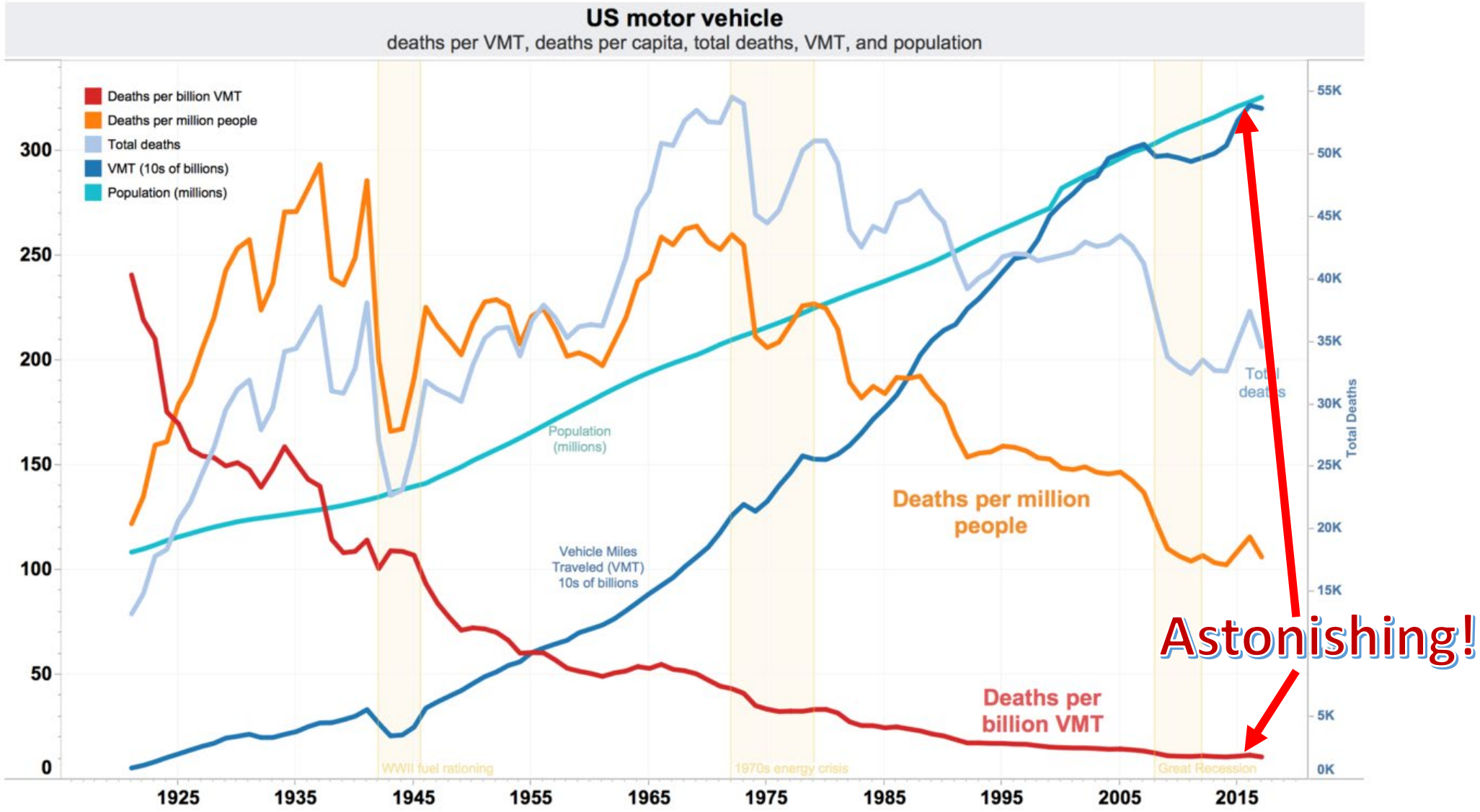
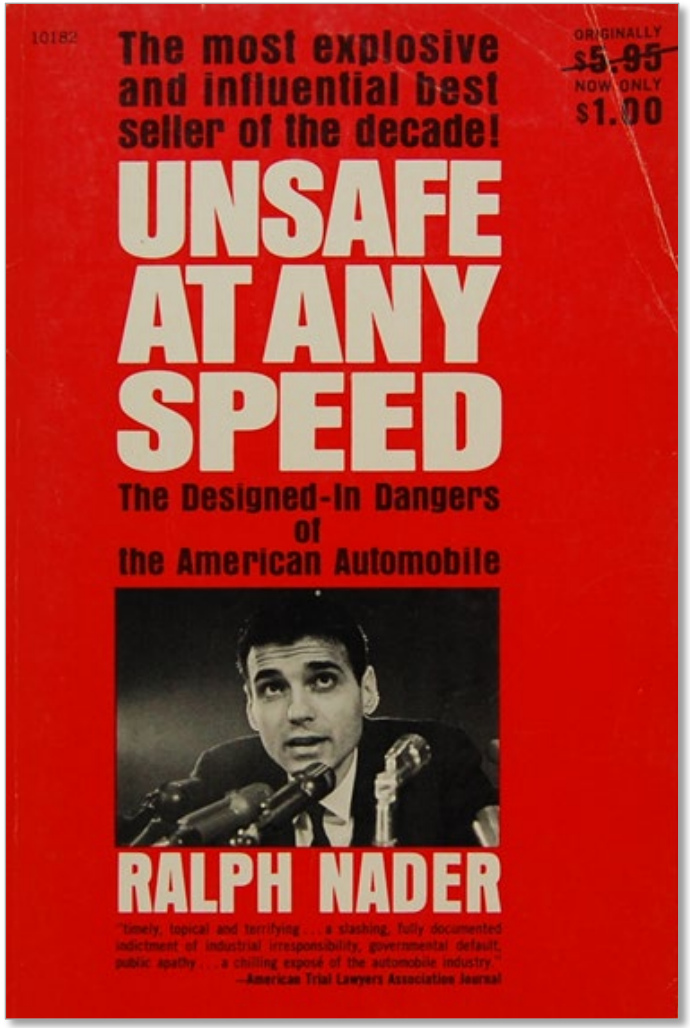
