

# It Takes a Village...

Applying Data to Problems...Today!  
a/k/a Less Sizzle, More Vegetarian, Free Range, Organic, Steak-like Risk  
Product

IT'S DANGEROUS TO GO  
ALONE! TAKE THIS.



# This Will Help You On Your Journey



# Our Basic Premise

We'll **never** have perfect data

But...we **don't need** perfect data

Because...we already have **good enough** data to make better risk decisions **today**

So...let's **show** how we can do this with current problems and data!

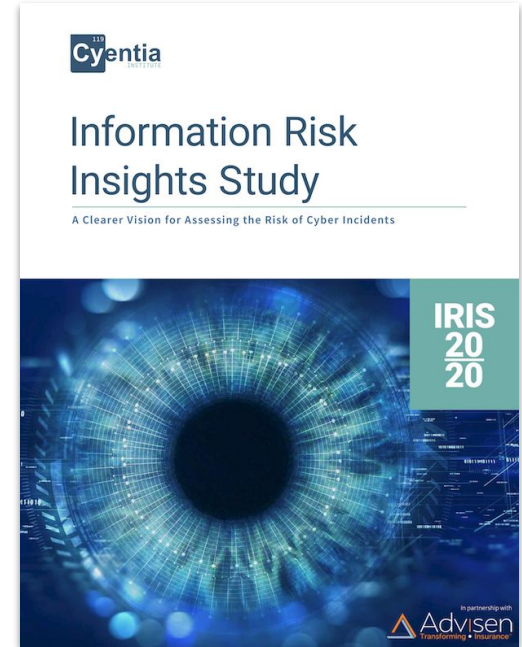
# Maturity Model for Risk Decision Making

Effort & Precision  
From Zero to Hero



# Loss Frequency – IRIS 20/20

Problem: How frequently do breaches occur?



