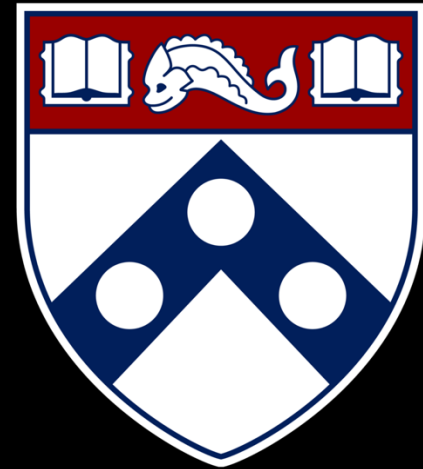


Empirical Security & Privacy, for Humans



UPenn CIS 7000-010
10/30/2025



Are Cyber Defenders Winning?

Reading

Are Cyber Defenders Winning x +

lawfaremedia.org/article/are-cyber-defenders-... ☆

Menu LAWFARE

Jason Healey, Tarang Jain

Monday, July 14, 2025, 10:50 AM

Share On: f X in X @

Attackers in cyberspace have long held system-wide advantages. Fighting back requires measuring progress.



Illustration of a lock with code on it, resting on a keyboard. (Photo: Pixabay, <https://tinyurl.com/yu6rnz55>, Free Use)

On June 6, President [Trump signed an executive order](#) to “reprioritize cybersecurity efforts to protect America,” outlining a rough agenda “to improve the security and resilience of the nation’s information systems...”



Jason Healey
X @jason_healey

Are cyber
defenders
winning?

Definition of *winning*:
Shifting systemic advantages
away from attackers

Problem: How to measure it?

Two principles, and a framework

1. Rely on data from those who are already collecting it, with scale and quality
2. Place that data into a context of **logical propositions**, to present a narrative of shifting advantages over time

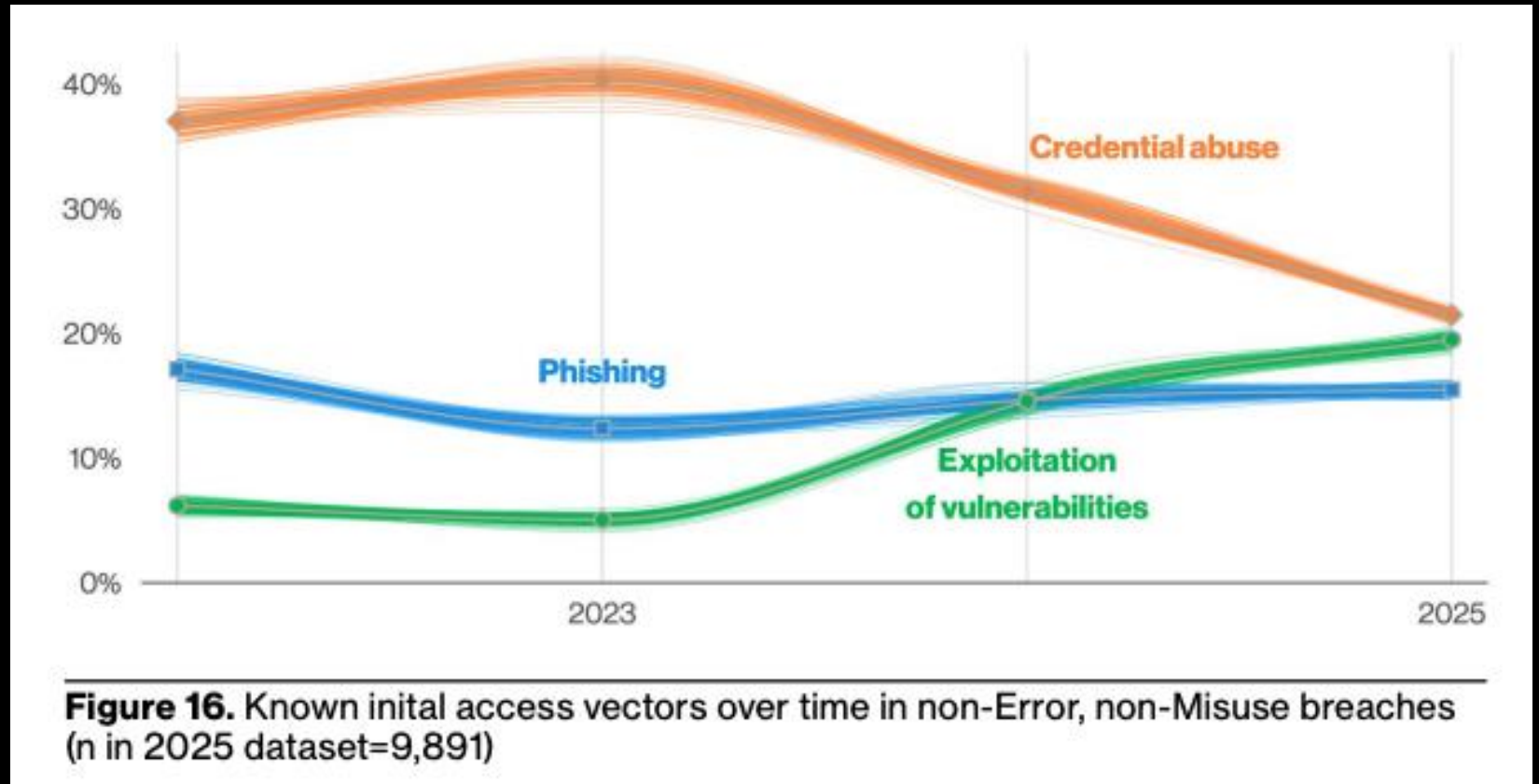
Table 1: Framework to Determine if Cyber Defenders are Winning		
Threat	Vulnerability	Impact
Operations	Software Ecosystem	System-wide Incidents
Ecosystem and Organization	Hardware Ecosystem	System-wide Costs
	Core Internet Infrastructure	Sectors, Systemically Important Entities and Groups
	Operational Technology	
	Sectors, Systemically Important Entities and Groups	

