Cyberthreat, Cybersecurity and Cyber Compliance in Clinical Research & Healthcare: One Size Fits None

Eric Perakslis PhD
Chief Science & Digital Officer
Duke Clinical Research Institute
Professor
Department of Population Health Sciences
& Chief Technology Strategist
Duke University School of Medicine
Twitter: @eperakslis

MEDECINS SANS FRONTIERES DOCTORS WITHOUT BORDERS · Celebrating 30 Years KidneyCancerAssociation Unstoppable Together. · HumanFirst · HARVARD MEDICAL SCHOOL DEPARTMENT OF Biomedical Informatics · IMIDomics · J&J Johnson & Johnson · Bristol Myers Squibb

Learning objectives

1. Gain an understanding of cyber philosophy, landscape and definitions
2. Understand current level, complexity and diversity of cyber threat
3. Understand the differences between privacy, security and compliance
4. Understand how to determine research boundaries for security characterization
5. Understand the basics of a framework for discussing cyber benefit-risk
6. Determine how many on NIH Collaboratory believe Die Hard is a Christmas movie

The terms Asymmetrical Warfare or Asymmetrical Threats can be summarized simply as the asymmetry that exists between two adversaries and the tactics used by the weaker adversary to render the strengths of the stronger adversary moot.

*Failure of imagination, unknown unknowns & black swans

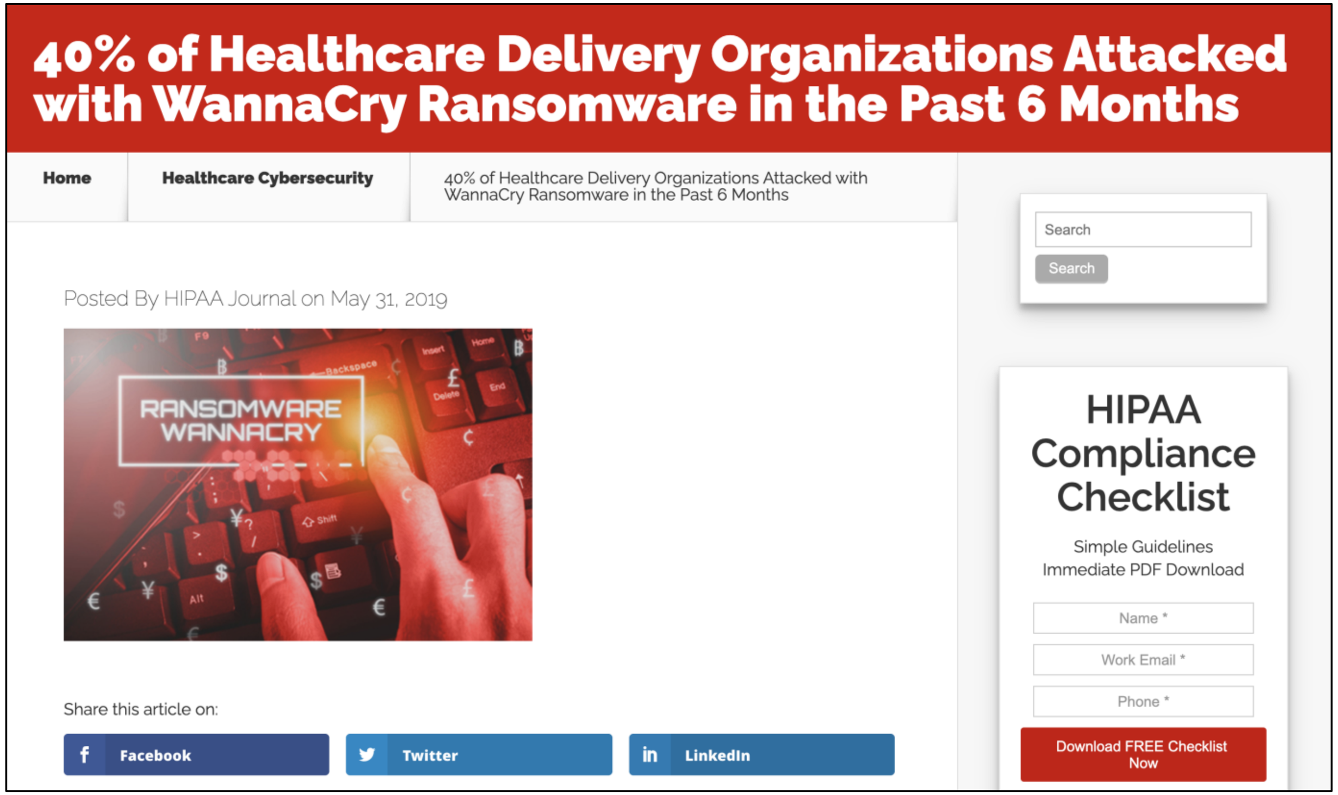
Arthur C Clark – '*To predict the future we need logic, but we also need faith and imagination, which can sometimes defy logic itself*'.   There are two types of failures of imagination, '*a failure of nerve and the failure to admit the possibility of the existence of vital facts*'.

Donald Rumsfeld in the wake of 9/11 – *'…as we know, there are known knowns, there are things we know that we know. We also know there are known unknowns, that is to say that we know there are some things we don't know. But there are also unknown unknowns…and these tend to be the difficult ones.'*

Nassim Taleb following the financial crisis of 2008 – popularized the phrase 'Black Swan' to describe unforeseen (no, low probability events) having such disproportionally large impact that they must be mitigated against and vigilantly monitored.

Whether we call these risks failure of imagination, black swans or unknown unknowns, the potential human Impact of widespread adverse events or the disruption of care is an intolerable risk that must be accounted for across all risk spaces (cyber, physical supply chain, vital infrastructure etc.,) all the while as we adopt technology breakthroughs.

*https://www.amazon.com/Digital-Health-Understanding-Benefit-Risk-Patient-Provider/dp/0197503144/ref=sr_1_1?keywords=perakslis&qid=1639138011&sr=8-1



40% of Healthcare Delivery Organizations Attacked with WannaCry Ransomware in the Past 6 Months

Home
Healthcare Cybersecurity
40% of Healthcare Delivery Organizations Attacked with WannaCry Ransomware in the Past 6 Months
Search
Search

Posted By HIPAA Journal on May 31, 2019

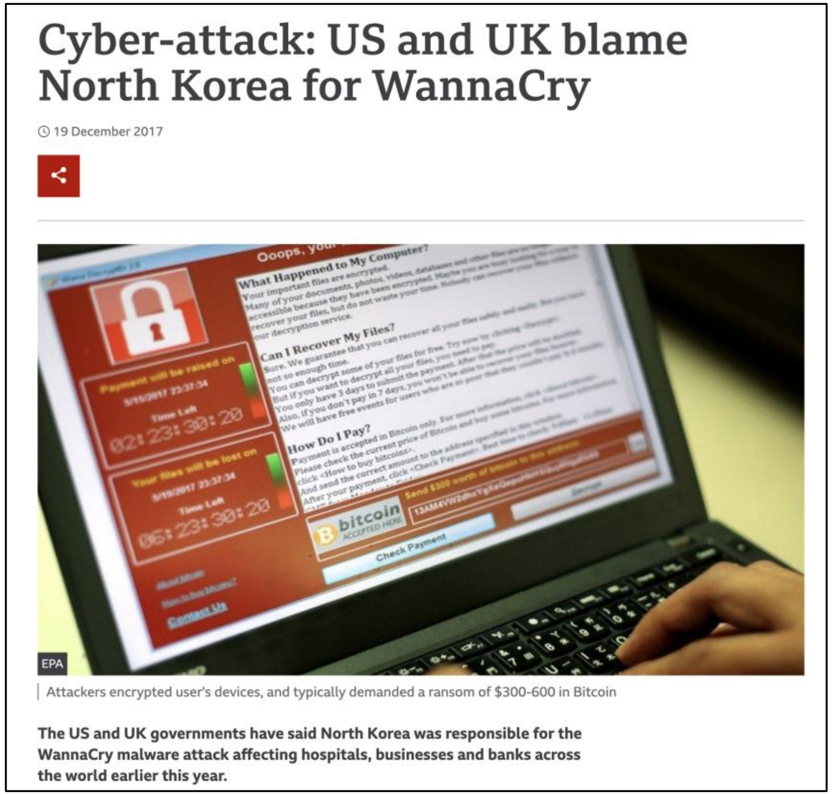
Share this article on:

Facebook
Twitter
LinkedIn

HIPAA Compliance Checklist

Simple Guidelines
Immediate PDF Download

Name *
Work Email *
Phone *
Download FREE Checklist Now

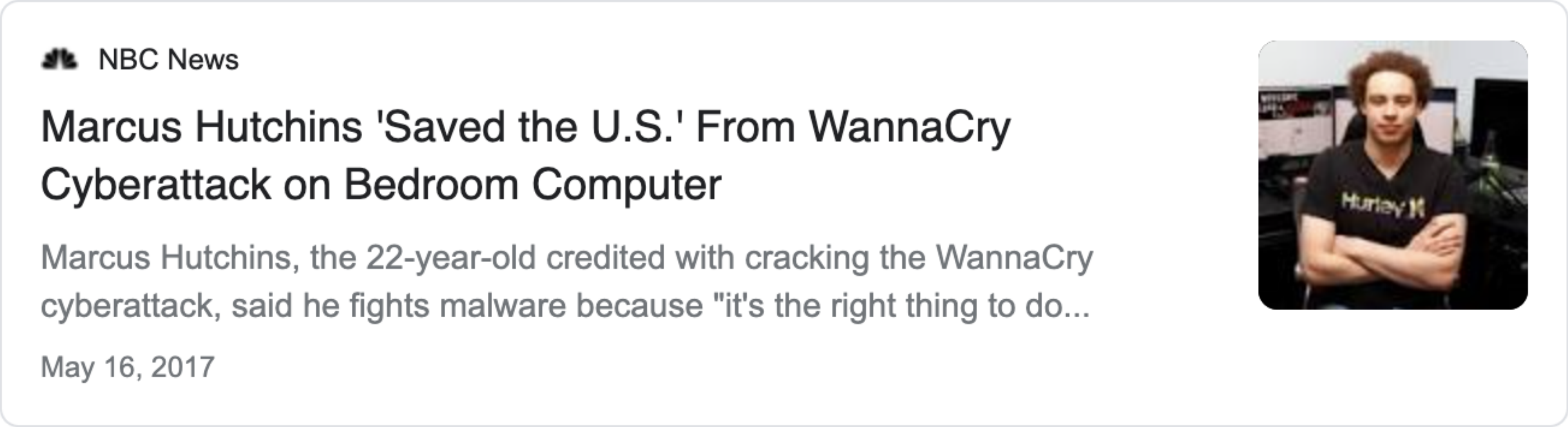


Cyber-attack: US and UK blame North Korea for WannaCry

19 December 2017

Attackers encrypted user's devices, and typically demanded a ransom of $300-600 in Bitcoin

The US and UK governments have said North Korea was responsible for the WannaCry malware attack affecting hospitals, businesses and banks across the world earlier this year.



NBC News

Marcus Hutchins 'Saved the U.S.' From WannaCry Cyberattack on Bedroom Computer

Marcus Hutchins, the 22-year-old credited with cracking the WannaCry cyberattack, said he fights malware because "it's the right thing to do...

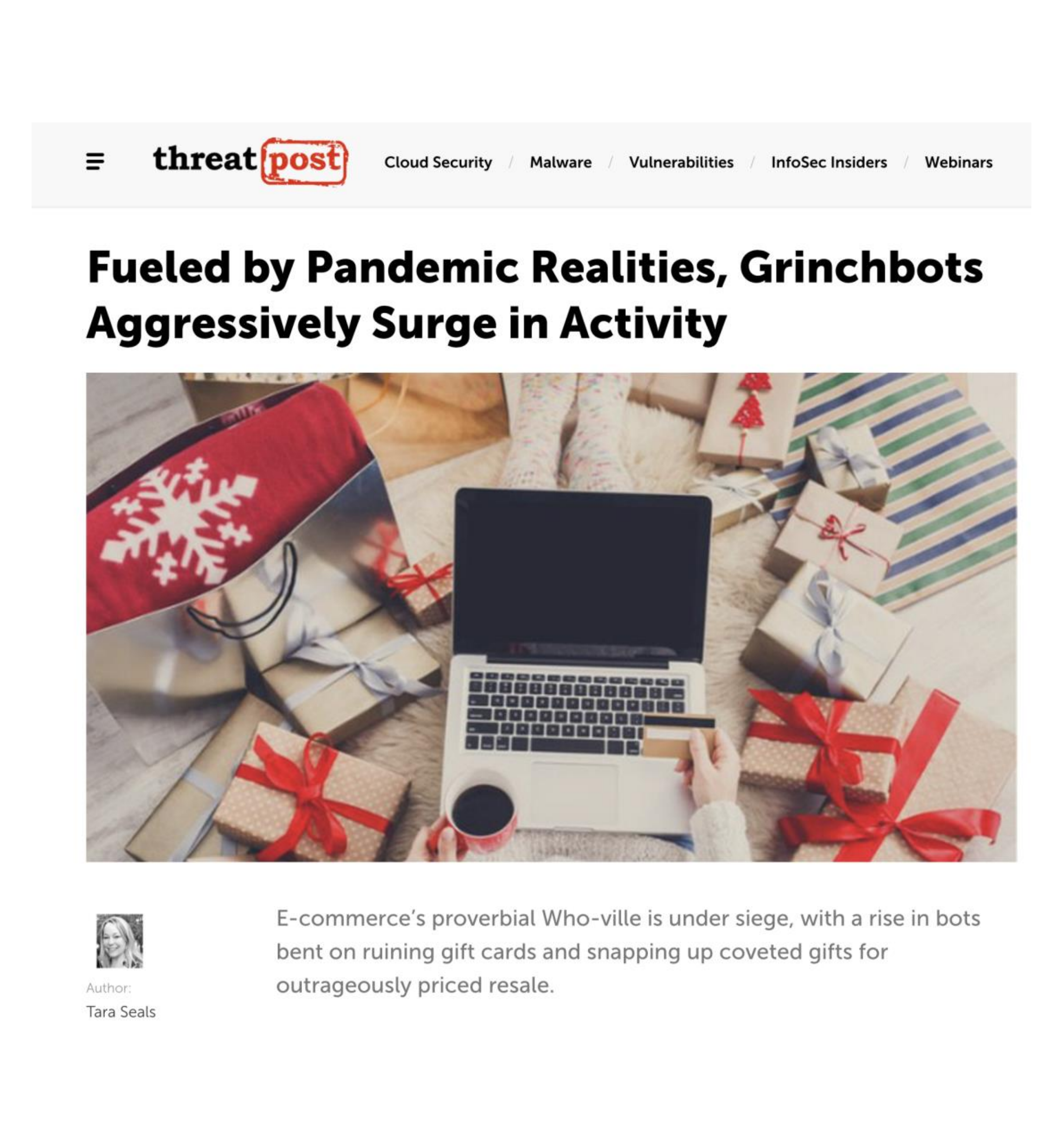
May 16, 2017

Cyberthreat by the Numbers

Statistic (USA)	Value	Reference
Hospitalizations in 2021	36,241,815	American Hospital Association
Compromised Medical Records	40,099,751	Healthcare IT News
% Breaches Business Associate Driven	52%	Critical Insight
Average Time to Recover	236 days	Fierce Healthcare
Medicare Estimated Improper Payments	$25.74 billion	CMS
Highest Grossing Drug - Humira	$19.8 billion	Becker’s Hospital Review
# New Malicious Programs Daily	350,000	DataProt

