Business School
UNIVERSITY OF COLORADO DENVER

IEEE
COMMUNICATIONS
SOCIETY
Denver Chapter

ITProfessional
Technology Solutions for the Enterprise

IT Risk and Resilience

Roadmaps for Risk Management

Resilience and Reliability

Tim Weil – IEEE Senior Member
CU-Denver School of Risk Management
http://comsoc.ieee-denver.org

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

Invited Talk
Denver, CO
Feb 8, 2022

Objectives of this Presentation

Cyberspace – Out Point of Departure

-- A Writer’s Life

-- Risk Landscape Evaluation

Information Security Management Models

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

-- FISMA and FedRamp

-- Center for Internet Security (CIS)

-- NIST Cybersecurity Frameworks

-- Cloud Computing

-- MITRE Att%ck Taxonomies and Methods

Global transformation caused by COVID-19

-- Global transformation of Information Technology Services

-- NIST Cybersecurity Framework (up close)

-- COVID Smackdown – NIST CSF vs Big Scary Monsters

-- Recovery and Resilience – IT Context for Business Continuity

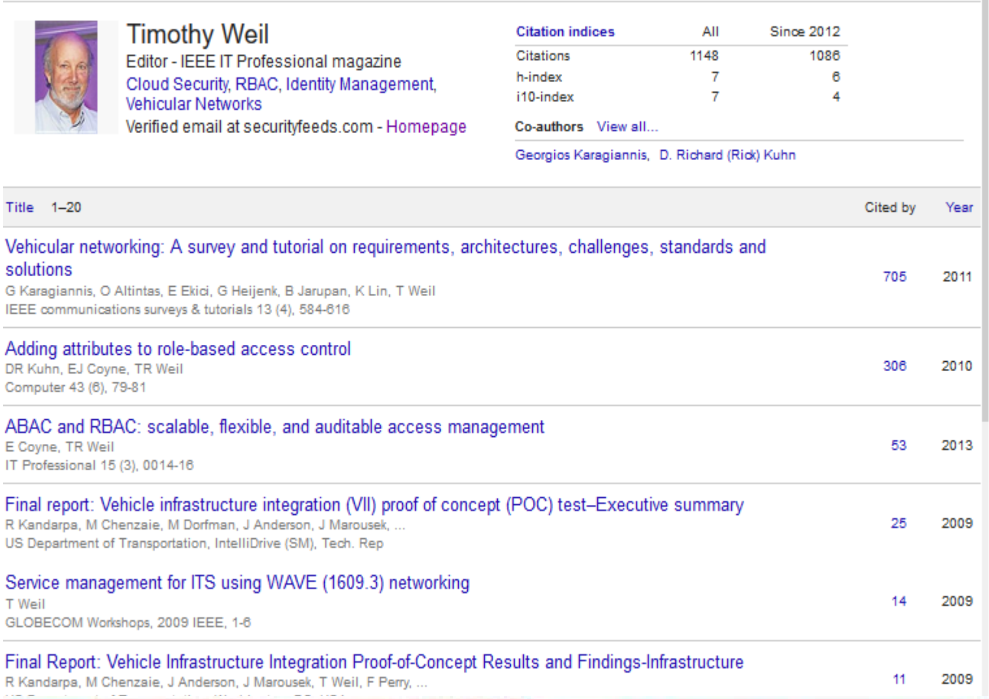
Emerging Road Maps for Risk Management

-- Project Management Institute (PMBOK)

-- Rational Cybersecurity for Business (Blum) vs Cybersecurity Management (Kshetri)

-- ISO Methods – Lead Cybersecurity Manager (ISO 27032) vs Information Security Managemenbt Systems (ISO 27001)

A Writer's Life –

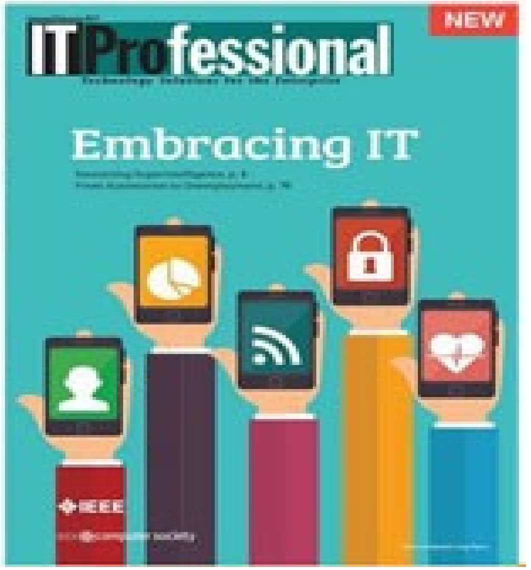


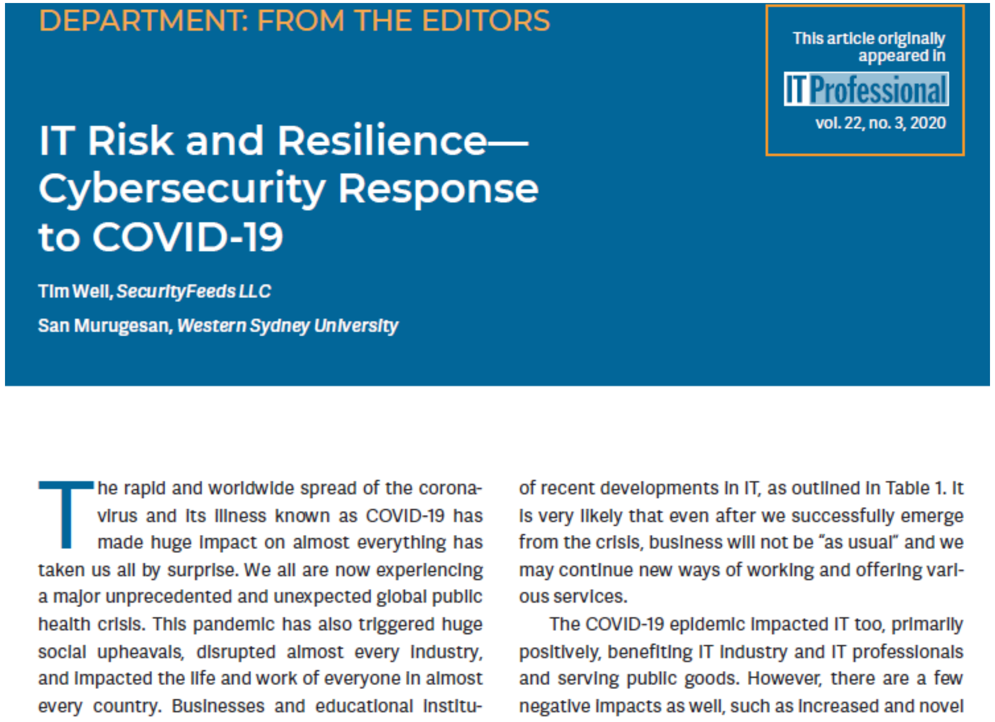
Timothy Weil
Editor - IEEE IT Professional magazine
Cloud Security, RBAC, Identity Management, Vehicular Networks
Verified email at securityfeeds.com - Homepage

Citation indices	All	Since 2012
Citations	1148	1086
h-index	7	6
i10-index	7	4

Co-authors View all...
Georgios Karagiannis, D. Richard (Rick) Kuhn

Title 1–20	Cited by	Year
Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions G Karagiannis, O Altintas, E Ekici, G Heijenk, B Jarupan, K Lin, T Weil IEEE communications surveys & tutorials 13 (4), 584-616	705	2011
Adding attributes to role-based access control DR Kuhn, EJ Coyne, TR Weil Computer 43 (6), 79-81	306	2010
ABAC and RBAC: scalable, flexible, and auditable access management E Coyne, TR Weil IT Professional 15 (3), 0014-16	53	2013
Final report: Vehicle infrastructure integration (VII) proof of concept (POC) test–Executive summary R Kandarpa, M Chenzaie, M Dorfman, J Anderson, J Marousek, ... US Department of Transportation, IntelliDrive (SM), Tech. Rep	25	2009
Service management for ITS using WAVE (1609.3) networking T Weil GLOBECOM Workshops, 2009 IEEE, 1-6	14	2009
Final Report: Vehicle Infrastructure Integration Proof-of-Concept Results and Findings-Infrastructure R Kandarpa, M Chenzaie, J Anderson, J Marousek, T Weil, F Perry, ...	11	2009





DEPARTMENT: FROM THE EDITORS

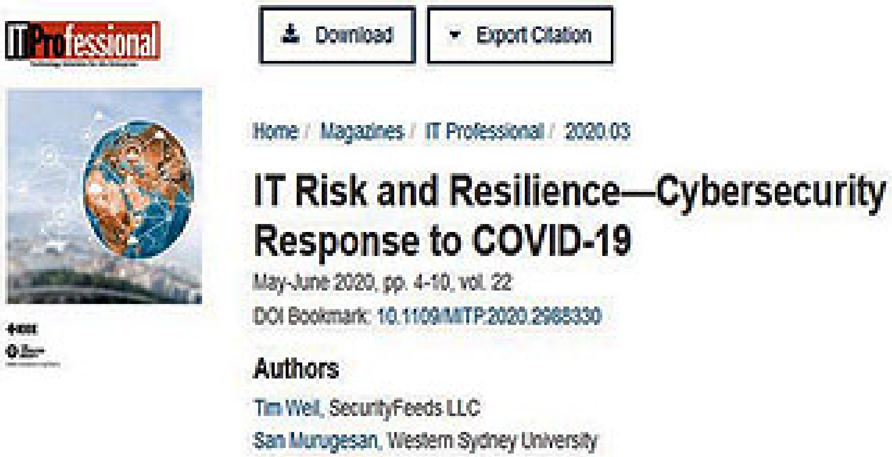
This article originally appeared in IT Professional vol. 22, no. 3, 2020

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 institutions 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



Home / Magazines / IT Professional / 2020.03

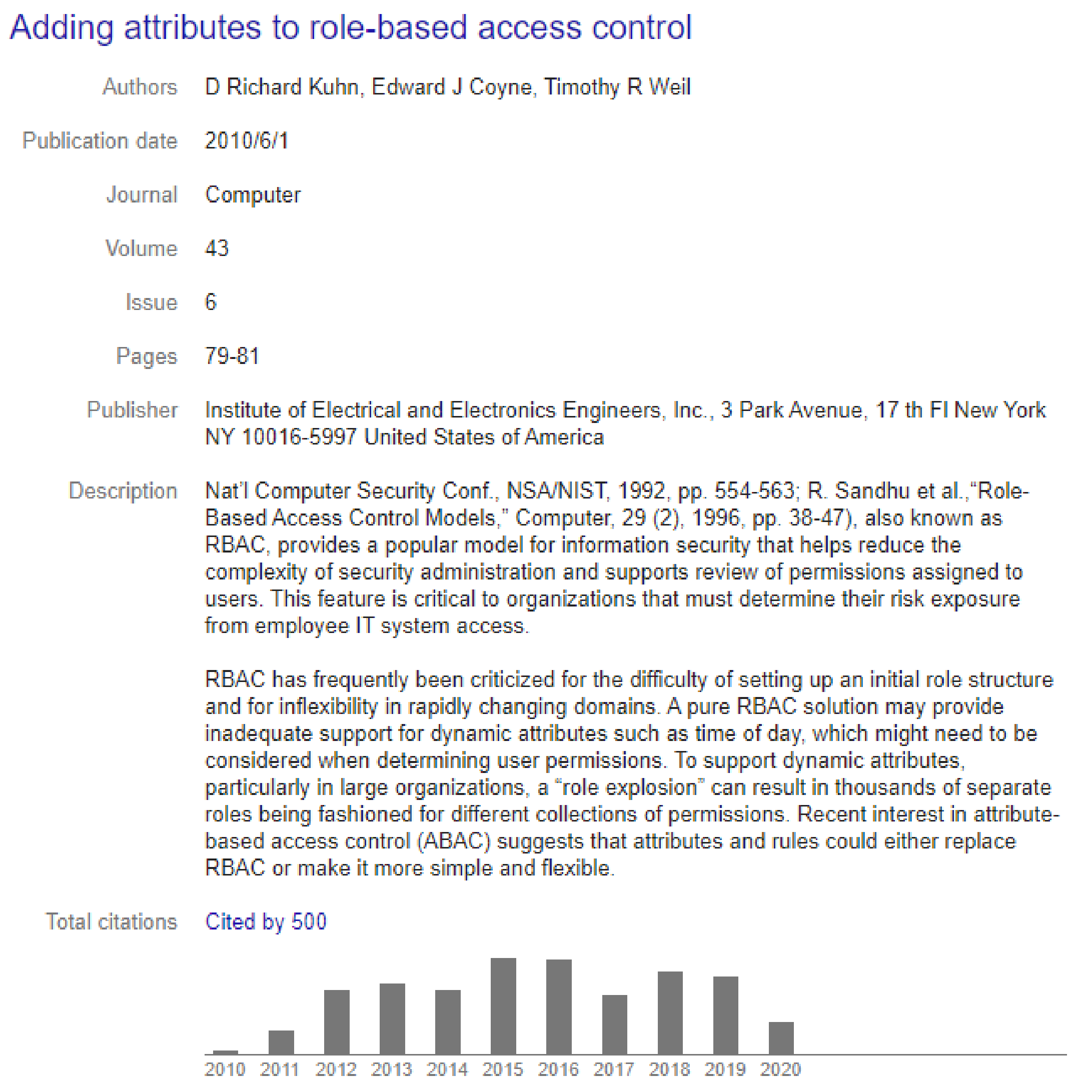
IT Risk and Resilience—Cybersecurity Response to COVID-19

May-June 2020, pp. 4-10, vol. 22
DOI Bookmark: 10.1109/MITP.2020.2988330

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

COMPUTING
edge
Security and Privacy
Data
Internet
Artificial Intelligence
IEEE
For Users of ZENITH Computers
SEXTANT
Video Image Processing With Zip and ImageWise —See page 4
Building the '248
Fast Fractals for Your '150 or '100
IBM Emulation With the Scottie Board
Time- and Date-Stamp Your CP/M Files
A Brain Transplant for the Z100
IT Professional
IT SECURITY
GREEN SOFTWARE 44
GRAPH DATABASES 58
IEEE
computer society
Computer
JUNE 2010
CAPTURING THE WORLD
VISUAL CONCEPT SEARCH P. 76
APPROPRIATE INTERACTION SURFACES P. 86
EMOTIONAL AND COGNITIVE OVERLOAD P. 96
IEEE
IEEE
SECURITY & PRIVACY
Risking Communications Security
POST
IEEE

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

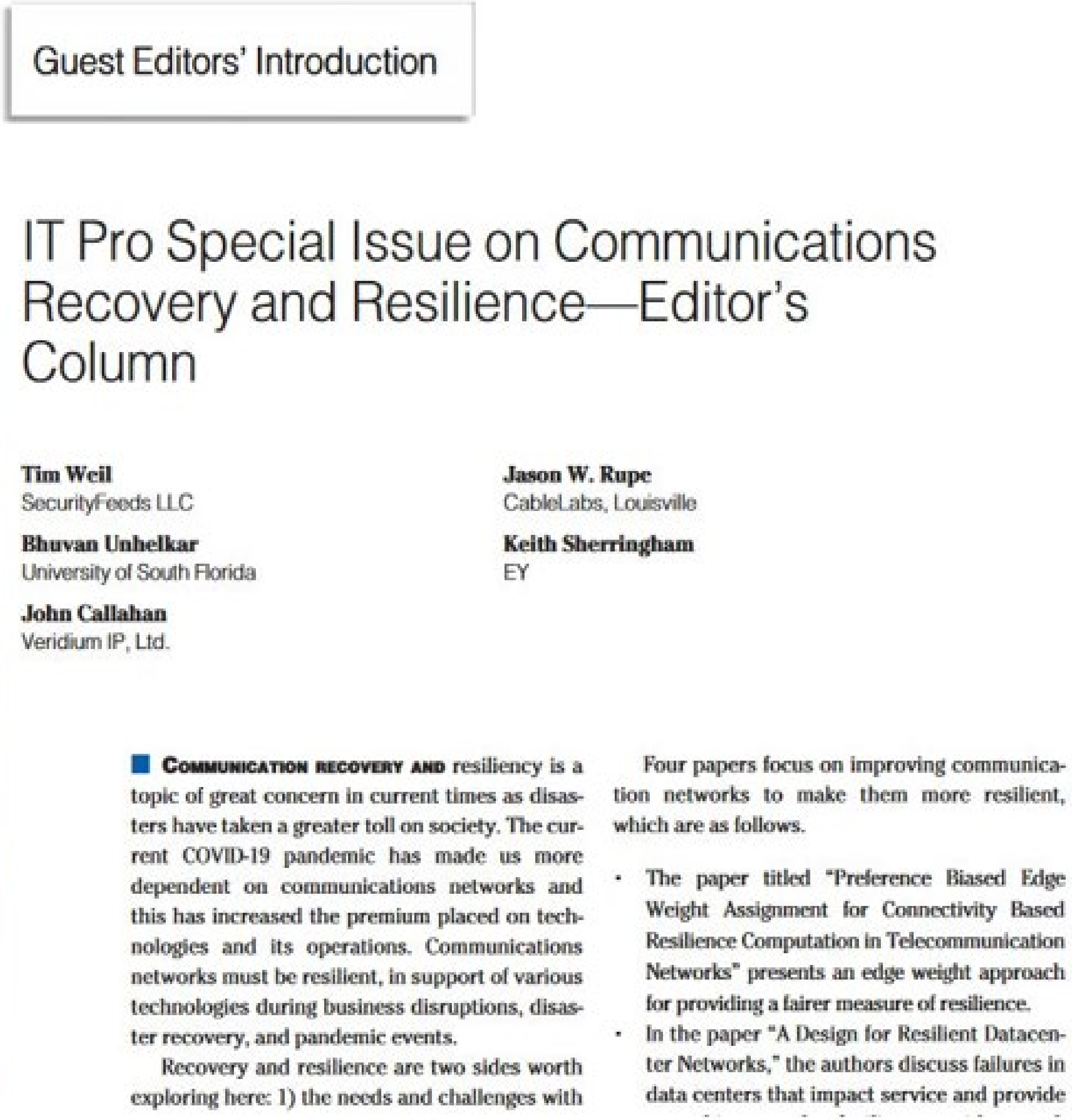
IT Professional

Technology Solutions for the Enterprise

VOLUME 22, NUMBER 6

NOVEMBER/DECEMBER 20

Resilience and Reliabilit



Guest Editors' Introduction

IT Pro Special Issue on Communications Recovery and Resilience—Editor's Column

Tim Weil
SecurityFeeds LLC

Bhuvan Unhelkar
University of South Florida

John Callahan
Veridium IP, Ltd.

Jason W. Rupe
CableLabs, Louisville

Keith Sherringham
EY

■ COMMUNICATION RECOVERY AND resiliency is a topic of great concern in current times as disasters have taken a greater toll on society. The current COVID-19 pandemic has made us more dependent on communications networks and this has increased the premium placed on technologies and its operations. Communications networks must be resilient, in support of various technologies during business disruptions, disaster recovery, and pandemic events.

Recovery and resilience are two sides worth exploring here: 1) the needs and challenges with

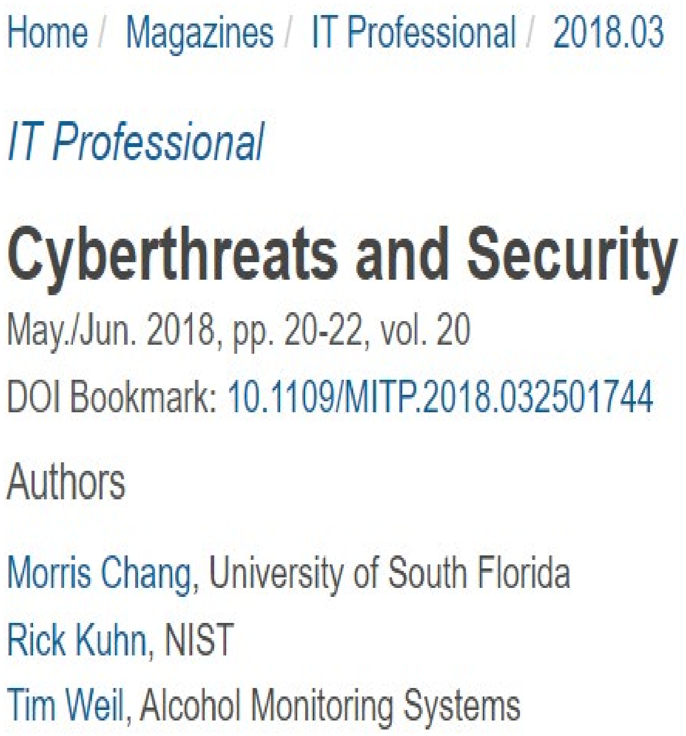
Four papers focus on improving communication networks to make them more resilient, which are as follows.

- The paper titled "Preference Biased Edge Weight Assignment for Connectivity Based Resilience Computation in Telecommunication Networks" presents an edge weight approach for providing a fairer measure of resilience.
- In the paper "A Design for Resilient Datacenter Networks," the authors discuss failures in data centers that impact service and provide

https://www.computer.org/csdl/magazine/it/2020/06/09250314/1oxkJTuIsMg

IT Professional
Technology Solutions for the Enterprise

IT Professional
Technology Solutions for the Enterprise
Cyberthreats and Security
IEEE
computer society


Home / Magazines / IT Professional / 2018.03

IT Professional

Cyberthreats and Security

May./Jun. 2018, pp. 20-22, vol. 20

DOI Bookmark: 10.1109/MITP.2018.032501744

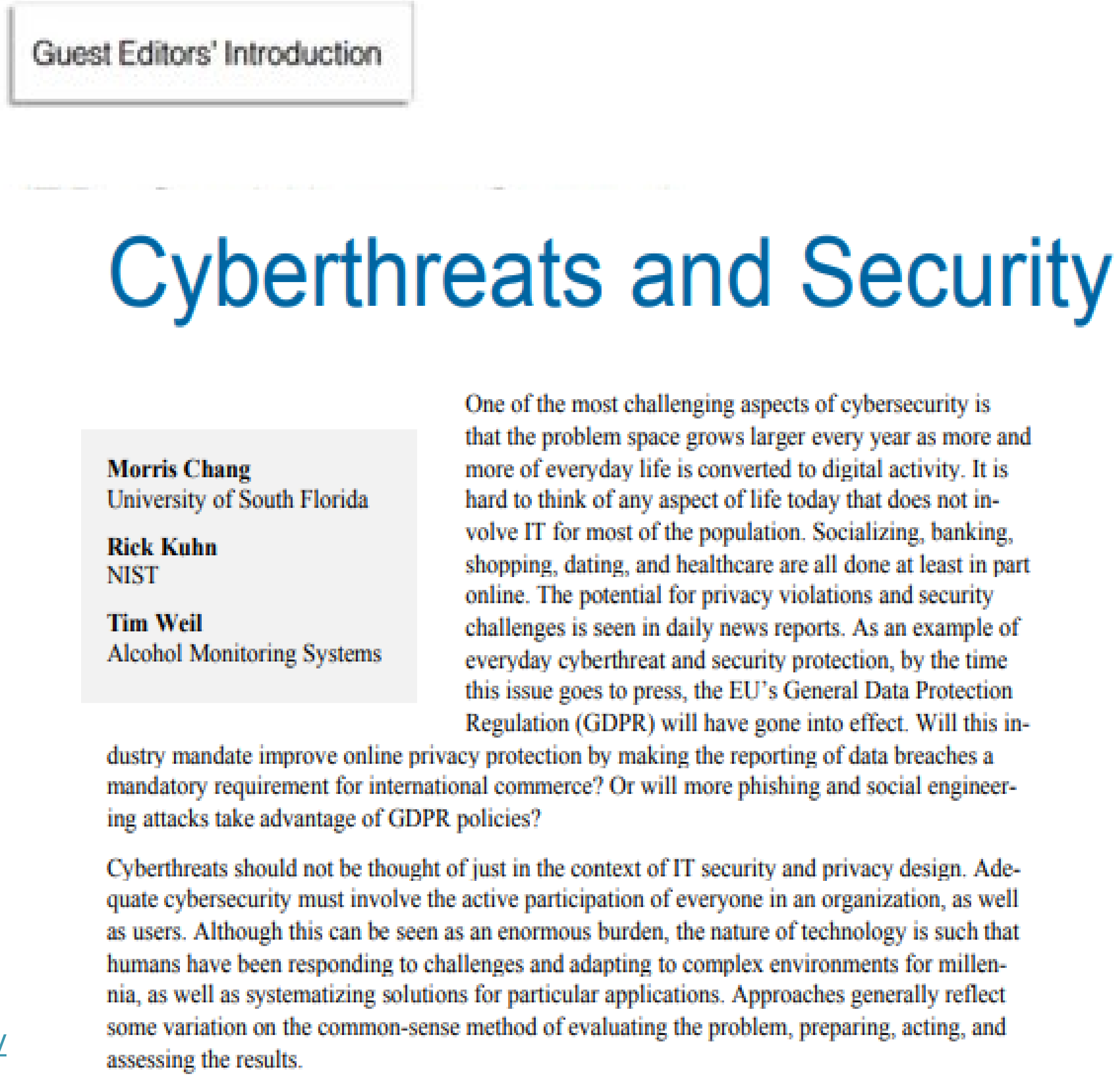
Authors

Morris Chang, University of South Florida

Rick Kuhn, NIST

Tim Weil, Alcohol Monitoring Systems

https://www.computer.org/csdl/magazine/it/2018/03/mit2018030020/13rRUIJuxty


Guest Editors' Introduction

Cyberthreats and Security

Morris Chang
University of South Florida

Rick Kuhn
NIST

Tim Weil
Alcohol Monitoring Systems

One of the most challenging aspects of cybersecurity is that the problem space grows larger every year as more and more of everyday life is converted to digital activity. It is hard to think of any aspect of life today that does not involve IT for most of the population. Socializing, banking, shopping, dating, and healthcare are all done at least in part online. The potential for privacy violations and security challenges is seen in daily news reports. As an example of everyday cyberthreat and security protection, by the time this issue goes to press, the EU's General Data Protection Regulation (GDPR) will have gone into effect. Will this industry mandate improve online privacy protection by making the reporting of data breaches a mandatory requirement for international commerce? Or will more phishing and social engineering attacks take advantage of GDPR policies?