Table 1: Tracking advantage across threat, vulnerability, and impact.

Connect data to explanatory hypotheses, getting closer to proper science

Threat: Operations

Prop: Adversaries need to shift from easier to harder tactics, techniques, and procedures (TTPs)



Source: 2025 Verizon Data Breach Investigation Report

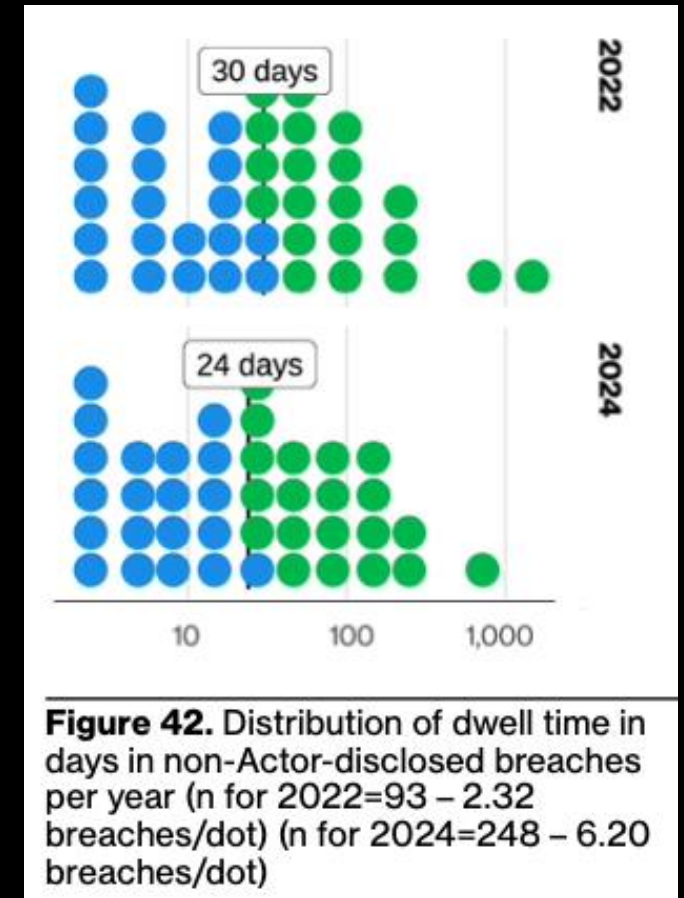
Threat: Operations

Adversaries are more quickly detected and ejected from their footholds within enterprises

