IEEE computer society

ITProfessional
Technology Solutions for the Enterprise

IEEE Computer Society – Northern Virginia / Washington DC Chapters

IT Risk and Resilience – Cybersecurity Response to COVID-19

VOLUME 20, NUMBER 3   MAY/JUNE 2018

Cyberthreats and Security

Tim Weil – IEEE Senior Member
Chair – IEEE Denver COMSOC Chapter
http://comsoc.ieee-denver.org

Cybersecurity Professional / Executive Advisor
SecurityFeeds – http://www.securityfeeds.com

Invited Talk
Denver, CO
Nov 10th, 2020

1

Objectives of this Presentation

Cyberspace – Out Point of Departure

-- A Writer's Life

-- Risk Landscape Evaluation

-- ISO 27001 Information Security Management (BOK)

Information Security Management Models

-- Risk Management Framework (NIST SP 800-37)

-- Deming Cycle - Plan-Do-Check-Act

-- OODA Loop (Joe Boyd, USAF Fighter Pilot)

-- NIST Cybersecurity Frameworks

Global transformation caused by COVID-19

-- Global transformation of Information Technology Services

-- NIST Cybersecurity Framework (up close)

-- Smackdown – NIST CSF vs Big Scary Monsters

-- Recovery and Resilience – IT Context for Business Continuity

Writing and Editing for Computer Society Publications

-- 1st Citation for 'IT Risk and Resilience – Cybersecurity Response to COVID-19'

-- Random Cybersecurity Attack Simulation Model (RCSM)

-- Write Stuff

11/7/2020

A Writer's Life –

IT Risk and Resilience—Cybersecurity Response to COVID-19

Tim Weil, *SecurityFeeds LLC*
San Murugesan, *Western Sydney University*

The rapid and worldwide spread of the coronavirus and its illness known as COVID-19 has made huge impact on almost everything has taken us all by surprise. We all are now experiencing a major unprecedented and unexpected global public health crisis. This pandemic has also triggered huge social upheavals, disrupted almost every industry, and impacted the life and work of everyone in almost every country. Businesses and educational institu-

of recent developments in IT, as outlined in Table 1. It is very likely that even after we successfully emerge from the crisis, business will not be "as usual" and we may continue new ways of working and offering various services.

The COVID-19 epidemic impacted IT too, primarily positively, benefiting IT industry and IT professionals and serving public goods. However, there are a few negative impacts as well, such as increased and novel

Download   **Export Citation**

Adding Attributes to Role Based Access Control reaches 500 citations on Google Scholar - https://lnkd.in/ew_BQaF

Adding attributes to role-based access control

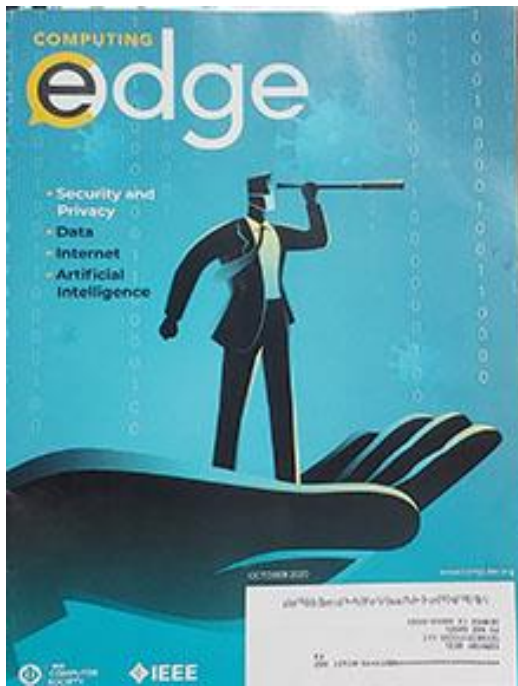|	
Authors	D Richard Kuhn, Edward J Coyne, Timothy R Weil
Publication date	2010/6/1
Journal	Computer
Volume	43
Issue	6
Pages	79-81
Publisher	Institute of Electrical and Electronics Engineers, Inc., 3 Park Avenue, 17 th Fl New York NY 10016-5997 United States of America
Description	Nat'l Computer Security Conf., NSA/NIST, 1992, pp. 554-563; R. Sandhu et al.,"Role-Based Access Control Models," Computer, 29 (2), 1996, pp. 38-47), also known as RBAC, provides a popular model for information security that helps reduce the complexity of security administration and supports review of permissions assigned to users. This feature is critical to organizations that must determine their risk exposure from employee IT system access.
	RBAC has frequently been criticized for the difficulty of setting up an initial role structure and for inflexibility in rapidly changing domains. A pure RBAC solution may provide inadequate support for dynamic attributes such as time of day, which might need to be considered when determining user permissions. To support dynamic attributes, particularly in large organizations, a "role explosion" can result in thousands of separate roles being fashioned for different collections of permissions. Recent interest in attribute-based access control (ABAC) suggests that attributes and rules could either replace RBAC or make it more simple and flexible.
Total citations	Cited by 500
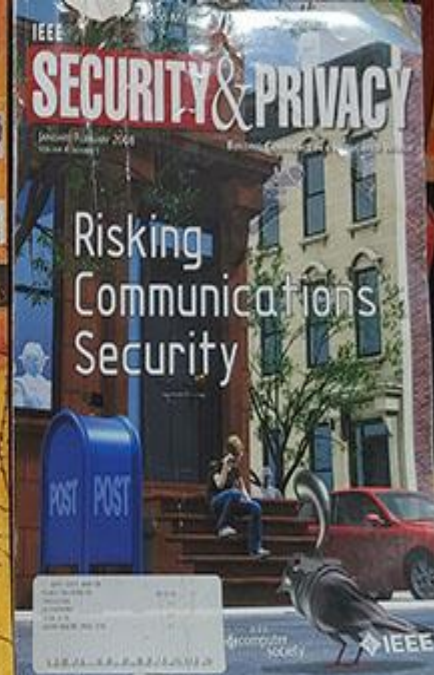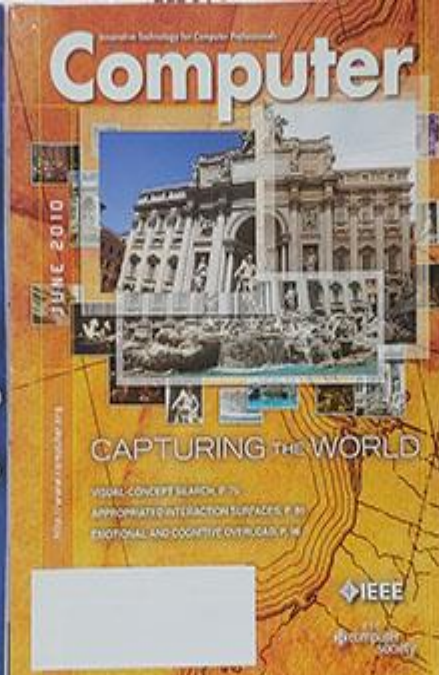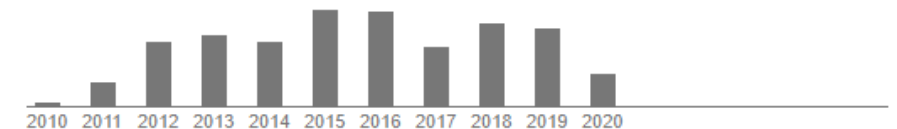
4

Table of Contents

▸ Cyberspace – Our Point of Departure

▸ Information Security Management Models

▸ Frameworks for Risk Management

▸ Smackdown – NIST CSF vs Big Scary Monsters

▸ Random Cybersecurity Attack Simulation Model (RCSM)

▸ References + Q&A

Cyberspace – Our Point of Departure – Wired Magazine (June '08) -
https://www.wired.com/2008/05/pentagon-define/

26 YEARS AFTER GIBSON, PENTAGON DEFINES 'CYBERSPACE'
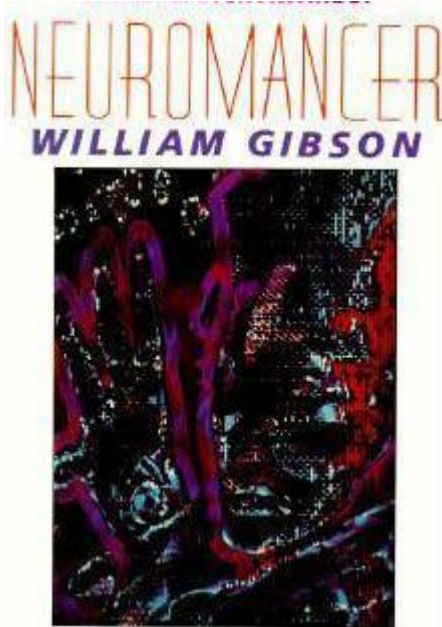
"More than two decades after novelist William Gibson coined the term cyberspace as a 'consensual hallucination' of data... the Pentagon has come up with its own definition,"* *Inside Defense reports. "A May 12 'for official use only' memo signed by Deputy Defense Secretary Gordon England... offers a 28-word meaning for the term." It is decidedly "less poetic" than Gibson's

Cyberspace, England writes, is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." *

*It is a far cry from the prose Gibson used in his 1984 novel "Neuromancer" to describe cyberspace: "A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding."

Communications Recovery and Resilience
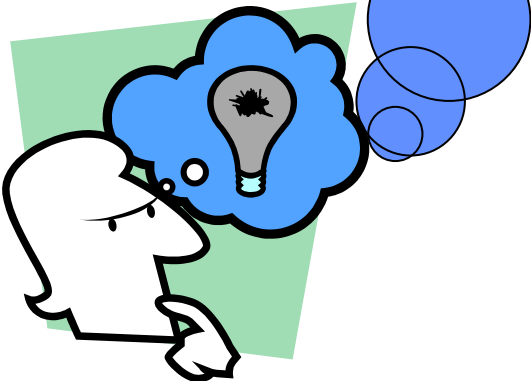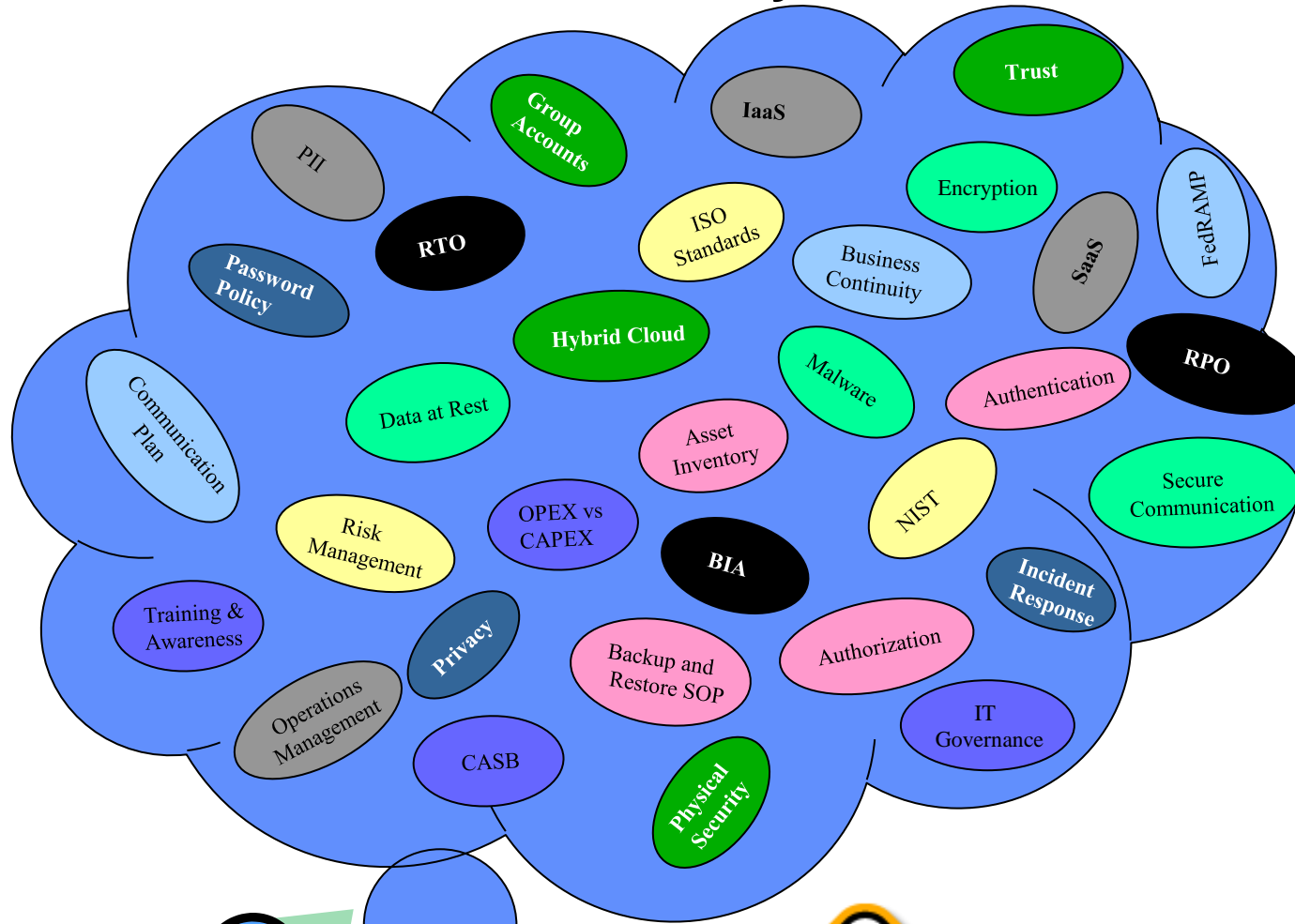
IT 101 – What Problems Are We Trying to Solve?