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. Although this can be seen as an enormous burden, the nature of technology is such that humans have been responding to challenges and adapting to complex environments for millennia, as well as systematizing solutions for particular applications. Approaches generally reflect some variation on the common-sense method of evaluating the problem, preparing, acting, and assessing the results.

https://www.securityfeeds.us/cyberthreats-and-security-ieee-it-professional-special-issue

Table of Contents

- Cyberspace – Our Point of Departure
- Information Security Management Models
- Frameworks for Risk Management
- COVID Smackdown – NIST CSF vs Big Scary Monsters
- Emerging Roads Maps to Risk Management
- References + Q&A

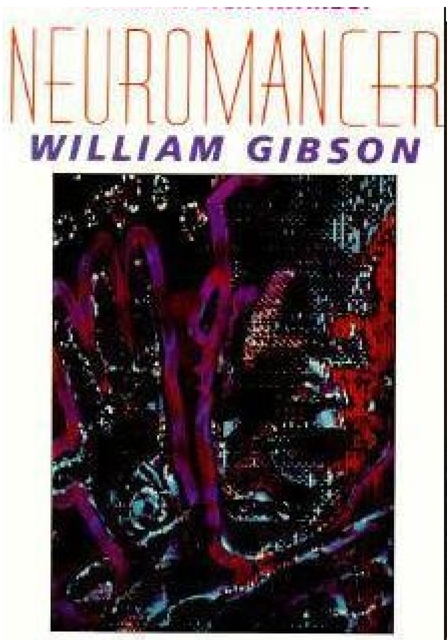
Cyberspace – Our Point of Departure – Wired Magazine (June ‘08) - https://www.wired.com/2008/05/pentagon-define/

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

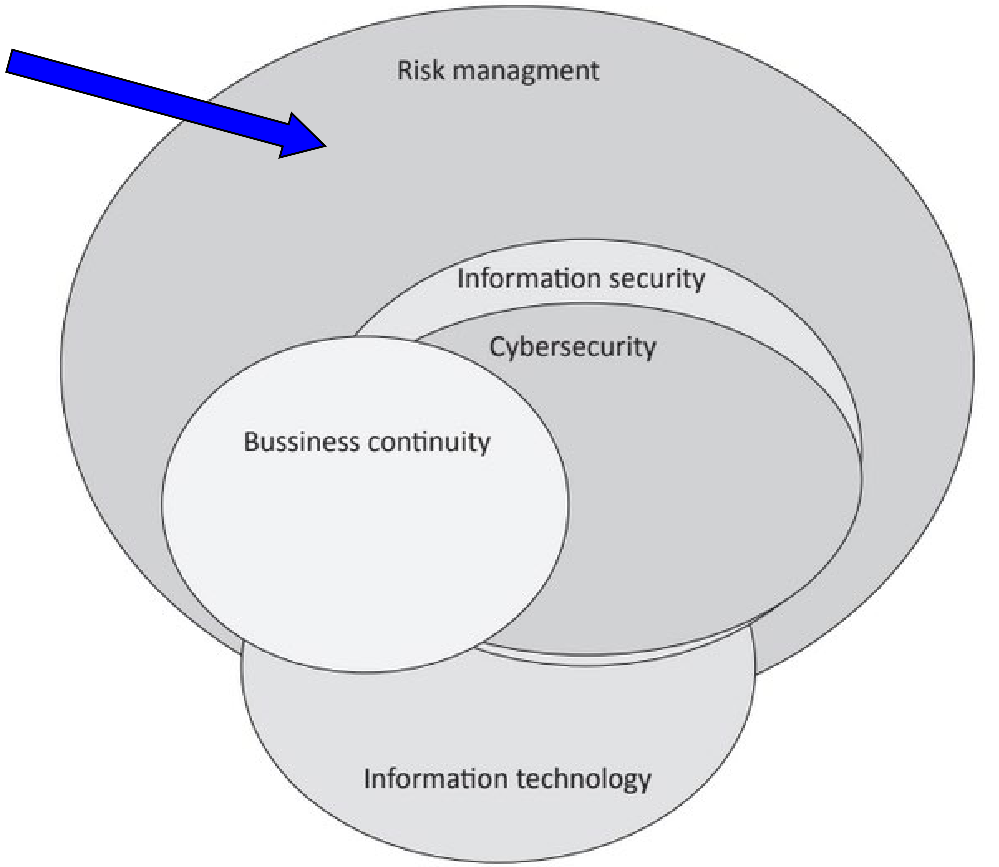
Cyberspace, England writes, is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” *

*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.”

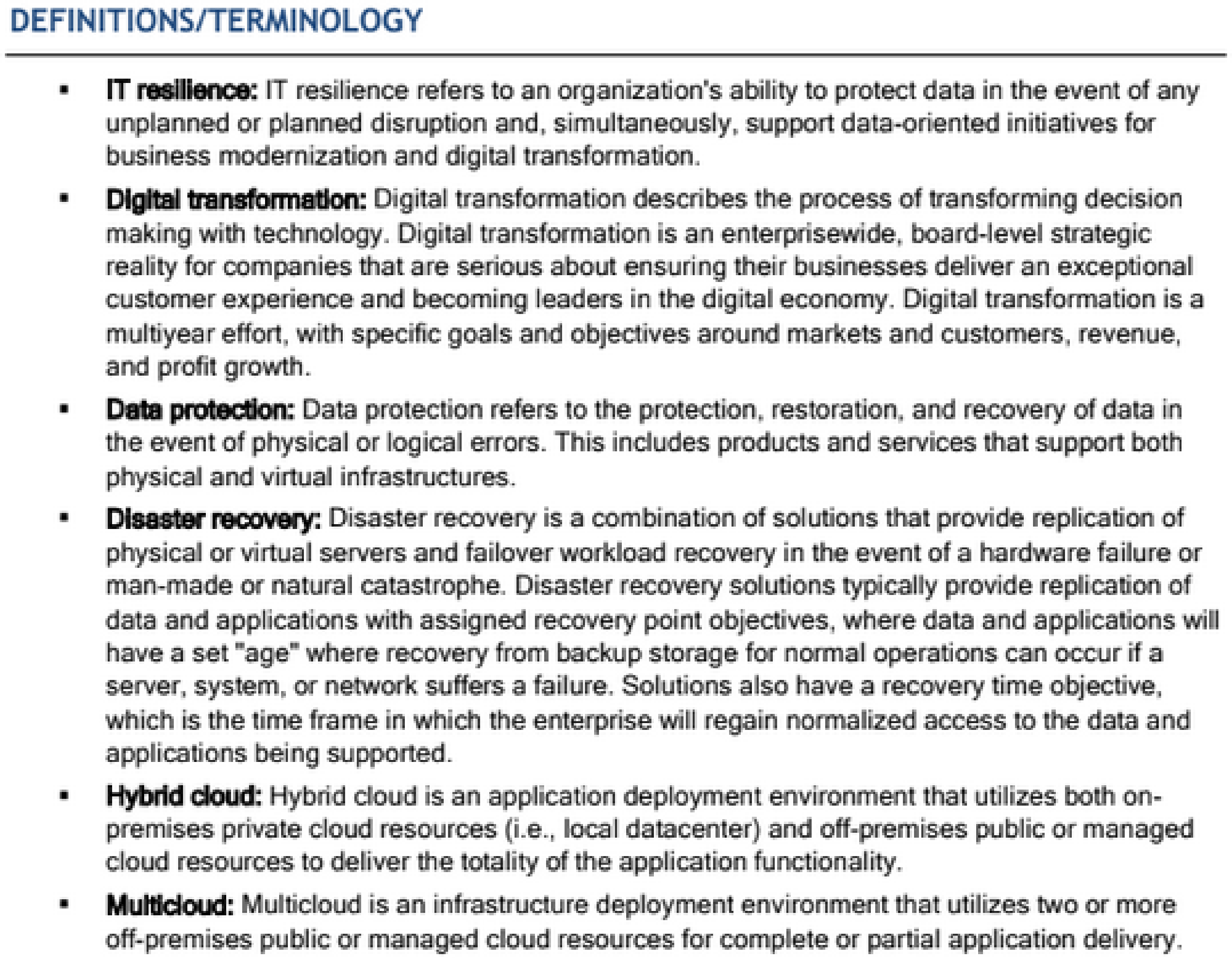


Recovery and Resilience – IT Context for Business Continuity

2.3 Where does business continuity belong?

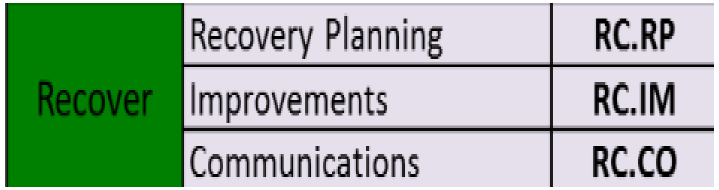


“”Becoming Resilient ” Dejan Kosutic



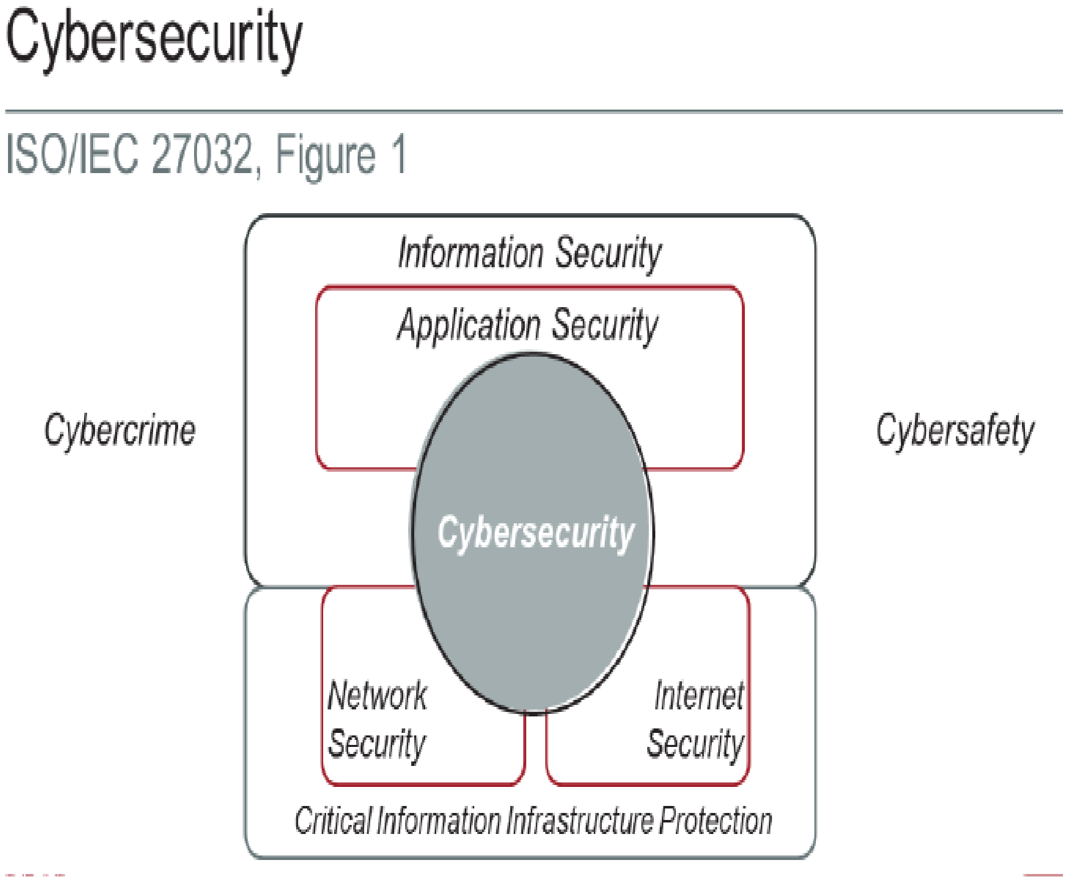
DEFINITIONS/TERMINOLOGY

- **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.



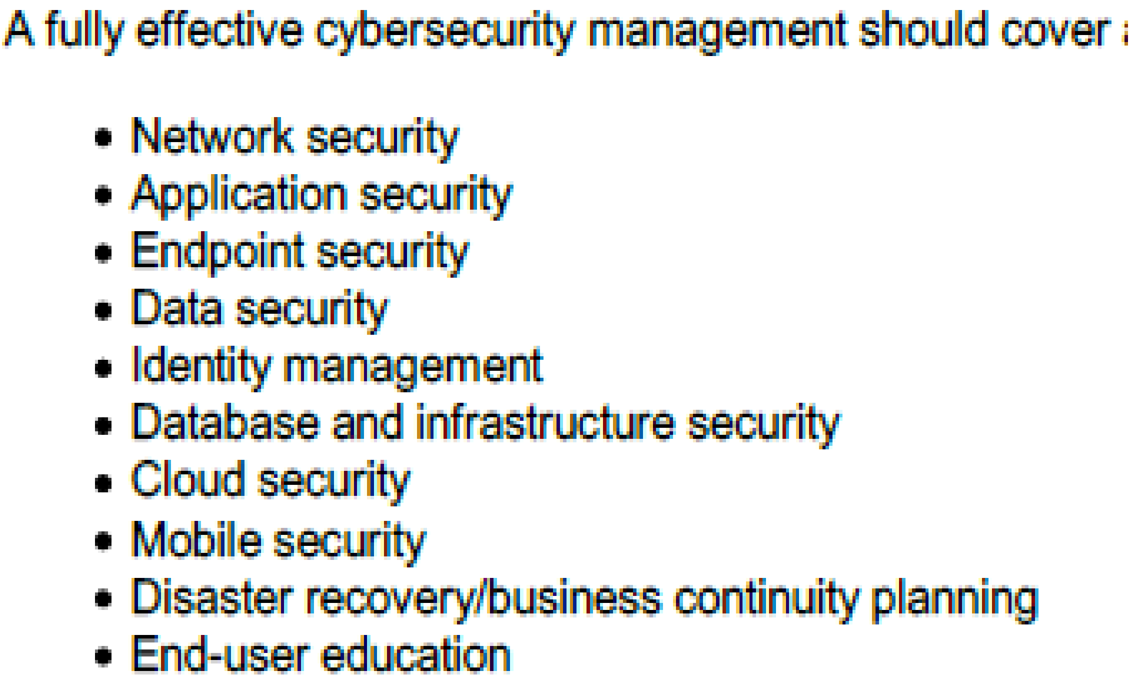
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Cybersecurity Model (per ISO 27032)



Cybersecurity

ISO/IEC 27032, Figure 1



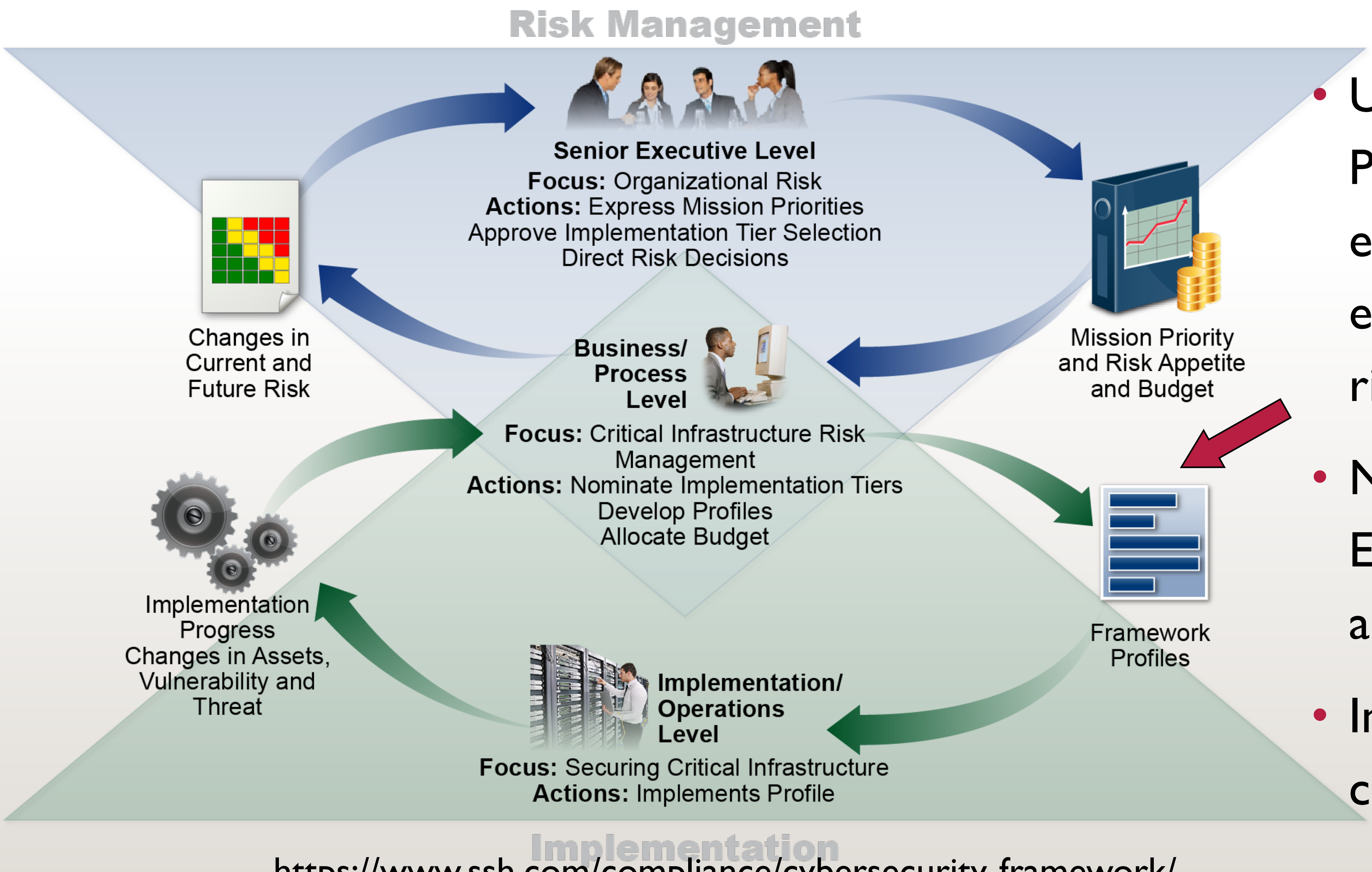
A fully effective cybersecurity management should cover

- Network security
- Application security
- Endpoint security
- Data security
- Identity management
- Database and infrastructure security
- Cloud security
- Mobile security
- Disaster recovery/business continuity planning
- End-user education

Information Security, Application Security, Network Security, Internet Security as an overlay to Cybersecurity and Information Technology

Table of Contents

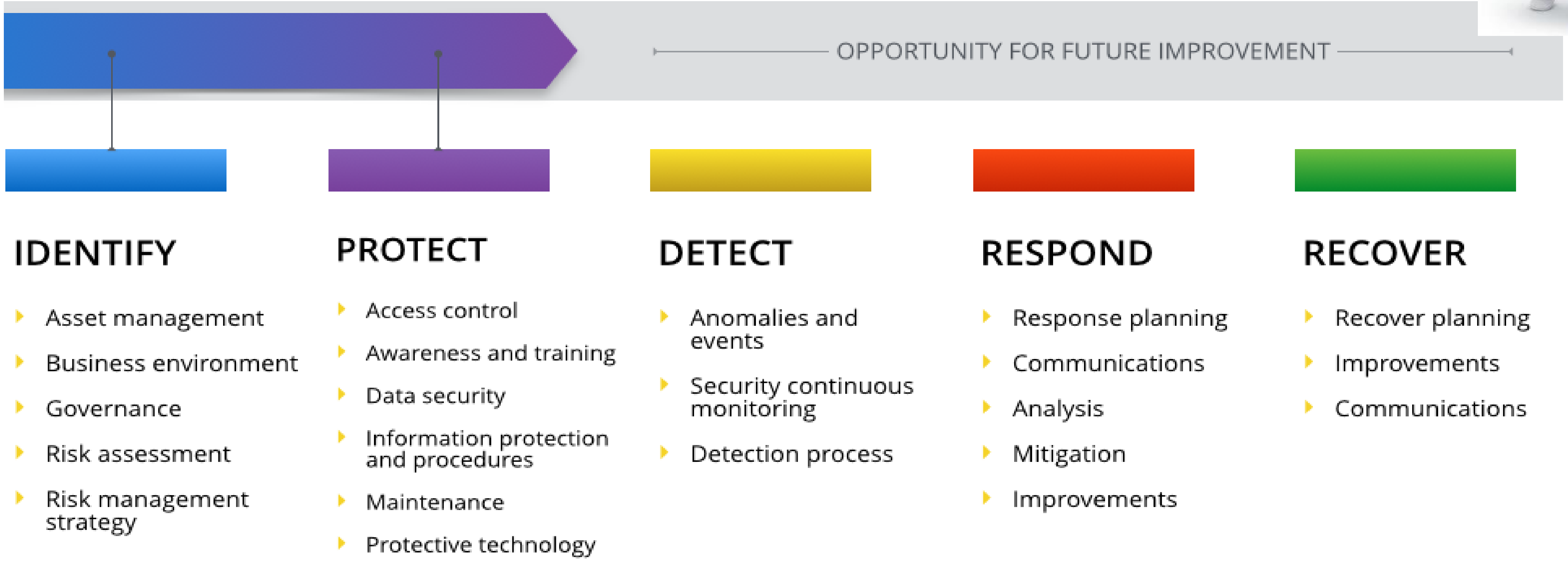
- Cyberspace – Our Point of Departure
- Information Security Management Models
- Frameworks for Risk Management
- COVID Smackdown – NIST CSF vs Big Scary Monsters
- Emerging Roads Maps to Risk Management
- References + Q&A


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

https://www.ssh.com/compliance/cybersecurity-framework/

- 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

NIST Cybersecurity Framework –



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

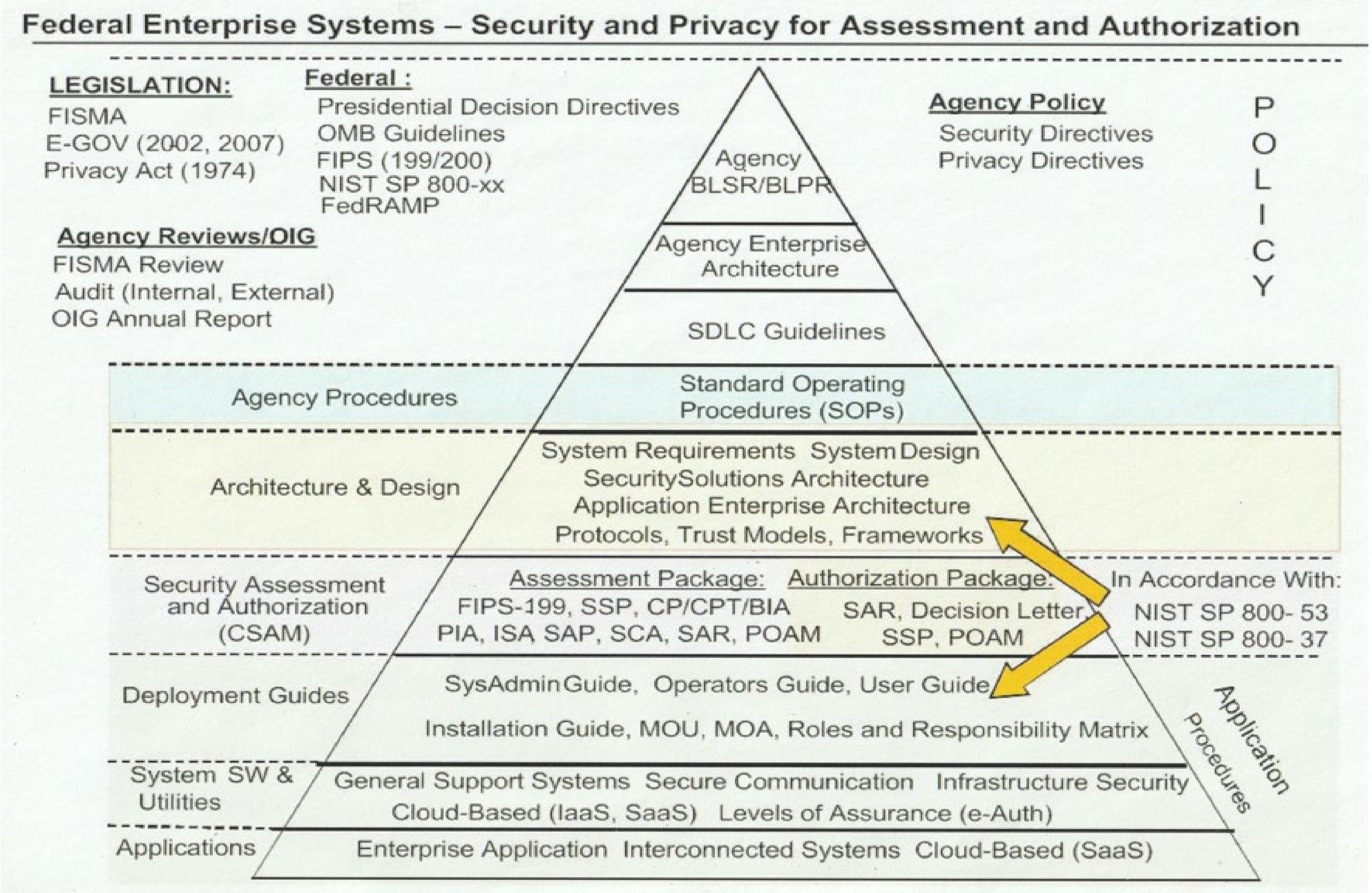
- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recover planning
- Improvements
- Communications

From process view, cybersecurity starts from understanding the organization, its mission, its risk tolerance. Part of this is understanding the organization's role in critical infrastructure. These are used to define roles, responsibilities, policies, and processes. Cybersecurity is realized as technical controls, monitoring, and planned responses. The processes are reviewed and improved based on experience.

