

# Cyber-Physical Safety

Where Bits & Bytes Meet Flesh & Blood

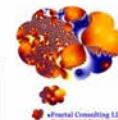
Duncan Sparrell  
Rochester Security Summit  
2-3 Oct, 2019



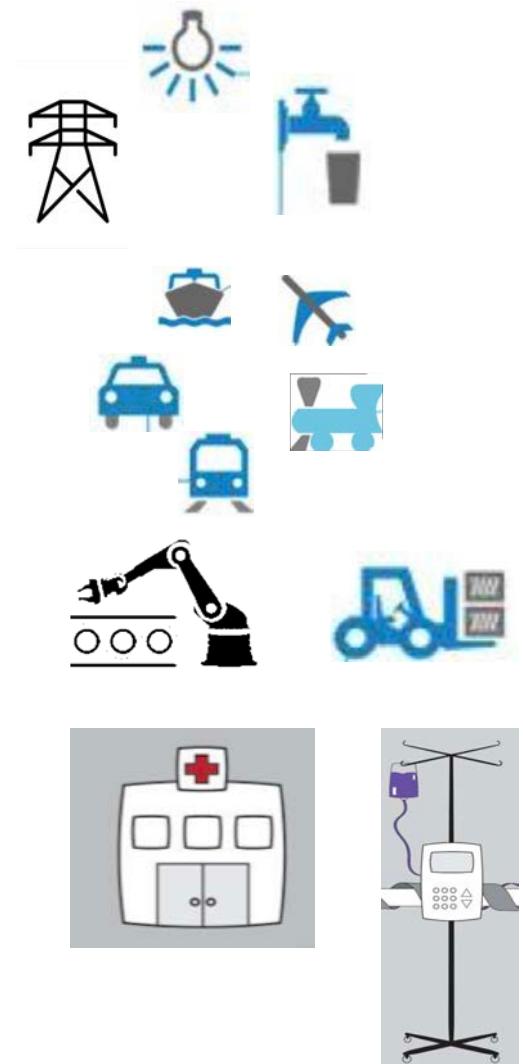
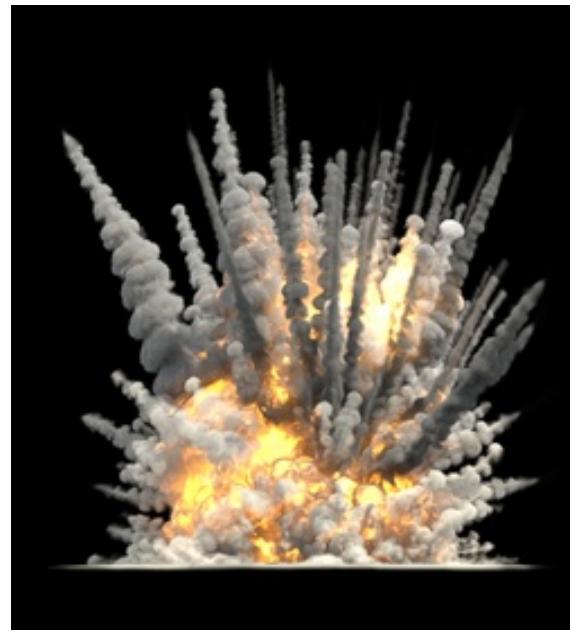
THINK EVILLY



Act Ethically



```
10101110010100011110110101  
0xFF 0x8E 0xBC 0xA2 0x7E 0x00  
11100101000111101101010011  
0x75 0x8E 0xBC 0xA2 0x7E 0x11  
10101110010100011110110101  
0xA2 0x7E 0x00 0xFF 0x8E 0xBC  
11100101000111101101010011  
0xBC 0xA2 0x75 0x8E 0x7E 0x11
```



# Flavors of IoT



This photo is under the [CC0 / Public Domain License](#). [Image Info](#)

# Where to insert the wedge?



CC0 from [here](#)

