ITU KALEIDOSCOPE
ATLANTA 2019

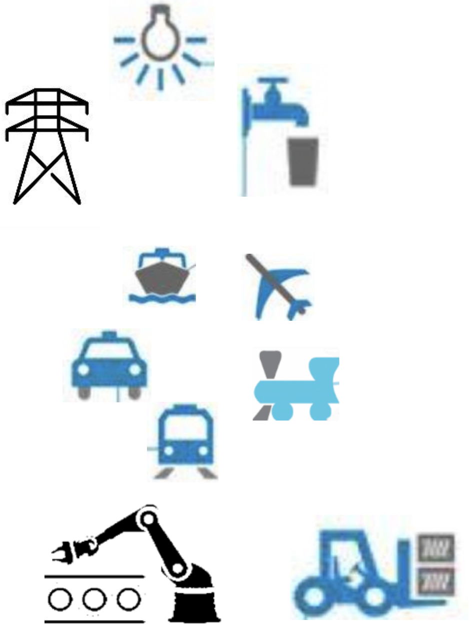
Cyber-Safety in Healthcare IoT

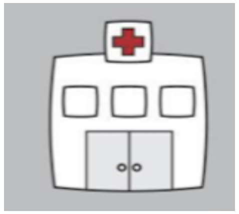
Duncan Sparrell
sFractal Consulting
duncan@sfractal.com
@dsparrell

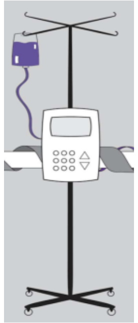
4-6 December
Atlanta, Georgia, USA

Fractal Consulting LLC
the closer you look, the more you see

```
1010111001010001111011010l
0xFF 0x8E 0xBC 0xA2 0x7E 0x00
1110010100011110110101001l
0x75 0x8E 0xBC 0xA2 0x7E 0x11
1010111001010001111011010l
 0xA2 0x7E 0x00 0xFF 0x8E 0xBC
1110010100011110110101001l
0xBC 0xA2 0x75 0x8E 0x7E 0x11
```



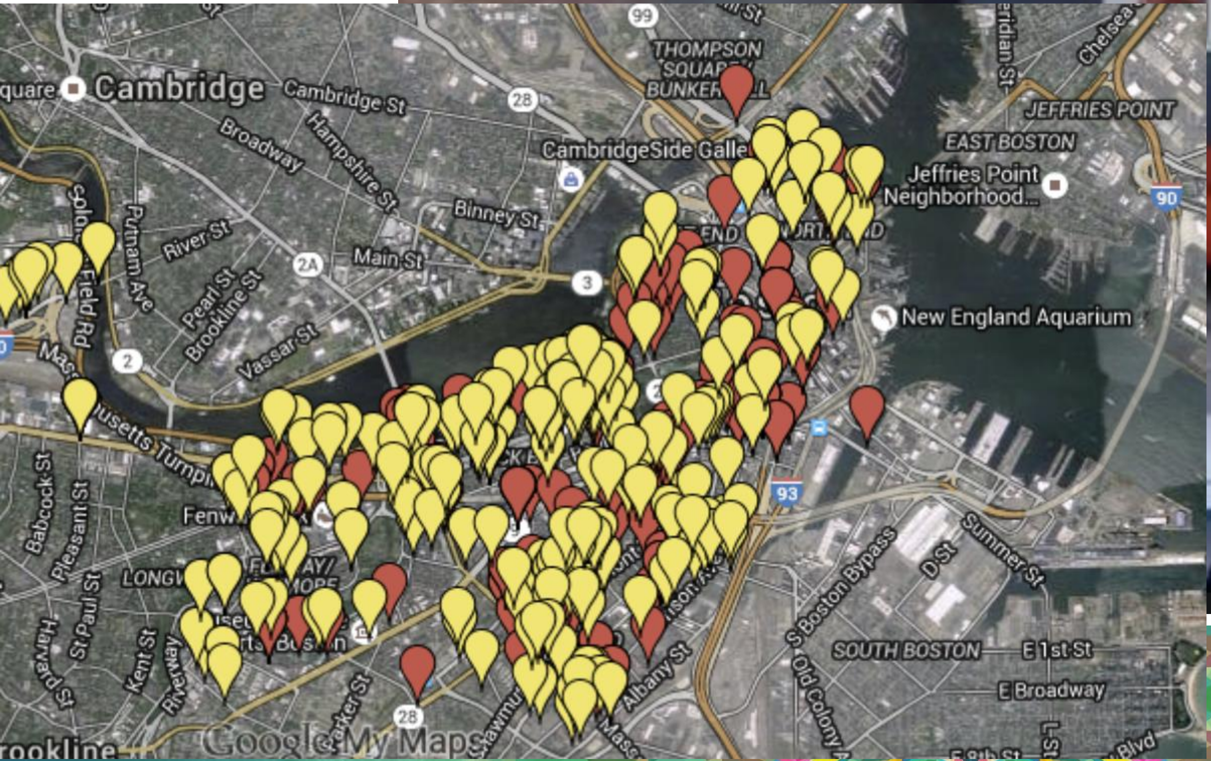




Where to insert the wedge?

Deepwater Horizon

Utilities


Cambridge
Cambridge St
Broadway
Hampshire St
Binney St
River St
Main St
Pearl St
Brookline St
Vassar St
Putnam Ave
Field Rd
CambridgeSide Galle
THOMPSON SQUARE
BUNKER HILL
EAST BOSTON
JEFFRIES POINT
Jeffries Point Neighborhood...
New England Aquarium
Chelsea
Meridian St
Summer St
D St
S Boston Bypass
Old Colony
SOUTH BOSTON
E 1st St
E Broadway
Albany St
Massachusetts Turnpike
Babcock St
Pleasant St
St Paul St
Harvard St
Kent St
Riverway
Fenway
Brookline
Google My Maps
99
28
2A
3
2
90
93
28