Types of Cyberthreat – Gamified Crime

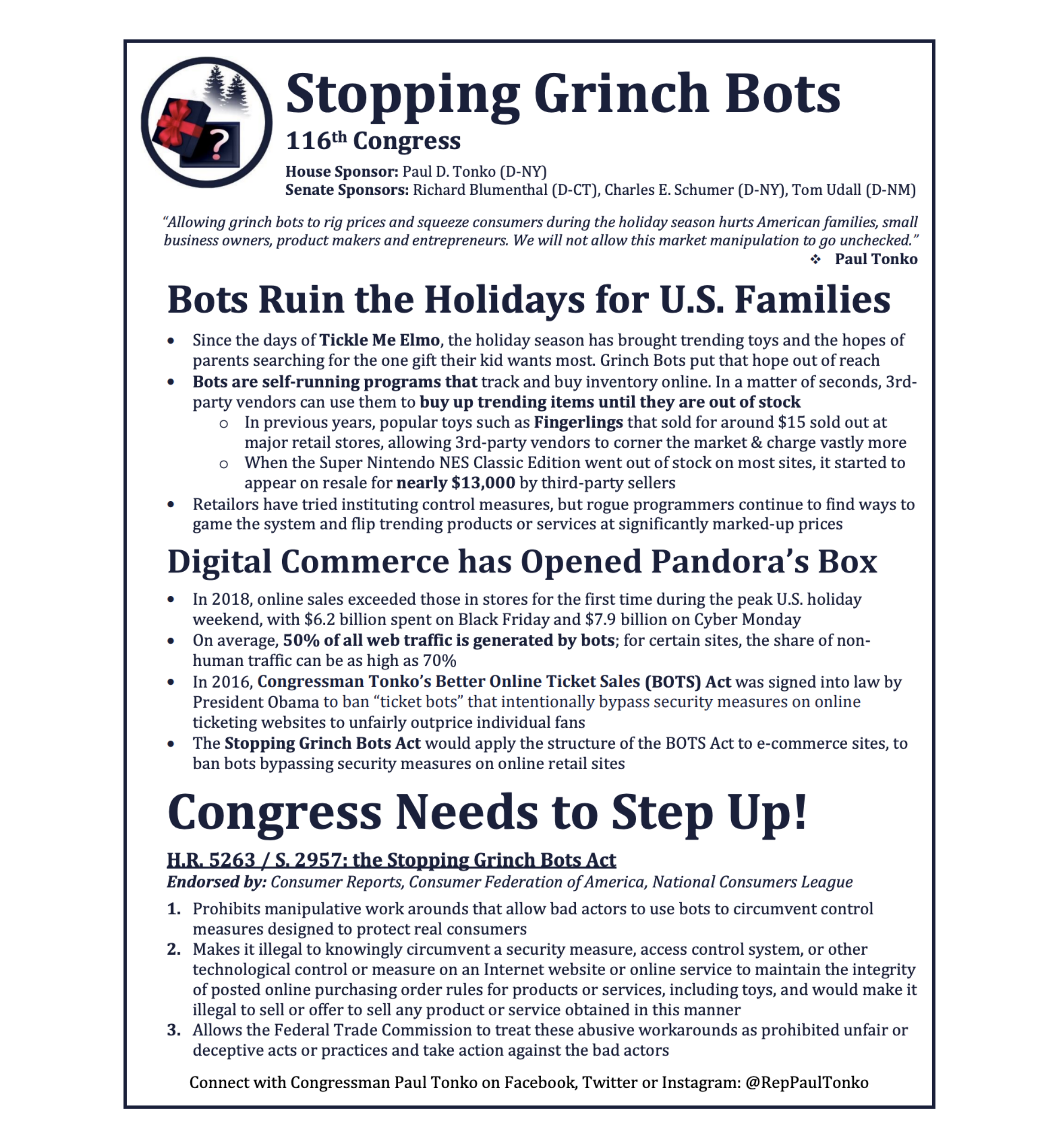
Threat	Description	Example
Ransomware	type of malware that denies legitimate users access to their system and requires a payment, or ransom, to regain access	Meet the ransomware gang behind 235 attacks on US hospitals
Malware	any program or code that is created with the intent to do harm to a computer, network or server	Hospital ransomware attack led to infant's death, lawsuit alleges
MaaS	In a Malware-as-a-service model, hackers are hired to conduct ransomware attacks on behalf of a third-party	The destructive rise of ransomware as a service
DOS & DDOS	a malicious, targeted attack that floods a network with false requests in order to disrupt business operations	Six lessons from Boston Children's Hospital "Hacktivist' attack
Phishing	uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information or to download malware	Hospitals said to tighten email security in response to CEO spear phishing attempts
MITM	Man-in-the-Middle attack, when a malicious actor eavesdrops on a conversation between a network user and a web application	MITM attacks on healthcare
XSS	Cross-site scripting is a code injection attack in which an adversary inserts malicious code within a legitimate website	Healthcare hit by 187 million monthly web attacks in 2020
SQL Injections	Hackers use SQL Injection techniques to alter, steal or erase data. XSS is client-side while SQL injection is server side	Philips Tasy EMR healthcare infomatics solution vulnerable to SQL injection
DNS Tunneling	leverages domain name system (DNS) queries & responses to bypass traditional security measures & transmit data and code within the network	HHS Cybersecurity Program
PWD Attack	any cyberattack wherein a hacker attempts to steal a user's password	Healthcare's Password Problem



Fueled by Pandemic Realities, Grinchbots Aggressively Surge in Activity

Author:
Tara Seals

E-commerce's proverbial Who-ville is under siege, with a rise in bots bent on ruining gift cards and snapping up coveted gifts for outrageously priced resale.



Stopping Grinch Bots

116th Congress

House Sponsor: Paul D. Tonko (D-NY)
Senate Sponsors: Richard Blumenthal (D-CT), Charles E. Schumer (D-NY), Tom Udall (D-NM)

"Allowing grinch bots to rig prices and squeeze consumers during the holiday season hurts American families, small business owners, product makers and entrepreneurs. We will not allow this market manipulation to go unchecked."
❖ **Paul Tonko**

Bots Ruin the Holidays for U.S. Families

- Since the days of **Tickle Me Elmo**, the holiday season has brought trending toys and the hopes of parents searching for the one gift their kid wants most. Grinch Bots put that hope out of reach
- **Bots are self-running programs that** track and buy inventory online. In a matter of seconds, 3rd-party vendors can use them to **buy up trending items until they are out of stock**
  - In previous years, popular toys such as **Fingerlings** that sold for around $15 sold out at major retail stores, allowing 3rd-party vendors to corner the market & charge vastly more
  - When the Super Nintendo NES Classic Edition went out of stock on most sites, it started to appear on resale for **nearly $13,000** by third-party sellers
- Retailers have tried instituting control measures, but rogue programmers continue to find ways to game the system and flip trending products or services at significantly marked-up prices

Digital Commerce has Opened Pandora's Box

- In 2018, online sales exceeded those in stores for the first time during the peak U.S. holiday weekend, with $6.2 billion spent on Black Friday and $7.9 billion on Cyber Monday
- On average, **50% of all web traffic is generated by bots**; for certain sites, the share of non-human traffic can be as high as 70%
- In 2016, **Congressman Tonko's Better Online Ticket Sales (BOTS) Act** was signed into law by President Obama to ban "ticket bots" that intentionally bypass security measures on online ticketing websites to unfairly outprice individual fans
- The **Stopping Grinch Bots Act** would apply the structure of the BOTS Act to e-commerce sites, to ban bots bypassing security measures on online retail sites

Congress Needs to Step Up!

H.R. 5263 / S. 2957: the Stopping Grinch Bots Act
Endorsed by: *Consumer Reports, Consumer Federation of America, National Consumers League*

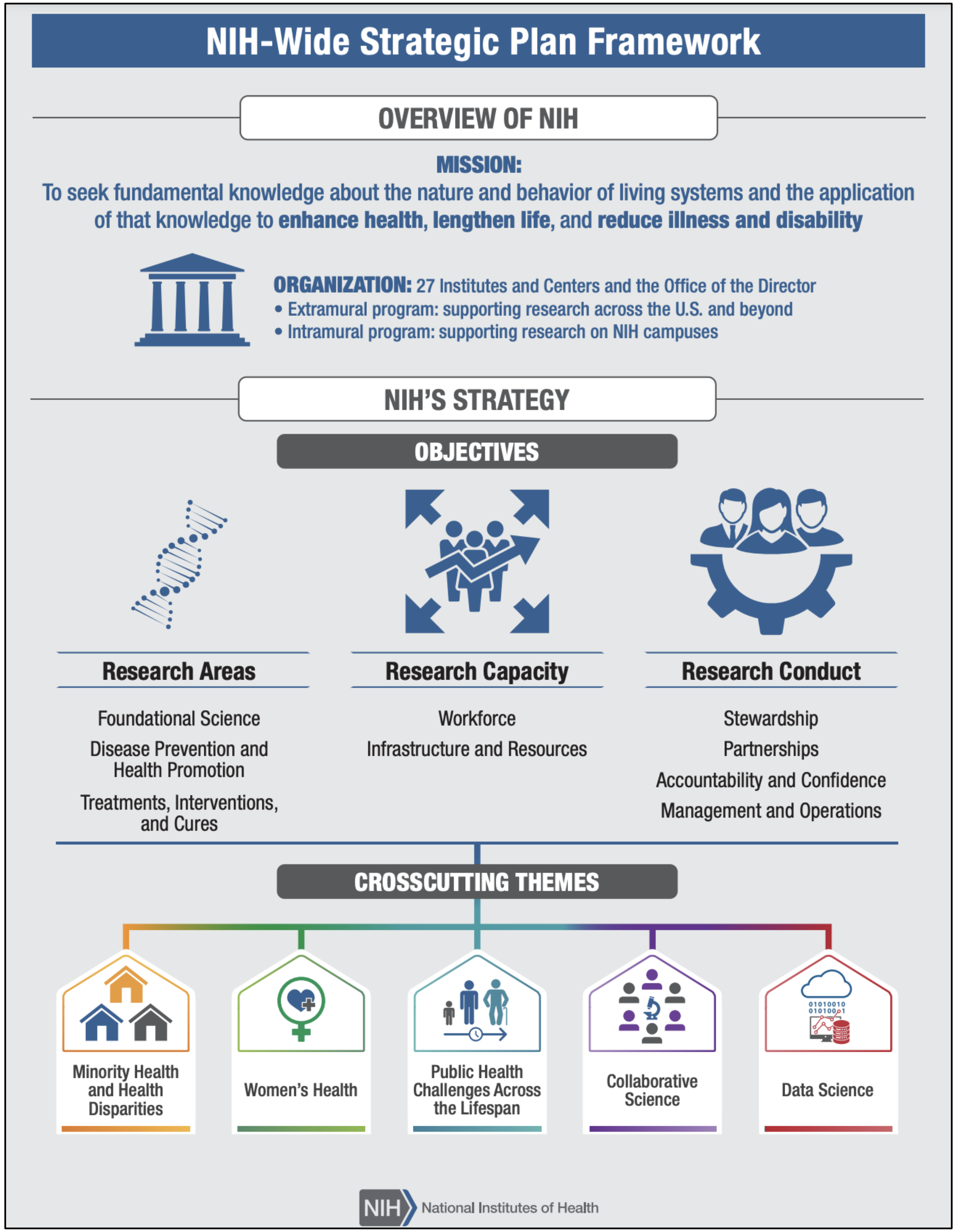
1. Prohibits manipulative work arounds that allow bad actors to use bots to circumvent control measures designed to protect real consumers
2. Makes it illegal to knowingly circumvent a security measure, access control system, or other technological control or measure on an Internet website or online service to maintain the integrity of posted online purchasing order rules for products or services, including toys, and would make it illegal to sell or offer to sell any product or service obtained in this manner
3. Allows the Federal Trade Commission to treat these abusive workarounds as prohibited unfair or deceptive acts or practices and take action against the bad actors

Connect with Congressman Paul Tonko on Facebook, Twitter or Instagram: @RepPaulTonko

If what you are doing is valuable, then someone is trying to steal it.

“I am an exceptional thief, Mrs. McClane, and since I'm moving up to kidnapping, you should be more polite…”.

What are our most common research priorities?



NIH-Wide Strategic Plan Framework

OVERVIEW OF NIH

MISSION:

To seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to **enhance health**, **lengthen life**, and **reduce illness and disability**

ORGANIZATION: 27 Institutes and Centers and the Office of the Director

- Extramural program: supporting research across the U.S. and beyond
- Intramural program: supporting research on NIH campuses

NIH'S STRATEGY

OBJECTIVES

Research Areas

Foundational Science

Disease Prevention and Health Promotion

Treatments, Interventions, and Cures

Research Capacity

Workforce

Infrastructure and Resources

Research Conduct

Stewardship

Partnerships

Accountability and Confidence

Management and Operations

CROSSCUTTING THEMES

Minority Health and Health Disparities

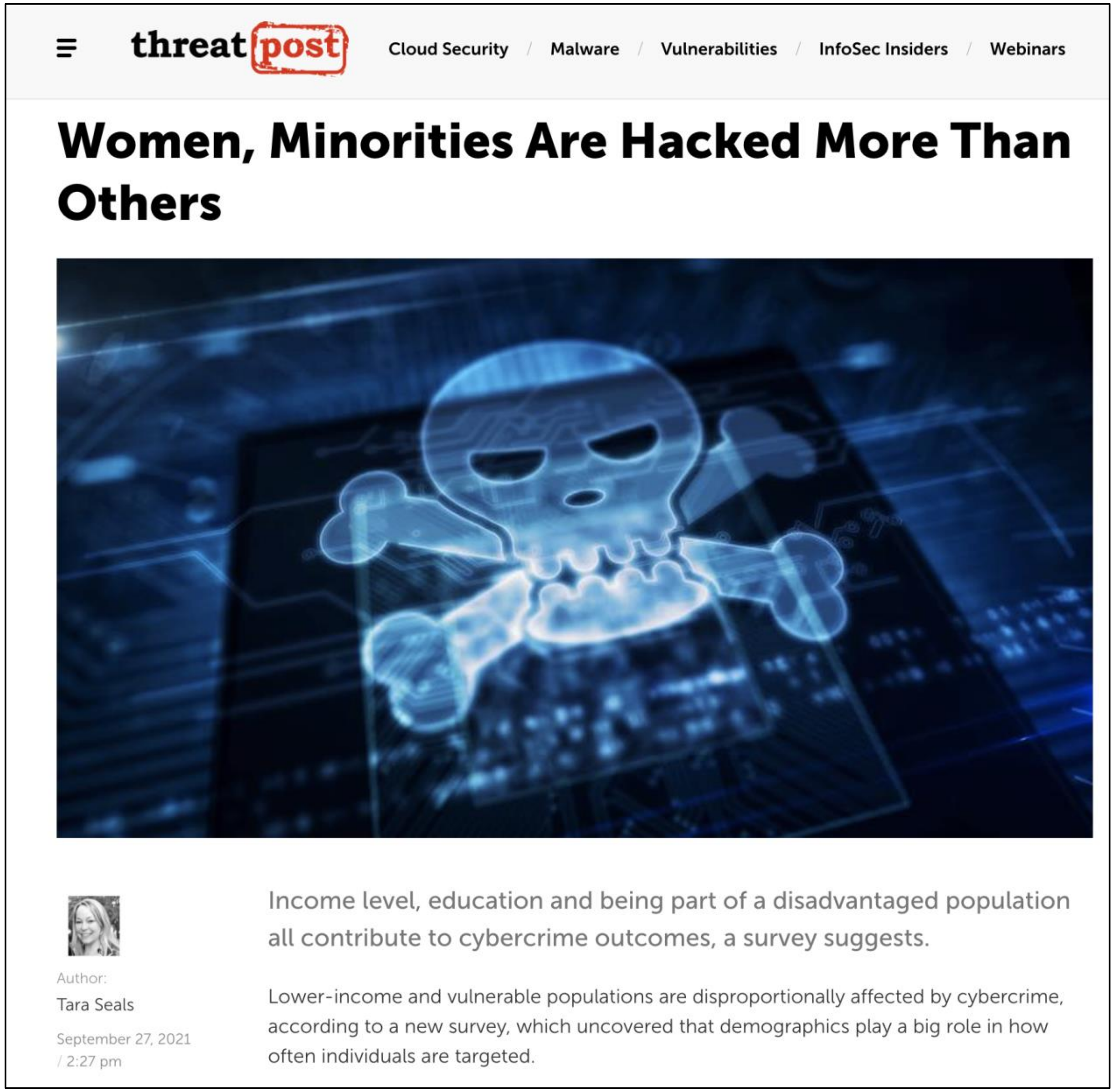
Women's Health

Public Health Challenges Across the Lifespan

Collaborative Science

Data Science

NIH National Institutes of Health


threatpost
Cloud Security / Malware / Vulnerabilities / InfoSec Insiders / Webinars

Women, Minorities Are Hacked More Than Others

Author:
Tara Seals

September 27, 2021
/ 2:27 pm

Income level, education and being part of a disadvantaged population all contribute to cybercrime outcomes, a survey suggests.

Lower-income and vulnerable populations are disproportionally affected by cybercrime, according to a new survey, which uncovered that demographics play a big role in how often individuals are targeted.

- Women receive text messages from unknown numbers that include potentially malicious links than men

- Black people, indigenous people and people of color (BIPOC) have their social-media accounts attacked more often than white people do

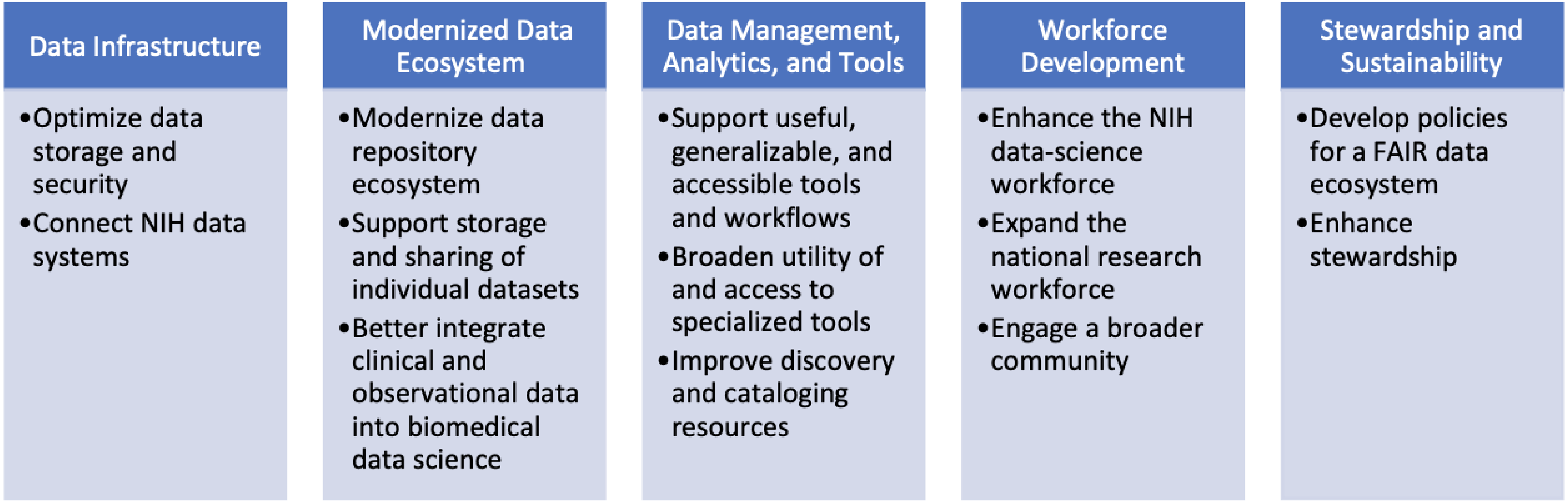
- BIPOC populations also face identity theft more often

- People aged 65 years or older account for 36 percent of credit-card information theft occurrences

- Individuals with a higher income feel safer online than individuals with a lower income

- Users who have the highest level of education feel more secure

‘It should be said that none of the respondents were successful in completely avoiding suspicious online activity, no matter their gender, race, age, income or education level.’

