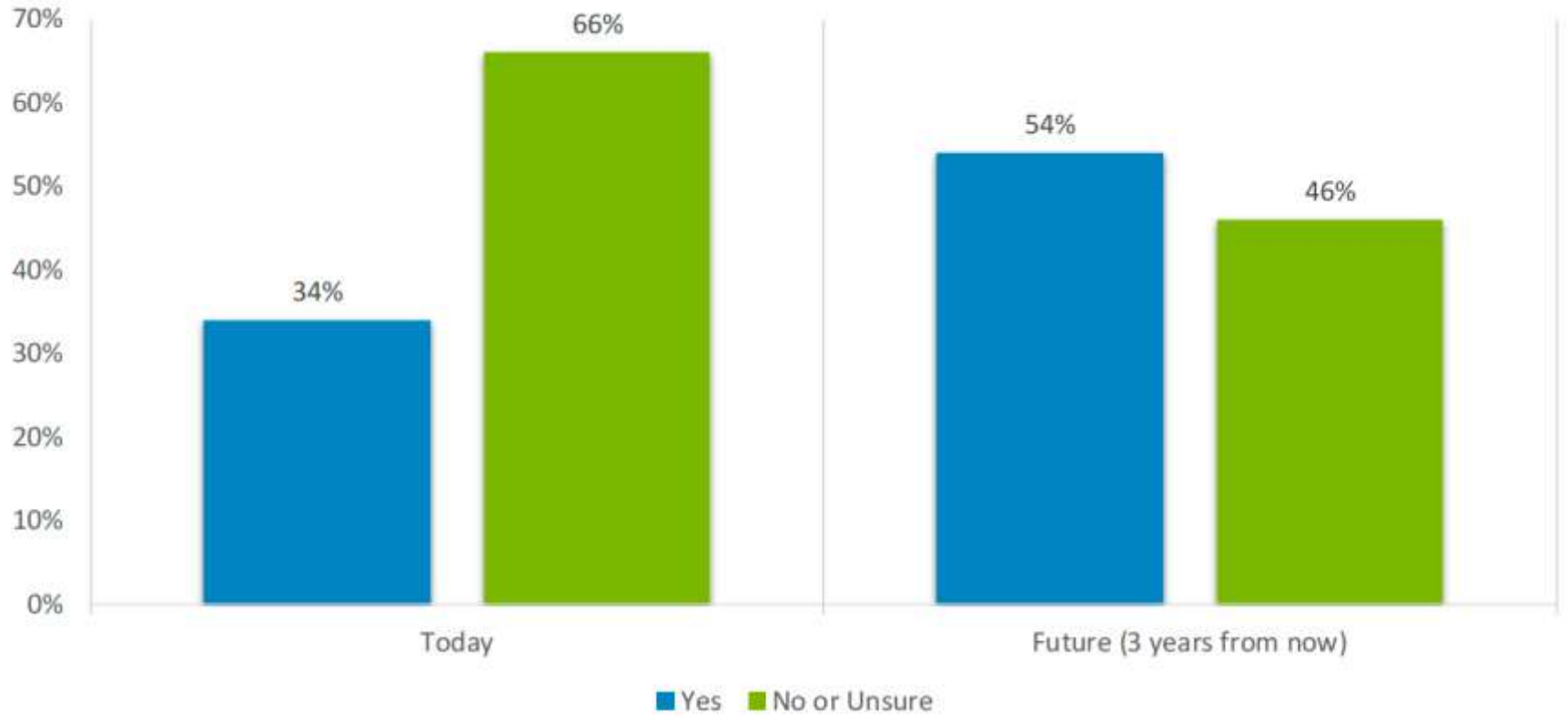

Risk
R
=
Threat
T
x
Vulnerability
V
x
Consequence
C
intent
capability
target
weakness
modified
consequences


Avoid
Accept
Risk
Transfer
Reduce

"You must not say 'never.' That is a lazy slurring-over of the facts. Actually, [risk analysis] predicts only probabilities. A particular event may be infinitesimally probable, but the probability is always greater than zero."

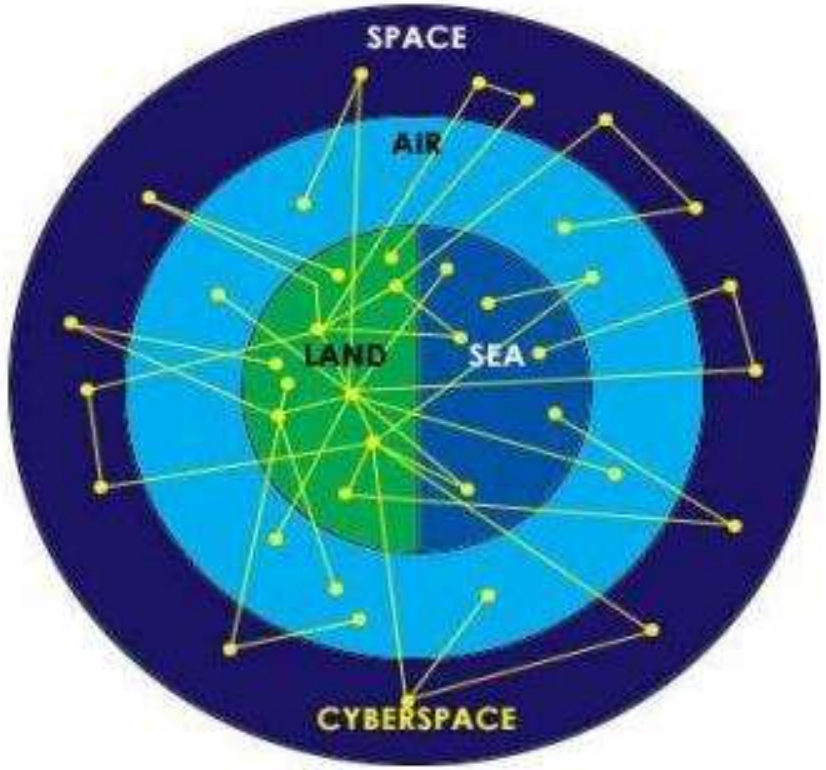
Second Foundation (Isaac Asimov)

Percentage of senior leadership that views cybersecurity as a strategic priority



Source: Ponemon Institute Research Report: 2015 Global Megatrends in Cybersecurity, February 2015

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

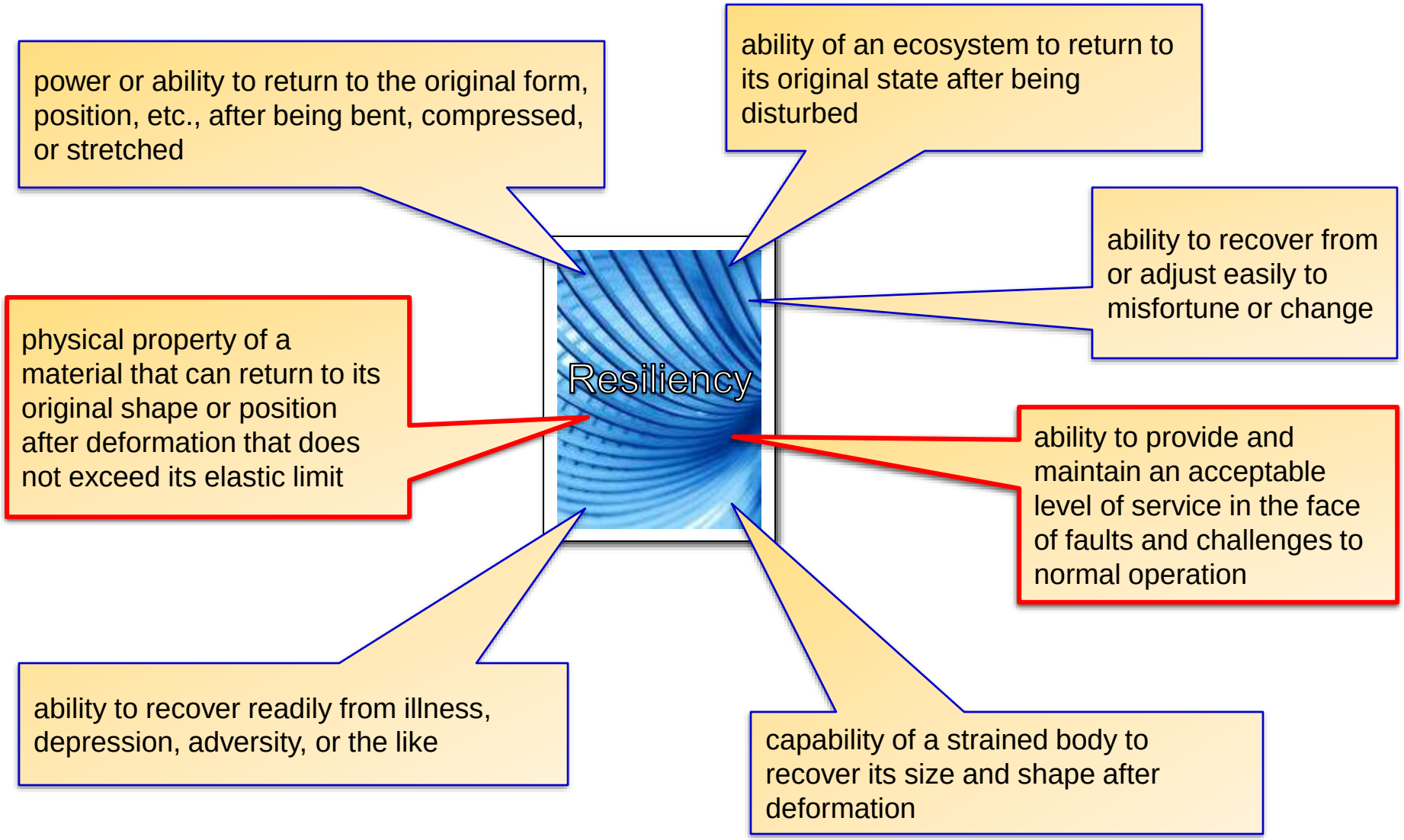


Security Risk Management

=

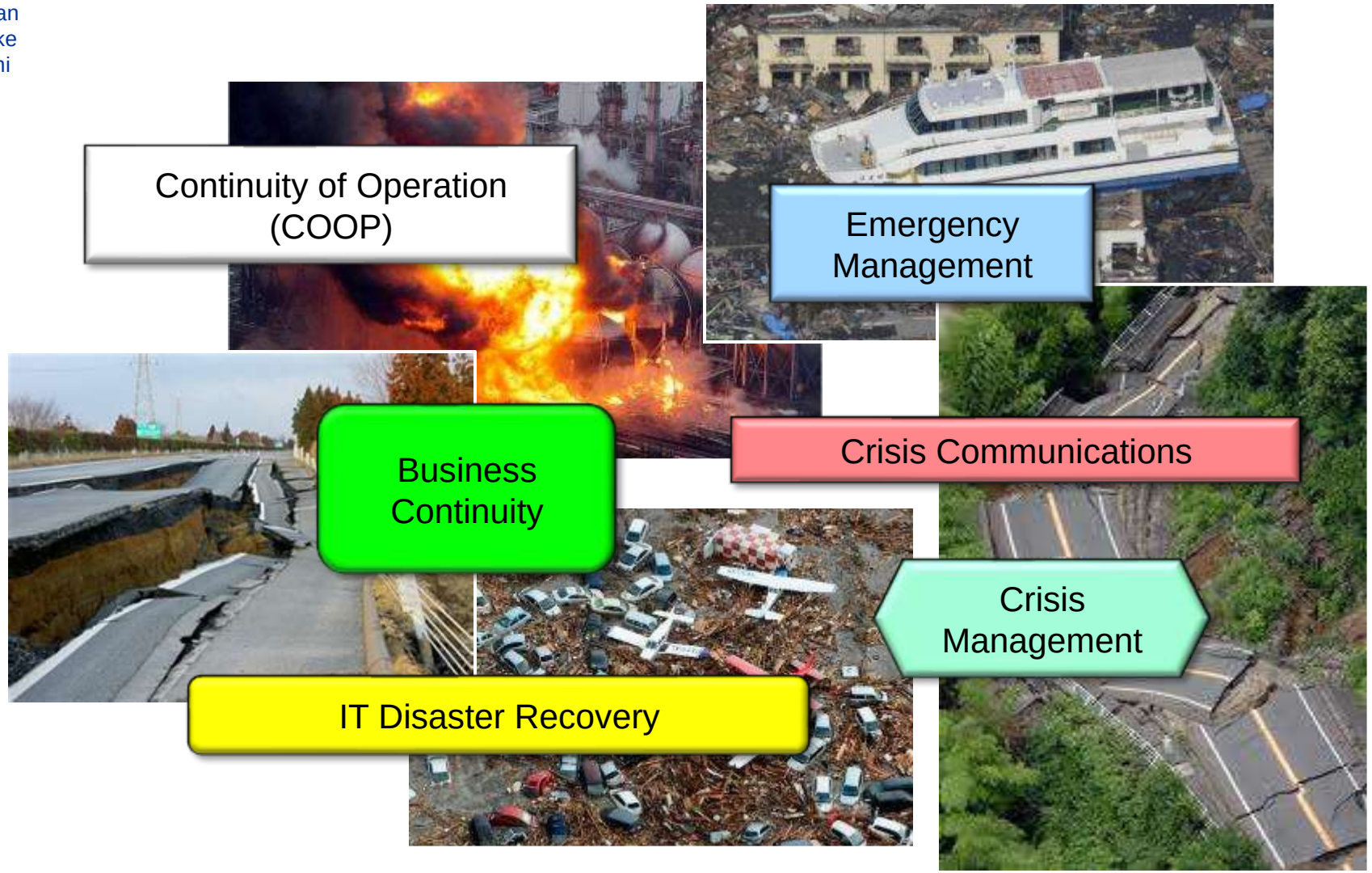
Resilience Management

re·sil·ience *noun* [ri-ˈzil-yəns]



Example

2011 Japan
Earthquake
& Tsunami



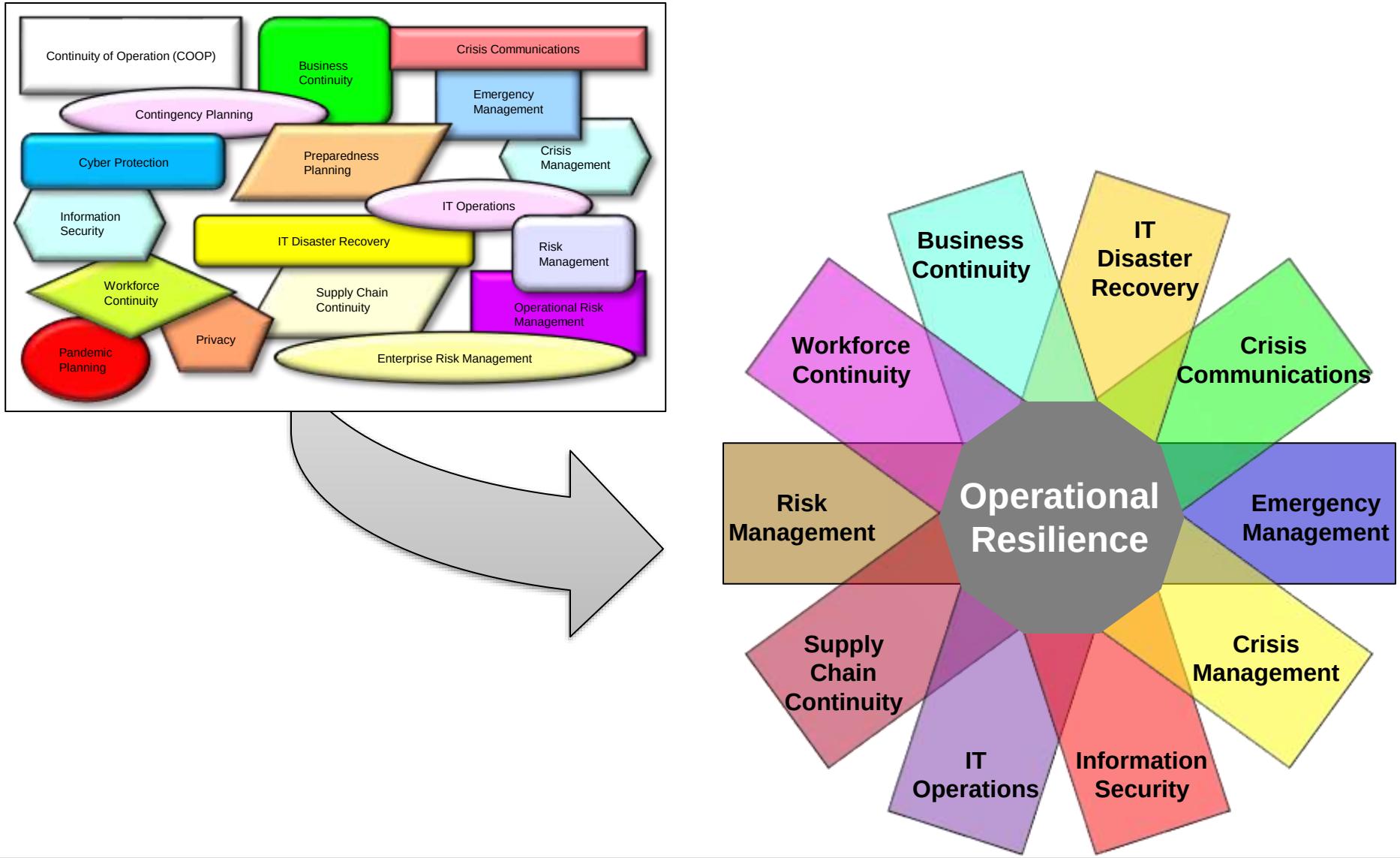
Example


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
Crisis Communications
COMPUTERWORLD
Sony cuts off Sony Online Entertainment service after hack
Robert McMillan
Comments (5)
Recommended (45)
Like 144
PLAYSTATION Network

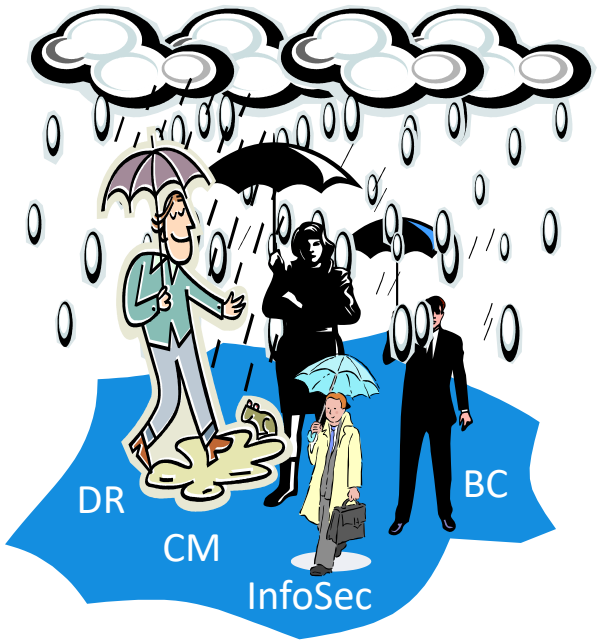
Example


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
ington Post Staff Writer
Wednesday, September 1, 2
A computer outage that ha
state agencies entered its s
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

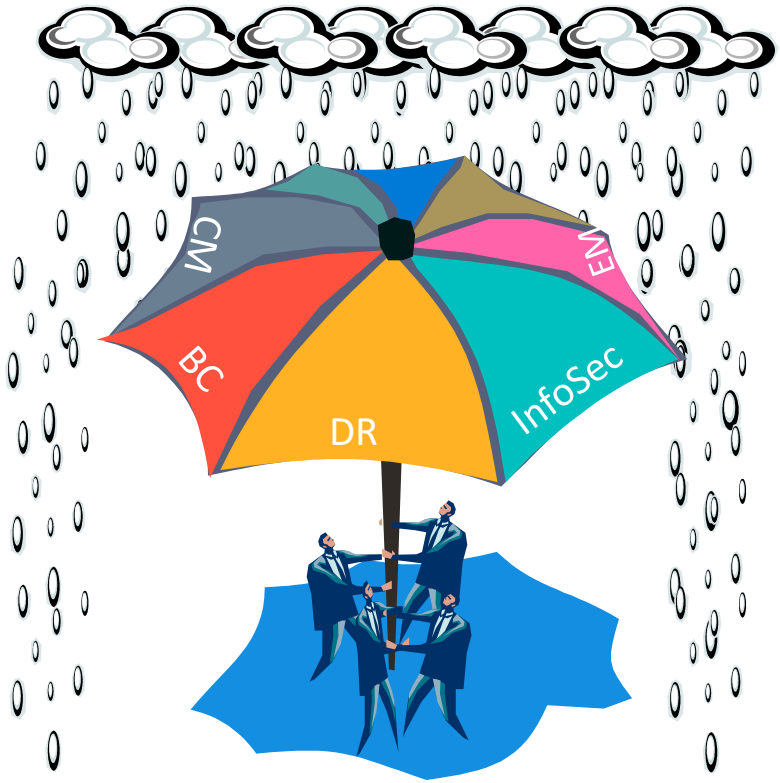
Convergence: An Analogy



Resilience = Convergence of efforts and responsibilities



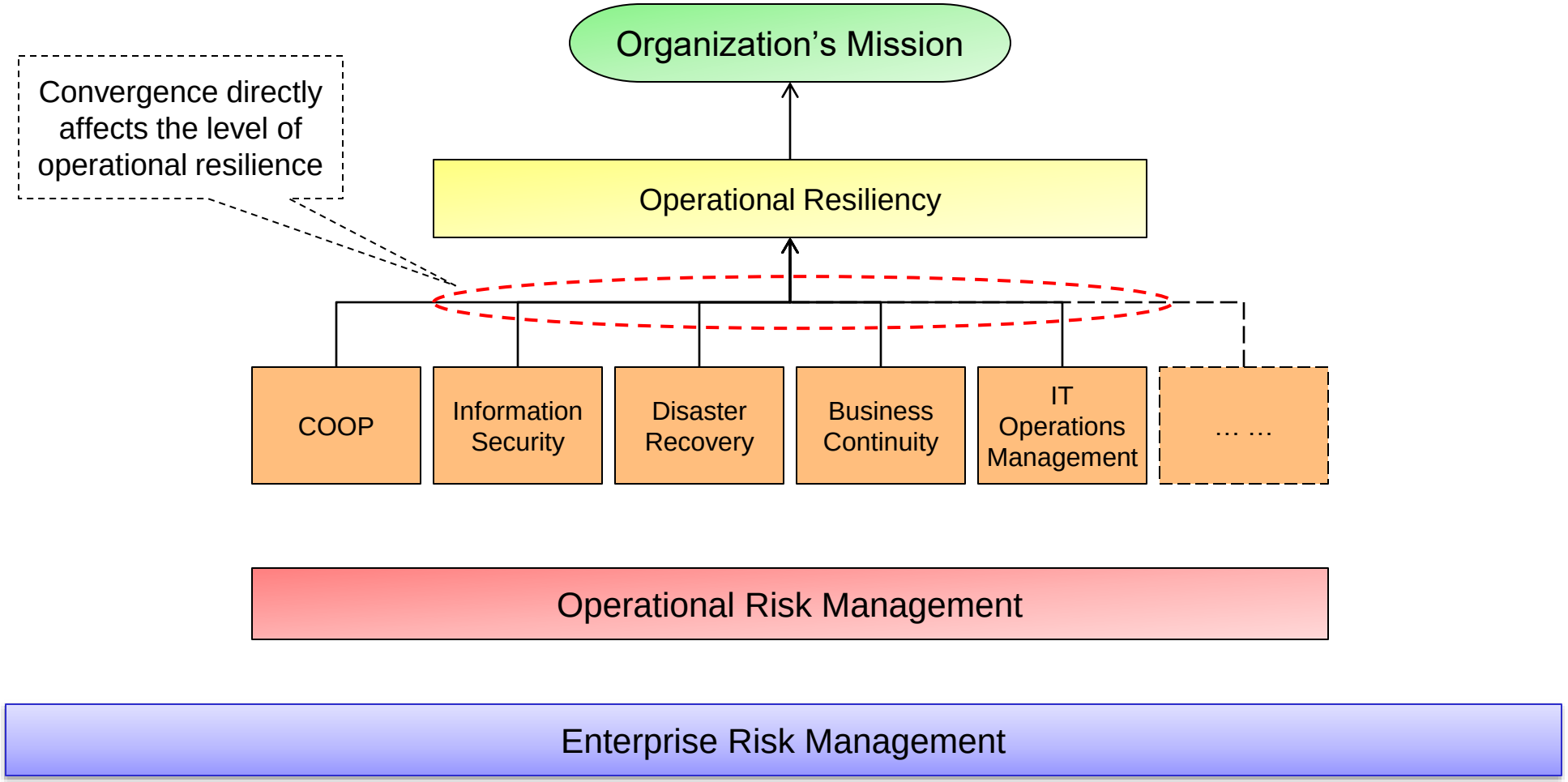
Convergence



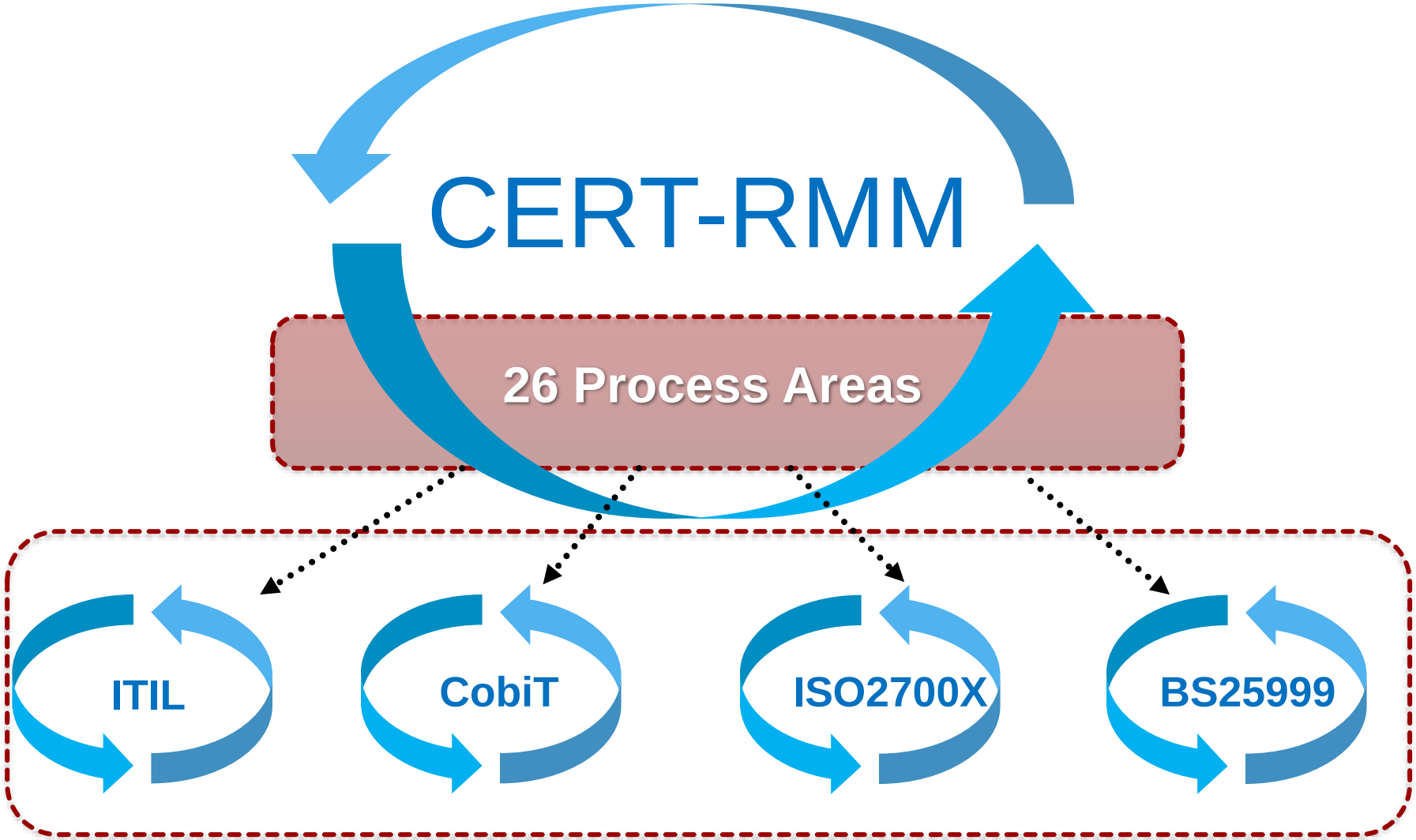
CERT® Resilience Management Model

http://www.cert.org/resilience/products-services/cert-rmm/

Convergence



CERT-RMM as an Organizing/Integrating Structure



RMM – The Model

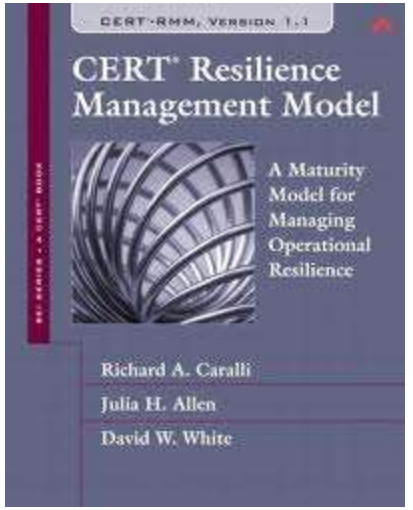
Guidelines and practices for

- 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



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

CERT-RMM: 26 процесни области в 4 категории

Инженерни

ADM – Дефиниране и управление на активите

RRD – Разработване на изисквания за устойчивост

RRM – Управление на изискванията за устойчивост

SC – Непрекъснатост на услугите

CTRL –Управление на контролите

RTSE – Инженеринг на устойчиви технически решения

Организационни

EF –Организационен фокус

COMP – Съответствия

FRM – Управление на финансовите ресурси

HRM – Управление на човешките ресурси

RISK – Управление на риска

COMM – Комуникации

OTA – Организационно обучение и осведомяване

Оперативни

PM – Управление на хората

KIM – Управление на информация и знания

TM – Управление на технологии

EC – Контрол на средата (съоръженията)