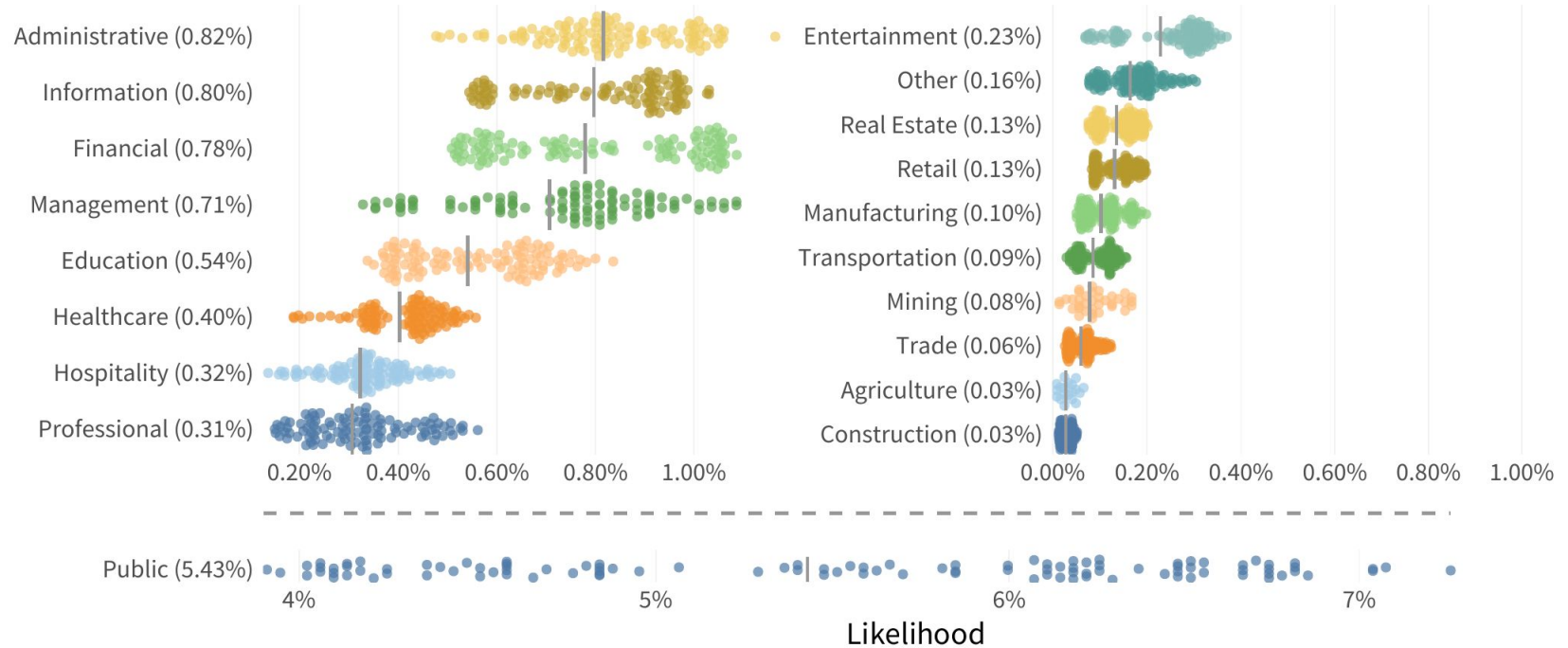
# Myth: Breaches Are Beyond Our Control

**Abandon All Hope...**

– Dante, Inferno

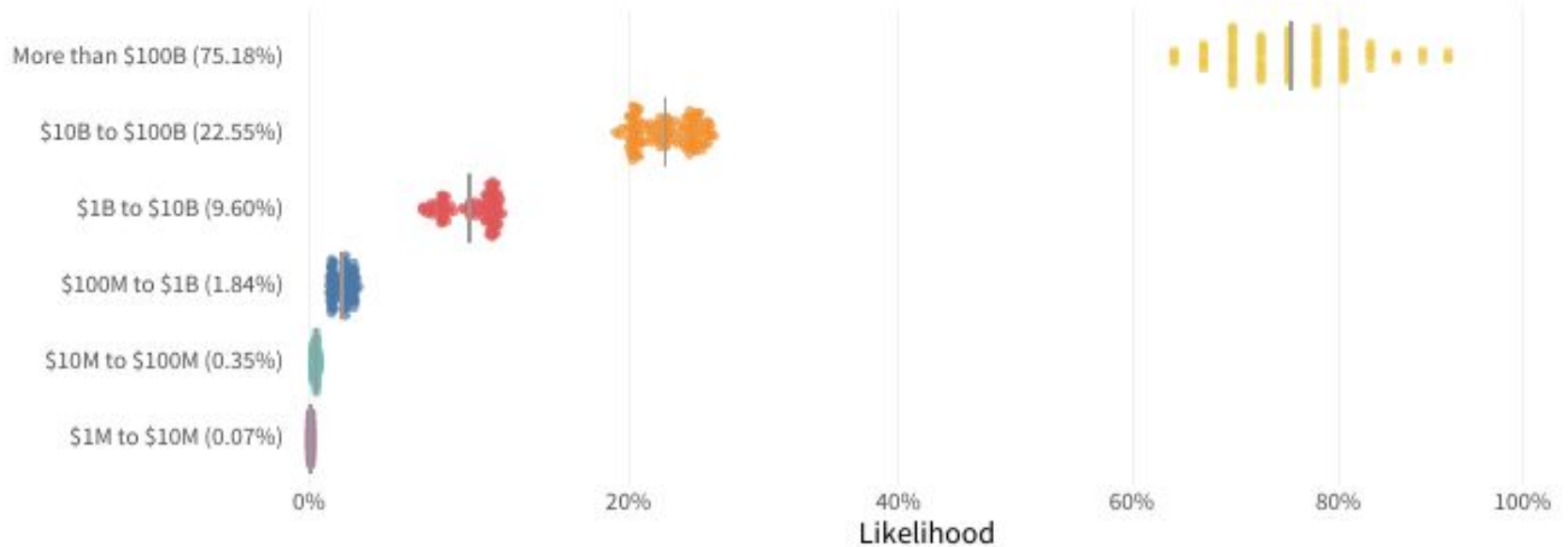


# Likelihood by Sector



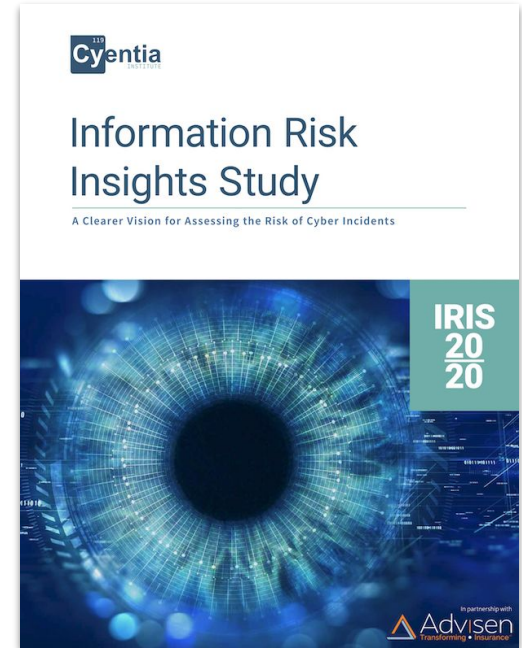


# Likelihood by Size

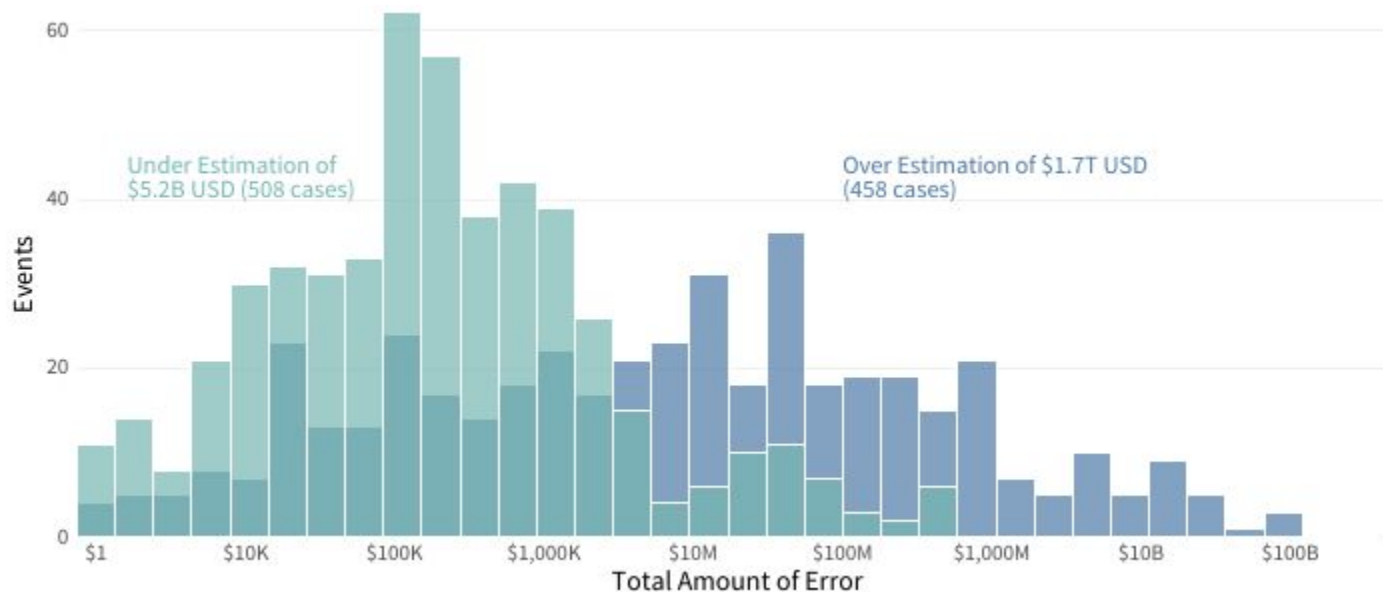


# Loss Size – IRIS 20/20

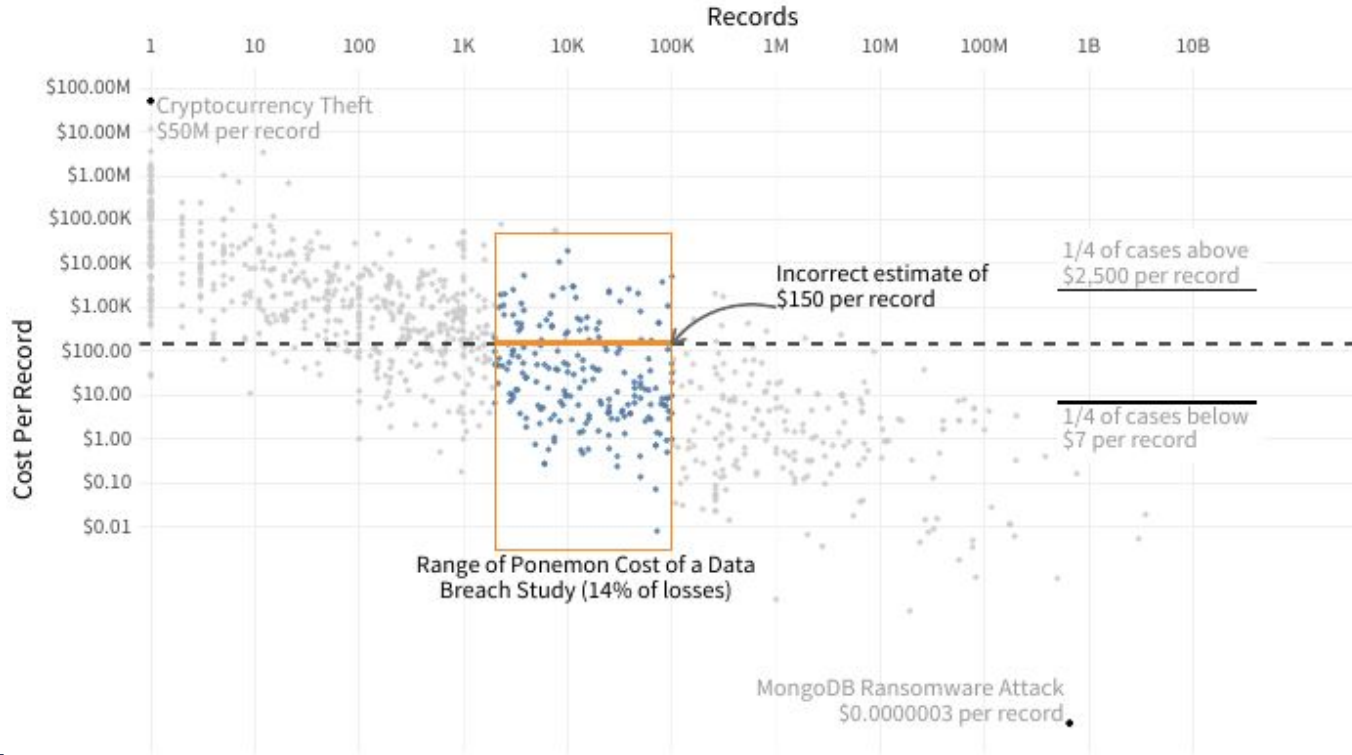
Problem: How much will a breach cost us?



# Myth: Losses are Linearly Dependent on the Number of Records



# The Failure of Linear Models



# If Cost Per Record Won't Save Us, What Will?



# How Much Will a Breach Cost Us?

| Records | Probability of At Least This Much Loss |        |       |       |        |      |
|---------|----------------------------------------|--------|-------|-------|--------|------|
|         | \$10K                                  | \$100K | \$1M  | \$10M | \$100M | \$1B |
| 100     | 82.0%                                  | 49.9%  | 17.8% | 3.3%  | 0.3%   | 0.0% |
| 1K      | 88.4%                                  | 60.9%  | 26.0% | 5.9%  | 0.7%   | 0.0% |
| 10K     | 93.0%                                  | 71.1%  | 35.8% | 10.0% | 1.4%   | 0.1% |
| 100K    | 96.0%                                  | 79.8%  | 46.7% | 15.8% | 2.7%   | 0.2% |
| 1M      | 97.9%                                  | 86.7%  | 57.7% | 23.5% | 5.0%   | 0.5% |
| 10M     | 99.0%                                  | 91.8%  | 68.2% | 32.8% | 8.6%   | 1.1% |
| 100M    | 99.5%                                  | 95.3%  | 77.4% | 43.4% | 13.9%  | 2.3% |
| 1B      | 99.8%                                  | 97.4%  | 84.9% | 54.5% | 21.0%  | 4.2% |
| 10B     | 99.9%                                  | 98.7%  | 90.5% | 65.3% | 30.0%  | 7.4% |

# Extreme Losses – A Sneak Peak of IRIS Xtreme

Problem: How do I address board-level catastrophic  
“risk” blobs?



Photo by [Max LaRochelle](#) on [Unsplash](#)