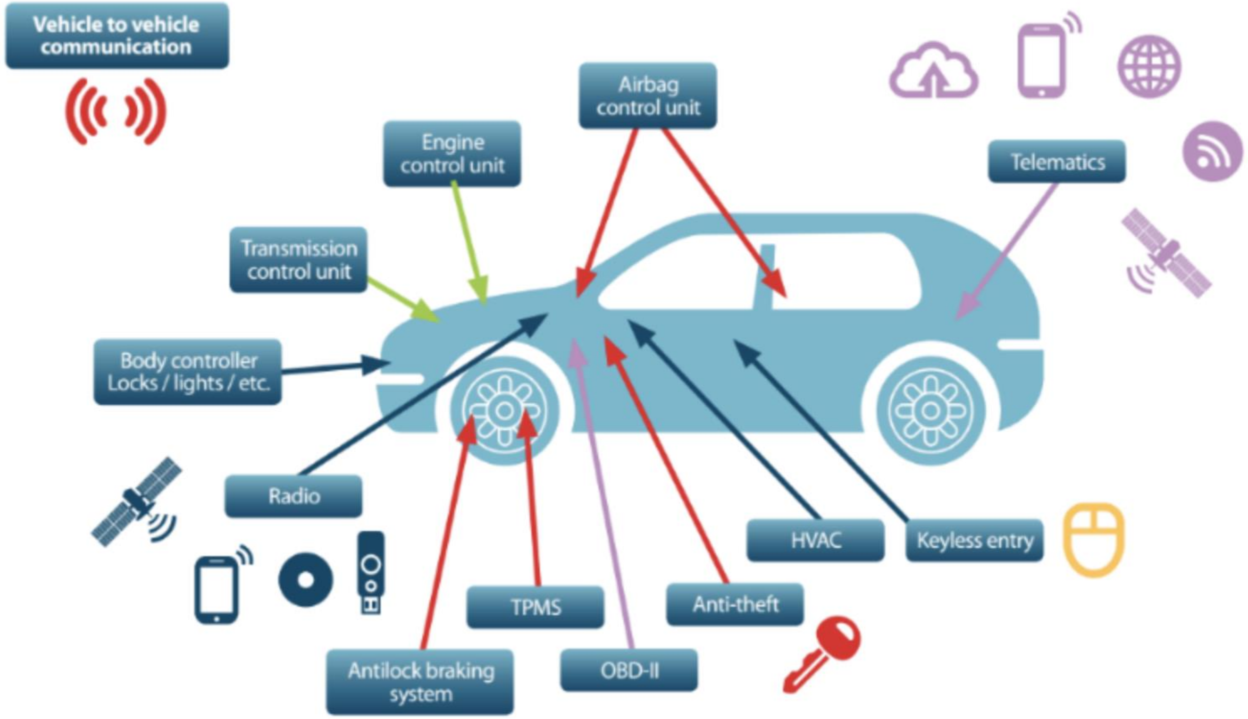


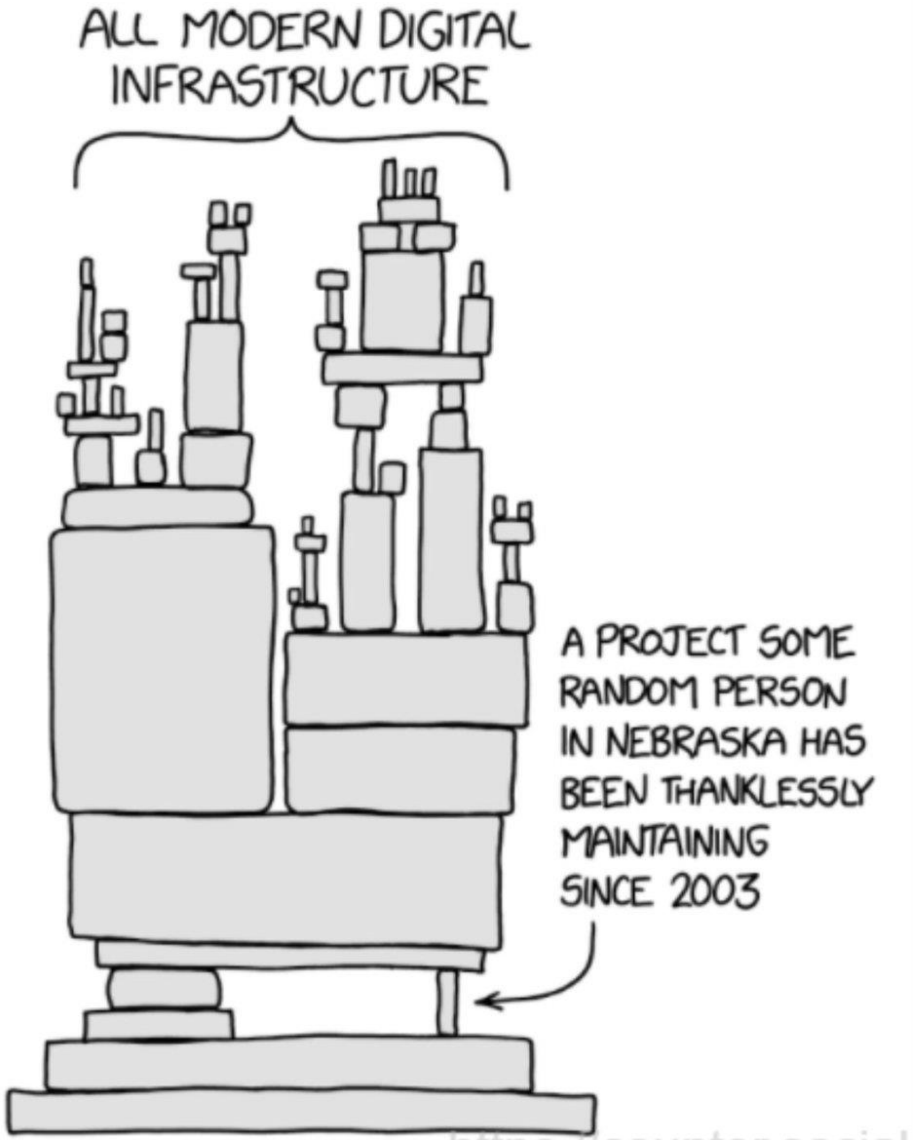
Data Infrastructure	Modernized Data Ecosystem	Data Management, Analytics, and Tools	Workforce Development	Stewardship and Sustainability
• Optimize data storage and security • Connect NIH data systems	• Modernize data repository ecosystem • Support storage and sharing of individual datasets • Better integrate clinical and observational data into biomedical data science	• Support useful, generalizable, and accessible tools and workflows • Broaden utility of and access to specialized tools • Improve discovery and cataloging resources	• Enhance the NIH data-science workforce • Expand the national research workforce • Engage a broader community	• Develop policies for a FAIR data ecosystem • Enhance stewardship

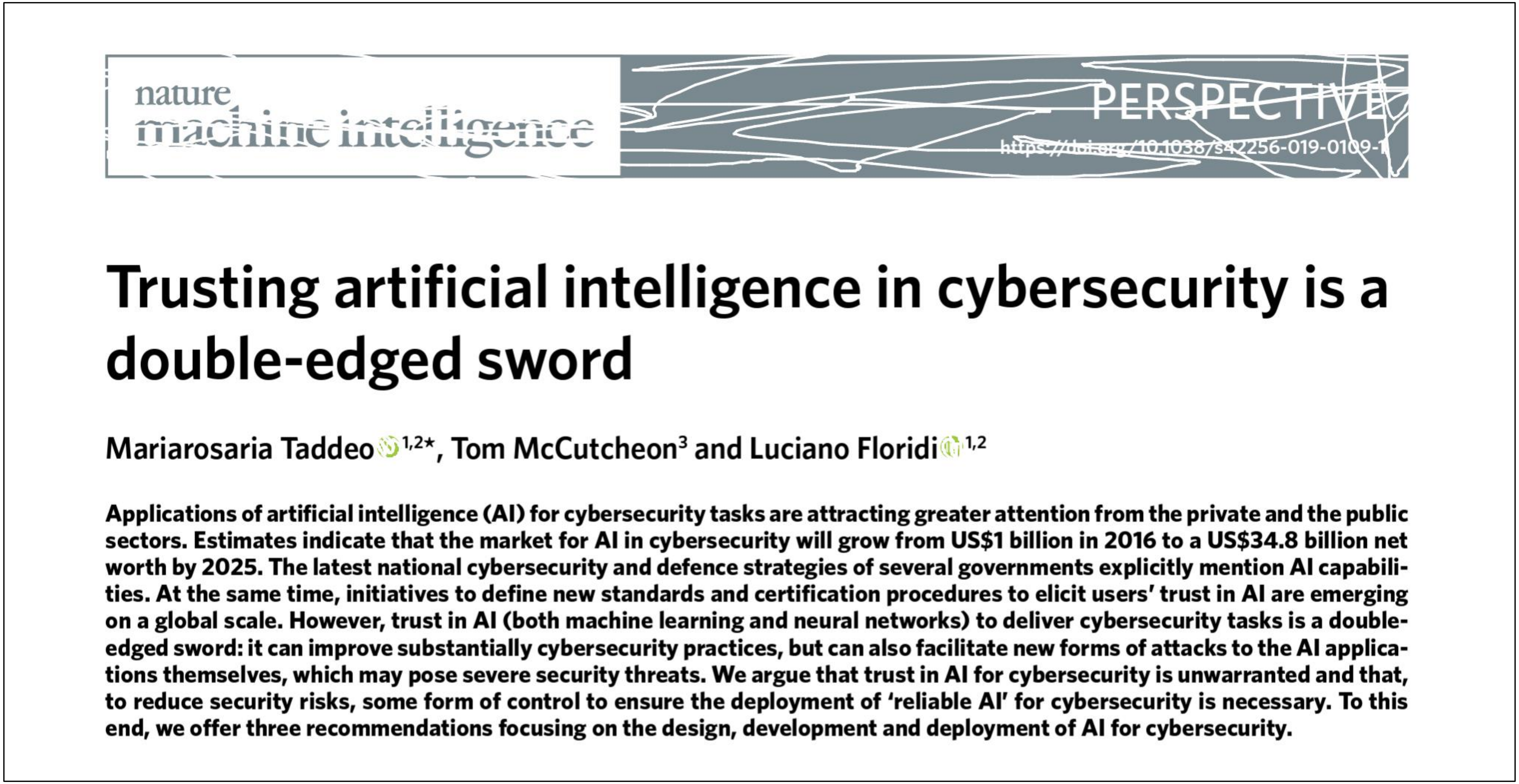
Figure 2. NIH Strategic Plan for Data Science: Overview of Goals and Objectives

The Attack Surface of a Connected Vehicle

The diagram below outlines some of the attack vectors constituting a connected vehicle's attack surface. It is through these "vectors" that a malicious actor could attempt to send malware to a connected vehicle. Such malware, if able to bypass the vehicle's security system(s), may potentially be able to affect the vehicle's non-safety and safety critical functions.




ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003



nature machine intelligence

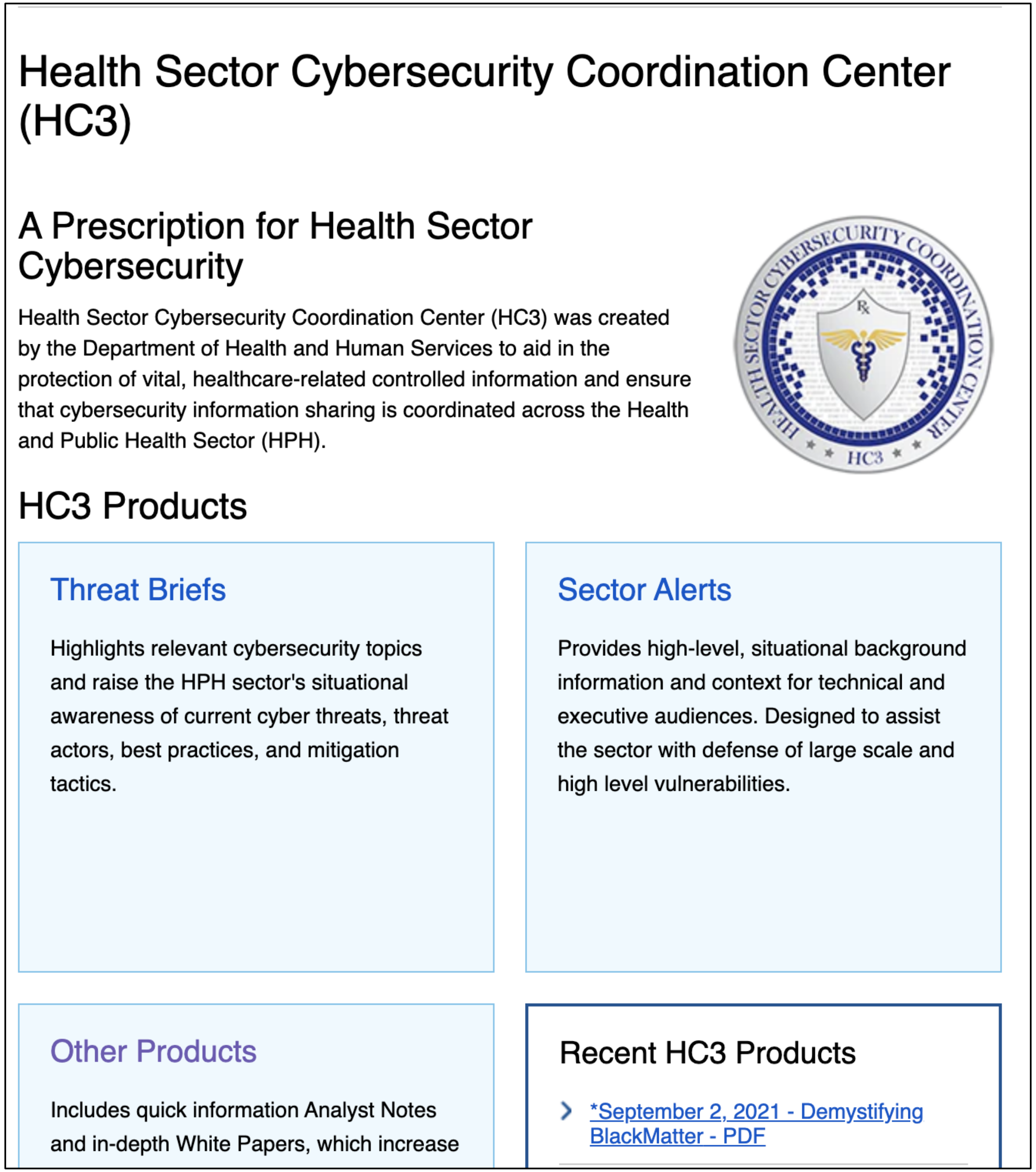
PERSPECTIVE

https://doi.org/10.1038/s42256-019-0109-1

Trusting artificial intelligence in cybersecurity is a double-edged sword

Mariarosaria Taddeo[1,2*], Tom McCutcheon[3] and Luciano Floridi[1,2]

Applications of artificial intelligence (AI) for cybersecurity tasks are attracting greater attention from the private and the public sectors. Estimates indicate that the market for AI in cybersecurity will grow from US$1 billion in 2016 to a US$34.8 billion net worth by 2025. The latest national cybersecurity and defence strategies of several governments explicitly mention AI capabilities. At the same time, initiatives to define new standards and certification procedures to elicit users' trust in AI are emerging on a global scale. However, trust in AI (both machine learning and neural networks) to deliver cybersecurity tasks is a double-edged sword: it can improve substantially cybersecurity practices, but can also facilitate new forms of attacks to the AI applications themselves, which may pose severe security threats. We argue that trust in AI for cybersecurity is unwarranted and that, to reduce security risks, some form of control to ensure the deployment of 'reliable AI' for cybersecurity is necessary. To this end, we offer three recommendations focusing on the design, development and deployment of AI for cybersecurity.



Health Sector Cybersecurity Coordination Center (HC3)

A Prescription for Health Sector Cybersecurity

Health Sector Cybersecurity Coordination Center (HC3) was created by the Department of Health and Human Services to aid in the protection of vital, healthcare-related controlled information and ensure that cybersecurity information sharing is coordinated across the Health and Public Health Sector (HPH).

HC3 Products

Threat Briefs

Highlights relevant cybersecurity topics and raise the HPH sector's situational awareness of current cyber threats, threat actors, best practices, and mitigation tactics.

Sector Alerts

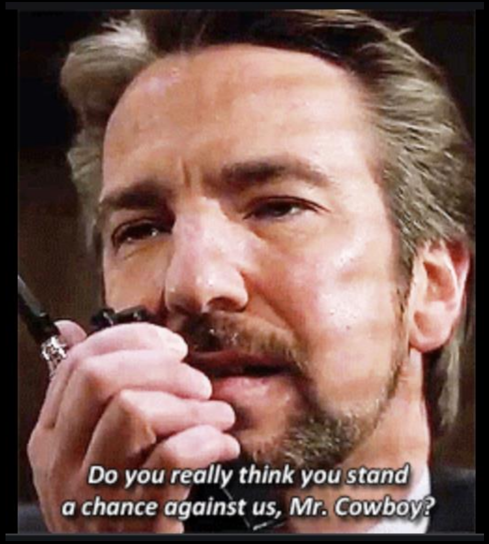
Provides high-level, situational background information and context for technical and executive audiences. Designed to assist the sector with defense of large scale and high level vulnerabilities.