FISMA Model - For Assessment and Authorization



Federal Enterprise Systems – Security and Privacy for Assessment and Authorization

LEGISLATION:
FISMA
E-GOV (2002, 2007)
Privacy Act (1974)

Federal :
Presidential Decision Directives
OMB Guidelines
FIPS (199/200)
NIST SP 800-xx
FedRAMP

Agency Reviews/OIG
FISMA Review
Audit (Internal, External)
OIG Annual Report

Agency Policy
Security Directives
Privacy Directives

P O L I C Y

Agency BLSR/BLPR

Agency Enterprise Architecture

SDLC Guidelines

Agency Procedures — Standard Operating Procedures (SOPs)

Architecture & Design — System Requirements System Design
SecuritySolutions Architecture
Application Enterprise Architecture
Protocols, Trust Models, Frameworks

Security Assessment and Authorization (CSAM)

Assessment Package:
FIPS-199, SSP, CP/CPT/BIA
PIA, ISA SAP, SCA, SAR, POAM

Authorization Package:
SAR, Decision Letter
SSP, POAM

In Accordance With:
NIST SP 800- 53
NIST SP 800- 37

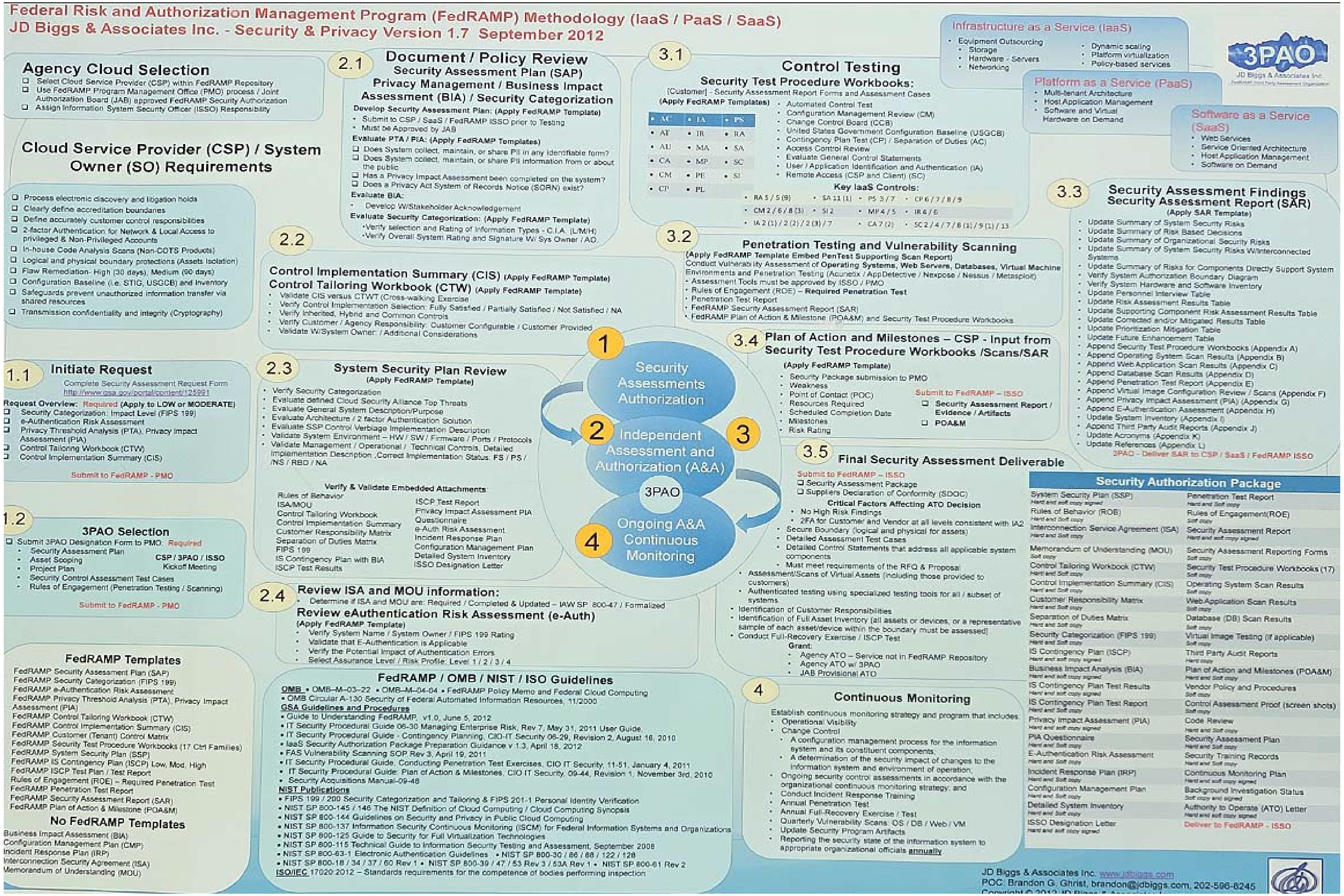
Deployment Guides — SysAdmin Guide, Operators Guide, User Guide
Installation Guide, MOU, MOA, Roles and Responsibility Matrix

Application Procedures

System SW & Utilities — General Support Systems Secure Communication Infrastructure Security
Cloud-Based (IaaS, SaaS) Levels of Assurance (e-Auth)

Applications — Enterprise Application Interconnected Systems Cloud-Based (SaaS)

FEDRAMP Model - For Assessment and Authorization



Federal Risk and Authorization Management Program (FedRAMP) Methodology (IaaS / PaaS / SaaS)
JD Biggs & Associates Inc. - Security & Privacy Version 1.7 September 2012

Agency Cloud Selection

- □ Select Cloud Service Provider (CSP) within FedRAMP Repository
- □ Use FedRAMP Program Management Office (PMO) process / Joint Authorization Board (JAB) approved FedRAMP Security Authorization
- □ Assign Information System Security Officer (ISSO) Responsibility

Cloud Service Provider (CSP) / System Owner (SO) Requirements

- □ Process electronic discovery and litigation holds
- □ Clearly define accreditation boundaries
- □ Define accurately customer control responsibilities
- □ 2-factor Authentication for Network & Local Access to privileged & Non-Privileged Accounts
- □ In-house Code Analysis Scans (Non-COTS Products)
- □ Logical and physical boundary protections (Assets Isolation)
- □ Flaw Remediation- High (30 days), Medium (90 days)
- □ Configuration Baseline (i.e. STIG, USGCB) and Inventory
- □ Safeguards prevent unauthorized information transfer via shared resources
- □ Transmission confidentiality and integrity (Cryptography)

1.1 Initiate Request

Complete Security Assessment Request Form
http://www.gsa.gov/portal/content/125991

Request Overview: Required **(Apply to LOW or MODERATE)**

- □ Security Categorization: Impact Level (FIPS 199)
- □ e-Authentication Risk Assessment
- □ Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA)
- □ Control Tailoring Workbook (CTW)
- □ Control Implementation Summary (CIS)

Submit to FedRAMP - PMO

1.2 3PAO Selection

- □ Submit 3PAO Designation Form to PMO: Required
  - Security Assessment Plan
  - Asset Scoping
  - Project Plan
  - Security Control Assessment Test Cases
  - Rules of Engagement (Penetration Testing / Scanning)

CSP / 3PAO / ISSO Kickoff Meeting

Submit to FedRAMP - PMO

FedRAMP Templates

FedRAMP Security Assessment Plan (SAP)
FedRAMP Security Categorization (FIPS 199)
FedRAMP e-Authentication Risk Assessment
FedRAMP Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA)
FedRAMP Control Tailoring Workbook (CTW)
FedRAMP Control Implementation Summary (CIS)
FedRAMP Customer (Tenant) Control Matrix
FedRAMP Security Test Procedure Workbooks (17 Ctrl Families)
FedRAMP System Security Plan (SSP)
FedRAMP IS Contingency Plan (ISCP) Low, Mod, High
FedRAMP ISCP Test Plan / Test Report
Rules of Engagement (ROE) – Required Penetration Test
FedRAMP Penetration Test Report
FedRAMP Security Assessment Report (SAR)
FedRAMP Plan of Action & Milestone (POA&M)

No FedRAMP Templates

Business Impact Assessment (BIA)
Configuration Management Plan (CMP)
Incident Response Plan (IRP)
Interconnection Security Agreement (ISA)
Memorandum of Understanding (MOU)

2.1 Document / Policy Review

Security Assessment Plan (SAP)
Privacy Management / Business Impact Assessment (BIA) / Security Categorization

Develop Security Assessment Plan: (Apply FedRAMP Template)

- Submit to CSP / SaaS / FedRAMP ISSO prior to Testing
- Must be Approved by JAB

Evaluate PTA / PIA: (Apply FedRAMP Templates)

- □ Does System collect, maintain, or share PII in any identifiable form?
- □ Does System collect, maintain, or share PII information from or about the public
- □ Has a Privacy Impact Assessment been completed on the system?
- □ Does a Privacy Act System of Records Notice (SORN) exist?

Evaluate BIA:

- Develop W/Stakeholder Acknowledgement

Evaluate Security Categorization: (Apply FedRAMP Template)

- Verify selection and Rating of Information Types - C.I.A. (L/M/H)
- Verify Overall System Rating and Signature W/ Sys Owner / AO.

2.2

Control Implementation Summary (CIS) (Apply FedRAMP Template)
Control Tailoring Workbook (CTW) (Apply FedRAMP Template)

- Validate CIS versus CTWT (Cross-walking Exercise
- Verify Control Implementation Selection: Fully Satisfied / Partially Satisfied / Not Satisfied / NA
- Verify Inherited, Hybrid and Common Controls
- Verify Customer / Agency Responsibility: Customer Configurable / Customer Provided
- Validate W/System Owner: / Additional Considerations

2.3 System Security Plan Review

(Apply FedRAMP Template)

- Verify Security Categorization
- Evaluate defined Cloud Security Alliance Top Threats
- Evaluate General System Description/Purpose
- Evaluate Architecture / 2 factor Authentication Solution
- Evaluate SSP Control Verbiage Implementation Description
- Validate System Environment – HW / SW / Firmware / Ports / Protocols
- Validate Management / Operational / Technical Controls, Detailed Implementation Description ,Correct Implementation Status: FS / PS / /NS / RBD / NA

Verify & Validate Embedded Attachments:

Rules of Behavior
ISA/MOU
Control Tailoring Workbook
Control Implementation Summary
Customer Responsibility Matrix
Separation of Duties Matrix
FIPS 199
IS Contingency Plan with BIA
ISCP Test Results

ISCP Test Report
Privacy Impact Assessment PIA Questionnaire
e-Auth Risk Assessment
Incident Response Plan
Configuration Management Plan
Detailed System Inventory
ISSO Designation Letter

2.4 Review ISA and MOU information:

- Determine if ISA and MOU are: Required / Completed & Updated – IAW SP 800-47 / Formalized

Review eAuthentication Risk Assessment (e-Auth)

(Apply FedRAMP Template)

- Verify System Name / System Owner / FIPS 199 Rating
- Validate that E-Authentication is Applicable
- Verify the Potential Impact of Authentication Errors
- Select Assurance Level / Risk Profile: Level 1 / 2 / 3 / 4

FedRAMP / OMB / NIST / ISO Guidelines

OMB • OMB–M–03–22 • OMB–M–04-04 • FedRAMP Policy Memo and Federal Cloud Computing
• OMB Circular A-130 Security of Federal Automated Information Resources, 11/2000

GSA Guidelines and Procedures

- Guide to Understanding FedRAMP, v1.0, June 5, 2012
- IT Security Procedural Guide 06-30 Managing Enterprise Risk, Rev 7, May 31, 2011 User Guide
- IT Security Procedural Guide - Contingency Planning, CIO-IT Security 06-29, Revision 2, August 16, 2010
- IaaS Security Authorization Package Preparation Guidance v 1.3, April 18, 2012
- FAS Vulnerability Scanning SOP Rev 3, April 19, 2011
- IT Security Procedural Guide, Conducting Penetration Test Exercises, CIO IT Security, 11-51, January 4, 2011
- IT Security Procedural Guide: Plan of Action & Milestones, CIO IT Security, 09-44, Revision 1, November 3rd, 2010
- Security Acquisitions Manual-09-48

NIST Publications

- FIPS 199 / 200 Security Categorization and Tailoring & FIPS 201-1 Personal Identity Verification
- NIST SP 800-145 / 146 The NIST Definition of Cloud Computing / Cloud Computing Synopsis
- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
- NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-125 Guide to Security for Full Virtualization Technologies
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, September 2008
- NIST SP 800-63-1 Electronic Authentication Guidelines • NIST SP 800-30 / 86 / 88 / 122 / 128
- NIST SP 800-18 / 34 / 37 / 60 Rev 1 • NIST SP 800-39 / 47 / 53 Rev 3 / 53A Rev 1 • NIST SP 800-61 Rev 2

ISO/IEC 17020:2012 – Standards requirements for the competence of bodies performing inspection

1
Security Assessments Authorization
2
Independent Assessment and Authorization (A&A)
3
3PAO
4
Ongoing A&A Continuous Monitoring

3.1 Control Testing

Security Test Procedure Workbooks:

[Customer] - Security Assessment Report Forms and Assessment Cases

(Apply FedRAMP Templates)

• AC	• IA	• PS
• AT	• IR	• RA
• AU	• MA	• SA
• CA	• MP	• SC
• CM	• PE	• SI
• CP	• PL	

- Automated Control Test
- Configuration Management Review (CM)
- Change Control Board (CCB)
- United States Government Configuration Baseline (USGCB)
- Contingency Plan Test (CP) / Separation of Duties (AC)
- Access Control Review
- Evaluate General Control Statements
- User / Application Identification and Authentication (IA)
- Remote Access (CSP and Client) (SC)

Key IaaS Controls:

• RA 5 / 5 (9)	• SA 11 (1)	• PS 3 / 7	• CP 6 / 7 / 8 / 9
• CM 2 / 6 / 8 (3)	• SI 2	• MP 4 / 5	• IR 4 / 5
• IA 2 (1) / 2 (2) / 2 (3) / 7		• CA 7 (2)	• SC 2 / 4 / 7 / 8 (1) / 9 (1) / 13

Infrastructure as a Service (IaaS)

- Equipment Outsourcing
  - Storage
  - Hardware - Servers
  - Networking
- Dynamic scaling
- Platform virtualization
- Policy-based services

Platform as a Service (PaaS)

- Multi-tenant Architecture
- Host Application Management
- Software and Virtual Hardware on Demand

Software as a Service (SaaS)

- Web Services
- Service Oriented Architecture
- Host Application Management
- Software on Demand

3PAO
JD Biggs & Associates Inc

3.2 Penetration Testing and Vulnerability Scanning

(Apply FedRAMP Template Embed PenTest Supporting Scan Report)

Conduct Vulnerability Assessment of **Operating Systems, Web Servers, Databases, Virtual Machine** Environments and Penetration Testing (Acunetix / AppDetective / Nexpose / Nessus / Metasploit)

- Assessment Tools must be approved by ISSO / PMO
- Rules of Engagement (ROE) – **Required Penetration Test**
- Penetration Test Report
- FedRAMP Security Assessment Report (SAR)
- FedRAMP Plan of Action & Milestone (POA&M) and Security Test Procedure Workbooks

3.3 Security Assessment Findings Security Assessment Report (SAR)

(Apply SAR Template)

- Update Summary of System Security Risks
- Update Summary of Risk Based Decisions
- Update Summary of Organizational Security Risks
- Update Summary of System Security Risks W/interconnected Systems
- Update Summary of Risks for Components Directly Support System
- Verify System Authorization Boundary Diagram
- Verify System Hardware and Software Inventory
- Update Personnel Interview Table
- Update Risk Assessment Results Table
- Update Supporting Component Risk Assessment Results Table
- Update Corrected and/or Mitigated Results Table
- Update Prioritization Mitigation Table
- Update Future Enhancement Table
- Append Security Test Procedure Workbooks (Appendix A)
- Append Operating System Scan Results (Appendix B)
- Append Web Application Scan Results (Appendix C)
- Append Database Scan Results (Appendix D)
- Append Penetration Test Report (Appendix E)
- Append Virtual Image Configuration Review / Scans (Appendix F)
- Append Privacy Impact Assessment (PIA) (Appendix G)
- Append E-Authentication Assessment (Appendix H)
- Update System Inventory (Appendix I)
- Append Third Party Audit Reports (Appendix J)
- Update Acronyms (Appendix K)
- Update References (Appendix L)

3PAO - Deliver SAR to CSP / SaaS / FedRAMP ISSO

3.4 Plan of Action and Milestones – CSP - Input from Security Test Procedure Workbooks /Scans/SAR

(Apply FedRAMP Template)

- Security Package submission to PMO
- Weakness
- Point of Contact (POC)
- Resources Required
- Scheduled Completion Date
- Milestones
- Risk Rating

Submit to FedRAMP – ISSO

- □ **Security Assessment Report / Evidence / Artifacts**
- □ **POA&M**

3.5 Final Security Assessment Deliverable

Submit to FedRAMP – ISSO

- □ Security Assessment Package
- □ Suppliers Declaration of Conformity (SDOC)

Critical Factors Affecting ATO Decision

- No High Risk Findings
- 2FA for Customer and Vendor at all levels consistent with IA2
- Secure Boundary (logical and physical for assets)
- Detailed Assessment Test Cases
- Detailed Control Statements that address all applicable system components
- Must meet requirements of the RFQ & Proposal
- Assessment/Scans of Virtual Assets (including those provided to customers)
- Authenticated testing using specialized testing tools for all / subset of systems
- Identification of Customer Responsibilities
- Identification of Full Asset Inventory [all assets or devices, or a representative sample of each asset/device within the boundary must be assessed]
- Conduct Full-Recovery Exercise / ISCP Test

Grant:

- Agency ATO – Service not in FedRAMP Repository
- Agency ATO w/ 3PAO
- JAB Provisional ATO

Security Authorization Package

System Security Plan (SSP) Hard and soft copy signed	Penetration Test Report Hard and Soft copy
Rules of Behavior (ROB) Hard and Soft copy	Rules of Engagement(ROE) Soft copy
Interconnection Service Agreement (ISA) Hard and Soft copy	Security Assessment Report Hard and soft copy signed
Memorandum of Understanding (MOU) Soft copy	Security Assessment Reporting Forms Soft copy
Control Tailoring Workbook (CTW) Hard and Soft copy	Security Test Procedure Workbooks (17) Soft copy
Control Implementation Summary (CIS) Hard and Soft copy	Operating System Scan Results Soft copy
Customer Responsibility Matrix Hard and Soft copy	Web Application Scan Results Soft copy
Separation of Duties Matrix Hard and Soft copy	Database (DB) Scan Results Soft copy
Security Categorization (FIPS 199) Hard and Soft copy	Virtual Image Testing (if applicable) Soft copy
IS Contingency Plan (ISCP) Hard and soft copy signed	Third Party Audit Reports Hard copy
Business Impact Analysis (BIA) Hard and soft copy signed	Plan of Action and Milestones (POA&M) Hard and Soft copy
IS Contingency Plan Test Results Hard and soft copy signed	Vendor Policy and Procedures Soft copy
IS Contingency Plan Test Report Hard and Soft copy	Control Assessment Proof (screen shots) Soft copy
Privacy Impact Assessment (PIA) Hard and soft copy signed	Code Review Hard and Soft copy
PIA Questionnaire Hard and Soft copy	Security Assessment Plan Hard and Soft copy
E-Authentication Risk Assessment Hard and Soft copy	Security Training Records Hard and Soft copy
Incident Response Plan (IRP) Hard and Soft copy	Continuous Monitoring Plan Hard and soft copy signed
Configuration Management Plan Hard and Soft copy	Background Investigation Status Soft copy and signed
Detailed System Inventory Hard and Soft copy	Authority to Operate (ATO) Letter Hard and soft copy signed
ISSO Designation Letter Hard and soft copy signed	Deliver to FedRAMP - ISSO

4 Continuous Monitoring

Establish continuous monitoring strategy and program that includes:

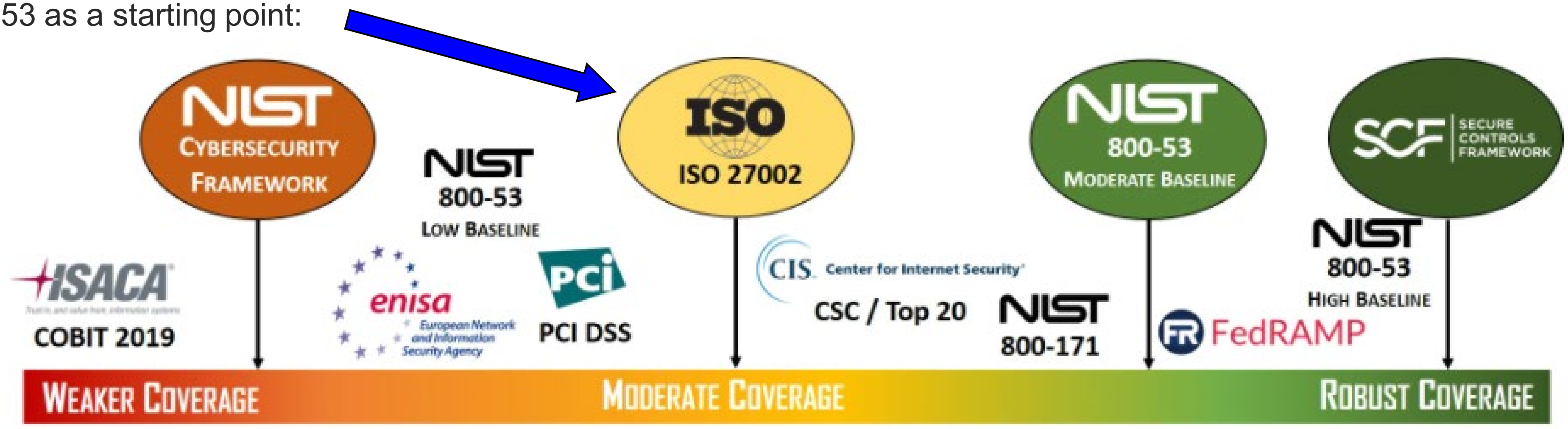
- Operational Visibility
- Change Control
  - A configuration management process for the information system and its constituent components;
  - A determination of the security impact of changes to the information system and environment of operation;
- Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
- Conduct Incident Response Training
- Annual Penetration Test
- Annual Full-Recovery Exercise / Test
- Quarterly Vulnerability Scans: OS / DB / Web / VM
- Update Security Program Artifacts
- Reporting the security state of the information system to appropriate organizational officials annually.

JD Biggs & Associates Inc. www.jdbiggs.com
POC: Brandon G. Ghrist, brandon@jdbiggs.com, 202-596-8245
Copyright © 2012 JD Biggs & Associates Inc

Which framework is right for my business?