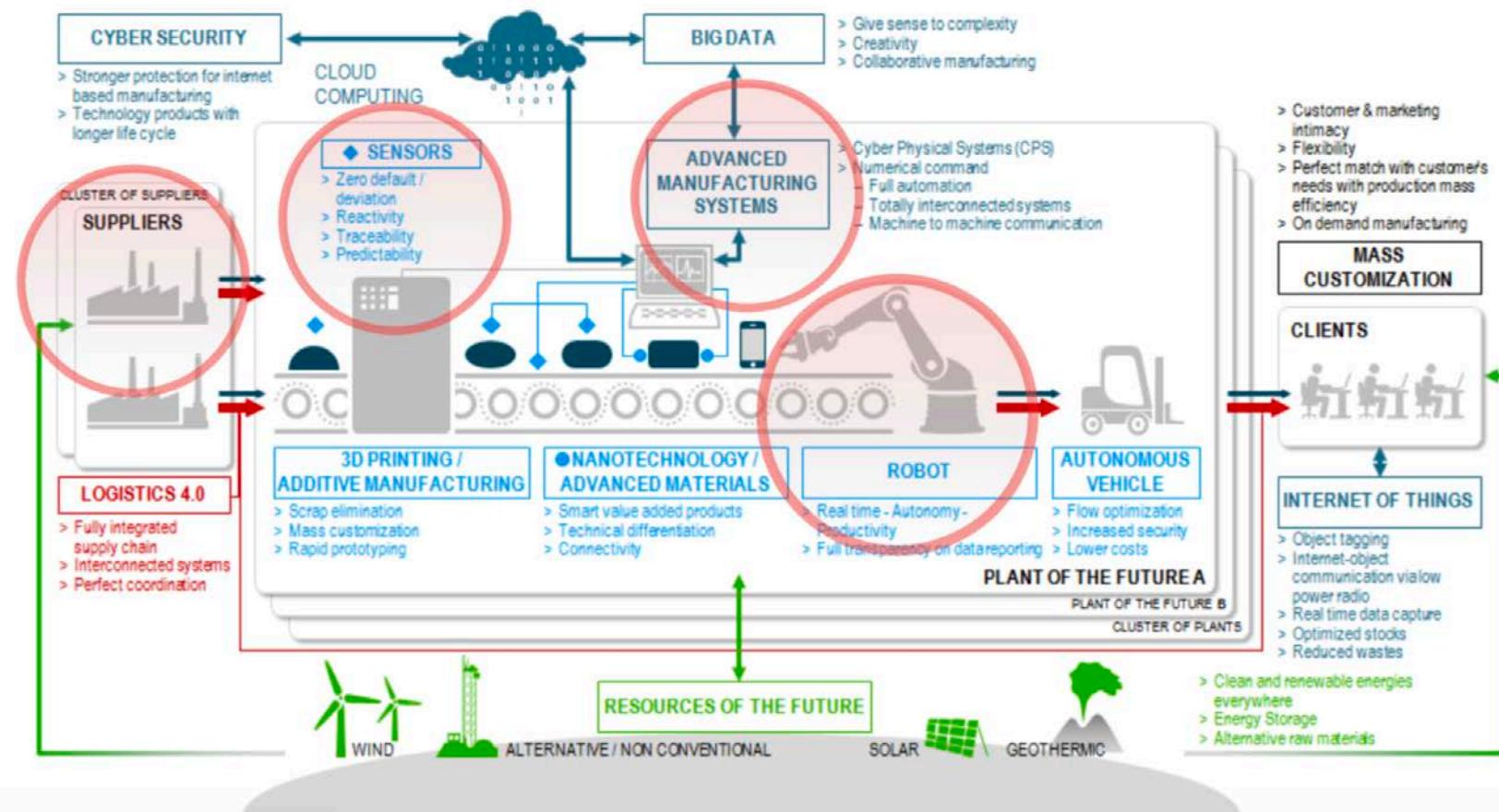


Photo credit: [Vestnikkavkaza.net](http://Vestnikkavkaza.net)

# Deepwater Horizon



# The Industry 4.0 ecosystem



# Computer Problems Caused Massive Failure Monday, Reports Say

SEPTA's system software froze on Monday night, leading to delays -

By Justin Heinze (Patch Staff) - October 25, 2016 7:26 pm ET

SF Muni hack contained. Next transit hack could be train wreck

## SF Muni hack contained. Next transit hack could be train wreck

The San Francisco transit system avoided paying a ransom to hackers who threatened to disable its rail systems. But the hack shows US infrastructure is vulnerable.

SEPTA

2015 Philadelphia train derailment



Date	May 12, 2015
Time	9:23 p.m. EDT (UTC-4)
Location	Port Richmond, Philadelphia, Pennsylvania
Coordinates	40°00'06"N 75°05'37"W
Rail line	Northeast Corridor
Operator	Amtrak
Type of incident	Derailment
Cause	Loss of situational awareness by train engineer

# Utilities







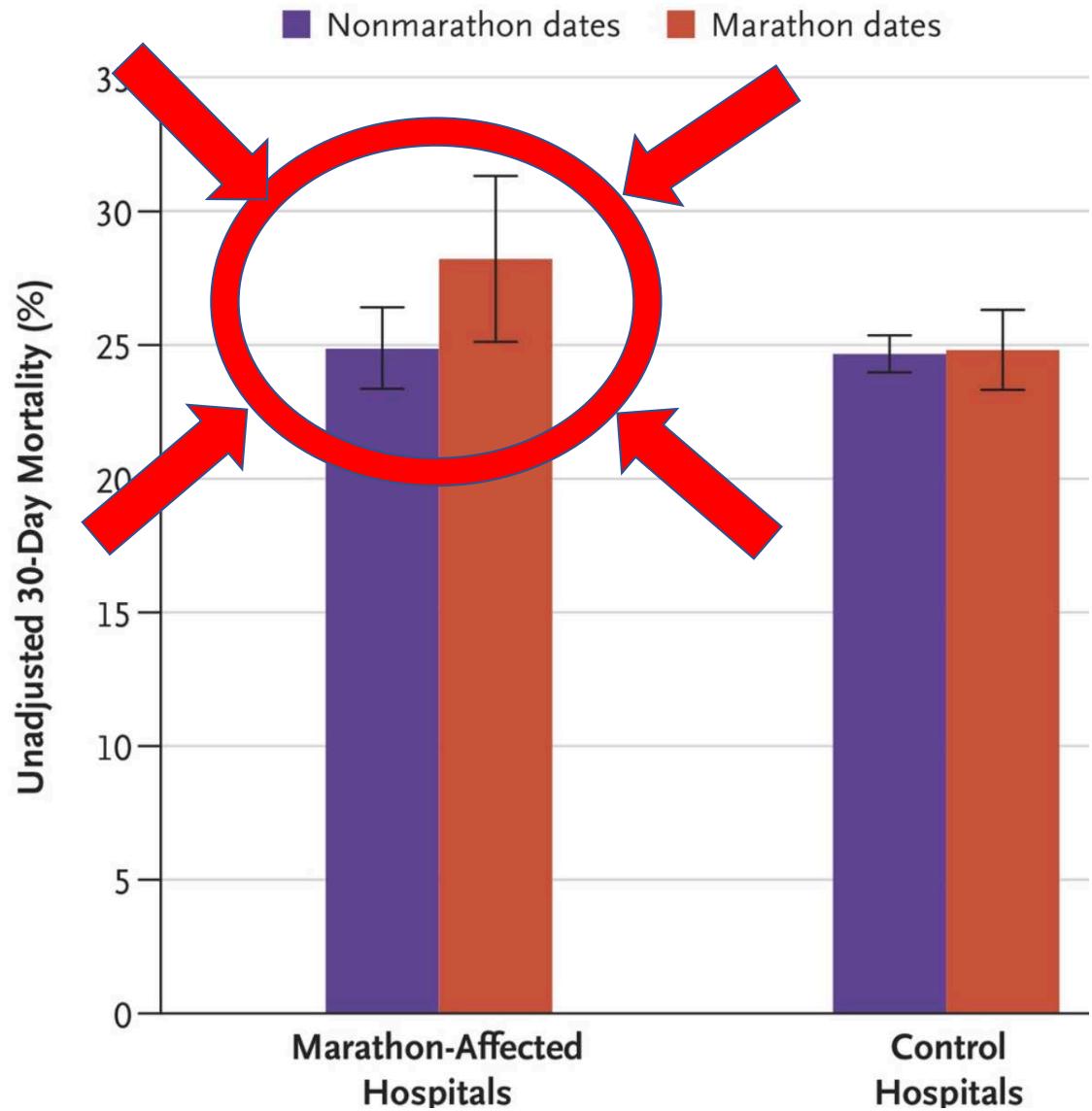
The NEW ENGLAND  
JOURNAL of MEDICINE

*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 for more than a week, \$3.6 million demanded as ransom