# Myth: “Cyber Risks” are Unmanageable

APT

Data Exposure

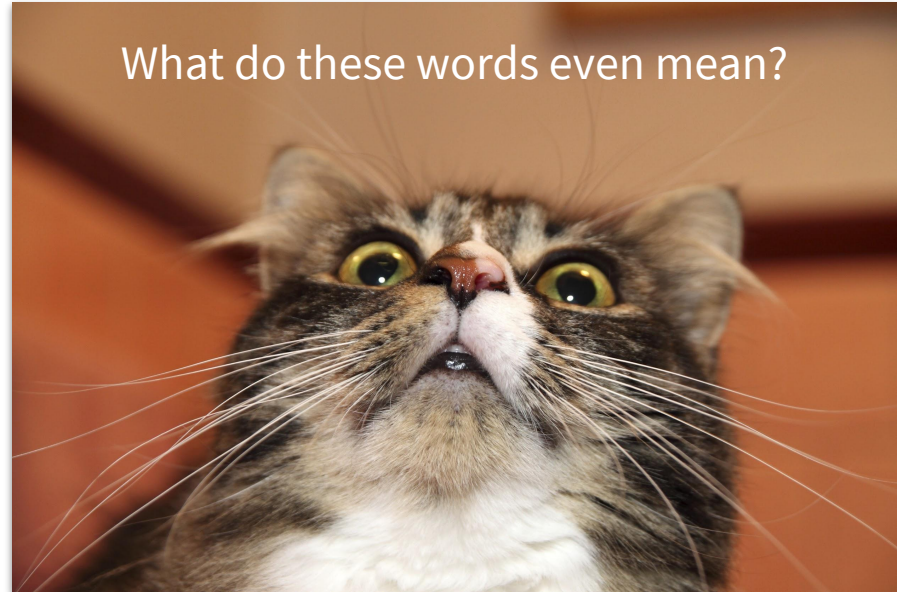
Hacking

Insider Abuse

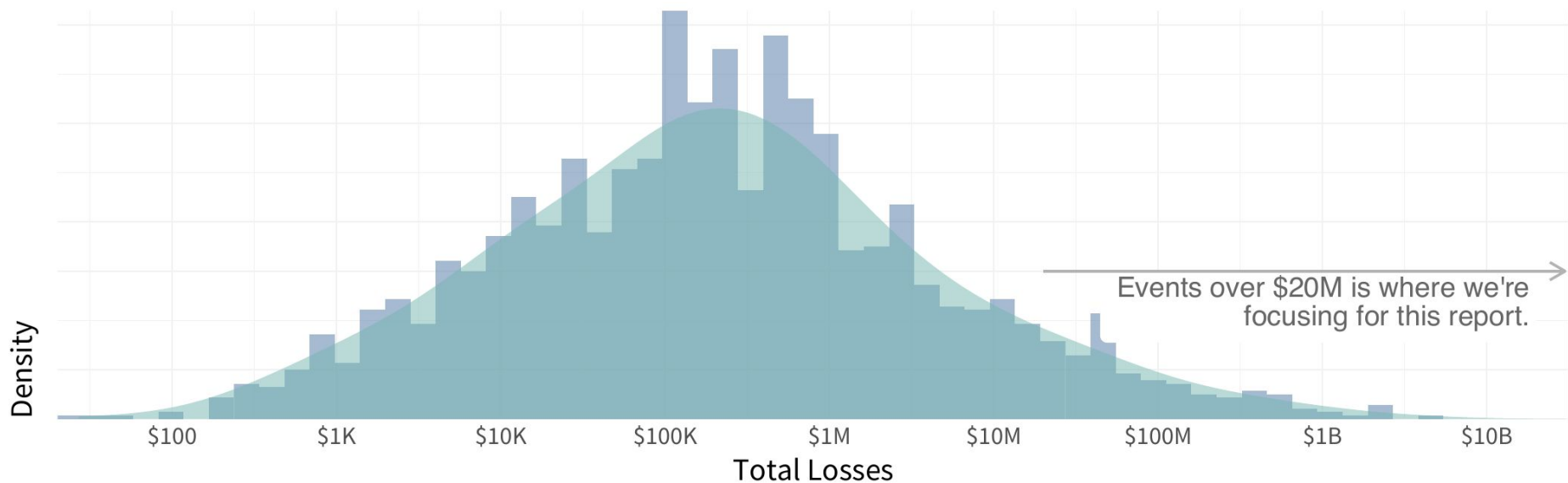
Physical

Ransomware

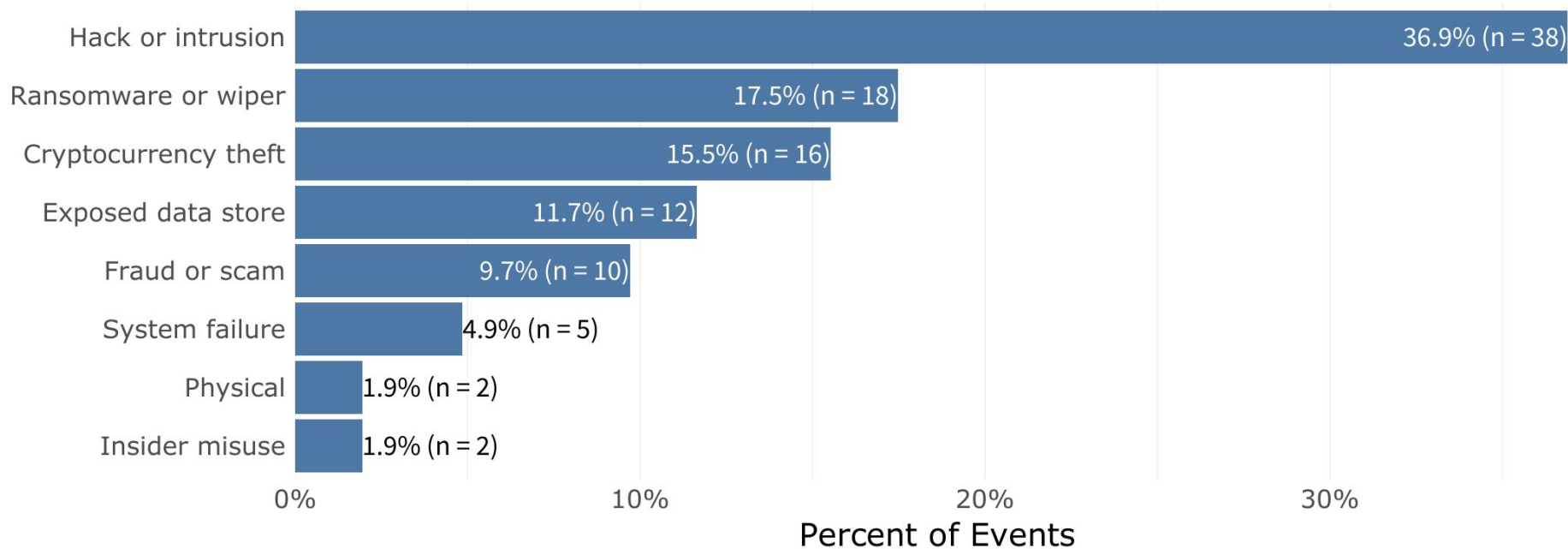
Service Interruption



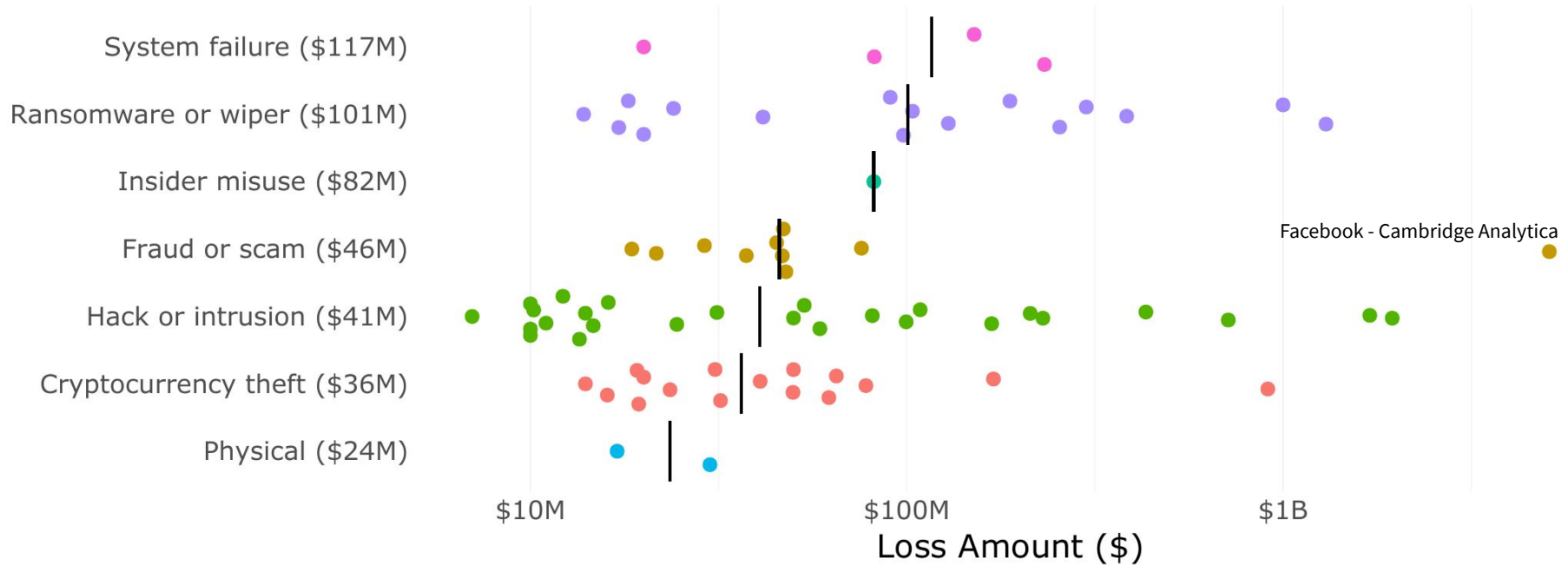
# Focusing on Tail Risk



# Event Types Occurring Most Frequently



# Event Types with the Largest Typical Losses



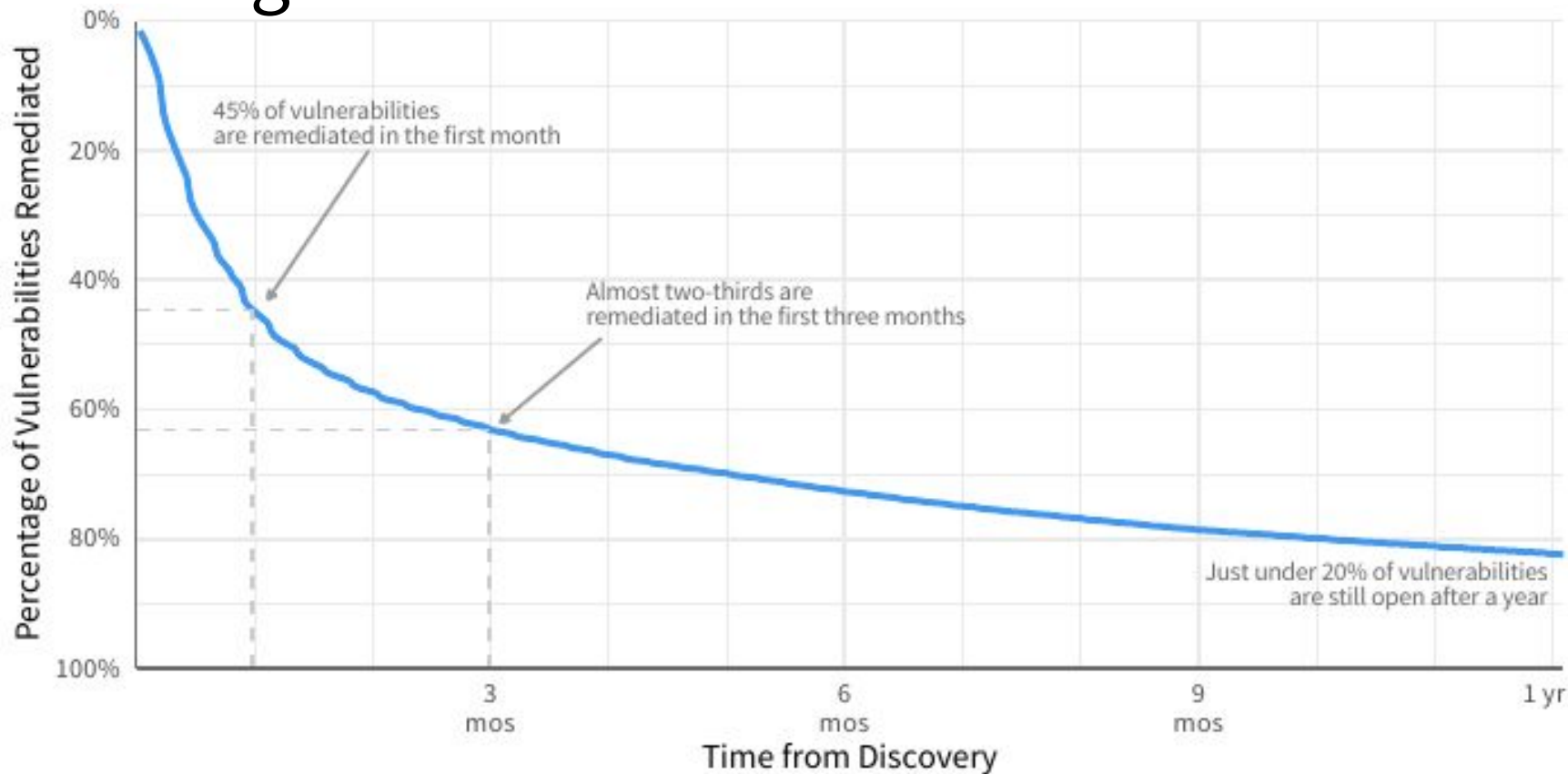


# Scenario Based Risk Analysis

Problem: How fast can vulnerabilities be remediated?