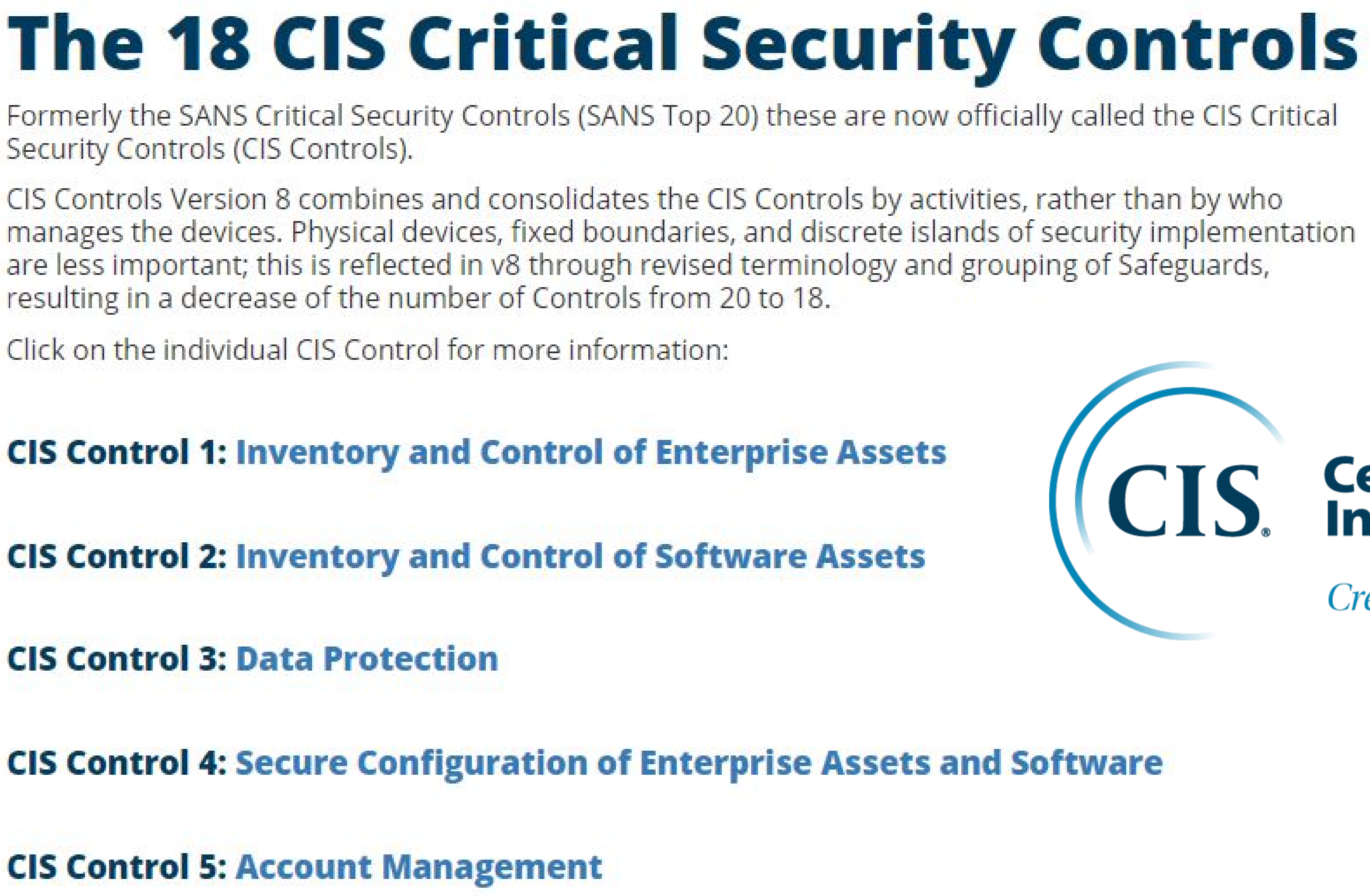
- **NIST Cybersecurity Framework** ***vs*** **ISO 27002** ***vs*** **NIST 800-53** ***vs*** **Secure Controls Framework**

- It is important to understand that ***picking a cybersecurity framework is more of a business decision and less of a technical decision***. Realistically, the process of selecting a cybersecurity framework must be driven by a fundamental understanding of what your organization needs to comply with from a statutory, regulatory and contractual perspective, since that understanding establishes the *minimum* set of requirements necessary to **(1)** not be considered negligent with reasonable expectations for security & privacy; **(2)** comply with applicable laws, regulations and contracts; and **(3)** implement the proper controls to secure your systems, applications and processes from reasonable threats. This understanding makes it pretty easy to determine where on the "framework spectrum" (shown below) you need to focus for selecting a set of cybersecurity principles to follow. This process generally leads to selecting either the NIST Cybersecurity Framework, ISO 27002 or NIST 800-53 as a starting point:


NIST Cybersecurity Framework
NIST 800-53 Low Baseline
ISO ISO 27002
NIST 800-53 Moderate Baseline
SCF Secure Controls Framework
ISACA COBIT 2019
enisa European Network and Information Security Agency
PCI PCI DSS
CIS Center for Internet Security CSC / Top 20
NIST 800-171
FedRAMP
NIST 800-53 High Baseline
Weaker Coverage
Moderate Coverage
Robust Coverage

https://www.complianceforge.com/faq/nist-800-53-vs-iso-27002-vs-nist-csf.html

Which framework is right for my business?



The 18 CIS Critical Security Controls

Formerly the SANS Critical Security Controls (SANS Top 20) these are now officially called the CIS Critical Security Controls (CIS Controls).

CIS Controls Version 8 combines and consolidates the CIS Controls by activities, rather than by who manages the devices. Physical devices, fixed boundaries, and discrete islands of security implementation are less important; this is reflected in v8 through revised terminology and grouping of Safeguards, resulting in a decrease of the number of Controls from 20 to 18.

Click on the individual CIS Control for more information:

CIS Control 1: Inventory and Control of Enterprise Assets

CIS Control 2: Inventory and Control of Software Assets

CIS Control 3: Data Protection

CIS Control 4: Secure Configuration of Enterprise Assets and Software

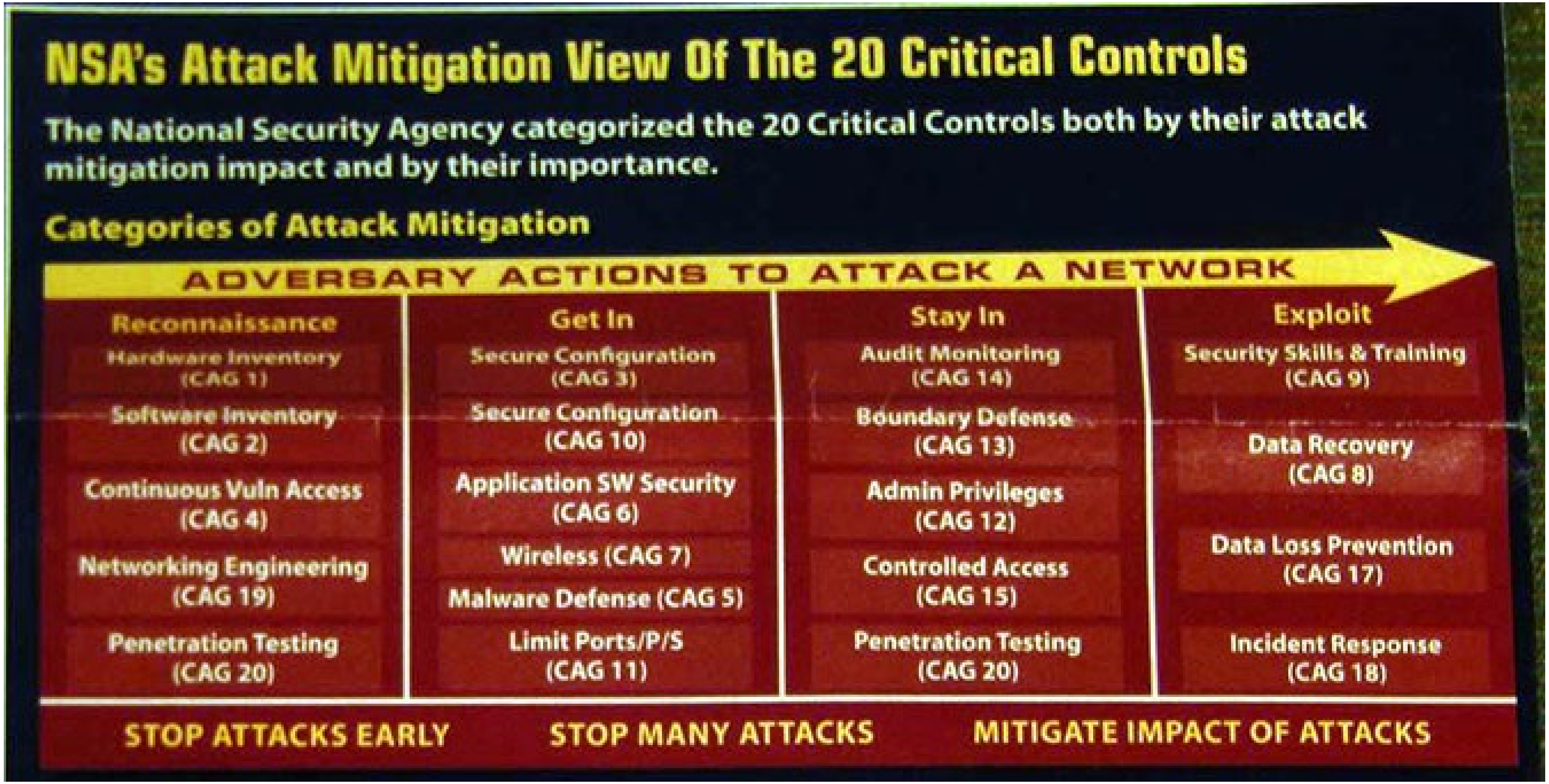
CIS Control 5: Account Management

CIS Center for Internet Security®

Creating Confidence in the Connected World.™

https://www.cisecurity.org/controls/cis-controls-list/

Which framework is right for my business?



NSA's Attack Mitigation View Of The 20 Critical Controls

The National Security Agency categorized the 20 Critical Controls both by their attack mitigation impact and by their importance.

Categories of Attack Mitigation

ADVERSARY ACTIONS TO ATTACK A NETWORK

Reconnaissance

- Hardware Inventory (CAG 1)
- Software Inventory (CAG 2)
- Continuous Vuln Access (CAG 4)
- Networking Engineering (CAG 19)
- Penetration Testing (CAG 20)

Get In

- Secure Configuration (CAG 3)
- Secure Configuration (CAG 10)
- Application SW Security (CAG 6)
- Wireless (CAG 7)
- Malware Defense (CAG 5)
- Limit Ports/P/S (CAG 11)

Stay In

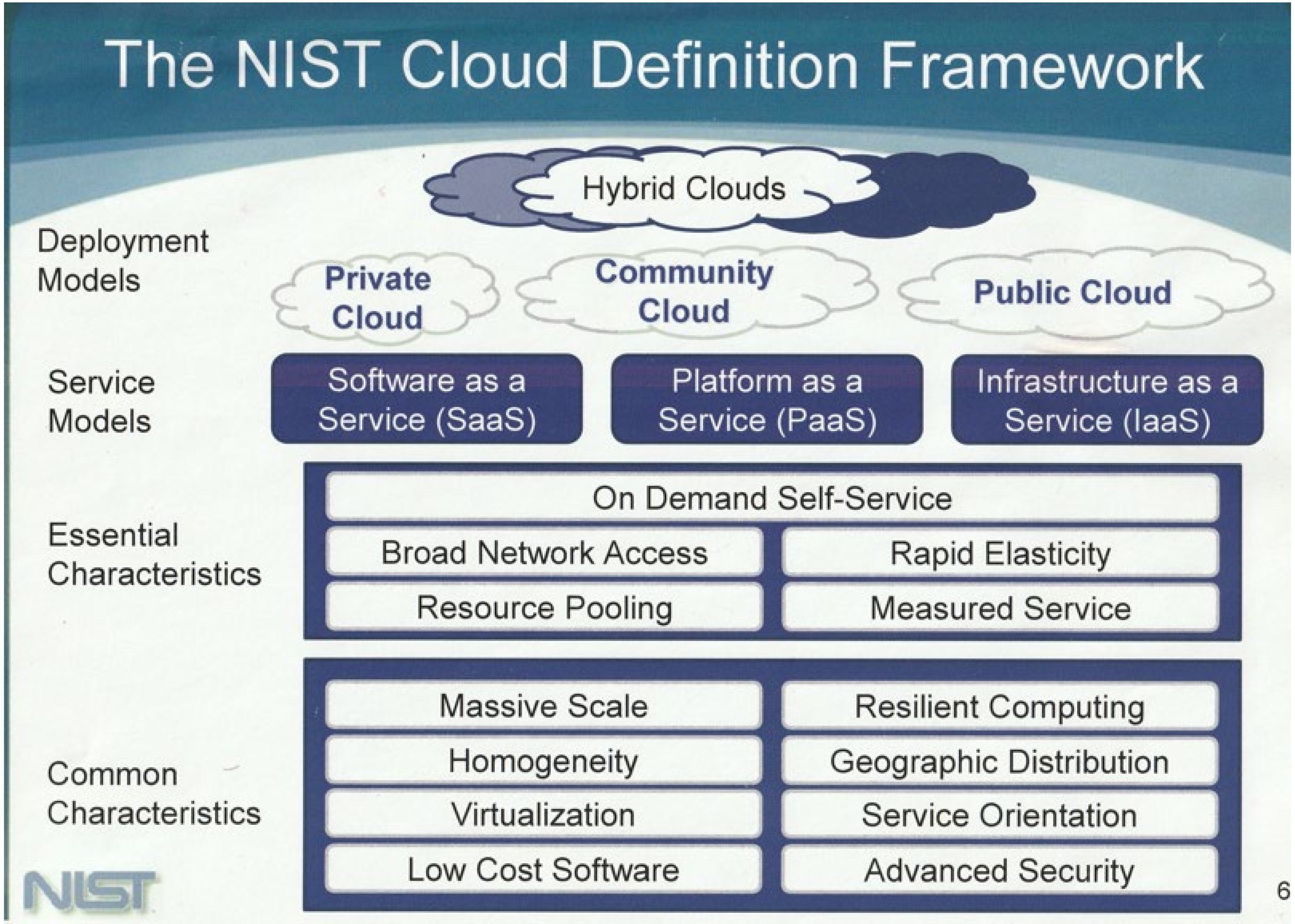
- Audit Monitoring (CAG 14)
- Boundary Defense (CAG 13)
- Admin Privileges (CAG 12)
- Controlled Access (CAG 15)
- Penetration Testing (CAG 20)

Exploit

- Security Skills & Training (CAG 9)
- Data Recovery (CAG 8)
- Data Loss Prevention (CAG 17)
- Incident Response (CAG 18)

STOP ATTACKS EARLY STOP MANY ATTACKS MITIGATE IMPACT OF ATTACKS

Which framework is right for my business?



The NIST Cloud Definition Framework

Deployment Models	Hybrid Clouds		
	Private Cloud	Community Cloud	Public Cloud
Service Models	Software as a Service (SaaS)	Platform as a Service (PaaS)	Infrastructure as a Service (IaaS)

Essential Characteristics

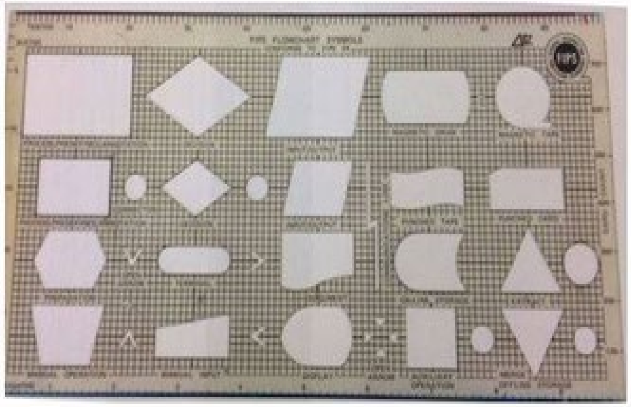
On Demand Self-Service	
Broad Network Access	Rapid Elasticity
Resource Pooling	Measured Service

Common Characteristics

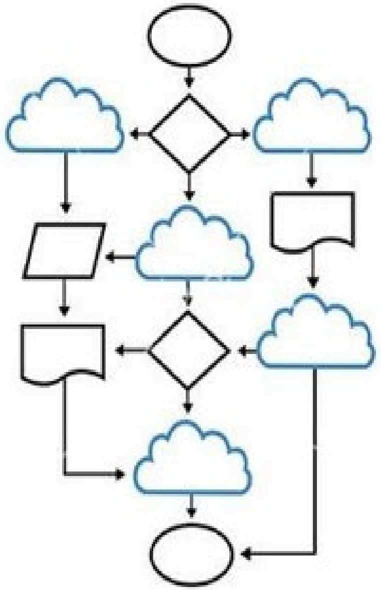
Massive Scale	Resilient Computing
Homogeneity	Geographic Distribution
Virtualization	Service Orientation
Low Cost Software	Advanced Security

6

Before

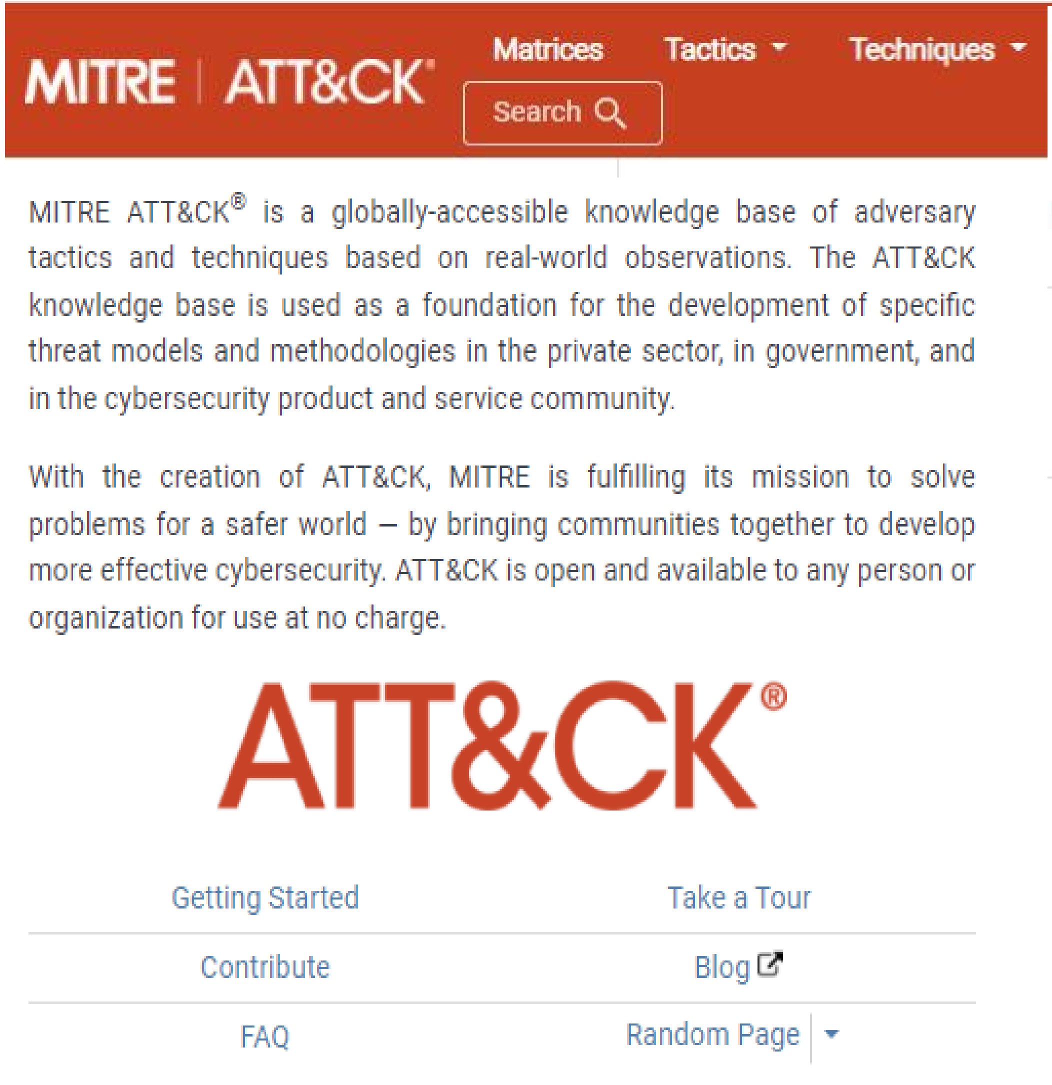


After



https://securityfeeds.us/cloud-security

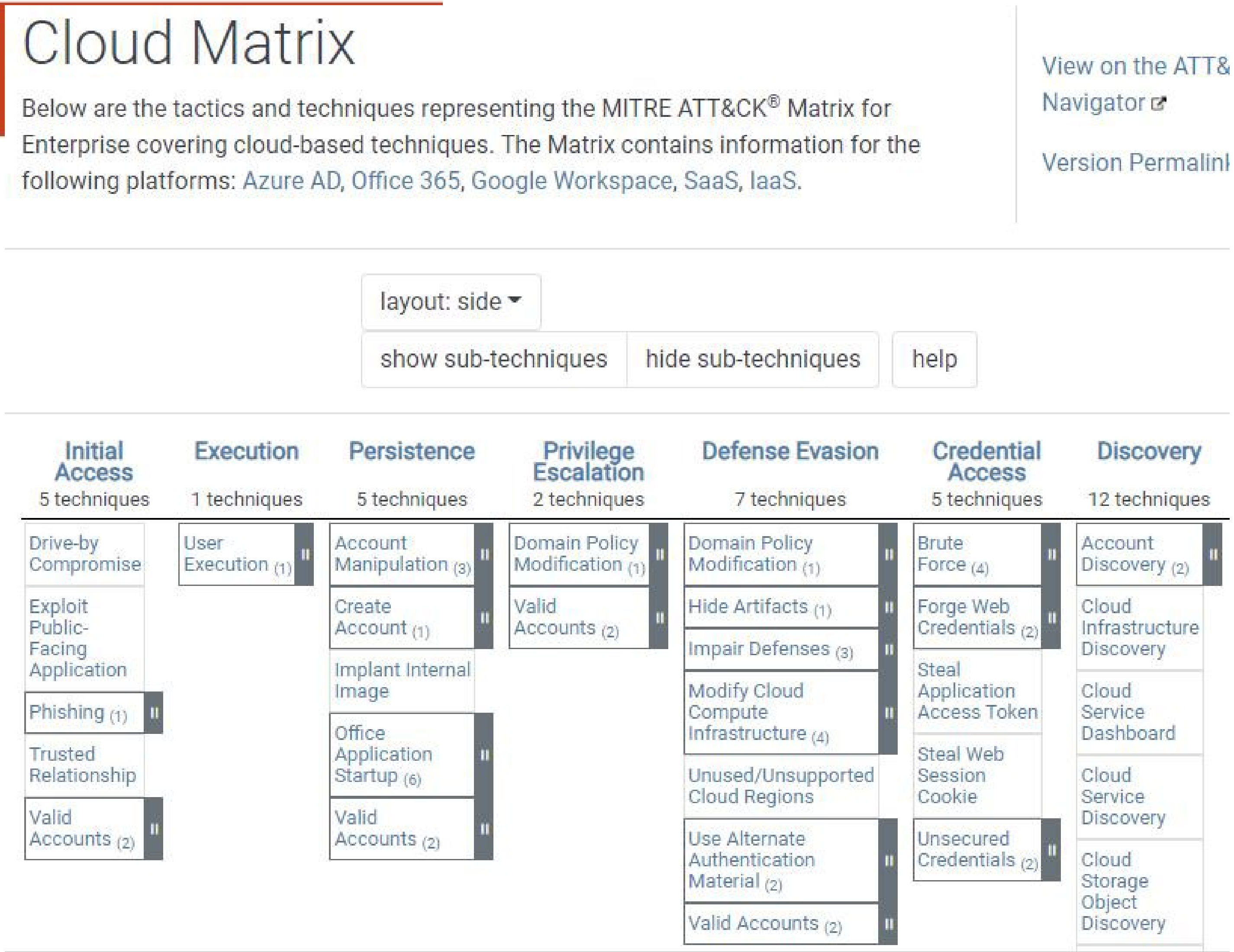
Which framework is right for my business?



MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

https://attack.mitre.org/



Cloud Matrix

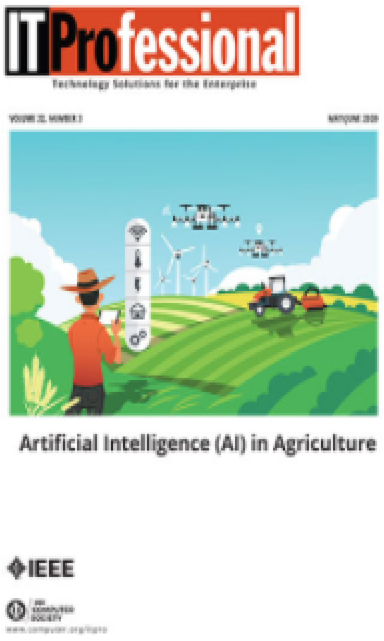
Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the following platforms: Azure AD, Office 365, Google Workspace, SaaS, IaaS.