AM – Управление на достъпа

ID - Управление на идентичностите

IMC – Управление и контрол на инцидентите

VAR – Анализ и адресиране на уязвимостите

EXD – Управление на външните зависимости

Процесни

MON – Мониторинг (наблюдение)

MA – Измерване и Анализ

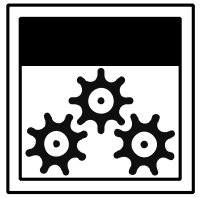
OPD – Дефиниране на организационни процеси

OPF – Фокус върху организационните процеси

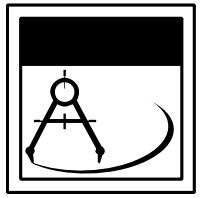
Model architecture

Composed of 26 process areas across four categories

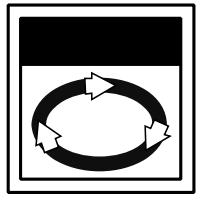
Enterprise Management



Operations Management

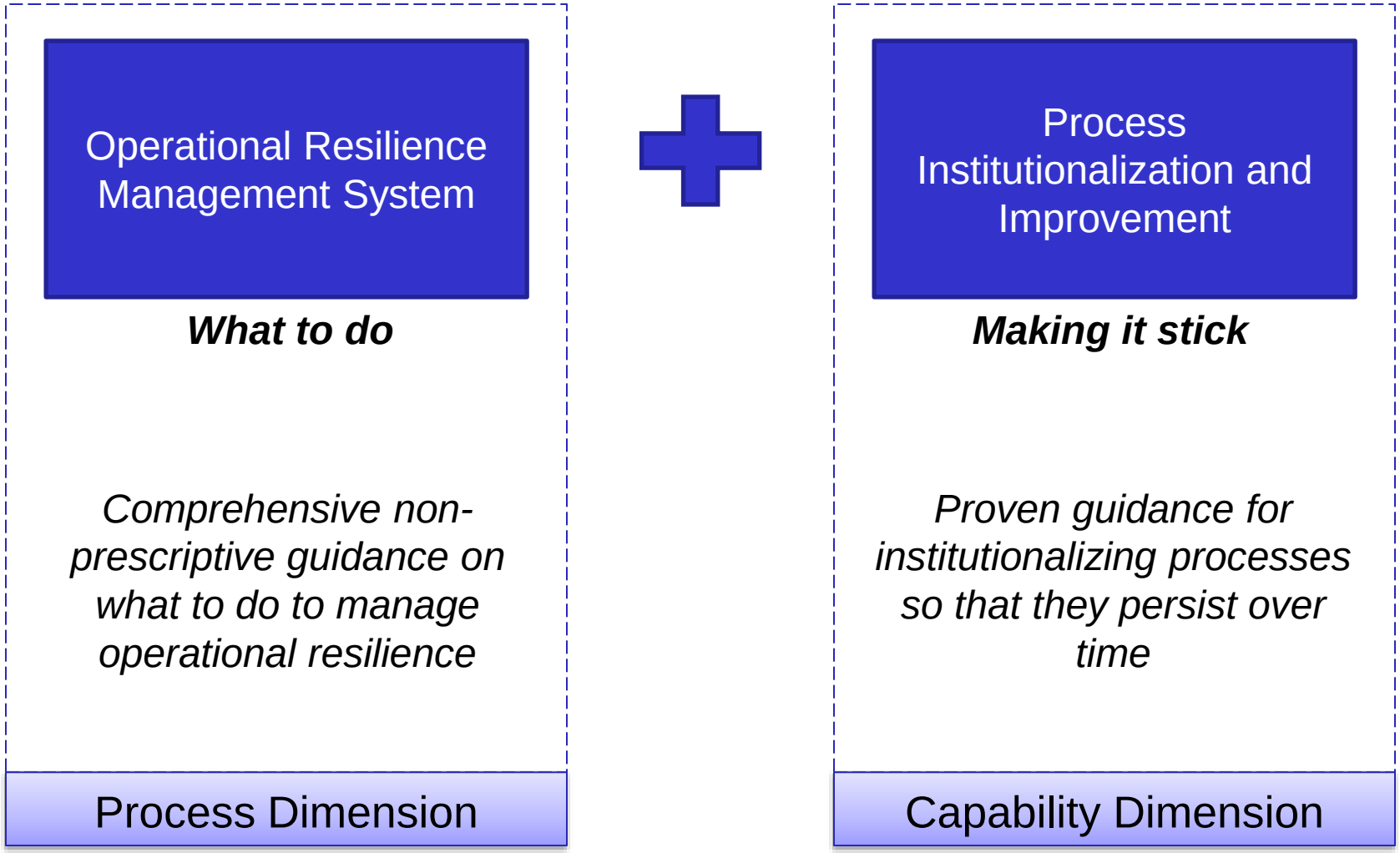


Engineering

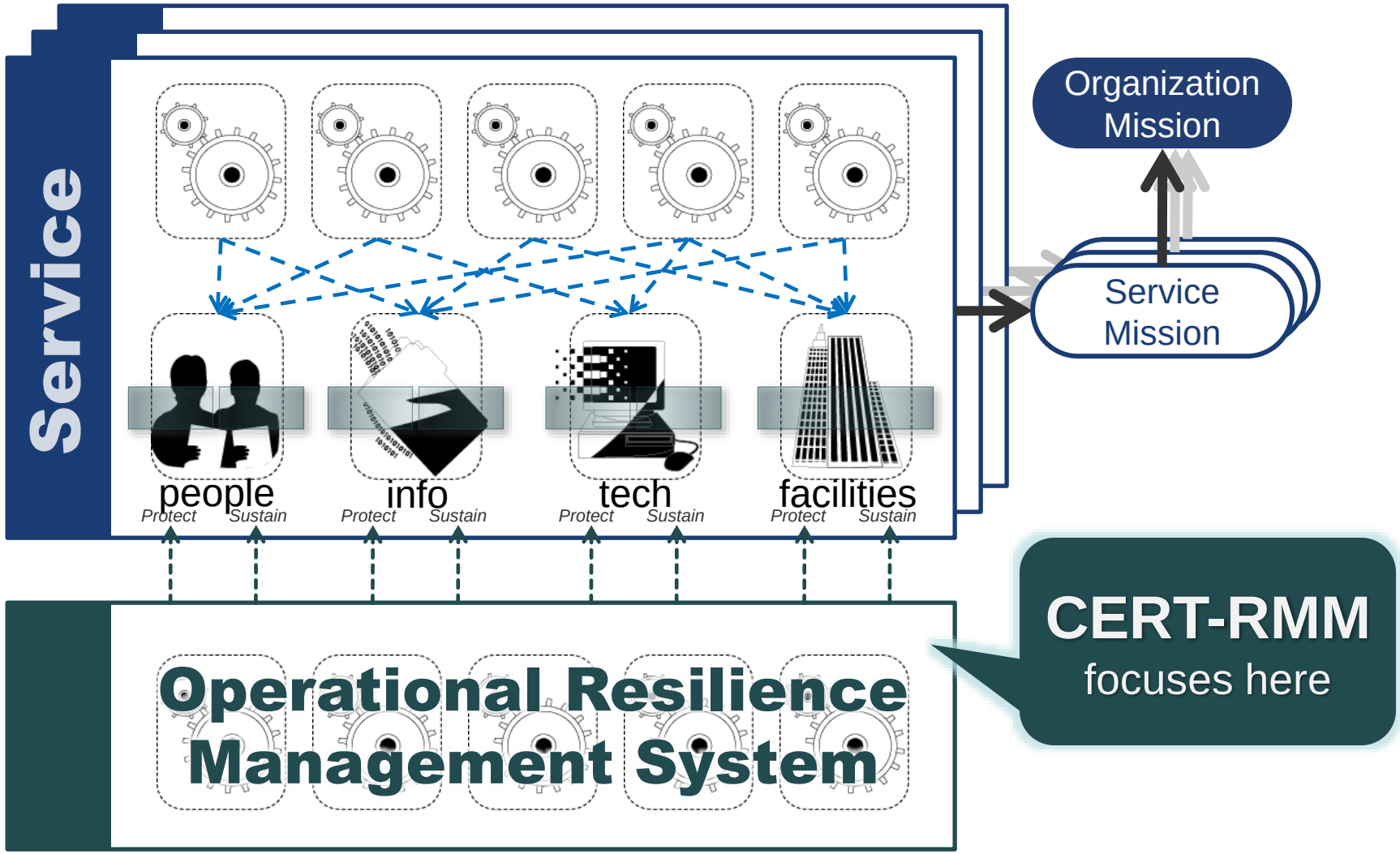


Process Management

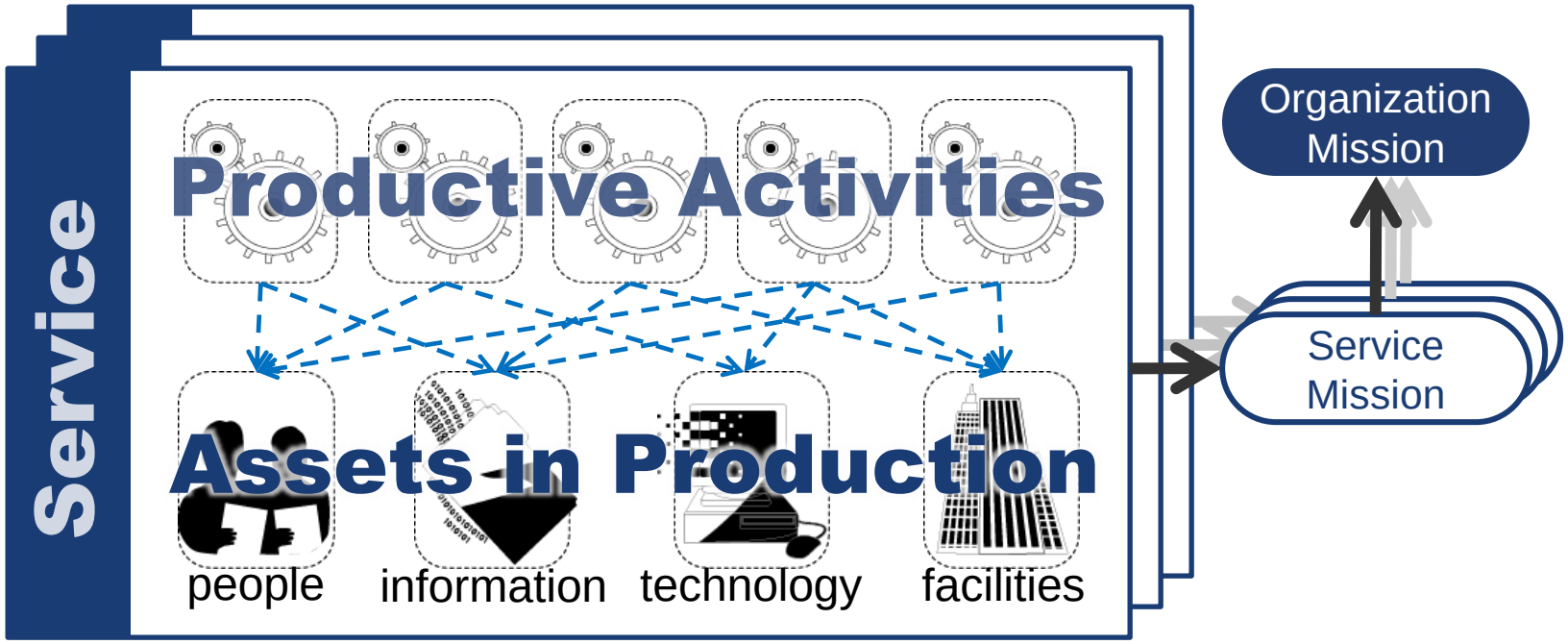
CERT-RMM Approach



Organizational context



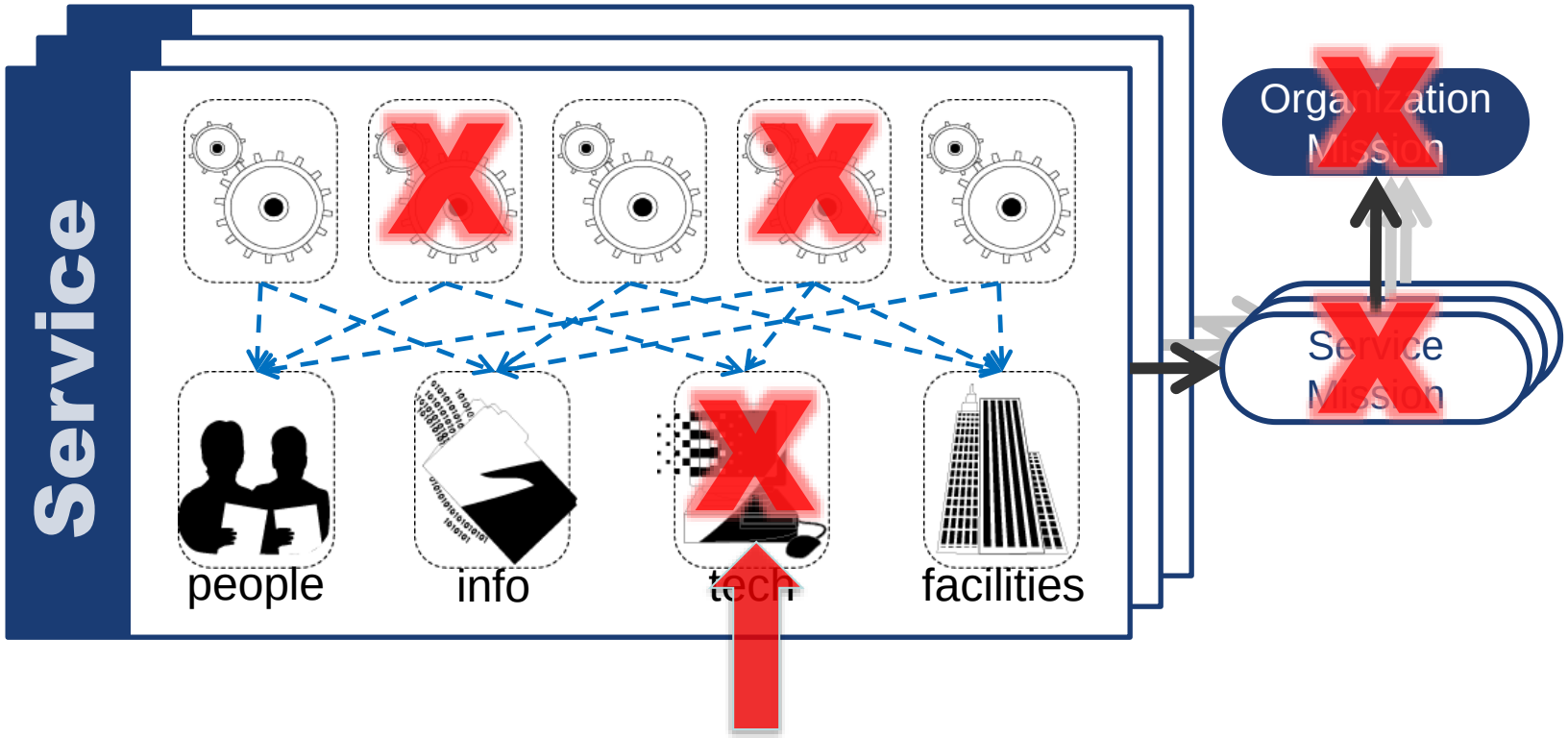
Organizational context



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 (Ford Pint

Event declaration (NYC snow emergencies)

Supply chain resilience (NASDAQ after 9/11)

People resilience (two banks after 9/11)

Changes in operational environment (USPS

Technology resilience (Egypt internet/cell ph

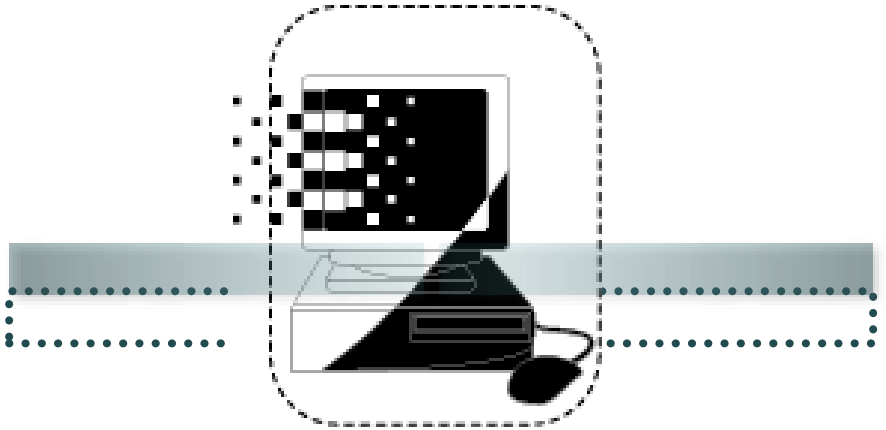
Prioritizing external relationships (based on

Determining critical assets (networked kiosk

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



Protect *Sustain*

Security Domain BC/DR Domain

Protection strategies	Sustainment strategies
Keep assets from exposure to disruption	Keep assets productive during adversity
Typically implemented as “security” activities	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

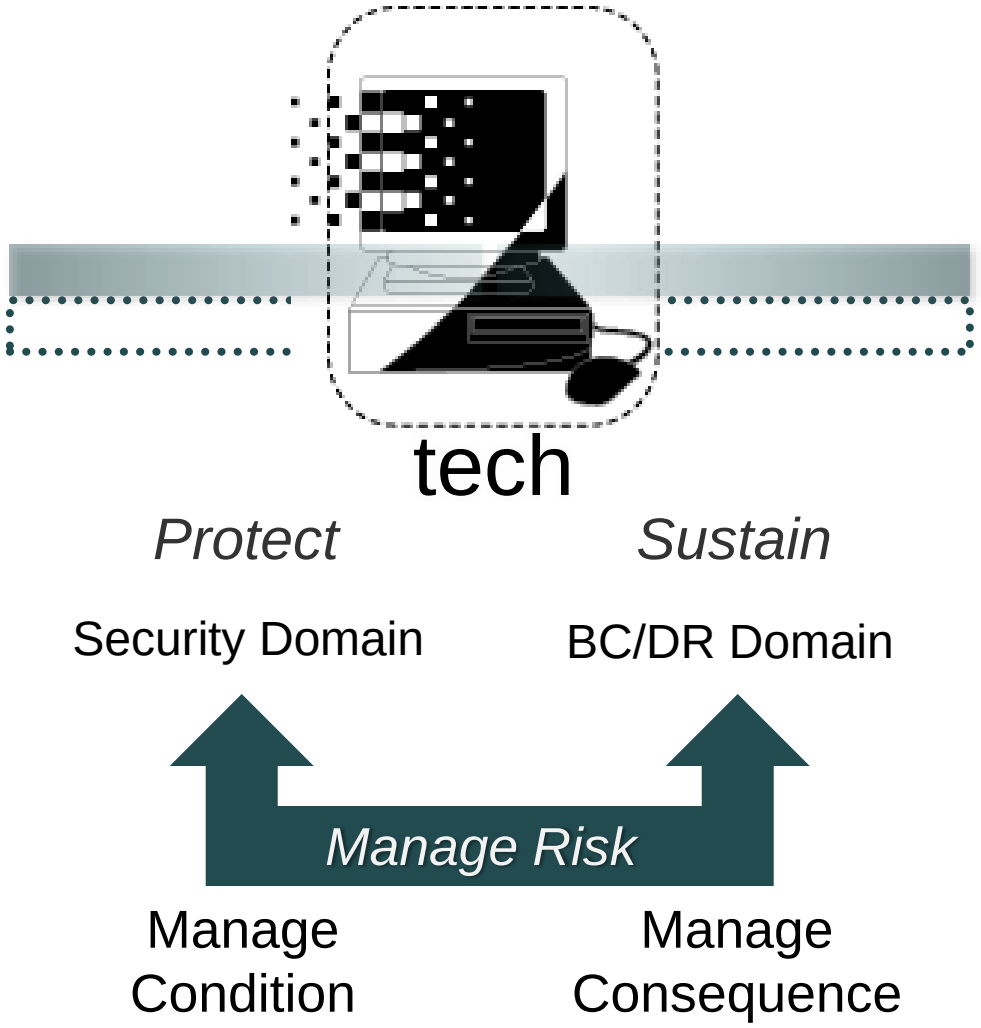
Availability – Ensuring that an asset remains accessible to authorized users (people, processes, or devices) whenever it is needed