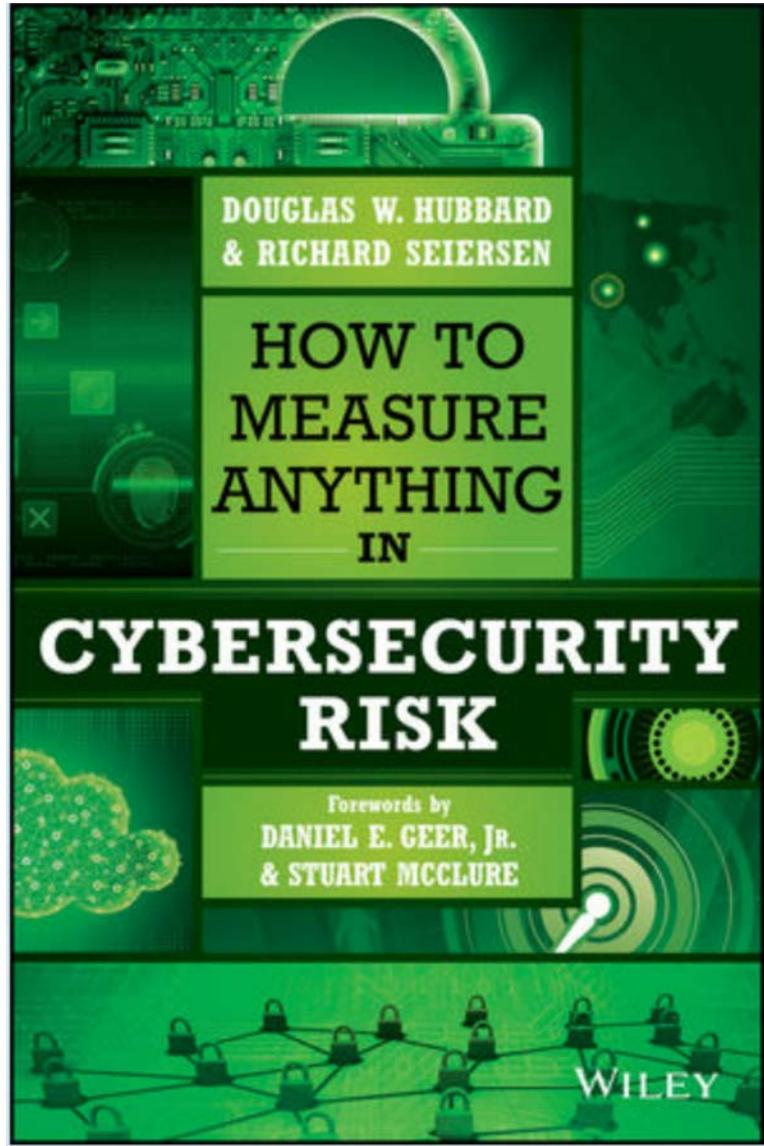
Hollywood Presbyterian Medical Center

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



## Use Science (not Fear) to size Cybersecurity Budgets





# Cybersecurity Needs to get over itself

**“there are plenty of fields  
with massive risk, minimal data,  
and profoundly chaotic actors  
that are regularly modeled  
using traditional mathematical methods”**