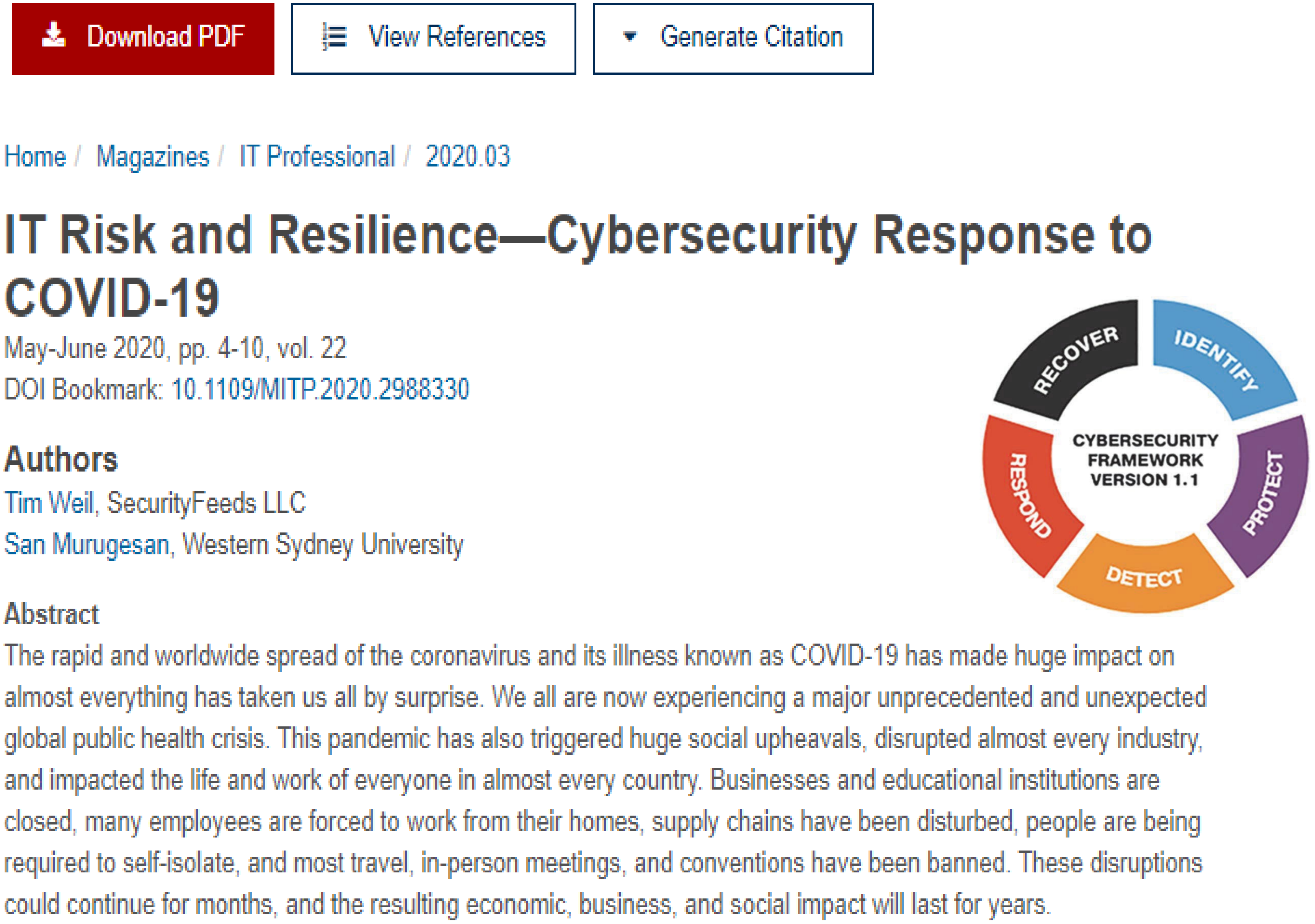
Initial Access 5 techniques	Execution 1 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Defense Evasion 7 techniques	Credential Access 5 techniques	Discovery 12 techniques
Drive-by Compromise	User Execution (1)	Account Manipulation (3)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)
Exploit Public-Facing Application		Create Account (1)	Valid Accounts (2)	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Infrastructure Discovery
Phishing (1)		Implant Internal Image		Impair Defenses (3)	Steal Application Access Token	Cloud Service Dashboard
Trusted Relationship		Office Application Startup (6)		Modify Cloud Compute Infrastructure (4)	Steal Web Session Cookie	Cloud Service Discovery
Valid Accounts (2)		Valid Accounts (2)		Unused/Unsupported Cloud Regions	Unsecured Credentials (2)	Cloud Storage Object Discovery
				Use Alternate Authentication Material (2)		
				Valid Accounts (2)		

Table of Contents

- Cyberspace – Our Point of Departure
- Information Security Management Models
- Frameworks for Risk Management
- COVID Smackdown – NIST CSF vs Big Scary Monsters
- Emerging Roads Maps to Risk Management
- References + Q&A

Global transformation caused by COVID-19


ITProfessional
Technology Solutions for the Enterprise
Artificial Intelligence (AI) in Agriculture
IEEE


Download PDF
View References
Generate Citation
Home / Magazines / IT Professional / 2020.03
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

IT Risk and Resilience—Cybersecurity Response to COVID-19

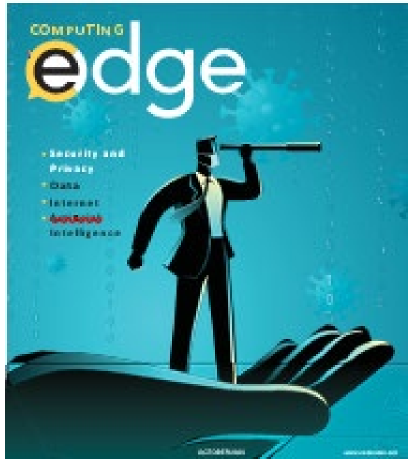
May-June 2020, pp. 4-10, vol. 22
DOI Bookmark: 10.1109/MITP.2020.2988330

Authors

Tim Weil, SecurityFeeds LLC
San Murugesan, Western Sydney University

Abstract

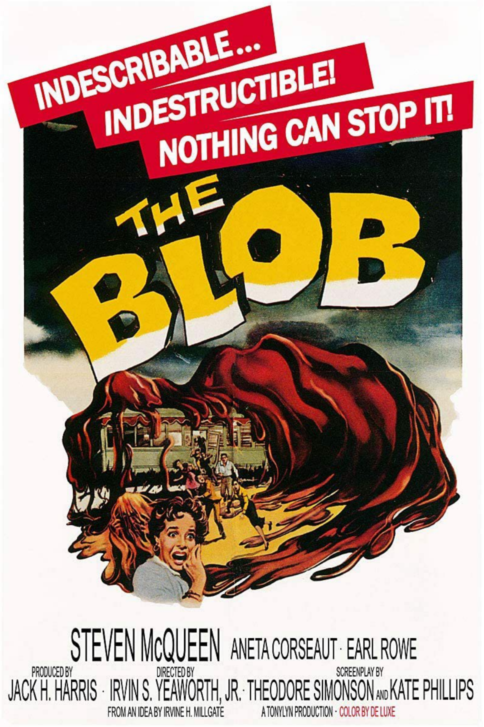
The rapid and worldwide spread of the coronavirus and its illness known as COVID-19 has made huge impact on almost everything has taken us all by surprise. We all are now experiencing a major unprecedented and unexpected global public health crisis. This pandemic has also triggered huge social upheavals, 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.



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

Big Scary Monsters - Global transformation caused by COVID-19

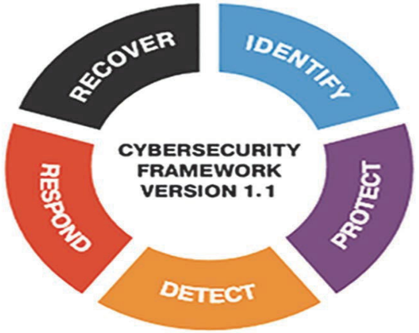

INDESCRIBABLE...
INDESTRUCTIBLE!
NOTHING CAN STOP IT!
THE BLOB
STEVEN McQUEEN ANETA CORSEAUT · EARL ROWE
PRODUCED BY JACK H. HARRIS · DIRECTED BY IRVIN S. YEAWORTH, JR. · SCREENPLAY BY THEODORE SIMONSON AND KATE PHILLIPS
FROM AN IDEA BY IRVINE H. MILLGATE
A TONYLYN PRODUCTION · COLOR BY DE LUXE

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

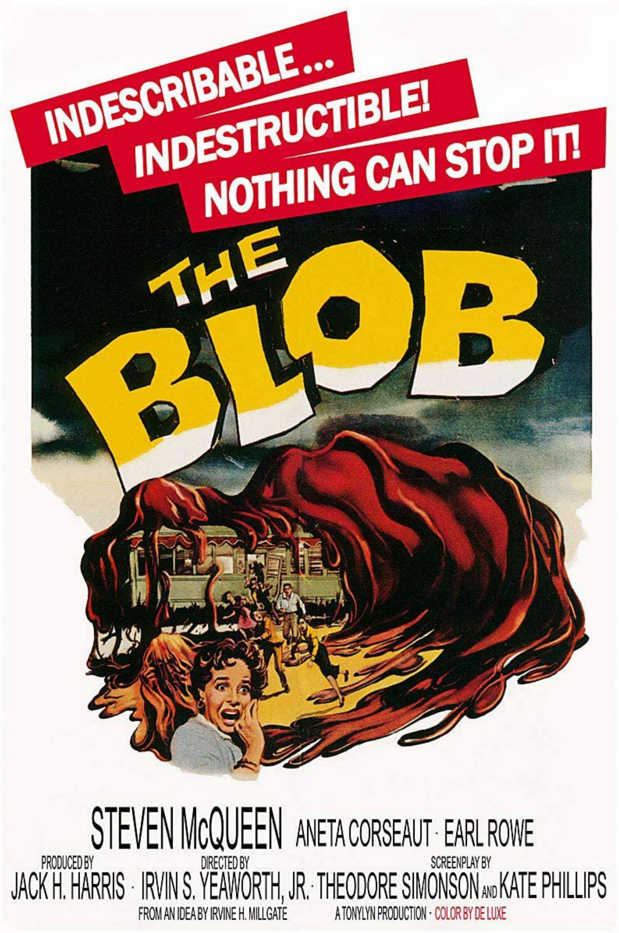
A HORROR HORDE OF CRAWL-AND-CRUSH GIANTS
CLAWING OUT OF THE EARTH
FROM MILE-DEEP
CATACOMBS!
"THEM"
"This city is under martial law until we annihilate THEM!"
Kill one and two take it's place!
THE AMAZING NEW WARNER BROS. SENSATION!
"THEM!" JAMES WHITMORE . EDMUND GWENN . JOAN WELDON . JAMES ARNESS

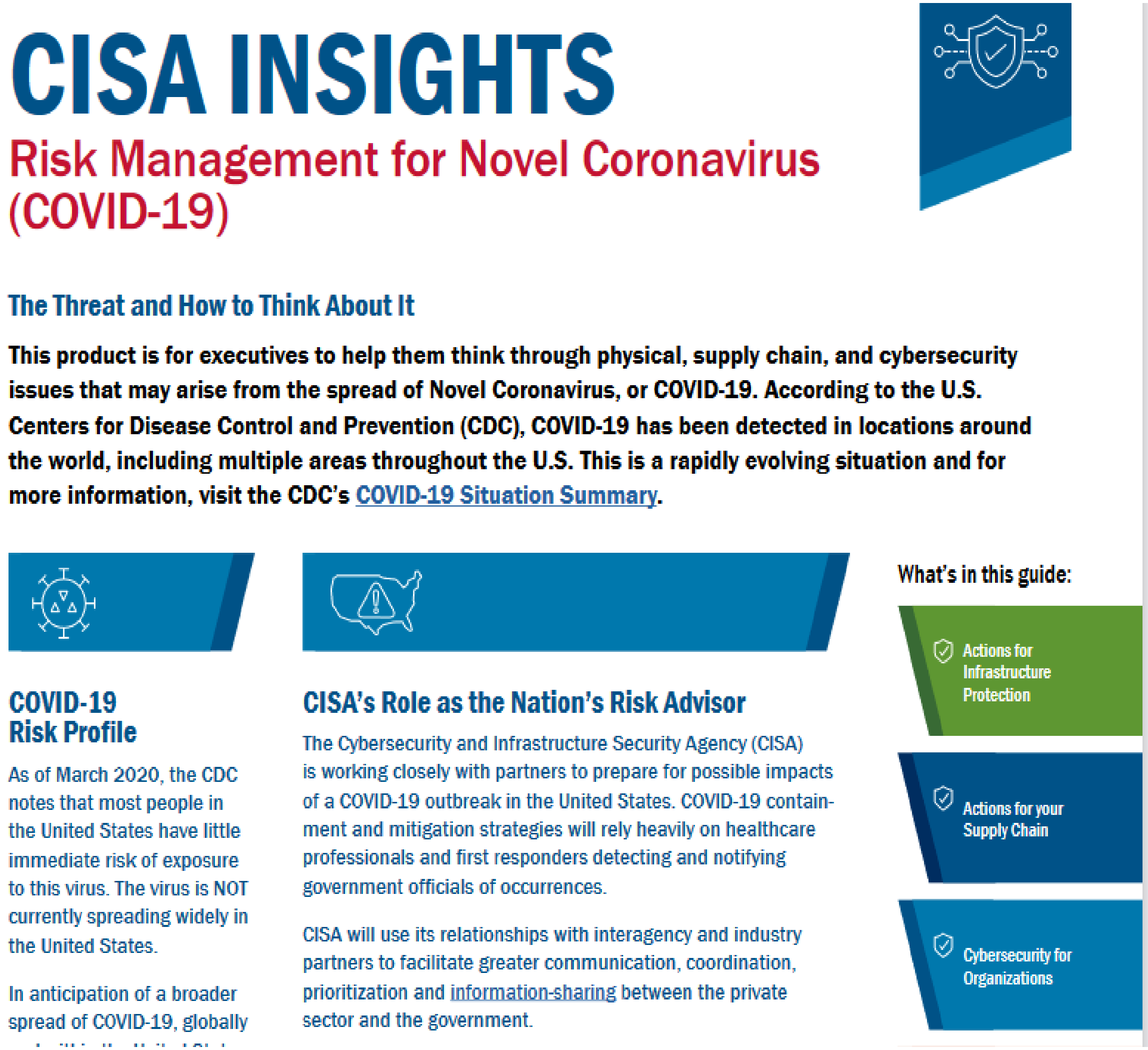
Them While investigating a series of mysterious deaths, Sergeant Ben Peterson finds a young girl agent Robert Graham and scientist Dr. Harold Medford), he discovers that all the incidents are due to giant ants that have been mutated by atomic radiation. Peterson and Graham, with the aid of the military,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

The FUD Factor – Fear, Uncertainty and Doubt



CSF Identify 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. · SCREENPLAY BY THEODORE SIMONSON AND KATE PHILLIPS
FROM AN IDEA BY IRVINE H. MILLGATE
A TONYLYN PRODUCTION · COLOR BY DE LUXE



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

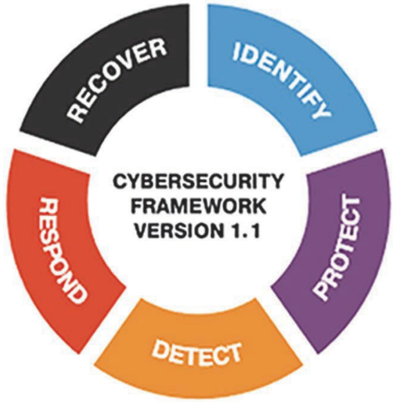
CISA's Role as the Nation's Risk Advisor

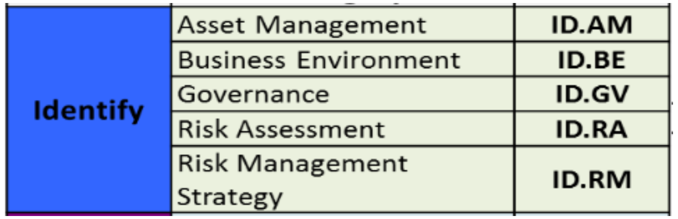
The Cybersecurity and Infrastructure Security Agency (CISA) is working closely with partners to prepare for possible impacts of a COVID-19 outbreak in the United States. COVID-19 containment and mitigation strategies will rely heavily on healthcare professionals and first responders detecting and notifying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





Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	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 Recover Controls for COVID-19 - https://www.acq.osd.mil/jrac/da2/index.html

Defense Assisted Acquisition (DA2) Cell

The DA2 has assumed the interagency efforts for COVID-19 medical resource acquisition previously coordinated by the DoD's Joint Acquisition Task Force (JATF). Nested within the Joint Rapid Acquisition Cell (JRAC), the DA2 is poised to rapidly respond to the nation's most urgent acquisition needs in current and future national emergencies.

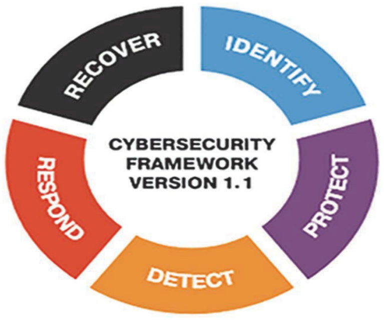
•DOD Awards $231.8 Million Contract to Ellume USA LLC to Increase Domestic Production Capacity and Deliver COVID-19 Home Tests

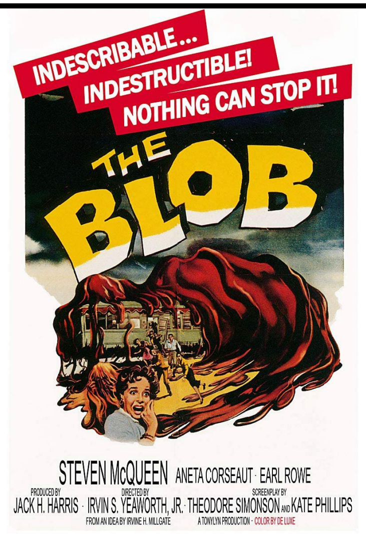
•DOD Awards $69.3 Million Contract to CONTINUUS Pharmaceuticals to Develop US-based Continuous Manufacturing Capability for Critical Medicines

•DOD Awards $110 Million Firm Fixed Price Contract Action to Puritan Medical Products to Increase Domestic Production Capacity of Foam Tip Swabs

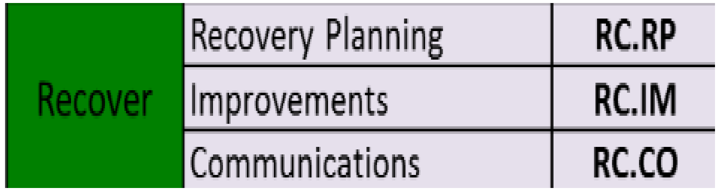
•DOD Awards $15 Million Firm Fixed Price Contract to Corning Incorporated to Increase Domestic Production Capacity of Robotic Pipette Tips

•DOD Awards $4.8 Million Indefinite Delivery/Indefinite Quantity to a Calibre Scientific Subsidiary, Anatrace, to Increase Domestic Production Capacity of COVID-19 Testing Reagents



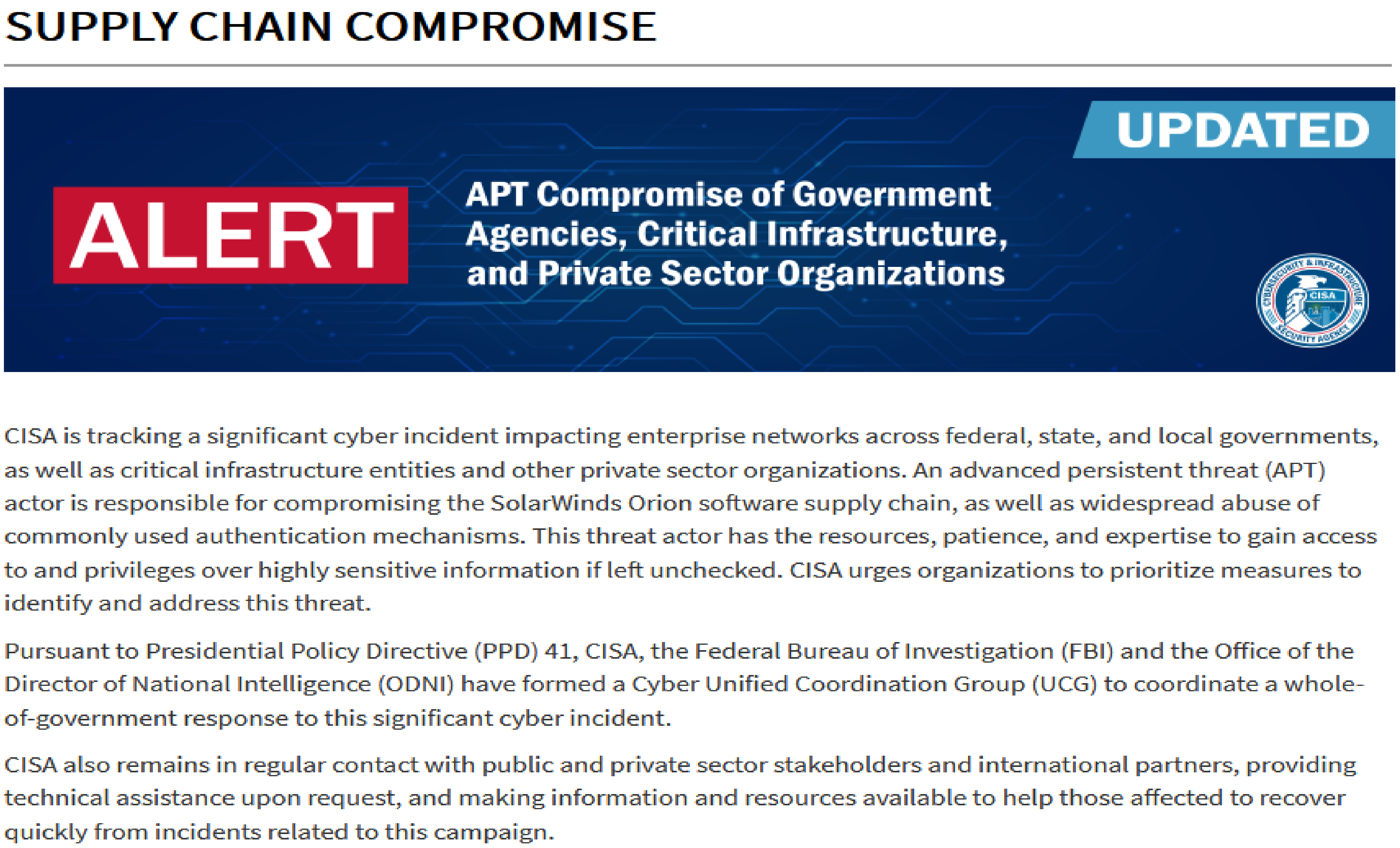

INDESCRIBABLE...
INDESTRUCTIBLE!
NOTHING CAN STOP IT!
THE BLOB
STEVEN McQUEEN ANETA CORSEAUT · EARL ROWE
JACK H. HARRIS · IRVIN S. YEAWORTH, JR. · THEODORE SIMONSON AND KATE PHILLIPS

A HORROR HORDE OF CRAWL-AND-CRUSH GIANTS
CLAWING OUT OF THE EARTH
FROM MILE-DEEP
CATACOMBS!
"THEM"
"This city is under martial law until we annihilate THEM!"
Kill one and two take it's place!
THE AMAZING NEW WARNER BROS. SENSATION!
"THEM!" JAMES WHITMORE . EDMUND GWENN . JOAN WELDON . JAMES ARNESS



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

SUNBURST - Solar Winds ORION NMS APT Attack (2019 - 2021) - Oops



SUPPLY CHAIN COMPROMISE

UPDATED

ALERT

APT Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

CISA is tracking a significant cyber incident impacting enterprise networks across federal, state, and local governments, as well as critical infrastructure entities and other private sector organizations. An advanced persistent threat (APT) actor is responsible for compromising the SolarWinds Orion software supply chain, as well as widespread abuse of commonly used authentication mechanisms. This threat actor has the resources, patience, and expertise to gain access to and privileges over highly sensitive information if left unchecked. CISA urges organizations to prioritize measures to identify and address this threat.

Pursuant to Presidential Policy Directive (PPD) 41, CISA, the Federal Bureau of Investigation (FBI) and the Office of the Director of National Intelligence (ODNI) have formed a Cyber Unified Coordination Group (UCG) to coordinate a whole-of-government response to this significant cyber incident.

CISA also remains in regular contact with public and private sector stakeholders and international partners, providing technical assistance upon request, and making information and resources available to help those affected to recover quickly from incidents related to this campaign.

https://www.cisa.gov/supply-chain-compromise

No One Knows How Deep Russia's Hacking Rampage Goes

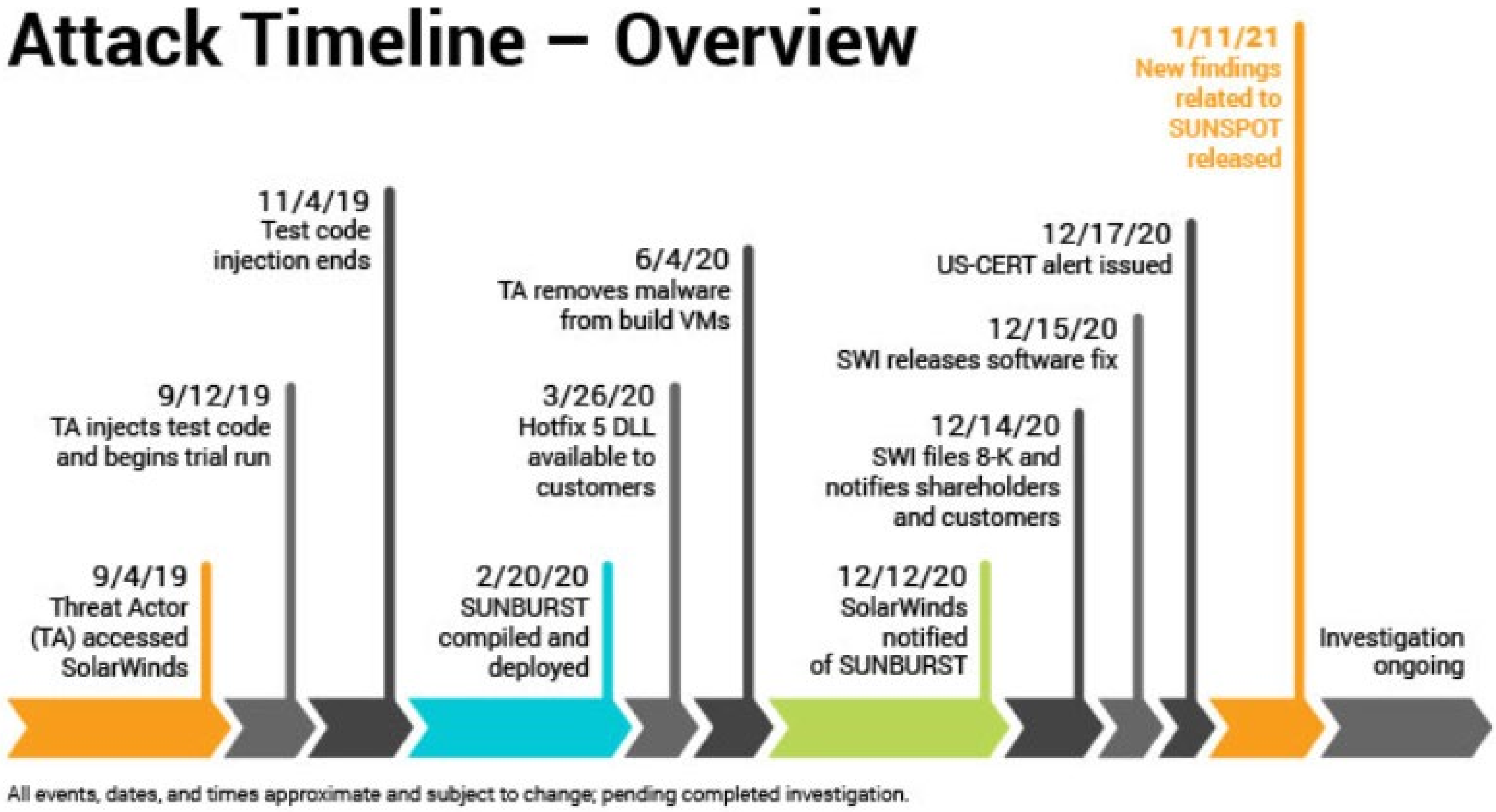
A supply chain attack against IT company SolarWinds has exposed as many as 18,000 companies to Cozy Bear's attacks.