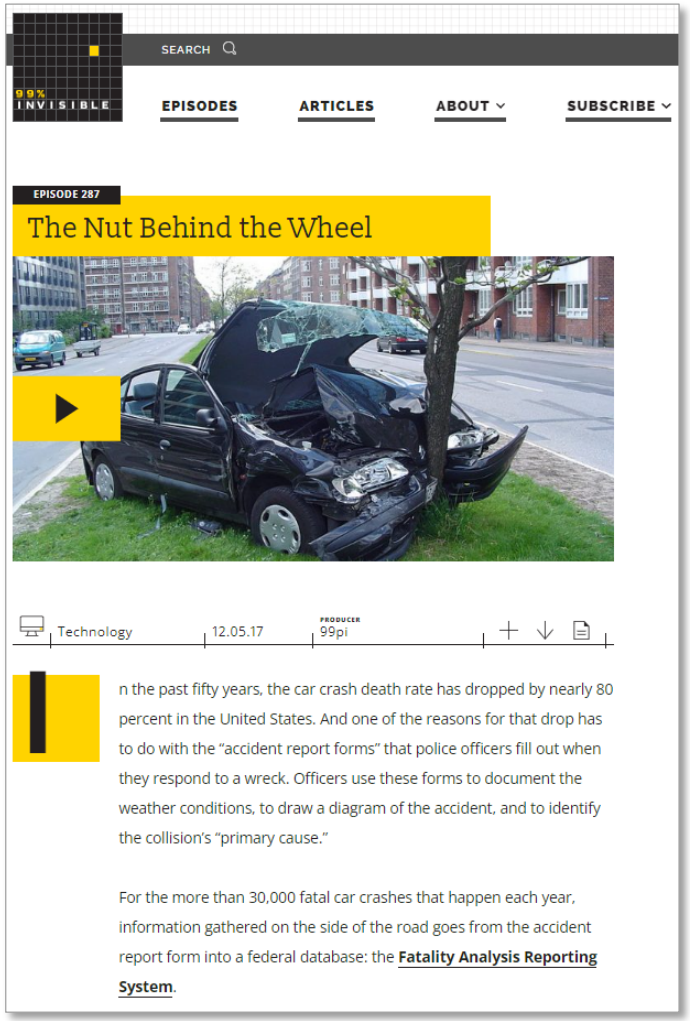
SECURE BY DESIGN & SECURE BY DEFAULT: CISA'S PATH FORWARD