#RSAC
RSAConference2018
#RSAC
RSAConference2018
RSAC

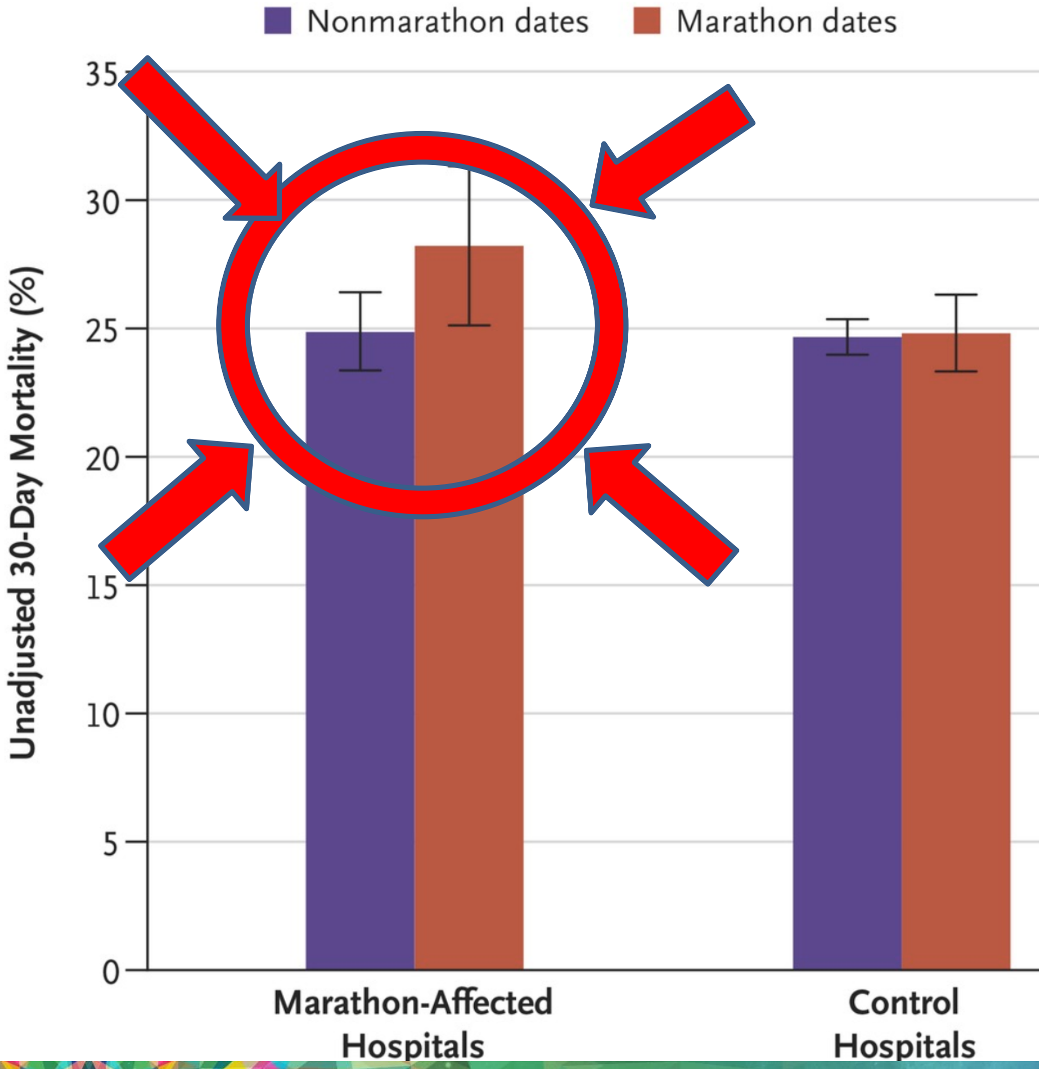
The NEW ENGLAND JOURNAL of MEDICINE

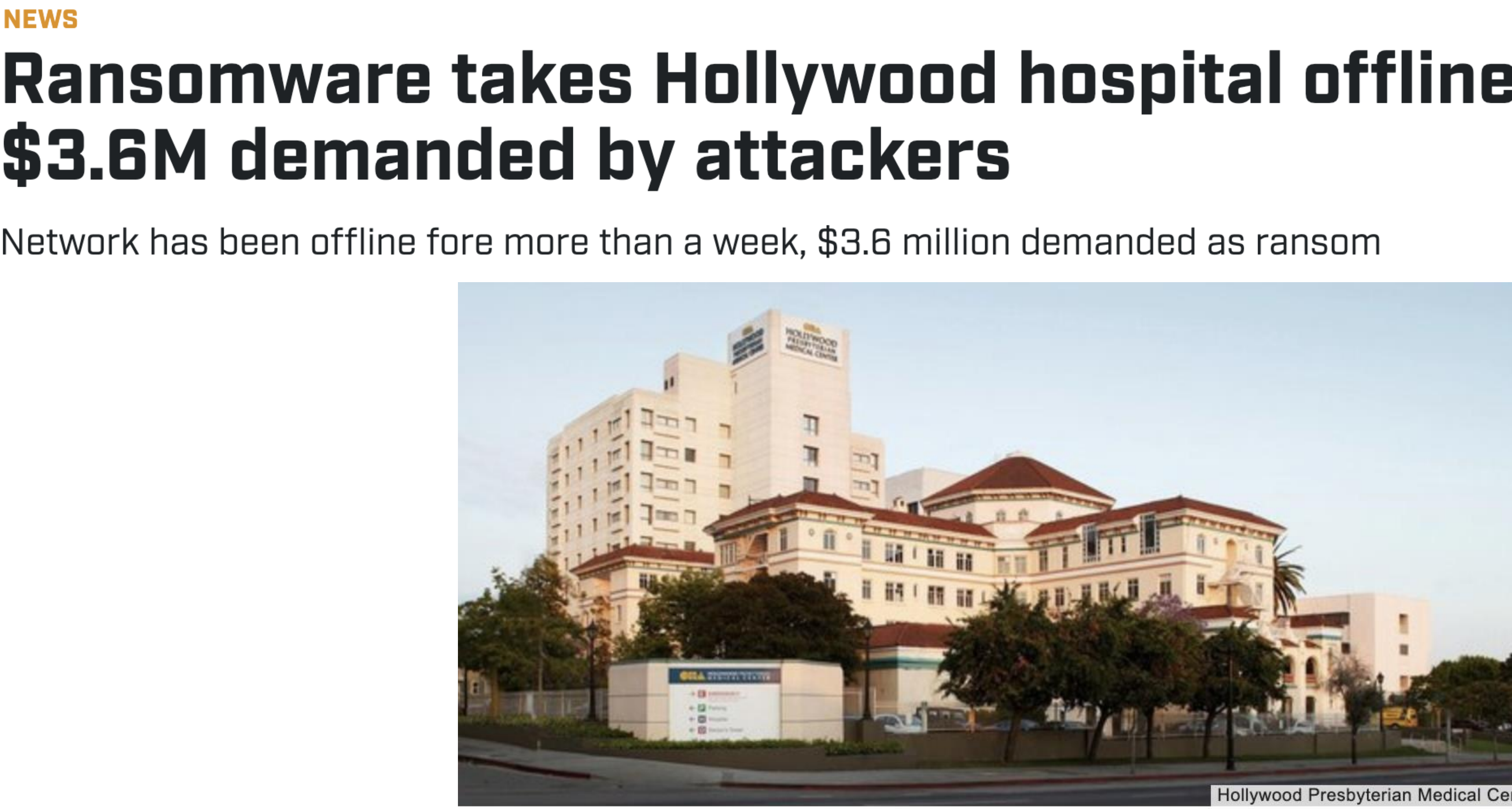
Special Article

Delays in Emergency Care And Mortality During Major U.S. Marathons

Anupam B. Jena, M.D., Ph.D.,
N. Clay Mann, Ph.D.,
Leia N. Wedlund,
Andrew Olenski, B.S.