- **SANS Bulletin - Threat Actors Behind SolarWinds Used Multiple Attack Vectors** - **(January 29 & February 1, 2021)**

- The *acting director of the US Cybersecurity and Infrastructure Security Agency (CISA)* says that "significant numbers of both the private-sector and government victims linked to this campaign had no direct connection to SolarWinds." The threat actors multiple attack vectors. (Please note that the WSJ story is behind a paywall.)

- **Read more in:**
  - **www.securityweek.com**: CISA Says Many Victims of SolarWinds Hackers Had No Direct Link to SolarWinds
  - **www.scmagazine.com**: Does SolarWinds change the rules in offensive cyber? Experts say no, but offer alternatives
  - **www.scmagazine.com**: As SolarWinds spooks tech firms into rechecking code, some won't like what they find
  - **www.zdnet.com**: SolarWinds attack is not an outlier, but a moment of reckoning for security industry, says Microsoft exec
  - **www.wsj.com**: Suspected Russian Hack Extends Far Beyond SolarWinds Software, Investigators Say (paywall)
  - **arstechnica.com**: 30% of "SolarWinds hack" victims didn't actually use SolarWinds

SUNBURST - Solar Winds ORION NMS APT Attack (2019 - 2021) - Oops



Attack Timeline – Overview

9/4/19
Threat Actor (TA) accessed SolarWinds

9/12/19
TA injects test code and begins trial run

11/4/19
Test code injection ends

2/20/20
SUNBURST compiled and deployed

3/26/20
Hotfix 5 DLL available to customers

6/4/20
TA removes malware from build VMs

12/12/20
SolarWinds notified of SUNBURST

12/14/20
SWI files 8-K and notifies shareholders and customers

12/15/20
SWI releases software fix

12/17/20
US-CERT alert issued

1/11/21
New findings related to SUNSPOT released

Investigation ongoing

All events, dates, and times approximate and subject to change; pending completed investigation.

https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details

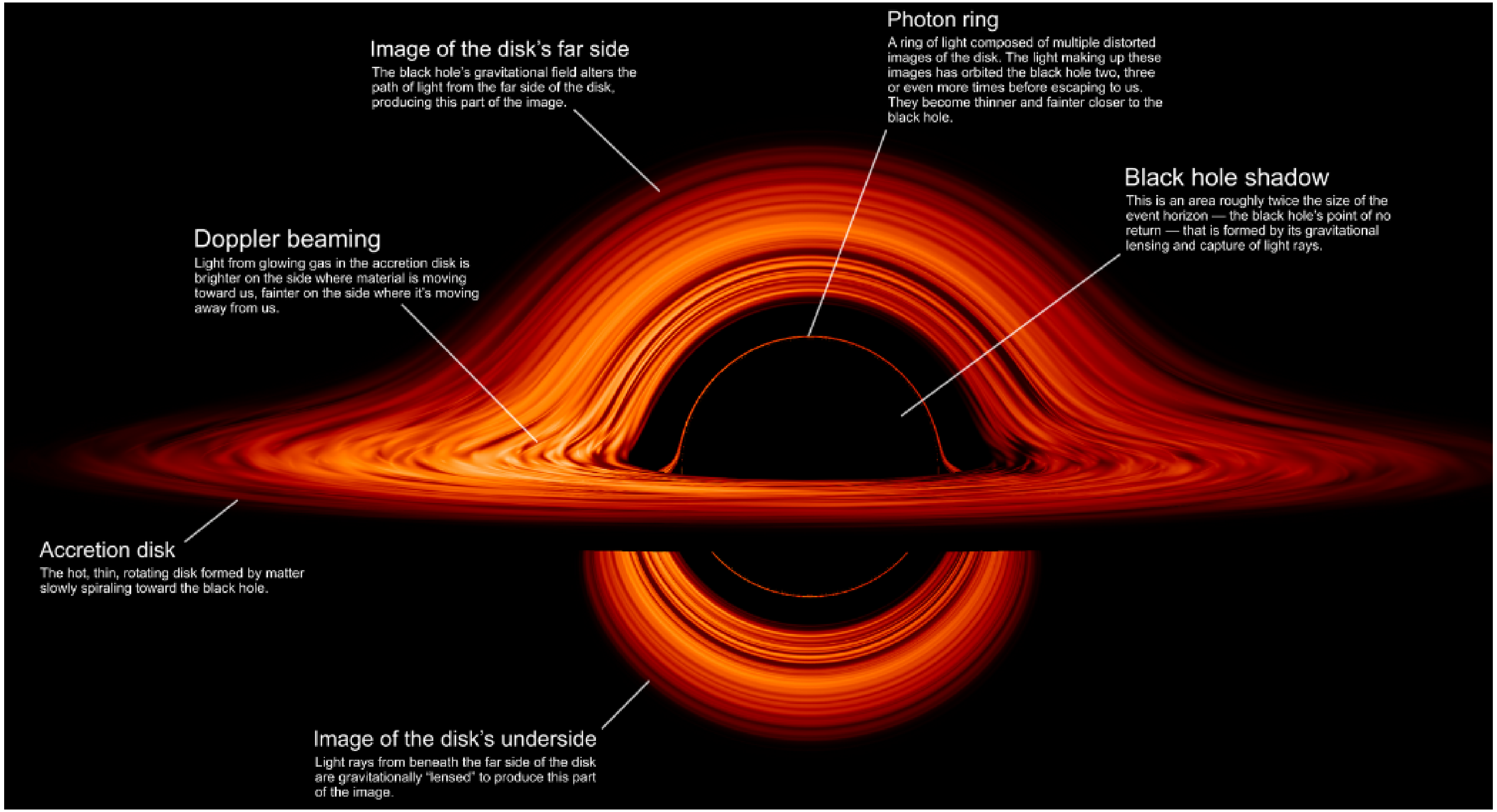


Image of the disk's far side
The black hole's gravitational field alters the path of light from the far side of the disk, producing this part of the image.
Photon ring
A ring of light composed of multiple distorted images of the disk. The light making up these images has orbited the black hole two, three or even more times before escaping to us. They become thinner and fainter closer to the black hole.
Black hole shadow
This is an area roughly twice the size of the event horizon — the black hole's point of no return — that is formed by its gravitational lensing and capture of light rays.
Doppler beaming
Light from glowing gas in the accretion disk is brighter on the side where material is moving toward us, fainter on the side where it's moving away from us.
Accretion disk
The hot, thin, rotating disk formed by matter slowly spiraling toward the black hole.
Image of the disk's underside
Light rays from beneath the far side of the disk are gravitationally "lensed" to produce this part of the image.

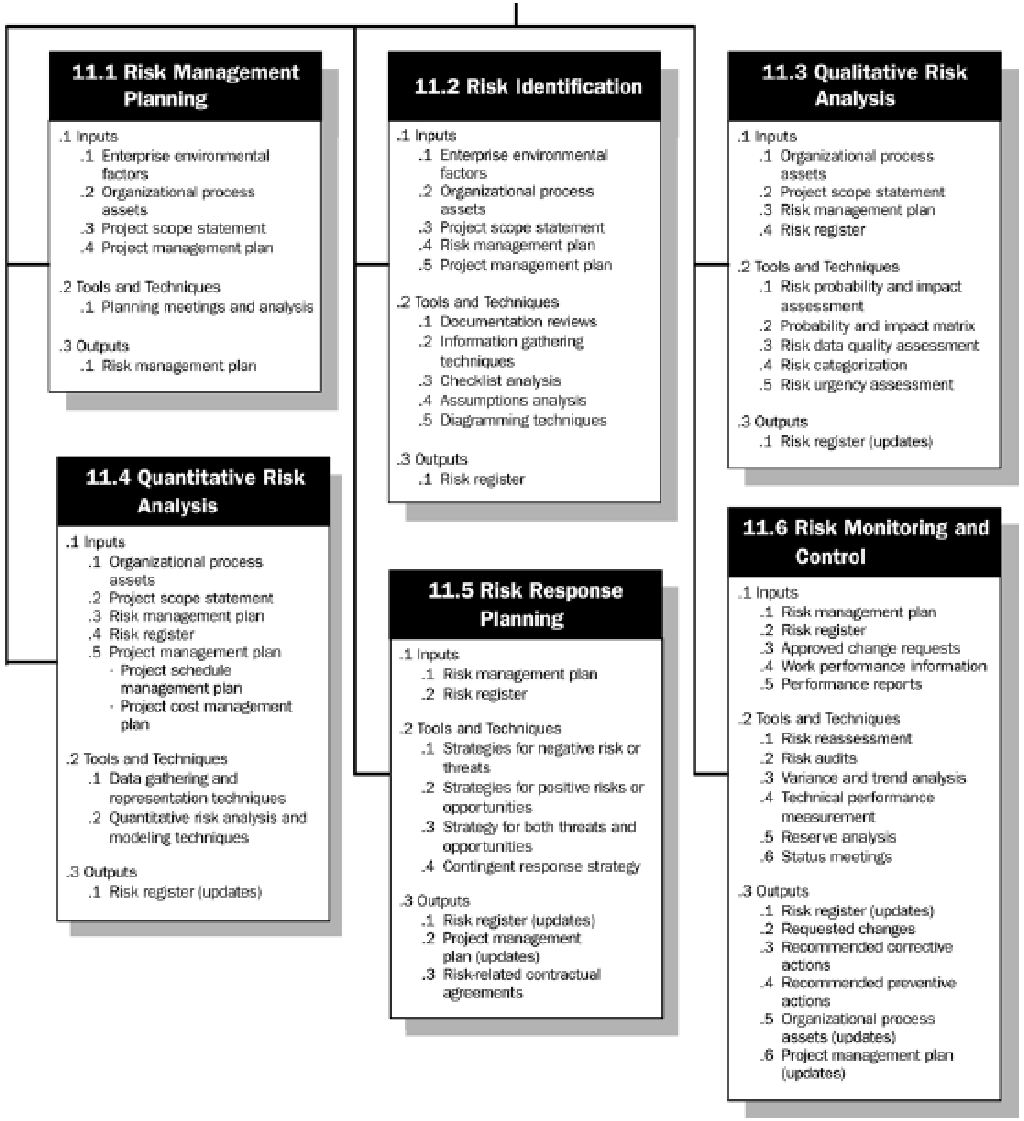
NASA Visualization Shows a Black Hole’s Warped World

This new visualization of a black hole illustrates how its gravity distorts our view, warping its surroundings as if seen in a carnival mirror. The visualization simulates the appearance of a black hole where infalling matter has collected into a thin, hot structure called an accretion disk. The black hole’s extreme gravity skews light emitted by different regions of the disk, producing the misshapen appearance.
https://www.nasa.gov/feature/goddard/2019/nasa-visualization-shows-a-black-hole-s-warped-world

Table of Contents

- Cyberspace – Our Point of Departure
- Information Security Management Models
- Frameworks for Risk Management
- COVID Smackdown – NIST CSF vs Big Scary Monsters
- Emerging Road Maps for Risk Management
- References

Practical Risk Management Methods (PMI PMBOK)



11.1 Risk Management Planning

.1 Inputs
- .1 Enterprise environmental factors
- .2 Organizational process assets
- .3 Project scope statement
- .4 Project management plan

.2 Tools and Techniques
- .1 Planning meetings and analysis

.3 Outputs
- .1 Risk management plan

11.2 Risk Identification

.1 Inputs
- .1 Enterprise environmental factors
- .2 Organizational process assets
- .3 Project scope statement
- .4 Risk management plan
- .5 Project management plan

.2 Tools and Techniques
- .1 Documentation reviews
- .2 Information gathering techniques
- .3 Checklist analysis
- .4 Assumptions analysis
- .5 Diagramming techniques

.3 Outputs
- .1 Risk register

11.3 Qualitative Risk Analysis

.1 Inputs
- .1 Organizational process assets
- .2 Project scope statement
- .3 Risk management plan
- .4 Risk register

.2 Tools and Techniques
- .1 Risk probability and impact assessment
- .2 Probability and impact matrix
- .3 Risk data quality assessment
- .4 Risk categorization
- .5 Risk urgency assessment

.3 Outputs
- .1 Risk register (updates)

11.4 Quantitative Risk Analysis

.1 Inputs
- .1 Organizational process assets
- .2 Project scope statement
- .3 Risk management plan
- .4 Risk register
- .5 Project management plan
  - Project schedule management plan
  - Project cost management plan

.2 Tools and Techniques
- .1 Data gathering and representation techniques
- .2 Quantitative risk analysis and modeling techniques

.3 Outputs
- .1 Risk register (updates)

11.5 Risk Response Planning

.1 Inputs
- .1 Risk management plan
- .2 Risk register

.2 Tools and Techniques
- .1 Strategies for negative risk or threats
- .2 Strategies for positive risks or opportunities
- .3 Strategy for both threats and opportunities
- .4 Contingent response strategy

.3 Outputs
- .1 Risk register (updates)
- .2 Project management plan (updates)
- .3 Risk-related contractual agreements

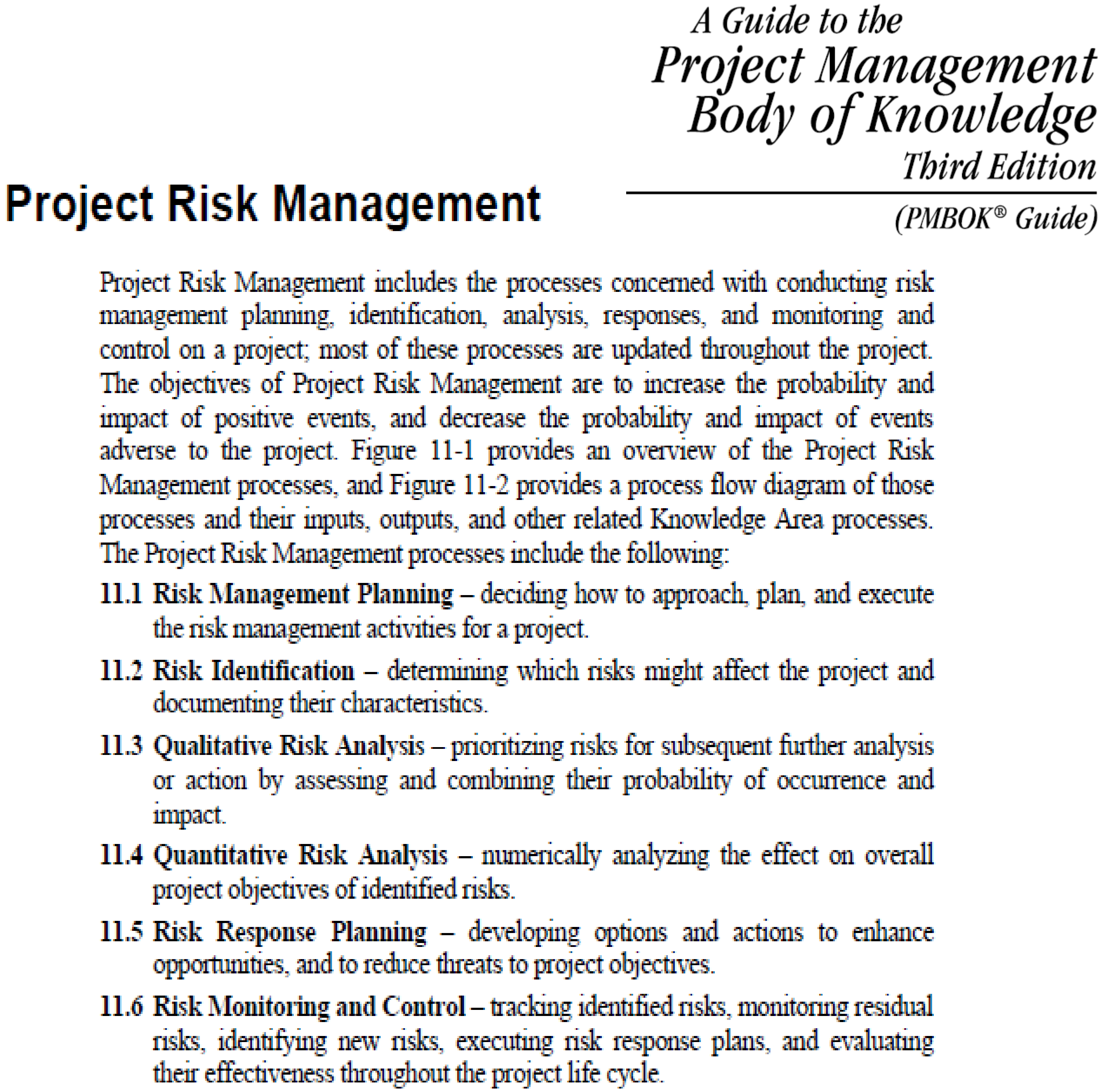
11.6 Risk Monitoring and Control

.1 Inputs
- .1 Risk management plan
- .2 Risk register
- .3 Approved change requests
- .4 Work performance information
- .5 Performance reports

.2 Tools and Techniques
- .1 Risk reassessment
- .2 Risk audits
- .3 Variance and trend analysis
- .4 Technical performance measurement
- .5 Reserve analysis
- .6 Status meetings

.3 Outputs
- .1 Risk register (updates)
- .2 Requested changes
- .3 Recommended corrective actions
- .4 Recommended preventive actions
- .5 Organizational process assets (updates)
- .6 Project management plan (updates)

Figure 11-1. Project Risk Management Overview



A Guide to the
Project Management Body of Knowledge
Third Edition
(PMBOK® Guide)

Project Risk Management

Project Risk Management includes the processes concerned with conducting risk management planning, identification, analysis, responses, and monitoring and control on a project; most of these processes are updated throughout the project. The objectives of Project Risk Management are to increase the probability and impact of positive events, and decrease the probability and impact of events adverse to the project. Figure 11-1 provides an overview of the Project Risk Management processes, and Figure 11-2 provides a process flow diagram of those processes and their inputs, outputs, and other related Knowledge Area processes. The Project Risk Management processes include the following:

11.1 **Risk Management Planning** – deciding how to approach, plan, and execute the risk management activities for a project.

11.2 **Risk Identification** – determining which risks might affect the project and documenting their characteristics.

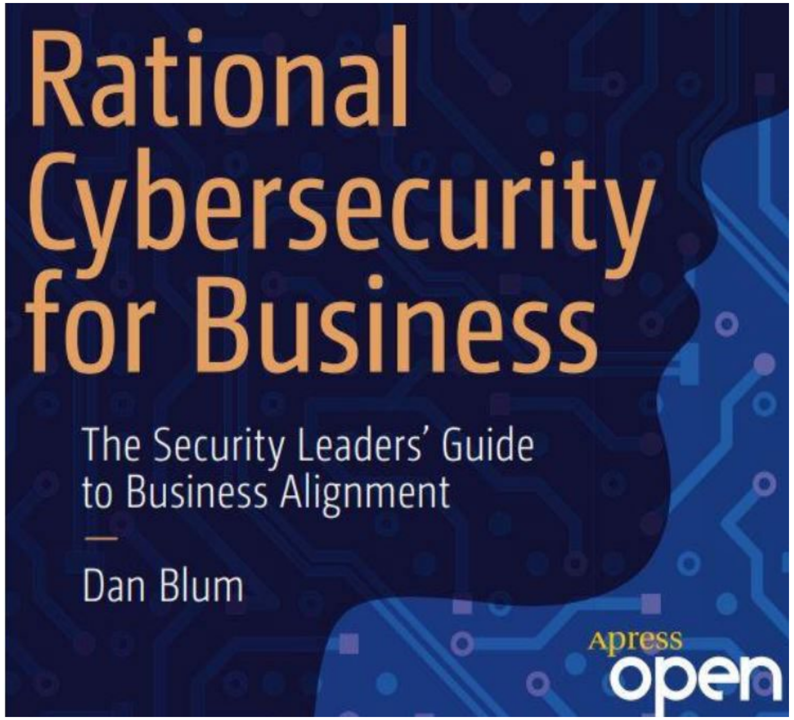
11.3 **Qualitative Risk Analysis** – prioritizing risks for subsequent further analysis or action by assessing and combining their probability of occurrence and impact.

11.4 **Quantitative Risk Analysis** – numerically analyzing the effect on overall project objectives of identified risks.

11.5 **Risk Response Planning** – developing options and actions to enhance opportunities, and to reduce threats to project objectives.

11.6 **Risk Monitoring and Control** – tracking identified risks, monitoring residual risks, identifying new risks, executing risk response plans, and evaluating their effectiveness throughout the project life cycle.