JACK CABLE


US motor vehicle
deaths per VMT, deaths per capita, total deaths, VMT, and population
Deaths per billion VMT
Deaths per million people
Total deaths
VMT (10s of billions)
Population (millions)
300
250
200
150
100
50
0
55K
50K
45K
40K
35K
30K
25K
20K
15K
5K
0K
Total Deaths
Population (millions)
Vehicle Miles Traveled (VMT) 10s of billions
Deaths per million people
Deaths per billion VMT
Astonishing!
WWII fuel rationing
1970s energy crisis
Great Recession
1925
1935
1945
1955
1965
1975
1985
1995
2005
2015





In the past fifty years, the car crash death rate has dropped by nearly 80 percent in the United States. And one of the reasons for that drop has to do with the "accident report forms" that police officers fill out when they respond to a wreck. Officers use these forms to document the weather conditions, to draw a diagram of the accident, and to identify the collision's "primary cause."

For the more than 30,000 fatal car crashes that happen each year, information gathered on the side of the road goes from the accident report form into a federal database: the **Fatality Analysis Reporting System**.

Stop Passing the Buck on Cybersecurity

Why Companies Must Build Safety Into Tech Products

By Jen Easterly and Eric Goldstein February 1, 2023

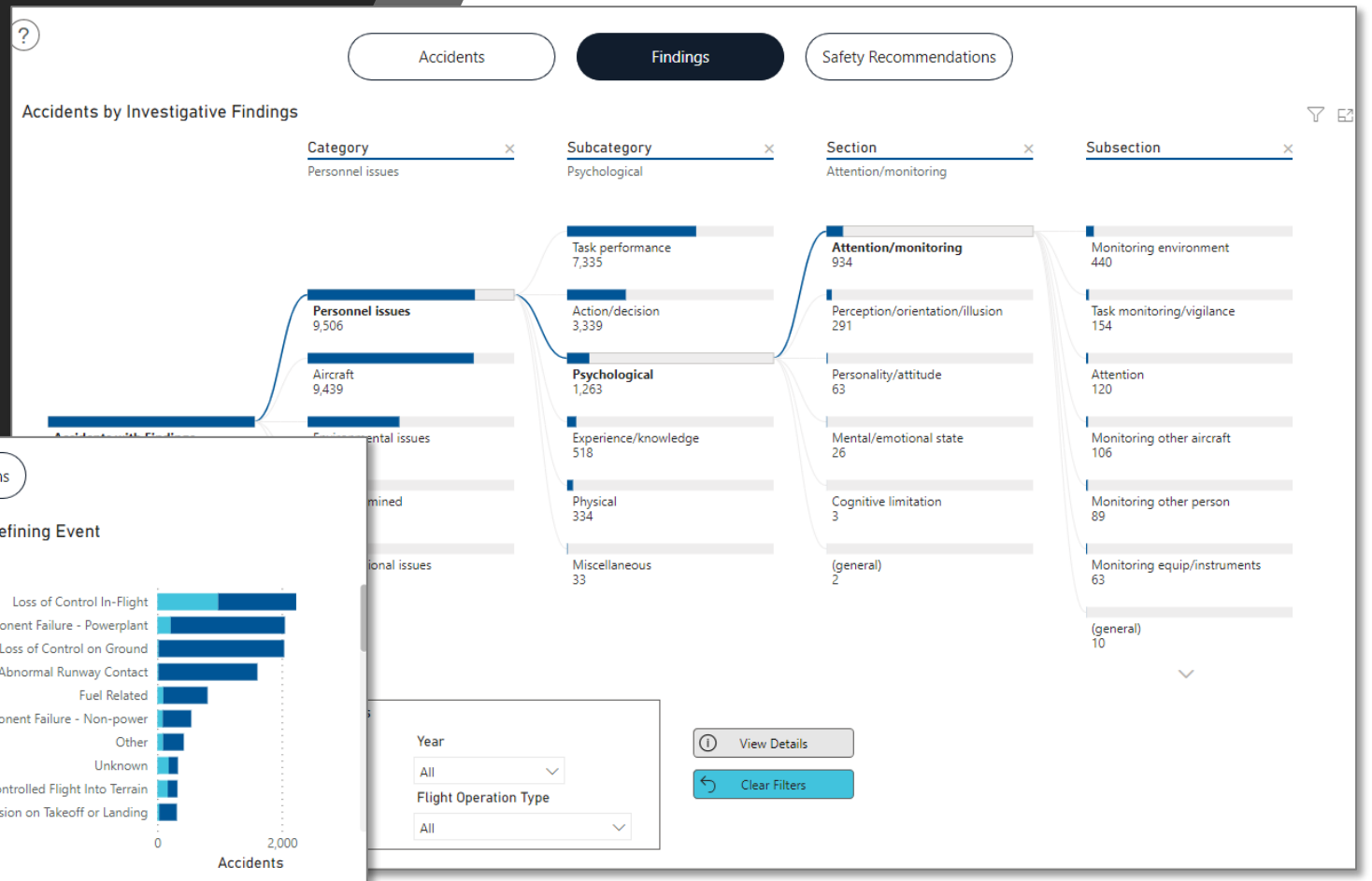
A man holding a laptop computer in Warsaw, June 2013
Kacper Pempel / Reuters