13 April 2017



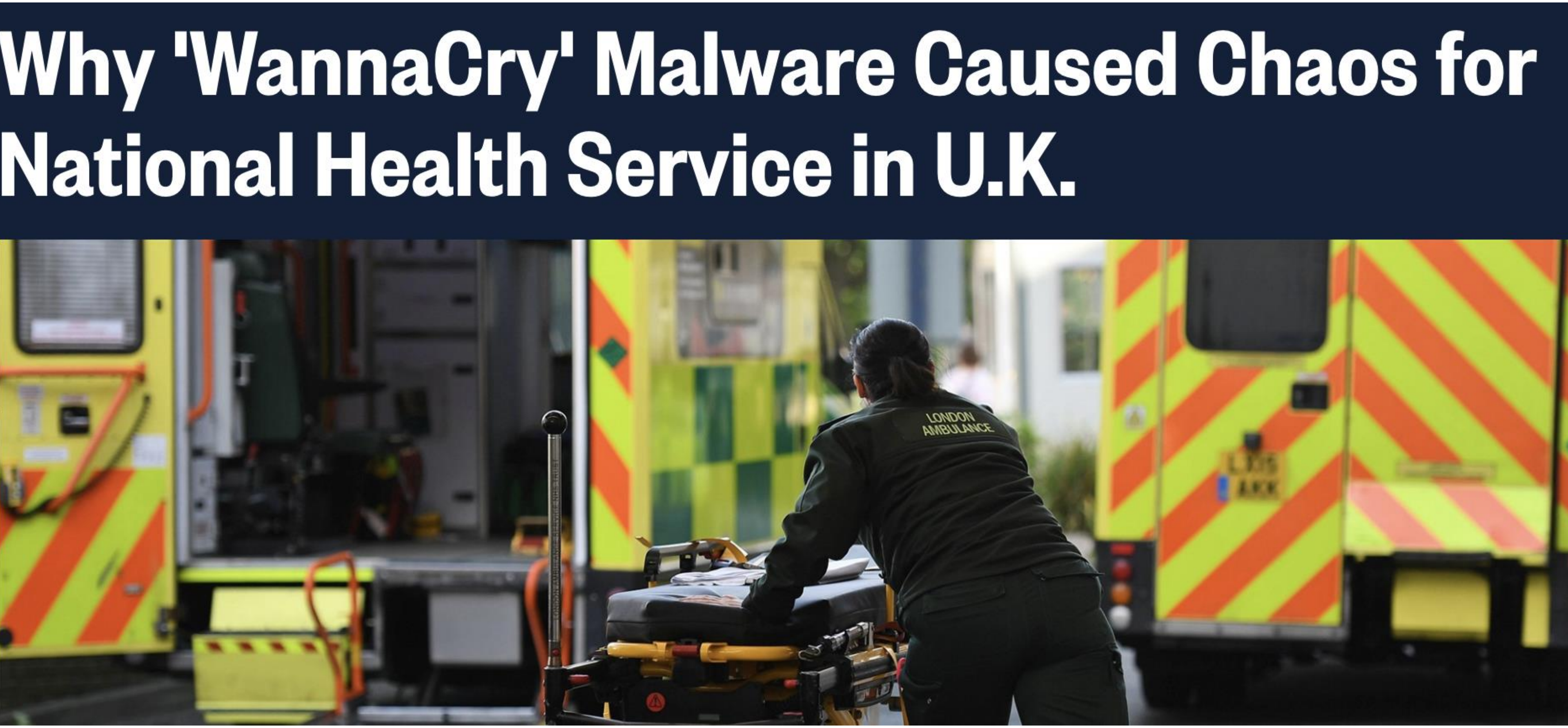


NEWS

Ransomware takes Hollywood hospital offline
$3.6M demanded by attackers

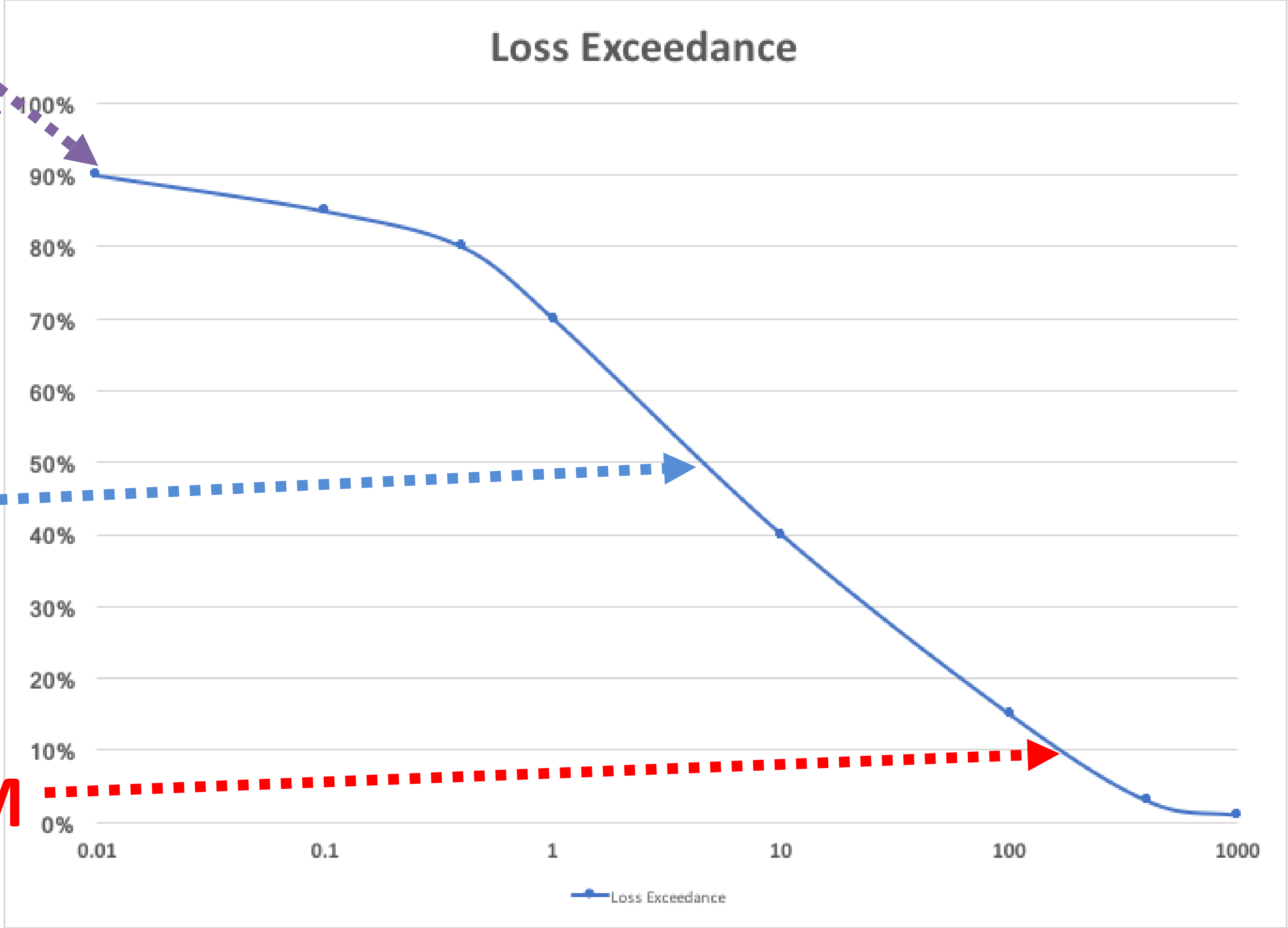
Network has been offline fore more than a week, $3.6 million demanded as ransom

Hollywood Presbyterian Medical Ce



Why 'WannaCry' Malware Caused Chaos for National Health Service in U.K.

Use Science (not Fear) to size Cybersecurity Budgets



90% > $10K

50% > $5M

10% > $110M

Comparing Alternatives

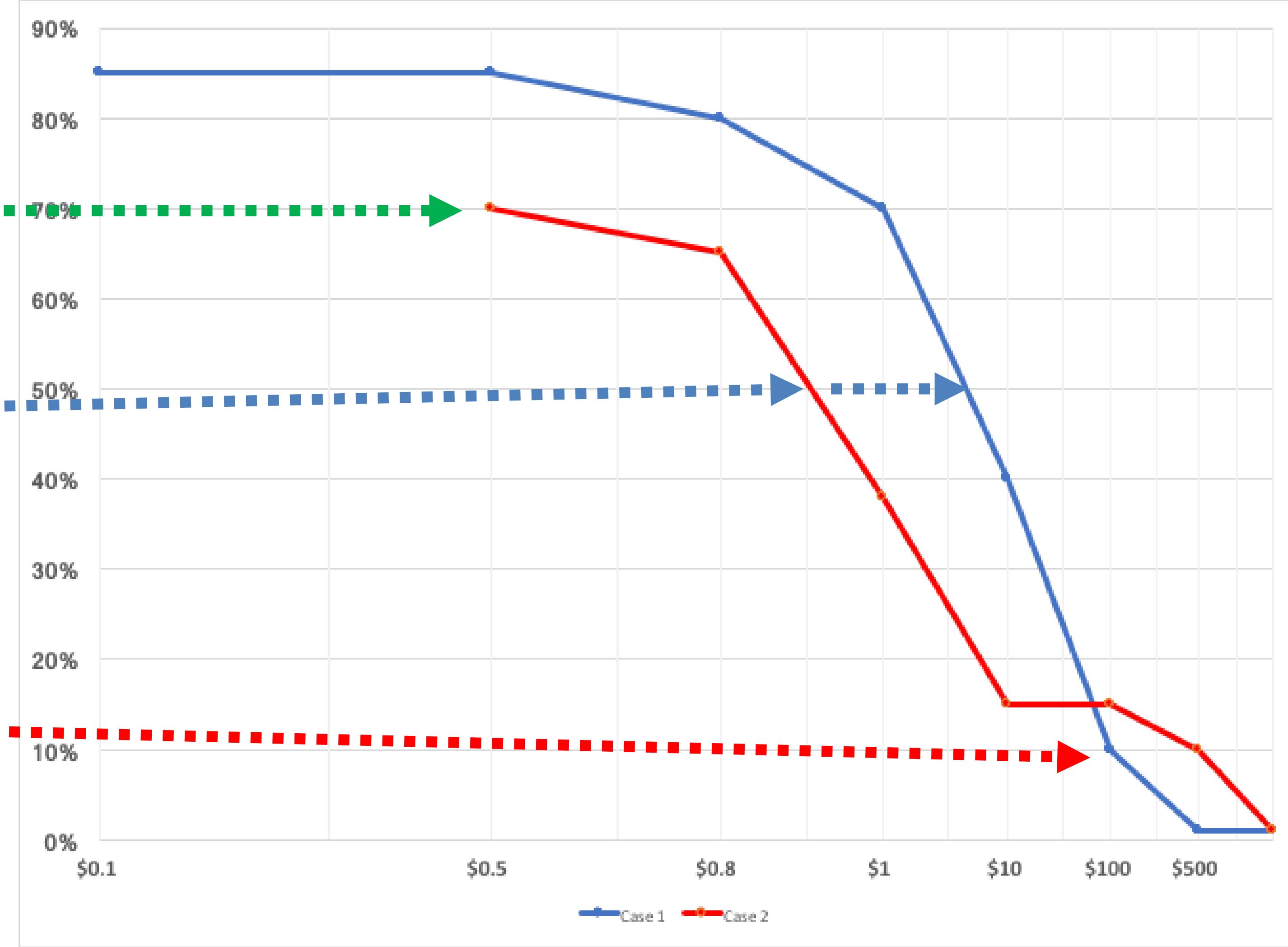
100% $500K

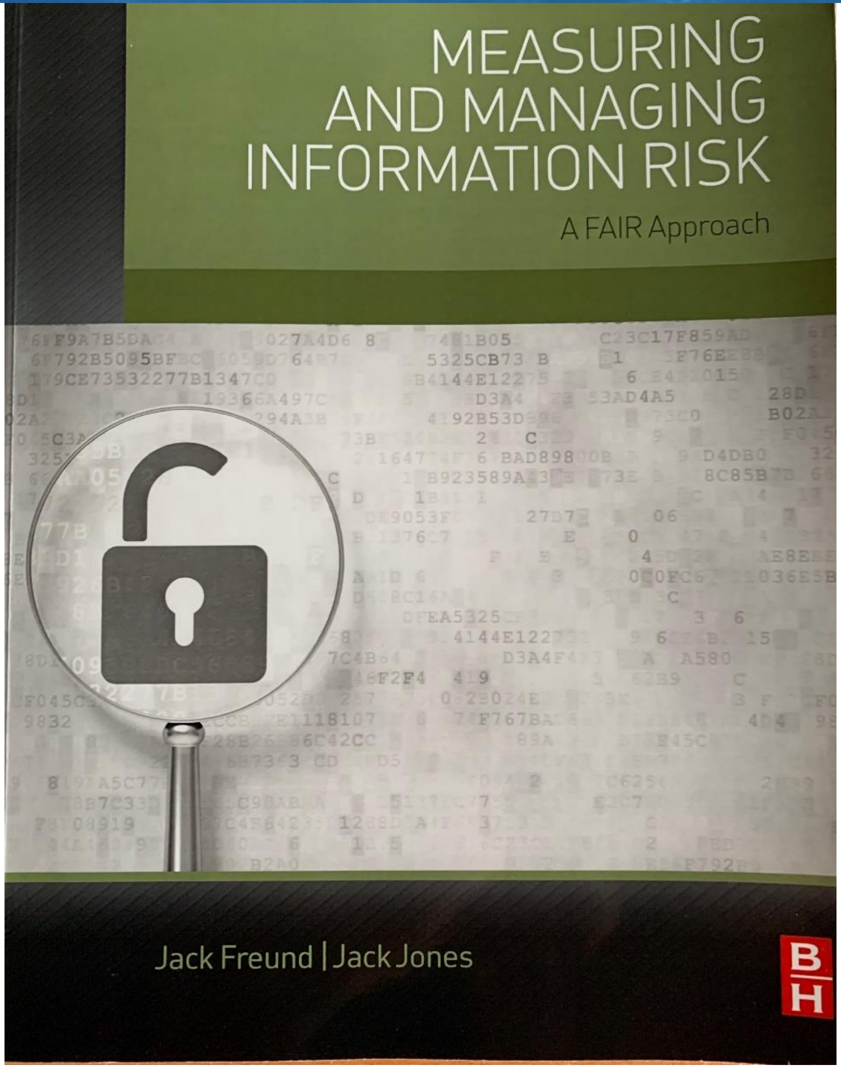
(purchase cost)