- Identify 'Fix-It' areas in the program
- Understand Current State (Remediation)
- Improve 'ad hoc', 'not my problem' state
- **Reduce Program Risk**
- Improve Continuous Monitoring Process

Antarctica, the only continent without coronavirus, braces for summer rotation

PUBLISHED SUN, SEP 27 2020·9:30 AM EDT | UPDATED SUN, SEP 27 2020·12:56 PM EDT

Emma Newburger
@EMMA_NEWBURGER

KEY POINTS
- Antarctica, the coldest and most isolated part of the world, is the only continent still untouched by the coronavirus.
- But as Antarctica's harsh winter comes to a close, critical global efforts are

TRENDING NOW

If you work due to Cov tax surpris coming

PERRY JOHNSON REGISTRARS, INC.

Certificate of Registration

Perry Johnson Registrars, Inc., has audited the Information Security Management System of:

Alcohol Monitoring Systems, Inc.
1241 West Mineral Avenue, Littleton, CO 80120 United States
(This is a multisite scheme. See Appendix for site specific details.)

(Hereinafter called the Organization) and hereby declares that Organization is in conformance with:

ISO/IEC 27001:2013

This Registration is in respect to the following scope:

Operation and Development of the SaaS Platform for Alcohol Monitoring, Offender Management, and Judicial Management Services

(Statement of Applicability: 6/5/2017)

After a thorough independent audit, SCRAM Systems has received ISO/IEC 27001:2013 **certification for alcohol monitoring, offender management, and judicial management services in SCRAMnet, our Software as a Service (SaaS) program**. This confirms that SCRAM Systems has implemented internationally-recognized best practices and standards for its Information Security Management System (ISMS).

The certification complements the ISO 9001 certification for quality management systems (QMS) acquired previously.

ISO is an independent, international organization that develops standards to help businesses create and deliver quality products, services, and systems. The International Electrotechnical Commission (IEC) develops standards for information technology (IT) and information and communications technology (ICT).nt.

11/7/2020

The ISO/IEC 27001 standard

ISO/IEC 27001 Controls

Risk assessment

Continual improvement

Asset register

Management system

Performance management

Resources and competence

Awareness and communication

Information security policies	Organisation of information security	Human resources security	Asset management
Access control	Cryptography	Physical and environmental security	Operations security
Communications security	System acquisition, development and maintenance	Supplier relationships	Incident management
	Business continuity management	Compliance	

Clauses 4 through 10 deal with:

- Scoping of the ISMS
- Identifying and evaluating Risks
- Risk Treatment and mitigation
- Managing and measuring performance of the ISMS
- Tracking non-conformities and resolution
- Continuous improvement

Annex A deals with:
114 Optional controls for risk mitigation

11/7/2020

9

Table of Contents

▸ Cyberspace – Our Point of Departure

▸ Information Security Management Models

▸ Frameworks for Risk Management

▸ Smackdown – NIST CSF vs Big Scary Monsters

▸ Random Cybersecurity Attack Simulation Model (RCSM)

▸ References + Q&A

Risk Management

Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget

Implementation Progress Changes in Assets, Vulnerability and Threat

Framework Profiles

Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation

- Use Risk Matrix to Prioritize actions and expenditures. Most economic value for each risk considered.

- Nominate Tasks and Expenditures for budget allocation

- Implementation of critical Infrastructure

Cybersecurity shouldn't be an afterthought

Cyberthreats should not be thought of just in the context of IT security and privacy design. Adequate cybersecurity must involve the active participation of everyone in an organization, as well as users.   Approaches generally reflect some variation on the common-sense method of evaluating the problem, preparing, acting, and assessing the results.

Federal agencies use the **Risk Management Framework (RMF)** to Assess and Authorize enterprise systems

The RMF model has been accelerated for **Cloud Environments (RMF4CE)**

Managers learn a **Plan-Do-Check-Act** (PDCA) cycle.

Fighter pilots are taught to **Observe-Orient-Decide-Act (OODA)**.

In cybersecurity the latest incarnation of this common-sense approach is the popular **NIST Cybersecurity Framework (CSF),** which teaches **Identify-Protect-Detect-Respond-Recover.**

As in other fields, these activities are intended to be performed in a continuous cycle, modifying plans and actions as the organization learns from successes and failures.

11/7/2020

The FISMA Risk Management Framework.

Information Risk Management (IRM) is the practice of determining which Information Assets need protection and what level of protection is required, then determining appropriate methods of achieving that level of protection by understanding the applicable vulnerabilities, threats and countermeasures.
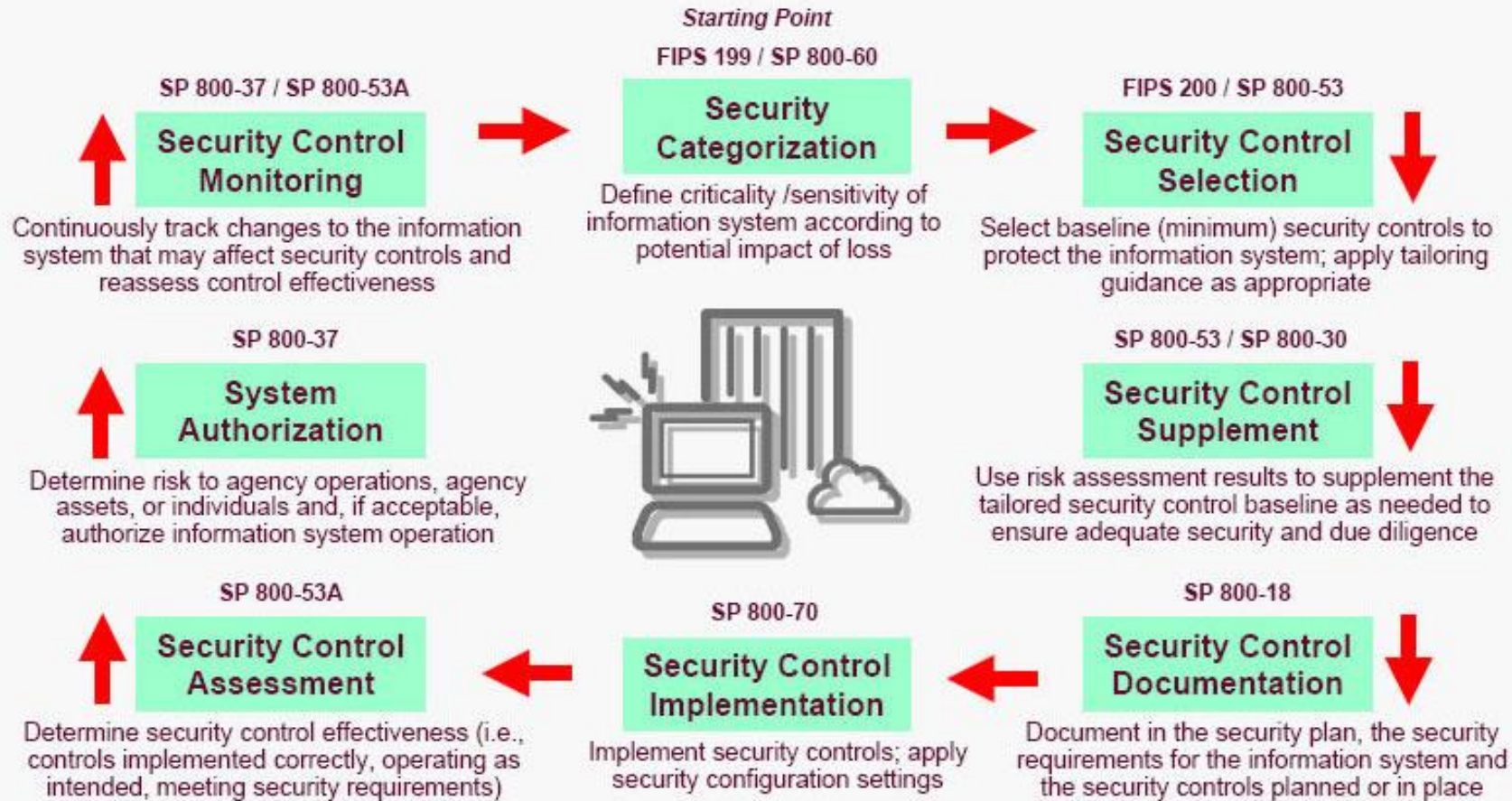
The FISMA Risk Management Framework.
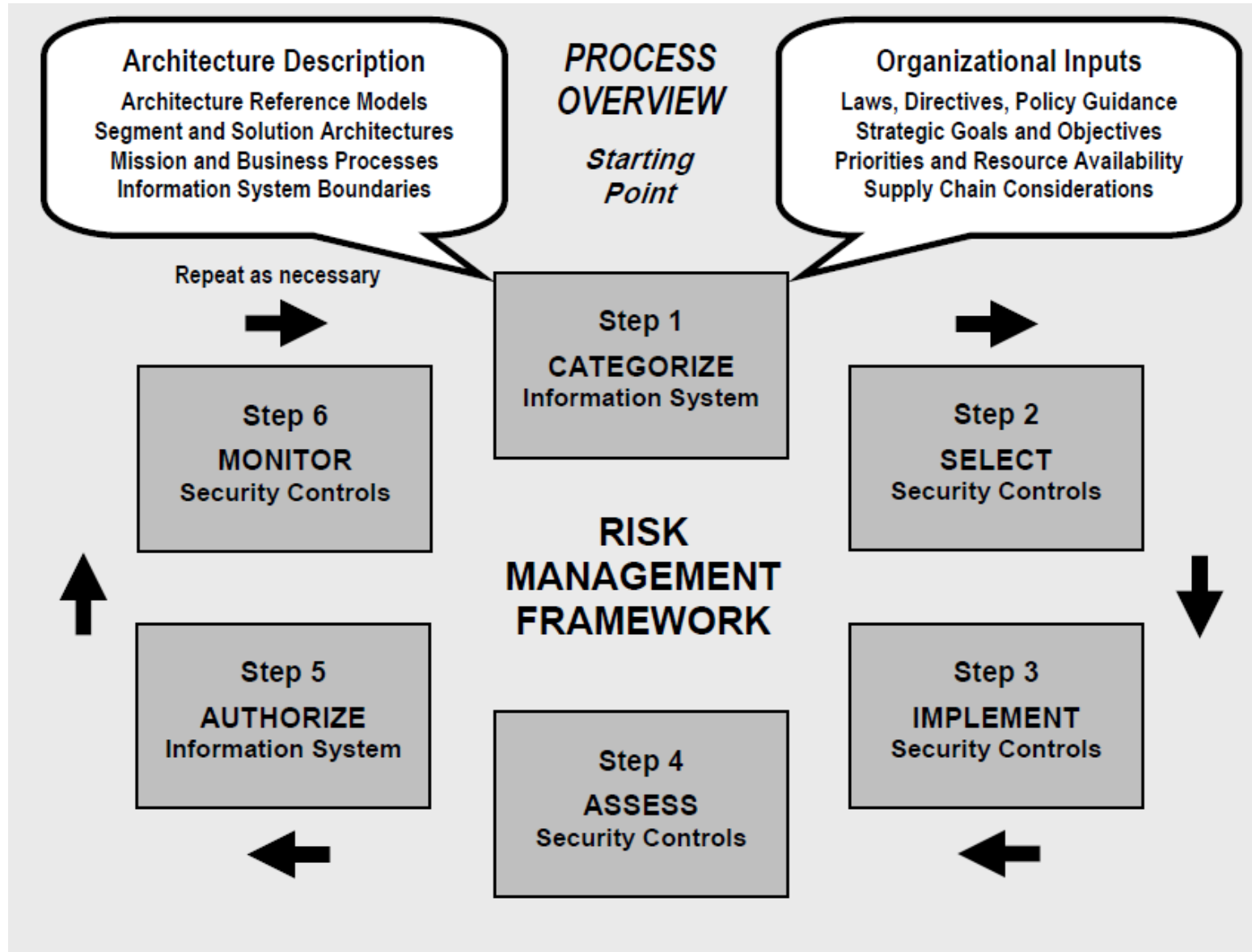
FIGURE 2-2: RISK MANAGEMENT FRAMEWORK