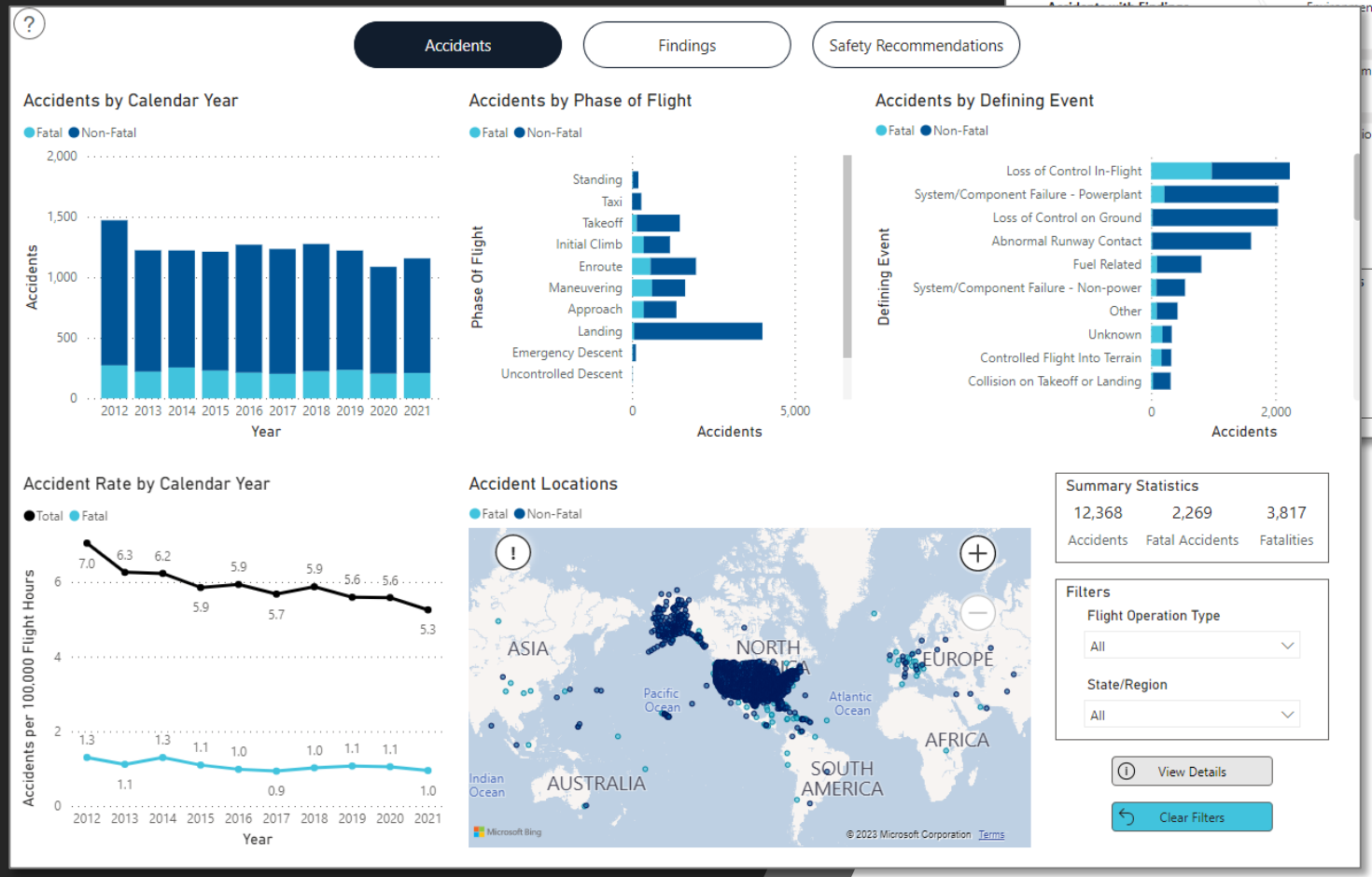
Despite a global multibillion-dollar cybersecurity industry, the threat from malicious cyber-activity, from both criminal and state actors, continues to grow. While many cyber incidents are never reported by their victims, Verizon's 2022 Data Breach Investigations Report noted that ransomware attacks rose 13 percent that year—more than the past five years combined. These breaches included attacks that threatened public health and safety, with several hospitals across the United States forced to cancel surgeries and divert patients because they were locked out of their systems.