$4.1M Savings

($900K vs $5M MLV)

Increased Risk





MEASURING AND MANAGING INFORMATION RISK

A FAIR Approach

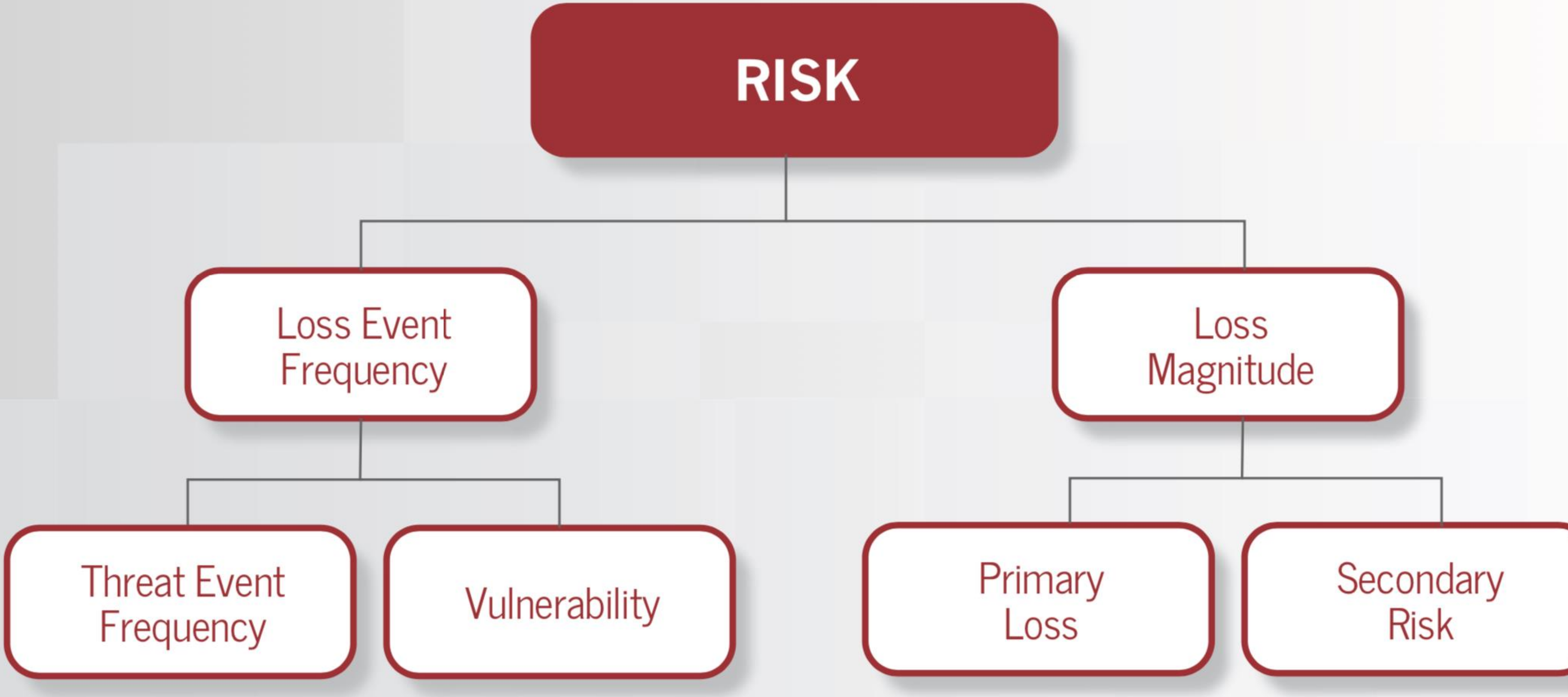
Jack Freund | Jack Jones

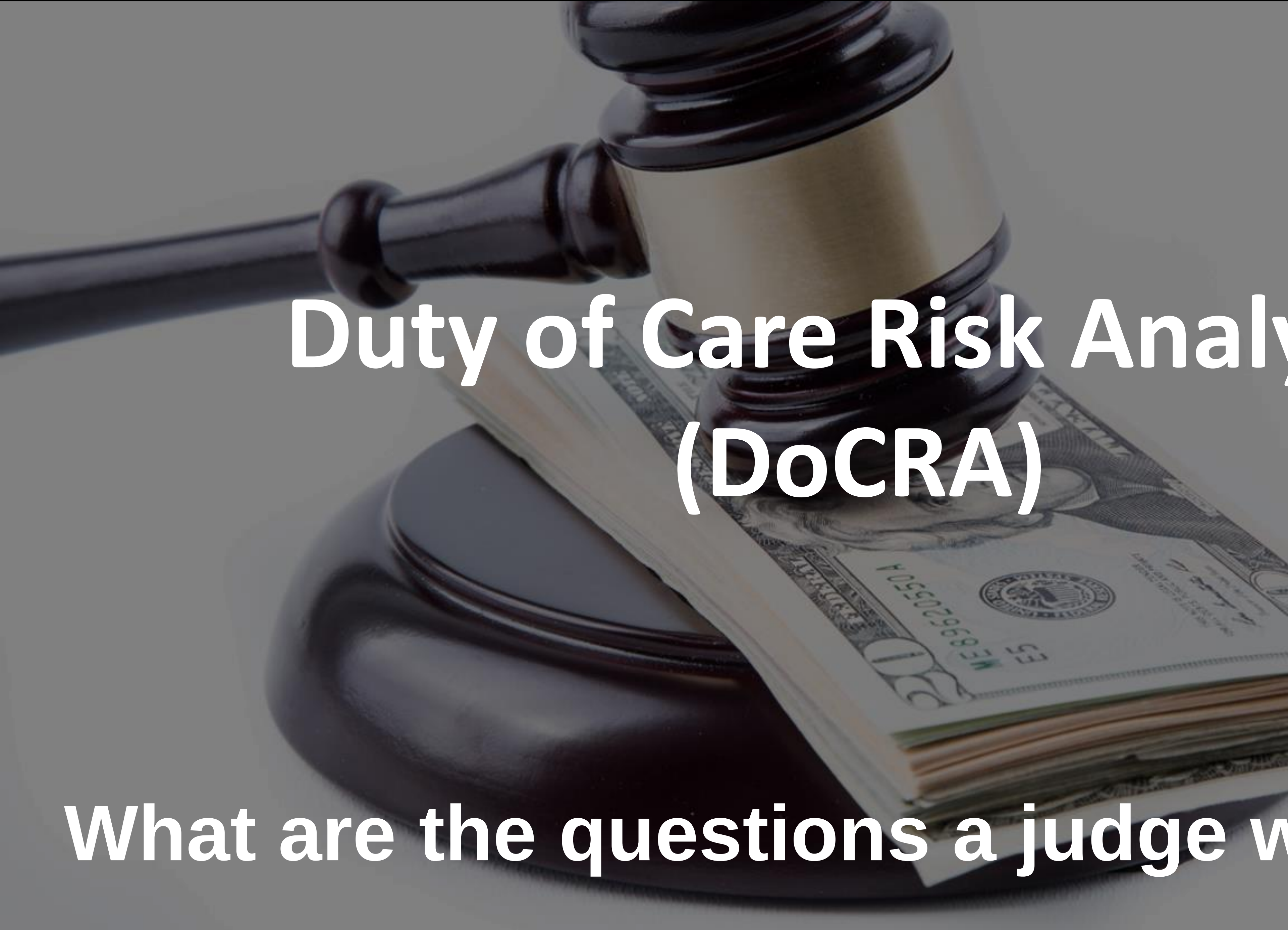
“In our experience
working with organizations of various sizes
in various industries,
we’ve found that between
70% and 90% of the “high risk” issues
these organizations are focused on
do not, in fact, represent high risk.”