Hubbard & Seiersen

*How to Measure Anything in Cybersecurity Risk*

# LOSS EXCEEDANCE CURVE

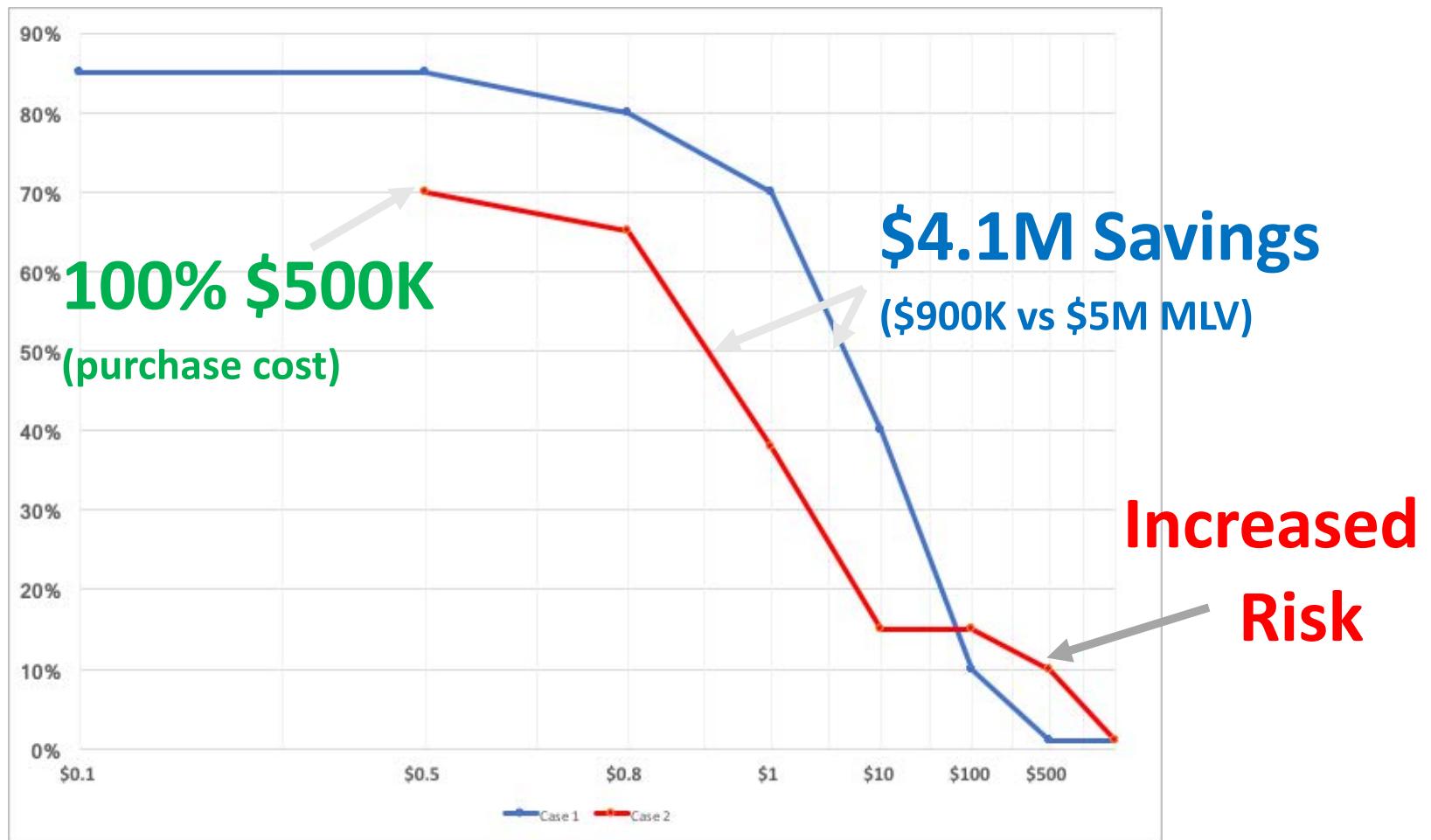
90% > \$10K



50% > \$5M

10% > \$110M

## Comparing Alternatives



# MEASURING AND MANAGING INFORMATION RISK

A FAIR Approach



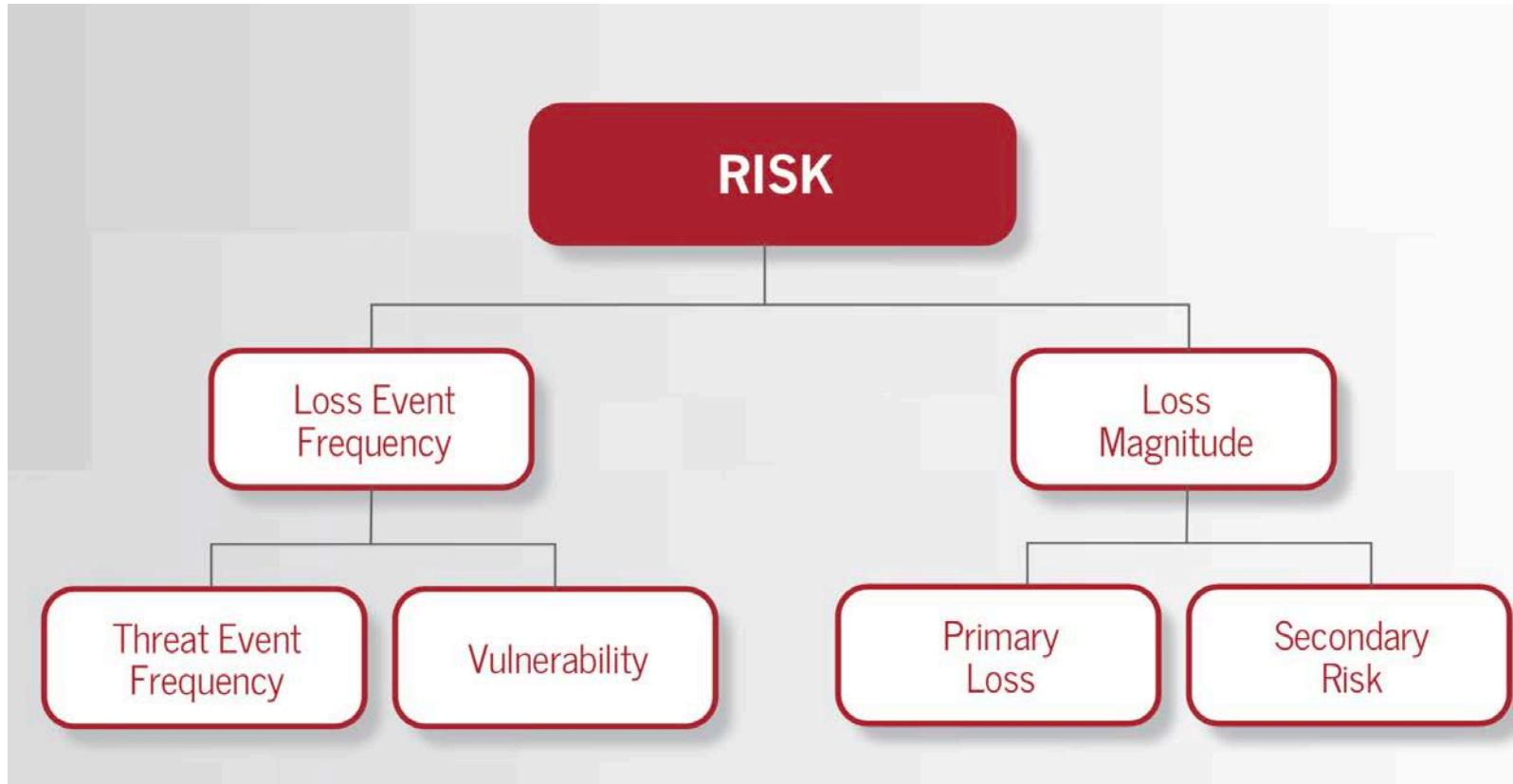
Jack Freund | Jack Jones



“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 Institute

# Factor Analysis of Information Risk



# CISQ Trustworthy Systems Manifesto



- 1. Engineering discipline in product and process**
- 2. Quality assurance to risk tolerance thresholds**
- 3. Traceable properties of system components**
- 4. Proactive defense of the system and its data**
- 5. Resilient and safe operations**

# I Am The Cavalry

The Cavalry isn't coming... It falls to us

## Problem Statement

Our society is adopting connected technology *faster than we are able to secure it.*

## Mission Statement

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



Medical



Automotive



Connected Home



Public Infrastructure

**Why** Trust, public safety, human life

**How** Education, outreach, research

**Who** Infosec research community

**Who** Global, grass roots initiative

**What** Long-term vision for cyber safety

**Collecting** existing research, researchers, and resources

**Connecting** researchers with each other, industry, media, policy, and legal

**Collaborating** across a broad range of backgrounds, interests, and skillsets

**Catalyzing** positive action sooner than it would have happened on its own

# 5-Star Framework

## Addressing Automotive Cyber Systems

### 5-Star Capabilities



- ★ **Safety by Design** – Anticipate failure and plan mitigation
- ★ **Third-Party Collaboration** – Engage willing allies
- ★ **Evidence Capture** – Observe and learn from failure
- ★ **Security Updates** – Respond quickly to issues discovered
- ★ **Segmentation & Isolation** – Prevent cascading failure