Over the past decade, adversaries of the United States have developed increasingly sophisticated offensive cyber-capabilities. As cybersecurity

What do *mature* industries look like?

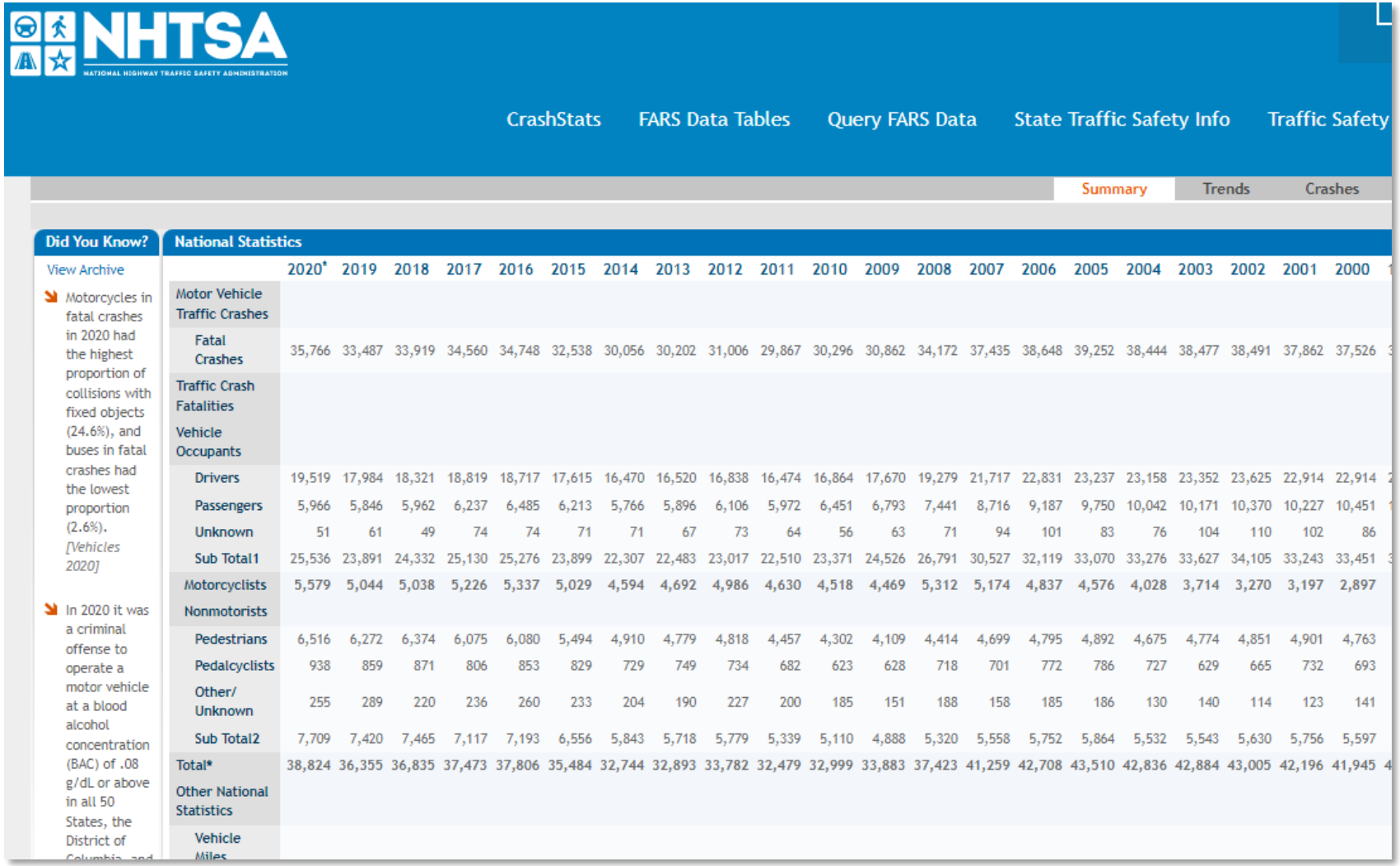
NTSB General Aviation Accident Dashboard





FARS

- Fatality Analysis Reporting System



NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

CrashStats | FARS Data Tables | Query FARS Data | State Traffic Safety Info | Traffic Safety