Global Median Dwell Time, 2011-2023

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
All	416	243	229	205	146	99	101	78	56	24	21	16	10
External	—	—	—	—	320	107	186	184	141	73	28	19	13
Internal	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9

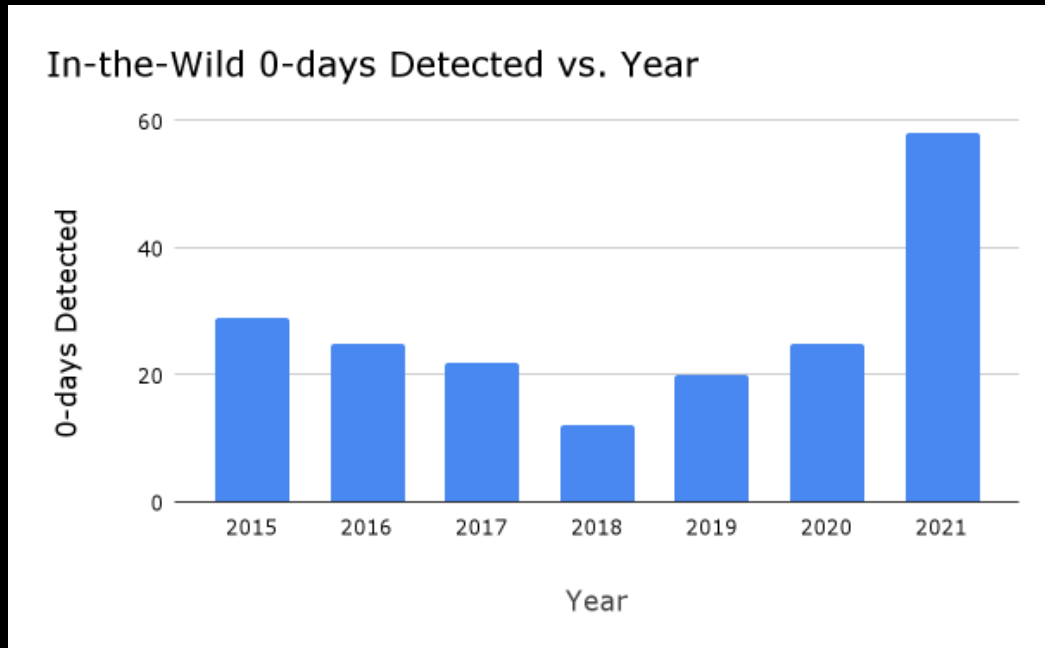
Source: 2024 Mandiant M-Trends Special Report



Source: 2025 Verizon Data Breach Investigation Report

Threat: Operations

Adversaries need to shift from easier to harder tactics, techniques, and procedures (TTPs)

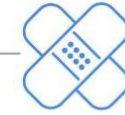


Source: Google Project Zero

Mandiant analyzed **138 exploited vulnerabilities** that were disclosed in 2023



70%
(97) of the vulnerabilities were first exploited as **zero-days**



Exploitation of an n-day vulnerability continues being most likely to occur before the end of the first month following the release of a patch



2021 & 2022



2023

We observed an **average Time-to-Exploit (TTE) of five days in 2023**, down notably from the previously observed average TTE of 32 days

We continue to assess that media attention and exploit availability do not guarantee exploitation, nor are they the primary indicators that a vulnerability will be exploited

Source: Mandiant 2024 Threat Intelligence Report

Attackers cannot keep exploiting the same vulnerabilities year after year

Threat: Operations

Other logical properties

- Adversaries need to rapidly update their TTPs
- Attackers must constantly rebuild their infrastructure
- More enterprises (and their key security vendors) detect adversaries themselves