### Connections and Ongoing Collaborations



Security  
Researchers



Automotive  
Engineers



Policy  
Makers



Insurance  
Analysts



Accident  
Investigators



Standards  
Organizations

# Hippocratic Oath

## Formal Capacities

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

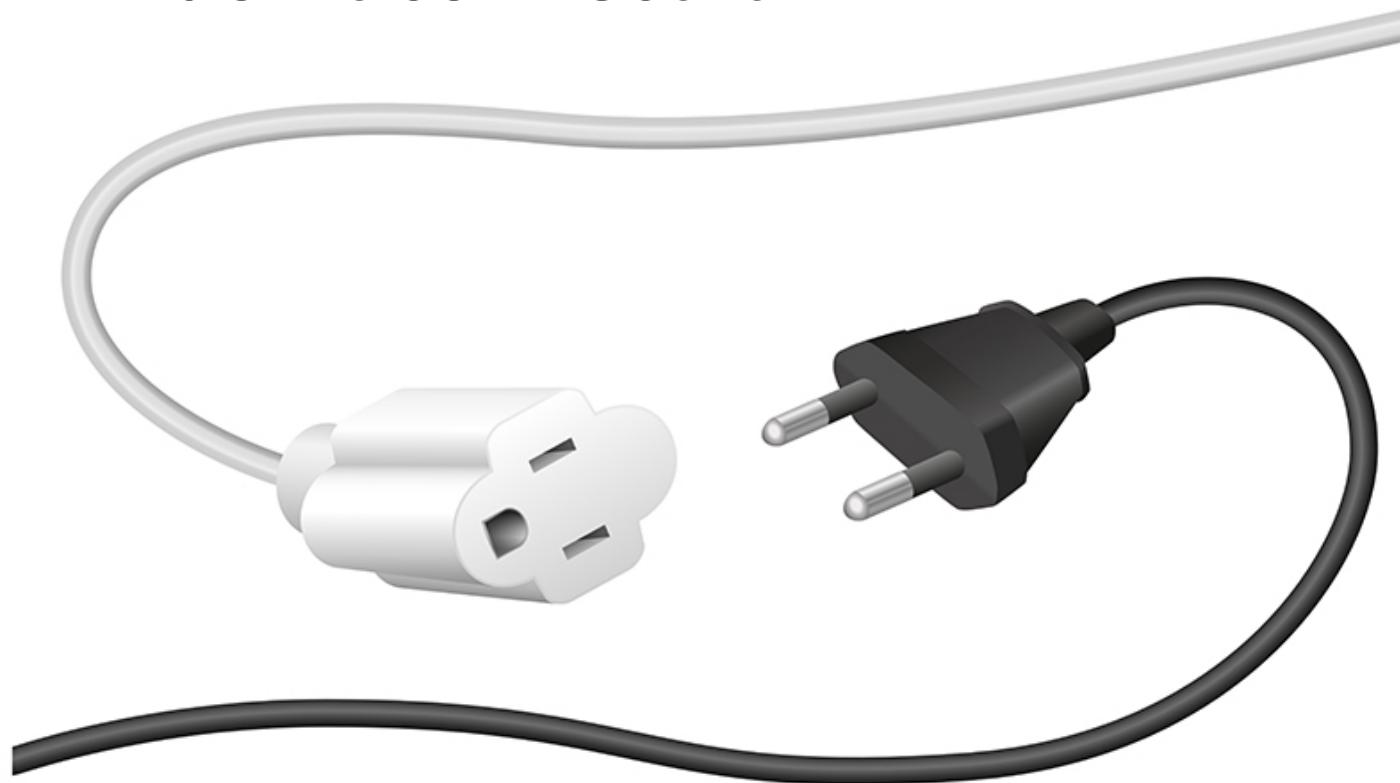
## Plain Speak

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

[www.iamthecavalry.org](http://www.iamthecavalry.org)  
@iamthecavalry



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



# NTIA Software component transparency



National Telecommunications and Information Administration  
United States Department of Commerce

Newsroom      Publications      Blog      Offices      About

[Home](#) » [Publications](#) » [Other Publications](#) » [2019](#)

## Topics

- + [Spectrum Management](#)
- + [Broadband](#)
- + [Internet Policy](#)
- + [Domain Name System](#)
- + [Public Safety](#)
- + [Grants](#)
- [Institute for Telecommunication Sciences](#)

## NTIA Software Component Transparency

### Topics:

[Internet Policy](#) [Internet Policy Task Force](#) [Cybersecurity](#) [Internet of Things](#)

### Date:

April 11, 2019

### Next Meeting:

The next meeting will be on June 27, 1:00pm - 4:30pm ET. This will be a “virtual meeting” with a call bridge and online slideshare. Details will be posted closer to the meeting. No registration is needed.

For more information, or to join a working group, please email [afriedman@ntia.doc.gov](mailto:afriedman@ntia.doc.gov).