Summary | Trends | Crashes

Did You Know?

View Archive

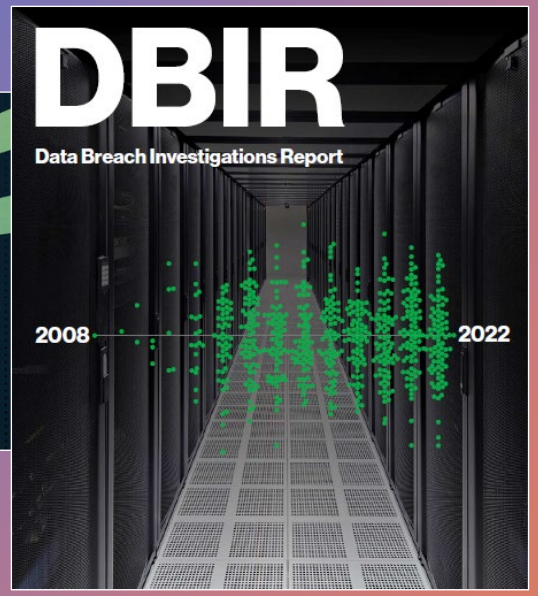
Motorcycles in fatal crashes in 2020 had the highest proportion of collisions with fixed objects (24.6%), and buses in fatal crashes had the lowest proportion (2.6%). *[Vehicles 2020]*

In 2020 it was a criminal offense to operate a motor vehicle at a blood alcohol concentration (BAC) of .08 g/dL or above in all 50 States, the District of Columbia, and