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

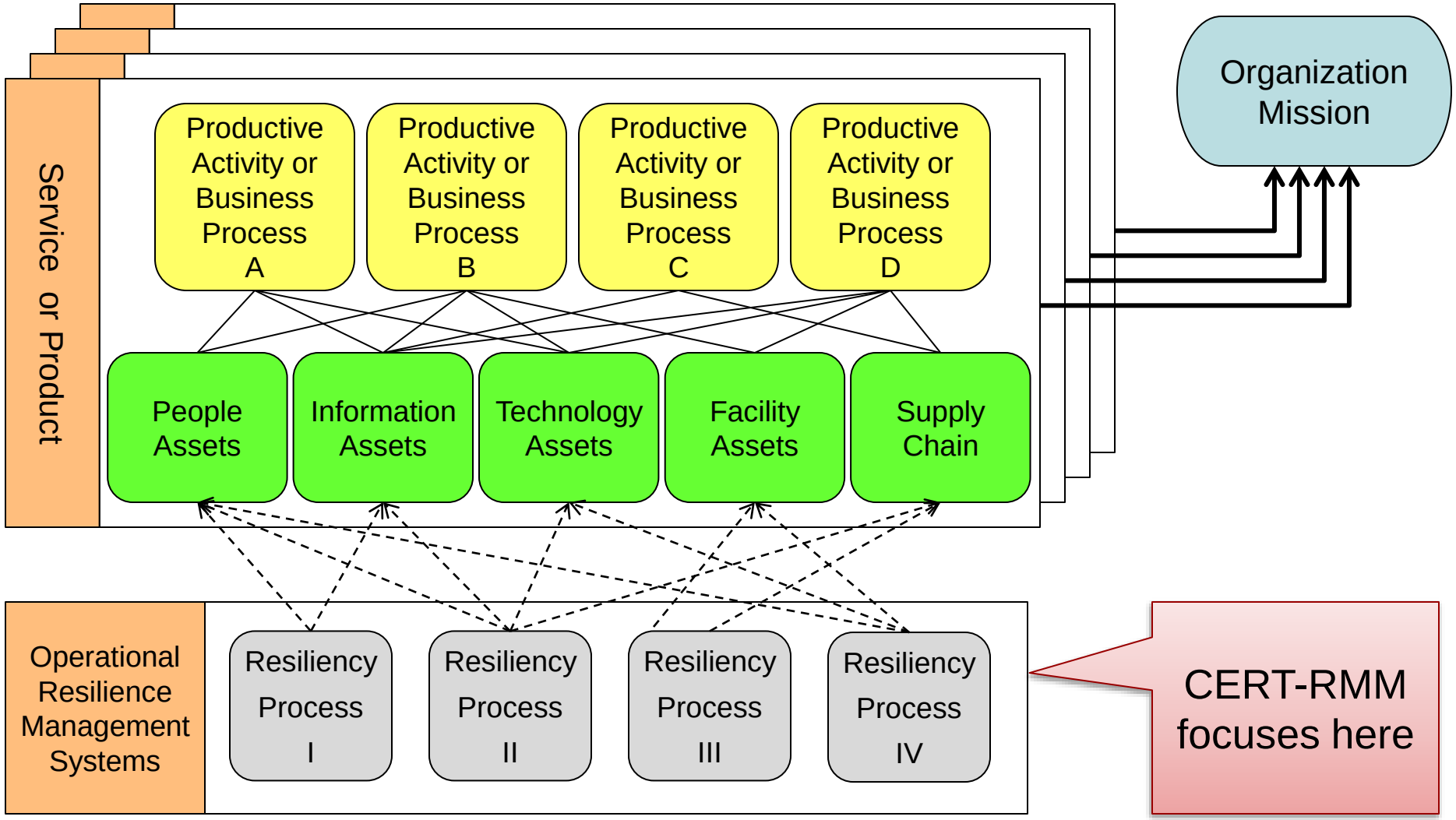


The optimal “mix” of protection and sustainment strategies

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

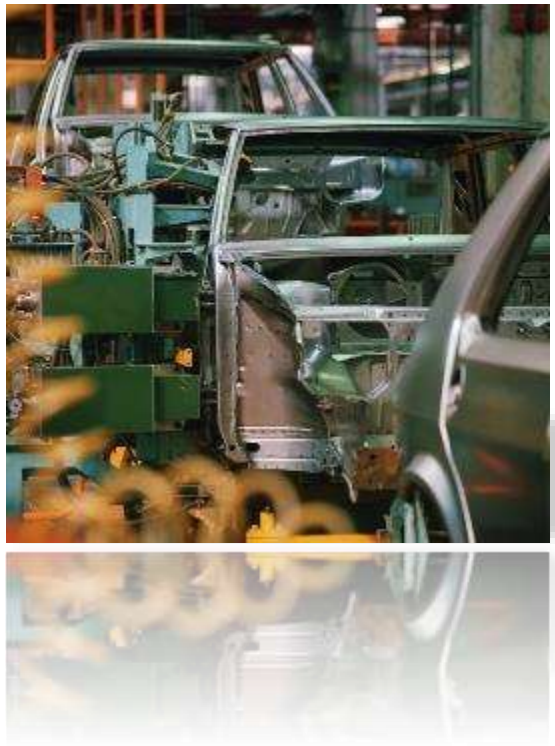
BC, security, & IT operations collaborating to manage risk

Organizational Context for Resiliency Activities



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

Engineering process areas

Establishing resilience for organizational assets and services

ADM – Asset Definition and Management

RRD – Resilience Requirements Development

RRM – Resilience Requirements Management

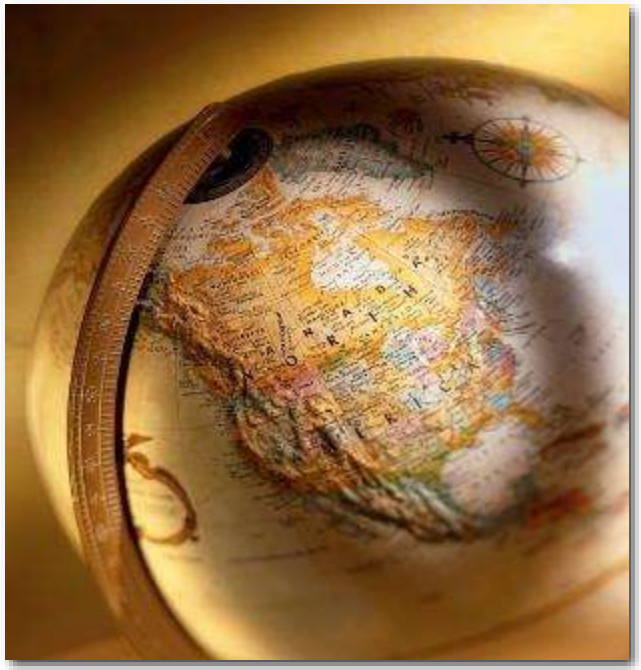
SC – Service Continuity

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

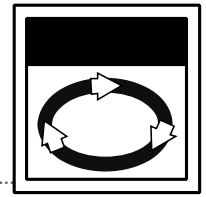
HRM – Human Resource Management

RISK – Risk Management

COMM – Communications

OTA – Organizational Training and Awareness

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

Process institutionalization in CERT-RMM

Process

A set of practices performed to achieve a given purpose

Utilizes people and technology

Defined at many levels

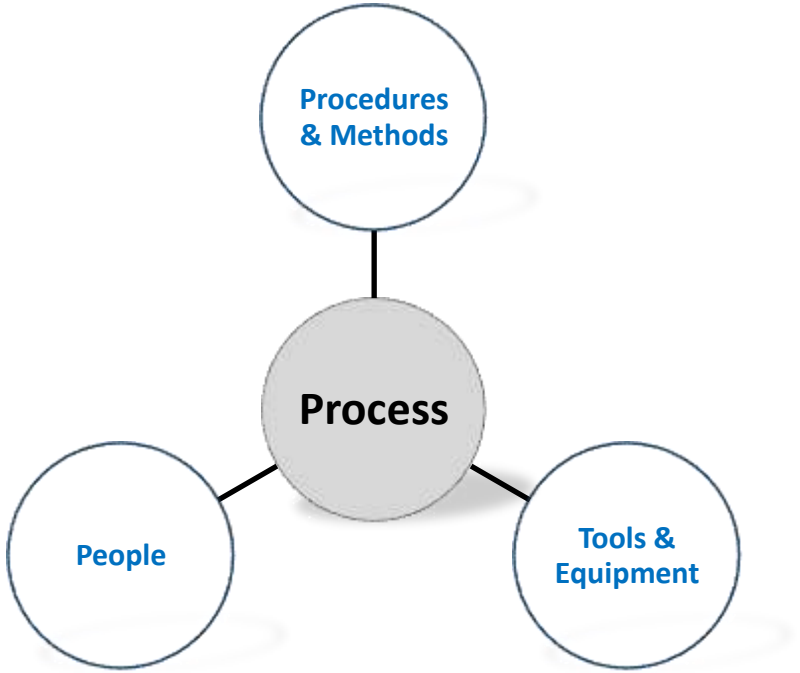
- Higher order “process” such as the “software engineering process” or the “resilience management process”
- Lower order “process” such as the invoicing process or the check cashing process

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

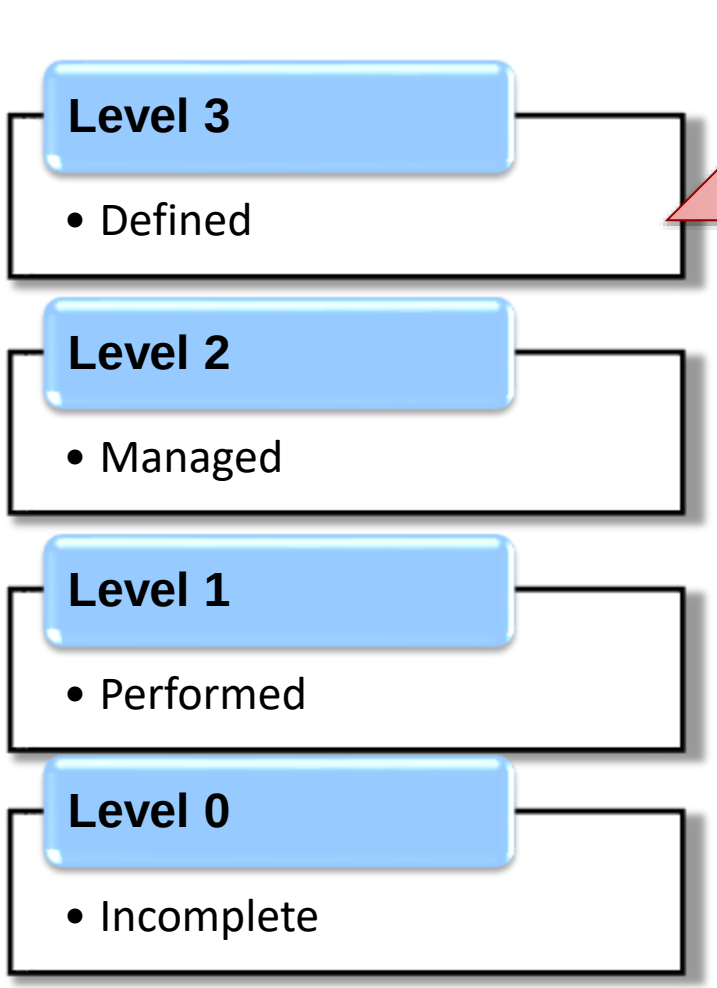
Process institutionalization in CERT-RMM

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

Processes are acculturated, defined, measured, and governed

Practices are performed

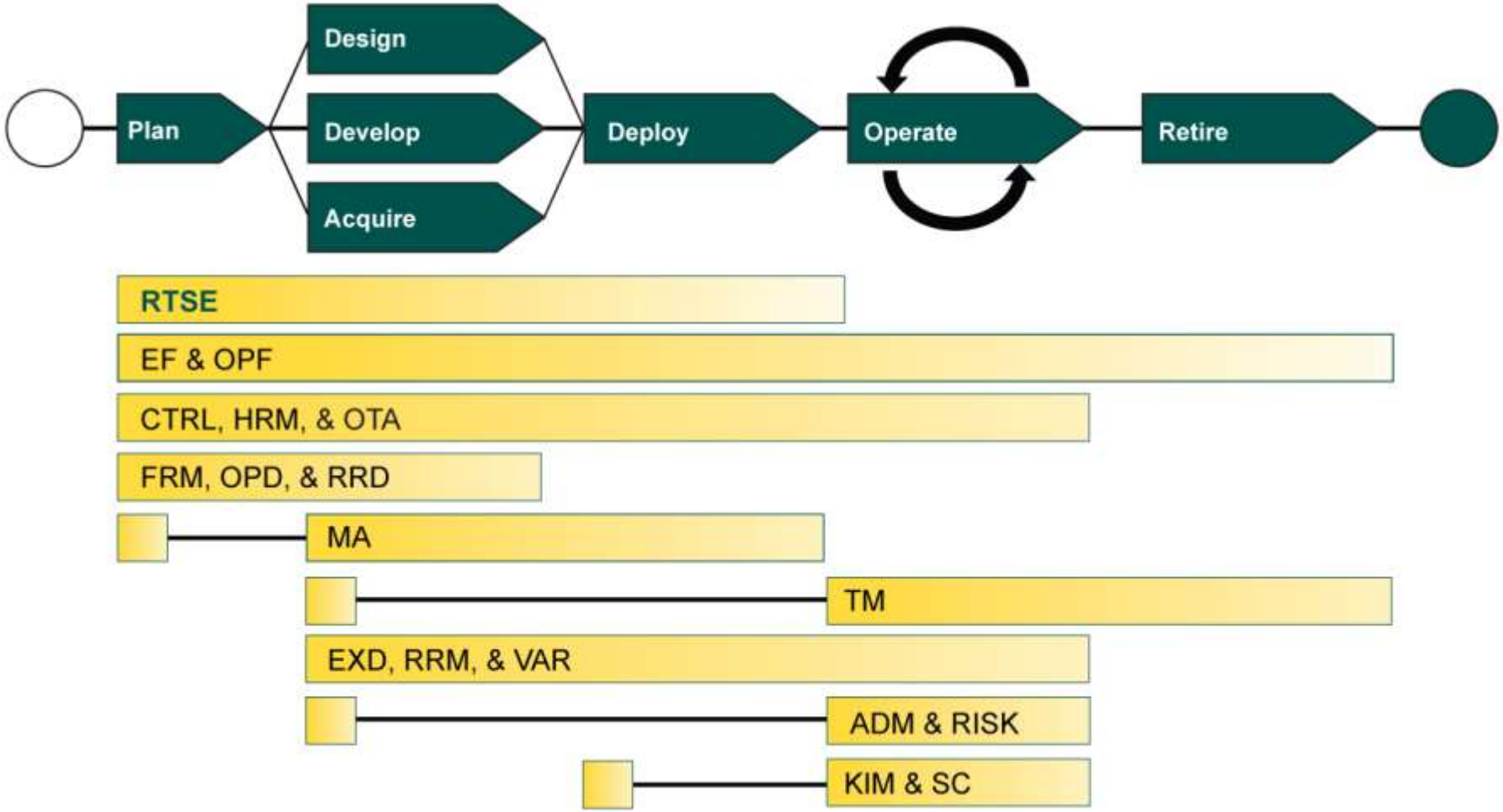
Practices are incomplete



Higher degrees of institutionalization translate to more stable processes that

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

CERT-RMM for software assurance



Example: Selected PAs 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

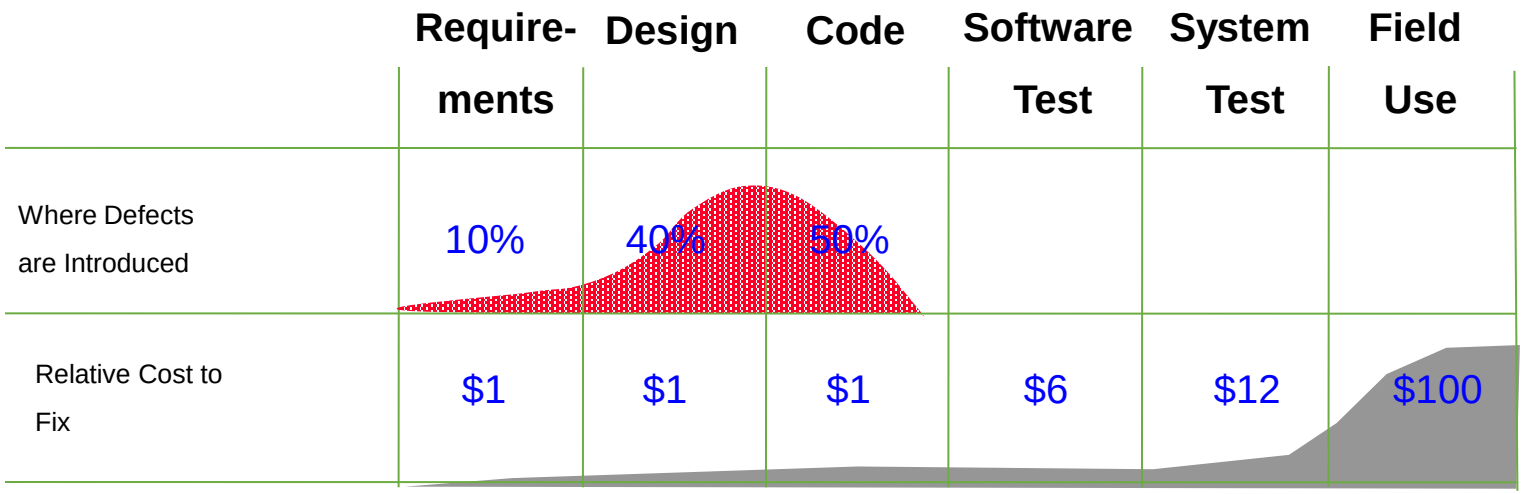
Measurement and Analysis
Monitoring
Organizational Process Focus
Organizational Process Definition
Organizational Training & Awareness
People Management
Resiliency Requirements Development
Resiliency Requirements Management
Resilient Technical Solution Engr.
Risk Management
Service Continuity
Technology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

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

Software & IT Services Quality
Defects : Insertion Pattern & Cost of Removal

Capability and maturity models (CMMI)

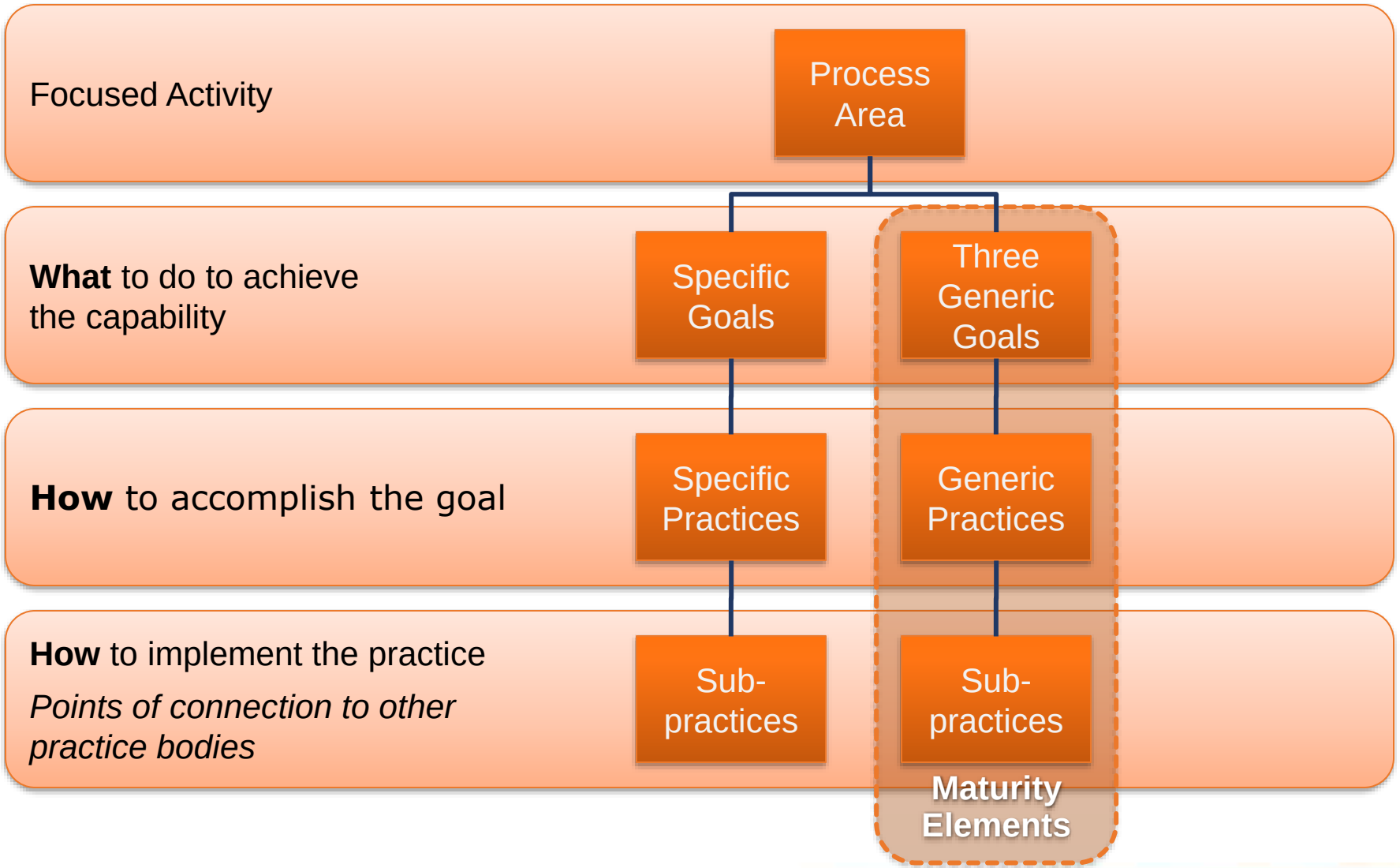


Source: SEPG Asia Pacific 2009
presented by Ravindra Nath, KUGLER MAAG CIE GmbH

But…this is also about SW Quality? What is the cost…

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

CERT-RMM Process Area Architecture



Generic goals and practices

Generic Goal 1
GG1 Achieve Specific Goals

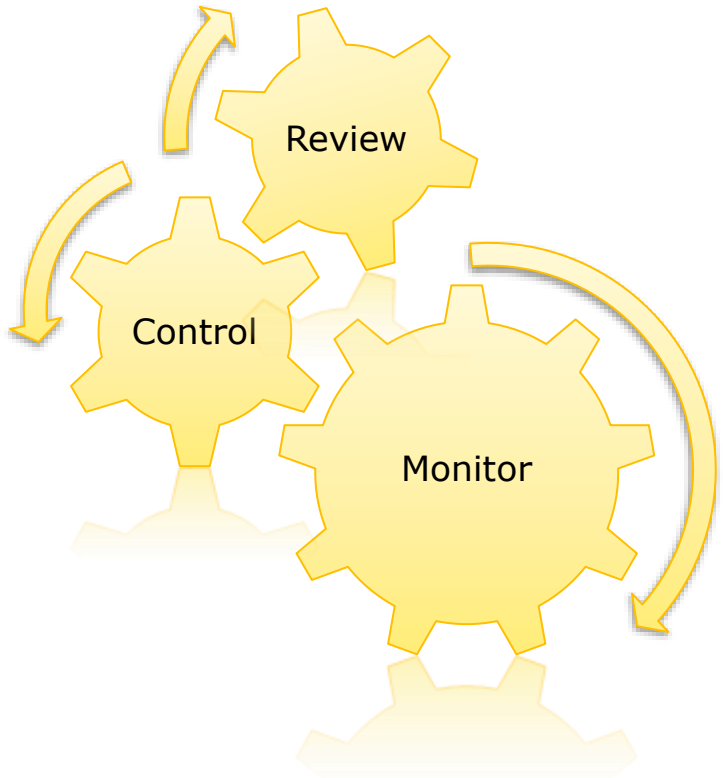
Number	Generic Practice
GG1.GP1	GG1.GP1 Perform Specific Practices

Generic Goal 3
GG3 Institutionalize a Defined Process

Number	Generic Practice
GG3.GP1	Establish a Defined Process
GG3.GP2	Collect Improvement Information

Generic goals and practices (as in CMMI models)

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

DO NOT FORGET!!!

Process ≠ Bureaucracy

Process = (Organized) Work

Selected CERT-RMM process areas

RTSE – Resilient Technical Solution Engineering

Purpose:

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

Software and systems are pervasive organizational assets that automate services and support business processes to help organizations meet their missions. The importance of resilient technical solutions—**software and systems that resist threats, function satisfactorily in the face of adversity, and continue to help services meet their missions during times of stress**—cannot be overstated.

Resilient software and systems **do not become survivable and resistant to threat without an organizational commitment to address resilience throughout the development process**.

These assets must be specifically designed and developed with consideration of the types of threats they will face, the operating conditions and changing risk environment in which they will operate, and the priority and sustainment needs of the services they support.

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 Specific Goals & Parctices

RTSE:SG1 Establish Guidelines for Resilient Technical Solution Development

Guidelines are developed to ensure proper consideration of resilience activities and controls in all phases of the life cycle

RTSE:SG1.SP1 Identify General Guidelines

RTSE:SG1.SP2 Identify Requirements Guidelines

RTSE:SG1.SP3 Identify Architecture and Design Guidelines

RTSE:SG1.SP4 Identify Implementation Guidelines

RTSE:SG1.SP5 Identify Assembly and Integration Guidelines

RTSE:SG2 Develop Resilient Technical Solution Development Plans

Plans for addressing resilience in the development life cycle are created, based on documented guidelines

RTSE:SG2.SP1 Select and Tailor Guidelines

RTSE:SG2.SP2 Integrate Selected Guidelines with a Defined Software and System Development Process

RTSE:SG3 Execute the Plan

Progress against the plan for developing resilient software and systems is monitored throughout the development life cycle

RTSE:SG3.SP1 Monitor Execution of the Development Plan

RTSE:SG3.SP2 Release Resilient Technical Solutions into Production

Example: RTSE:SG1.SP4 Identify Implementation Guidelines

Typical work products

1. Coding guidelines for resilient software
2. Testing guidelines for resilient software
3. Testing guidelines for resilient systems

Subpractices

1. **Identify coding guidelines for the development of resilient software.**

- risk analysis during coding
- threat analysis during coding
- attack surface evaluation and mitigation
- secure design patterns at the implementation level
- secure coding standards (language-specific)
- code checklists, reviews, inspections, and static and dynamic code analysis, including tools to support these, which can be used to verify

...

2. Identify testing guidelines for the development of resilient software.

- risk analysis during software testing
- threat analysis during software testing
- attack surface reevaluation and mitigation

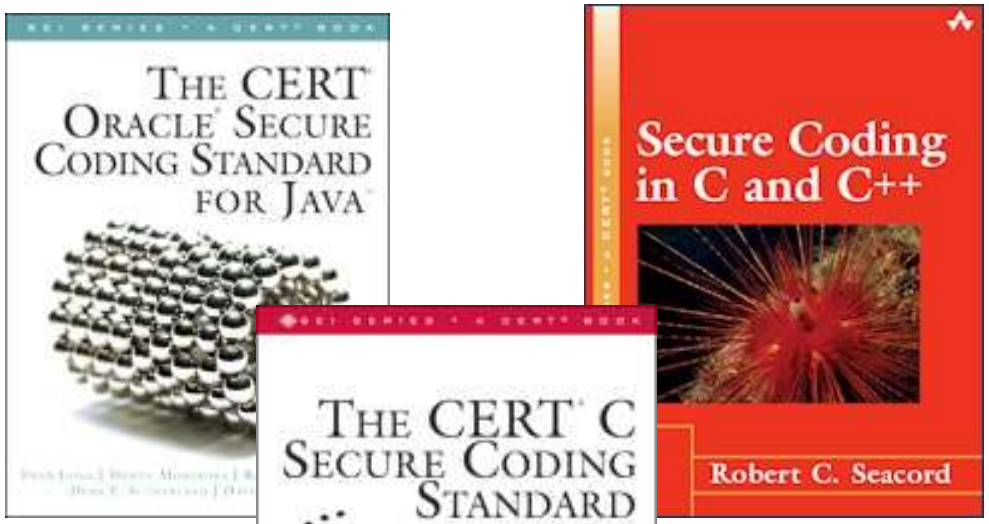
3. Identify testing guidelines for the development of resilient systems.