Threat: Organization and Ecosystem

- If defenders are succeeding, then threat actors have lower profits.
- As a consequence of lower profits, threat actors become consolidated into larger, more capable groups.
- There is decreased trust between threat-actor groups, as they are targeted and infiltrated.
- Threat actors struggle to find talent: too risky



Vulnerability: Software

Table 1: Framework to Determine if Cyber Defenders are Winning		
Threat	Vulnerability	Impact
Operations	Software Ecosystem	System-wide Incidents
Ecosystem and Organization	Hardware Ecosystem	System-wide Costs
	Core Internet Infrastructure	Sectors, Systemically Important Entities and Groups
	Operational Technology	
	Sectors, Systemically Important Entities and Groups	

Table 1: Tracking advantage across threat, vulnerability, and impact.

- Vulnerabilities will be less stubborn as users patch more quickly, at scale
- Vulnerabilities will be less severe and less easily exploited by adversaries

Cobalt (pen testing co.):

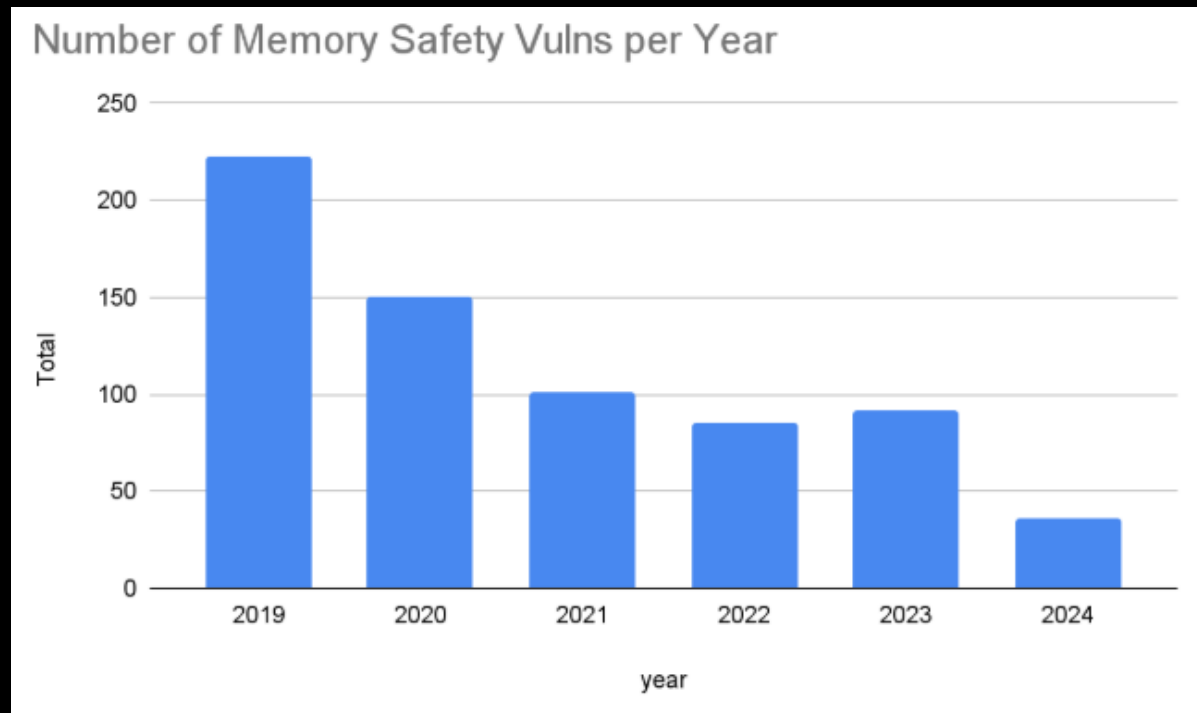
- The proportion of serious findings in pentests has declined from 20% to 11% over 10 years
- Since 2017, the median time to resolve serious vulnerabilities has decreased from 112 days down to 37 days