# 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.

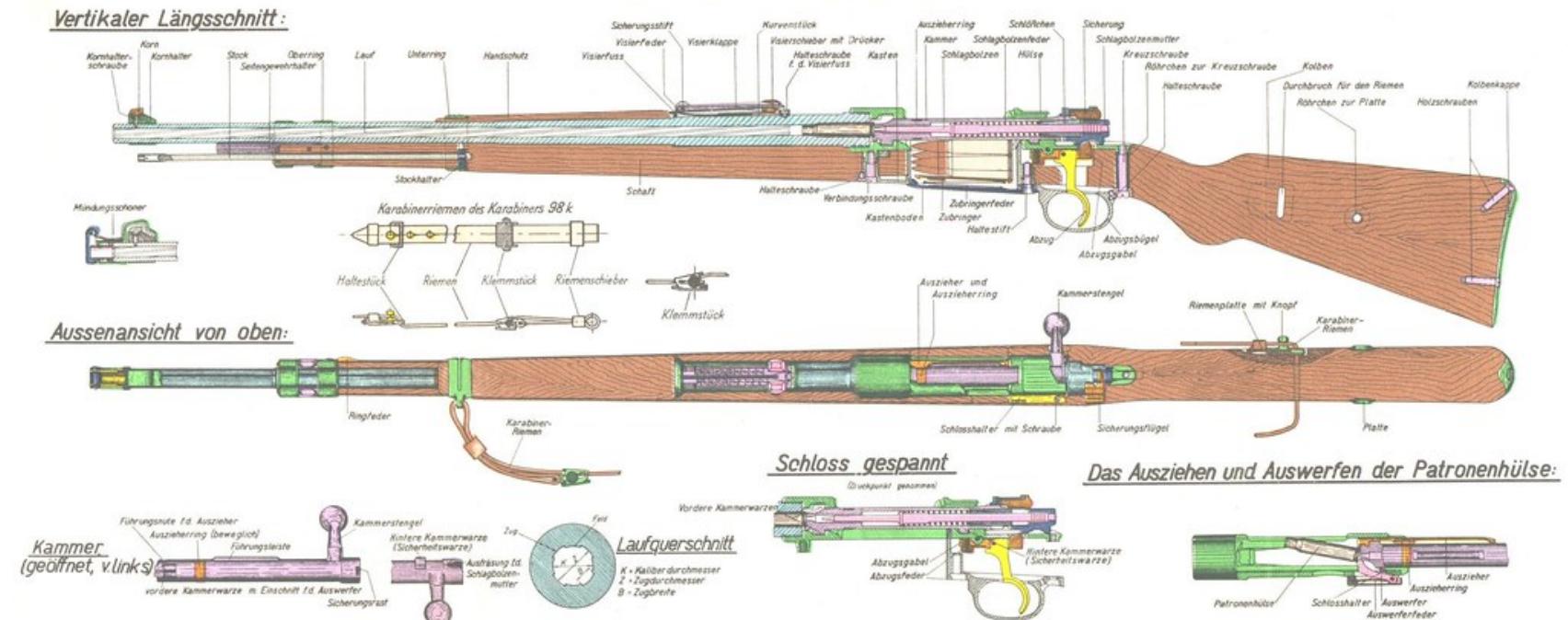
4

∞



# All analogies are wrong, some are useful

## Der Karabiner 98k



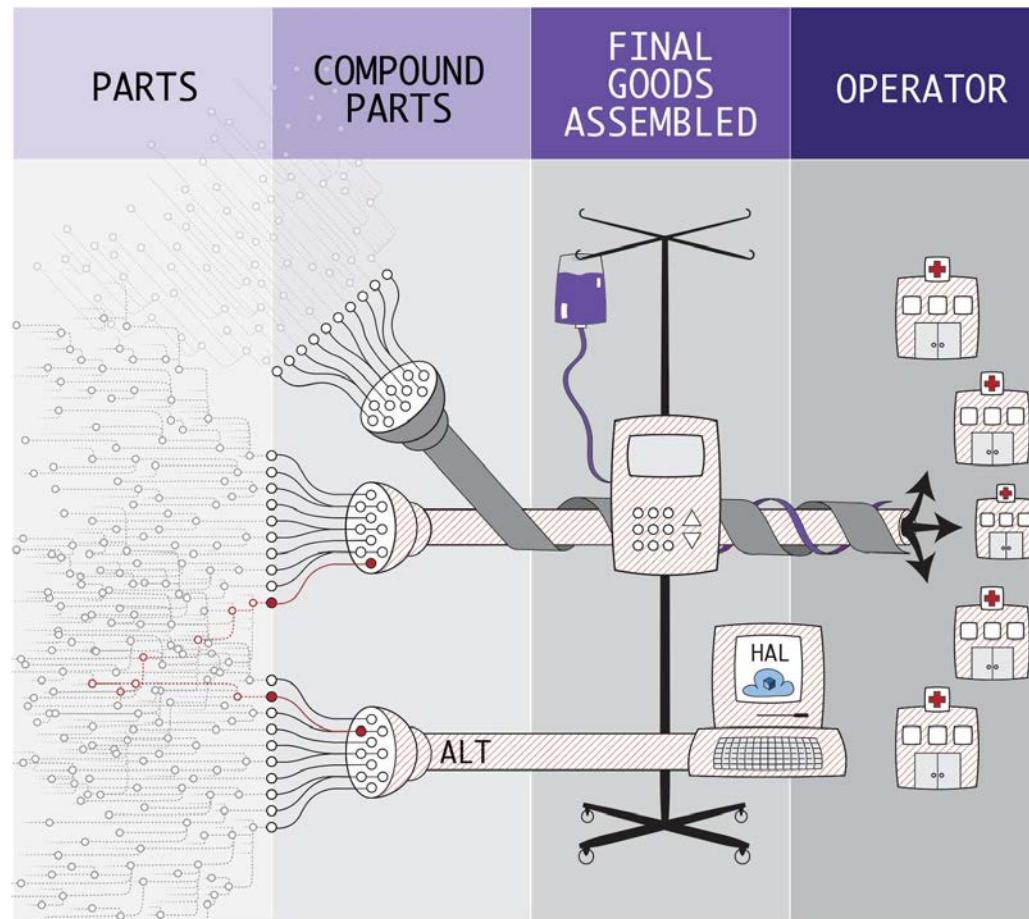
Vervielfältigung der ersten Übersichtsseite (Format 97 x 130 cm) „Der Karabiner 98k“, Verlag R. Eisenschmidt, Berlin NW7, Mittenstraße 18

Rev. 05.05.2001 A.J. Temmink

"Mauser K98k parts diagram (in German)" by [Lyle58](#) is licensed under [CC BY-NC 2.0](#)