Jack Jones

Co-Founder FAIR Institut

Factor Analysis of Information Risk





Duty of Care Risk Analy
(DoCRA)

What are the questions a judge w

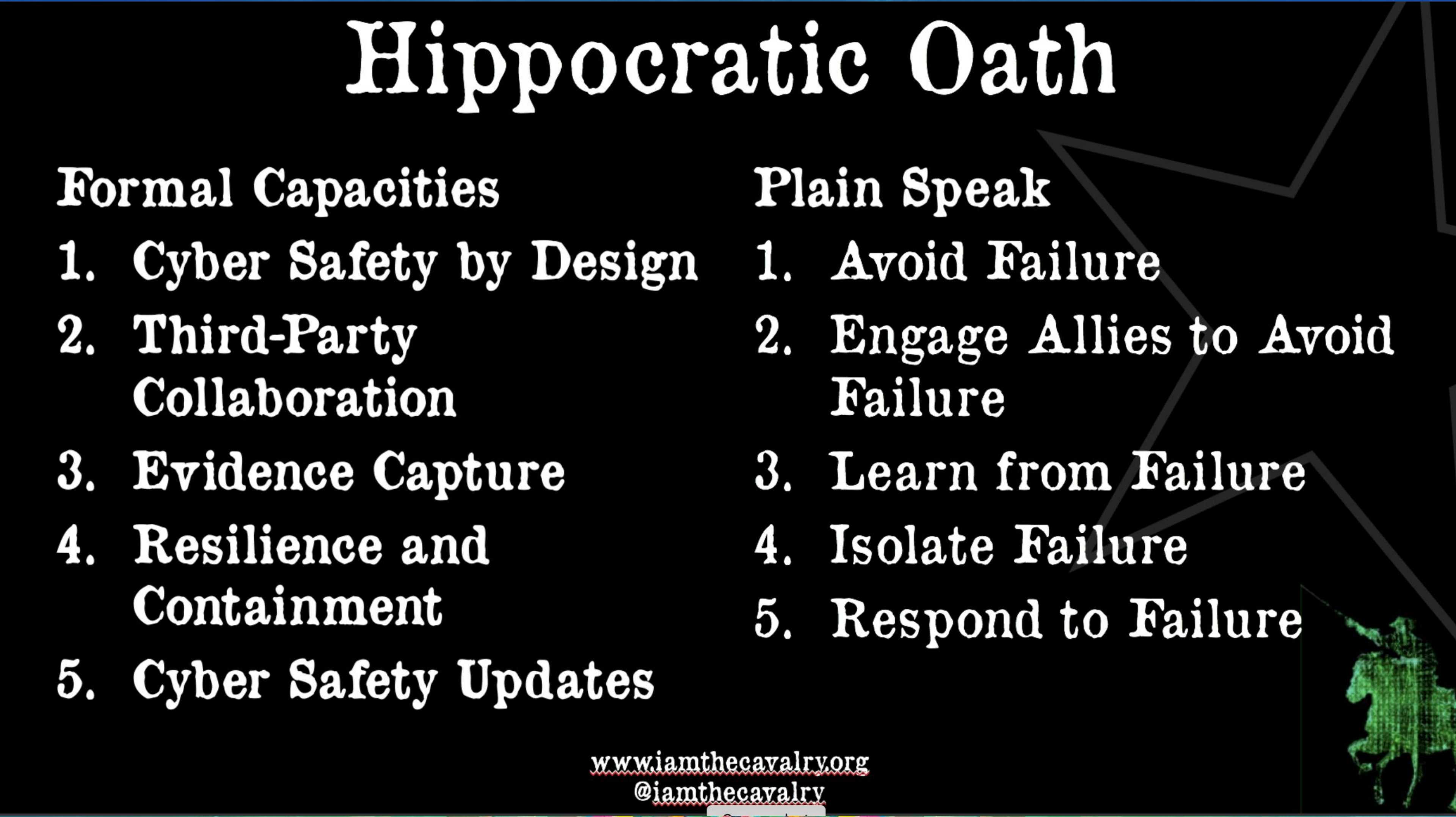
I Am The Cavalry

The Cavalry isn’t coming … It falls to us

Medical
Automotive
Connected Home
Public Infrastructure

Mission Statement

To ensure connected technologies
with the potential
to impact public safety and human life
are worthy of our trust.



Hippocratic Oath

Formal Capacities

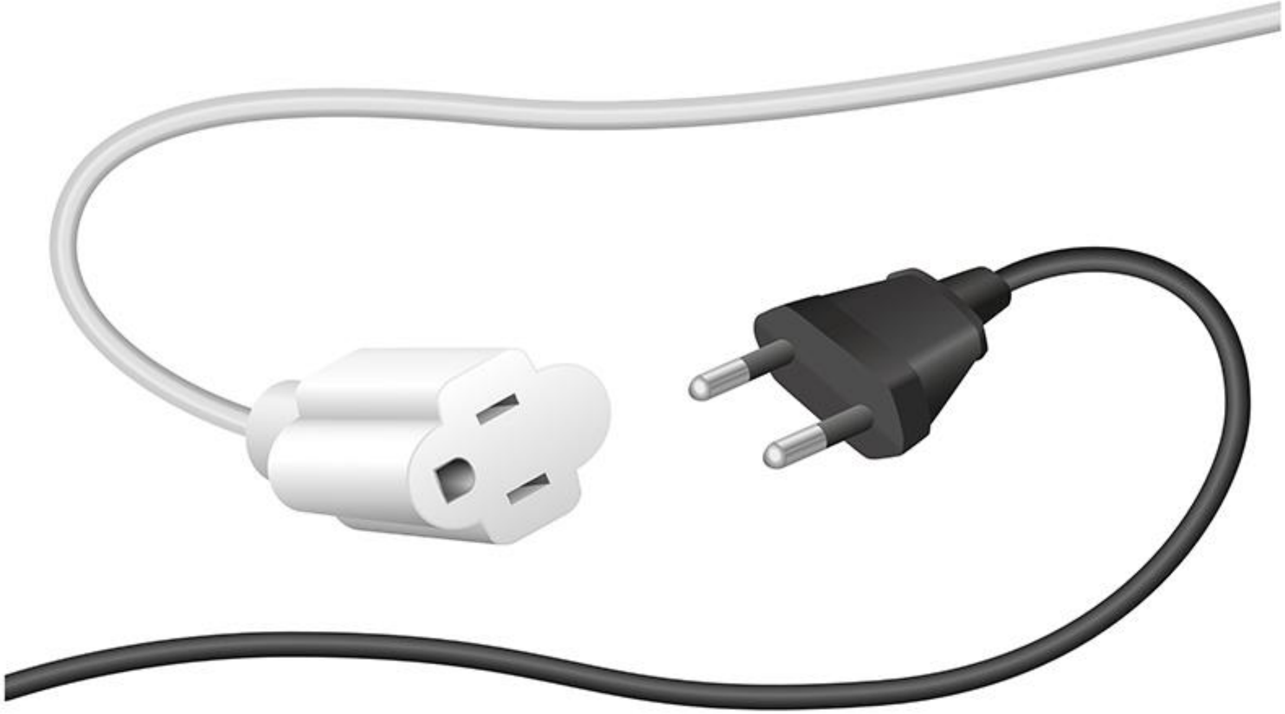
1. Cyber Safety by Design
2. Third-Party Collaboration
3. Evidence Capture
4. Resilience and Containment
5. Cyber Safety Updates

Plain Speak

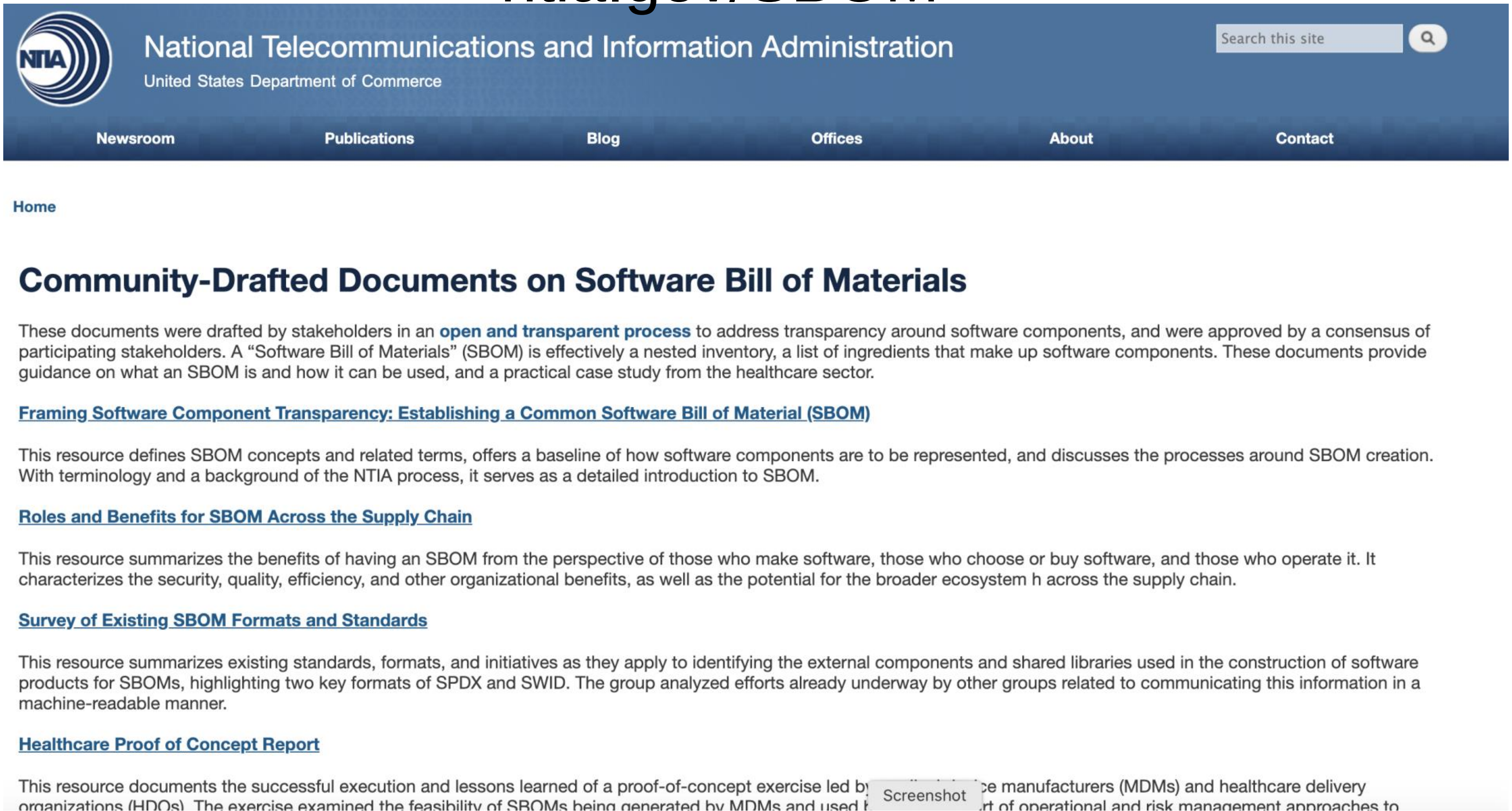
1. Avoid Failure
2. Engage Allies to Avoid Failure
3. Learn from Failure
4. Isolate Failure
5. Respond to Failure

www.iamthecavalry.org
@iamthecavalry

If you can't protect it, don't connect it



ntia.gov/SBOM


NTIA
National Telecommunications and Information Administration
United States Department of Commerce
Search this site
Newsroom
Publications
Blog
Offices
About
Contact
Home
Screenshot