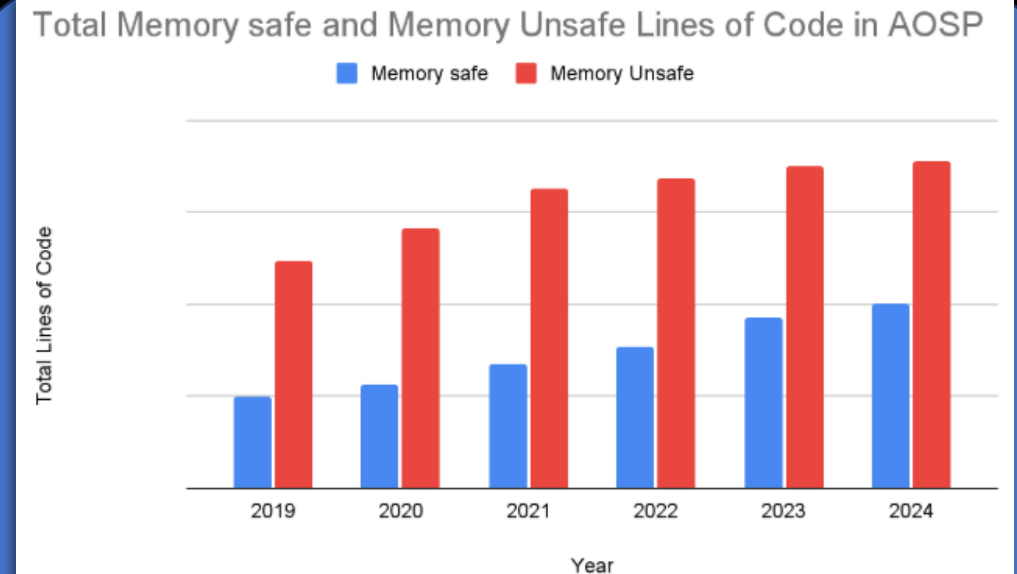
Source: Veracode 2025 Annual Report on the State of Application Security

Vulnerability: Software

- Vulnerabilities will be more diverse, as vendors improve security-by-design



Source: Google Security Blog



Vulnerability

Other logical properties, areas

- Software: There will be a reduced tail of abandoned code still used in critical systems



Table 1: Framework to Determine if Cyber Defenders are Winning		
Threat	Vulnerability	Impact
Operations	Software Ecosystem	System-wide Incidents
Ecosystem and Organization	Hardware Ecosystem	System-wide Costs
	Core Internet Infrastructure	Sectors, Systemically Important Entities and Groups
	Operational Technology	
	Sectors, Systemically Important Entities and Groups	

Table 1: Tracking advantage across threat, vulnerability, and impact.

Impact

- Fewer overall cyber incidents.
- Fewer records stolen in each incident and in aggregate.
- Fewer one-on-multiplicity and cascading cyber incidents.
- Fewer national-security-relevant incidents.