RMF For Cloud Environments

RMF4CE: Additional Tasks for a Cloud Consumer

RMF4CE — Cloud Ecosystem Consumer's Global View

STEP 6:
ONGOING MONITORING OF CONSUMER'S CONTROLS
ONGOING MONITORING OF PROVIDER'S OPERATIONS
RE-AUTHORIZE PROVIDER
MONITOR — Risk control

STEP 1:
➤ IMPACT ANALYSIS
➤ SYSTEM CATEGORIZATION
CATEGORIZE — Risk assessment

STEP 2:
➤ IDENTIFY & SELECT CAPABILITIES
➤ SELECT BASELINE CONTROLS
➤ TAILOR & SUPPLEMENT CONTROLS
➤ IDENTIFY & SELECT BEST-FITTING CLOUD ARCHITECTURE
➤ SELECT CLOUD PROVIDER
➤ NEGOTIATE SLA, METRICS, SIGN CONTRACT
➤ DEVELOP SECURITY PLAN
SELECT

STEP 5:
AUTHORIZE CLOUD-BASED INFORMATION SYSTEM
(BASED UPON RESIDUAL RISK & RISK TOLERANCE)
AUTHORIZE

STEP 4:
ASSESS SECURITY CONTROLS MANAGED BY PROVIDER
ASSESS SECURITY CONTROLS MANAGED BY CONSUMER
ASSESS — Risk treatement

STEP 3:
➤ IMPLEMENT SECURITY CONTROLS UNDER CONSUMER'S MANAGEMENT
IMPLEMENT

RMF For Cloud Environments

CLOUD SECURITY ARCHITECTURE TOOL (CSAT)
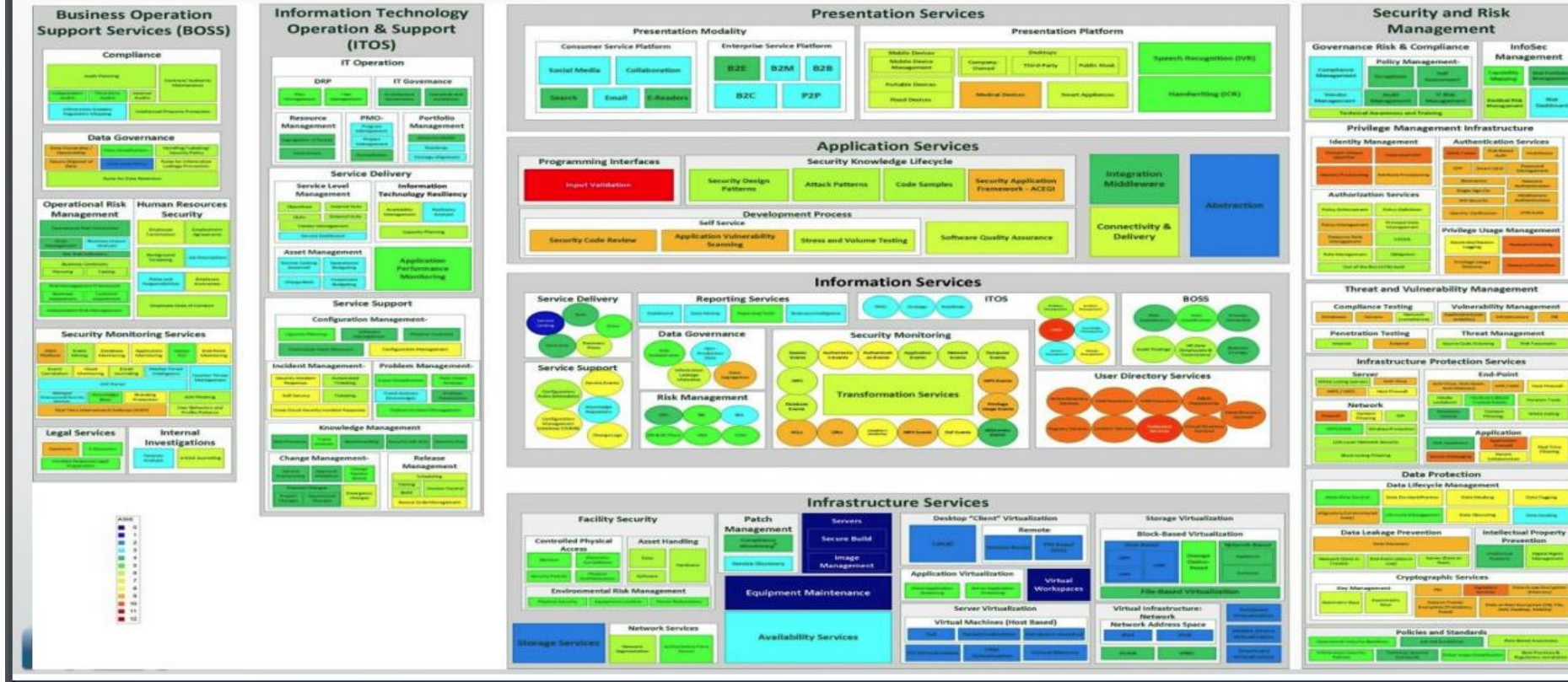
ISMS PROCESS CYCLE – ISO 27001
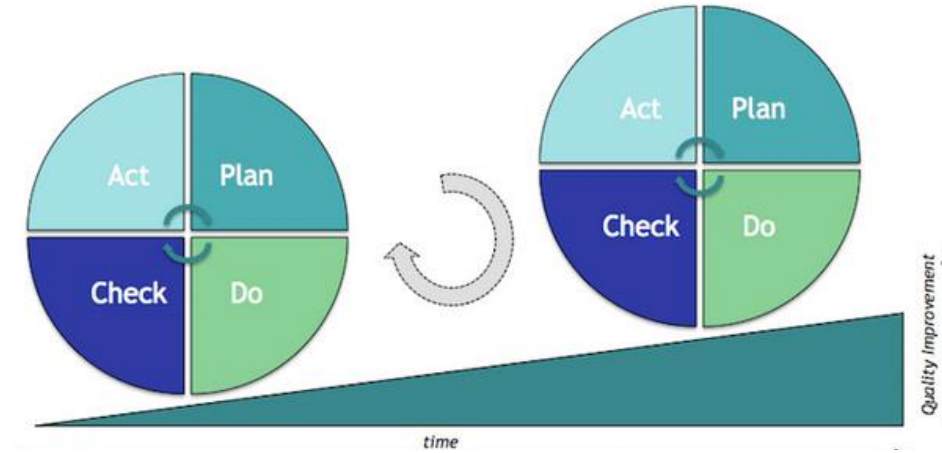
The origins of PDCA: The Deming cycle
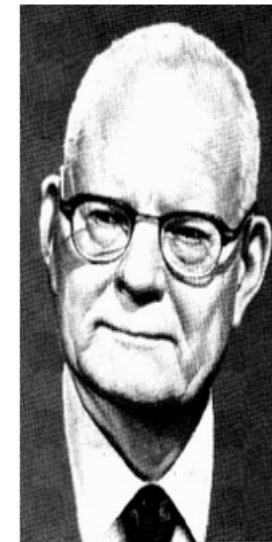
Plan-Do-Check-Act is also called the Deming Cycle because it was popularised by William Edwards Deming (image from Wikipedia). Deming was an American productivity consultant who lived from 1900-1993. Deming himself popularised his improvement cycle when visiting Japan after the second world war. He based his ideas on continuous improvement on the work of Walter Shewhart, and always referred to 'his' cycle as the Shewhart cycle.

The cycle is called Plan-Do-Check-Act because it consists of these four step (plan, do, check and act). Deming himself renamed the check step to study so a better name would have been Plan-Do-Study-Act or PDSA. Whatever name you choose, it all refers to the same framework for achieving continuous improvement. Deming developed the cycle when teaching in Japan in the 1950s.

17

Plan Do Check Act

4 Context of the organization	5 Leadership	6 Planning	7 Support	8 Operation	9 Performance Evaluation	10 Improvement
4.1 Understanding the organization and its context	5.1 Leadership & Commitment	6.1 Actions to address risks & opportunities	7.1 Resources	8.1 Operational planning & control	9.1 Monitoring measurement analysis & evaluation	10.1 Nonconformity & Corrective action
4.2 Understanding needs and expectations of third parties	5.2 Policy	6.1.2 IS Risk assessment process	7.2 Competence	8.2 Information security risk assesment	9.2 Internal audit	10.2 Continual improvement
4.3 Determining scope of ISMS	5.3 Org roles & responsibilities	6.1.3 IS rRsk treatment process	7.3 Awareness	8.3 Information security risk assessment	9.3 Management review	
4.4 ISMS		6.2 InfoSec objectives & plans to achieve them	7.4 Communication			
			7.5 Documented information			

Plan   Do   Check   Act

Risk Management - *OODA Loop*

Act

Accept, Transfer, Mitigate, Remediate, or Avoid the risk

Observe

Requirements and Work Products

On the surface – and how many people still interpret the OODA model – it seems to be a simple step-by-step loop. For our purposes here, in this series, we could reframe '**Observe' as 'sense**' – the process of sensing out what seems to be happening in our world – and '**Orient' as 'make-sense**' – literally 'sensemaking' from what we've observed – which leads us onward to **decide and act,** at which point we loop back to sense and make-sense again.