Other Products

Includes quick information Analyst Notes and in-depth White Papers, which increase

Recent HC3 Products

- *September 2, 2021 - Demystifying BlackMatter - PDF

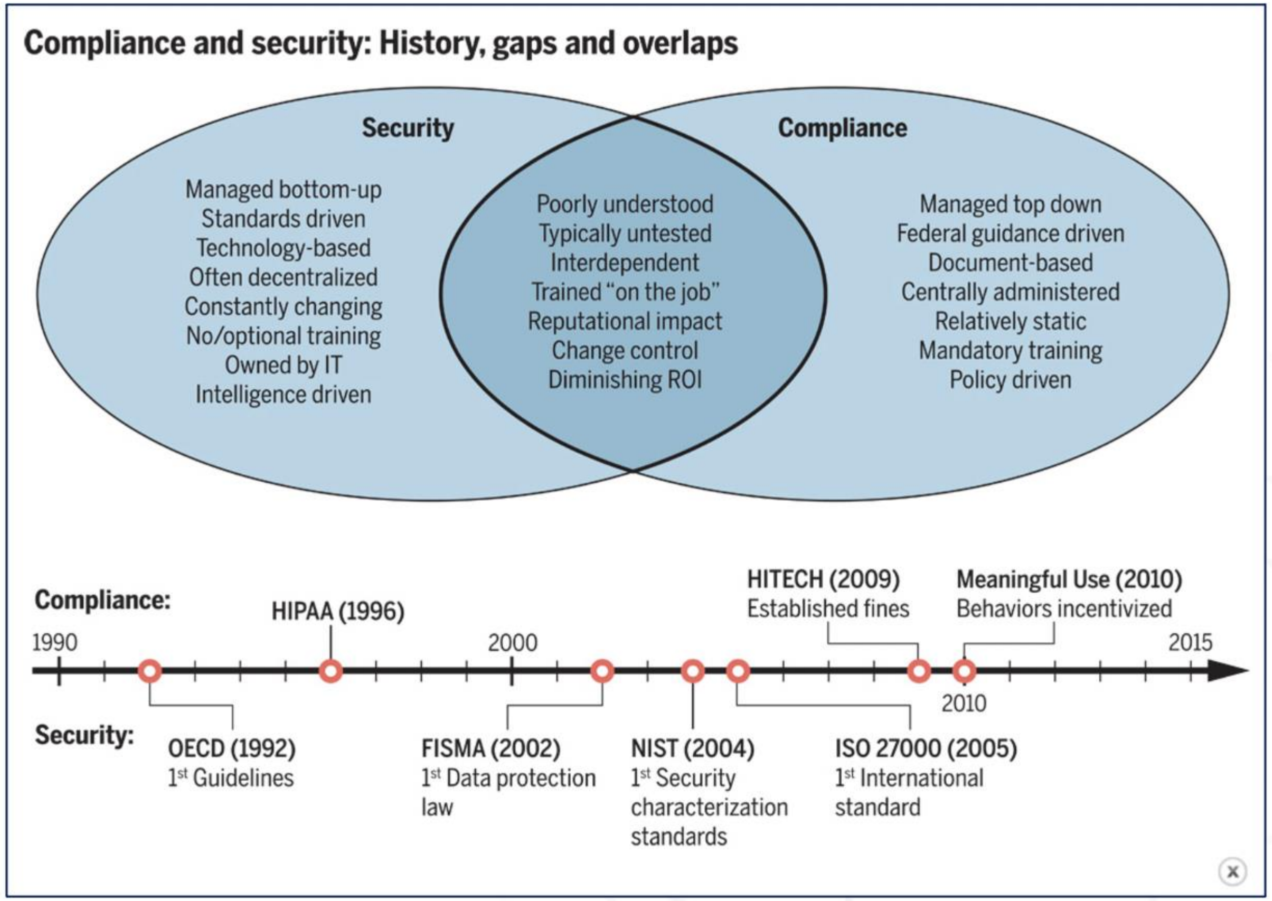

Do you really think you stand a chance against us, Mr. Cowboy?

Cyber-Compliance

Sci Transl Med. 2016 Jan 20;8(322):322ps2. doi: 10.1126/scitranslmed.aaa4493.

A cybersecurity primer for translational research.

Perakslis ED[1], Stanley M[2].



Compliance and security: History, gaps and overlaps

Security

Managed bottom-up
Standards driven
Technology-based
Often decentralized
Constantly changing
No/optional training
Owned by IT
Intelligence driven

Poorly understood
Typically untested
Interdependent
Trained "on the job"
Reputational impact
Change control
Diminishing ROI

Compliance

Managed top down
Federal guidance driven
Document-based
Centrally administered
Relatively static
Mandatory training
Policy driven

Compliance:

HIPAA (1996)

HITECH (2009)
Established fines

Meaningful Use (2010)
Behaviors incentivized

Security:

OECD (1992)
1st Guidelines

FISMA (2002)
1st Data protection law

NIST (2004)
1st Security characterization standards

ISO 27000 (2005)
1st International standard

Duke

https://www.ncbi.nlm.nih.gov/pubmed/26791947

Perfection Does Not Exist

Security ≠ Privacy -> data can be secure, but an organization may share that data without permission

You can have security without privacy, but you cannot have privacy without security.

Compliance ≠ Security -> an organization may not be compliant with its own policies

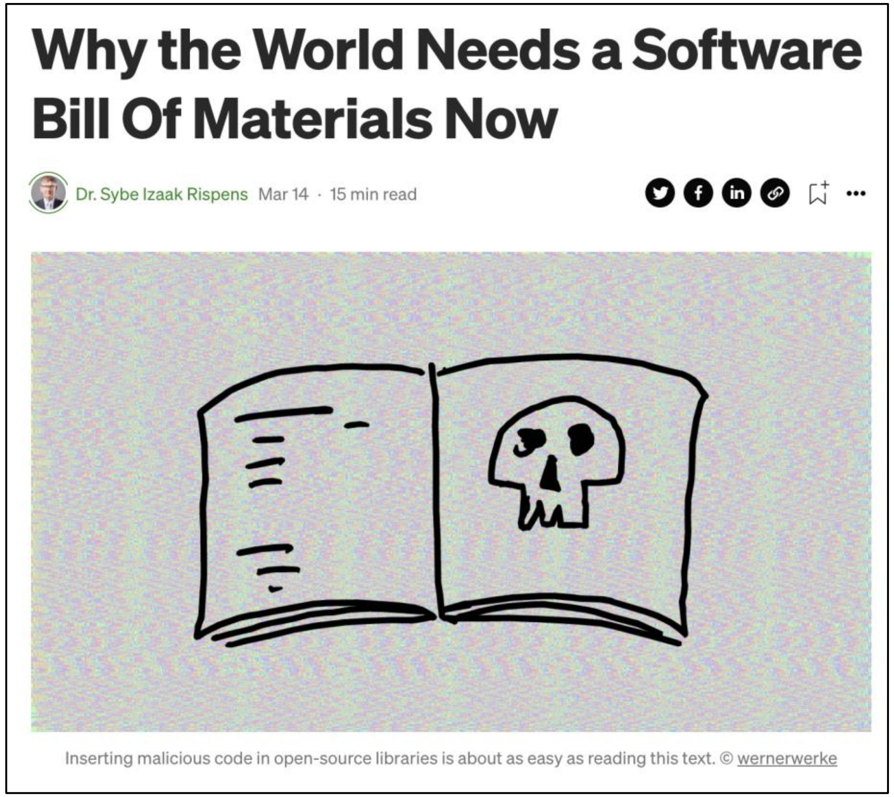
technical environments may not conform with design

users may subvert compliance policies that hinder essential work

any system can be hacked, especially as controls and technology age

You may know the ingredients of a Twinkie
but do your systems have ingredient lists?

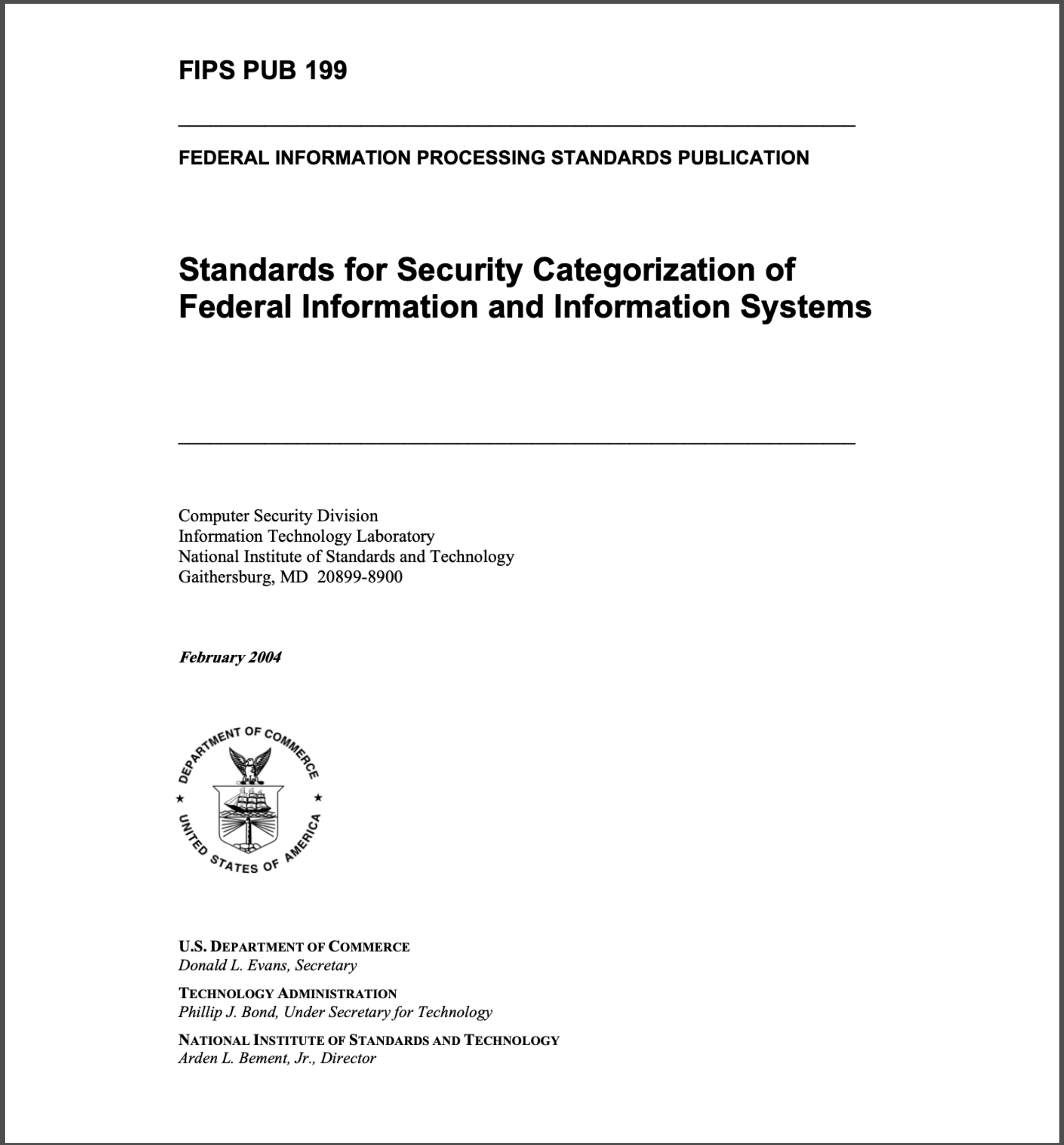
A "Software Bill of Materials" (SBOM) is a nested inventory for software, a list of all ingredients that make up software components.



Why the World Needs a Software Bill Of Materials Now

Dr. Sybe Izaak Rispens Mar 14 · 15 min read

Inserting malicious code in open-source libraries is about as easy as reading this text. © wernerwerke



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

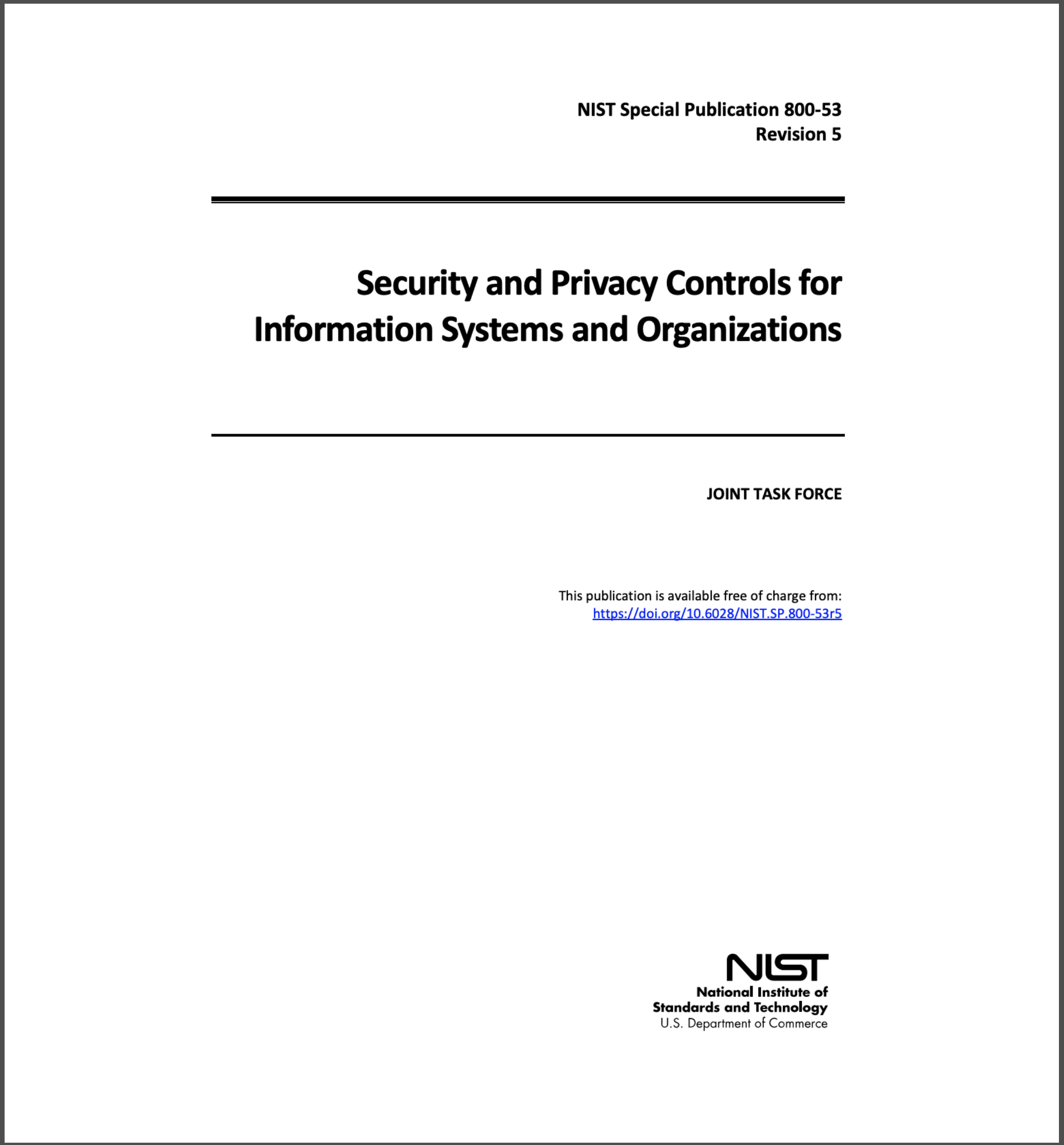
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director



NIST Special Publication 800-53
Revision 5

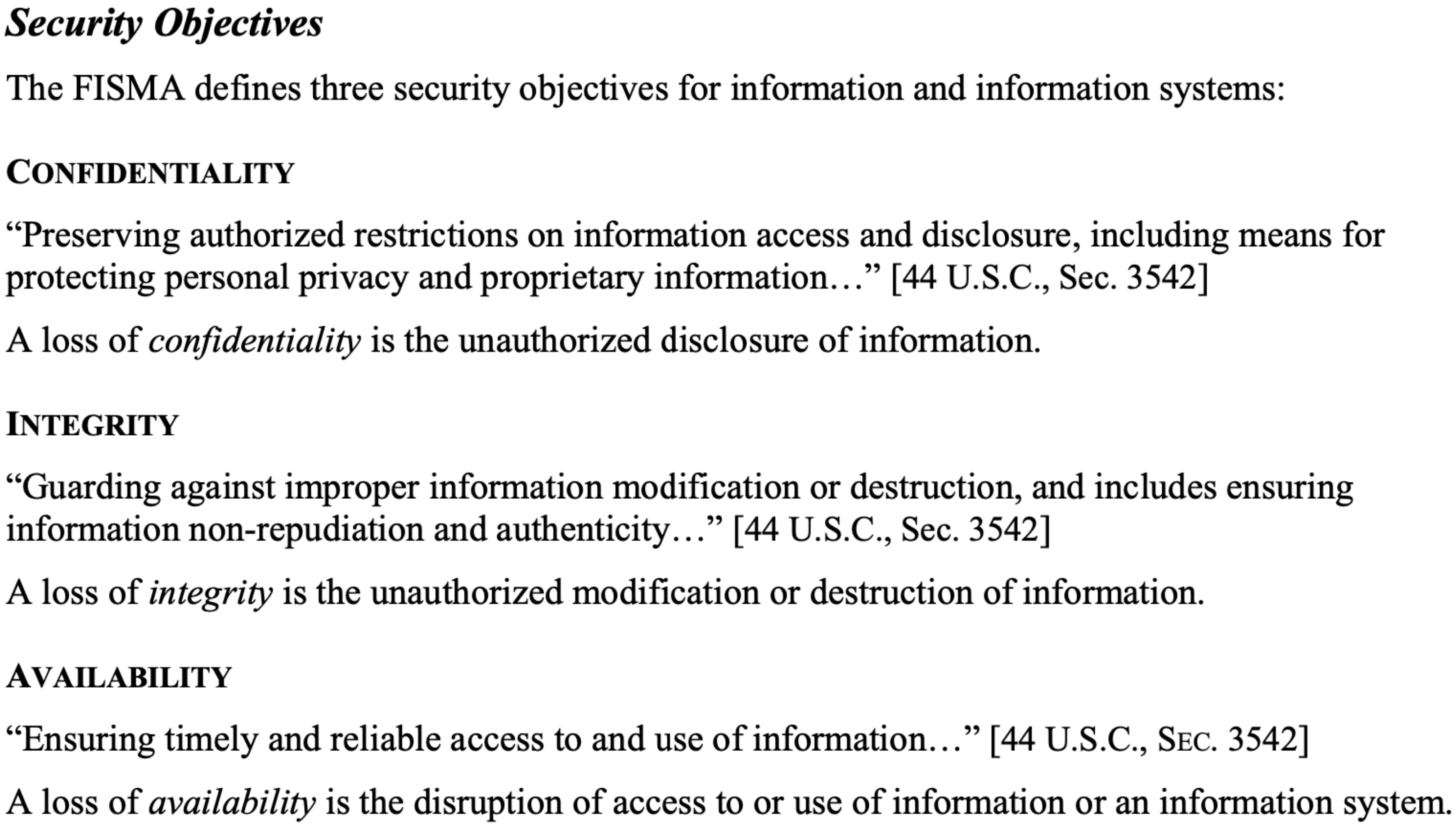
Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

FIPS-199: Security Objectives



Security Objectives

The FISMA defines three security objectives for information and information systems:

CONFIDENTIALITY

“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec. 3542]

A loss of *confidentiality* is the unauthorized disclosure of information.