- risk analysis during system testing
- threat analysis during system testing
- attack surface reevaluation and mitigation
- at the system level, methods for
    - resilience requirements functional testing
    - black box testing that focuses on the system's externally visible behavior
    - fuzz testing
    - penetration testing
    - testing for specific vulnerabilities as well as vulnerability regression testing
    - application of threat and attack models
    - integration testing

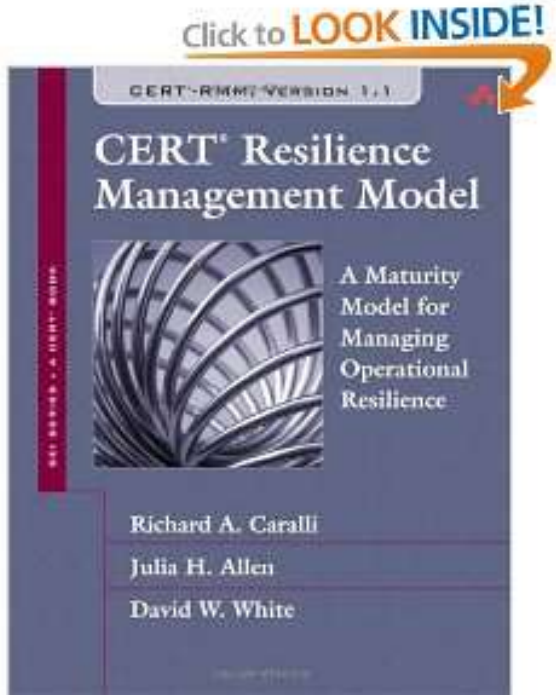
Remember: Computer Emergency Response Team

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]



Secure coding: top 10 recommendations

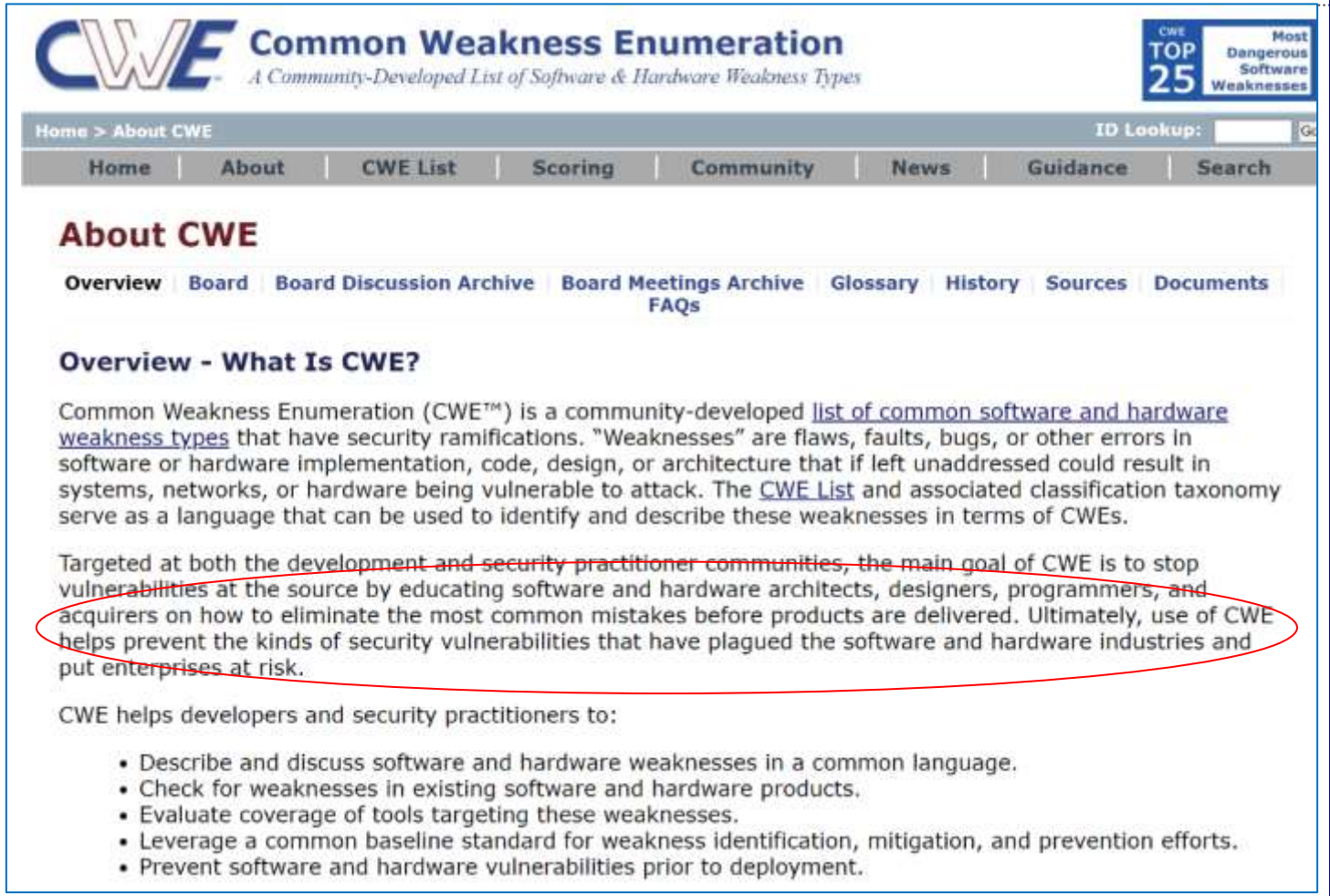
1. **Validate input** - be suspicious of most external data sources
2. **Heed compiler warnings –** compile highest warning level available
3. **Architect and design for security policies –** e.g. divide the systems into intercommunicating subsystems, each with an appropriate privilege set
4. **Keep 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**
- **Study, Model and Simulate threats (and attacks) >>>** **Pen Testing (Red Teaming)**

Stop vulnerabilities at the source

https://cwe.mitre.org/about/index.html



CWE Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

CWE TOP 25 Most Dangerous Software Weaknesses

Home > About CWE ID Lookup:

Home | About | CWE List | Scoring | Community | News | Guidance | Search

About CWE

Overview | Board | Board Discussion Archive | Board Meetings Archive | Glossary | History | Sources | Documents | FAQs

Overview - What Is CWE?

Common Weakness Enumeration (CWE™) is a community-developed list of common software and hardware weakness types that have security ramifications. "Weaknesses" are flaws, faults, bugs, or other errors in software or hardware implementation, code, design, or architecture that if left unaddressed could result in systems, networks, or hardware being vulnerable to attack. The CWE List and associated classification taxonomy serve as a language that can be used to identify and describe these weaknesses in terms of CWEs.

Targeted at both the development and security practitioner communities, the main goal of CWE is to stop vulnerabilities at the source by educating software and hardware architects, designers, programmers, and acquirers on how to eliminate the most common mistakes before products are delivered. Ultimately, use of CWE helps prevent the kinds of security vulnerabilities that have plagued the software and hardware industries and put enterprises at risk.

CWE helps developers and security practitioners to:

- Describe and discuss software and hardware weaknesses in a common language.
- Check for weaknesses in existing software and hardware products.
- Evaluate coverage of tools targeting these weaknesses.
- Leverage a common baseline standard for weakness identification, mitigation, and prevention efforts.
- Prevent software and hardware vulnerabilities prior to deployment.

CWE refers to the types of software weaknesses, rather than specific instances of vulnerabilities within products or systems. Essentially, **CWE** is a "dictionary" of software vulnerabilities, while **CVE** is a list of known instances of vulnerability **for** specific products or systems.

Examples of Weaknesses

Software

- buffer overflows, format strings, etc.
- structure and validity problems
- common special element manipulations
- channel and path errors
- handler errors
- user interface errors
- pathname traversal and equivalence errors
- authentication errors
- resource management errors
- insufficient verification of data
- code evaluation and injection
- randomness and predictability

Hardware

- core and compute issues typically associated with CPUs, Graphics, Vision, AI, FPGA, and uControllers
- privilege separation and access control issues related to identity and policy, shared resources, locking controls, registers, and other features and mechanisms
- power, clock, and reset concerns related to voltage, electrical current, temperature, clock control, and state saving/restoring

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

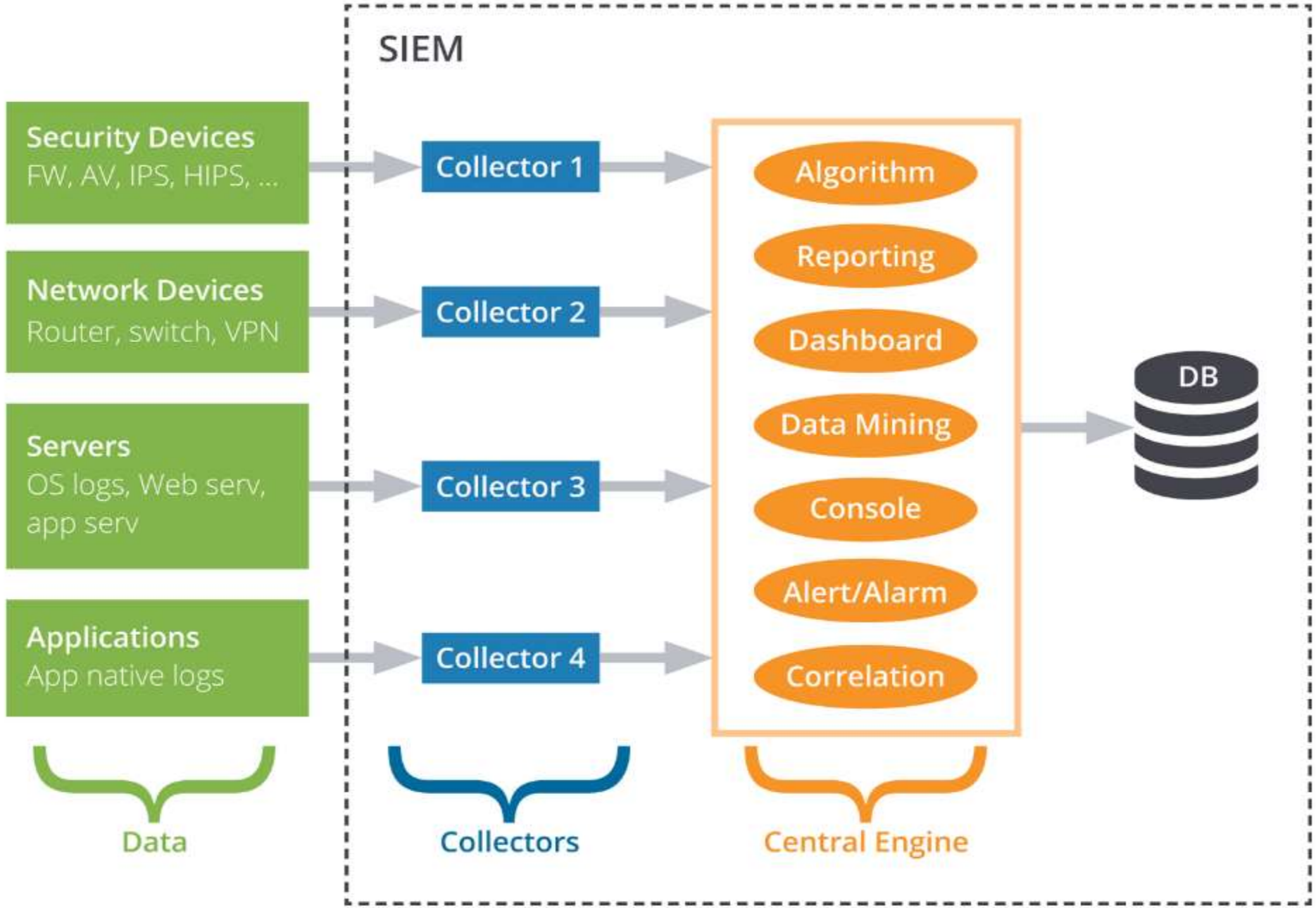
(2) efficiently managing logs.

These objectives were respectively called **security event management (SEM)** and **security information managemen (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.).

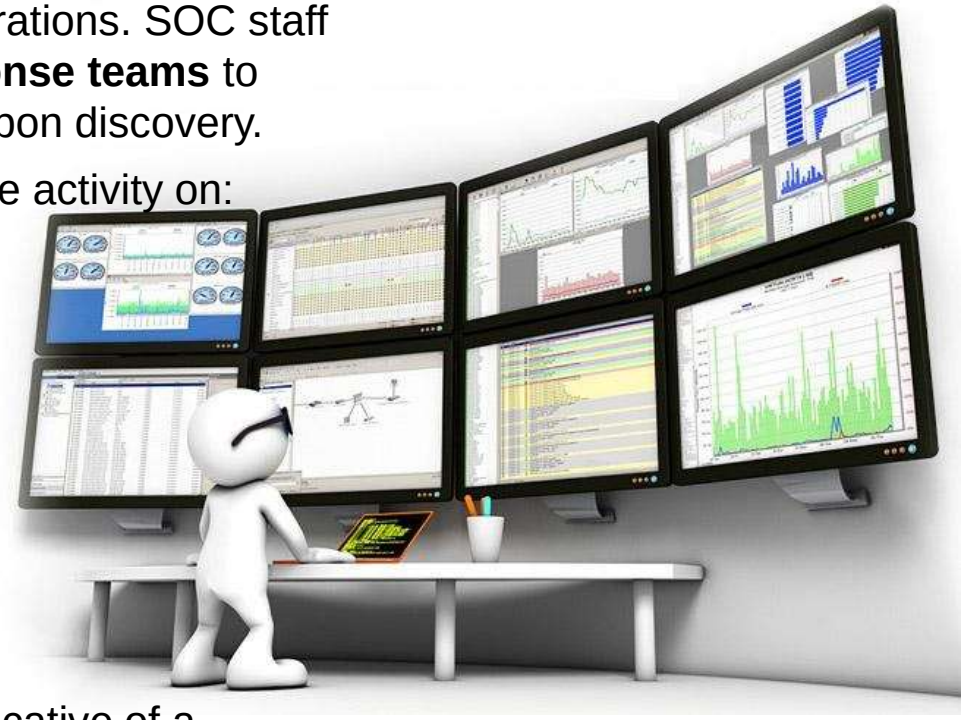
When successfully deployed and configured, a SIEM helps organizations:

- 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

Security Operations Center

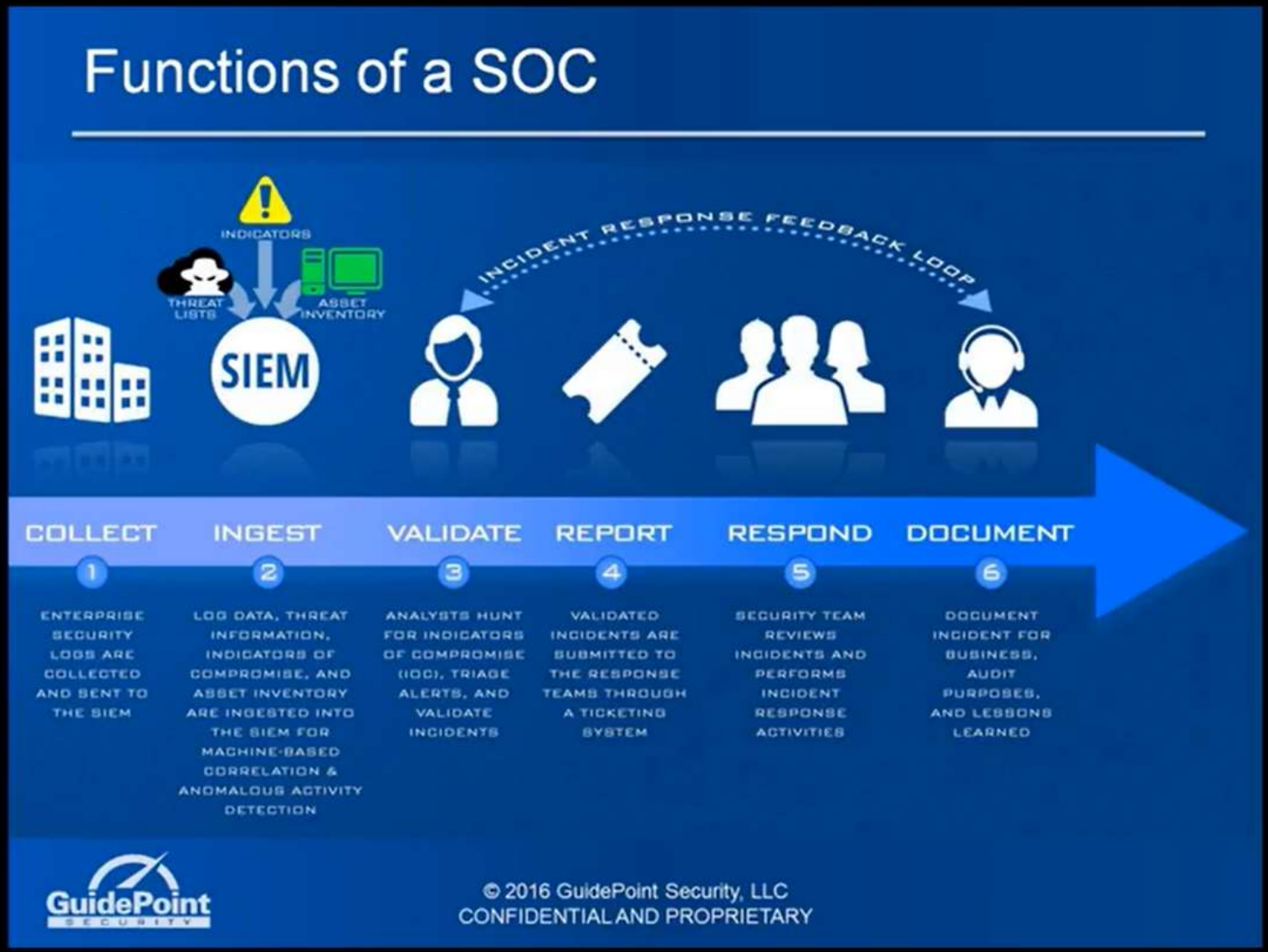
A security operations center (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work close with **organizational incident response teams** to ensure security issues are addressed quickly upon discovery.



Security operations centers monitor and analyze activity on:

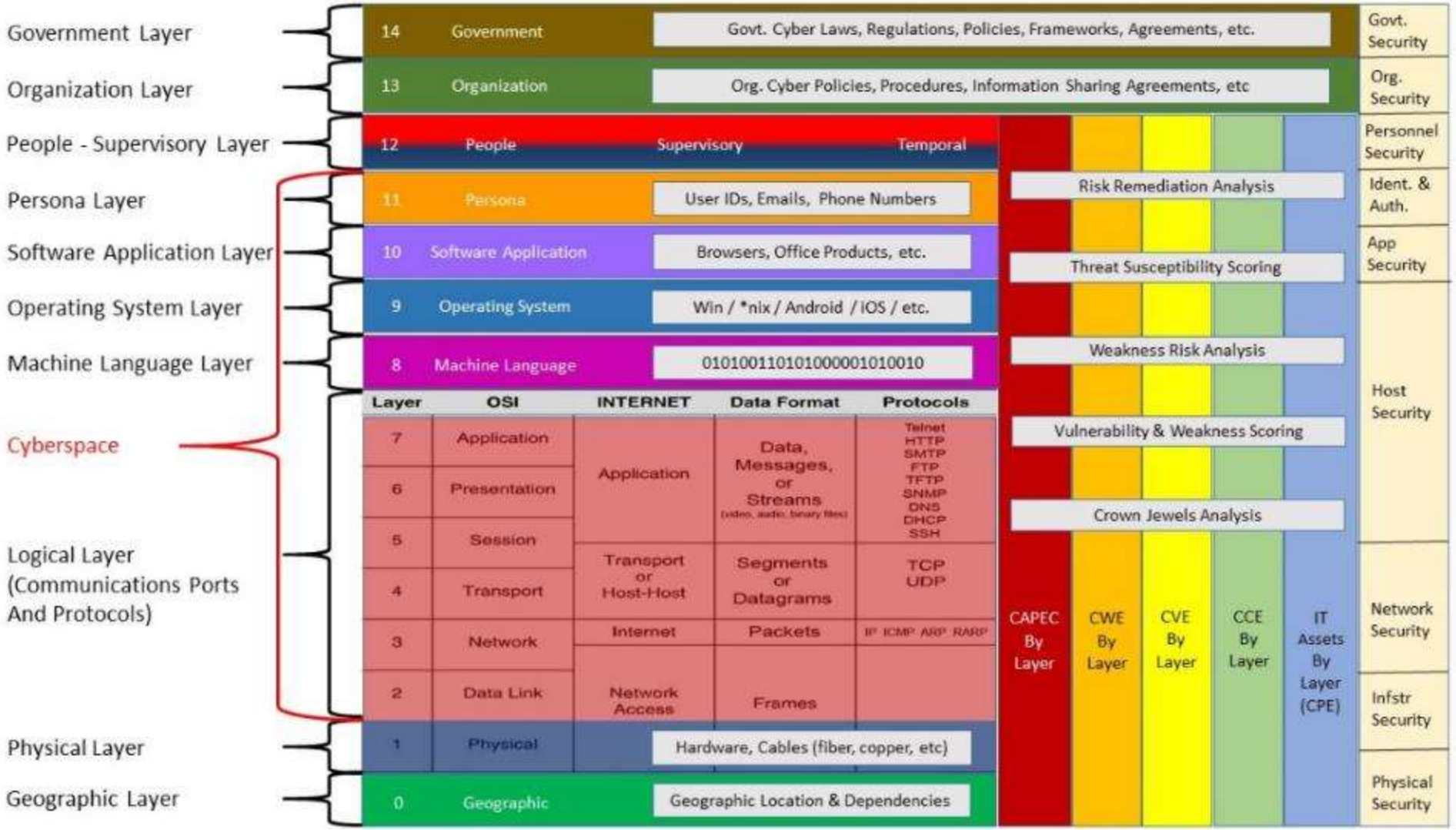
- Networks
- Servers
- Endpoints
- Databases
- Applications
- Websites
- and other systems

looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

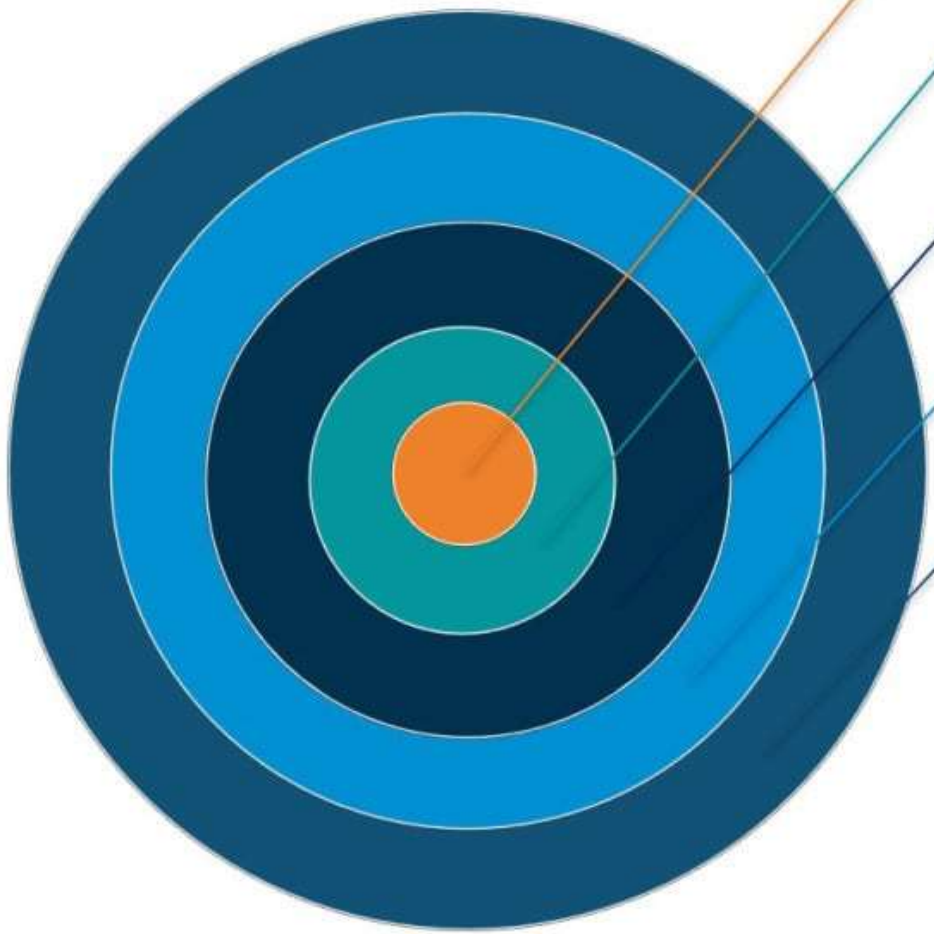


https://solutionsreview.com/security-information-event-management/694/

Remember: Cyber Terrain



Defense-in-depth



Application and Data Security: Timely patching, encrypting sensitive data, etc.

Host Security: Timely patching of AV, restricting unwanted services, dynamic whitelisting, write and read protection

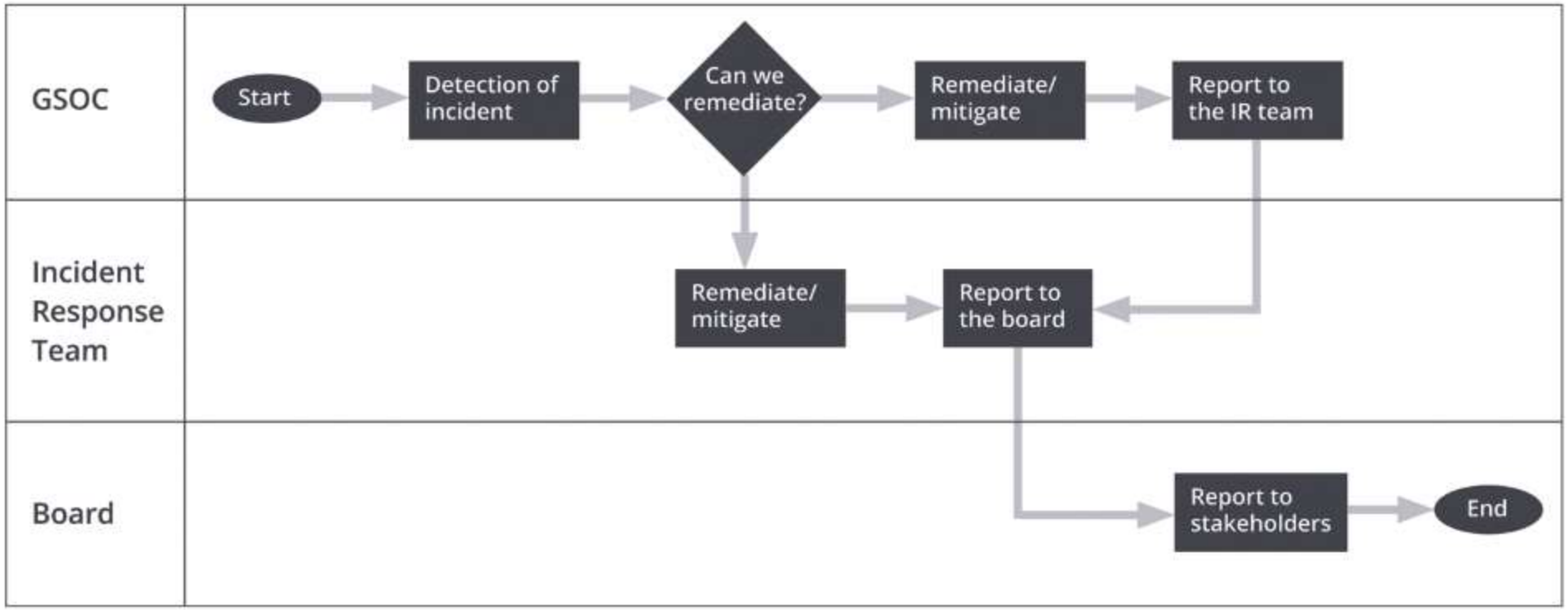
Network Security (Corporate + ICS): Firewall, sandboxing, IDS/IPS, VPNs, monitoring and alerting

Physical Security: ID cards, CCTV, fences, etc.