Decide

IT management goals for reducing risk

Recommended approaches

Allocate Budget and Resource

Orient (*You are here***)**

Identify trends

Remember This?

Distill the areas of risk

Identify a coordinator

Streamline the process & incorporate best practices

John Boyd's OODA Loop
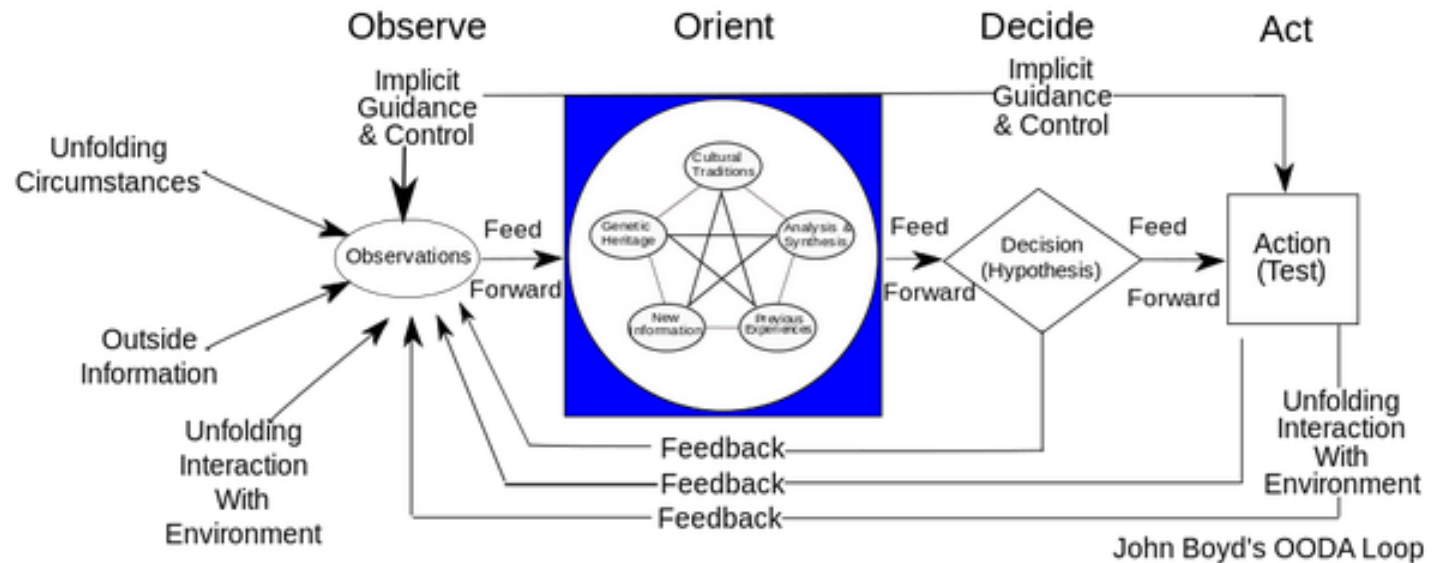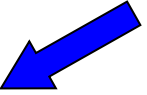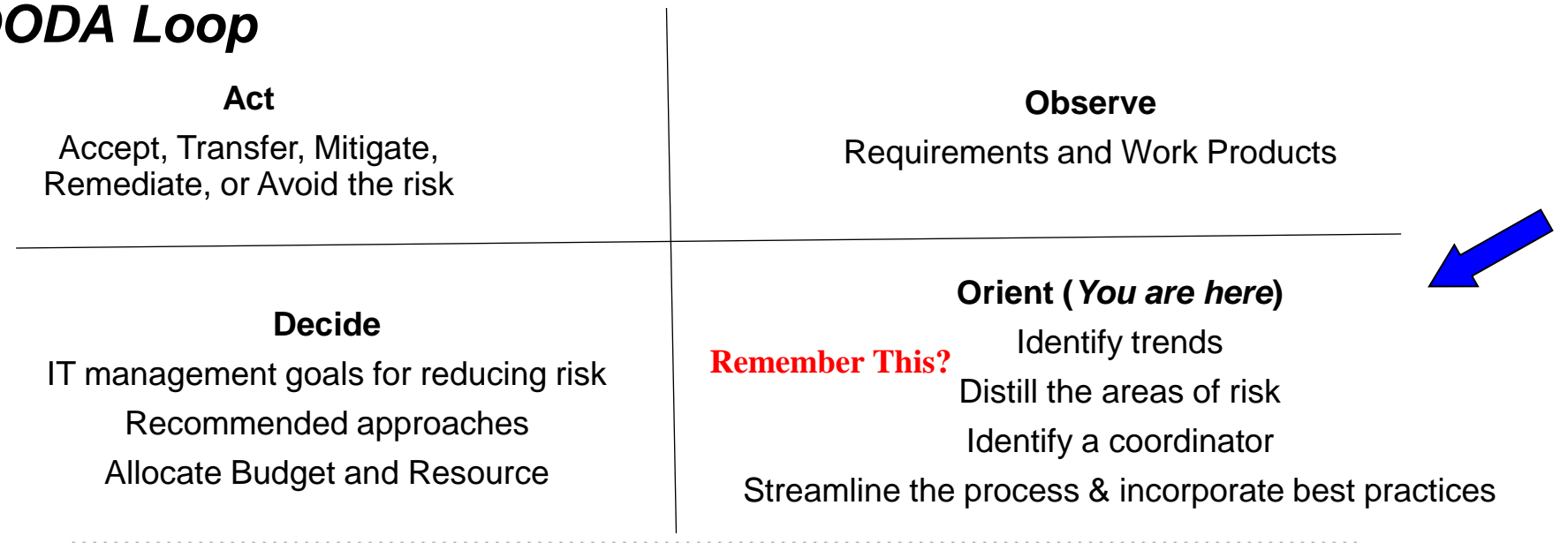
NIST Cybersecurity Framework –
Scope of The CSO office (CSF NIST 800-53)

OPPORTUNITY FOR FUTURE IMPROVEMENT

IDENTIFY

- ▸ Asset management
- ▸ Business environment
- ▸ Governance
- ▸ Risk assessment
- ▸ Risk management strategy

PROTECT

- ▸ Access control
- ▸ Awareness and training
- ▸ Data security
- ▸ Information protection and procedures
- ▸ Maintenance
- ▸ Protective technology

DETECT

- ▸ Anomalies and events
- ▸ Security continuous monitoring
- ▸ Detection process

RESPOND

- ▸ Response planning
- ▸ Communications
- ▸ Analysis
- ▸ Mitigation
- ▸ Improvements

RECOVER

- ▸ Recover planning
- ▸ Improvements
- ▸ Communications

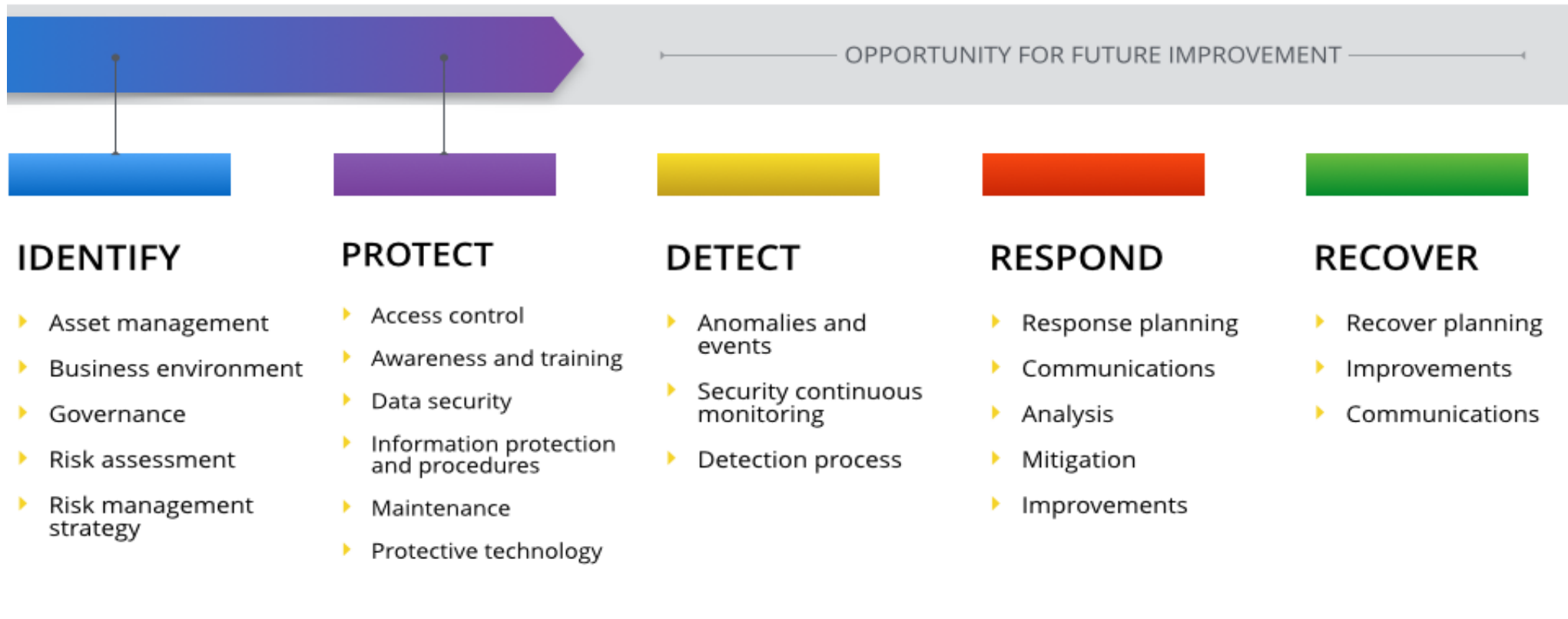# Table of Contents

▸ Cyberspace – Our Point of Departure

▸ Information Security Management Models

▸ Frameworks for Risk Management

▸ Smackdown – NIST CSF vs Big Scary Monsters

▸ Random Cybersecurity Attack Simulation Model (RCSM)

▸ References + Q&A

Global transformation caused by COVID-19

Artificial Intelligence (AI) in Agriculture

Home / Magazines / IT Professional / 2020.03

IT Risk and Resilience—Cybersecurity Response to COVID-19

Authors

Tim Weil, SecurityFeeds LLC
San Murugesan, Western Sydney University

Abstract

The rapid and worldwide spread of the coronavirus and its illness known as COVID-19 has made huge impact on almost everything has taken us all by surprise. We all are now experiencing a major unprecedented and unexpected global public health crisis. This pandemic has also triggered huge social upheavals, disrupted almost every industry, and impacted the life and work of everyone in almost every country. Businesses and educational institutions are closed, many employees are forced to work from their homes, supply chains have been disturbed, people are being required to self-isolate, and most travel, in-person meetings, and conventions have been banned. These disruptions could continue for months, and the resulting economic, business, and social impact will last for years.