INTEGRITY

“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…” [44 U.S.C., Sec. 3542]

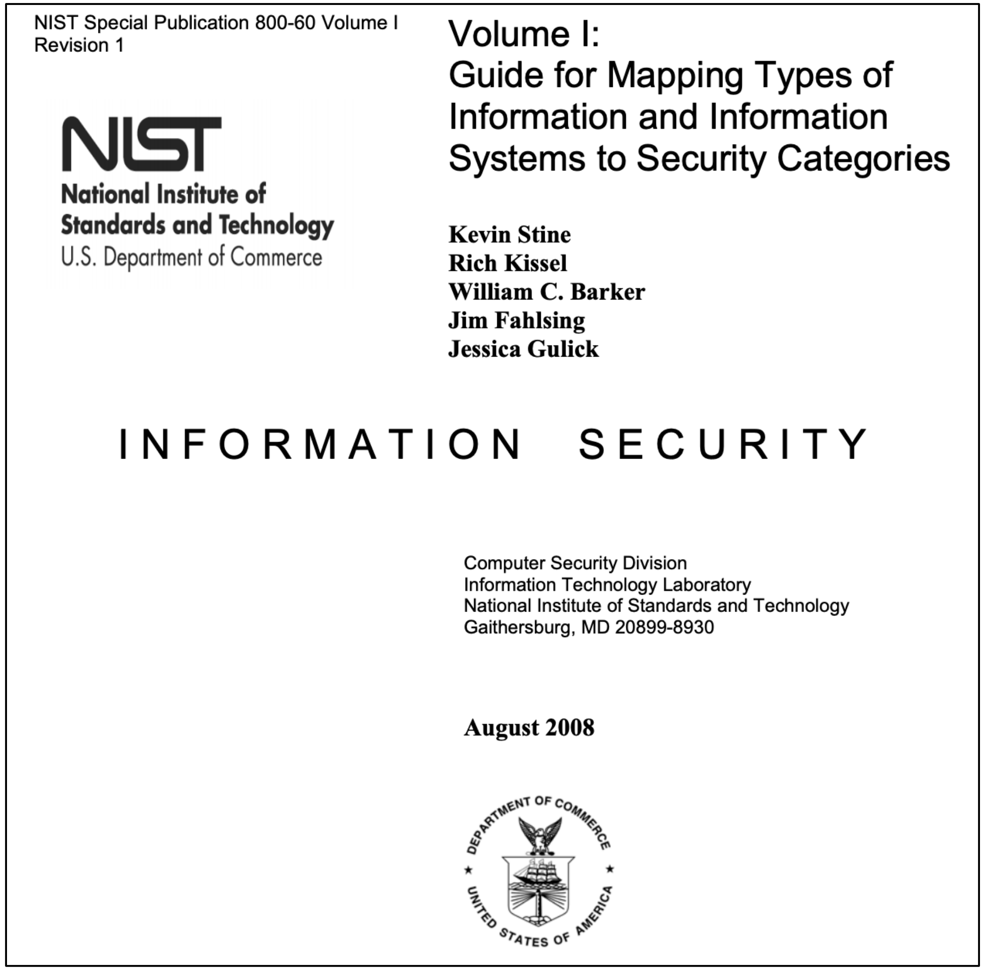
A loss of *integrity* is the unauthorized modification or destruction of information.

AVAILABILITY

“Ensuring timely and reliable access to and use of information…” [44 U.S.C., Sec. 3542]

A loss of *availability* is the disruption of access to or use of information or an information system.

NIST 800-60



NIST Special Publication 800-60 Volume I
Revision 1

National Institute of Standards and Technology
U.S. Department of Commerce

Volume I:
Guide for Mapping Types of Information and Information Systems to Security Categories

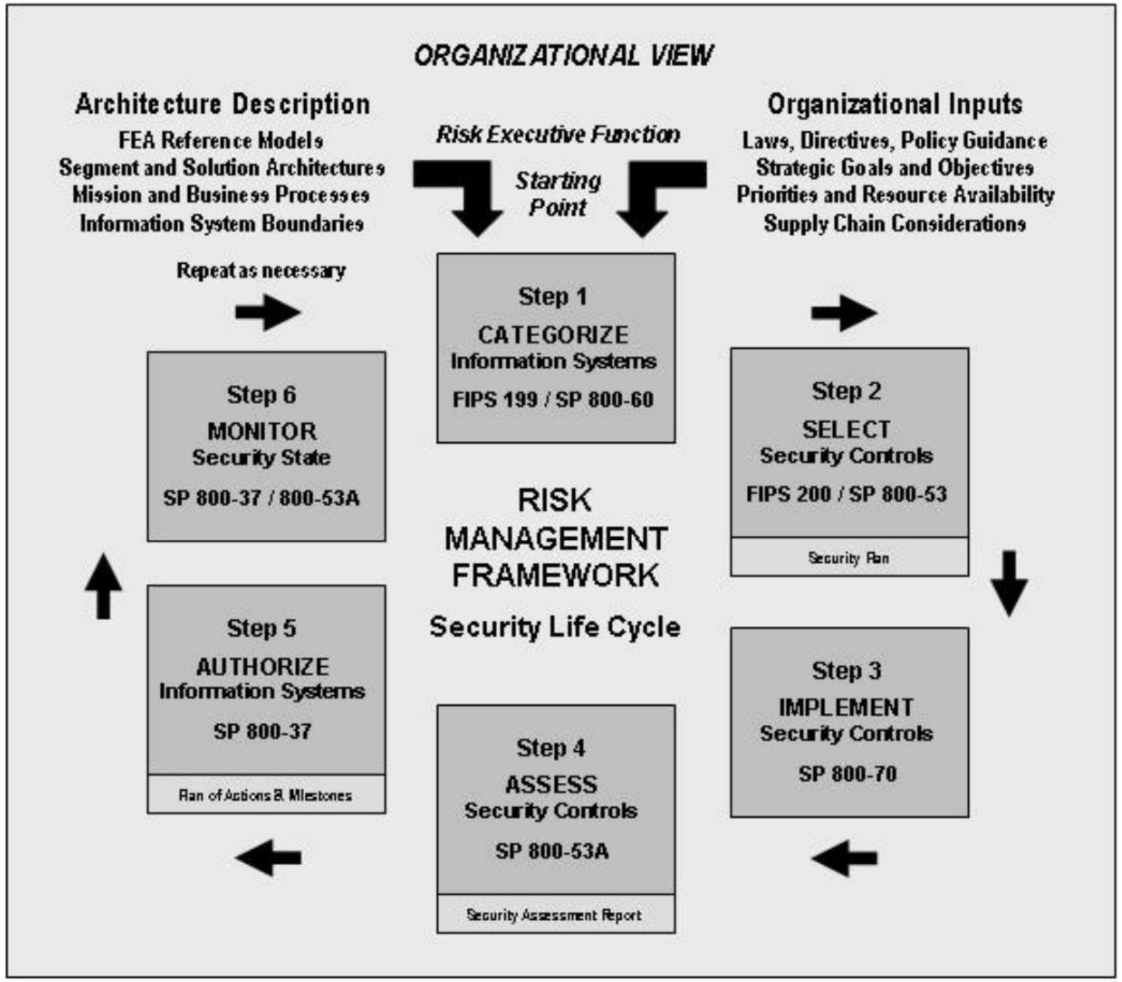
Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2008

DEPARTMENT OF COMMERCE · UNITED STATES OF AMERICA



ORGANIZATIONAL VIEW

Architecture Description
FEA Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

Risk Executive Function

Starting Point

Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Repeat as necessary

Step 1
CATEGORIZE
Information Systems
FIPS 199 / SP 800-60

Step 2
SELECT
Security Controls
FIPS 200 / SP 800-53
Security Plan

Step 3
IMPLEMENT
Security Controls
SP 800-70

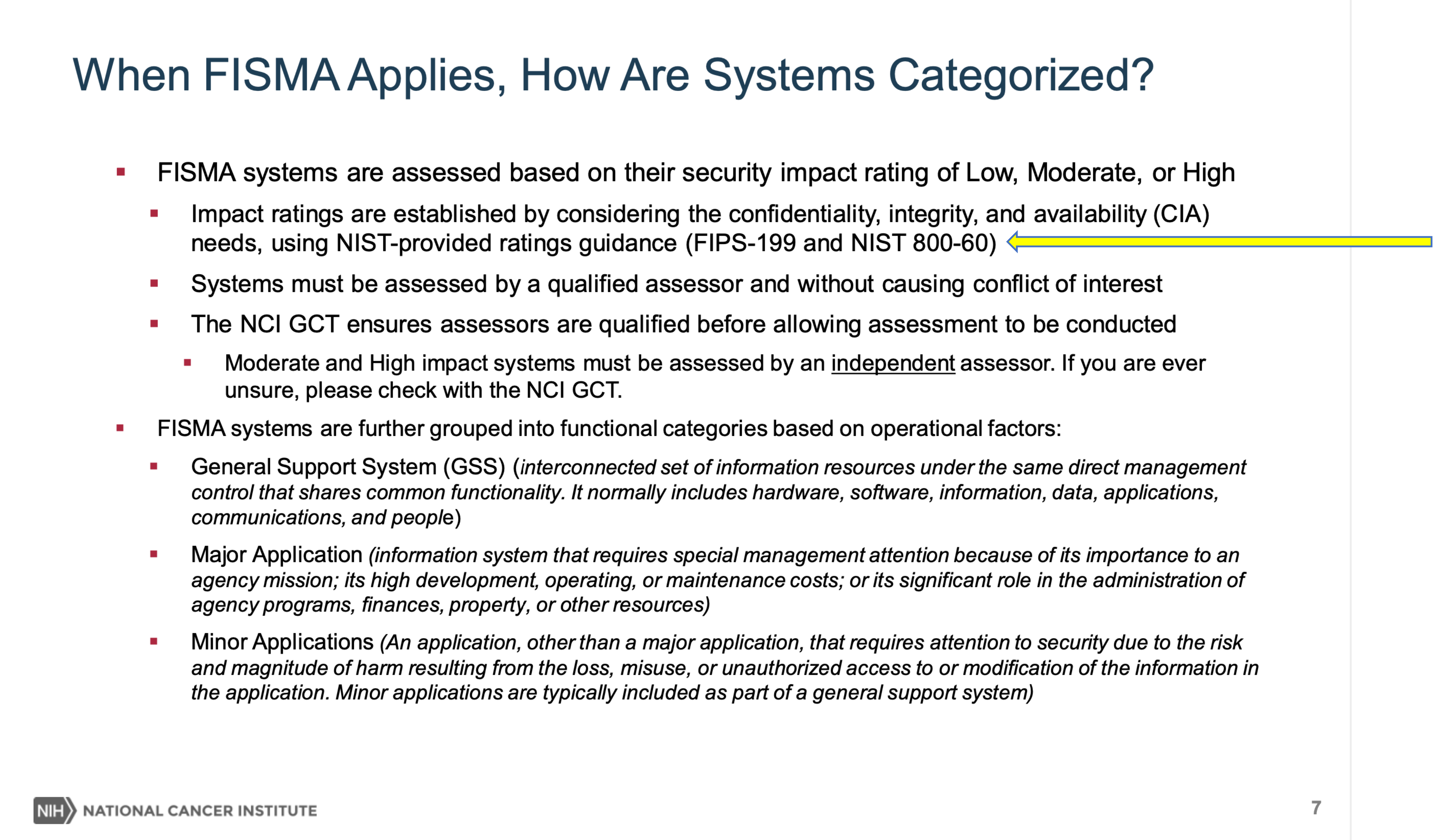
Step 4
ASSESS
Security Controls
SP 800-53A
Security Assessment Report