# Software Bill of Materials



# 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

# Will hackers benefit???

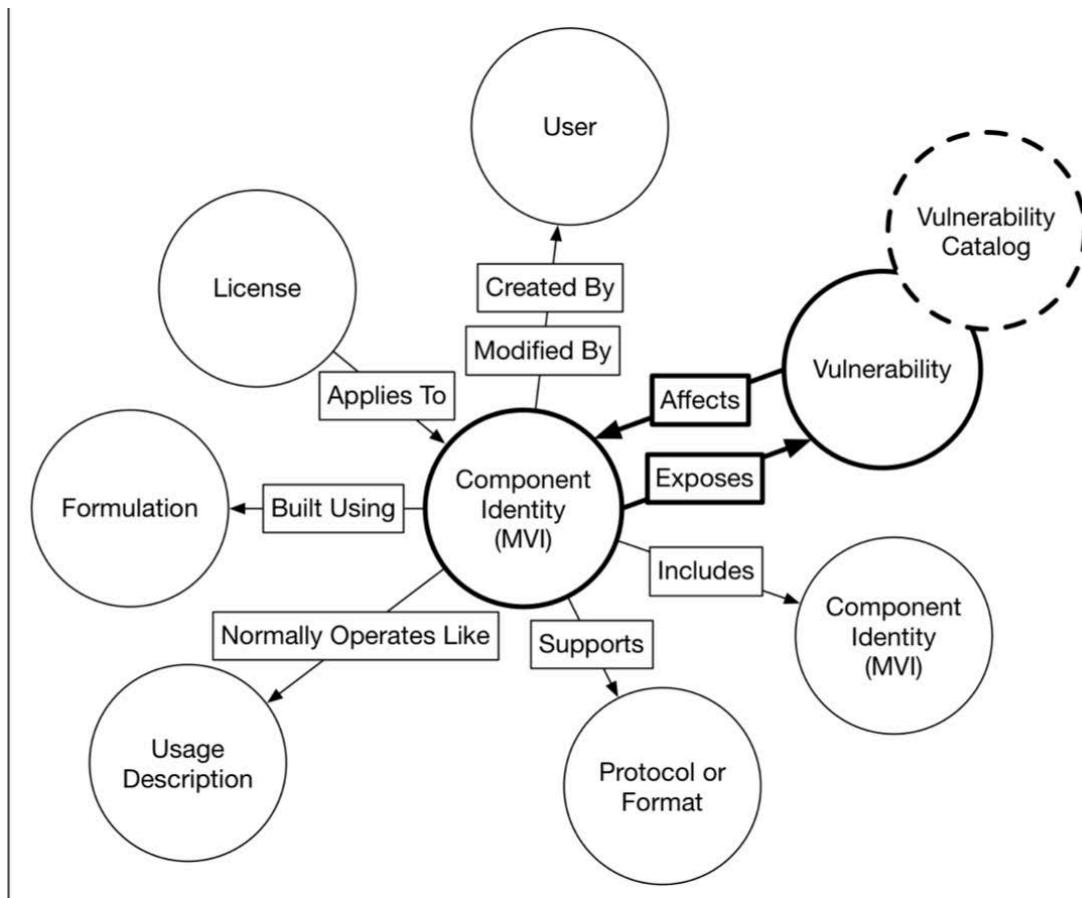


Photo: by [hadsie](#)  
licensed under

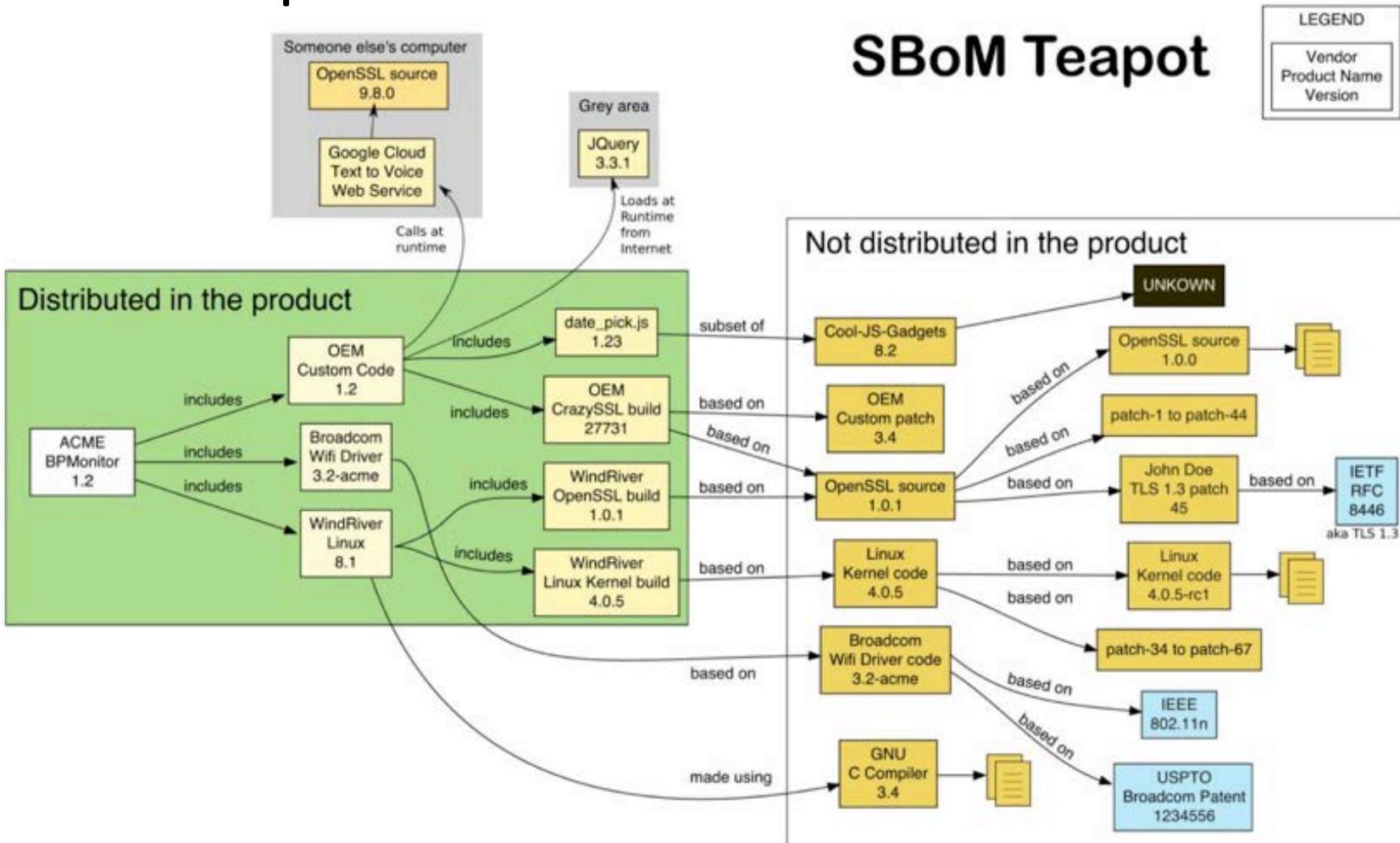
[CC BY-NC-SA 2.0](#)