Taking Risk Management to the Boardroom

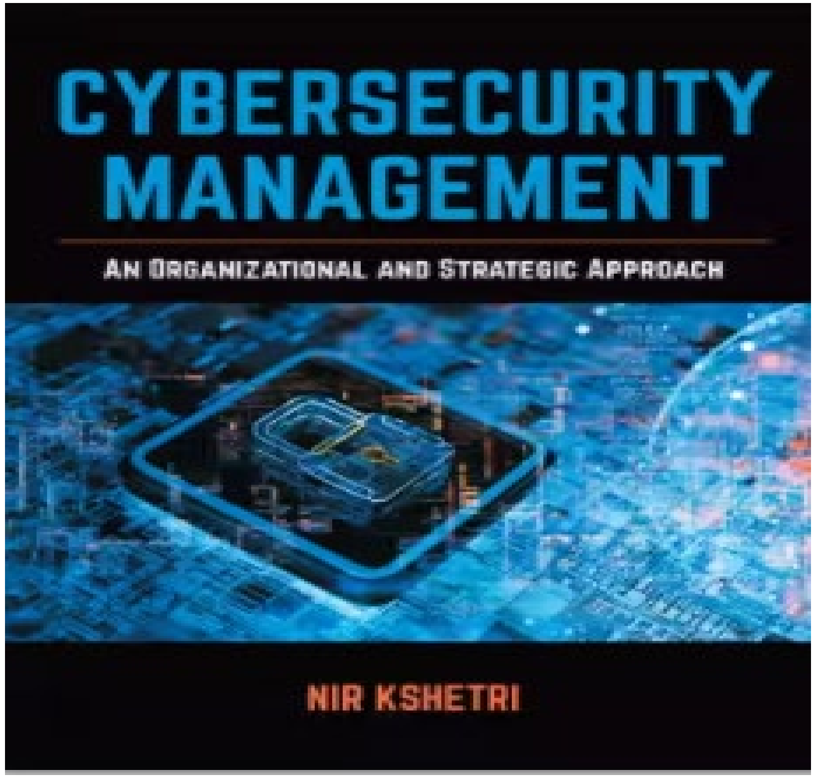


Rational Cybersecurity for Business

The Security Leaders' Guide to Business Alignment

Dan Blum

Apress open



CYBERSECURITY MANAGEMENT

AN ORGANIZATIONAL AND STRATEGIC APPROACH

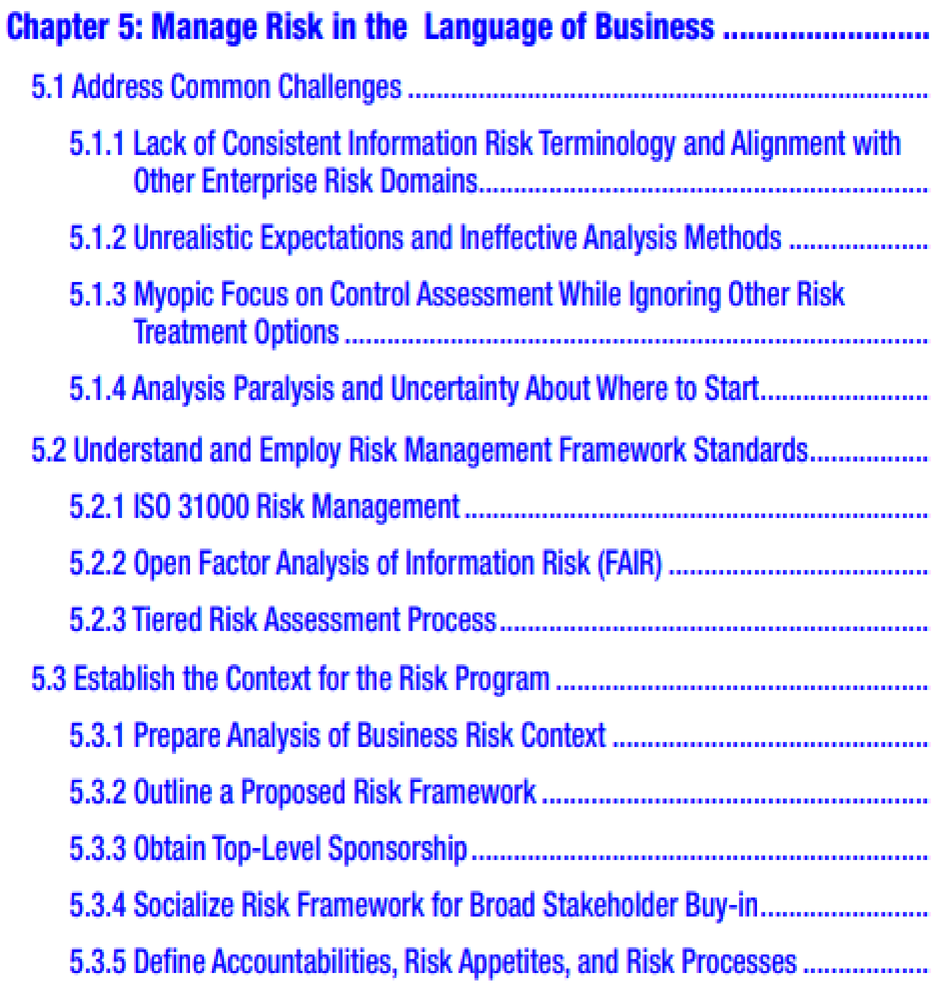
NIR KSHETRI

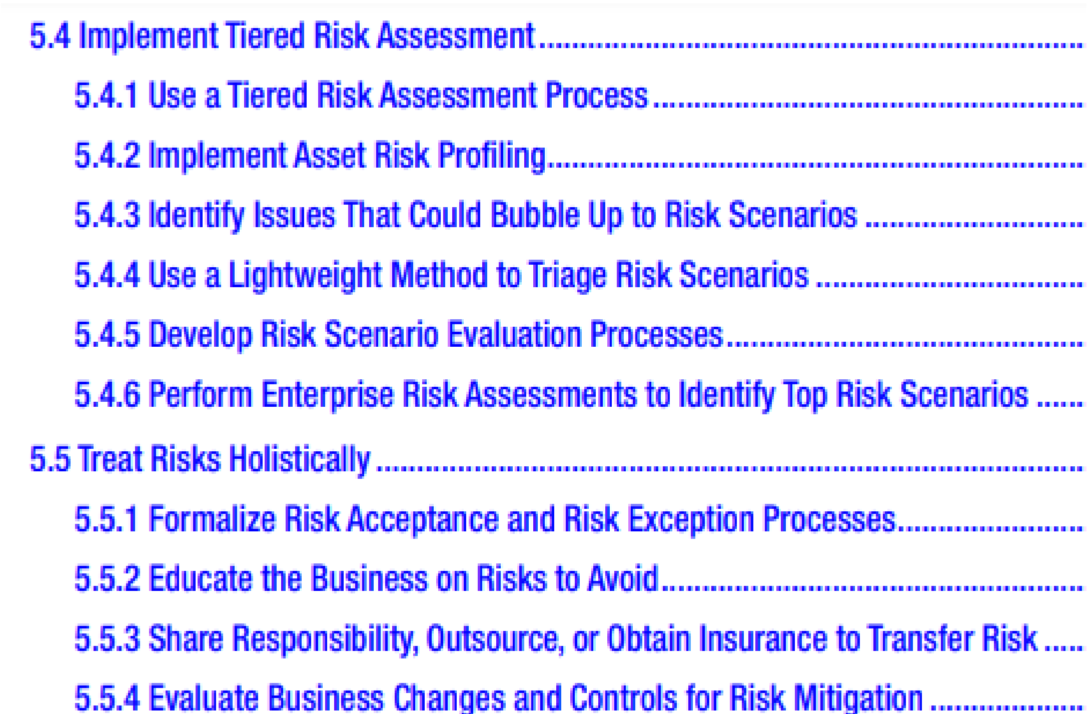
The first comprehensive field guide to cybersecurity-business alignment. Focuses on six areas to maximize the effectiveness of your cybersecurity program: risk management, control baseline, security culture, IT rationalization, access control, and cyber-resilience

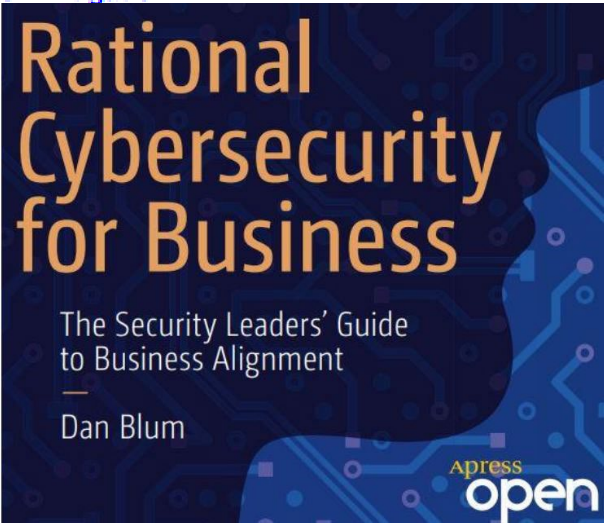
•Includes more than 50 keys to alignment and advice on how to scale them for businesses of different types and sizes

Cyberthreats are among the most critical issues facing the world today. *Cybersecurity Management* draws on case studies to analyze cybercrime at the macro level, and evaluates the strategic and organizational issues connected to cybersecurity. Cross-disciplinary in its focus, orientation, and scope, this book looks at emerging communication technologies that are currently under development to tackle emerging threats to data privacy.

Rational Cybersecurity for Business – Dan Blum







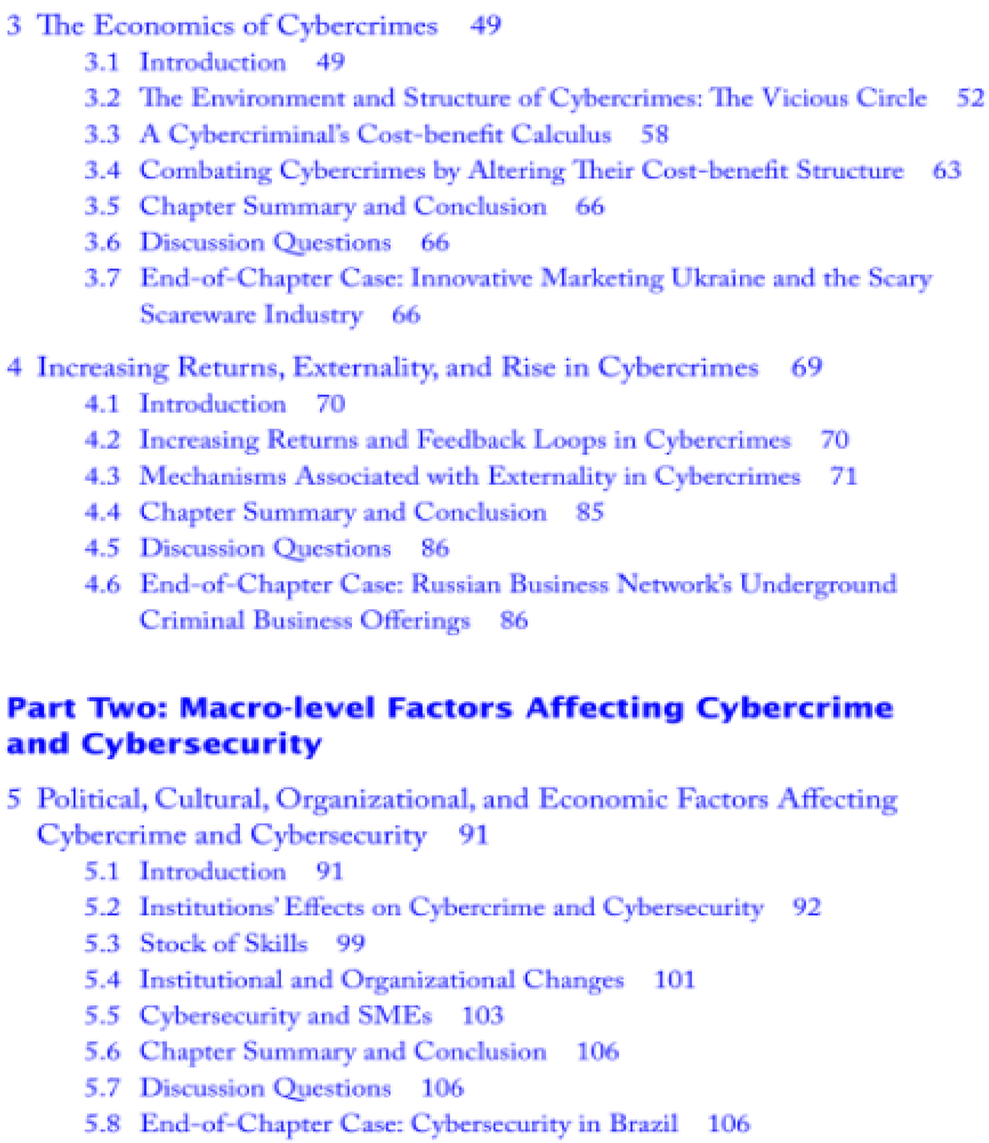
Rational Cybersecurity for Business

The Security Leaders' Guide to Business Alignment

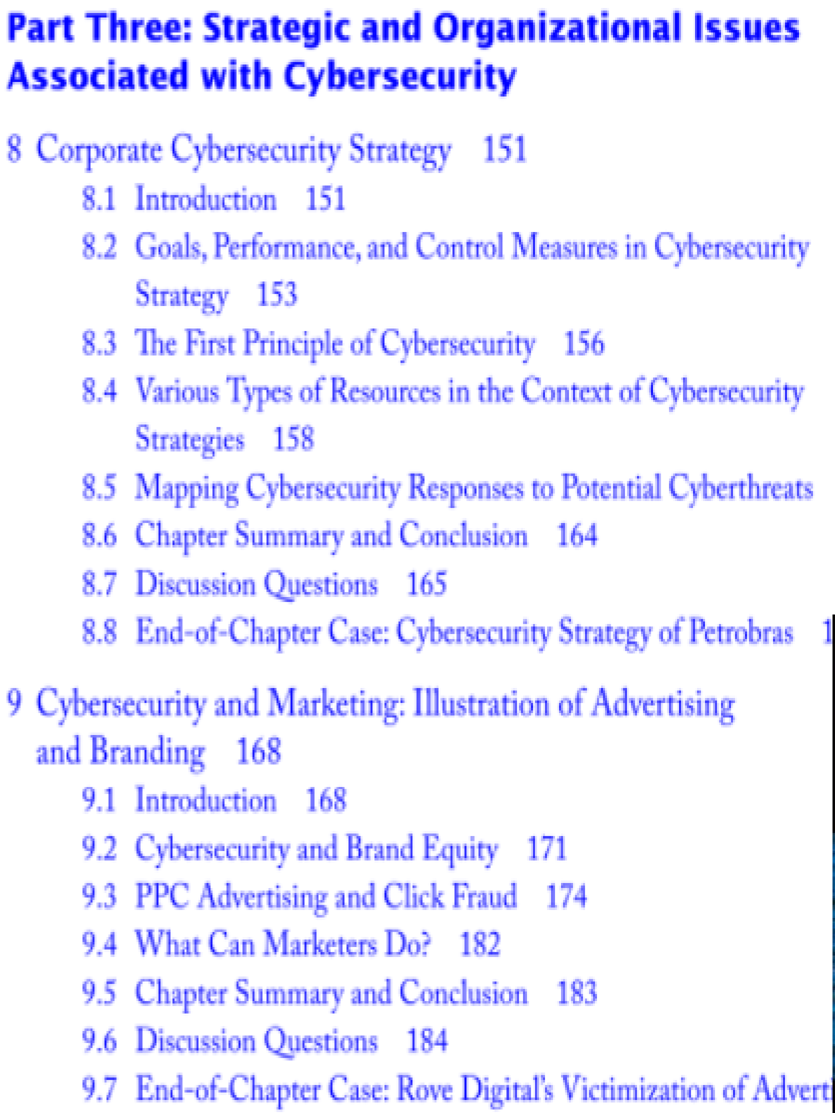
Dan Blum

Apress open

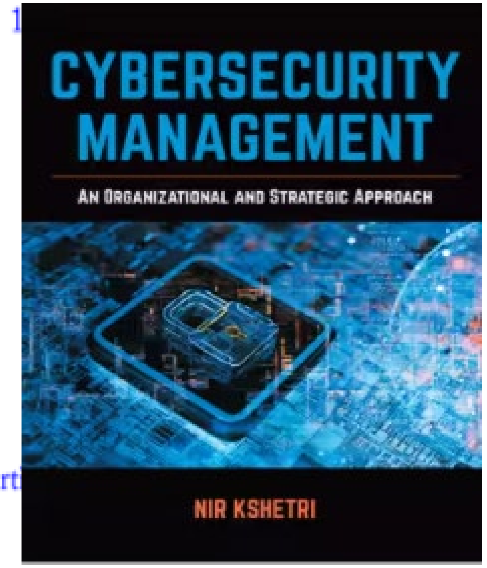
Cybersecurity Management – Nir Kshetri



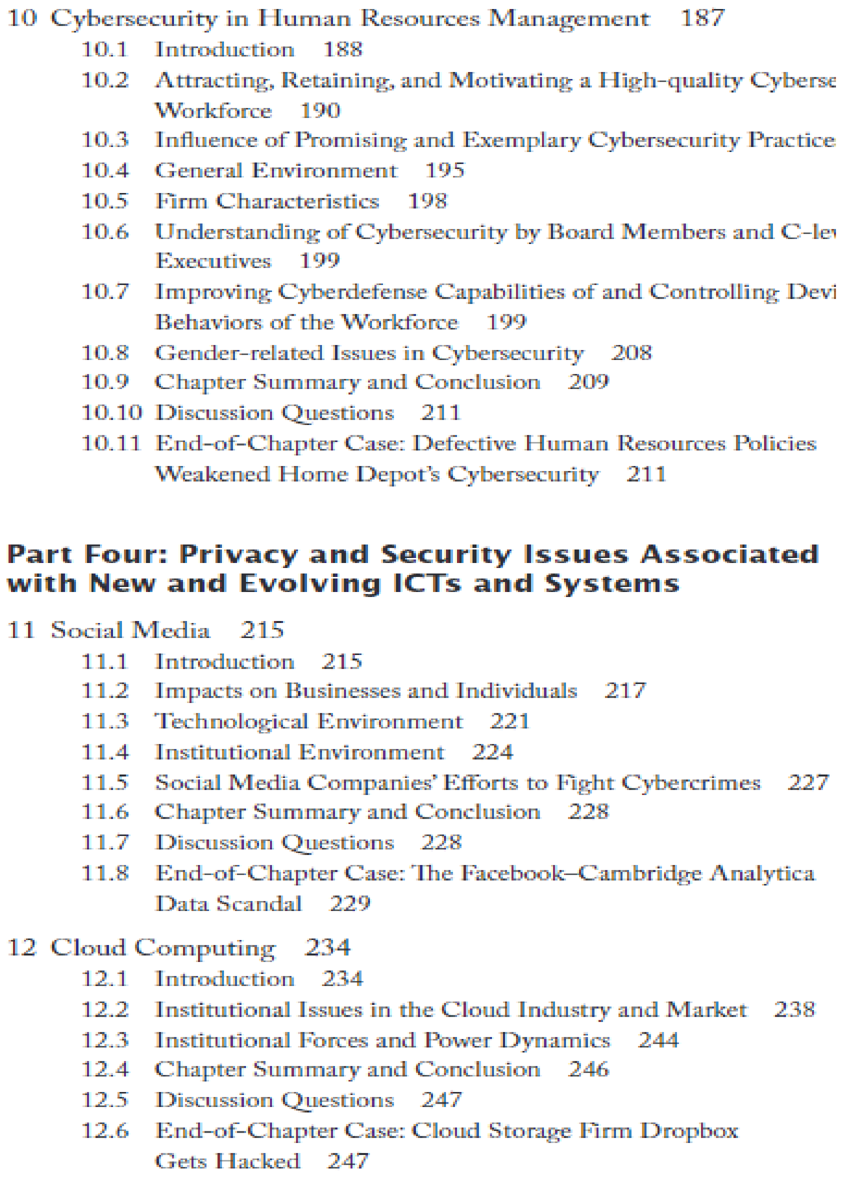
Part Two: Macro-level Factors Affecting Cybercrime and Cybersecurity



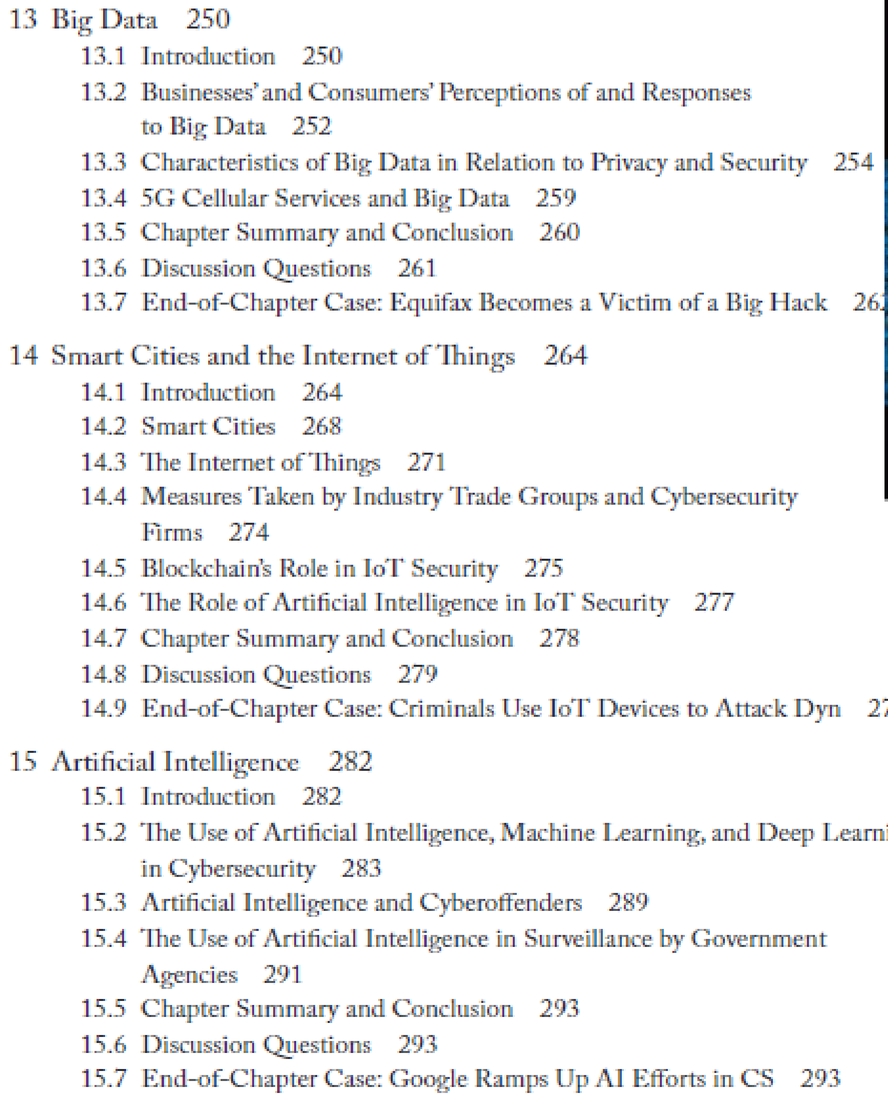
Part Three: Strategic and Organizational Issues Associated with Cybersecurity

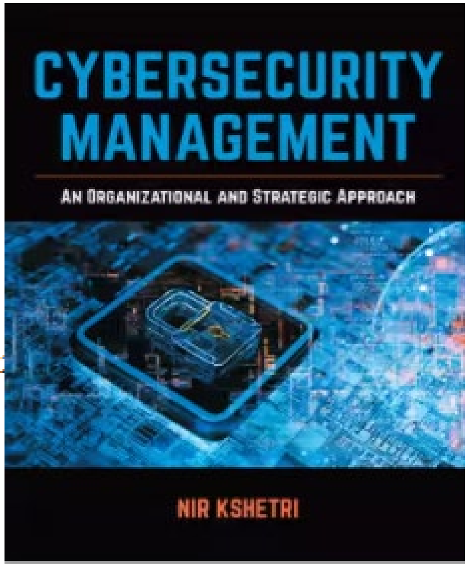


Cybersecurity Management – Nir Kshetri



Part Four: Privacy and Security Issues Associated with New and Evolving ICTs and Systems



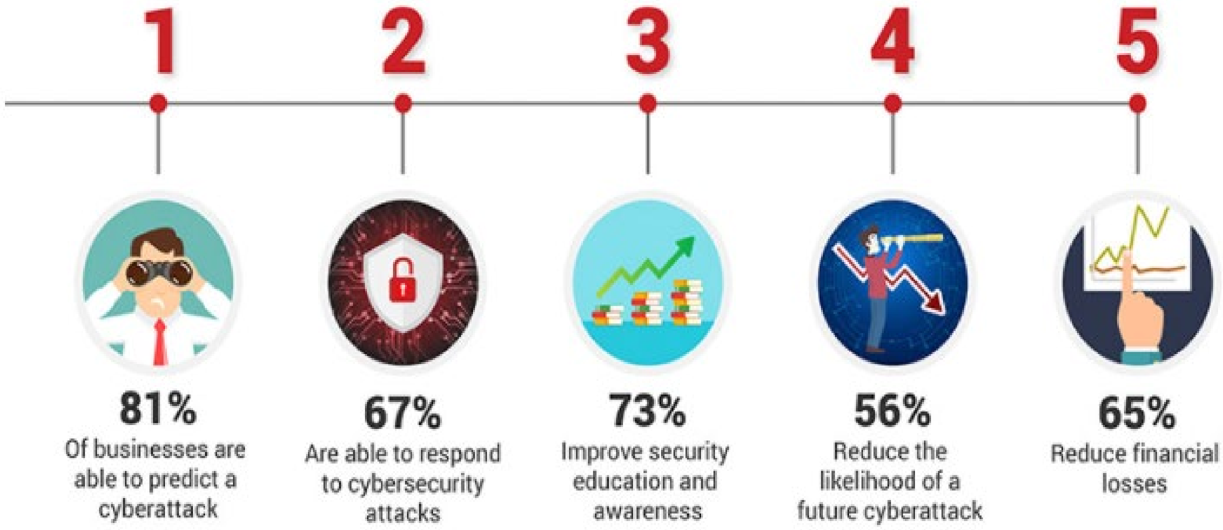


ISO 27032 Lead Cybersecurity Manager

Benefits of ISO/IEC 27032 Cybersecurity Management

Becoming a Certified ISO/IEC 27032 Cybersecurity Management enables you to:

- Protect the organization's data and privacy from cyber threats
- Strengthen your skills in the establishment and maintenance of a Cybersecurity program
- Develop best practices to managing cybersecurity policies
- Improve the security system of organization and its business continuity
- Build confidence to stakeholders for your security measures.
- Respond and recover faster in the event of an incident



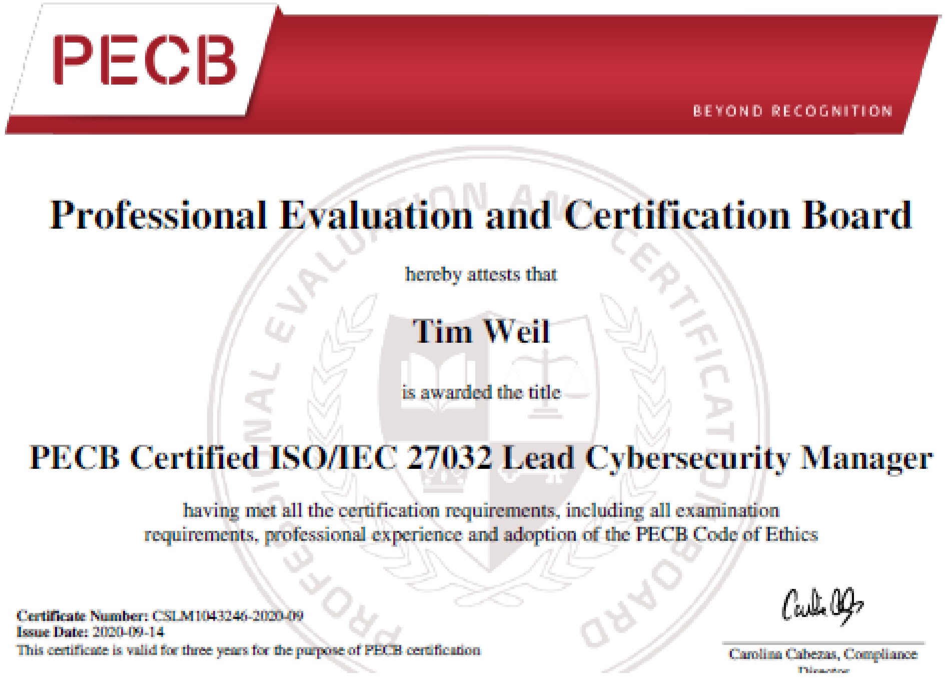
81% Of businesses are able to predict a cyberattack

67% Are able to respond to cybersecurity attacks

73% Improve security education and awareness

56% Reduce the likelihood of a future cyberattack

65% Reduce financial losses



PECB

BEYOND RECOGNITION

Professional Evaluation and Certification Board

hereby attests that

Tim Weil

is awarded the title

PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: CSLM1043246-2020-09
Issue Date: 2020-09-14
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas, Compliance Director

ISO/IEC 27032 Cybersecurity training provides a real-world solution to individuals in protecting their privacy and organization data from phishing scams, cyber-attacks, hacking, data breaches, spyware, espionage, sabotage and other cyber threats. Being certified with ISO/IEC 27032 will demonstrate to your clients and stakeholders that you can manage and provide solutions to their cyber security issues.