11/7/2020

Global transformation caused by COVID-19

Industry	Response/Impact	Response	Underlying technology/ operation
Education	Widespread closure of educational institutions; access to labs is restricted; projects have been mothballed; and fieldwork interrupted	Virtual learning environment (online teaching, presentation, assessment, and consultation); convocation online	Online video conferencing software, virtual labs on cloud
Healthcare	Overcrowded hospitals, inability to meet the demands on them	Contact tracing, forecasting resource requirements, allotment of scare resources based on a patient's survivability, COVID-19 vaccine development, telehealth (online consultation with a doctor or medical professional); automated diagnosis	AI, ML, cloud computing, chatbot
Business	Closure of business, avoidance ofin-person retail shopping	Adherence to social distancing, services online, work from home	Chatbot, drone delivery, online meeting software, virtual office/desktop, remote access to work
Industry	Closure of business, avoidance of in-person retail shopping	Work from home, remote operations, automation and autonomous operation	Robots, automation, 3-D printing
Retail	Stores closed, only online service, avoidance of retail shopping	Online shopping, home delivery	The Web, online payment, contactless payment
Government	Spike in demands from citizens for assistance, disruption to normal operations	Migration to online services	Cloud, the Web, online meeting application
Entertainment	Entertainment venues (parks, cinema) closed, sports without spectators	Viewing online	Audio and video streaming, virtual reality
Personal life and social interaction	Lockdown	Indoor activities	Phone, audio and video chats, streaming, online gaming
Spirituality and religious practices	Places of worship closed	Online participation, prayers from home, worship through livestream	Audio and video streaming, virtual reality
Conferences	In-person conferences banned; virtual conferences	Online presentation and discussion	Video streaming, virtual conference software

11/7/2020

Global transformation caused by COVID-19

https://www.thinkcsc.com/nist-cybersecurity-framework/

COVID-19 Made a NIST Cybersecurity Framework More Critical for Ohio Businesses

The Ohio Data Protection Act

As a refresher, the Ohio Data Protection Act provides businesses that store or transmit personal information a safe harbor in the event they experience a breach. However, you can only qualify if you follow the NIST cybersecurity framework. This Act is a significant step forward for all organizations interested in limiting their liability should a data breach occur. It offers clear steps to organizations on what they must do to qualify for safe harbor under the Act. With or without a pandemic, minimizing risk of liability while simultaneously establishing better protocols to protect your customers and your data is a win-win.

Principals of a NIST-Based Cybersecurity Network

The threat landscape continues to grow more complex. As a result, cyberattacks are more sophisticated than ever. New threats are discovered daily. The NIST framework is designed to help you have a comprehensive cybersecurity strategy in place to protect your organization, your people, your data, and your customers.

The principals of the NIST framework are:

- Use common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors, and uses
- Risk-based
- Based on international standards
- A living document
- Guided by many perspectives – private sector, academia, public sector

11/7/2020

Global transformation caused by COVID-19

CYBERSECURITY FRAMEWORK (CSF)

CSF Core

What processes and assets
need protection?

What safeguards are available?

What techniques can identify
incidents?

What techniques can contain
impact of incidents?

What techniques can restore
capabilities?

Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**
Detect	Anomalies and Events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detection Processes	**DE.DP**
Respond	Response Planning	**RS.RP**
	Communications	**RS.CO**
	Analysis	**RS.AN**
	Mitigation	**RS.MI**
	Improvements	**RS.IM**
Recover	Recovery Planning	**RC.RP**
	Improvements	**RC.IM**
	Communications	**RC.CO**

Figure 2: Some online and virtual computing services promoted by
COVID-19 induced social distancing.

11/7/2020

Global transformation caused by COVID-19

CYBERSECURITY FRAMEWORK (CSF)

CSF Core

Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**
Detect	Anomalies and Events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detection Processes	**DE.DP**
Respond	Response Planning	**RS.RP**
	Communications	**RS.CO**
	Analysis	**RS.AN**
	Mitigation	**RS.MI**
	Improvements	**RS.IM**
Recover	Recovery Planning	**RC.RP**
	Improvements	**RC.IM**
	Communications	**RC.CO**

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

Figure 2: Some online and virtual computing services promoted by COVID-19 induced social distancing.

Global transformation caused by COVID-19 - CYBERSECURITY FRAMEWORK (CSF) - Recover

IS Audit/Assurance Progam Cybersecurity: Based on the NIST Cybersecurity Framework - Recover					
Process Sub-Area	**Ref. Risk**	**Control Objectives**	**Controls**	**Testing Step**	**Ref. Framework/ Standards**
Recovery Planning		Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	Recovery plan is executed during or after an event.	1. Obtain a copy of the organization's recovery plans and procedures (e.g., business continuity plan, incident response plan, disaster recovery plan, cybersecurity incident plan) and the documented results of recent cybersecurity events or event tests. 2. Evaluate documentation for the following: a. Frequency of testing b. Coverage of critical pieces of the organization's recovery plans and procedures c. Documentation of incidents (e.g. power outages, communication failures, system outages, attempted and successful malicious or careless unauthorized access or disruption).	ISO/IEC 27001:2013 A.16.1.5
Improvements		Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery plans incorporate lessons learned.	1. Obtain a copy of results of recent cybersecurity events or event tests. 2. Evaluate documentation for the following: a. Documented lessons learned and analysis of failed or missing controls b. Action items designed to improve recovery plans and procedures based on the lessons learned and analysis	
			Recovery strategies are updated.	1. Obtain a copy of the organization's recovery plans and procedures (e.g., business continuity plan, incident response plan, disaster recovery plan, cybersecurity incident plan) and the documented results of recent cybersecurity events or event tests. 2. Determine if recovery plans and procedures are reviewed, updated and approved on a regular basis or as changes are made to systems and controls.	

Figure 2: Some online and virtual computing services promoted by COVID-19 induced social distancing.

11/7/2020

The NIST Cybersecurity Framework (CSF)
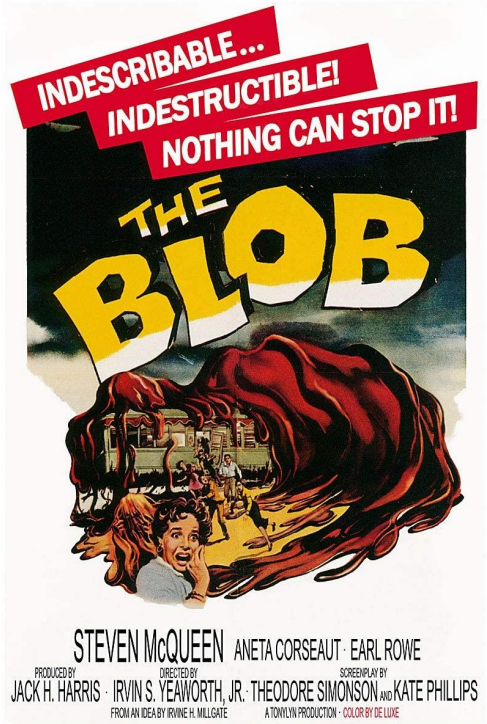
The Blob is an amorphous mass of alien goo that appears in the 1958 film of the same name. Appearing as nothing more than a mass of red gelatin, this creature possesses animalistic intelligence, acting purely on the instinct to feed. It feeds on flesh and gains mass as it consumes other creatures

Them While investigating a series of mysterious deaths, Sergeant Ben Peterson finds a young girl agent Robert Graham and scientist Dr. Harold Medford), he discovers that all the incidents are due to giant ants that have been mutated by atomic radiation. Peterson and Graham, with the aid of the military, attempt to find the queen ants and destroy the nests before the danger spreads.

The NIST CSF industry experts and members of the National Institute of Standards and Technology (NIST), a federal agency within the U.S. Department of Commerce. NIST CSF focuses on five core functions: **Identify, Protect, Detect, Respond and Recover**. These categories cover all aspects of cybersecurity, which makes this framework a complete, risk-based approach to securing almost any organization

11/7/2020

CSF Identify Categories related to COVID-19
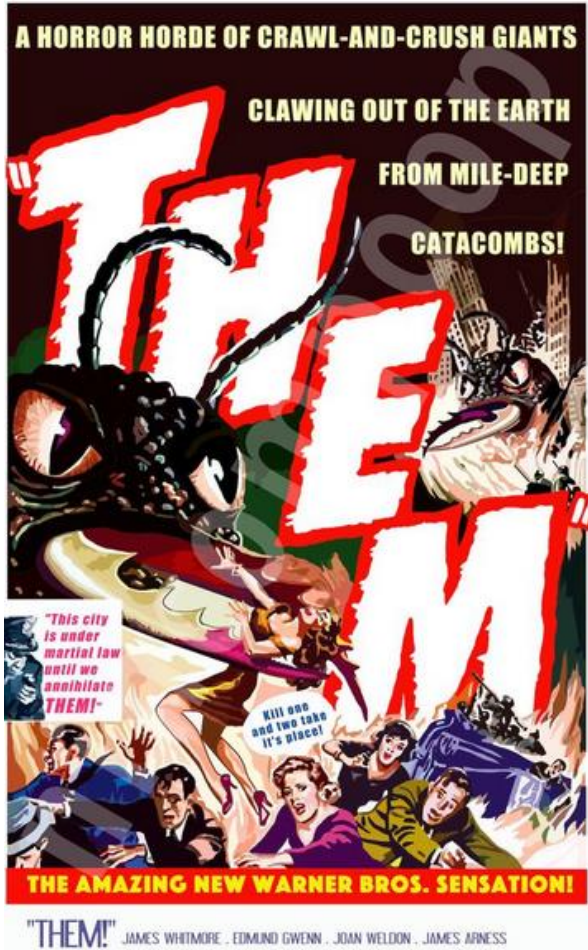
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM

Cybersecurity management response	Online resource
CxO Education (Security Architects Partners)	https://security-architect.com/waking-up-to-the-new-covid-19-cybersecurity-reality/
COVID-19 Joint Acquisition Task Force	https://www.acq.osd.mil/jatf.html
US DHS Cyber and Infrastructure Agency (CISA)	https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf
NIST SP 800-46 Guide to enterprise telework, remote access, and BYOD security	https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

11/7/2020

CSF Identify Controls for COVID-19
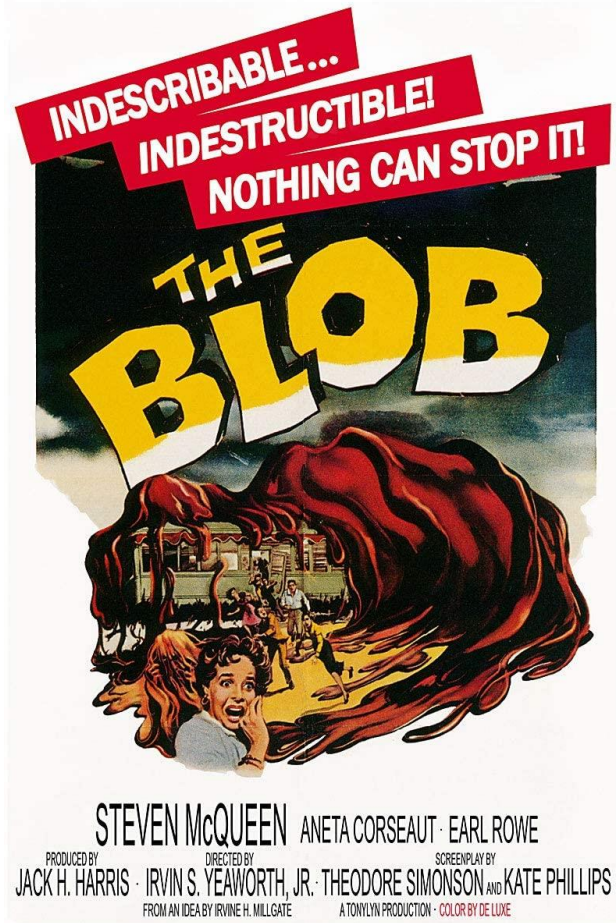
CISA INSIGHTS
Risk Management for Novel Coronavirus (COVID-19)

The Threat and How to Think About It

This product is for executives to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19. According to the U.S. Centers for Disease Control and Prevention (CDC), COVID-19 has been detected in locations around the world, including multiple areas throughout the U.S. This is a rapidly evolving situation and for more information, visit the CDC's COVID-19 Situation Summary.