Step 5
AUTHORIZE
Information Systems
SP 800-37
Plan of Actions & Milestones

Step 6
MONITOR
Security State
SP 800-37 / 800-53A

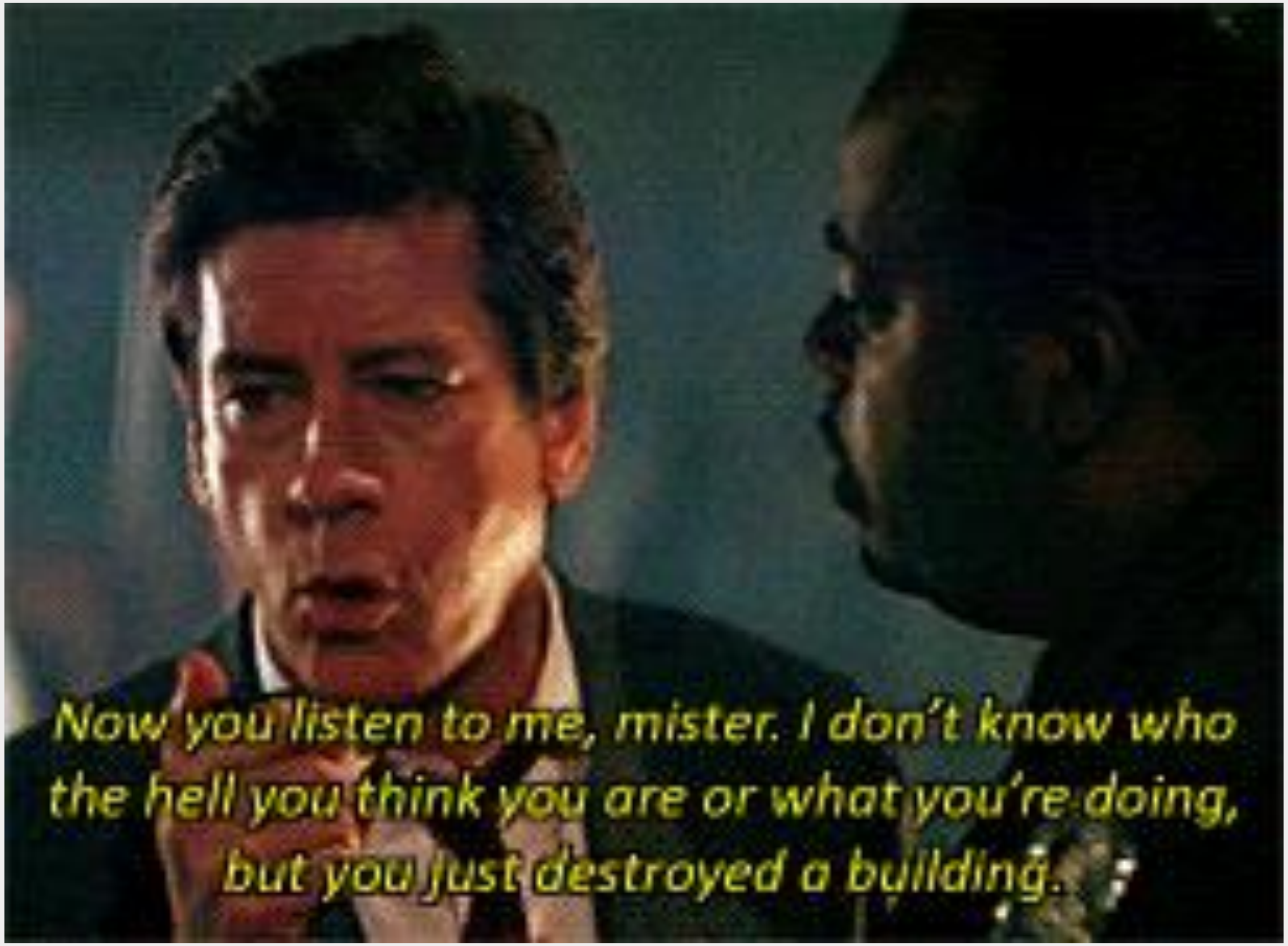
RISK MANAGEMENT FRAMEWORK

Security Life Cycle

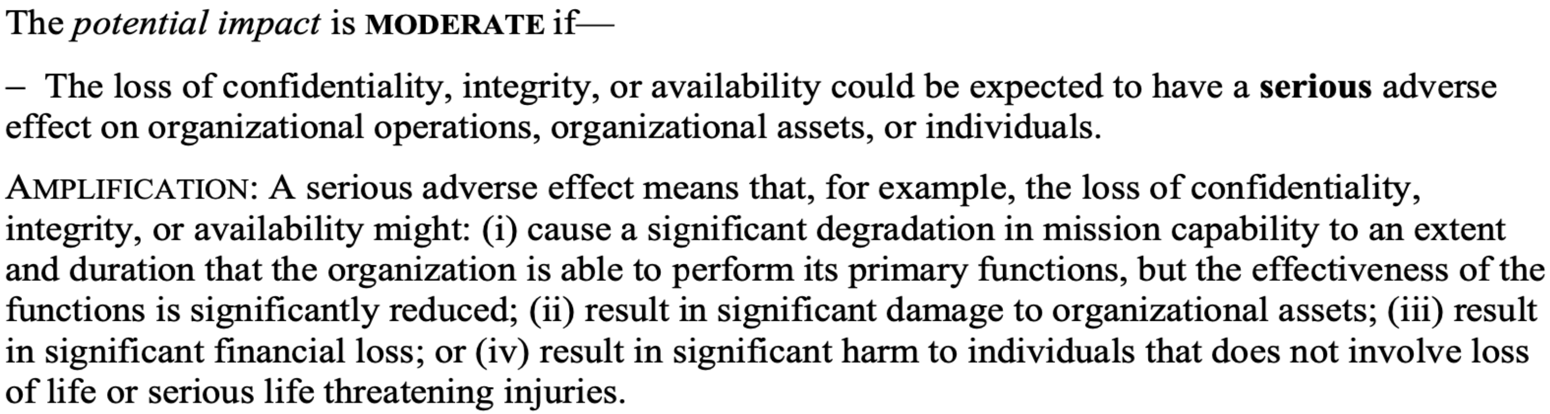


When FISMA Applies, How Are Systems Categorized?

- FISMA systems are assessed based on their security impact rating of Low, Moderate, or High
  - Impact ratings are established by considering the confidentiality, integrity, and availability (CIA) needs, using NIST-provided ratings guidance (FIPS-199 and NIST 800-60)
  - Systems must be assessed by a qualified assessor and without causing conflict of interest
  - The NCI GCT ensures assessors are qualified before allowing assessment to be conducted
    - Moderate and High impact systems must be assessed by an independent assessor. If you are ever unsure, please check with the NCI GCT.
- FISMA systems are further grouped into functional categories based on operational factors:
  - General Support System (GSS) (*interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people*)
  - Major Application *(information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources)*
  - Minor Applications *(An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system)*


Now you listen to me, mister. I don't know who
the hell you think you are or what you're doing,
but you just destroyed a building.

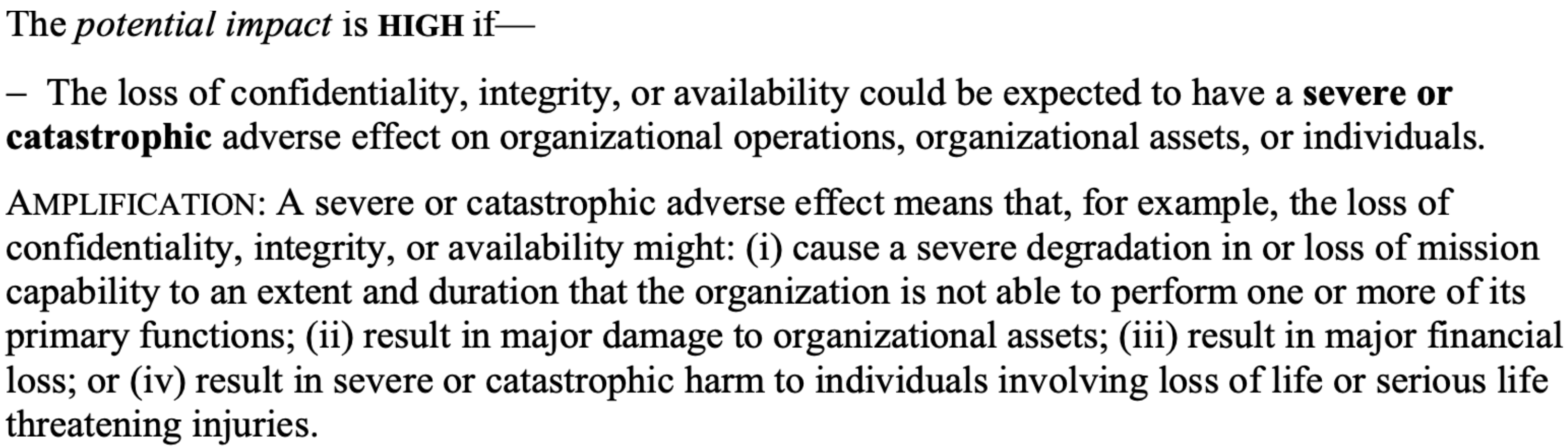
FIPS-199: Potential Impact



The *potential impact* is **MODERATE** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

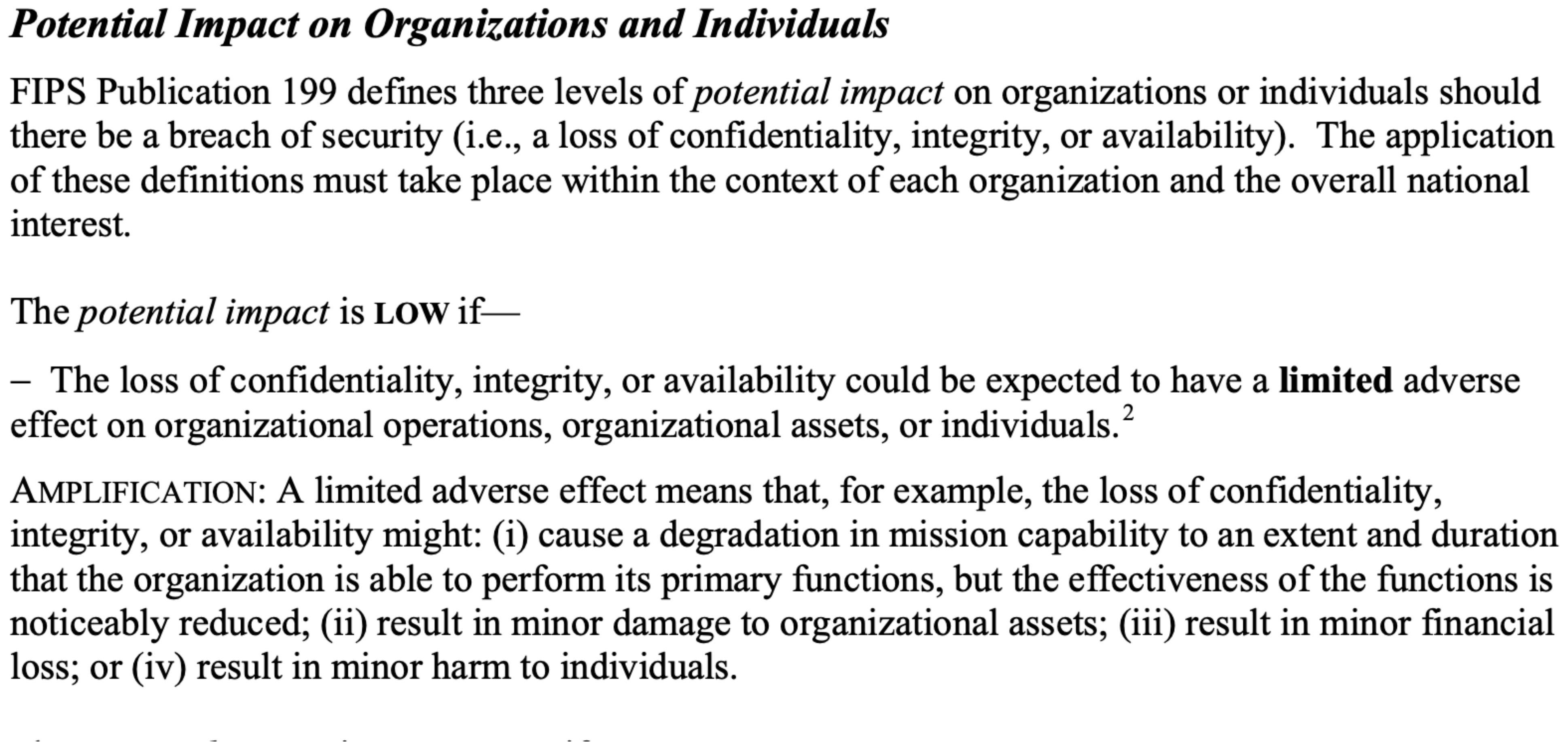


The *potential impact* is **HIGH** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

FIPS-199: Potential Impact



Potential Impact on Organizations and Individuals

FIPS Publication 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

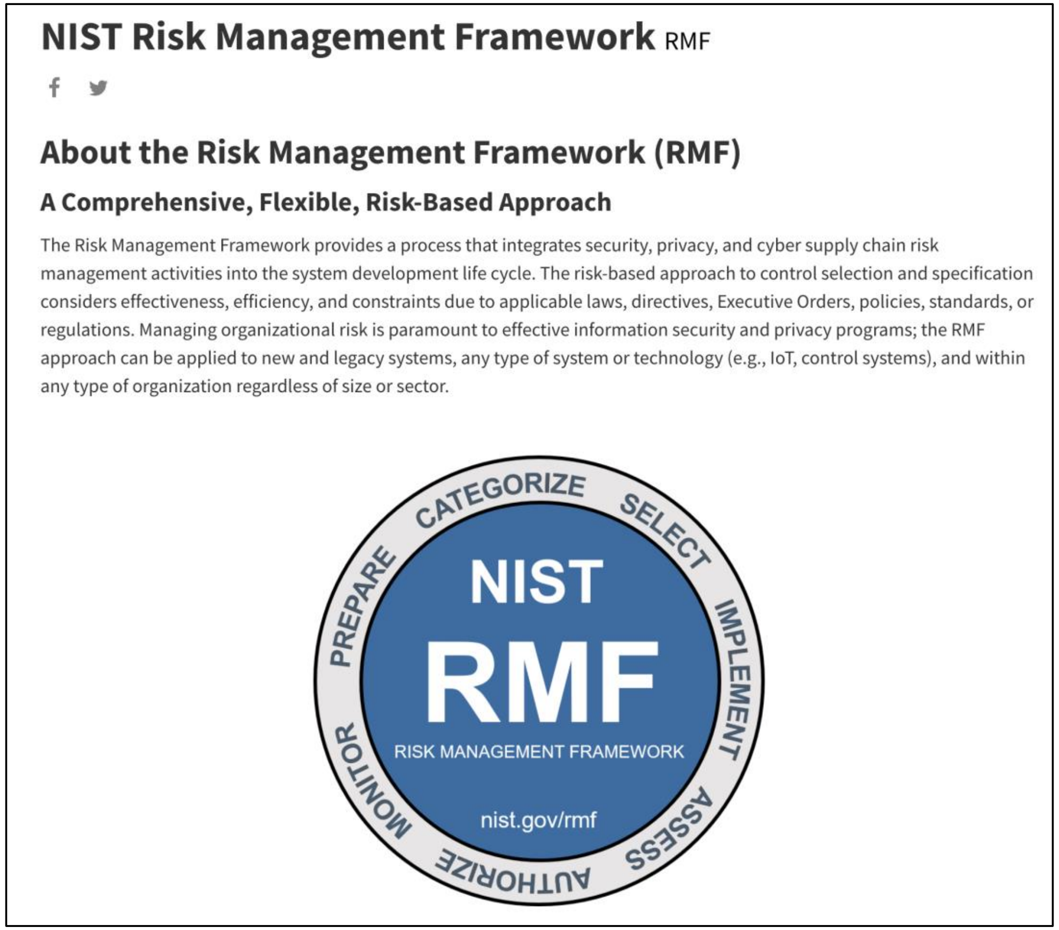
The *potential impact* is **LOW** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.[2]

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Cyber Risk Equation

Risk = Threat * Vulnerability * Impact * Likelihood

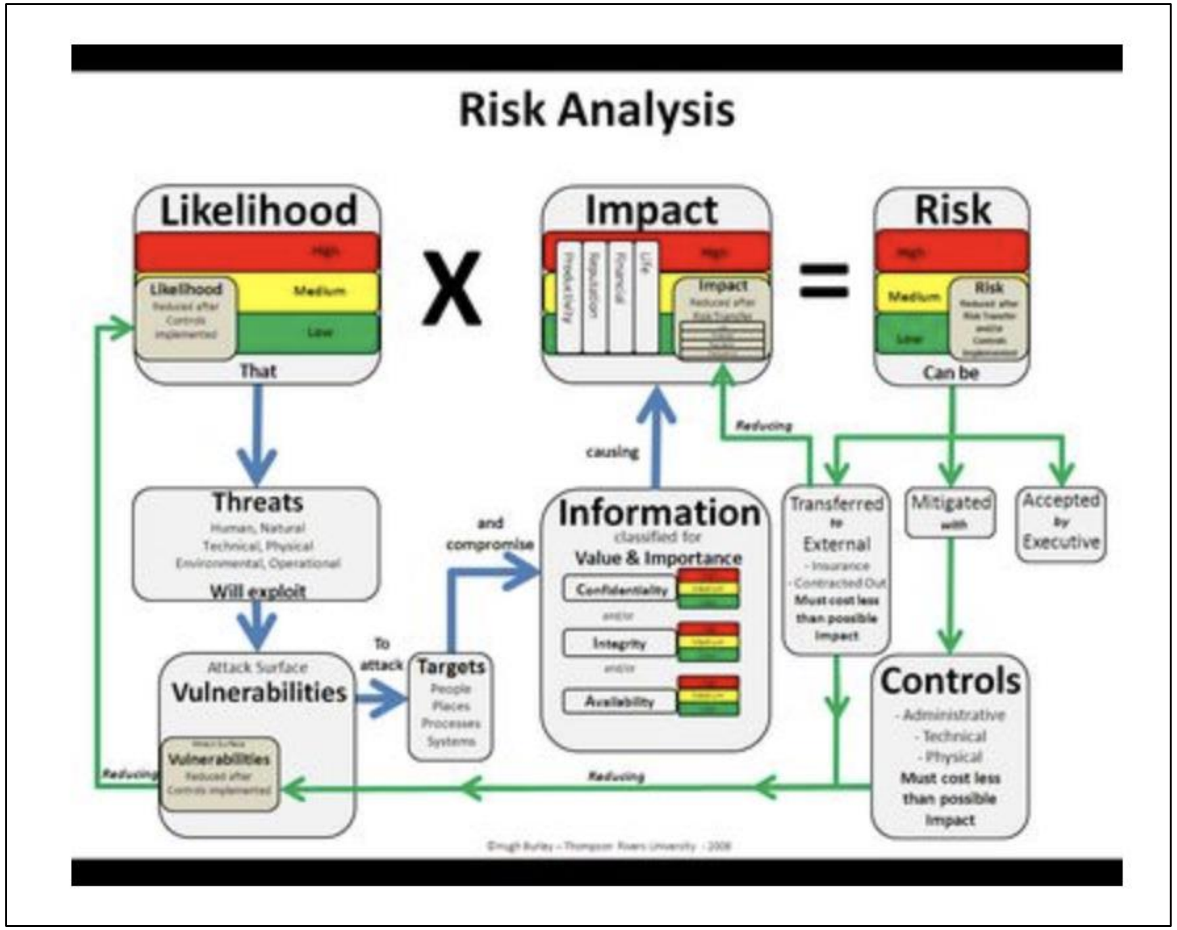


NIST Risk Management Framework RMF

About the Risk Management Framework (RMF)

A Comprehensive, Flexible, Risk-Based Approach

The Risk Management Framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. Managing organizational risk is paramount to effective information security and privacy programs; the RMF approach can be applied to new and legacy systems, any type of system or technology (e.g., IoT, control systems), and within any type of organization regardless of size or sector.



Risk Analysis

©Hugh Burley – Thompson Rivers University - 2008

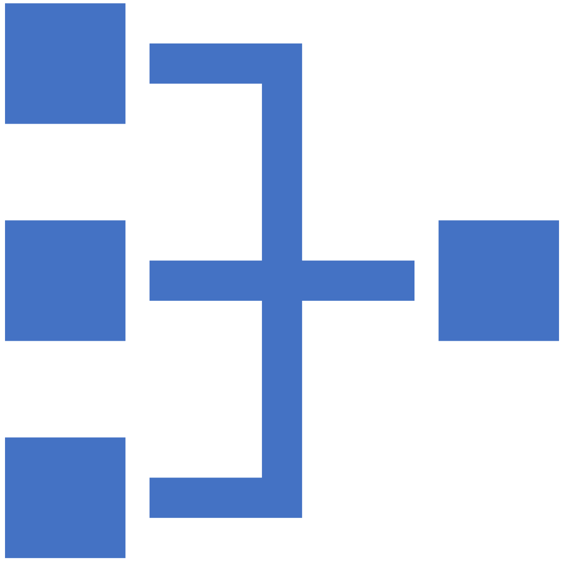
Practical Approaches that Researchers Can Control

1. Data flows & system boundaries

System boundaries, such as FISMA boundaries, are based upon workflow. By proactively designing data flows, researchers can control system boundaries.