Community-Drafted Documents on Software Bill of Materials

These documents were drafted by stakeholders in an **open and transparent process** to address transparency around software components, and were approved by a consensus of participating stakeholders. A “Software Bill of Materials” (SBOM) is effectively a nested inventory, a list of ingredients that make up software components. These documents provide guidance on what an SBOM is and how it can be used, and a practical case study from the healthcare sector.

Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)

This resource defines SBOM concepts and related terms, offers a baseline of how software components are to be represented, and discusses the processes around SBOM creation. With terminology and a background of the NTIA process, it serves as a detailed introduction to SBOM.

Roles and Benefits for SBOM Across the Supply Chain

This resource summarizes the benefits of having an SBOM from the perspective of those who make software, those who choose or buy software, and those who operate it. It characterizes the security, quality, efficiency, and other organizational benefits, as well as the potential for the broader ecosystem h across the supply chain.

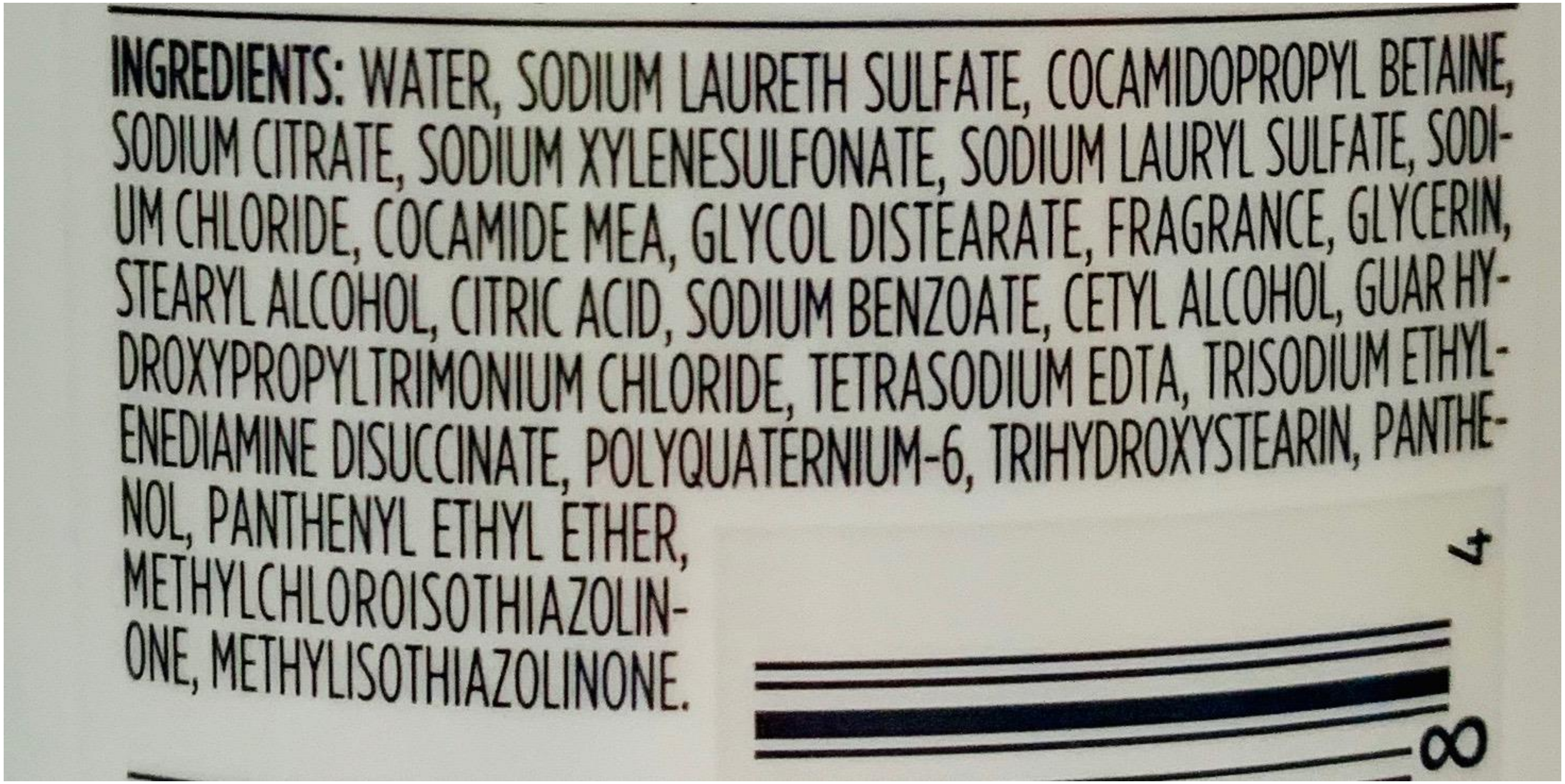
Survey of Existing SBOM Formats and Standards

This resource summarizes existing standards, formats, and initiatives as they apply to identifying the external components and shared libraries used in the construction of software products for SBOMs, highlighting two key formats of SPDX and SWID. The group analyzed efforts already underway by other groups related to communicating this information in a machine-readable manner.

Healthcare Proof of Concept Report

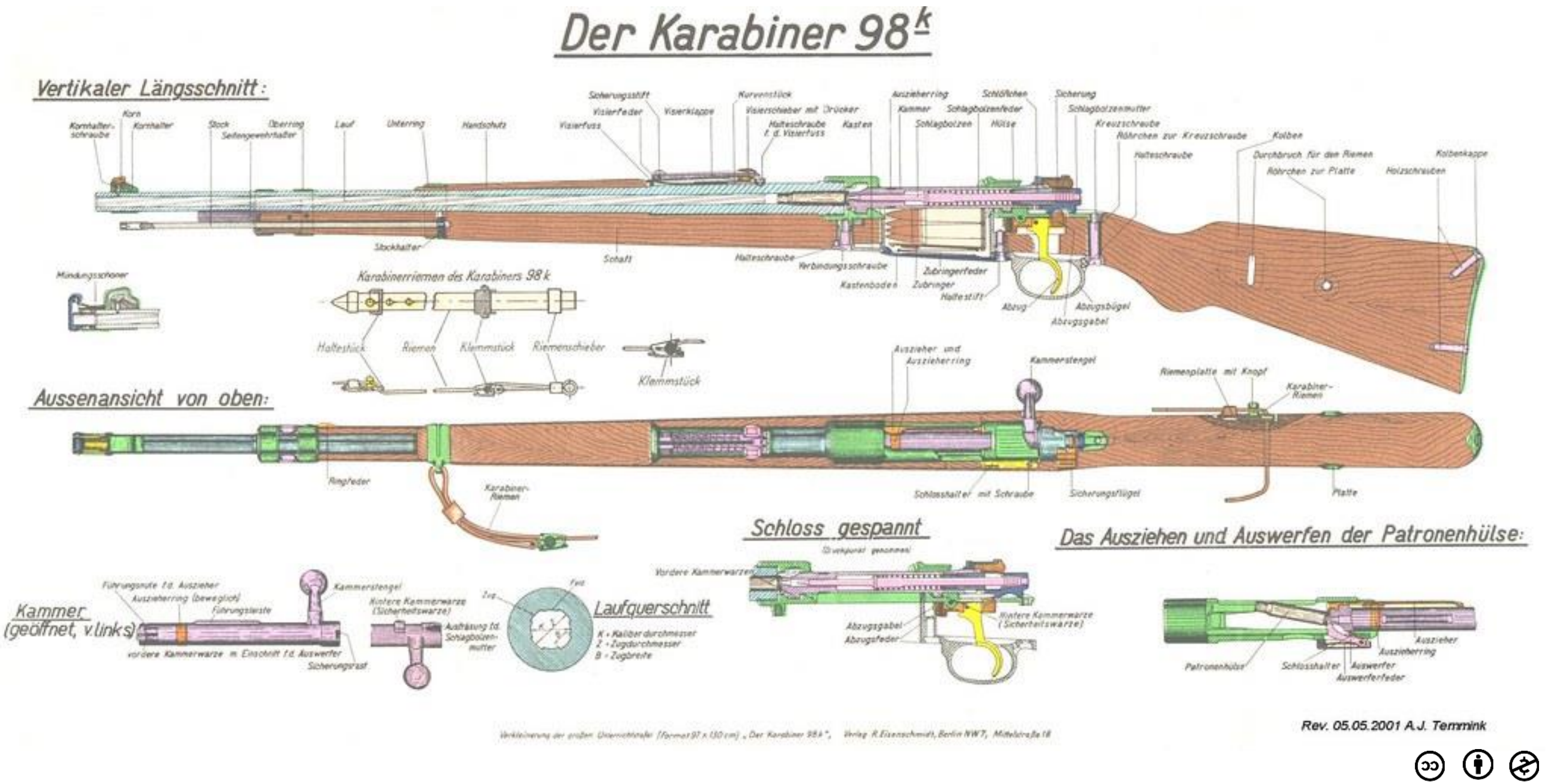
This resource documents the successful execution and lessons learned of a proof-of-concept exercise led by ce manufacturers (MDMs) and healthcare delivery organizations (HDOs). The exercise examined the feasibility of SBOMs being generated by MDMs and used b rt of operational and risk management approaches to