COVID-19 Risk Profile

As of March 2020, the CDC notes that most people in the United States have little immediate risk of exposure to this virus. The virus is NOT currently spreading widely in the United States.

In anticipation of a broader spread of COVID-19, globally

CISA's Role as the Nation's Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is working closely with partners to prepare for possible impacts of a COVID-19 outbreak in the United States. COVID-19 containment and mitigation strategies will rely heavily on healthcare professionals and first responders detecting and notifying government officials of occurrences.

CISA will use its relationships with interagency and industry partners to facilitate greater communication, coordination, prioritization and information-sharing between the private sector and the government.

What's in this guide:
- Actions for Infrastructure Protection
- Actions for your Supply Chain
- Cybersecurity for Organizations

	Asset Management	ID.AM
	Business Environment	ID.BE
Identify	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM

https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf

CSF Protect Controls for COVID-19 –

https://security-architect.com/waking-up-to-the-new-covid-19-cybersecurity-reality/

# This Pandemic is Making Amateur Epidemiologists of Us All

We're living in trying times and it's clear that the coronavirus (aka COVID-19) will be a landmark event for us all including yourself, your business, and your security team.

Last week I was busy trying to get in touch with CISOs and other business or security leaders. I was attempting to complete 100 interviews before my book Rational Cybersecurity for Business publishes soon. But nobody was getting back to me. I noticed that just about every conversation seemed to start with the Coronavirus.

Half the time we wouldn't even say "coronavirus" but just refer to "it." We'd each know exactly what the other was talking about. We've been re-examining our lives as individuals, families, teams, and businesses in the light of the new reality.

Top Security Concerns in Coronavirus Times

- Securing remote access
- Mitigating new fraud and malware threats
- Assessing new suppliers
- Ensuring core information system security and availability
- Refactoring security programs for new architectural realities (or budget cuts)
- Maintaining security team morale, focus
- Aligning with business leadership
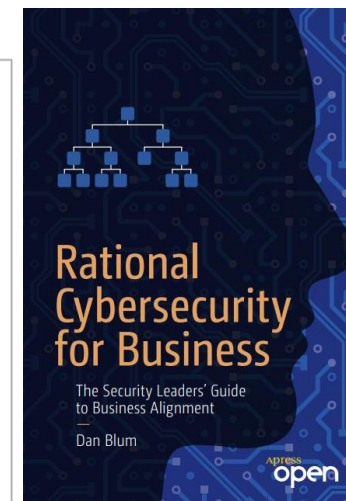
Rational Cybersecurity for Business
The Security Leaders' Guide to Business Alignment
Dan Blum
Apress open

Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT

Rational Cybersecurity for Business The Security Leaders' Guide to Business Alignment Authors: Dan Blum
https://www.apress.com/us/book/9781484259511

11/7/2020

CSF Protect Controls for COVID-19 –

Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP

Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT

Exposure
- Phishing and Malware
- Remote Work Tools
- Shadow IT
- Remote Desktops
- Personnel Disruption

Remediation
- Security Monitoring
- Data Protection and Privacy
- Application Security / VPN for Telework
- Secure Privileged Access Management
- Risk-based Threat Monitoring Program

11/7/2020

CSF Detect Controls for COVID-19 - Threats and Vulnerabilities

Threats and Vulnerabilities provides industry example of the CSF Protect / Detect examples listed here. They include: –

ZOOM bombing - Security and privacy vulnerabilities in teleconferencing software allow trolling hackers to intercept authentication credentials and inject objectionable content

COVID-19 phishing attacks – As reported in FBI bulletins there were fake, malicious emails that appeared to be from the Center for Disease Control (CDC). They contained malware attachments, or aimed to hijack user credentials.

Malware – An example of malware is a Corona Trojan overwriting master boot record (mbr) and disabling hard disk storage. Ransomware attacks on healthcare systems have been escalating during the pandemic.

Network Availability –While performance of core communication networks and clouds remained satisfactory despite substantial increase in traffic, some collaborative applications faced spikes in service outages

Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP

Threats and Vulnerabilities	Online Resource
ZOOM bombing	https://delta.ncsu.edu/news/2020/04/02/zoom-security-and-privacy/
Spyware and Phishing	https://www.coalfire.com/The-Coalfire-Blog/March-2020/COVID-19-incites-cyber-crimes-of-opportunity
Malware and Phishing	https://www.webarxsecurity.com/covid-19-cyber-attacks/
Health Check – ISPs, Cloud Providers, UCaaS During Pandemic_	https://www.networkworld.com/article/3534130/covid-19-weekly-health-check-of-isps-cloud-providers-and-conferencing-services.html
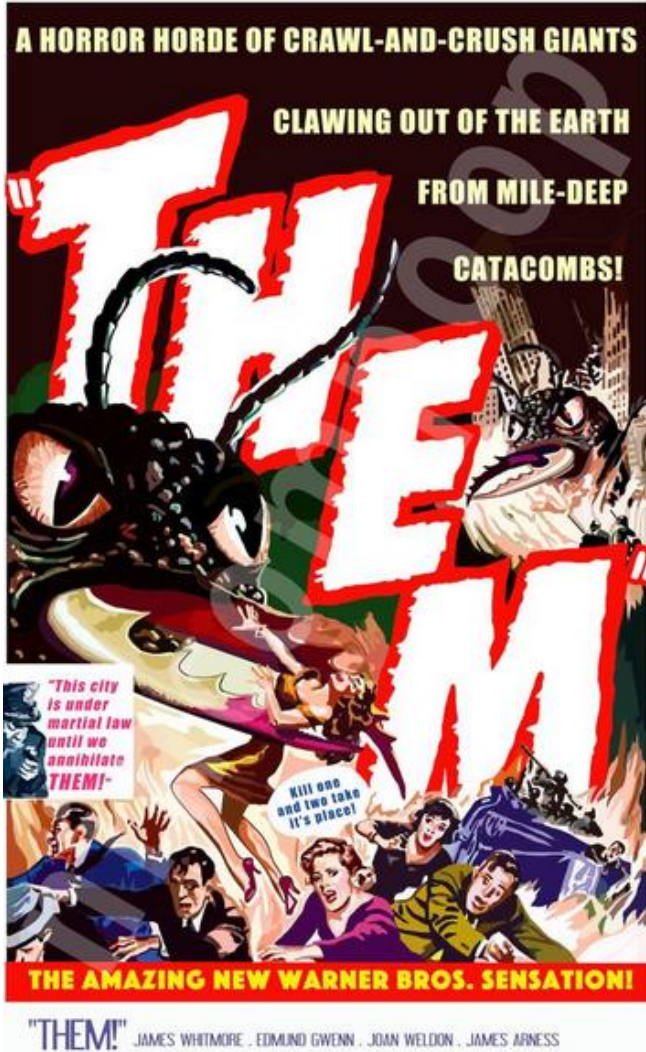
11/7/2020

CSF Detect Controls for COVID-19

Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP

Date	Description of cyber attack	Type of attack
4/8/2020	The exposure to compromised e-commerce websites is greater than ever. 26% increase in web skimming in March.	Malware
4/8/2020	'Latest vaccine release for Corona-virus (COVID-19)' mall spam spreads NanocoreRAT malware	Malware
4/8/2020	NCSC Advisory: COVID-19 exploited by malicious cyber actors	Social Engineering
4/7/2020	Fake COVID19 website is spreading FirebirdRAT via fake DHL emails	Malware
4/6/2020	Rush to adopt online learning under COVID-19 exposes schools to cyberattacks	Zoom bombing
4/4/2020	Sophisticated COVID-19–Based Phishing Attacks Leverage PDF Attachments and SaaS to Bypass Defenses	Phishing, Malware
4/4/2020	CDC Warns of COVID-19-Related Phone Scams, Phishing Attacks	Phishing

https://www.webarxsecurity.com/covid-19-cyber-attacks/

11/7/2020

CSF Respond Controls for COVID-19

INDESCRIBABLE...
INDESTRUCTIBLE!
NOTHING CAN STOP IT!

THE BLOB

STEVEN McQUEEN · ANETA CORSEAUT · EARL ROWE
PRODUCED BY JACK H. HARRIS · DIRECTED BY IRVIN S. YEAWORTH, JR. · THEODORE SIMONSON AND KATE PHILLIPS
FROM AN IDEA BY IRVINE H. MILLGATE · A TONYLYN PRODUCTION · COLOR BY DE LUXE

Wanted urgently: People who know a half century-old computer language so states can process unemployment claims

By Alicia Lee, CNN

Two men operating a mainframe computer, circa 1960.

CYBERSECURITY FRAMEWORK VERSION 1.1
RECOVER · IDENTIFY · PROTECT · DETECT · RESPOND

Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM

Cybersecurity risk mitigations	Online resource
Organizational resilience (Deloitte)	https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/about-deloitte/CoronaVirus_POV_People%20Technology%20Path_Central_Europe.pdf
Legacy Software (COBOL) Supporting Financial Systems	https://www.cnn.com/2020/04/08/business/coronavirus-cobol-programmers-new-jersey-trnd/index.html
Fired Americans Send Unemployment Websites Crashing Down	https://www.bloomberg.com/news/articles/2020-03-25/fired-americans-send-state- unemployment-websites-crashing-down

11/7/2020

"THEM!" JAMES WHITMORE . EDMUND GWENN . JOAN WELDON . JAMES ARNESS

COVID-19

People, technology, and the path to organizational resilience

Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM

› **Response strategy:**
- review BC/disaster recovery plans;
- establish a crisis management office;
- develop a communications plan.

› Personnel management (health and safety):
o - enforce precautionary measures and revisit sick leave policies;
o - review/amend policies for remote work, including guidelines on travel;
o plan for absenteeism.

› **Continuity of operation:**
- rationalize technology projects and portfolios;
- equip your connectivity, security, and infrastructure for new traffic and use patterns;
- be ready for disruptions in your business and technology ecosystem.

11/7/2020

CSF Recover Controls for COVID-19 –
https://www.securityfeeds.us/pandemic-response-risk-and-resilience

SecurityFeeds
Your source for enterprise security management

Pandemic Response (Risk And Resilience)
Home

Pandemic Response (Risk And Resilience)

- DHS CISA Insights (COVID-19) Portal
- Uptime Institute - Data Center Response Bulletin to COVID-19
- COVID-19 Through the Business Technology Lens (Cutter Group)
- Cybersecurity's New Reality from COVID-19 (Security Architects Partners)
- Johns Hopkins COVID-19 Resource Center
- US Drive-Through Testing for COVID-19
- Teleconference Security and Privacy (ZOOM)
- SIR Model for COVID-19 Contagion in Italy
- IBM Watson - International 'Chatbot' for COVID-19 Support
- Global Systemic Risk and Resilience for COVID-19 (Wiley CFP)
- Economic Impact of Coronavirus (World Economic Forum)
- COVID-19 Medical Research (Reddit)
- Staying Secure in Response to COVID-19 (Optiv)
- US DoD (OSD) - COVID-19 Joint Acquistion Task Force

|	Response Planning	RS.RP
Respond	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM

Steve fends off the encroaching Blob with a fire extinguisher, which leads to the discovery that the Blob hates the cold. Steve relays this info to the police, and soon the people of Downingtown band together to take down the Blob.