Considerations:

- is all data of the same sensitivity?
- do all sites have similar capabilities?
- where can you air-gap a site, network or process?
- what types of controls can be built into the study design de novo?
- which research roles need to have access to all the data?
- are infosec and infosec compliance requirements properly stated with contracts?
- can the network be segmented?
- **Avoid having to retrofit security at ALL costs!**



Practical Approaches that Researchers Can Control

2. Minimize Attack Surface

Every partner, participant subcontractor and unique system login adds to overall attack surface.

Considerations:

- As numbers of partners, subcontractors and sites grow, consider more centralized data management
- Embrace Zero Trust - a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration & posture before being granted or keeping access to applications & data
- Minimize accounts at 3rd-party partners, many aren't necessary or even justified
- **Set the default setting to the internet to OFF!**

Remember what we know about weakest links…

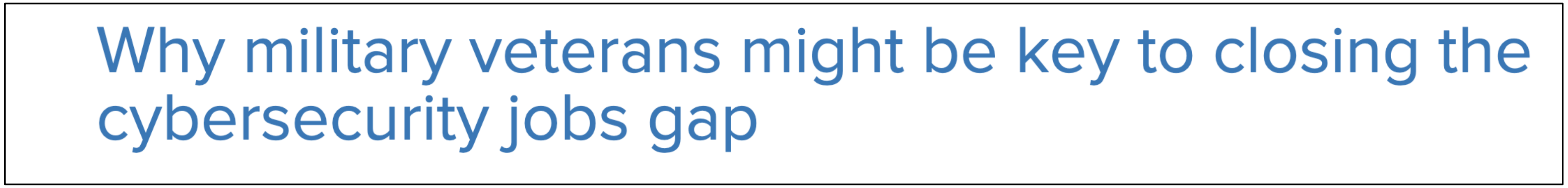
Practical Approaches that Researchers Can Control

3. Add InfoSec expertise to the design team

Information Security Professionals are highly in demand, yet most IT departments are under-staffed.

Considerations:

- Ensure the local InfoSec team is aware and engaged
- Work through them to add resources (internal or external)
- Some parts of the process can be outsourced, such as penetration testing, BUT internal resources must supervise
- Some internal departments lack expertise, use grant funding to bridge essential skill sets such as design, forensic evaluation, penetration testing
- Add a security threat research professional SAB or other governing structure



Why military veterans might be key to closing the cybersecurity jobs gap

WELCOME TO THE
PARTY, PAL.

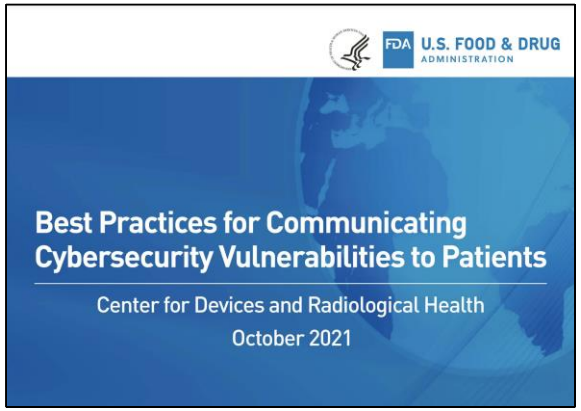
Practical Approaches that Researchers Can Control

4. <u>Lean-in to innovation</u>

The best research may happen with fully-identified cohorts.

Considerations:

- De-identification is a tactic, not a strategy
- Linked data is a data type, not a strategy
- We have not pushed the boundaries of what can be done with consented data
- Consider identity-monitoring or other services in addition to payment for research subjects
- You have access to the right expertise, do the benefit-risk calculus and aim for impact

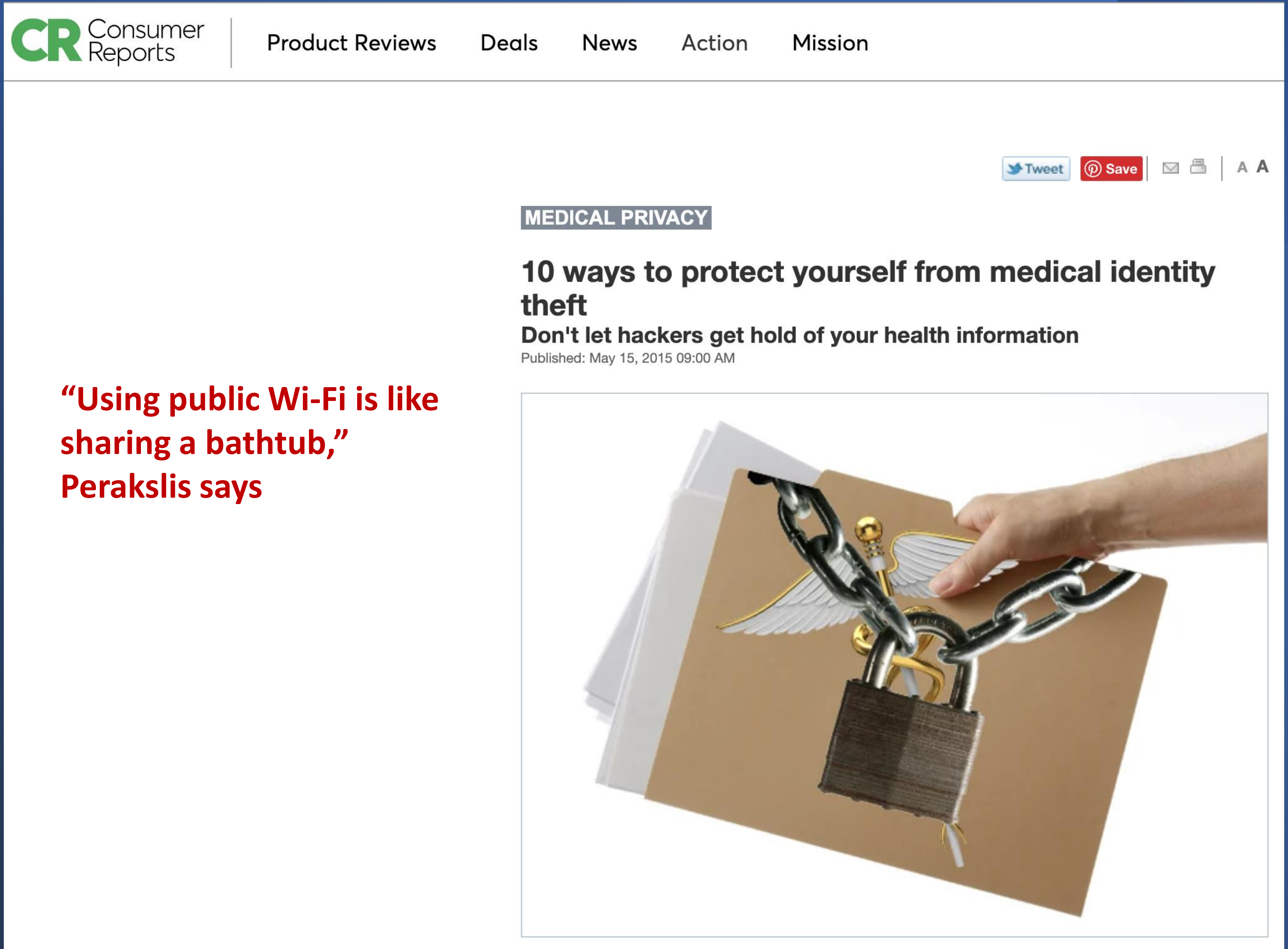


FDA U.S. FOOD & DRUG ADMINISTRATION

Best Practices for Communicating Cybersecurity Vulnerabilities to Patients

Center for Devices and Radiological Health

October 2021



MEDICAL PRIVACY

10 ways to protect yourself from medical identity theft

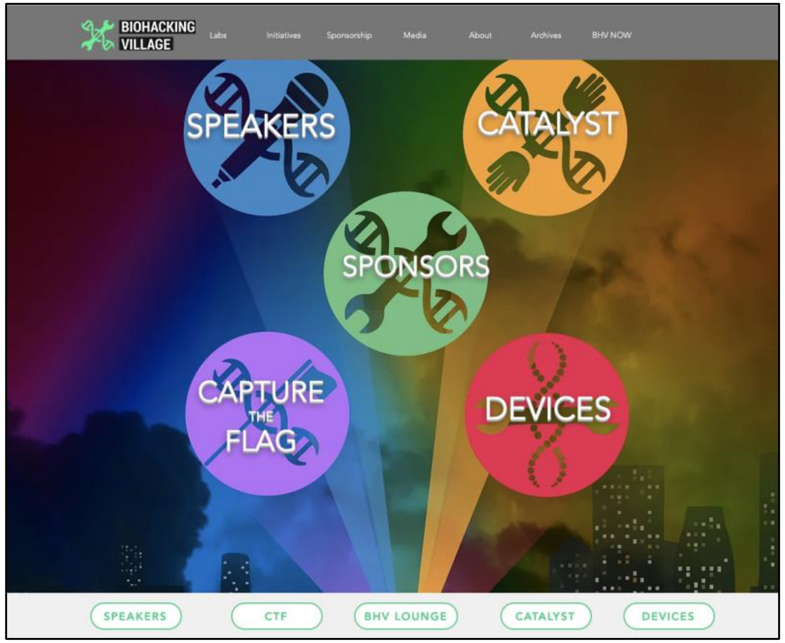
Don't let hackers get hold of your health information

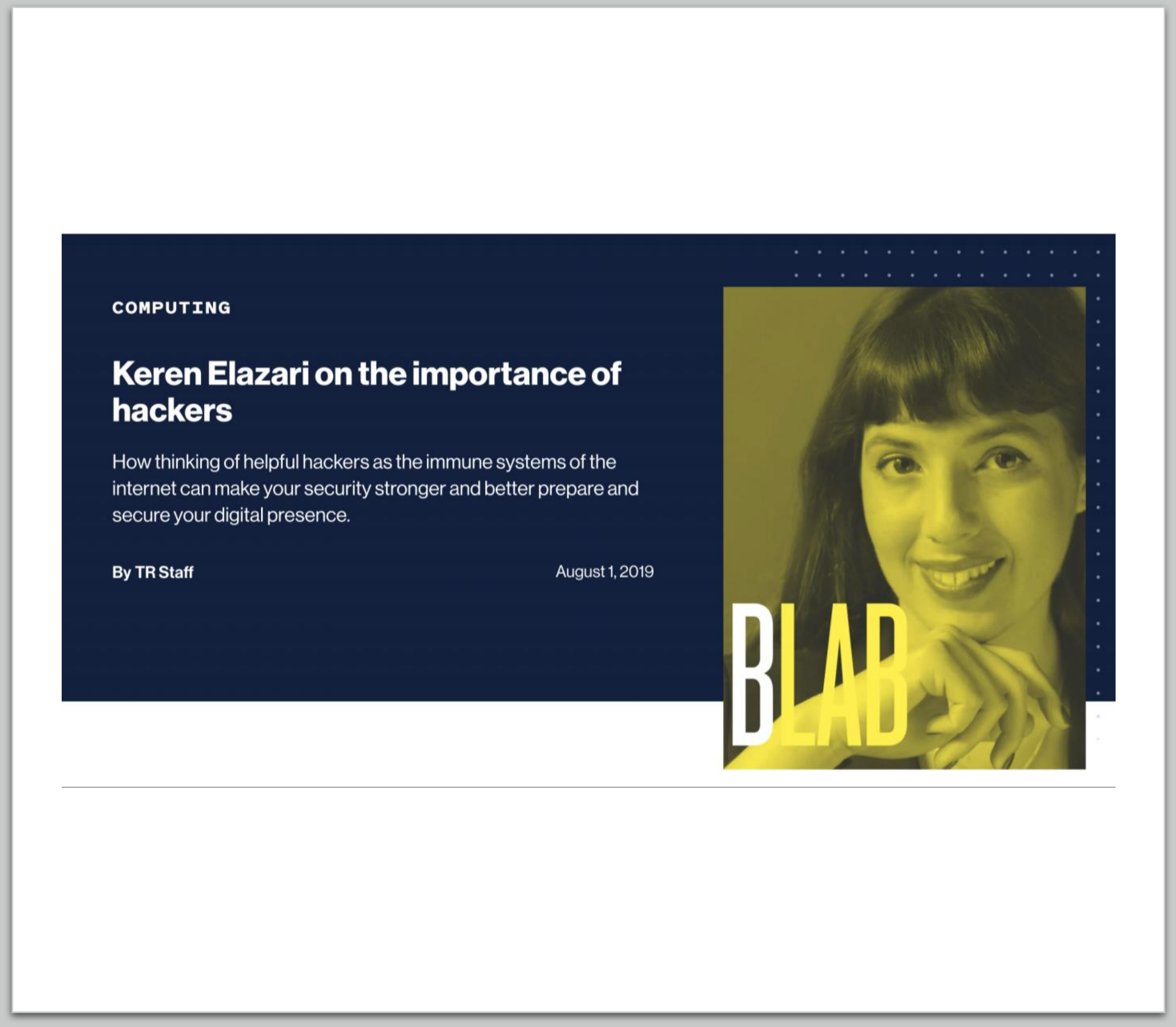
Published: May 15, 2015 09:00 AM

“Using public Wi-Fi is like sharing a bathtub,” Perakslis says

Practical Approaches that Researchers Can Control

5. Join the ethical hacking community





COMPUTING

Keren Elazari on the importance of hackers

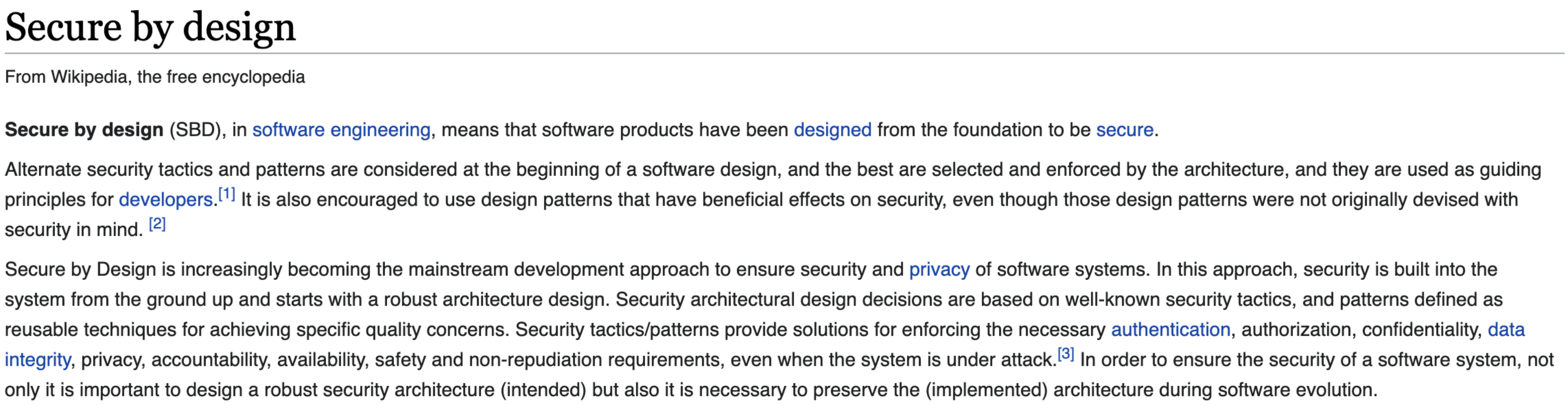
How thinking of helpful hackers as the immune systems of the internet can make your security stronger and better prepare and secure your digital presence.

By TR Staff

August 1, 2019

Practical Approaches that Researchers Can Control

6. Get to Know Security by Design: One Size Fits None



Secure by design

From Wikipedia, the free encyclopedia

Secure by design (SBD), in software engineering, means that software products have been designed from the foundation to be secure.