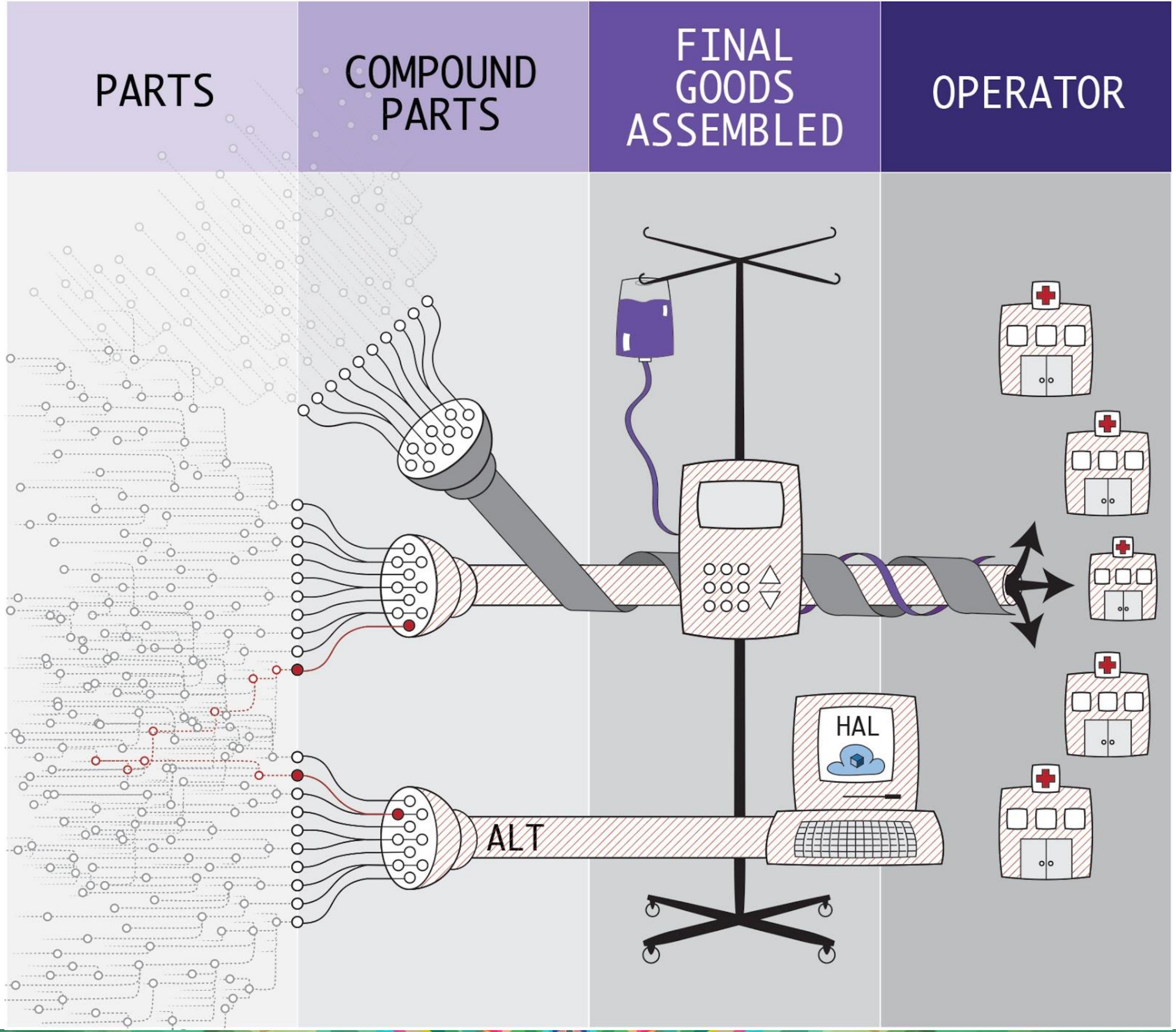
All analogies are wrong, some are useful



INGREDIENTS: WATER, SODIUM LAURETH SULFATE, COCAMIDOPROPYL BETAINE, SODIUM CITRATE, SODIUM XYLENESULFONATE, SODIUM LAURYL SULFATE, SODIUM CHLORIDE, COCAMIDE MEA, GLYCOL DISTEARATE, FRAGRANCE, GLYCERIN, STEARYL ALCOHOL, CITRIC ACID, SODIUM BENZOATE, CETYL ALCOHOL, GUAR HYDROXYPROPYLTRIMONIUM CHLORIDE, TETRASODIUM EDTA, TRISODIUM ETHYLENEDIAMINE DISUCCINATE, POLYQUATERNIUM-6, TRIHYDROXYSTEARIN, PANTHENOL, PANTHENYL ETHYL ETHER, METHYLCHLOROISOTHIAZOLINONE, METHYLISOTHIAZOLINONE.