There's no way to kill the Blob, so the Air Force stuffs it in a giant box and dumps it in the Arctic.

Recovery and Resilience – IT Context for Business Continuity

2.3 Where does business continuity belong?

Risk managment

Information security

Cybersecurity

Bussiness continuity

Information technology
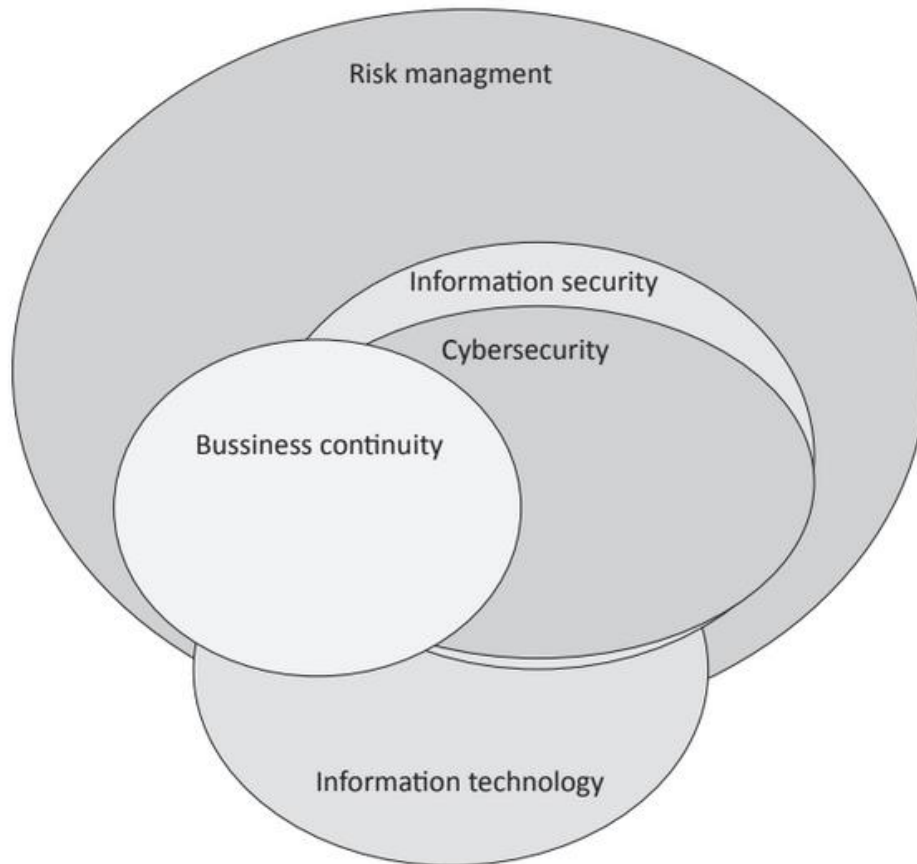
DEFINITIONS/TERMINOLOGY

- **IT resilience:** IT resilience refers to an organization's ability to protect data in the event of any unplanned or planned disruption and, simultaneously, support data-oriented initiatives for business modernization and digital transformation.

- **Digital transformation:** Digital transformation describes the process of transforming decision making with technology. Digital transformation is an enterprisewide, board-level strategic reality for companies that are serious about ensuring their businesses deliver an exceptional customer experience and becoming leaders in the digital economy. Digital transformation is a multiyear effort, with specific goals and objectives around markets and customers, revenue, and profit growth.

- **Data protection:** Data protection refers to the protection, restoration, and recovery of data in the event of physical or logical errors. This includes products and services that support both physical and virtual infrastructures.

- **Disaster recovery:** Disaster recovery is a combination of solutions that provide replication of physical or virtual servers and failover workload recovery in the event of a hardware failure or man-made or natural catastrophe. Disaster recovery solutions typically provide replication of data and applications with assigned recovery point objectives, where data and applications will have a set "age" where recovery from backup storage for normal operations can occur if a server, system, or network suffers a failure. Solutions also have a recovery time objective, which is the time frame in which the enterprise will regain normalized access to the data and applications being supported.

- **Hybrid cloud:** Hybrid cloud is an application deployment environment that utilizes both on-premises private cloud resources (i.e., local datacenter) and off-premises public or managed cloud resources to deliver the totality of the application functionality.

- **Multicloud:** Multicloud is an infrastructure deployment environment that utilizes two or more off-premises public or managed cloud resources for complete or partial application delivery.

""Becoming Resilient " Dejan Kosutic

11/7/2020

	Recovery Planning	RC.RP
Recover	Improvements	RC.IM
	Communications	RC.CO

CSF Recover Controls for COVID-19

https://www.acq.osd.mil/jatf.html

Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

11/7/2020

Table of Contents

▶ Cyberspace – Our Point of Departure

▶ Information Security Management Models

▶ Frameworks for Risk Management

▶ Smackdown – NIST CSF vs Big Scary Monsters

▶ Random Cybersecurity Attack Simulation Model (RCSM)

▶ References + Q&A

1st Citation for 'IT Risk and Resilience – Cybersecurity Response to COVID-19'

IT Risk and Resilience-Cybersecurity Response to COVID-19.

☐ Search within citing articles

[PDF] Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era

K Okereafor, O Adelaiye - researchgate.net

The social distancing practices triggered by the COVID-19 pandemic have caused a huge growth in the use of online technologies to support remote work, resulting in a sharp rise in computer crimes, privacy breaches and service disruptions across the globe. Cyber …

☆ 〝 All 2 versions ≫

[PDF] researchgate.net

Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP

▸ Cyber attackers are taking advantage of COVID-19 anxiety to launch email scams, misinform and mislead unsuspecting targets, and propagate harmful software using various threats. The trend beckons for a more proactive cybersecurity approach to detect, prevent, and mitigate potential computer crimes. This paper proposes **a Randomized Cyberattack Simulation Model (RCSM),** an enhanced cyber attack readiness checklist for tackling computer crimes in advance. The RCSM extends traditional incident response and offers **a pre-forensic guide as a precursor to the redefinition of cybersecurity in the post COVID-19 digital era.**

▸ Cyber attack incidents have been on a steady increase, with their impacts including rising financial implications [4] and millions of dollars [5] in tangential losses. Most attacks occur even in the midst of traditional mitigation methods, using obfuscation to evade [6] detection and gain persistence in the system [7]. **Most recent cyber attacks use un-identified attack methods, which make signature-based detection grossly ineffective** [8], including the recovery approach proposed by *Weil and Murugesan [9]*.

Global transformation caused by COVID-19

Table 1: Popular cyber attacks and threats in the COVID-19 pandemic

SN	Cyber threat	Impact	Mitigation
1.	**Spear phishing and spam emails:** Unsolicited and deceptive emails that impersonate known brands and high-profile personalities, with the intention to extract confidential information or propagate other malware.	• Data leak • Data alteration • Data loss • Privacy infringement • System crash • Identity theft • Reputational damage • Revenue loss • Service disruption • Operational inefficiency • Regulatory fines • Public disclosure • Litigation • Scandal and fatality	• Intrusion detection • Intrusion prevention • Anti-malware tools • Cybersecurity awareness • Security training • Endpoint protection • Perimeter protection • Firewalling • Proper encryption • Steganography • Machine learning • Anomaly detection
2.	**Malware:** Hostile and disruptive software code that causes harm and undesirable outcome on the victim's computer or digital asset including unauthorized access and illegal data alteration. E.g. ransomware, computer virus, adware, spyware, worms, trojan, etc.		
3.	**Website highjack:** The seizure of a website by a cyber attacker who has gained full administrative control of the entire contents of the website for malicious intents including posting offensive content and propagating own ideologies.	• Ransom demand • Defaced content • Deep fakes • Fake news • Scandal • Image smearing • Service disruption • Occupational nuisance • Reputational damage	• Proper encryption • Sound password ethics • Biometric authentication • Multi-factor authentication • Steganography • Honeypot • Public disclaimer • Corporate damage control
4.	**Website cloning:** The illegal replication of a victim's		

Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP

Cyber attacks during COVID-19
- Spear phishing and SPAM email
- Malware
- Website highjack
- Website cloning
- Cyber espionage

Okereafor, Kenneth & Adelaiye, Oluwasegun. (2020). Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. 05. 61-72.

11/7/2020

Global transformation caused by COVID-19
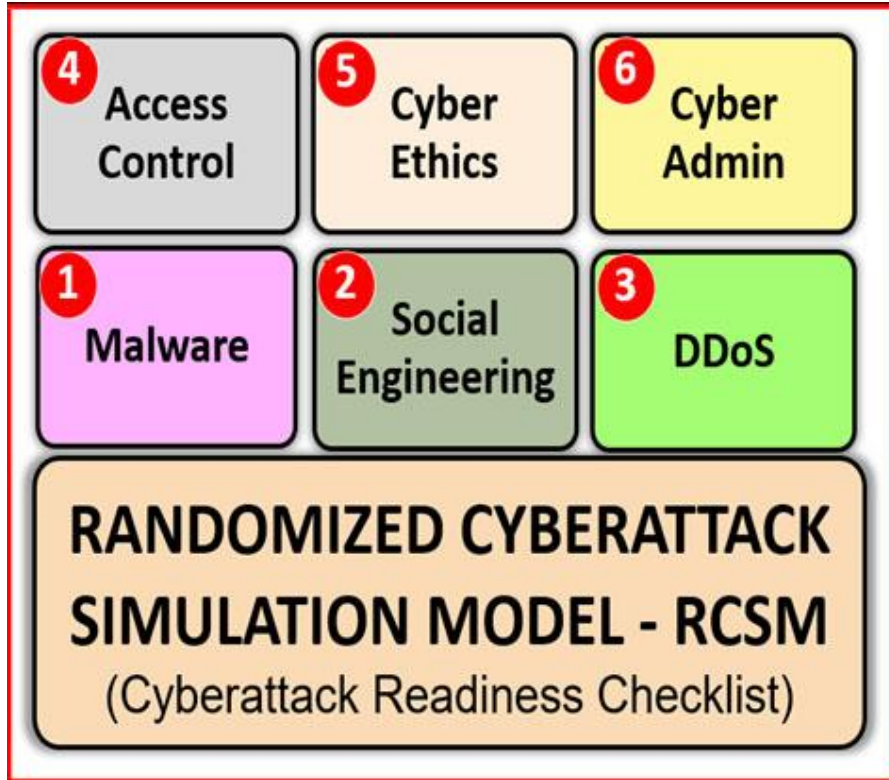
Okereafor, Kenneth & Adelaiye, Oluwasegun. (2020). Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. 05. 61-72.

Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT

The RCSM provides an easy-to-reference set of best practices for incident response teams to evaluate and assess, in advance, the IT infrastructure's resilience and preparedness to neutralize malicious activities and resist spontaneous cyber attacks. As a novel cyber attack simulation approach, it is designed to offer an instantaneous checklist for the cyber defence preparedness of the organization, with the following key features:

1. Proactively analyses the scope of vulnerabilities in critical applications.
2. Appraises the strengths and capabilities of existing controls.
3. Strengthens the organization's pre-forensic and cybersecurity functions.
4. Differs from a pre-scheduled vulnerability and penetration testing.
5. Deployed rather spontaneously in a typical security drill fashion.
6. Detects weak controls that must be compulsorily fixed in advance.
7. Evaluates how incident responders truly react to unexpected attacks.