Problem: How can we prioritize remediation efforts?

# The Big Picture

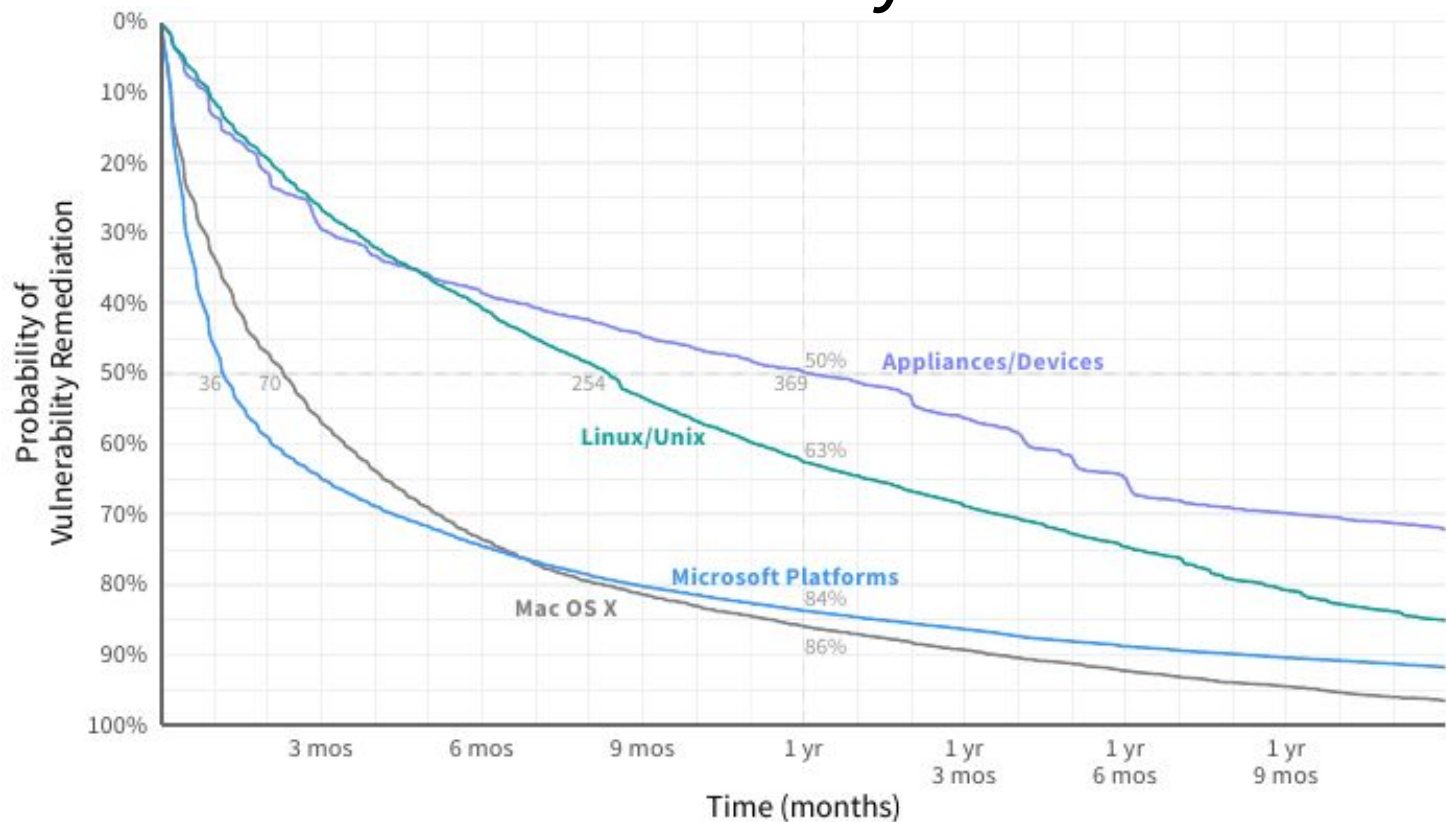


# Vulnerabilities are Not Evenly Distributed

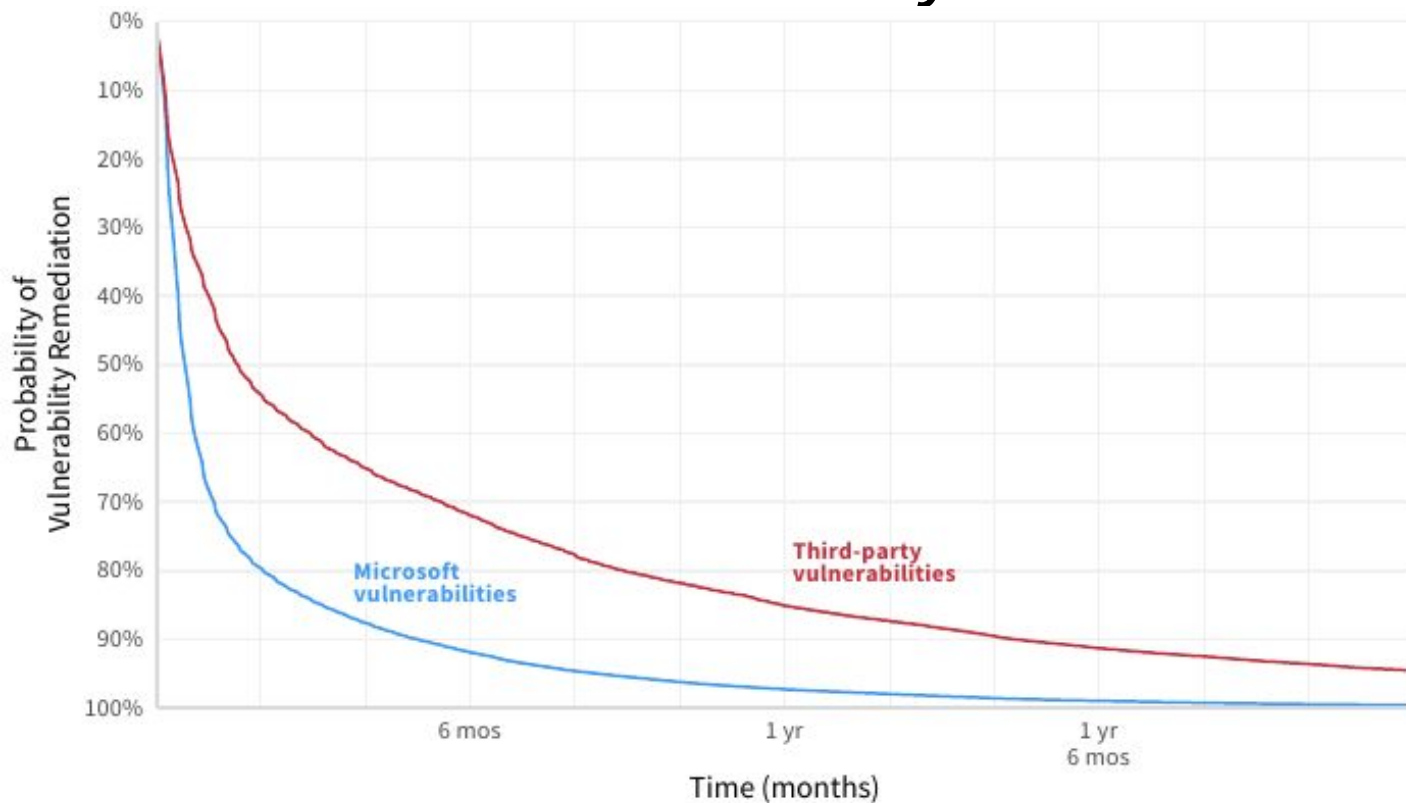




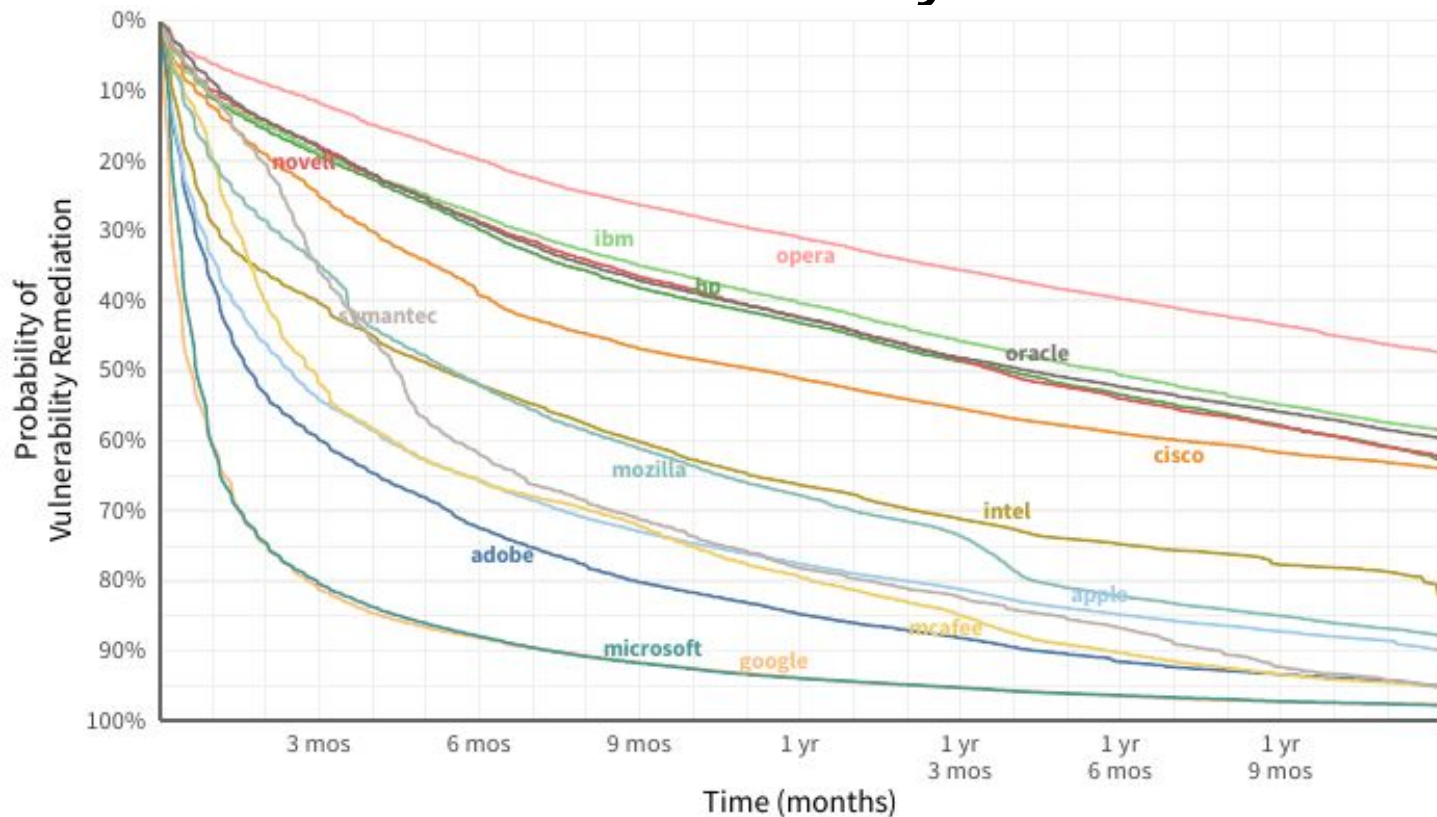
# Remediation is Not Evenly Distributed



# Remediation is Not Evenly Distributed



# Remediation is Not Evenly Distributed



# Exploit Prediction Scoring System (EPSS)

Improving Vulnerability Remediation  
Through Better Exploit Prediction



## Exploit Prediction Scoring System (EPSS)

Jay Jacobs @jayjacobs  
Michael Roytman, @mroytman

Jay  
jay@cornell.edu  
Cornell University



Cornell University

arXiv.org > cs > arXiv:1908.04856

Search... All fields Search  
Help | Advanced Search

Computer Science > Cryptography and Security

[Submitted on 13 Aug 2019]

### Exploit Prediction Scoring System (EPSS)

Jay Jacobs, Sasha Romanosky, Benjamin Edwards, Michael Roytman, Idris Adjerid

Despite the massive investments in information security technologies and research over the past decades, the information security industry is still immature. In particular, the prioritization of remediation efforts within vulnerability management programs predominantly relies on a mixture of subjective expert opinion, severity scores, and incomplete data. Compounding the need for prioritization is the increase in the number of vulnerabilities the average enterprise has to remediate. This paper produces the first open, data-driven framework for assessing vulnerability threat, that is, the probability that a vulnerability will be exploited in the wild within the first twelve months after public disclosure. This scoring system has been designed to be simple enough to be implemented by practitioners without specialized tools or software, yet provides accurate estimates of exploitation. Moreover, the implementation is flexible enough that it can be updated as more, and better, data becomes available. We call this system the Exploit Prediction Scoring System, EPSS.