Policy and Procedures: Risk management, incident response management, supply chain management, audit and assessment, training and awareness

monitor-and-respond strategy

Security Operation Center [SOC]



Reacting upon incident flow chart.

SIEM/SOC as TARGET

17 December 2020

ZDNet | SCANDINAVIA | AFRICA | UK | ITALY | SPAIN | MORE | NEWSLETTERS | ALL WRITERS

MUST READ: US, China or Europe? Here's who is really winning the global race for AI

Third malware strain discovered in SolarWinds supply chain attack

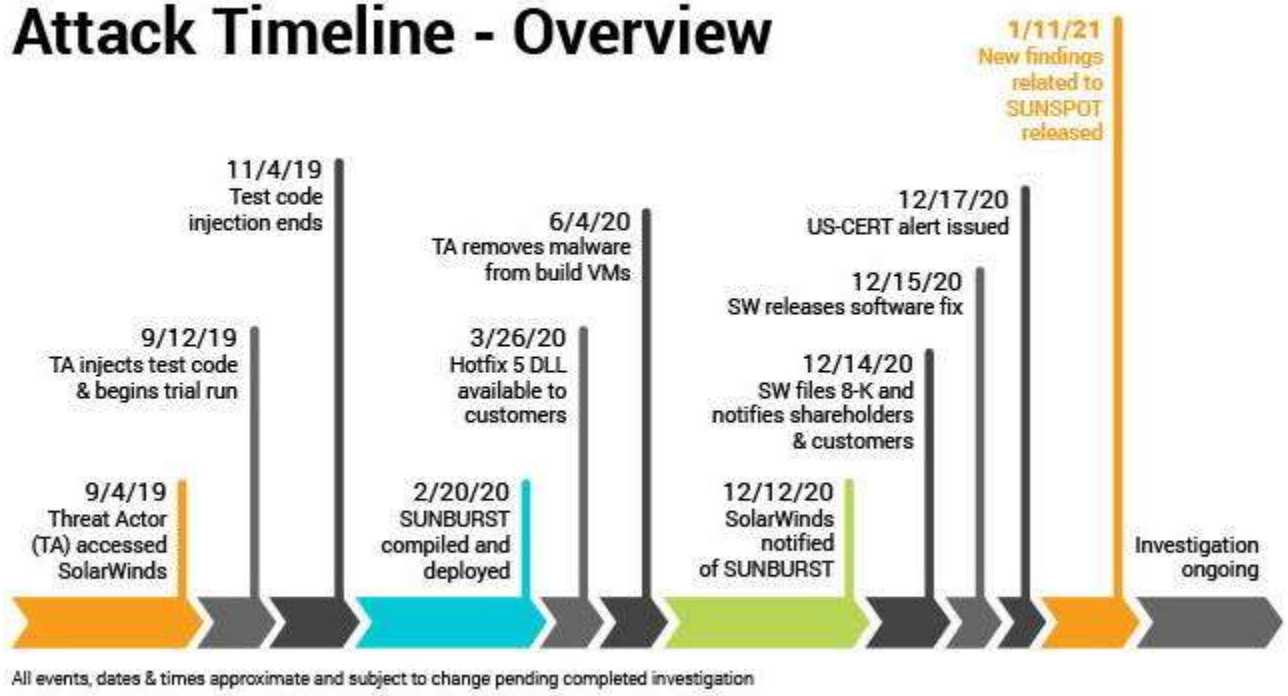
CrowdStrike, one of the two security firms formally investigating the hack, sheds some light on how hackers compromised the SolarWinds Orion app build process.

[Third malware strain discovered in SolarWinds supply chain attack | ZDNet]

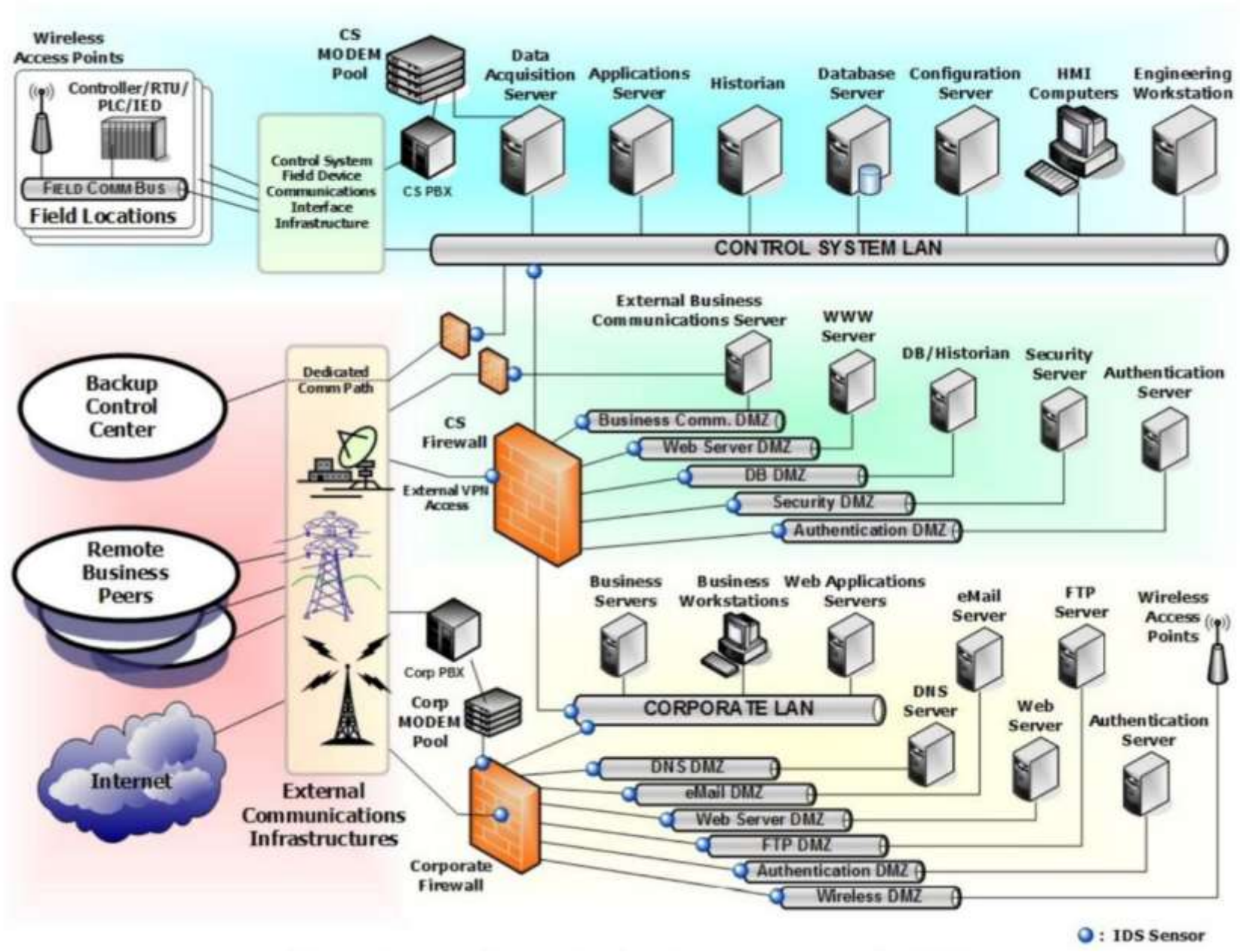
CODE OVERLAP WITH TURLA MALWARE

On top of this, security firm Kaspersky also published its own findings earlier in the day in a separate report.

Kaspersky, which was not part of the formal investigation of the SolarWinds attack but still analyzed the malware, said that it looked into the Sunburst malware source code and found code overlaps between Sunburst and Kazuar, a strain of malware linked to the Turla group, Russia's most sophisticated state-sponsored cyber-espionage outfit.

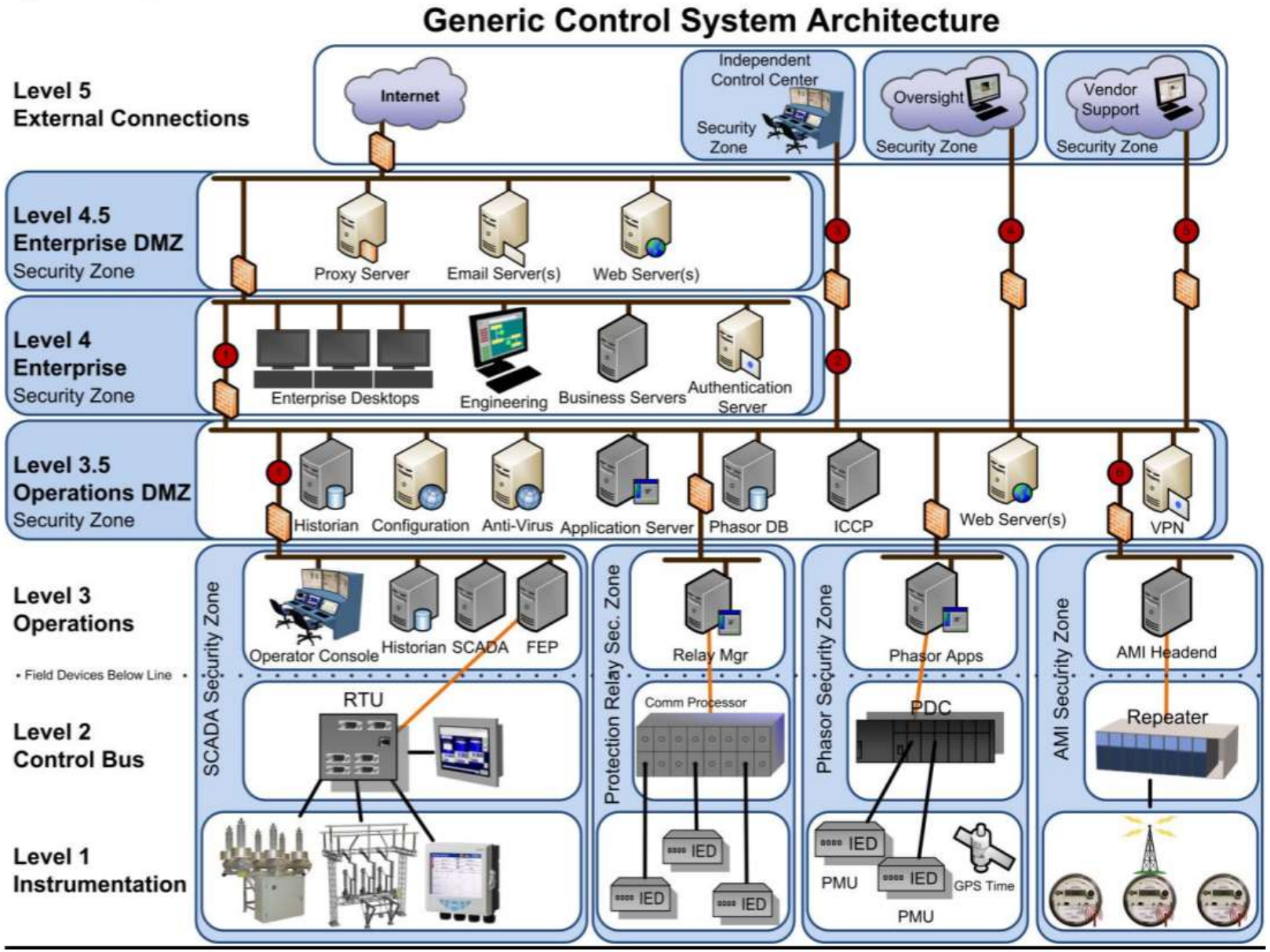


Example Defense-in-Depth with IDS (Intrusion Detection System)



Example: Generic SCADA Architecture

Figure 2. Proposed SCADA Architecture



The State of SCADA HMI Vulnerabilities

TREND MICRO

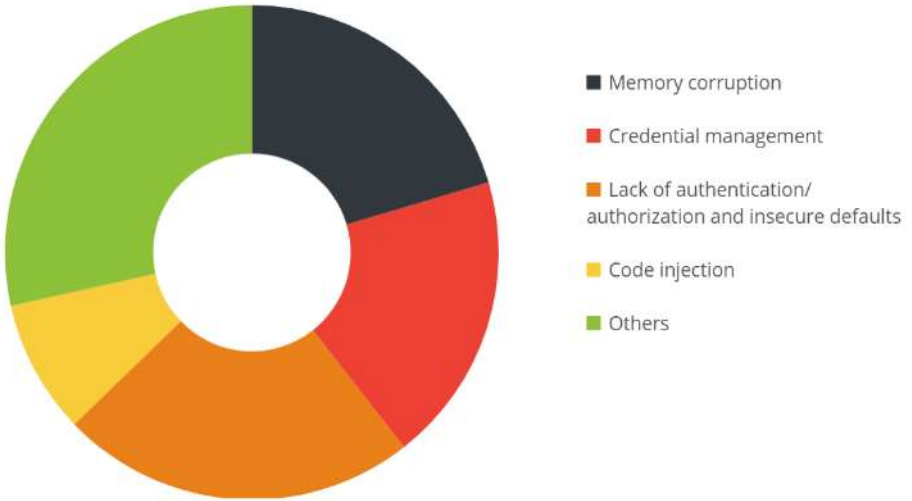
Produkty Rozwiązania Dlaczego warto wybrać Trend Micro Bac

Dla firm | Dla domu

Most Common HMI Vulnerability Categories

We at the Trend Micro Zero Day Initiative (ZDI) Team examined the current state of SCADA HMI security by reviewing all publicly disclosed vulnerabilities in SCADA software that have been fixed from 2015 and 2016, including 250 vulnerabilities acquired through the ZDI program.

We found that most of these vulnerabilities are in the areas of memory corruption, poor credential management, lack of authentication/authorization and insecure defaults, and code injection bugs, all of which are preventable through secure development practices.



Attacking SCADA Through HMIs

SCADA systems run the world's various critical infrastructure sectors and are thus inherently attractive to different threat actors. Threat actors can use their access to SCADA systems to gather information such as a facility's layout, critical thresholds, or device settings for use in later attacks. Sabotage, including disruption of services or triggering dangerous and even lethal situations involving flammable or critical resources, represent an undesirable extreme.

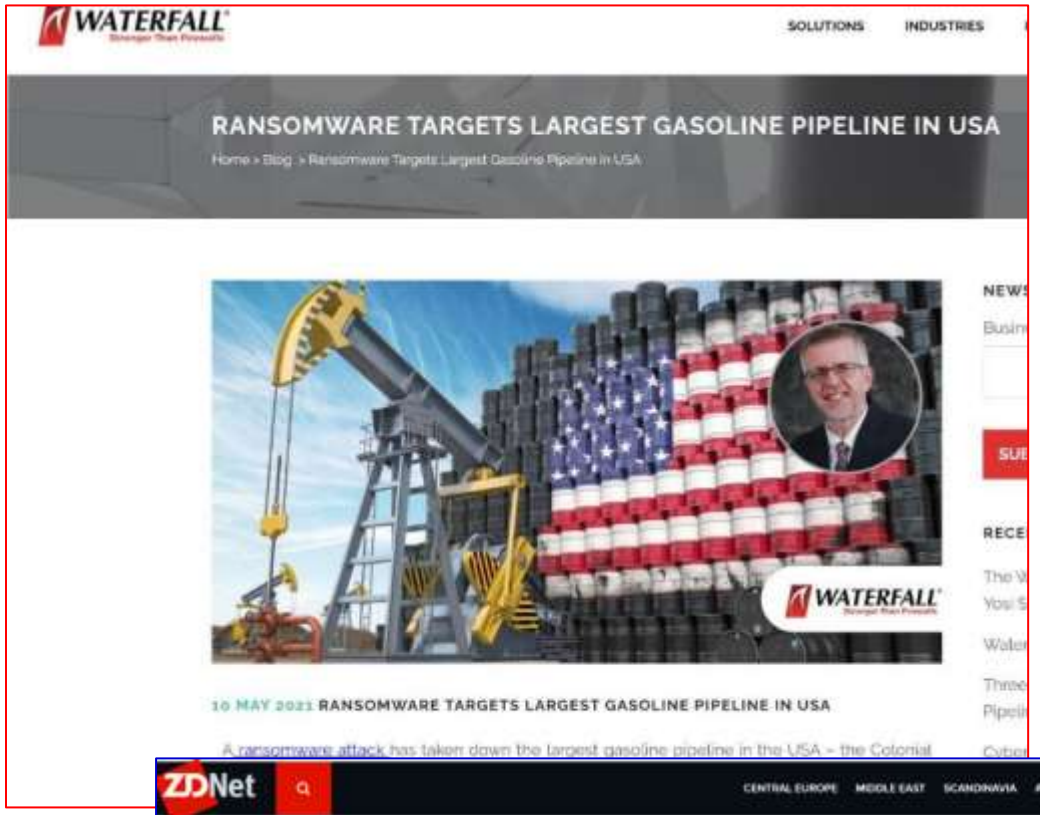
14 Major SCADA Attacks and What You Can Learn From Them

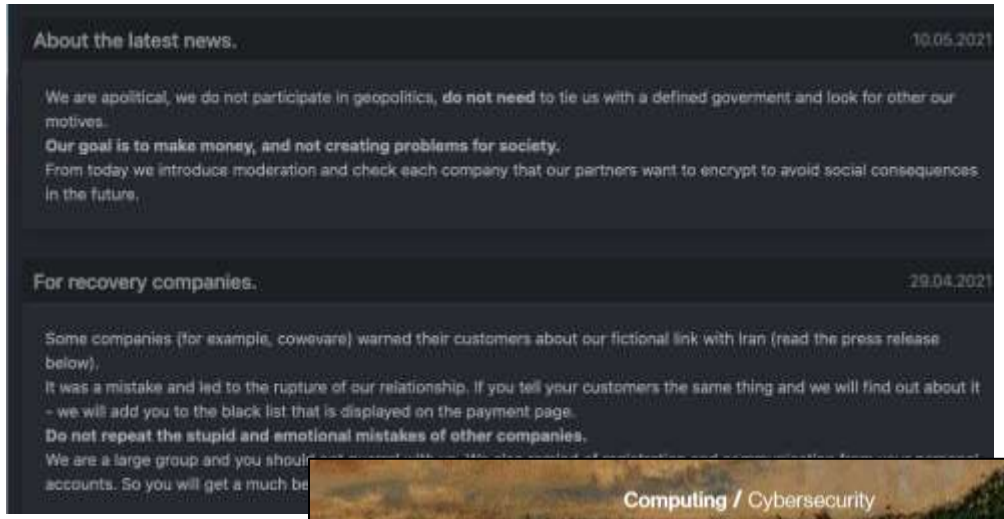
https://www.dpstele.com/blog/major-scada-hacks.php

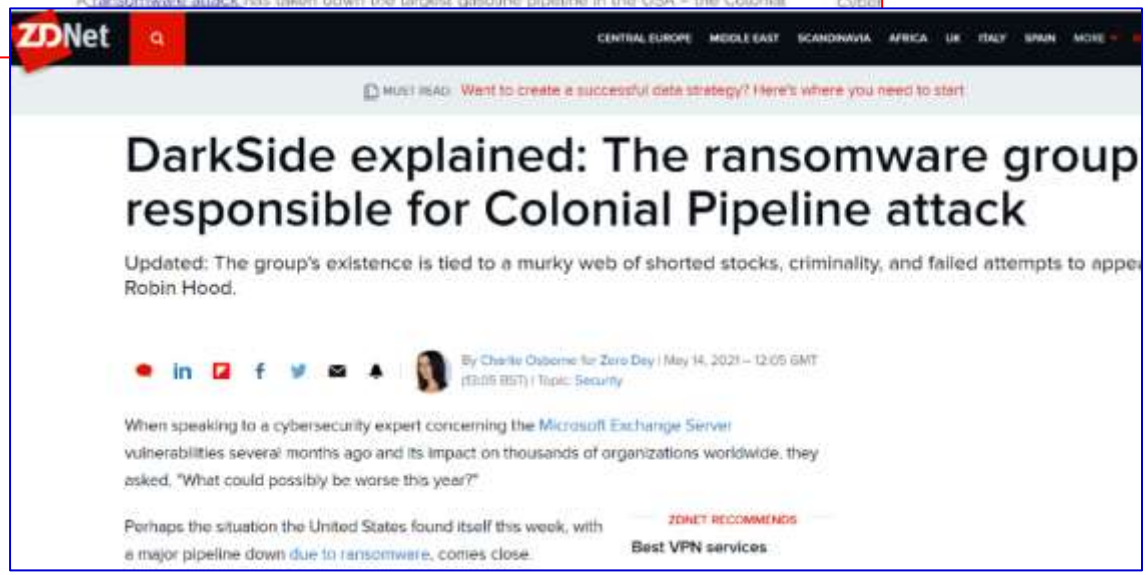
10 MAY 2021 – Biggest Impact in History

RANSOMWARE TARGETS LARGEST GASOLINE PIPELINE IN USA

https://www.bankinfosecurity.com/fbi-darkside-ransomware-used-in-colonial-pipeline-attack-a-16555







https://www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/

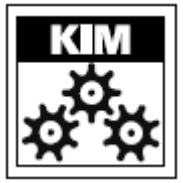
https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/

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


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

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

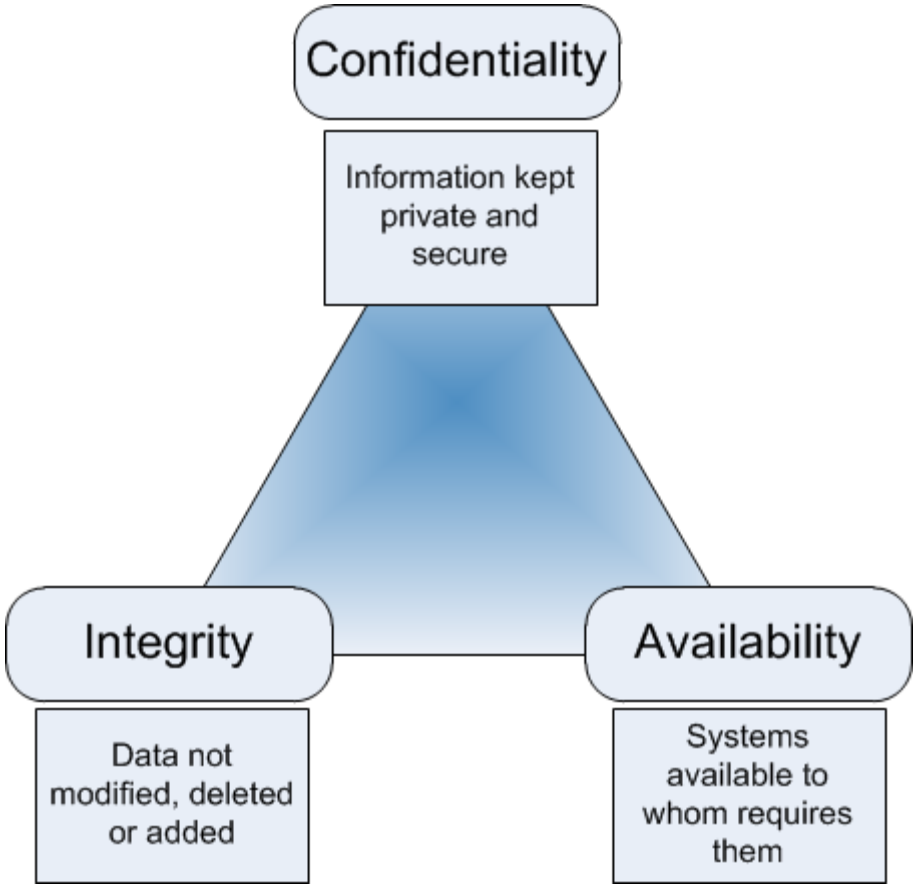
privacy

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

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

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

General methodology - ADM: Asset Definition and Management

Goals **Practices**

ADM:SG1 Establish Organizational Assets

ADM:SG1.SP1 Inventory Assets

ADM:SG1.SP2 Establish a Common Understanding

ADM:SG1.SP3 Establish Ownership and Custodianship

ADM:SG2 Establish the Relationship Between Assets and Services

ADM:SG2.SP1 Associate Assets with Services

ADM:SG2.SP2 Analyze Asset-Service Dependencies

ADM:SG3 Manage Assets

ADM:SG3.SP1 Identify Change Criteria

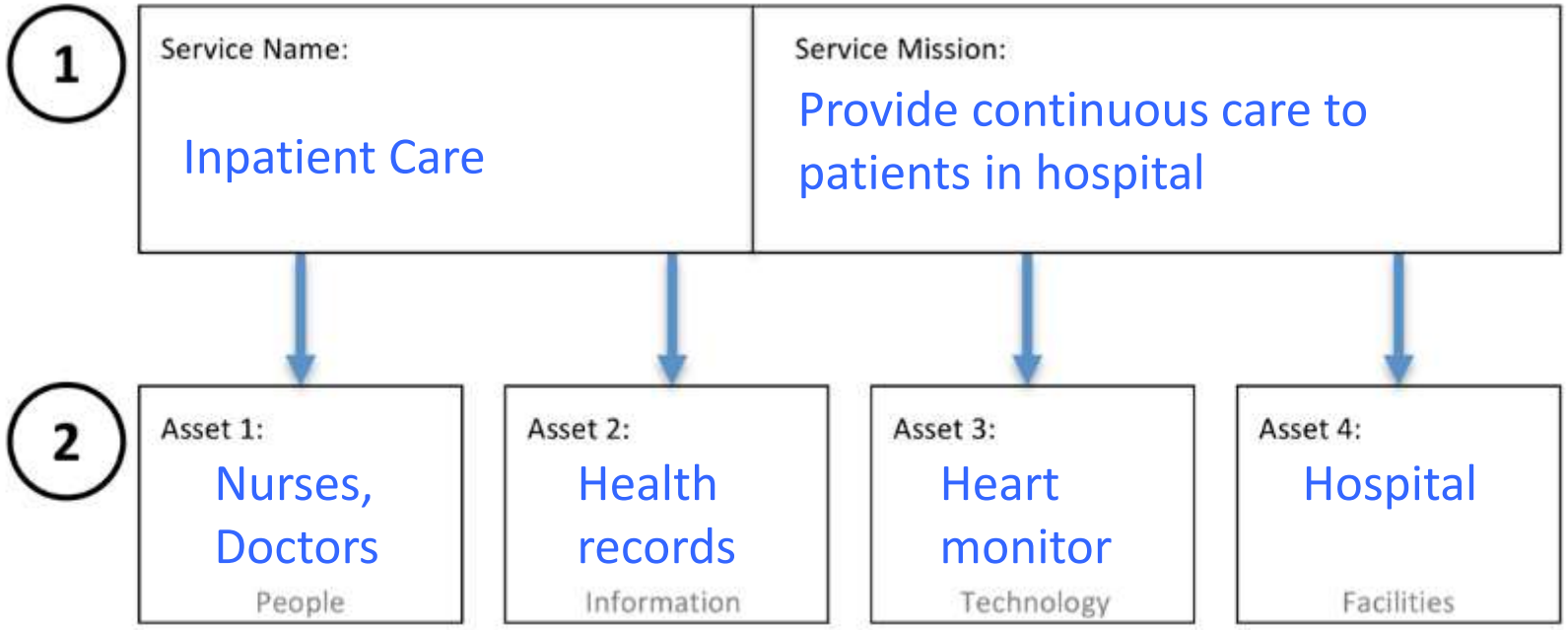
ADM:SG3.SP2 Maintain Changes to Assets and Inventory