[PDF] IT Risk and Resilience-Cybersecurity Response to COVID-19.
T Weil, S Murugesan - securityfeeds.us
The rapid and worldwide spread of the coronavirus and its illness known as COVID-19 has made huge impact on almost everything has taken us all by surprise. We all are now experiencing a major unprecedented and unexpected global public health crisis. This …
☆ 〰 Cited by 2 Related articles ⨠

11/7/2020

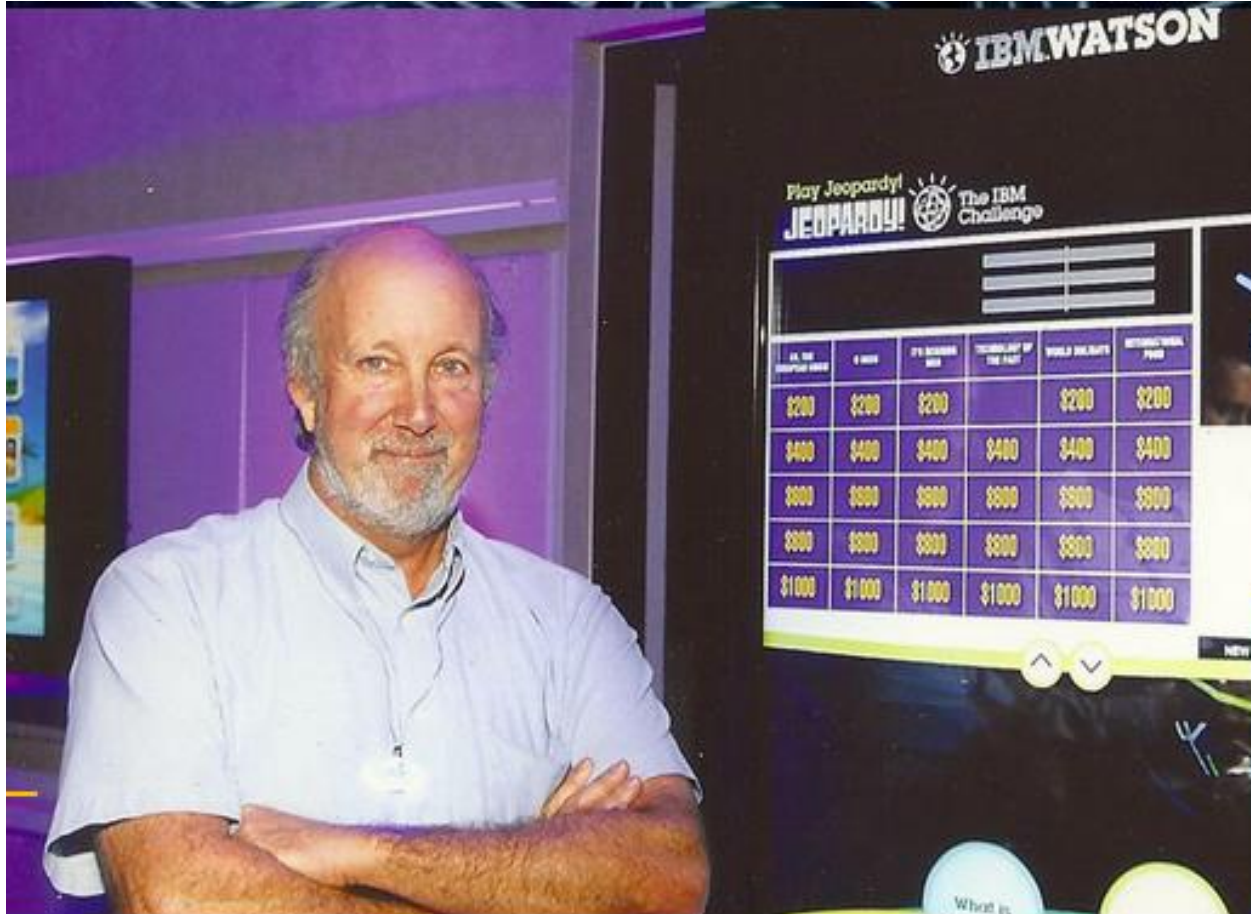# Assessing Cybersecurity Response to COVID-19 – Blue Sky or Rain?

Table of Contents

▸ Cyberspace – Our Point of Departure

▸ Cyberspace – Our Point of Departure

▸ Information Security Management Models

▸ Standards for Cloud Risk Assessment - What's Missing?

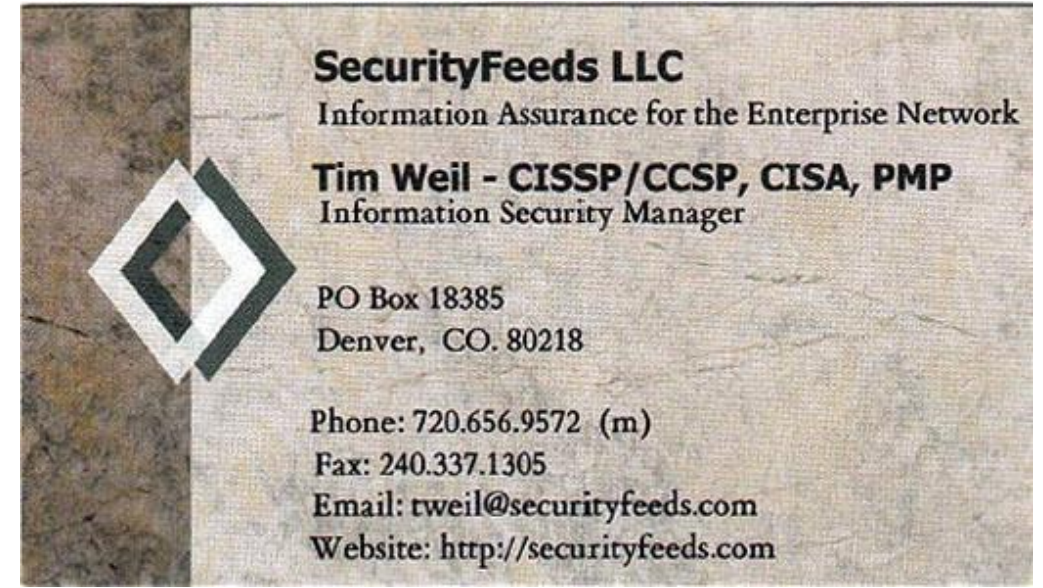▸ Tools and Techniques for Cloud Security Risk Assessments

▸ References + Q&A

References – IT Risk and Resilience – Cybersecurity Response to COVID-19

▶ T. Weil and S. Murugesan, "IT Risk and Resilience—Cybersecurity Response to COVID-19," in IT Professional, vol. 22, no. 3, pp. 4-10, 1 May-June 2020, doi: 10.1109/MITP.2020.2988330. https://ieeecs-media.computer.org/media/marketing/cedge_digital/ce-oct20-final.pdf

▶ Okereafor, Kenneth & Adelaiye, Oluwasegun. (2020). Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. 05. 61-72.

▶ M. Reeves, et al., "Sensing and shaping the post-COVID era," Boston Consulting Group, Apr. 3, 2020. [Online]. Available: https://www.bcg.com/publications/2020/8-ways-companies-can-shap-reality-post-covid-19.aspx

▶ "Five functions of the cybersecurity framework," NIST. Apr. 2018. [Online]. Available:https://www.nist.gov/cyberframework/online-learning/five-functions

▶ Cybersecurity framework," NIST. Apr. 2018. [Online]. Available: http://www.nist.gov/cyberframework

▶ "CISA INSIGHTS: Risk Management for Novel Coronavirus (COVID-19)," CISA. Mar. 18, 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf

Thank you for joining us!

SecurityFeeds LLC
Information Assurance for the Enterprise Network

Tim Weil - CISSP/CCSP, CISA, PMP
Information Security Manager

PO Box 18385
Denver, CO. 80218

Phone: 720.656.9572 (m)
Fax: 240.337.1305
Email: tweil@securityfeeds.com
Website: http://securityfeeds.com

SecurityFeeds LLC provides IT Management Consulting services

- Communications and Security Engineering
- Data Processing (Systems Engineering)
- Project and Program Management
- Risk Management (ISO 27001)

Our expertise includes Enterprise Security Architecture, Cloud Security, Program Management, and Network Engineering.

"RISK is a four-letter word"

http://www.securityfeeds.com - **trweil@ieee.org**

SecurityFeeds
Your source for enterprise security management

Your Source For Enterprise Security Management

Security Architecture | Cloud Security | Program Management | Systems Engineering | ISO 27001 | Risk Management and Compliance | Secure Automotive Network (V-PKI Hits the Highway) | Secure Automotive Networking for ITS

IT Professional
Technology Solutions for the Enterprise

VOLUME 20, NUMBER 3   MAY/JUNE 2018

Welcome To SecurityFeeds

Tim Weil is an IT Security Program Manager with over twenty five years' experience in data processing, communications engineering, and information assurance (IA).

His areas of expertise include FedRAMP/FISMA compliance for federal agencies and cloud service providers, IT Service Management, cloud security (FedRAMP), enterprise risk management (NIST) for federal agencies and ISO 27001 compliance for commercial clients.

48

The Write Stuff – Submitting articles to IT Professional

General Submissions (IT Pro Magazine)

IT Professional, an IEEE Computer Society magazine designed for developers and managers of enterprise information systems, seeks original submissions for publication.   Articles should be approximately 4,200 words (with about three figures or images counting as 300 words each) and no more than 20 references. Also consider providing background materials in sidebars for nonexpert readers. For more information and instructions on presentation and formatting, please visit our Author Resources page.

Authors for the Cybersecurity Column Department or other IT Pro departments can submit short articles (approximately 1,500 words) suitable for any of the departments to the respective editor or the editor in chief (for contact information, see our editorial staff directory). The process for submitting longer articles is described below.

A recent sampling for our IT Pro Cybersecurity column include these articles –

- Spammers Are Becoming "Smarter" on Twitter
- Addressing Pressing Cybersecurity Issues through Collaboration (NCCOE)
- Defeating Buffer Overflow: A Trivial but Dangerous Bug
- VPKI Hits the Highway: Secure Communication for the Connected Vehicle Program
- Bystanders' Privacy
- Can Blockchain Strengthen the Internet of Things?

COMPUTING TRENDS AND IDEAS

A searchable index of front covers and articles from 18 IEEE Computer Society and ACM

Covers	Articles	About

- **43070** articles from **18** sources
  - ☑ IEEE Software (**3317** articles) - explore
  - ☑ IEEE Computer (**6769** articles) - explore
  - ☑ IEEE Security & Privacy (**1595** articles) - explore
  - ☑ IEEE Cloud (**231** articles) - explore
  - ☑ IEEE Internet Computing (**1834** articles) - explore
  - ☑ IEEE IT Professional (**1206** articles) - explore
  - ☑ IEEE Intelligent Systems (**2130** articles) - explore
  - ☑ IEEE Pervasive Computing (**951** articles) - explore
  - ☑ IEEE Computer Graphics & Applications (**2666** articles) - explore
  - ☑ IEEE Multimedia (**1183** articles) - explore
  - ☑ IEEE Computing in Science & Engineering (**1574** articles) - explore
  - ☑ Communications of the ACM (**12524** articles) - explore
  - ☑ ACM interactions (**2463** articles) - explore
  - ☑ ACM queue (**1080** articles) - explore
  - ☑ IEEE Micro (**2101** articles) - explore
  - ☑ ACM Computing Surveys (**1638** articles) - explore
  - ☑ SE Radio (**299** articles) - explore
  - ☑ Selected Software Engineering Books (**Loading...**) - explore