#### Download:

- PDF only  
(license)

Current browse context:  
cs.CR

< prev | next >  
new | recent | 1908

Change to browse by:  
cs

#### References & Citations

- NASA ADS
- Google Scholar
- Semantic Scholar

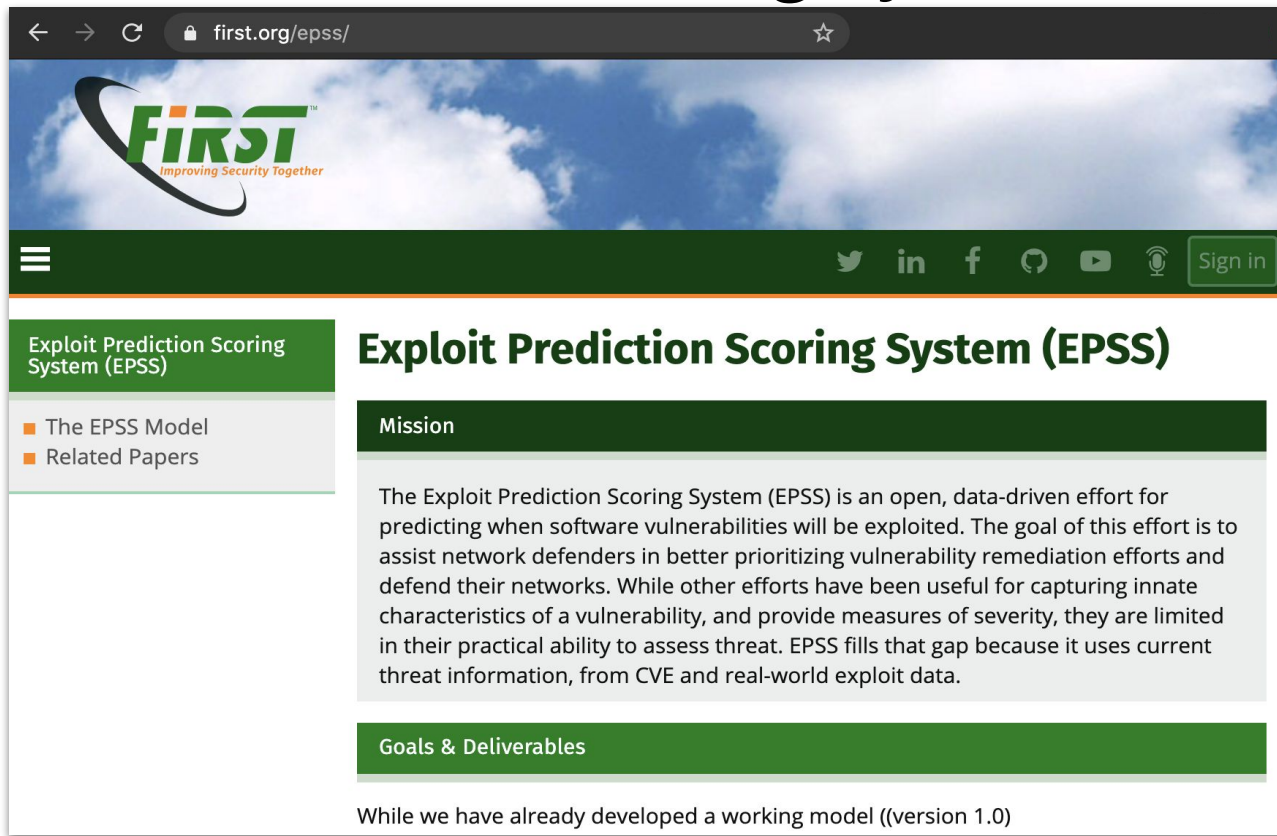
Export citation

#### Bookmark



Despite  
years, the  
ability to  
vulnerabi  
cope, fin  
though t  
existed  
remedia  
attempt  
coverag  
low-risk  
be high  
vulnera  
learning

# Exploit Prediction Scoring System (EPSS)



The screenshot shows the website first.org/epss/. The header features the FIRST logo with the tagline "Improving Security Together" against a blue sky background. Below the header is a green navigation bar with a hamburger menu icon, social media icons for Twitter, LinkedIn, Facebook, GitHub, YouTube, and a microphone icon, and a "Sign in" button. The main content area has a green sidebar on the left with the title "Exploit Prediction Scoring System (EPSS)" and two links: "The EPSS Model" and "Related Papers". The main content area has a green header with the title "Exploit Prediction Scoring System (EPSS)". Below this is a "Mission" section with a green header and a paragraph of text. Below the "Mission" section is a "Goals & Deliverables" section with a green header. At the bottom of the page, there is a line of text: "While we have already developed a working model ((version 1.0))".

first.org/epss/

**FIRST**  
Improving Security Together

Sign in

Exploit Prediction Scoring System (EPSS)