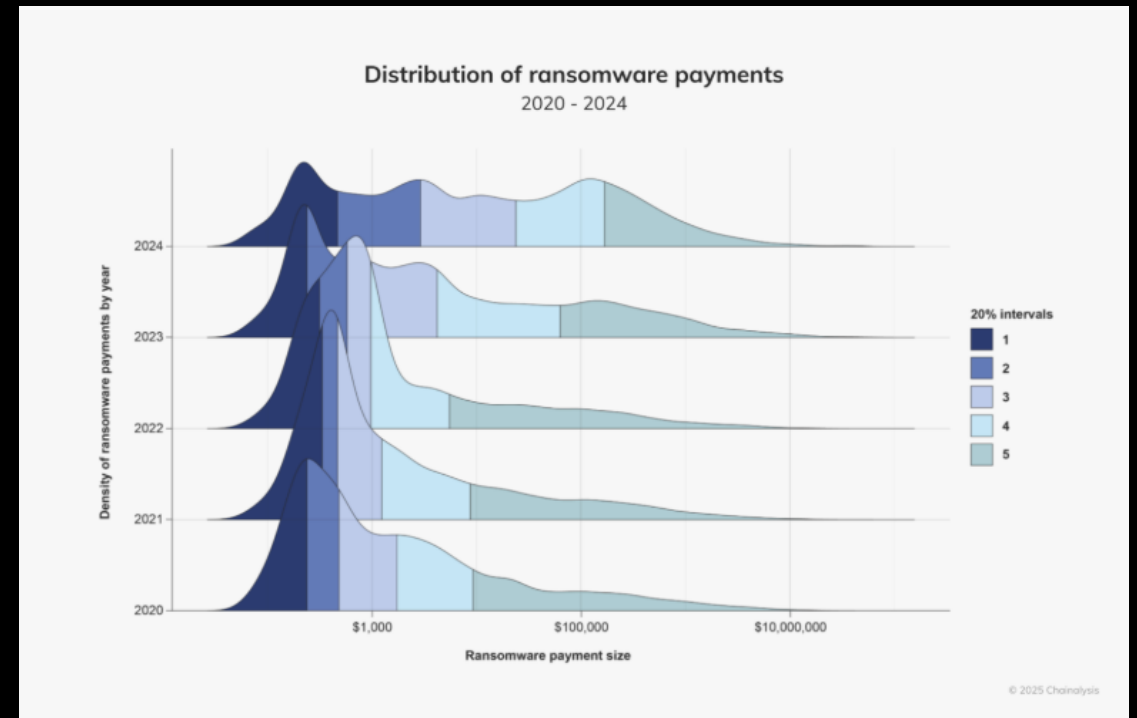
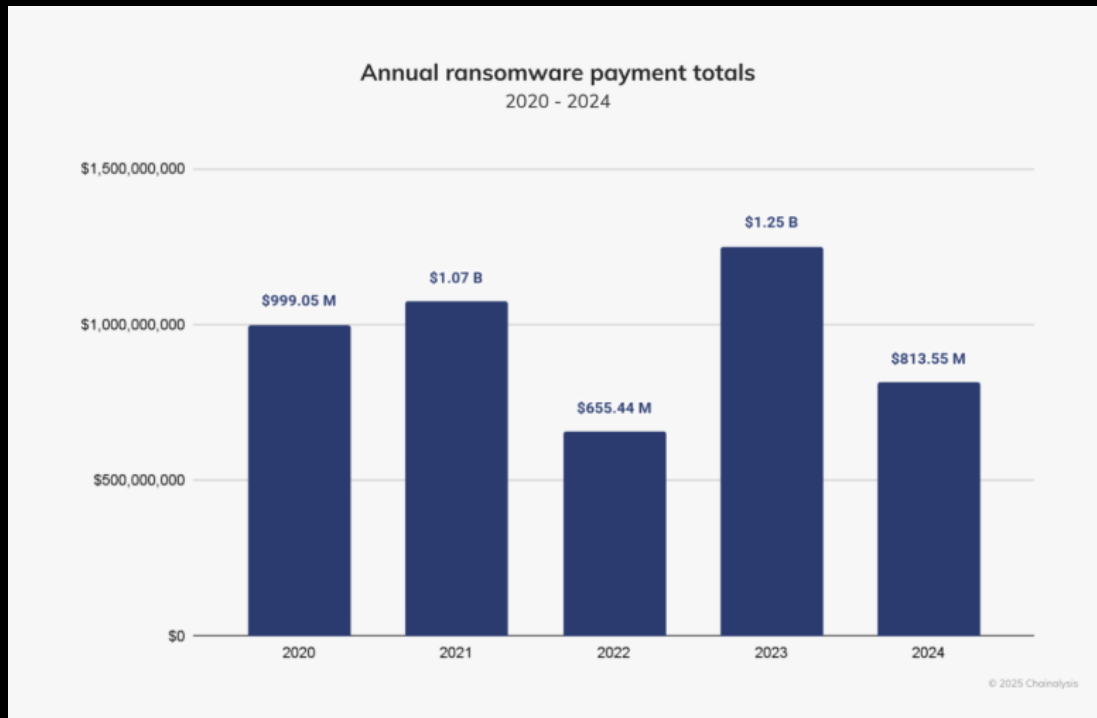
Table 1: Framework to Determine if Cyber Defenders are Winning		
Threat	Vulnerability	Impact
Operations	Software Ecosystem	System-wide Incidents
Ecosystem and Organization	Hardware Ecosystem	System-wide Costs
	Core Internet Infrastructure	Sectors, Systemically Important Entities and Groups
	Operational Technology	
	Sectors, Systemically Important Entities and Groups	