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

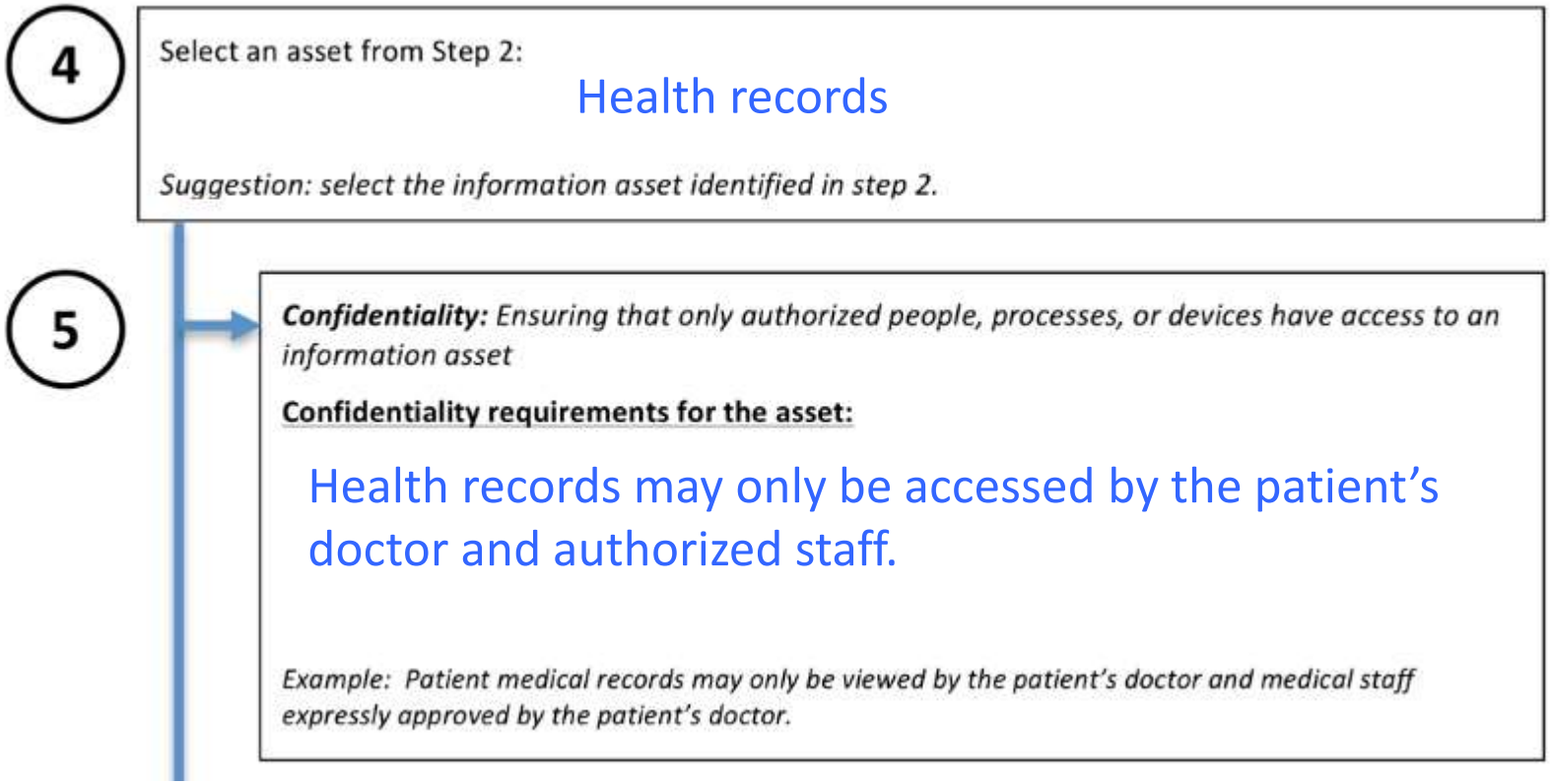
C. What would be the impact on the service mission if the asset were disrupted?

Patients might not receive appropriate or timely care

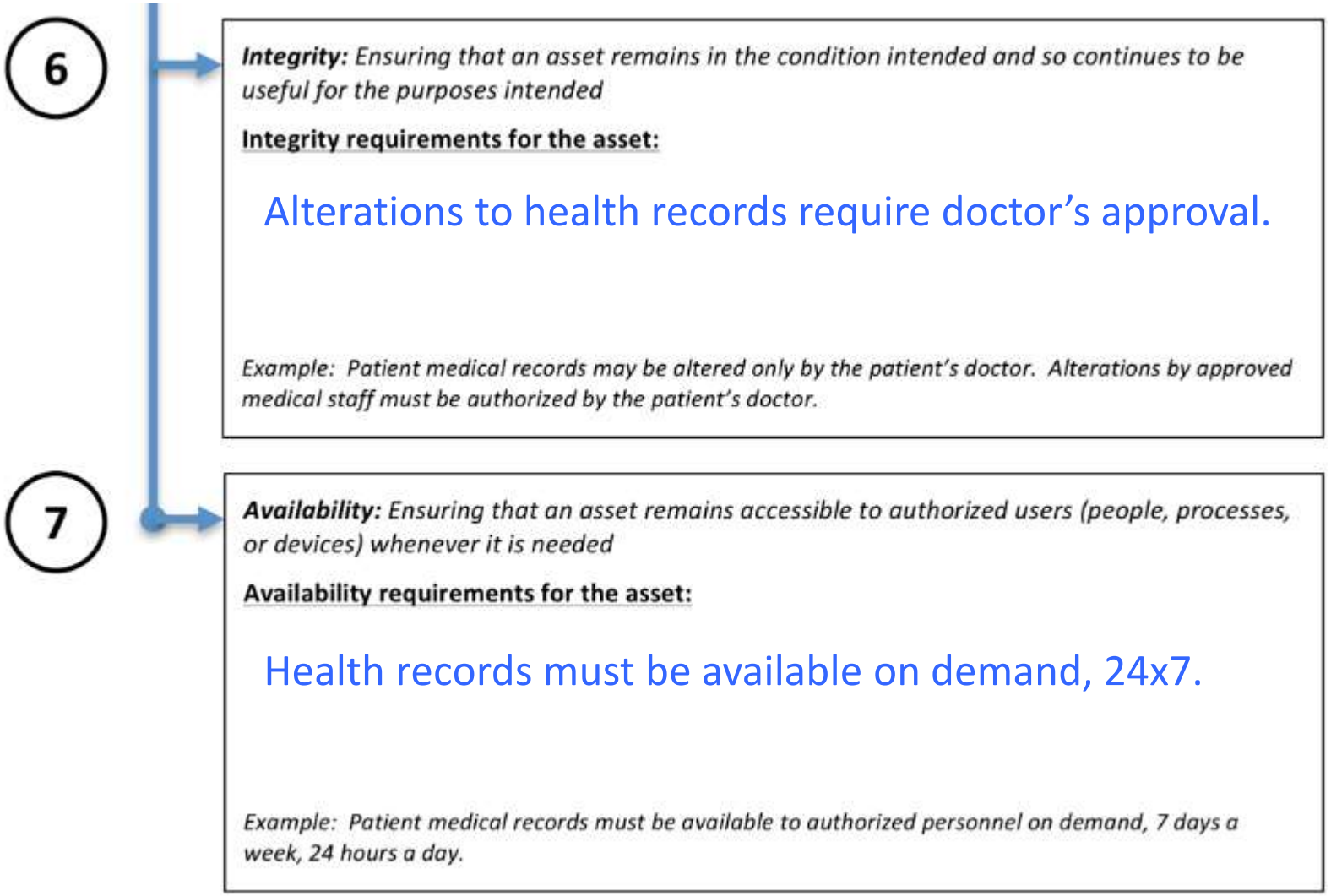
D. What consequences, if any, would the organization experience? Consider a) reputational harm, b) impacts to life, safety, and health of employees and customers, c) legal fines or penalties, and d) other financial losses.

Potential loss of life, serious reputational and financial harm

Exercise part 2, steps 4 & 5



Exercise part 2, steps 6 & 7



8

Asset from Step 4:	

9

PROTECT	SUSTAIN
Based on the resilience requirements, the <u>protection</u> strategy for this asset is: *Example: The protection strategy for patient medical records is to strictly limit viewing and modification access to authorized personnel.*	**Based on the resilience requirements, the <u>sustainment</u> strategy for this asset is:** *Example: The sustainment strategy is to ensure that authorized medical personnel have access even if the original electronic paper records are unavailable.*
The strategy would be implemented through these controls: *Administrative:* *Example: create and enforce an access policy*	**The strategy would be implemented through these controls:** *Administrative:* *Example: develop, test and maintain continuity plans*
Technical: *Example: require ID/password to access electronic medical records, electronic IDs to access data center*	*Technical:* *Example: Scan all paper records for digital storage; synchronize electronic storage to redundant data center for failover; automatically backup data*
Physical: *Example: lock data center and strictly limit access*	*Physical:* *Example: physically separate primary and secondary data centers; store backups offsite*

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 Multifactor Authentication

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

Multi-Factor Authentication

POSSESION

Access badges, Cell phones, OTPs, Laptops

+

KNOWLEDGE

Passwords, PINs, Answers to security questions

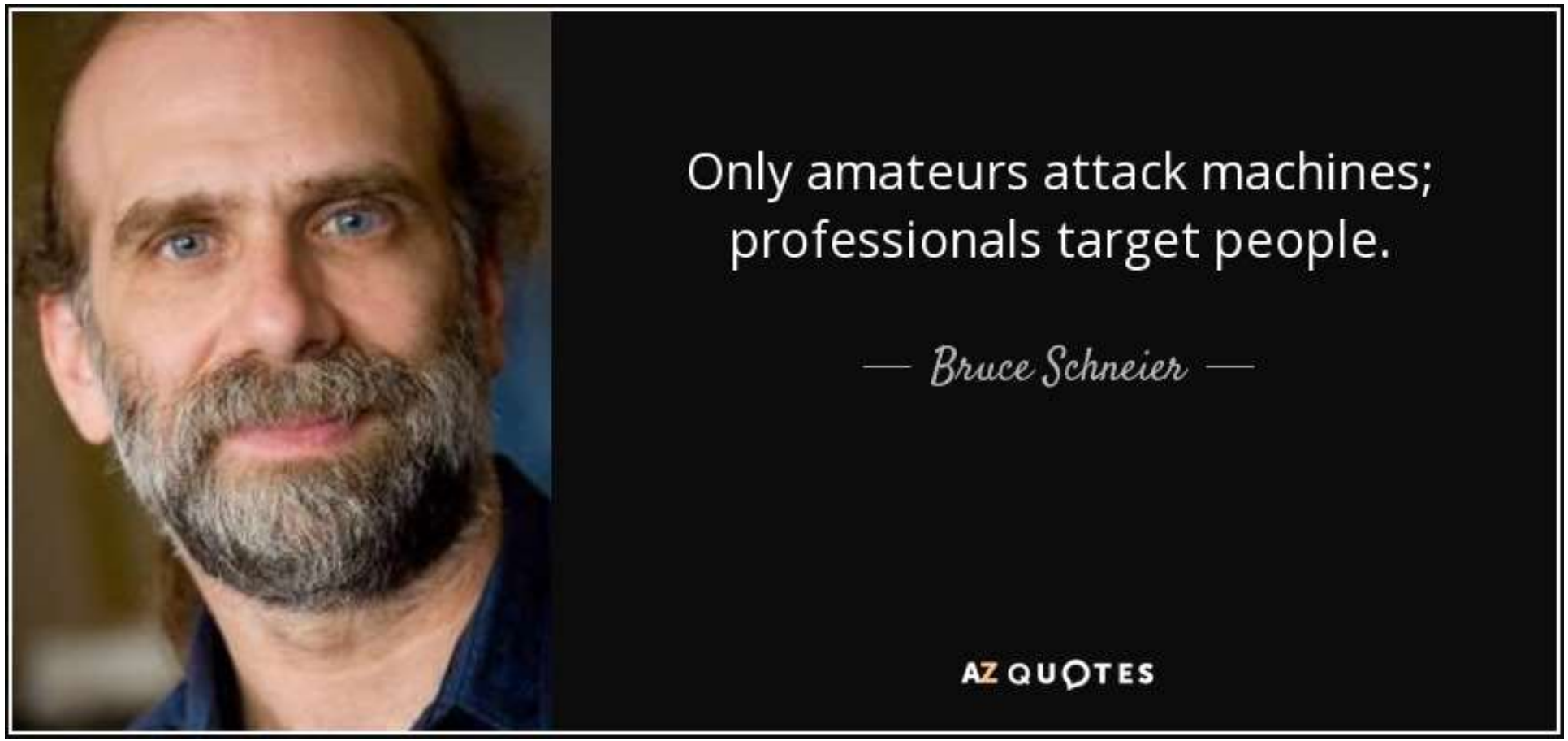
+

BEING

Fingerprint, Iris scanning, other biometrics

Identity Review

Source: Spanning


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

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**...

Additional presentation & exercise on:

ESI European Software Institute Center Eastern Europe

CY RES LAB

SOCIAL ENGINEERING

In computer science, social engineering is “the act of manipulating a person to take an action that may or may not be in the target’s best interest”.

– Cristopher Hadnagy, “Social Engineering: The Art of Human Hacking”

IMPORTANT NOTIONS

- *Social engineering is “always psychological and sometimes technical”*
- *“The psychological aspect of social engineering is what makes the attack, not the technical”*
- *We will focus mostly on the technical aspect, while still acknowledging the psychological factors are leading*
- *It can be mitigated somewhat with technical means*

$ 5 billion stollen

2013-2016 worldwide through SE

PhisMe, 2017. Link

Only about 3% of malware tries to exploit an exclusively technical flaw.
The other 97% instead targets users through SE.

KnowBe4, 2016. Link

91%

Through E-mail
Mimecast, 2018

55%

Emails = Spam
Symantec, 2018

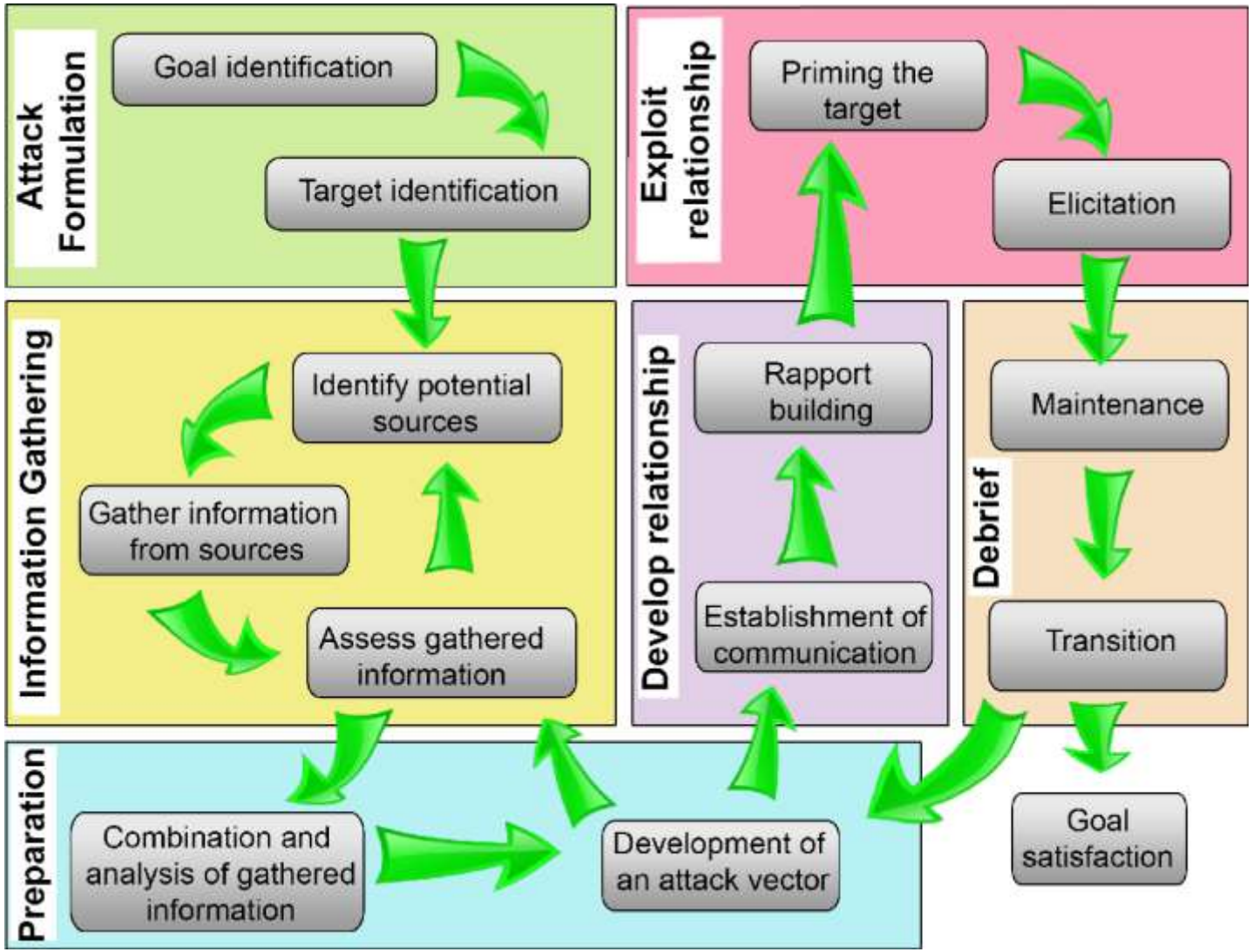
A SUCCESSFUL SOCIAL ENGINEERING ATTACK

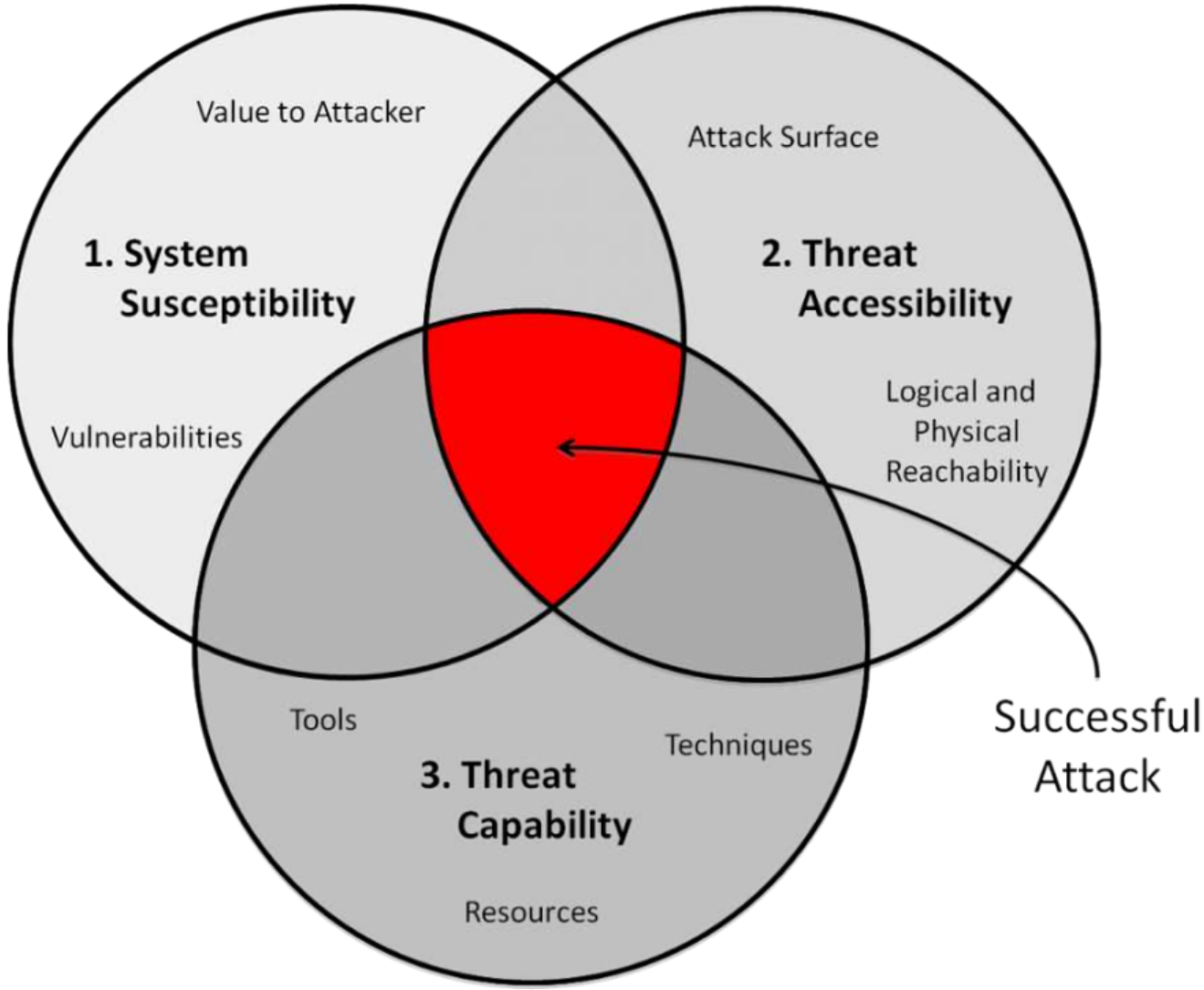
=

A HUMAN HAS BEEN MANIPULATED TO BYPASS AN ACCESS CONTROL RESULTING IN UNAUTHORIZED ACCESS TO INFORMATION.

Social Engineering Attack Framework

Mouton et al., (2016) Social engineering attack examples, templates and scenarios



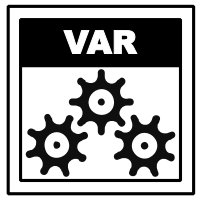

Value to Attacker
1. System Susceptibility
Vulnerabilities
Attack Surface
2. Threat Accessibility
Logical and Physical Reachability
Tools
Techniques
3. Threat Capability
Resources
Successful Attack

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.