ISO 27032 Lead Cybersecurity Manager

Day 1 | Introduction to Cybersecurity and related concepts as recommended by ISO/IEC 27032

- Course objectives and structure
- Standards and regulatory frameworks
- Fundamental concepts in cybersecurity
- Cybersecurity program
- Initiating a cybersecurity program
- Analyzing the organization
- Leadership

Day 2 | Cybersecurity policies, risk management and attack mechanisms

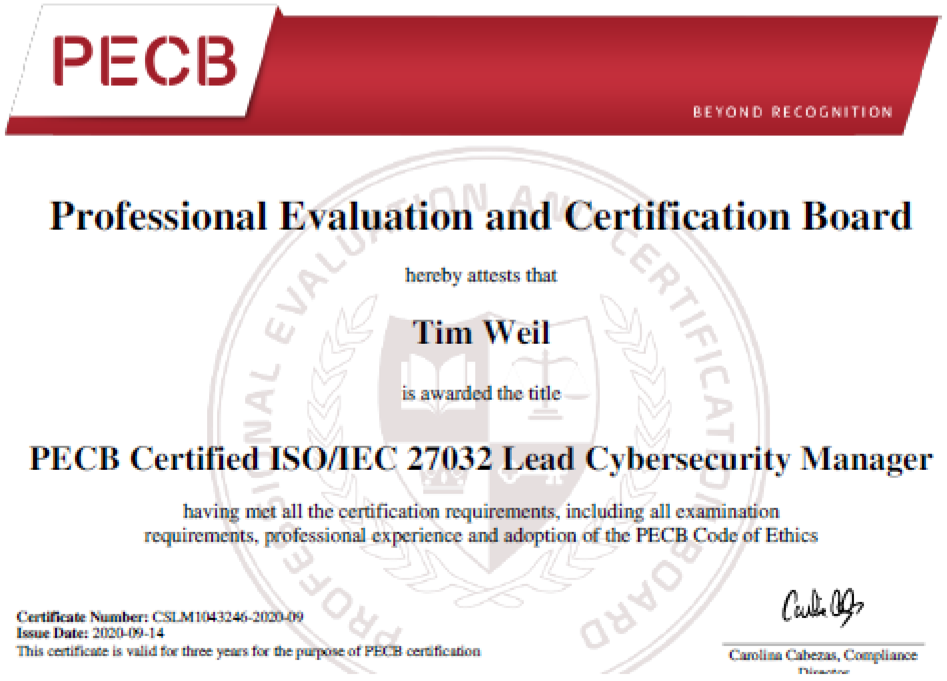
- Cybersecurity policies
- Cybersecurity risk management
- Attack mechanisms

Day 3 | Cybersecurity controls, information sharing and coordination

- Cybersecurity controls
- Information sharing and coordination
- Training and awareness program

Day 4 | Incident management, monitoring and continuous improvement

- Business continuity
- Cybersecurity incident management
- Cybersecurity incident response and recovery
- Testing in Cybersecurity
- Performance measurement
- Continuous improvement
- Closing the training



PECB

BEYOND RECOGNITION

Professional Evaluation and Certification Board

hereby attests that

Tim Weil

is awarded the title

PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: CSLM1043246-2020-09
Issue Date: 2020-09-14
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas, Compliance Director

Domain 1 | Fundamental principles and concepts of cybersecurity

Domain 2 | Roles and responsibilities of stakeholders

Domain 3 | Cybersecurity Risk Management

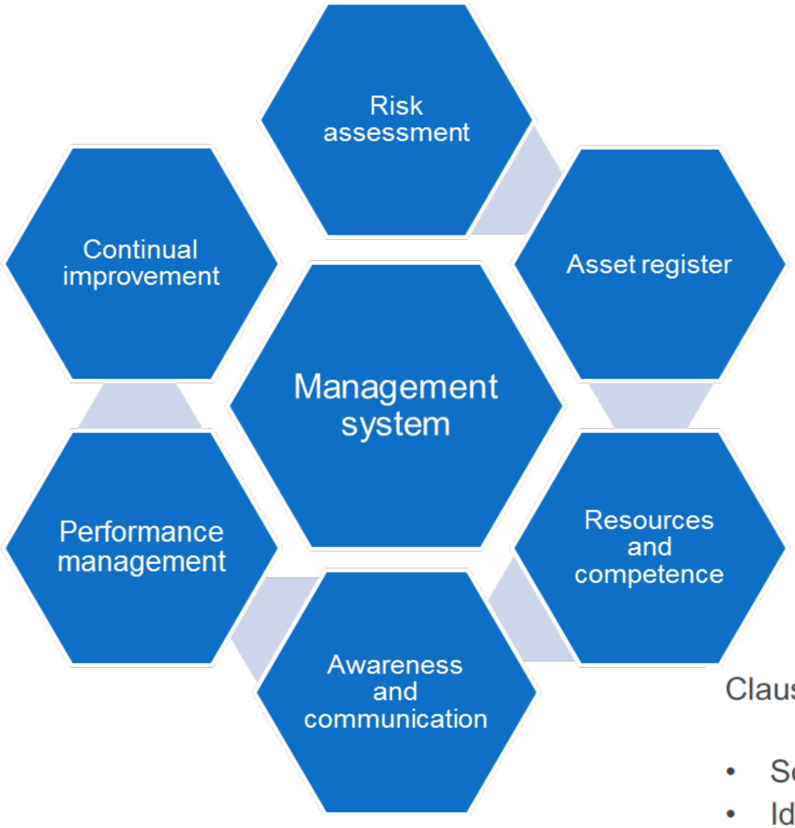
Domain 4 | Attack mechanisms and cybersecurity controls

Domain 5 | Information sharing and coordination

Domain 6 | Integrating cybersecurity program in Business Continuity Management (BCM)

Domain 7 | Cybersecurity incident management and performance measurement

The ISO/IEC 27001 standard



Clauses 4 through 10 deal with:

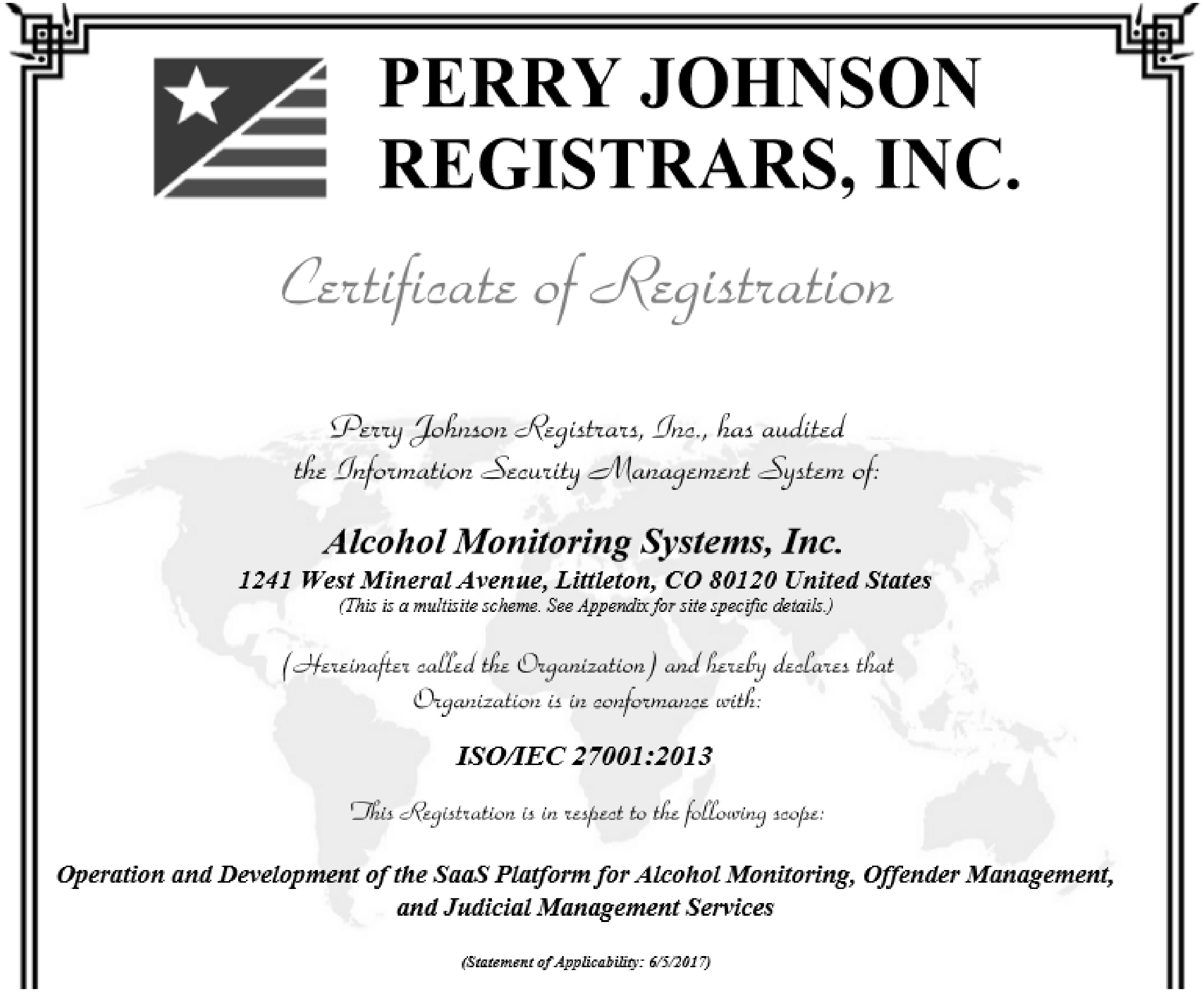
- Scoping of the ISMS
- Identifying and evaluating Risks
- Risk Treatment and mitigation
- Managing and measuring performance of the ISMS
- Tracking non-conformities and resolution
- Continuous improvement

Annex A deals with:
114 Optional controls for risk mitigation

ISO/IEC 27001 Controls

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	

Context of the Risk Assessment – AMS Products and Services – http://www.scramsystems.com



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:

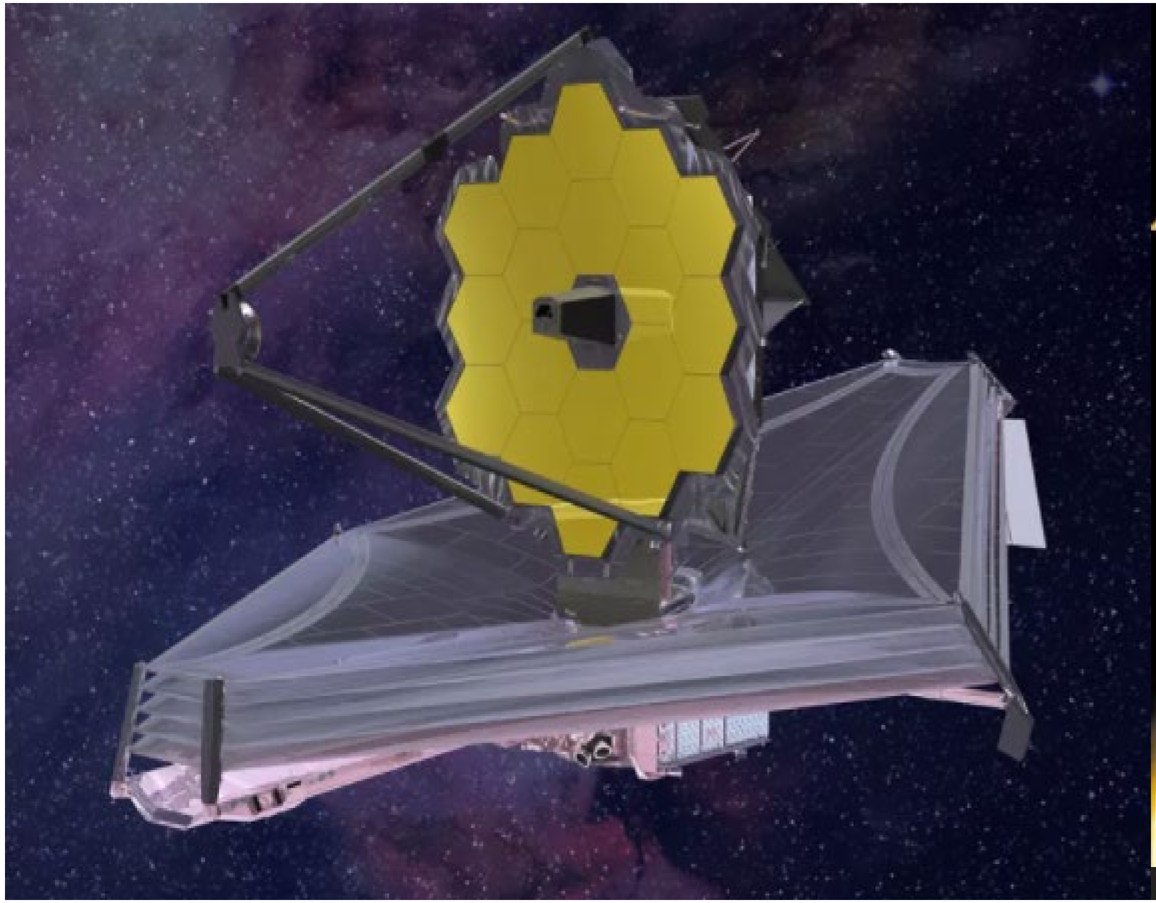
Operation and Development of the SaaS Platform for Alcohol Monitoring, Offender Management, and Judicial Management Services

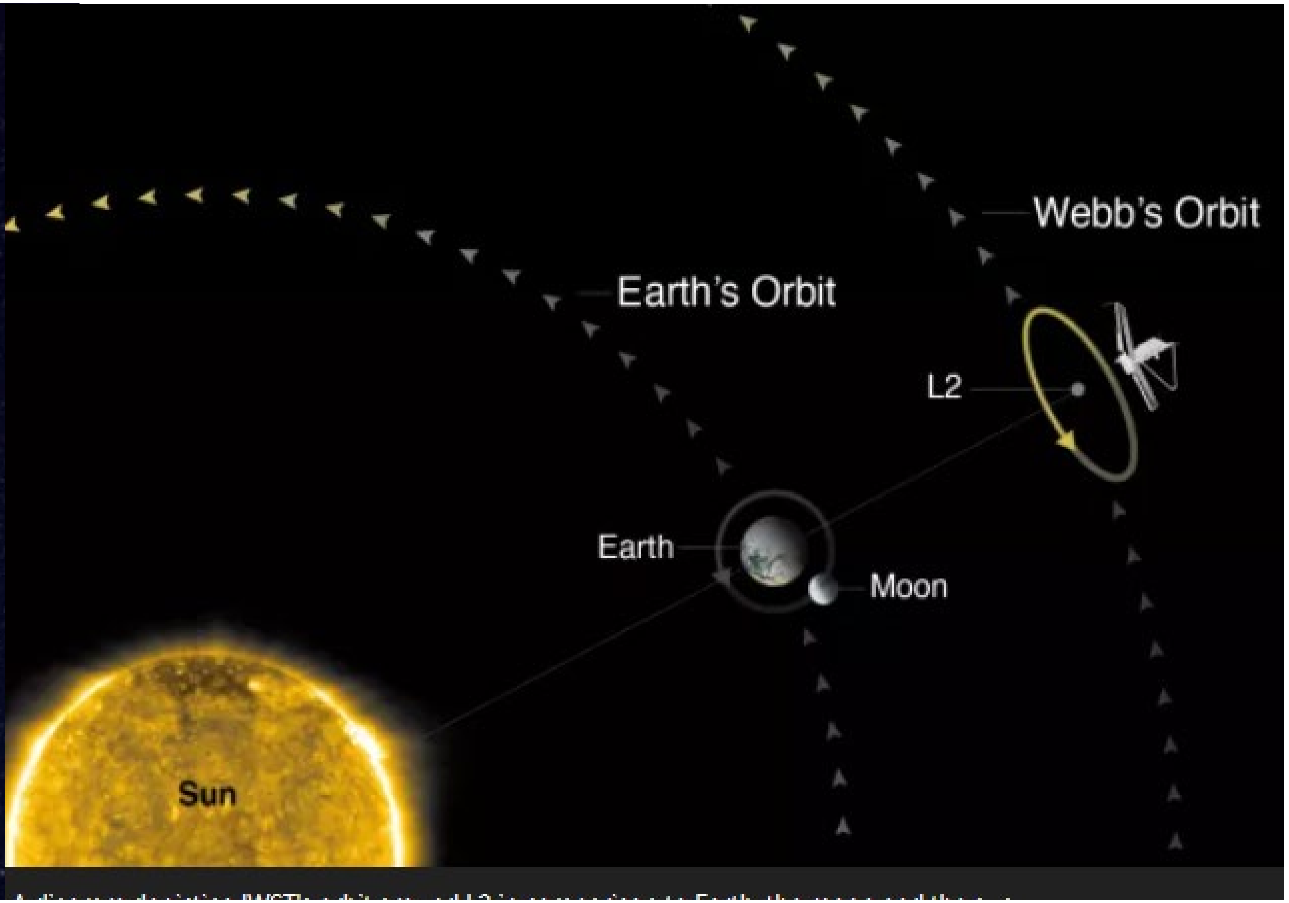
(Statement of Applicability: 6/5/2017)

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.





https://www.space.com/james-webb-space-telescope-mission-explained

How the James Webb Space Telescope works in pictures

The James Webb Space Telescope, also known as Webb or JWST, is a high-capability space observatory designed to revolutionize fields of astronomy ranging from star formation to galaxy evolution and from the very first galaxies of the universe to the properties of planetary systems. However, because JWST is a project of unprecedented complexity, the mission has struggled to launch. What had initially been proposed as a $1 billion observatory launching in 2007 has become a $10 billion project launching in 2021.

You don’t need a weatherman to tell which way the wind blows.

Table of Contents

- Cyberspace – Our Point of Departure
- Information Security Management Models
- Frameworks for Risk Management
- COVID Smackdown – NIST CSF vs Big Scary Monsters
- Emerging Roads Maps to Risk Management
- References + Q&A

Books Cited in this Presentation

Rational Cybersecurity for Business by Dan Blum, 2020 | 1st ed.Apress (Verlag), 978-1-4842-5951-1 (ISBN) .https://link.springer.com/content/pdf/10.1007%2F978-1-4842-5952-8.pdf

Cybersecurity Management by Nir Kshetri, Kshetri, Nir. *Cybersecurity Management: An Organizational and Strategic Approach*, University of Toronto Press. https://www.book2look.com/book/9781487523626

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

- IT Pro Special Issue on Communications Recovery and Resilience - Editor's Column" by Tim Weil, Bhuvan Unhelkar, John Callahan, Jason W. Rupe, Keith Sherringham Recovery and resilience are two sides worth exploring here: 1) the needs and challenges with recovering from disasters of all types, and 2) how to enhance the resiliency of communication networks to provide better support in these difficult operations https://doi.org/10.1109/MITP.2020.3031443 https://www.computer.org/csdl/magazine/it/2020/06/09250314/1oxkJTuIsMg

- 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

- T. Weil, R. Kuhn, M. Chang https://www.securityfeeds.us/cyberthreats-and-security-ieee-it-professional-special-issue

- 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-shape-reality-post-covid-19

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

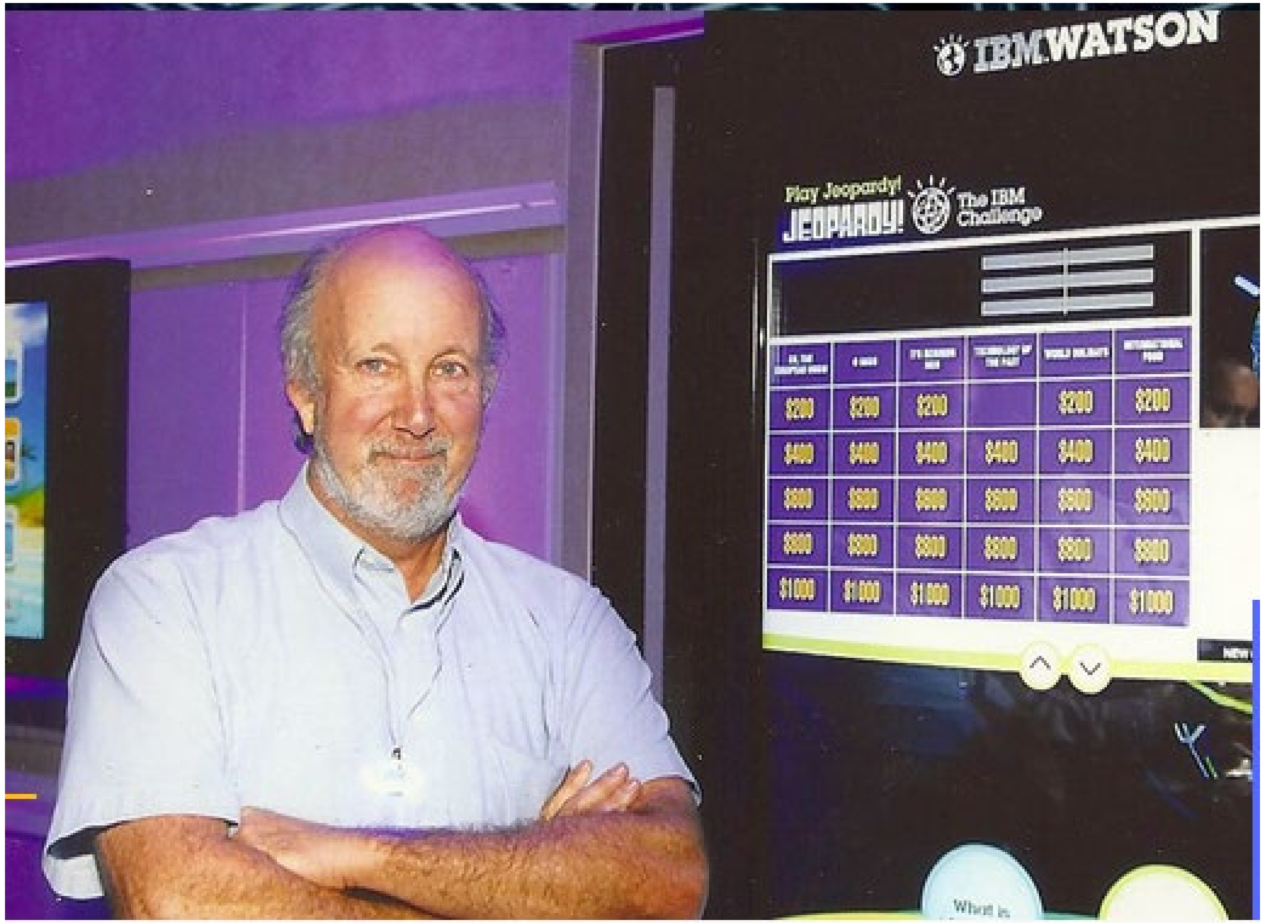
- NIST Cybersecurity Framework (CSF) [Online]: http://www.nist.gov/cyberframework

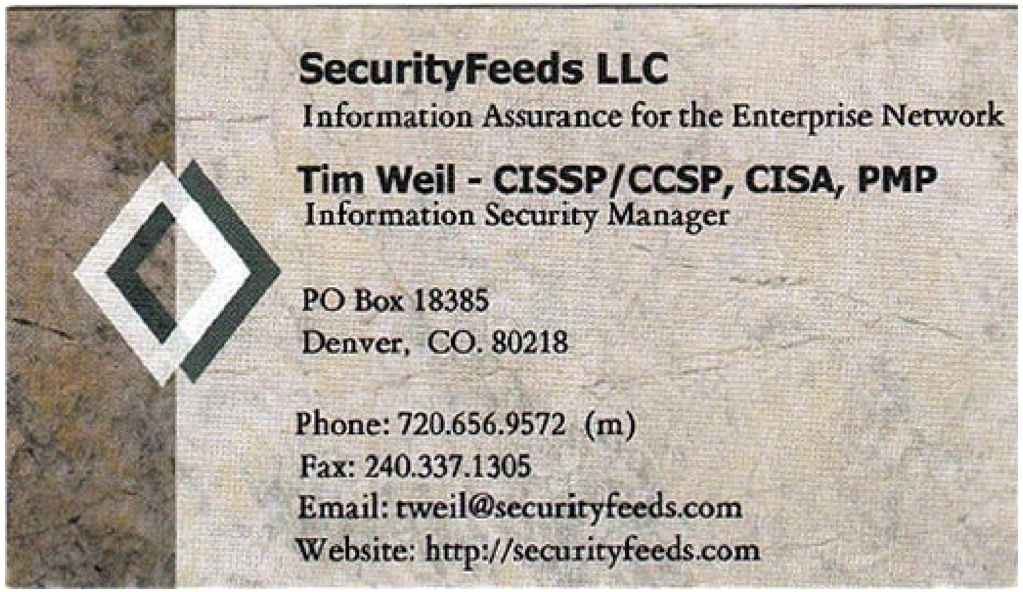
- “CISA INSIGHTS:TRUSTED INTERNET CONNECTIONS 3.0 INTERIM TELEWORK GUIDANCE: https://www.cisa.gov/publication/tic-30-interim-telework-guidance

- “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

ICT - Science & Engineering Journalism – 1984 - 2020

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