Table 1: Tracking advantage across threat, vulnerability, and impact.

- Reduced monetary losses from individual cyber incidents and cumulative economic impact.
- Fewer catastrophic cyber incidents.
- Fewer direct and indirect deaths from cyber incidents.

Impact: Costs

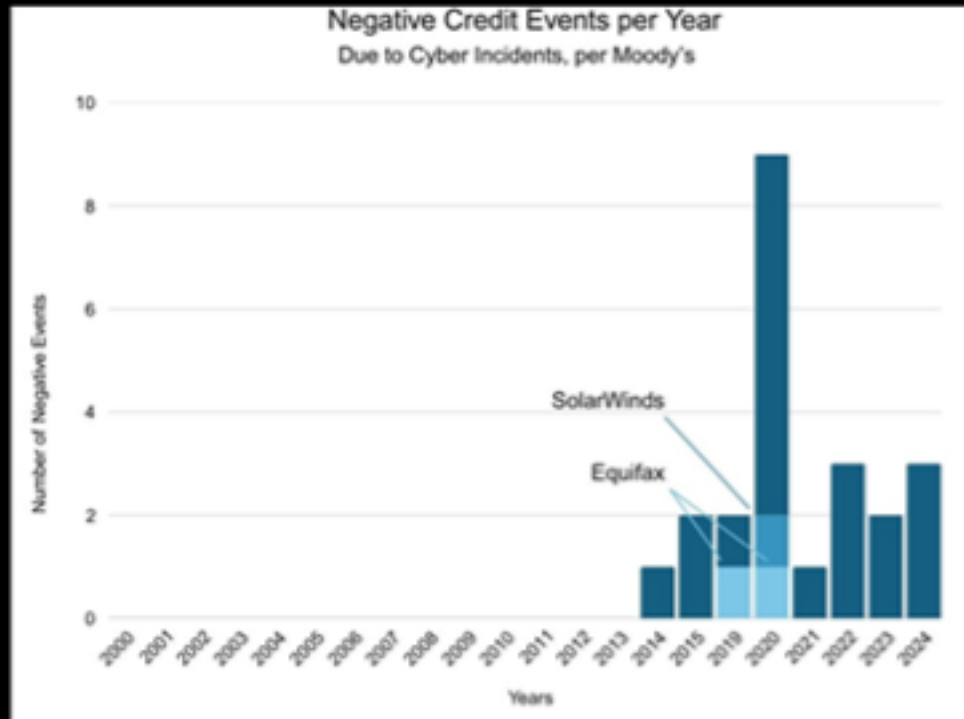
- Reduced monetary losses from individual cyber incidents and cumulative economic impact.



Source: Chainalysis 2025 report

Impact: Costs

- Reduced monetary losses from individual cyber incidents and cumulative economic impact.



Source: Moody's data, 2025



Source: FBI 2023 Internet Crime Report

Summing up

- Indicators gathered in this report seem to be going both directions:
 - Vulnerabilities are harder to exploit, with some counts are going down
 - Some costs are going down, but overall incidents and per-incident costs, remain high
- There is a lack of data for many of the logical propositions
- Next steps:
 - Create a more complete catalog of indicators across threat, vulnerability, and consequence
 - Encourage cybersecurity companies (and others with data) to report defensibility-relevant statistics in time-series, mapped to the catalog
 - Drive improved analysis and reporting

Discussion questions

- What do you think of the overall goal of the work?
- How could it be improved, both strategically and tactically?
- What data is missing, or most suspect?