AM:SG1 Manage and Control Access

- AM:SG1.SP1 **Enable Access**
- AM:SG1.SP2 **Manage Changes to Access Privileges**
- AM:SG1.SP3 **Periodically Review** and Maintain Access Privileges
- AM:SG1.SP4 **Correct Inconsistencies**



VAR: VULNERABILITY ANALYSIS AND RESOLUTION

Related PAs: RISK, MON , IMC

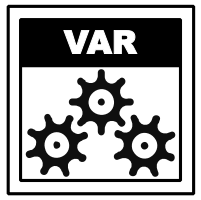
Purpose: *The purpose of Vulnerability Analysis and Resolution is to identify, analyze, and manage vulnerabilities in an organization's operating environment.*

VAR:SG1 Prepare for Vulnerability Analysis and Resolution

VAR:SG2 Identify and Analyze Vulnerabilities

VAR:SG3 Manage Exposure to Vulnerabilities

VAR:SG4 Identify Root Causes



VAR: VULNERABILITY ANALYSIS AND RESOLUTION

Samples

VAR:SG1 Prepare for Vulnerability Analysis and Resolution

VAR:SG1.SP1 Establish Scope

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

An asset and the services are vulnerable to disruption if there is a weakness that is not currently ***remediated by an administrative, technical, or physical control.*** *The universe of potential vulnerabilities in an organization's operational environment is almost limitless. The organization must therefore focus its vulnerability analysis and resolution activities toward* ***identifying the vulnerabilities to the organization's most high-value assets and services.*** *Otherwise, the organization can expend significant human and financial resources identifying vulnerabilities that have limited potential for posing operational risk to the organization.*

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

A comprehensive vulnerability management strategy addresses items such as

- *the determination and documentation of the scope of vulnerability analysis and resolution*
- *a plan for performing vulnerability analysis and resolution*
- *resources and accountability for vulnerability identification and remediation*
- *approved methods and tools to be used for the identification, analysis, remediation, monitoring, and communication of vulnerabilities*
- *a process for organizing, categorizing, comparing, and consolidating vulnerabilities*
- *thresholds for remediation and resolution activities*
- *time intervals for vulnerability identification and monitoring activities*

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.SP2 Discover Vulnerabilities

A process is established to actively discover vulnerabilities. These include:

- *performing internal vulnerability audits or assessments (using tools, techniques, and methods)*
- *performing external-entity assessments*
- *reviewing the results of internal and external audits*
- ***periodically reviewing vulnerability catalogs, such as the US-CERT Vulnerability Notes Database and the MITRE Corporation's Common Vulnerabilities and Exposures list***
- *subscribing to vendor notification services*
- *subscribing to vulnerability notification services (mailing lists)*
- *reviewing reports from industry groups*
- *reviewing vulnerability newsgroups*
- *using lessons-learned databases, such as the incident knowledgebase (The incident knowledgebase is addressed in the Incident Management and Control process area.)*
- *monitoring high-value organizational processes and infrastructure (Monitoring for events, incidents, and vulnerabilities is addressed in the Monitoring process area.)*
- *using reports of vulnerabilities from other processes such as the organization's service desk or the problem management process*

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“

OWASP Top Ten

Main | Translation_Efforts | Sponsors | Data_2020

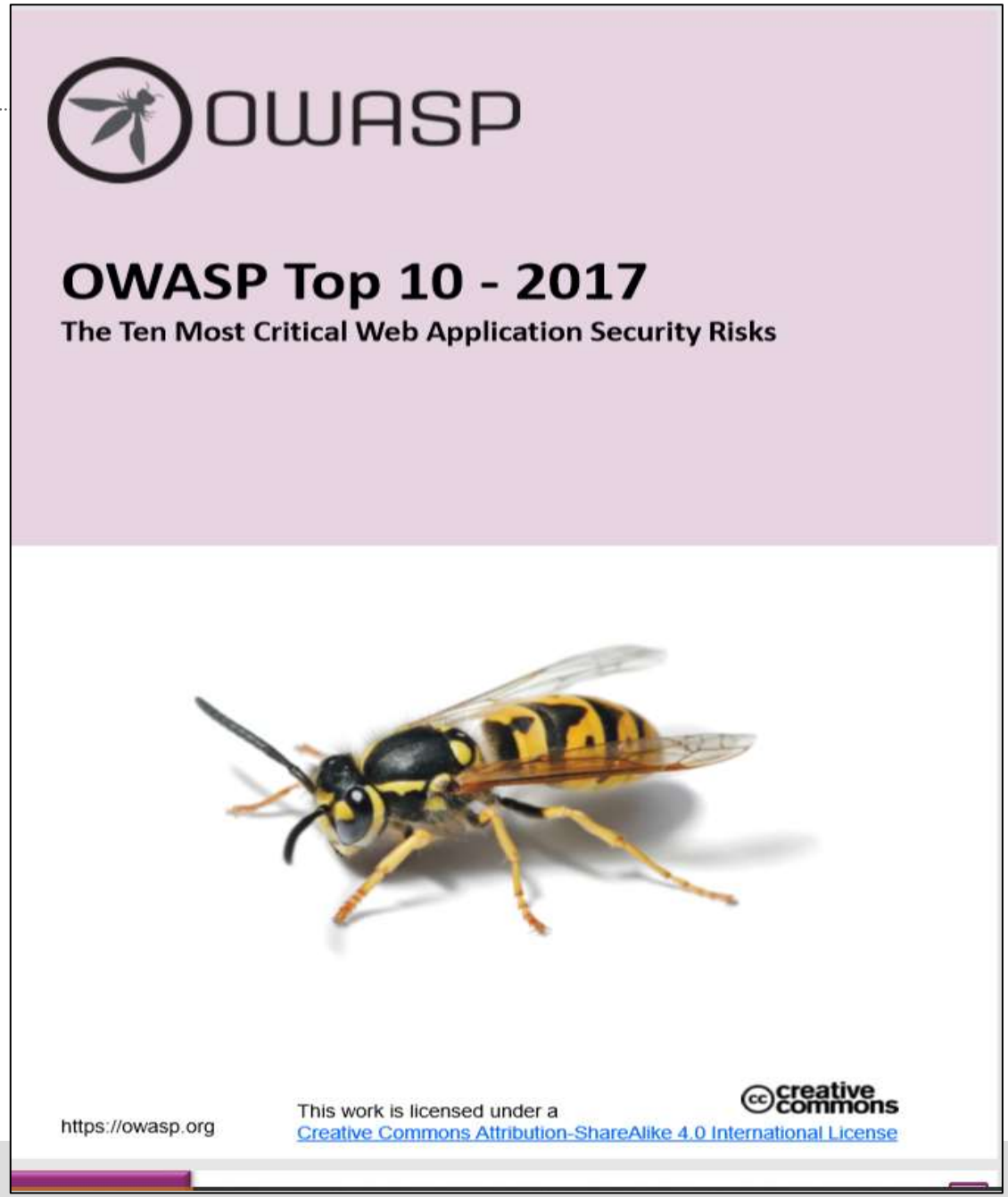
The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Globally recognized by developers as the first step towards more secure coding.

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

Top 10 Web Application Security Risks

1. **Injection**. Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
2. **Broken Authentication**. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
3. **Sensitive Data Exposure**. Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
4. **XML External Entities (XXE)**. Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
5. **Broken Access Control**. Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
6. **Security Misconfiguration**. Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
7. **Cross-Site Scripting XSS**. XSS flaws occur whenever an application includes untrusted data in a new web

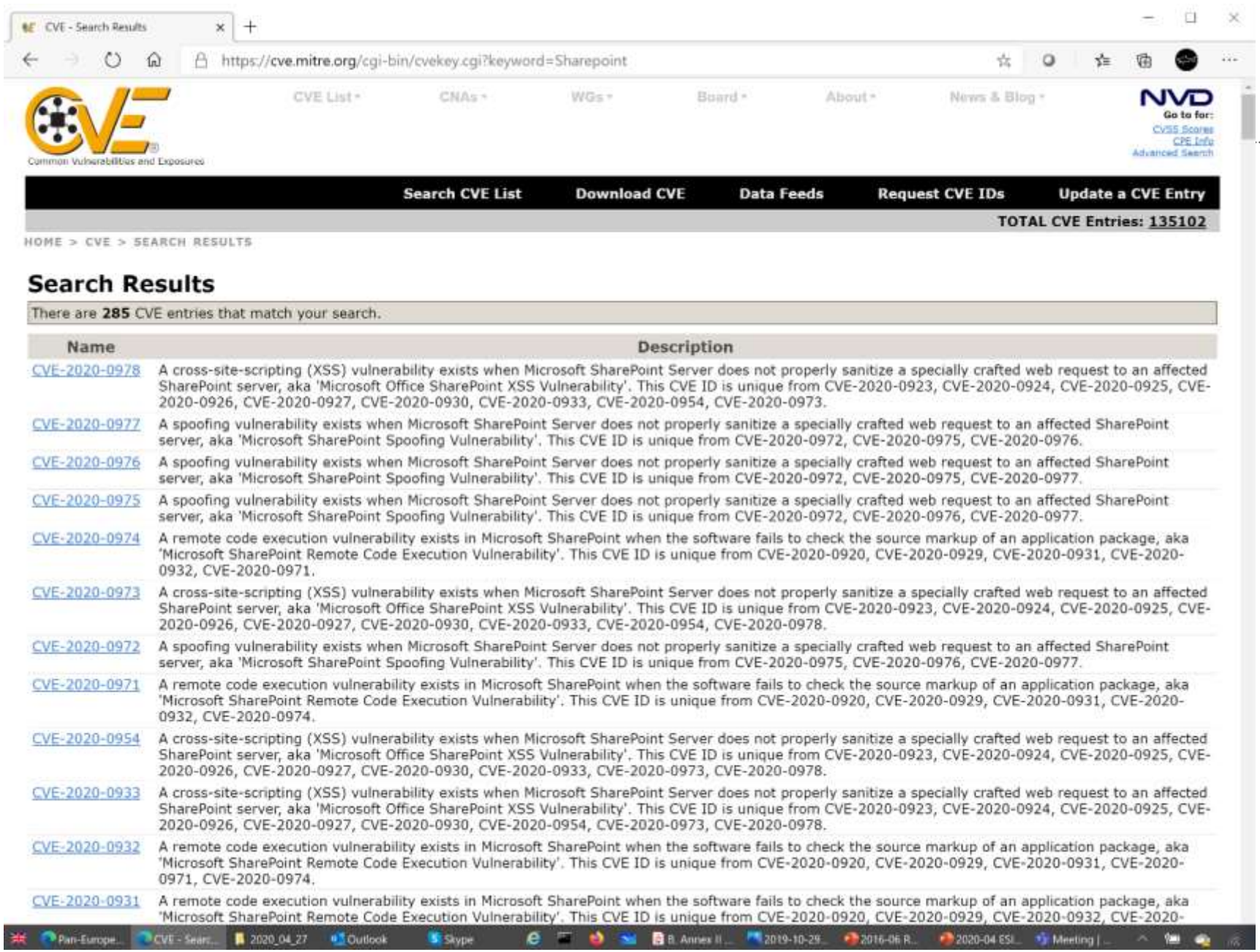


https://owasp.org/

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://cve.mitre.org/index.html



https://cve.mitre.org/index.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9070

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾

Common Vulnerabilities and Exposures

NVD
Go to for:
CVSS Scores
CPE Info
Advanced Search

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 135102

HOME > CVE > CVE-2020-9070

Printer-Friendly View

CVE-ID

CVE-2020-9070 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Huawei smartphones Taurus-AL00B with versions earlier than 10.0.0.205(C00E201R7P2) have an improper authentication vulnerability. The software insufficiently validate the user's identity when a user wants to do certain operation. An attacker can trick user into installing a malicious application to exploit this vulnerability. Successful exploit may cause some information disclosure.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200415-01-smartphone-en
- CONFIRM:https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200415-01-smartphone-en

Assigning CNA

Huawei Technologies

Date Entry Created

20200218 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20200218)

Votes (Legacy)

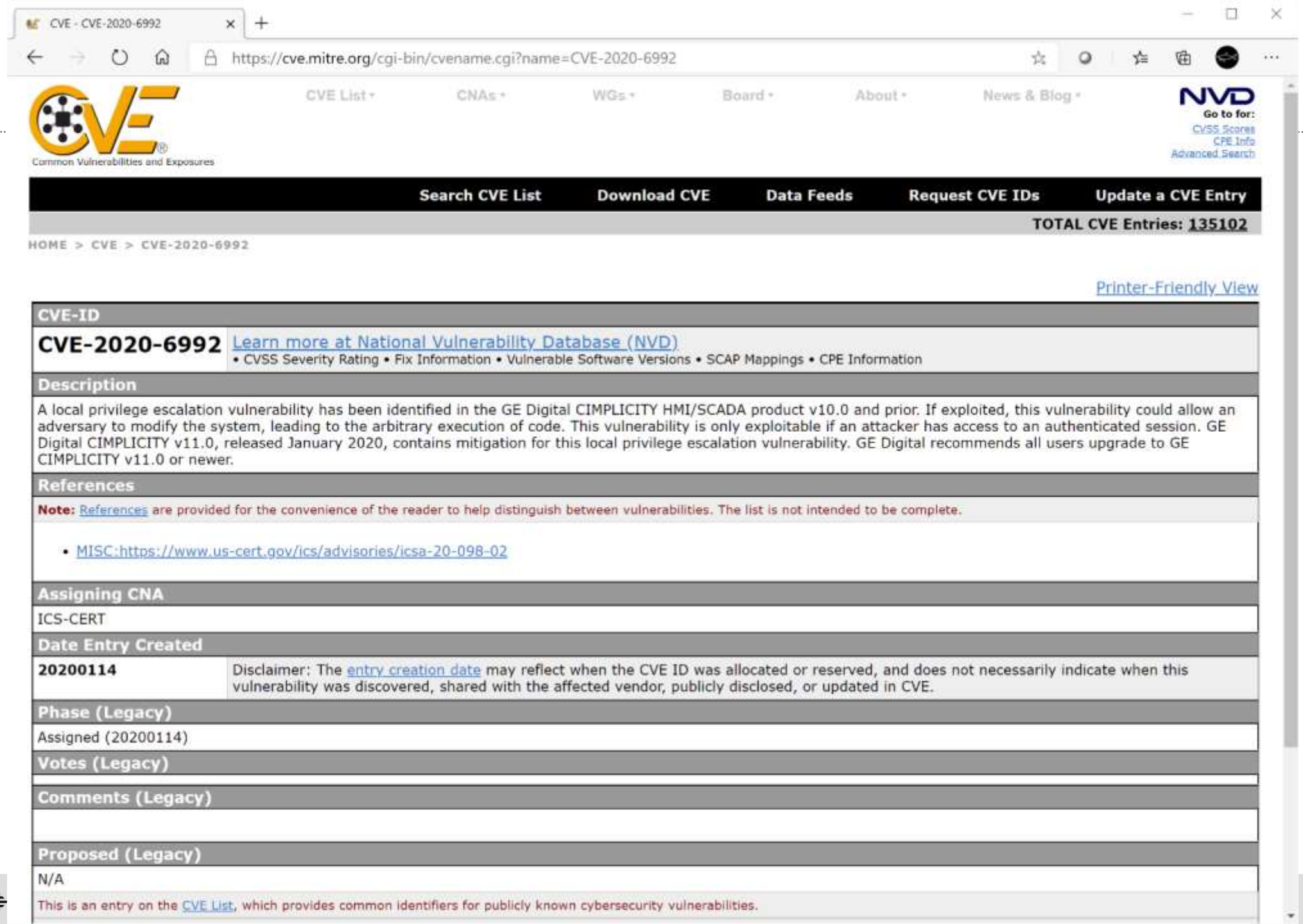
Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit



CVE - CVE-2020-6992

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6992

CVE List • CNAs • WGs • Board • About • News & Blog •

NVD
Go to for:
CVSS Scores
CPE Info
Advanced Search

Common Vulnerabilities and Exposures

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 135102

HOME > CVE > CVE-2020-6992

Printer-Friendly View

CVE-ID

CVE-2020-6992 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A local privilege escalation vulnerability has been identified in the GE Digital CIMPLICITY HMI/SCADA product v10.0 and prior. If exploited, this vulnerability could allow an adversary to modify the system, leading to the arbitrary execution of code. This vulnerability is only exploitable if an attacker has access to an authenticated session. GE Digital CIMPLICITY v11.0, released January 2020, contains mitigation for this local privilege escalation vulnerability. GE Digital recommends all users upgrade to GE CIMPLICITY v11.0 or newer.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://www.us-cert.gov/ics/advisories/icsa-20-098-02

Assigning CNA

ICS-CERT

Date Entry Created

20200114 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20200114)

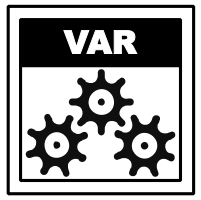
Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.



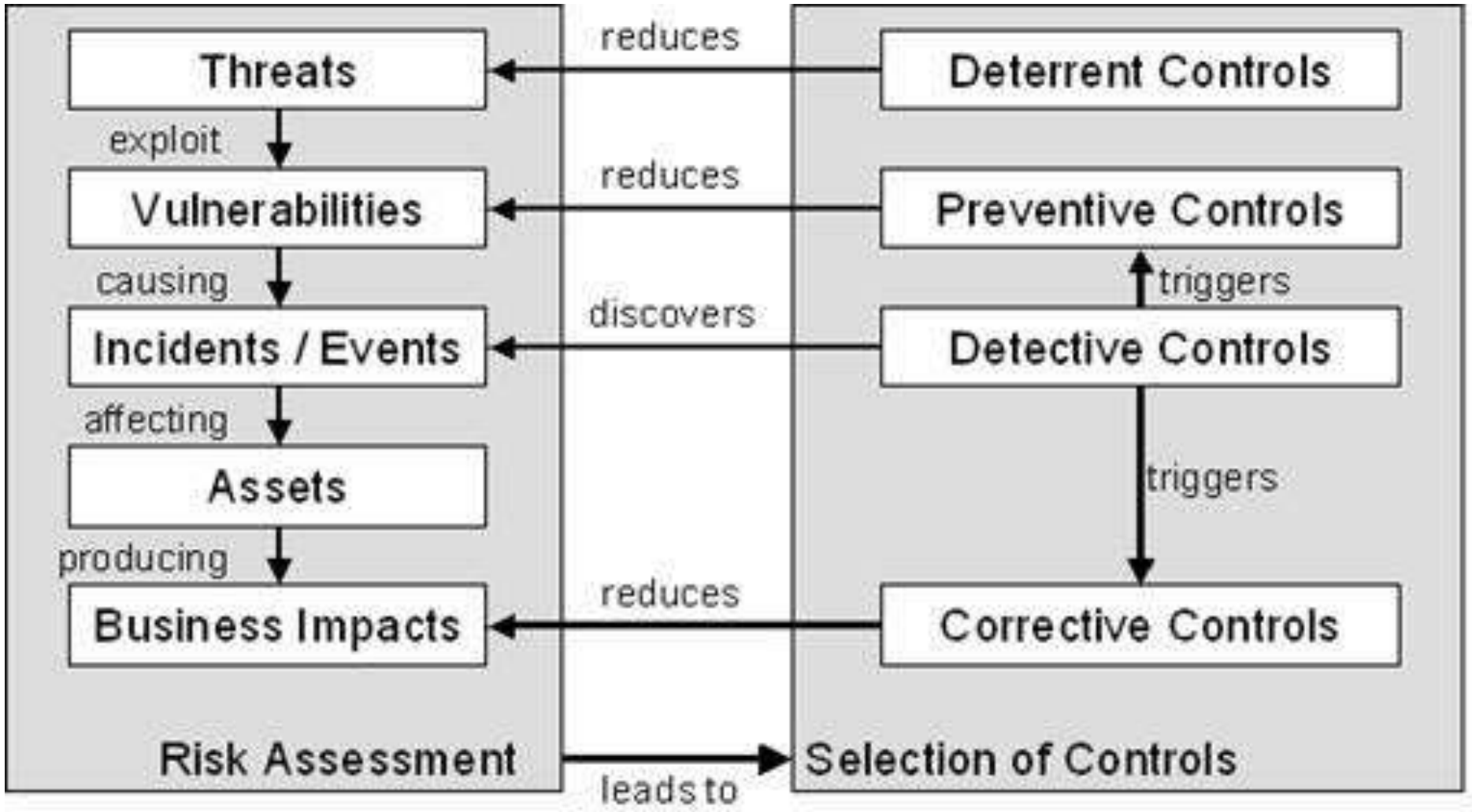
VAR:SG2.SP3 Analyze Vulnerabilities

Vulnerabilities are analyzed to determine whether they have to be reduced or eliminated.

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.*



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

Triton Malware Details Show the

https://www.wi...

WIRED BUSINESS CULTURE GEAR IDEAS SCIENCE MORE MY ACCOUNT GIVE A GIFT

LILY HAY NEWMAN SECURITY 01.10.2018 07.17 PM

Menacing Malware Shows the Dangers of Industrial System Sabotage

New details about Triton malware should put industrial systems and critical infrastructure on notice.

It's still unknown exactly what industrial plant Triton malware struck, or where. But new details show just how dangerous its brand of sabotage could be. ZOHAZHUANG/GETTY IMAGES

A RECENT DIGITAL attack on the control systems of an industrial plant has renewed concerns about the threat hacking poses to critical infrastructure. And while security researchers offered some analysis last month of the malware used in the attack, called Triton or Trisis, newly revealed details of how it works expose just how vulnerable industrial plants—and their failsafe mechanisms—could be to manipulation.

At the S4 security conference on Thursday, researchers from the industrial control company Schneider Electric, whose

Triton/Trisis Attack Was More Wi

https://www.darkreading.com/attacks-breaches/triton-trisis-attac...

InformationWeek IT NETWORK Dark Reading Network Computing About Us **Advertise** Register Login to your account Welcome Guest

DARKReading | SIGN UP FOR OUR NEWSLETTERS

Search Dark Reading

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News Follow DR:

THE EDGE | ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | OPERATIONS | PERIMETER | RISK | THREAT INTELLIGENCE | VULNS / THREATS

ATTACKS/BREACHES

1/16/2019
10:20 AM

Kelly Jackson Higgins
News

Connect Directly

0 COMMENTS
COMMENT NOW

Login
50% 50%

Like Tweet

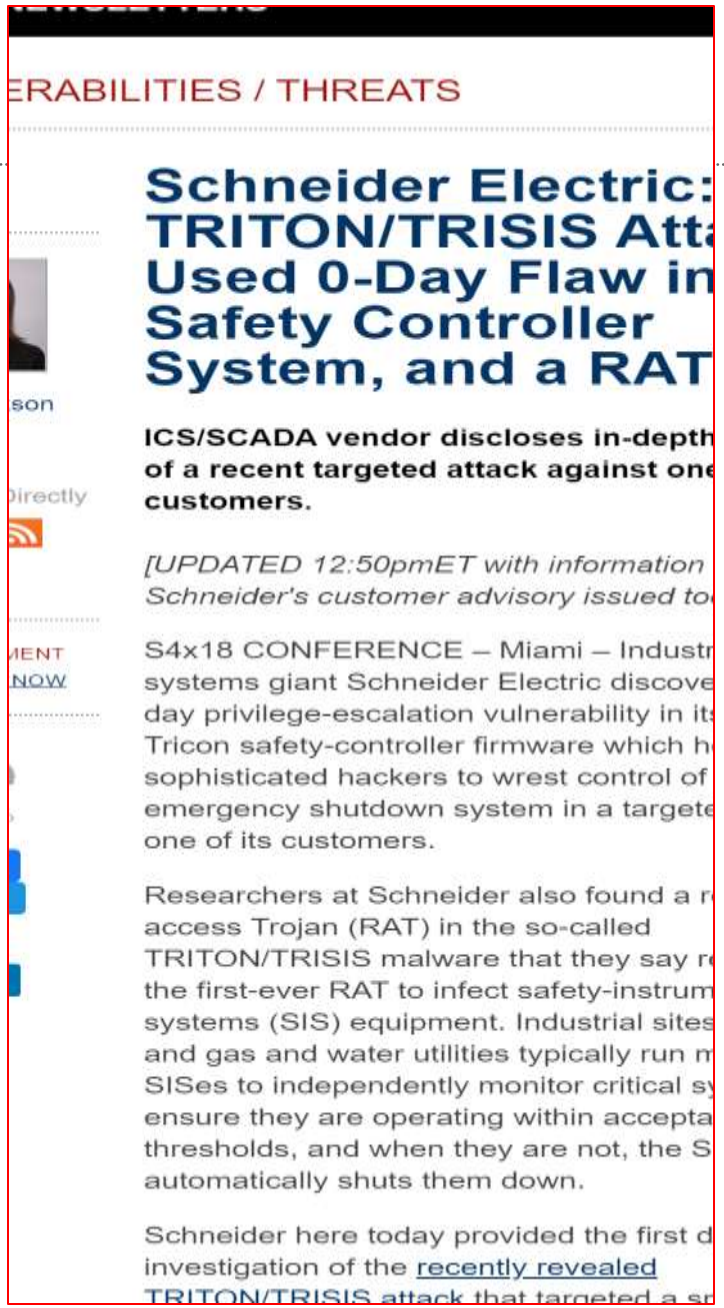
Triton/Trisis Attack Was More Widespread Than Publicly Known

Signs of the attack first showed up two months before it was identified as a cyberattack, but they were mistaken for a pure equipment failure by Schneider Electric, security expert reveals at S4x19.

[UPDATED 1/16/2019 7:40PM with updated new comments from Schneider Electric]

S4x19 -- Miami -- New details have emerged about the 2017 Triton/Trisis cyberattack on a Middle East plant's safety instrumentation system -- including a missed opportunity to quash it two months earlier than its ultimate discovery, according to an ICS security expert who assisted in the incident response.

New information also shows that the attackers infected six engineering systems, not just two as investigators had reported, said Julian Gutmanis, who was working out of a major oil and gas organization in Saudi Arabia at the time of the attacks, in a presentation here at S4. The publicly revealed attack on Aug. 7, 2017, was not the first incident suffered by the victim at the hands of the Triton/Trisis attackers, he said. In June 2017, an emergency plant-process shutdow
the Midd
petroche
but not p



ERABILITIES / THREATS

Schneider Electric: TRITON/TRISIS Att Used 0-Day Flaw in Safety Controller System, and a RAT

ICS/SCADA vendor discloses in-depth of a recent targeted attack against one customers.

[UPDATED 12:50pmET with information Schneider's customer advisory issued to

S4x18 CONFERENCE – Miami – Industr systems giant Schneider Electric discove day privilege-escalation vulnerability in it Tricon safety-controller firmware which h sophisticated hackers to wrest control of emergency shutdown system in a targete one of its customers.

Researchers at Schneider also found a r access Trojan (RAT) in the so-called TRITON/TRISIS malware that they say r the first-ever RAT to infect safety-instrum systems (SIS) equipment. Industrial sites and gas and water utilities typically run n SISes to independently monitor critical sy ensure they are operating within accepta thresholds, and when they are not, the S automatically shuts them down.