- The EPSS Model
- Related Papers

## Exploit Prediction Scoring System (EPSS)

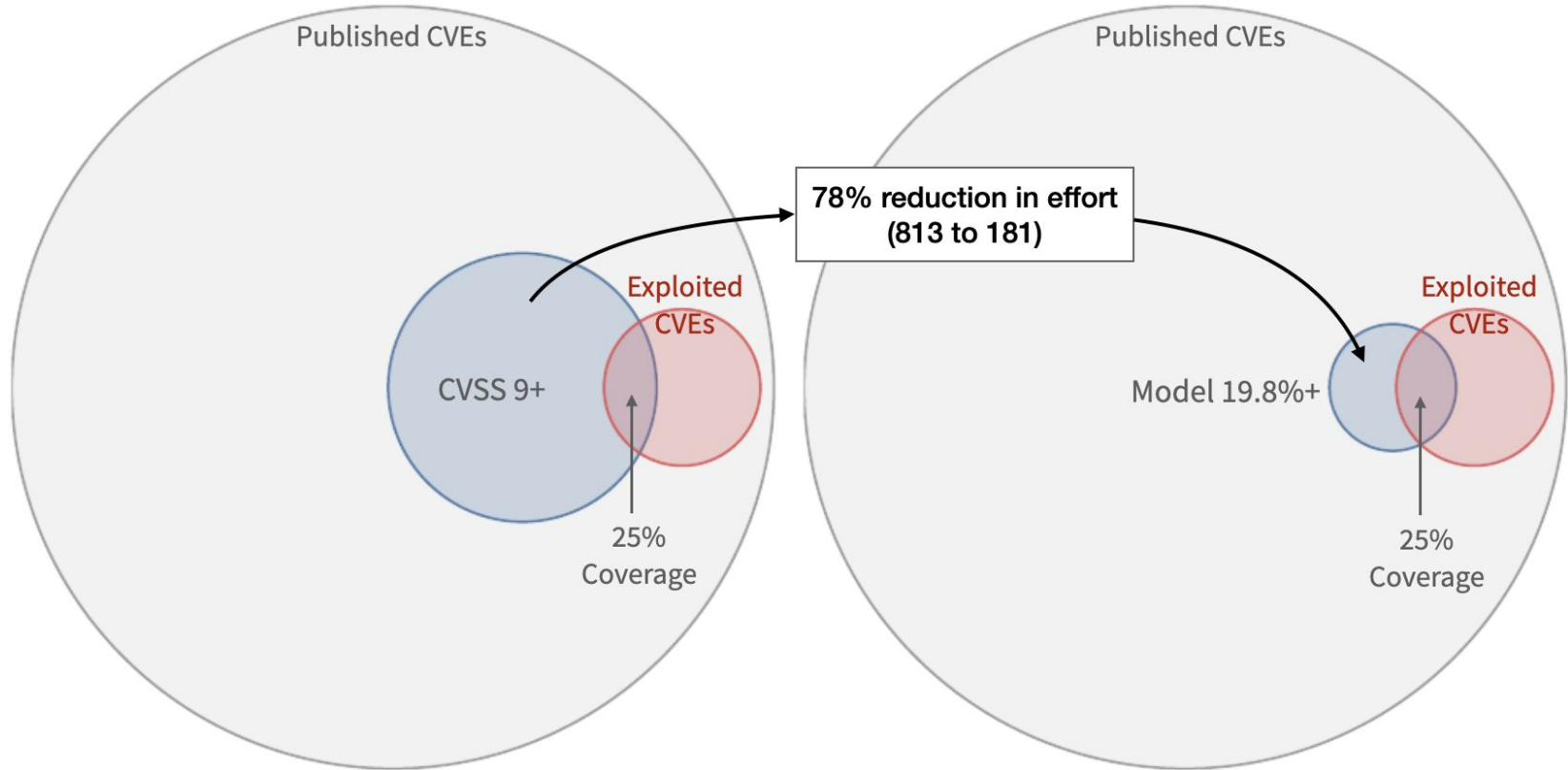
### Mission

The Exploit Prediction Scoring System (EPSS) is an open, data-driven effort for predicting when software vulnerabilities will be exploited. The goal of this effort is to assist network defenders in better prioritizing vulnerability remediation efforts and defend their networks. While other efforts have been useful for capturing innate characteristics of a vulnerability, and provide measures of severity, they are limited in their practical ability to assess threat. EPSS fills that gap because it uses current threat information, from CVE and real-world exploit data.

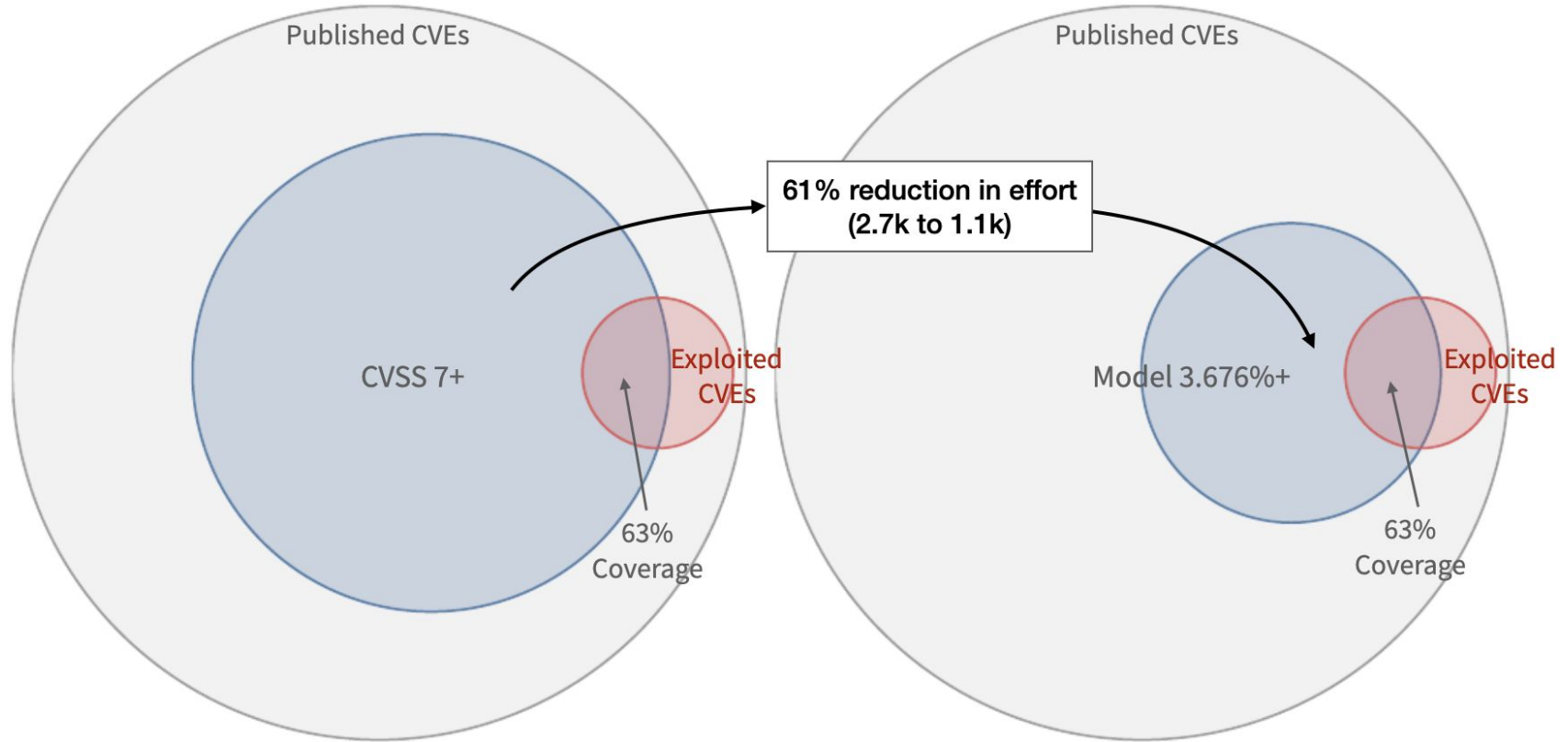
### Goals & Deliverables

While we have already developed a working model ((version 1.0))

# Exploit Prediction Scoring System (EPSS)



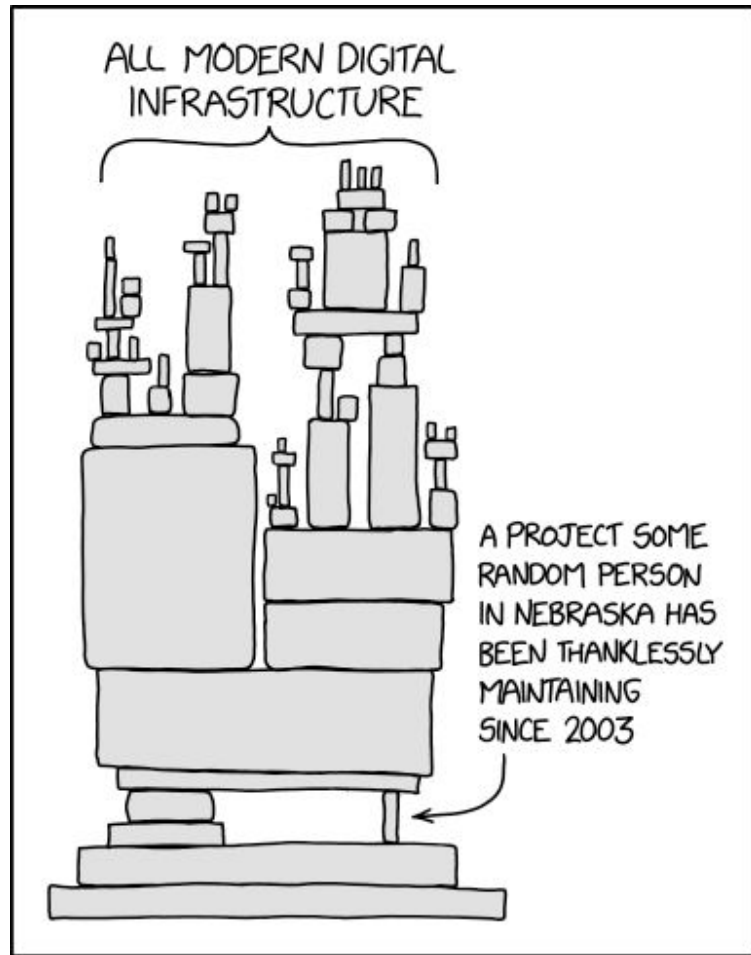
# Exploit Prediction Scoring System (EPSS)