Alternate security tactics and patterns are considered at the beginning of a software design, and the best are selected and enforced by the architecture, and they are used as guiding principles for developers.[1] It is also encouraged to use design patterns that have beneficial effects on security, even though those design patterns were not originally devised with security in mind. [2]

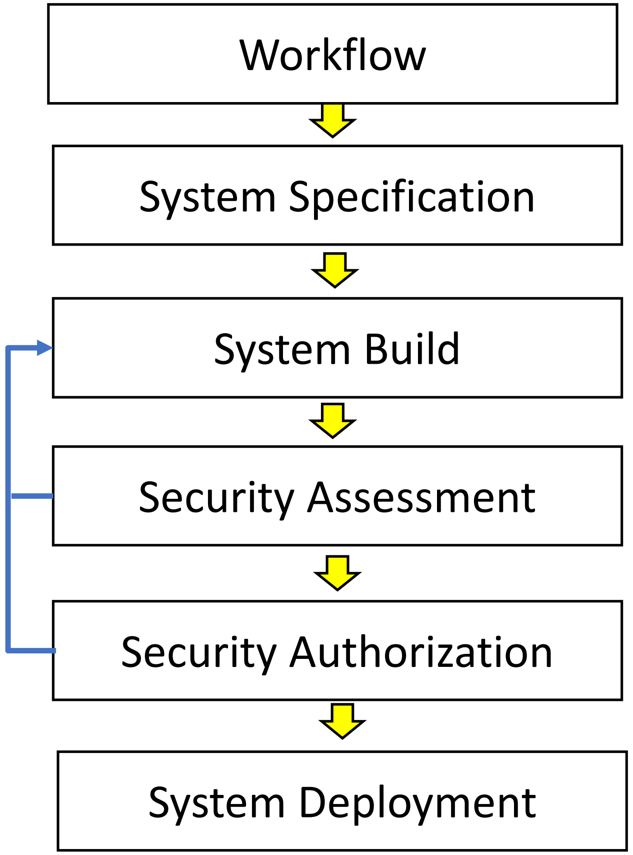
Secure by Design is increasingly becoming the mainstream development approach to ensure security and privacy of software systems. In this approach, security is built into the system from the ground up and starts with a robust architecture design. Security architectural design decisions are based on well-known security tactics, and patterns defined as reusable techniques for achieving specific quality concerns. Security tactics/patterns provide solutions for enforcing the necessary authentication, authorization, confidentiality, data integrity, privacy, accountability, availability, safety and non-repudiation requirements, even when the system is under attack.[3] In order to ensure the security of a software system, not only it is important to design a robust security architecture (intended) but also it is necessary to preserve the (implemented) architecture during software evolution.

Security by Design in Practice

Past

Workflow & system selection occur without the inclusion of Intentional security risk-management design. This results in late & reactive security categorization.

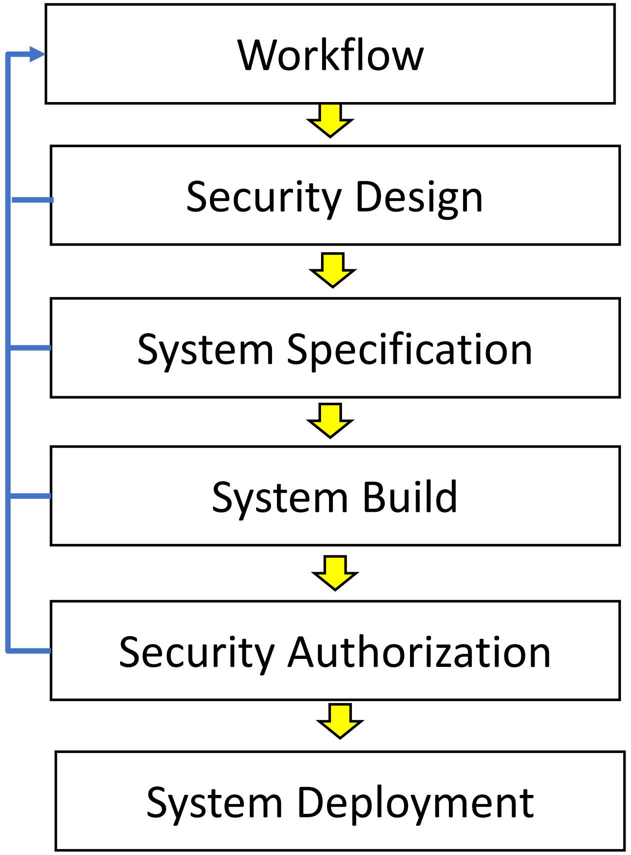
FISMA Moderate/High

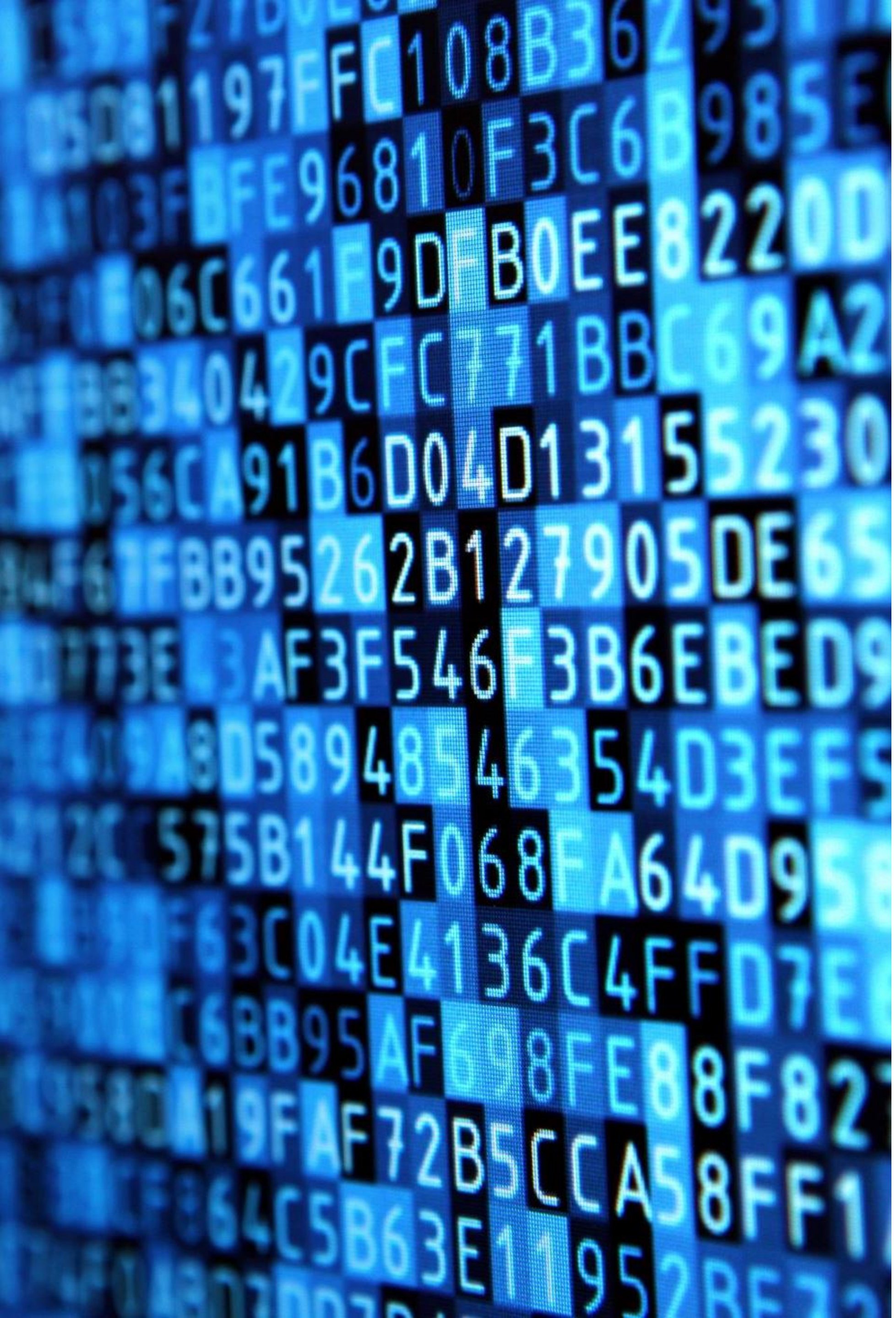


Future

Instead, we can design our security strategy concurrently with study design to intentionally influence the final security impact levels and final FISMA level.

FISMA Low





Practical Approaches that Researchers Can Control

7. <u>Budget for a System Security Plan</u>

At the end of the day, compliance is about time and money

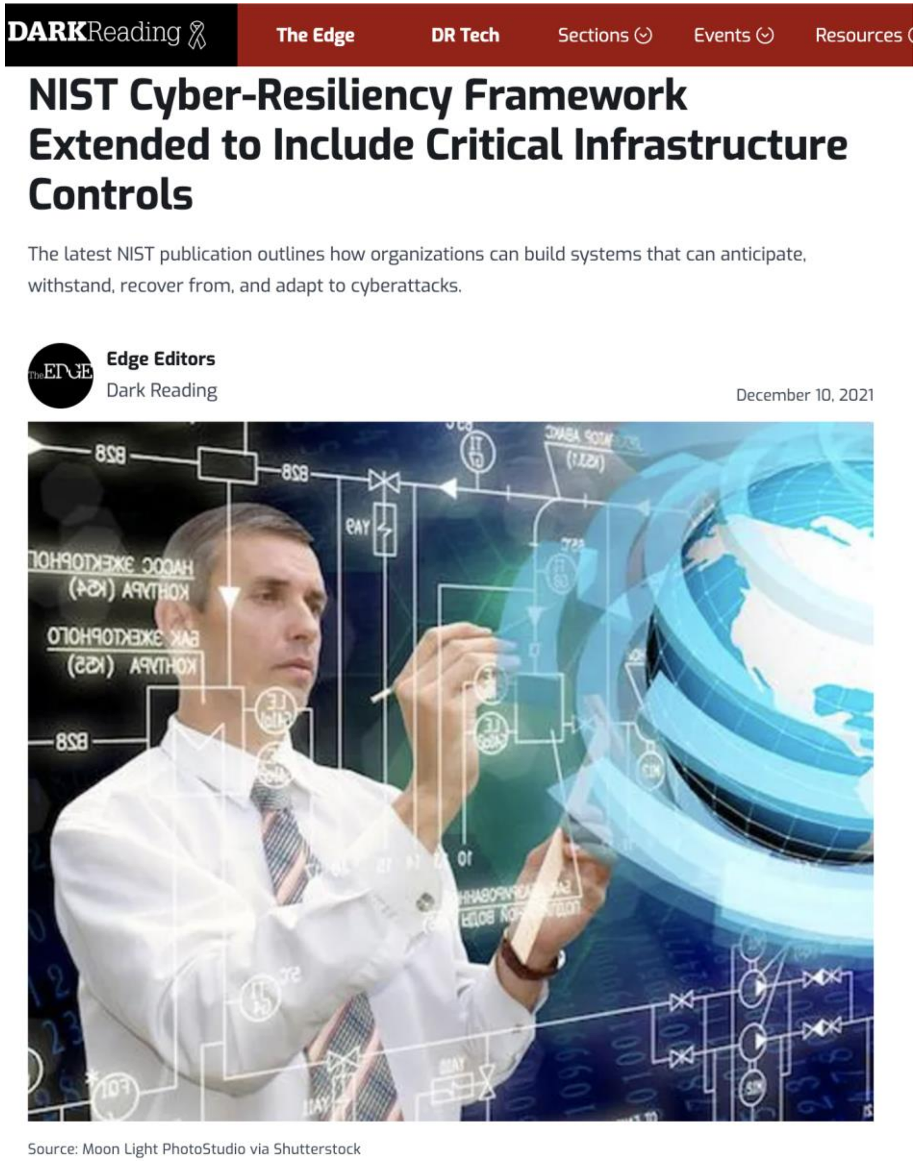
Considerations assuming steps 1-6 have been considered:

- For technology infrastructure under $500k, adding 30% is a safe estimate
- For technology infrastructure over $500k, this number can be 10-15% lower
- Platform as a service offerings from FedRAMP-certified cloud partners can save time, money and risk
- Optimally, these costs are written into budget proposals. The earlier, the better

Cyber-resiliency engineering combines specialty systems engineering, systems security engineering, and resilience engineering to architect, design, develop, implement, maintain, and sustain the trustworthiness of systems. The point of cyber-resiliency engineering is to develop “survivable, trustworthy secure systems” that can anticipate, withstand, recover from, and adapt to adverse conditions and attacks, NIST says.

Being cyber-resilient can help organizations reduce the risks of security incidents because the potential damage – the blast radius – is contained.

Cyber-resiliency assumes the attacker has already gained access to a system or will



NIST Cyber-Resiliency Framework Extended to Include Critical Infrastructure Controls

The latest NIST publication outlines how organizations can build systems that can anticipate, withstand, recover from, and adapt to cyberattacks.

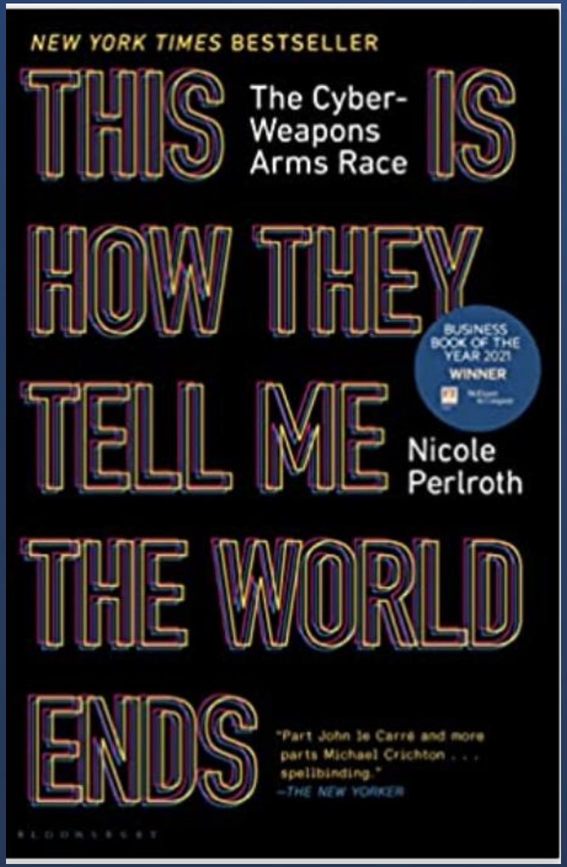
Edge Editors
Dark Reading

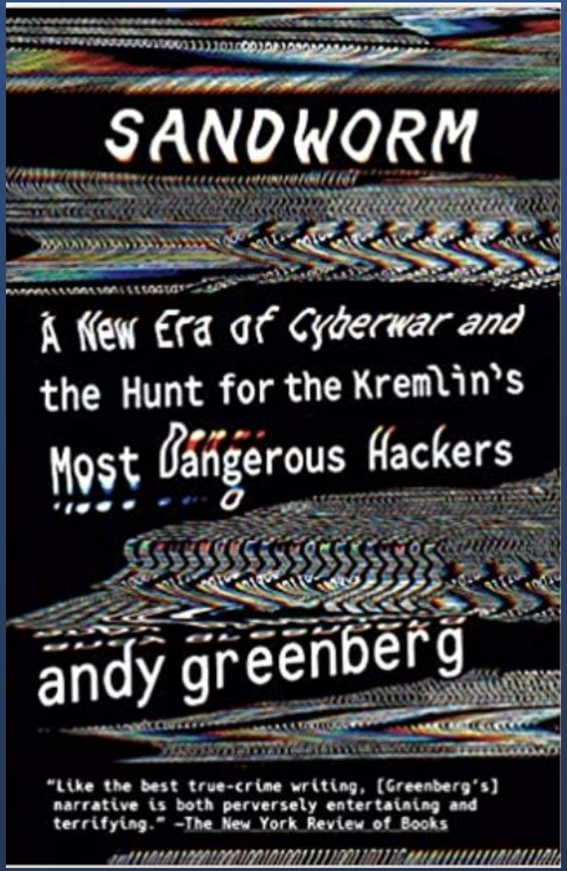
December 10, 2021

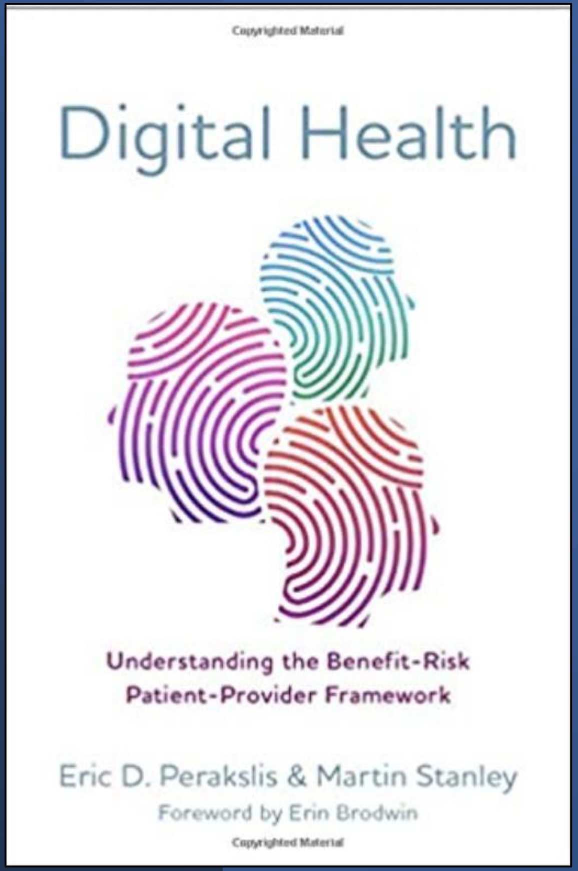
Source: Moon Light PhotoStudio via Shutterstock

Practical Approaches that Researchers Can Control

7. Educate yourself and your research team with some light reading


NEW YORK TIMES BESTSELLER
THIS IS HOW THEY TELL ME THE WORLD ENDS
The Cyber-Weapons Arms Race
BUSINESS BOOK OF THE YEAR 2021 WINNER
Nicole Perlroth
"Part John le Carré and more parts Michael Crichton . . . spellbinding."
—THE NEW YORKER
BLOOMSBURY


SANDWORM
A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers
andy greenberg
"Like the best true-crime writing, [Greenberg's] narrative is both perversely entertaining and terrifying." —The New York Review of Books


Copyrighted Material
Digital Health
Understanding the Benefit-Risk Patient-Provider Framework
Eric D. Perakslis & Martin Stanley
Foreword by Erin Brodwin
Copyrighted Material