# Vulnerability Management

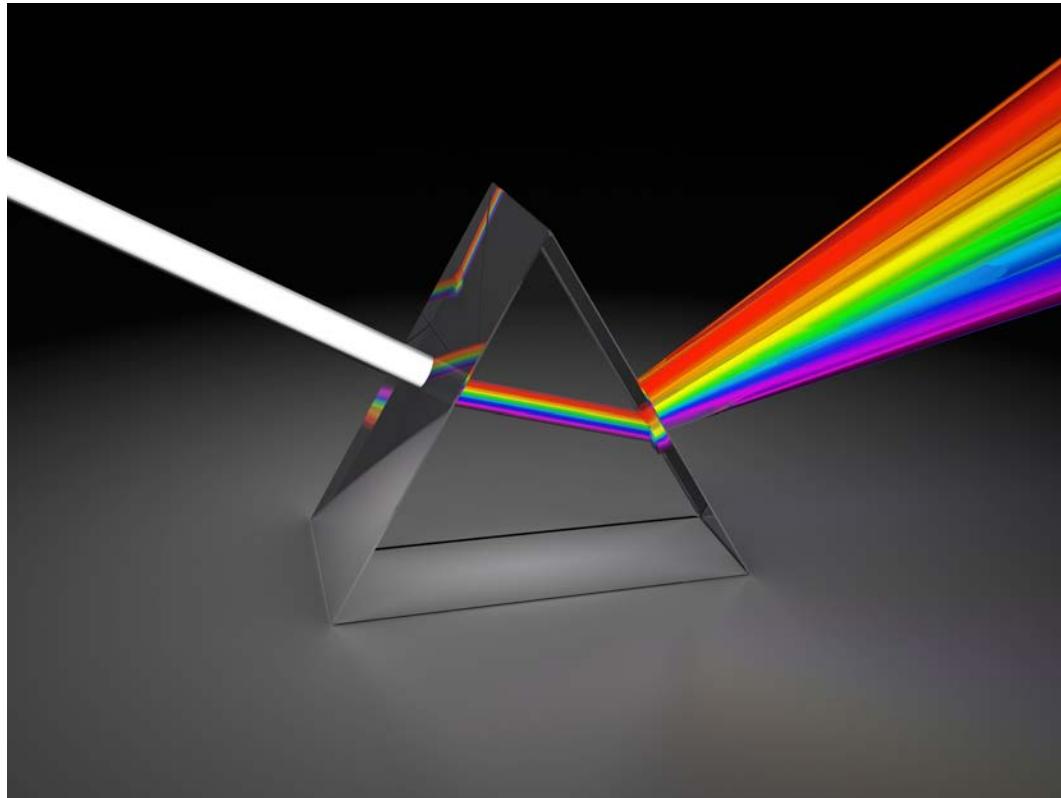


# Relationships in SBoM



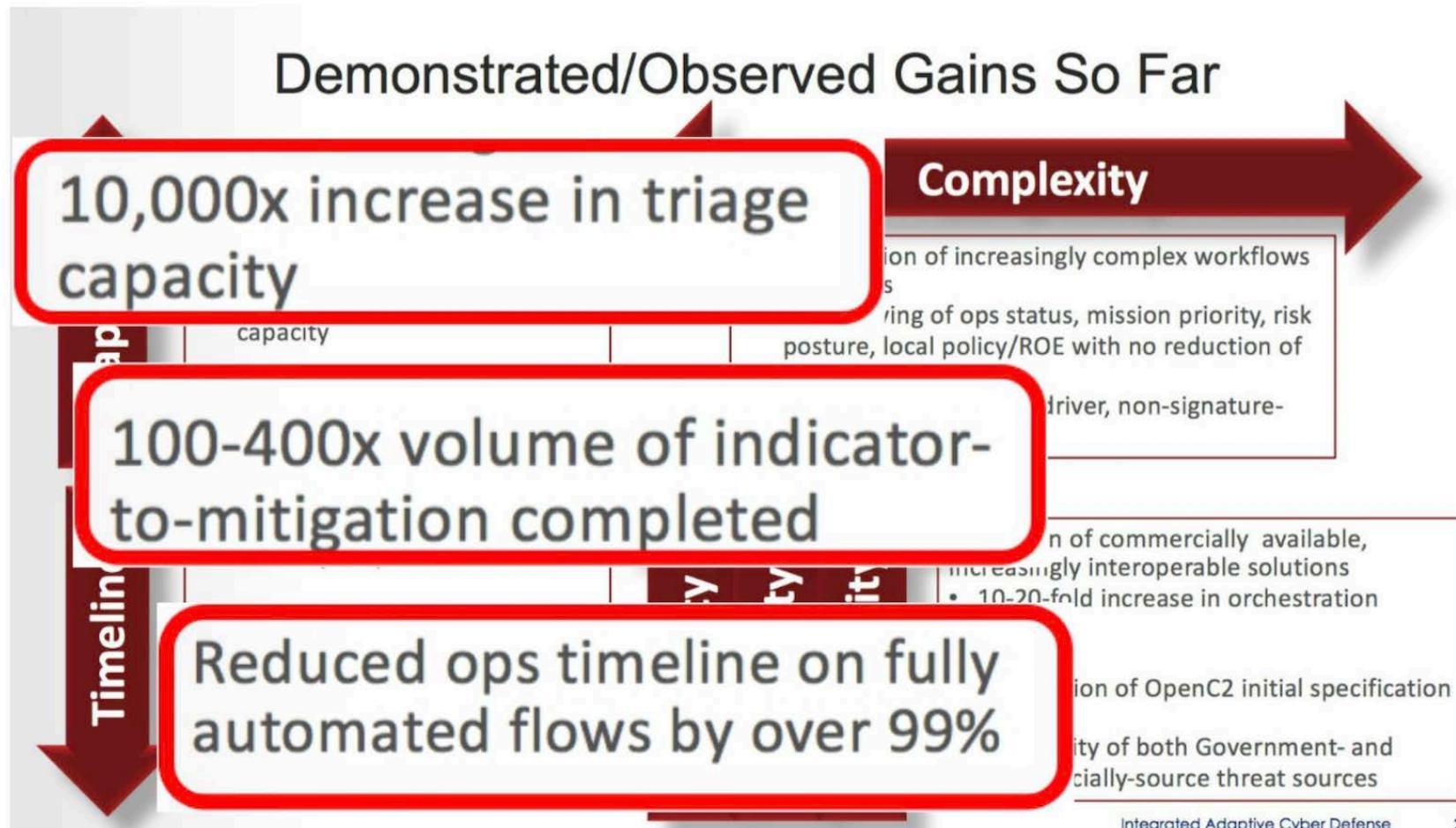
# SBoM Mechanics

- **Software ID (SWID)**
  - ISO/IEC 19770
  - [www.iso.org/standard/65666.html](http://www.iso.org/standard/65666.html)
- **Software Package Data Exchange (SPDX)**
  - [spdx.org](http://spdx.org)
- **Cyclone DX**
  - [cyclonedx.org](http://cyclonedx.org)



**From the speed of light  
To the speed of lawyers**





Software developer



develops

software



has



exploits



OpenC2



CACAO

STIX™  
TAXII™



# Takeaways



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

"PC020195" by [EdKopp4](#) is licensed under [CC BY-NC-SA 2.0](#)

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



Dan Geer



Duncan Sparrell



@dsparrell



sFractal



sparrell



duncan@sfractal.com



<https://www.linkedin.com/in/duncan-sparrell-cissp-csslp-ccsk-038137/>