# Application Security Management

- Getting ahead of the vulnerabilities

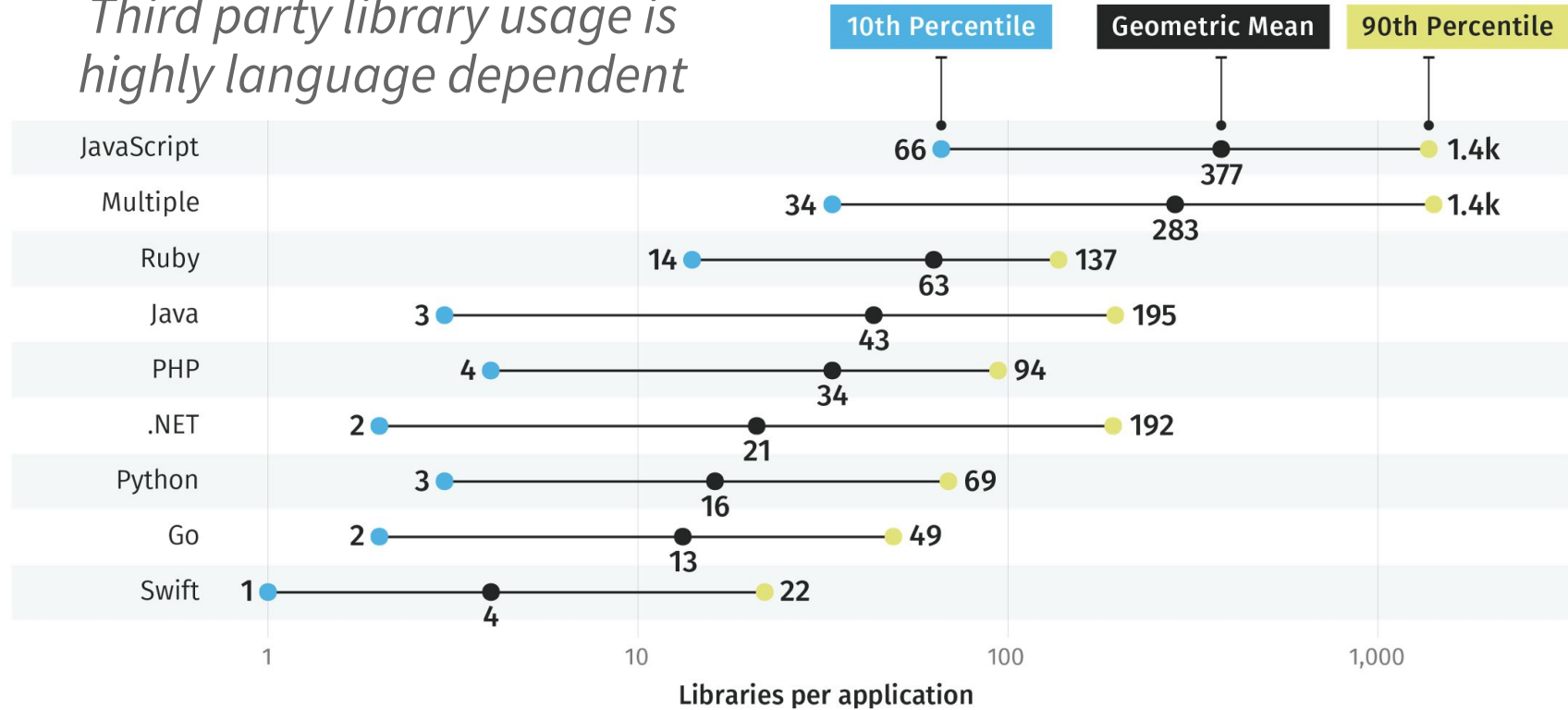


<https://xkcd.com/2347/>

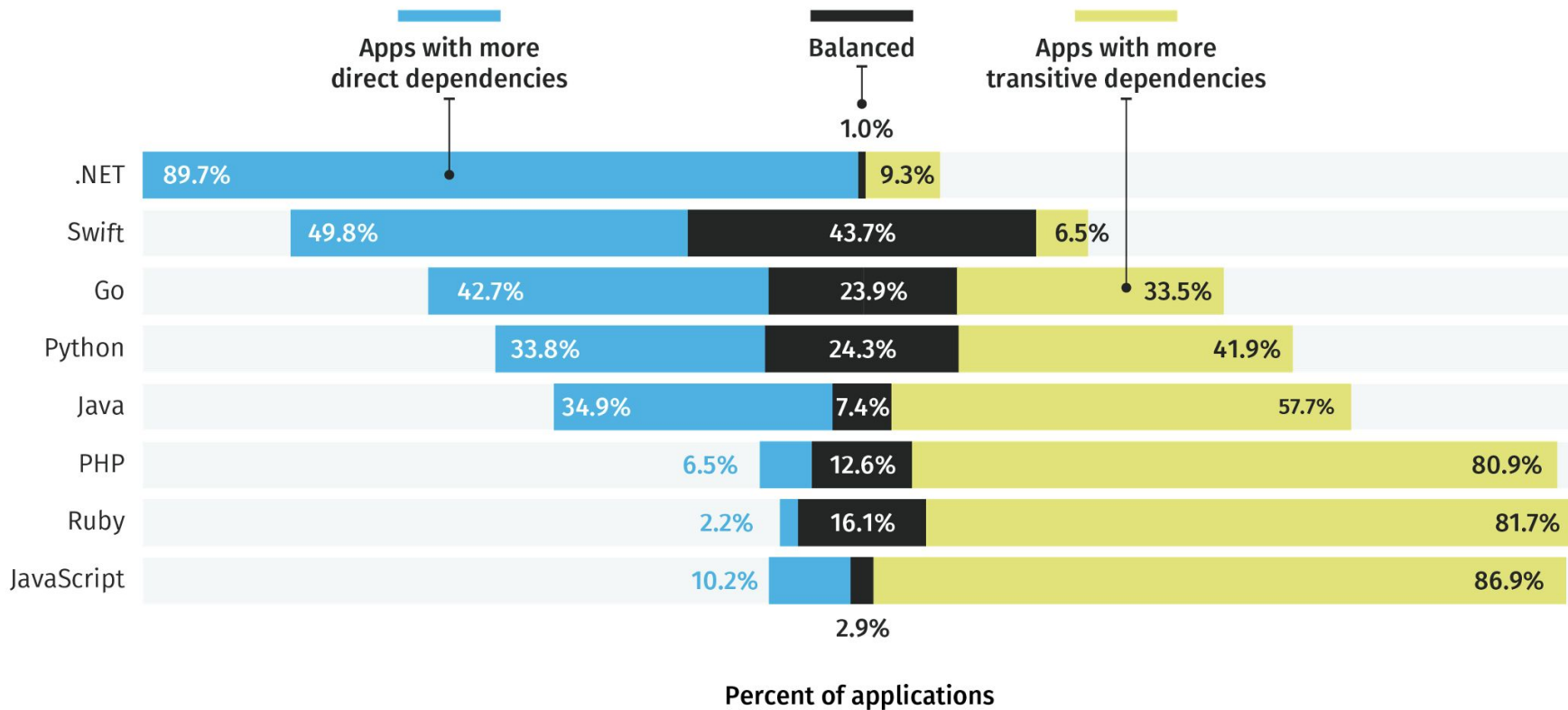
#SIRAcon

# Software Composition Analysis

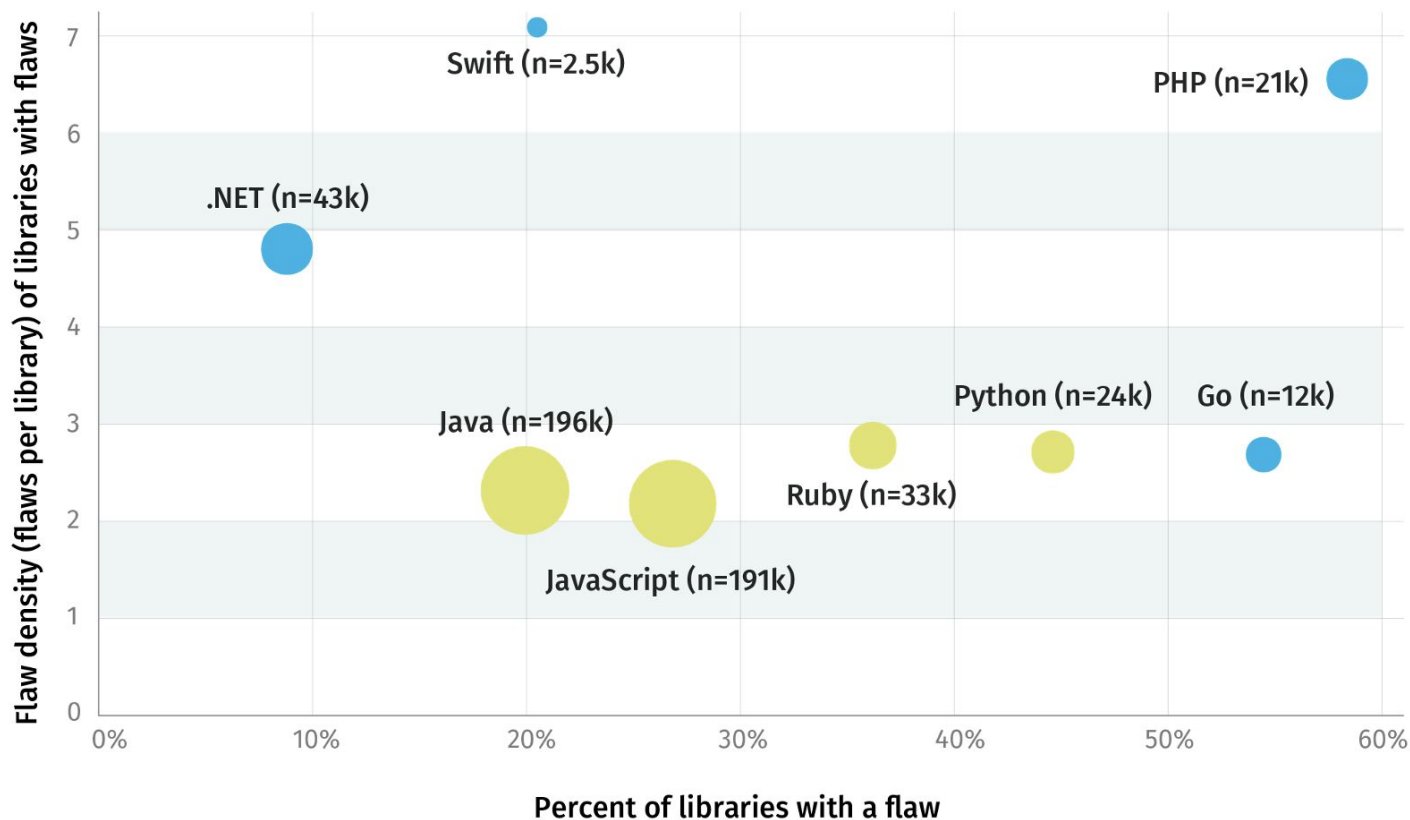
*Third party library usage is highly language dependent*