All analogies are wrong, some are useful



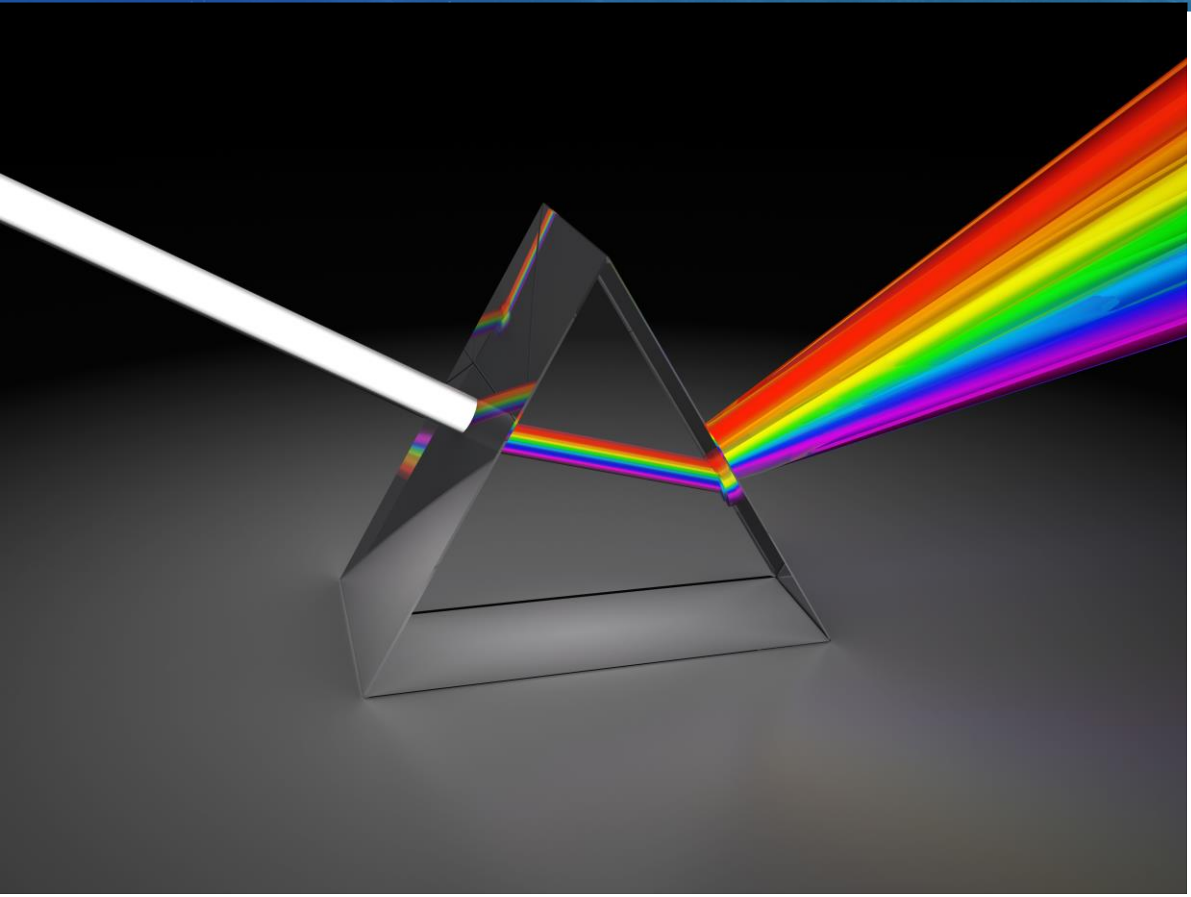

PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR
HAL
ALT

Supply chain perspectives

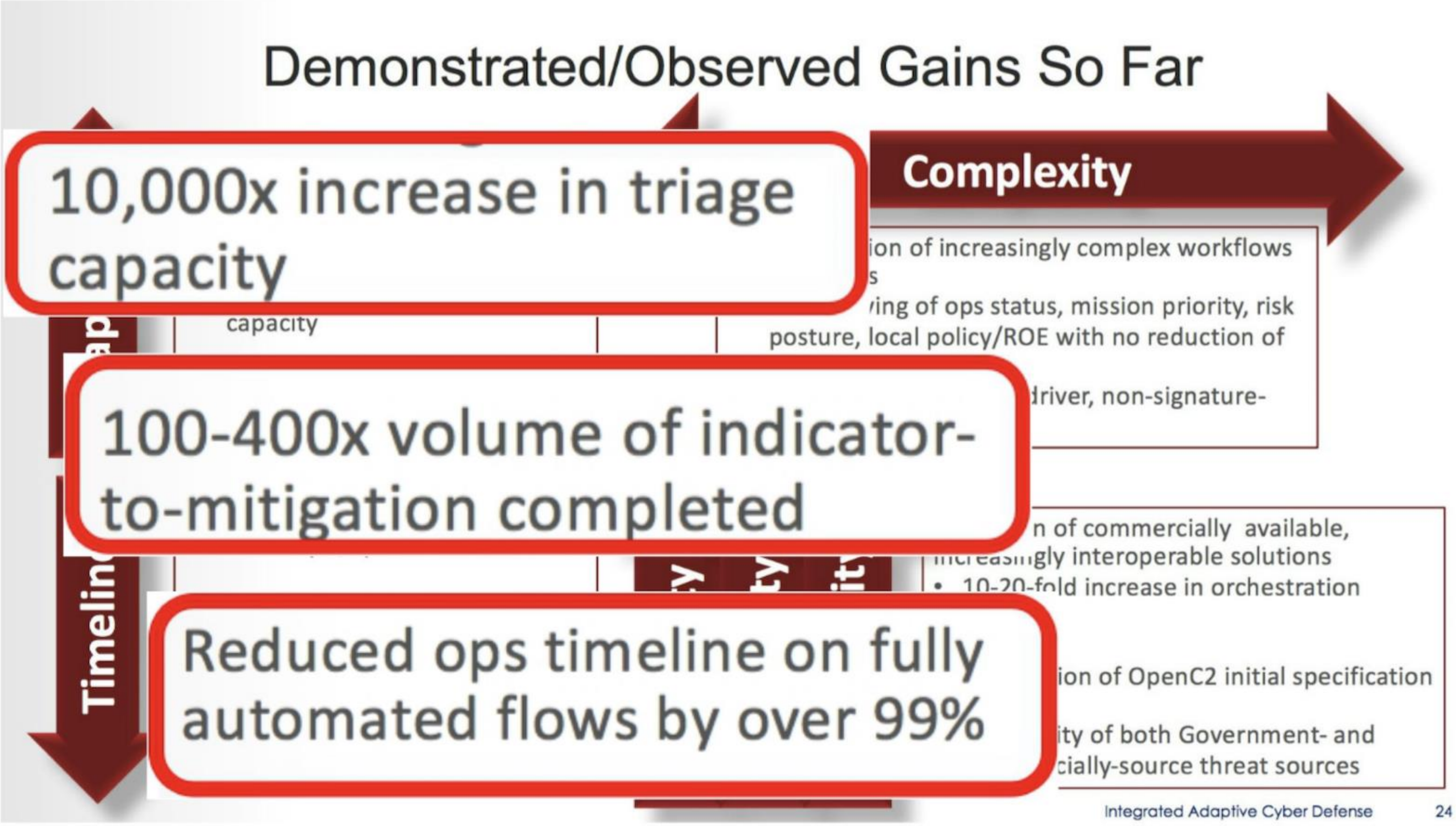
- **Produce**
  - the person/organization that creates a software component or software for use by others [write/create/assemble/package]
- **Choose**
  - the person/organization that decides the software/products/suppliers for use [purchase/acquire/source/select/approve]
- **Operate**
  - the person/organization that operates the software component [uses/monitor/maintain/defend/respond]

SBoM Benefits

- Cost
- Security
- License
- Compliance
- High Assurance



From the speed of light
To the speed of lawyers



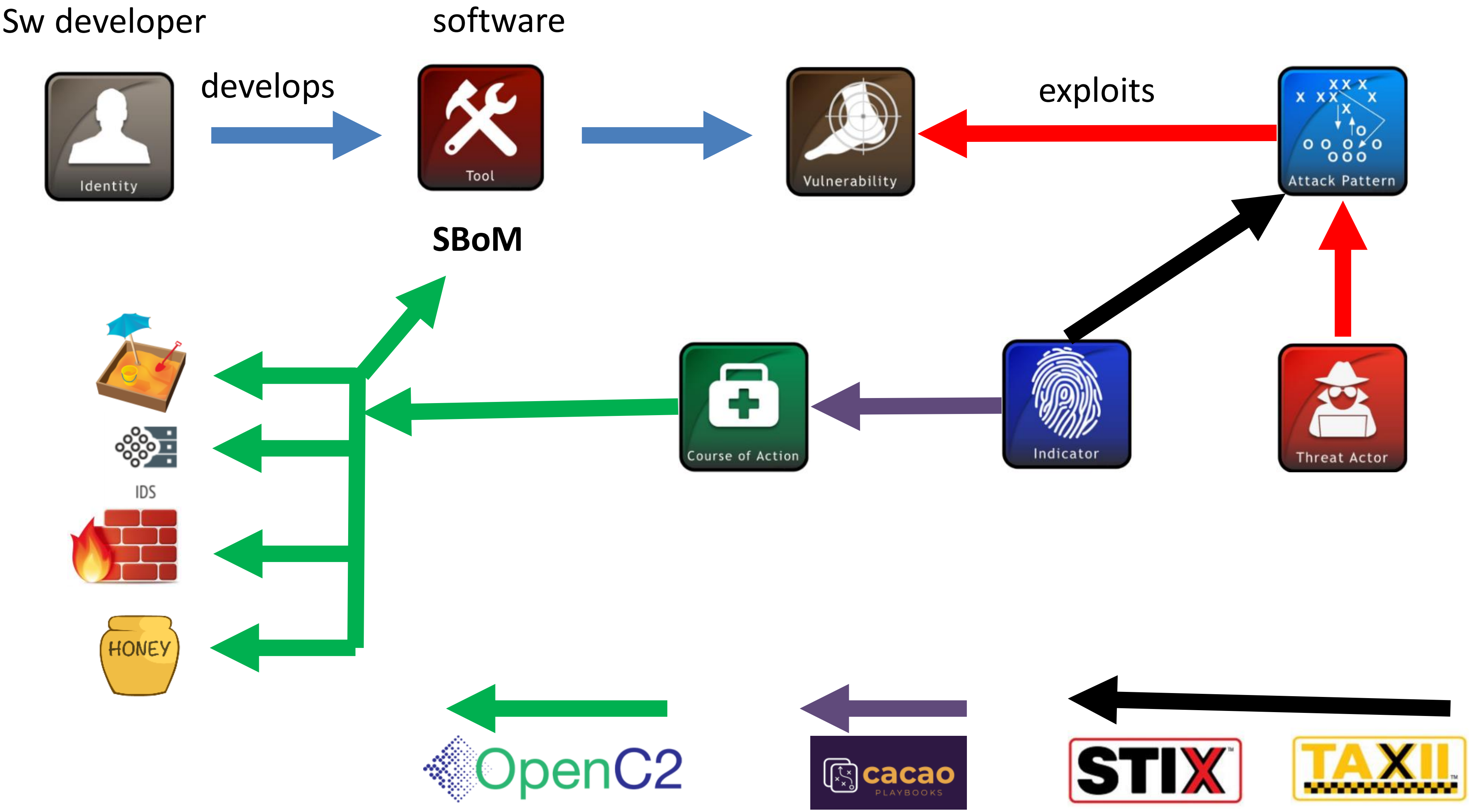
Demonstrated/Observed Gains So Far

10,000x increase in triage capacity

100-400x volume of indicator-to-mitigation completed

Reduced ops timeline on fully automated flows by over 99%

Complexity
Timeline
capacity
ion of increasingly complex workflows
s
ving of ops status, mission priority, risk
posture, local policy/ROE with no reduction of
driver, non-signature-
n of commercially available,
increasingly interoperable solutions
• 10-20-fold increase in orchestration
ion of OpenC2 initial specification
ity of both Government- and
cially-source threat sources
Integrated Adaptive Cyber Defense
24


Sw developer
software
develops
Identity
Tool
Vulnerability
exploits
Attack Pattern
SBoM
IDS
HONEY
Course of Action
Indicator
Threat Actor
OpenC2
cacao
PLAYBOOKS
STIX
TAXII

Takeaways

"PC020195" by EdKopp4 is licensed under CC BY-NC-SA 2.0

- Think Evilly, Act Ethically
- Loss exceedance curves
- If you can't protect it,
  don't connect it
- Require SBoM's
- Automate & Share
  - OpenC2,
  - CACAO,
  - STIX/TAXII

“There is never enough time,
Thank you for yours.”

Dan Geer

ITU KALEIDOSCOPE
ATLANTA 2019

Thank you