Schneider here today provided the first d investigation of the recently revealed TRITON/TRISIS attack that targeted a sr

CVE - CVE-2018-8872 | NVD - Calculator Product | NVD - Categories | NVD - CVSS v3 Calculator

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8872

Common Vulnerabilities and Exposures

CVE List | CNAs | WGs | Board | About | News & Blog

NVD
Go to for:
CVSS Scores
CPE Info
Advanced Search

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 135102

HOME > CVE > CVE-2018-8872

Printer-Friendly View

CVE-ID

CVE-2018-8872 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

In Schneider Electric Triconex Tricon MP model 3008 firmware versions 10.0-10.4, system calls read directly from memory addresses within the control program area without any verification. Manipulating this data could allow attacker data to be copied anywhere within memory.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:103947
- URL:http://www.securityfocus.com/bid/103947
- CONFIRM:https://www.schneider-electric.com/en/download/document/SEVD-2017-347-01/
- MISC:https://ics-cert.us-cert.gov/advisories/ICSA-18-107-02

Assigning CNA

ICS-CERT

Date Entry Created

20180320 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20180320)

Votes (Legacy)

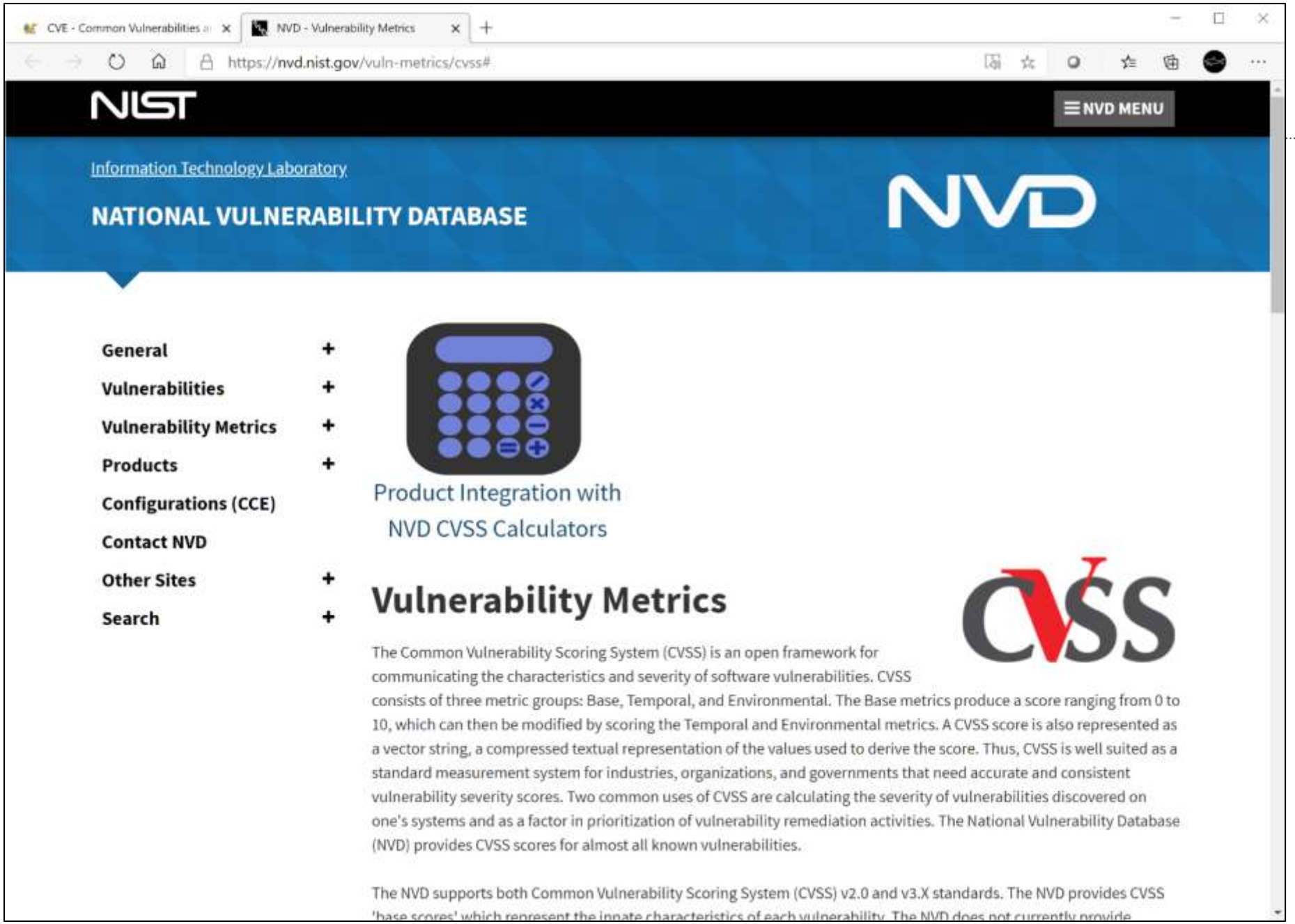
Comments (Legacy)

Proposed (Legacy)

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

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

https://www.cvedetails.com/



https://nvd.nist.gov/vuln-metrics/cvss#

CVSS v3.1 Equations

The CVSS v3.1 equations are defined below.

Base

The Base Score is a function of the Impact and Exploitability sub score equations. Where the Base score is defined as,

If (Impact sub score <= 0) *0 else,*
Scope Unchanged$_4$ $Roundup(Minimum[(Impact + Exploitability), 10])$
Scope Changed $Roundup(Minimum[1.08 \times (Impact + Exploitability), 10])$

and the Impact sub score (ISC) is defined as,

Scope Unchanged $6.42 \times ISC_{\text{Base}}$
Scope Changed $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

Where,

$ISC_{Base} = 1 - [(1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail})]$

And the Exploitability sub score is,

$8.22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$**Temporal**

The Temporal score is defined as,

$Roundup(BaseScore \times ExploitCodeMaturity \times RemediationLevel \times ReportConfidence)$

Environmental

The environmental score is defined as,

If (Modified Impact Sub score <= 0) 0 else,
If Modified Scope is Unchanged Round up(Round up (Minimum [(M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)

If Modified Scope is Changed Round up(Round up (Minimum [1.08 × (M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)

And the modified Impact sub score is defined as,

If Modified Scope is Unchanged $6.42 \times [ISC_{Modified}]$

If Modified Scope is Changed $7.52 \times [ISC_{Modified} - 0.029]$-$3.25 \times [ISC_{Modified} \times 0.9731 - 0.02]$ 13

Where,

$ISC_{Modified} = Minimum$ [$[1 - (1 - M.IConf \times CR) \times (1 - M.IInteg \times IR) \times (1 - M.IAvail \times AR)]$, 0.915]

The Modified Exploitability sub score is,

$8.22 \times M.AttackVector \times M.AttackComplexity \times M.PrivilegeRequired \times M.UserInteraction$4 Where “Round up” is defined as the smallest number, specified to one decimal place, that is equal to or higher than its input. For example, Round up (4.02) is 4.1; and Round up (4.00) is 4.0.

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:

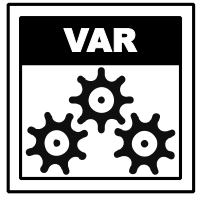
Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)

- **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



VAR:SG3 Manage Exposure to Vulnerabilities

VAR:SG3.SP1 Manage Exposure to Vulnerabilities

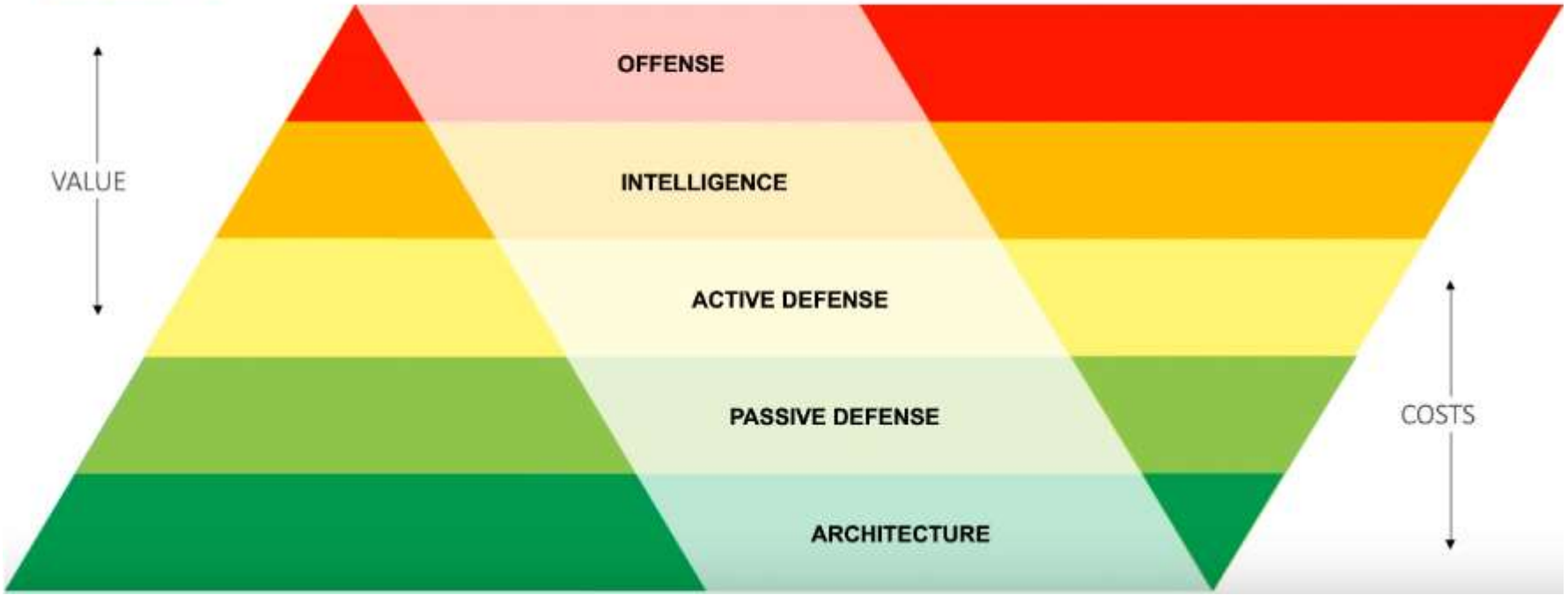
VAR:SG4 Identify Root Causes

The root causes of vulnerabilities are examined to improve vulnerability analysis and resolution and reduce organizational exposure.

VAR:SG4.SP1 Perform Root-Cause Analysis

Sliding Scale of Cyber Security

Source: SANS



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.

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

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:

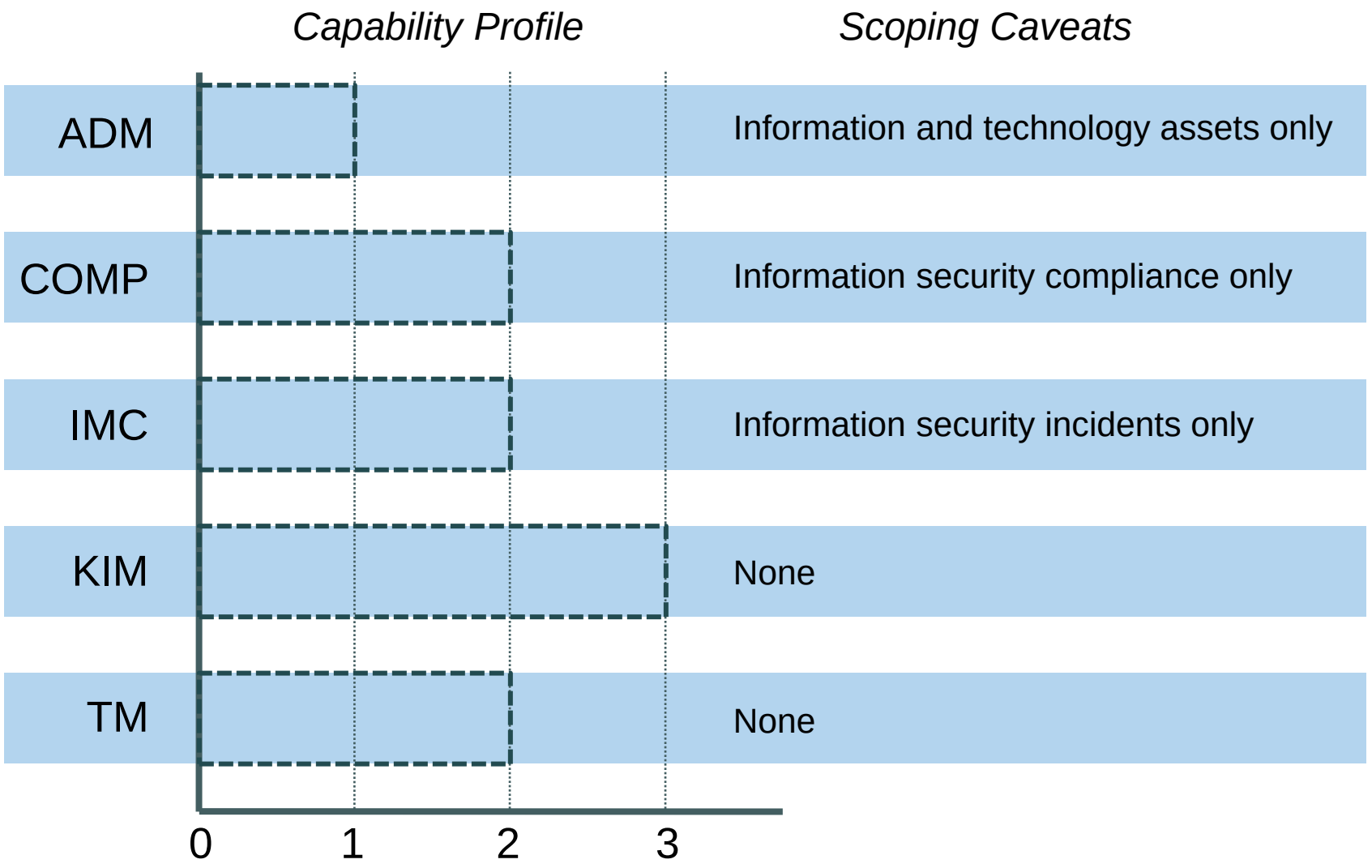
Goal Ratings

S	Satisfied
NS	Not Satisfied

Practice Characterizations

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

CERT-RMM model scope example



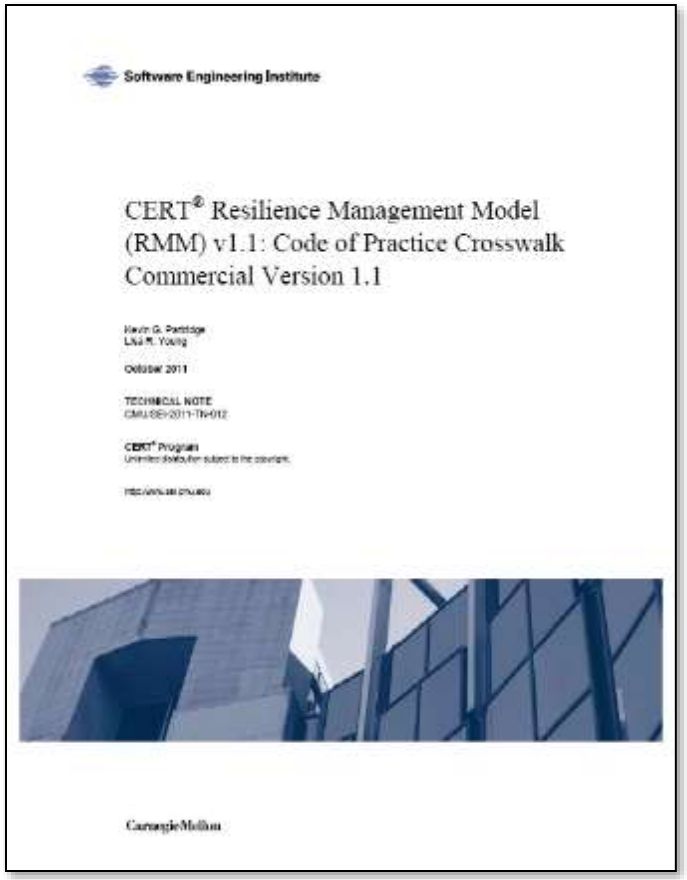
RMM Code of Practice Crosswalk

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.



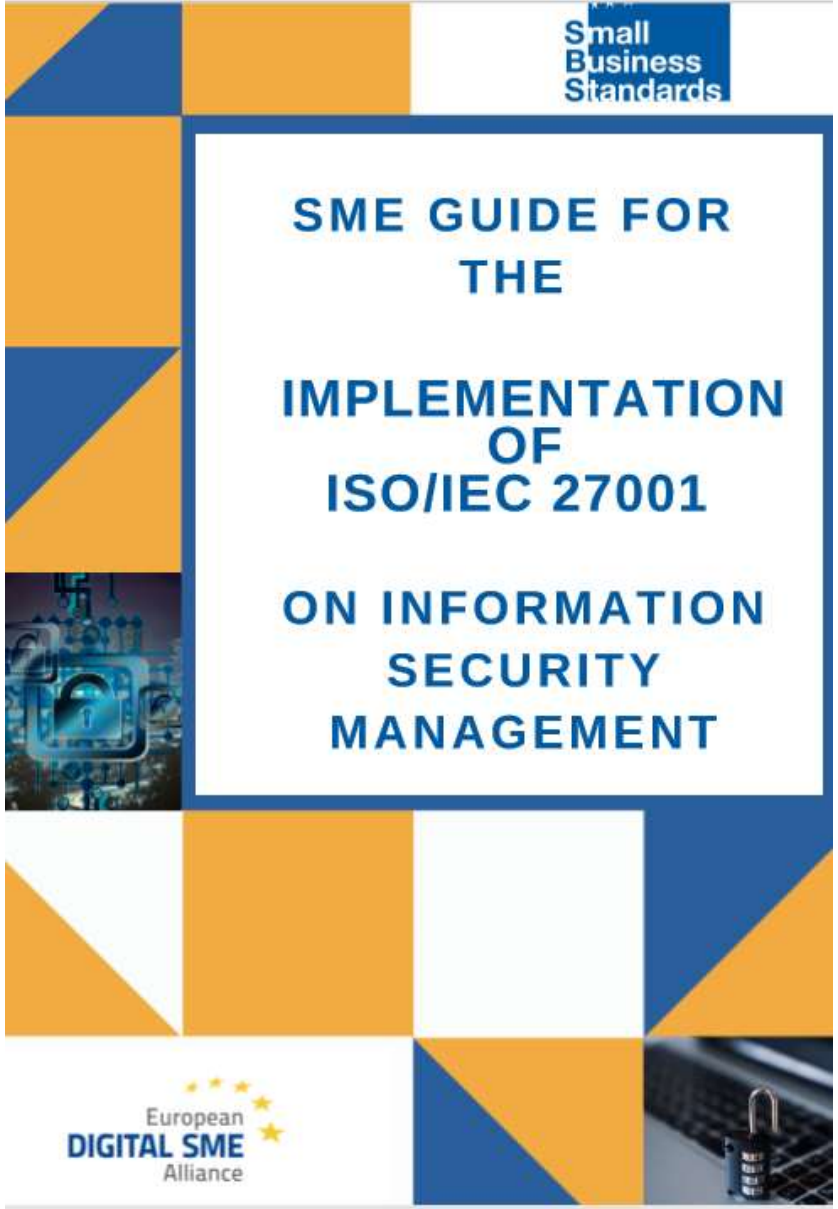
RMM NIST Crosswalk

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.

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/

About Cyber Essentials - NCSC.G

https://www.ncsc.gov.uk/cyberessentials/overview

National Cyber Security Centre

Go to ncsc.gov.uk >

CYBER ESSENTIALS

Overview | Certificate search | Advice | Resources | Contact | News

About Cyber Essentials

Cyber Essentials helps you to guard your organisation against cyber attack.

Cyber Essentials helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security.

What is Cyber Essentials?

Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

Cyber attacks come in many shapes and sizes, but the vast

Want to get certified?

Our Cyber Essentials Partner

Additional requirements and compliances

NIS Directive (EU, EP)

Cyber Act (ENISA, Cybersecurity Certification Schemes)

After 16 Dec 2020

NISD-2 (Essential Services > CI > Resilience)

CER (Critical Entities Resilience)

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 (GDPR)

Deadlines: May 2018

PSD2 (Payment Services Directive – Advanced)

CIP

Critical infrastructure protection (CIP) is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation.

***Critical infrastructure** (or critical national infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy – the infrastructure.*

The systems and networks that make up the infrastructure of society are often taken for granted, yet a disruption to just one of those systems can have dire consequences across other sectors.

*The process includes **assessments** of:*

- ***Protection** - Can be defined as the state of being defended, safeguarded, or shielded from injury, loss, or destruction from natural or unnatural forces.*
- ***Vulnerability** – The quality of being susceptible to attack or injury, warranted or unwarranted, by accident or by design.*
- ***Risk** – The possibility or likelihood of being attacked or injured.*
- ***Mitigation** – The ability to alleviate, reduce, or moderate a vulnerability, thus reducing or eliminating risk.*

DESIGN

Plans and policies for response, mitigation and reconstitution to incidents

PLAN

Plan to eliminate significant vulnerabilities

DEVELOP

Develop systems to identify and prevent attempted attacks

ASSESS

Assess vulnerabilities to both physical or cyber attacks

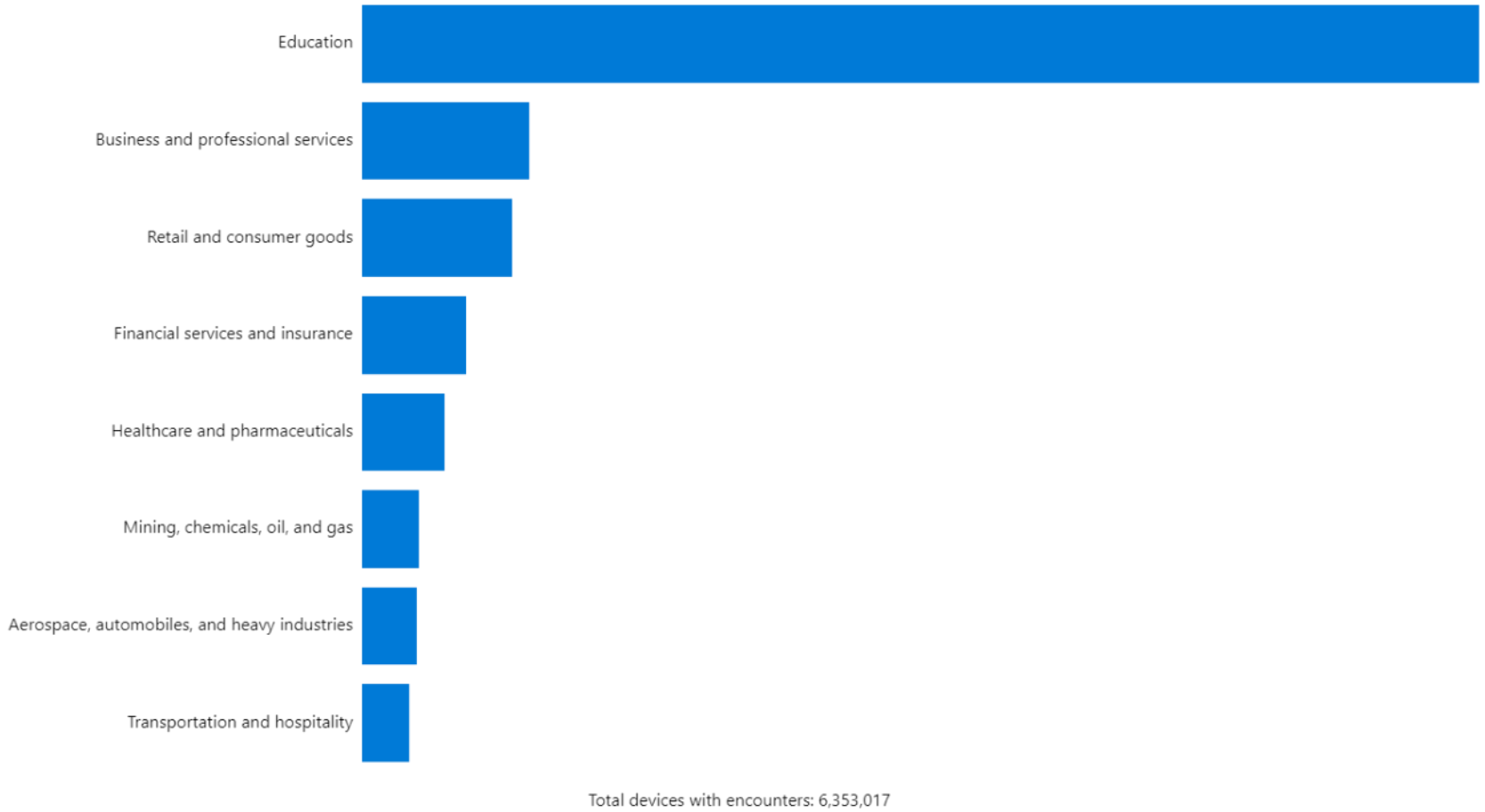
ALERT

Alert, contain and rebuff attacks and rebuild essential capabilities in the aftermath

CIP

MOST AFFECTED INDUSTRIES BY MALWARE

Reported malware encounters in the last 30 days



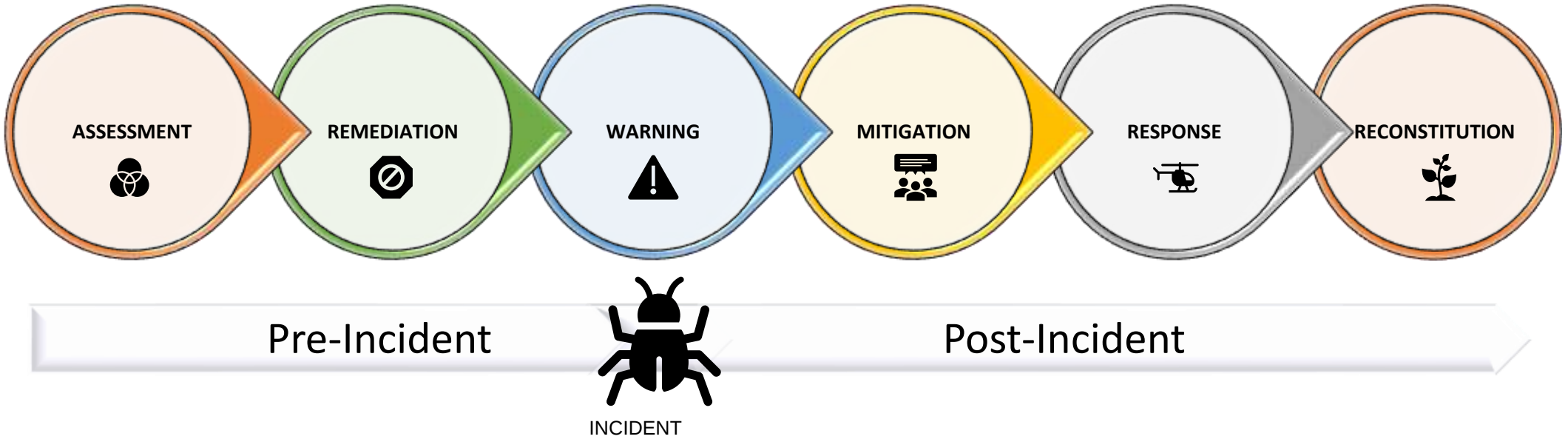
Source: Microsoft Security Intelligence, Most affected industries, statistic as of 24 April 2020

GLOBAL THREAT ACTIVITY

Countries and regions with the most malware encounters in the last 30 days

Source: Microsoft Security Intelligence, statistic as of 24 April 2020

CIP Lifecycle



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.

2020-2021

Update on cybersecurity standards and certifications (EU/EC)