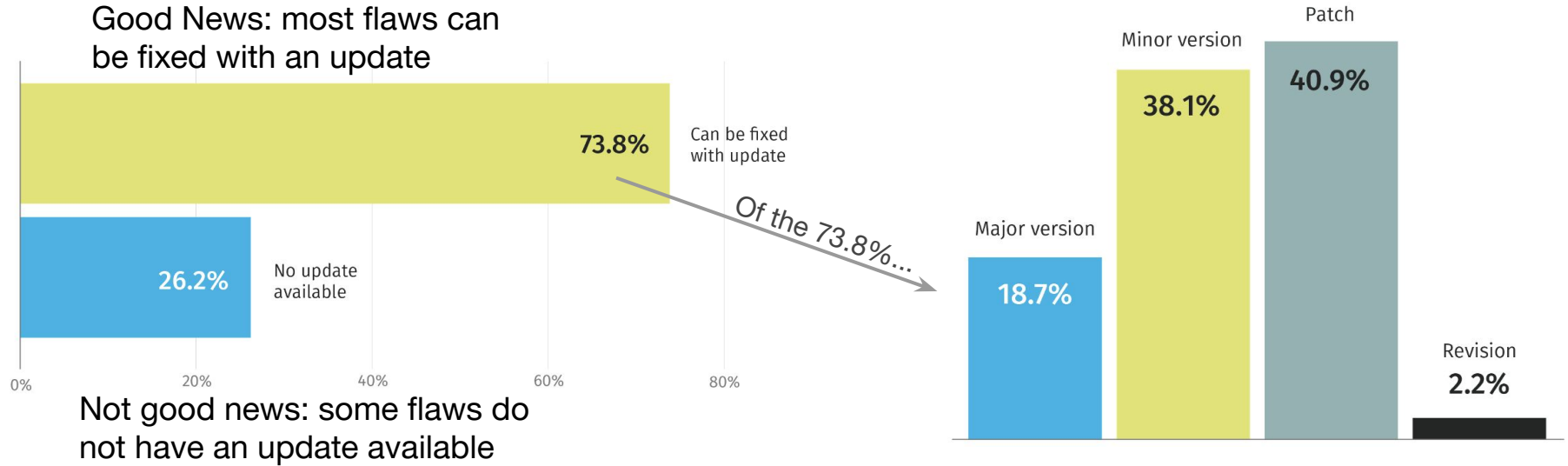
# Software Composition Analysis



# Software Composition Analysis



# Software Composition Analysis



# Leveraging Community Knowledge

Problem: How do we make future me better  
than current me?



# Cyentia Library

Sources: **739**

Documents: **2,246**

Pages: **55,503**

Cyentia Cybersecurity Research Library

Sources Tags About Return to Cyentia.com

## Cyentia Cybersecurity Research Library


Subscribe to the Library Newsletter

Your Email Address

Search the Library

Search All Report Metadata


Report missing? Write to us today!



**The state of vulnerability management in the cloud and on-premises**

A survey-based report of 1,848 IT and IT Security professionals on the challenges with vulnerability prioritization and the importance of patch management for the prevention of breaches. (more available)


Added: August 18, 2020



**Implementing Cloud Security Best Practices**

This report covers findings from a survey conducted by Dimensional Research in July 2020. A total of 310 qualified individuals completed the survey. (more available)


Added: August 17, 2020



**The CISO Current Report**  
Q2, 2020

This paper compiles observations as well as predictions on the state of cybersecurity in 2020.


Added: August 17, 2020



**2020 Mid Year Report**  
Data Breach Quickview

This mid year report covers publicly disclosed data breaches first reported between January 1, 2020 and June 30, 2020 and compares current observations to the same time period for prior years. (more available)


Added: August 17, 2020



**Global Threat Landscape Report: August 2020**

Using data from Fortinet's global product offerings, this semi-annual report covers the attack trends seen during the first half of 2020. (more available)

Added: August 13, 2020

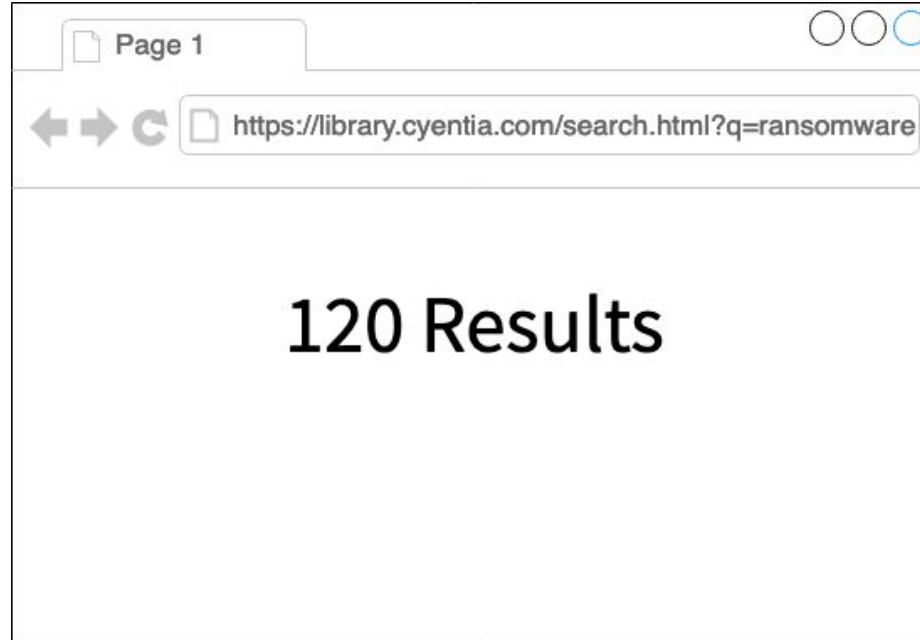


**2020 State of the Software Supply Chain**

A combination of survey data and Sonatype's own product information, this sixth annual report covers the state and practices in open source software development with a special focus on the security practices and outcomes found within the open source community. (more available)



# Searching the CyentiaLibrary for Ransomware



# Statements on Frequency and Loss

## 2019 Paid Ransomware Report, Kivu

- “2019, Kivu facilitated ransom payments in 143 cases, paying a total of over US\$17M.”
- “...average ransomware payment for Kivu’s clients was \$123,037.56 in 2019.”

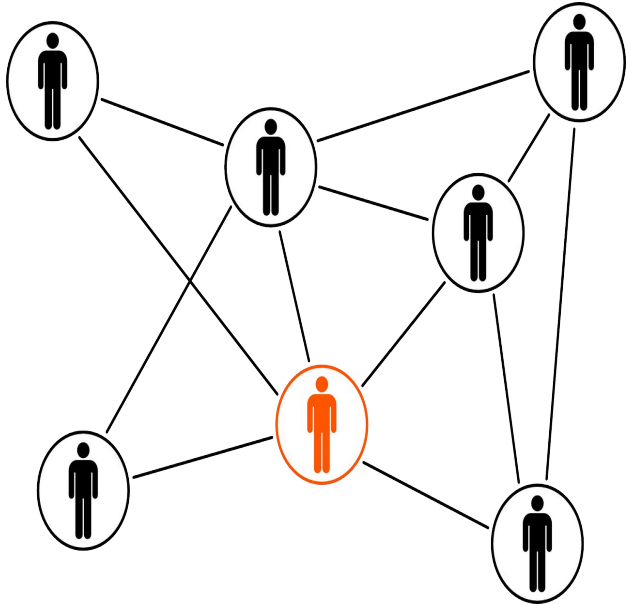
## 2020 Incident Response and Data Breach Report, Crypsis

- “...one third of our overall matters in 2019 were BEC attacks”
- Average requested ransom \$115,123

## How Ransomware Attacks, Sophos

- “Paying the ransom doubles the cost of dealing with a ransomware attack. The average cost to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) is US\$732,520 for organizations that don’t pay the ransom, rising to US\$1,448,458 for organizations that do pay.”

## Bringing It Back To the Real



**Remember:** Risk management does take a village

**Ask:** Where do I need to be on the maturity model?

**Act:**

- Go to the Library for one of your problems
- Pick up a report and give it a read
- Keep up to date with the Cyentia Podcast and Library Newsletter

# Would You Like to Know More?

Web: [cyentia.com](https://cyentia.com)

Library: [library.cyentia.com](https://library.cyentia.com)

Twitter: [@cyentinst](https://twitter.com/cyentinst)

Email: [research@cyentia.com](mailto:research@cyentia.com)

LinkedIn: [cyentia-institute](https://www.linkedin.com/company/cyentia-institute)