National Statistics

	2020*	2019	2018	2017	2016	2015	2014	2013	2012	2011	2010	2009	2008	2007	2006	2005	2004	2003	2002	2001	2000
Motor Vehicle Traffic Crashes																					
Fatal Crashes	35,766	33,487	33,919	34,560	34,748	32,538	30,056	30,202	31,006	29,867	30,296	30,862	34,172	37,435	38,648	39,252	38,444	38,477	38,491	37,862	37,526
Traffic Crash Fatalities																					
Vehicle Occupants																					
Drivers	19,519	17,984	18,321	18,819	18,717	17,615	16,470	16,520	16,838	16,474	16,864	17,670	19,279	21,717	22,831	23,237	23,158	23,352	23,625	22,914	22,914
Passengers	5,966	5,846	5,962	6,237	6,485	6,213	5,766	5,896	6,106	5,972	6,451	6,793	7,441	8,716	9,187	9,750	10,042	10,171	10,370	10,227	10,451
Unknown	51	61	49	74	74	71	71	67	73	64	56	63	71	94	101	83	76	104	110	102	86
Sub Total1	25,536	23,891	24,332	25,130	25,276	23,899	22,307	22,483	23,017	22,510	23,371	24,526	26,791	30,527	32,119	33,070	33,276	33,627	34,105	33,243	33,451
Motorcyclists	5,579	5,044	5,038	5,226	5,337	5,029	4,594	4,692	4,986	4,630	4,518	4,469	5,312	5,174	4,837	4,576	4,028	3,714	3,270	3,197	2,897
Nonmotorists																					
Pedestrians	6,516	6,272	6,374	6,075	6,080	5,494	4,910	4,779	4,818	4,457	4,302	4,109	4,414	4,699	4,795	4,892	4,675	4,774	4,851	4,901	4,763
Pedalcyclists	938	859	871	806	853	829	729	749	734	682	623	628	718	701	772	786	727	629	665	732	693
Other/ Unknown	255	289	220	236	260	233	204	190	227	200	185	151	188	158	185	186	130	140	114	123	141
Sub Total2	7,709	7,420	7,465	7,117	7,193	6,556	5,843	5,718	5,779	5,339	5,110	4,888	5,320	5,558	5,752	5,864	5,532	5,543	5,630	5,756	5,597
Total*	38,824	36,355	36,835	37,473	37,806	35,484	32,744	32,893	33,782	32,479	32,999	33,883	37,423	41,259	42,708	43,510	42,836	42,884	43,005	42,196	41,945
Other National Statistics																					
Vehicle Miles																					

How do we compare?



Sources of info

- **Private** fire brigade reports (no NTSB)
- Do they help?
  - Do they help customers?
  - Do they help manufacturers?
  - Do they show the same trendlines every issue?
  - Do they hold vendors accountable for software quality?

CISA Whitepaper

- On 4/13, CISA and 9 U.S. and international partners released a whitepaper on Secure by Design & Secure by Default
- This will be an iterative process – we look to many stakeholder verticals to help refine future iterations

TLP:CLEAR

National Cyber Security Centre

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

certnz

National Cyber Security Centre

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default

Publication: April 13, 2023

Cybersecurity and Infrastructure Security Agency

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

Disclaimer: This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

TLP:CLEAR

daily life. Internet-facing systems are
our economic prosperity, livelihoods, and
gement to medical care. As only one
ls cancelling surgeries and diverting patient
ties in critical systems may invite malicious
[1] risks.

anufacturers to make Secure-by-Design and
gn and development processes. Some
stry forward in software assurance, while
y encourage every technology manufacturer
omers from having to constantly perform
on their systems to mitigate cyber
ownership of improving the security
ogy manufacturers have relied on fixing
loyed the products, requiring the customers
by incorporating Secure-by-Design practices
lying fixes.

urity, the authoring agencies encourage
uct security as a critical prerequisite to
ring teams will be able to establish a new
ed-in and takes less effort to maintain.
einforces the importance of product security
ufacturers should implement security
nt manufacturers from introducing

ed products are safer for customers, the
their design and development programs to
ts to be shipped to customers. Products that
of the customers is a core business goal,
ducts start with that goal before
re those that are secure to use "out of the
sary and security features available without

[1] The authoring agencies recognize that the term "safety" has multiple meanings depending on the context its used. For the purposes of this guide, "safety" will refer to raising technology security standards to protect customers from malicious cyber activity.

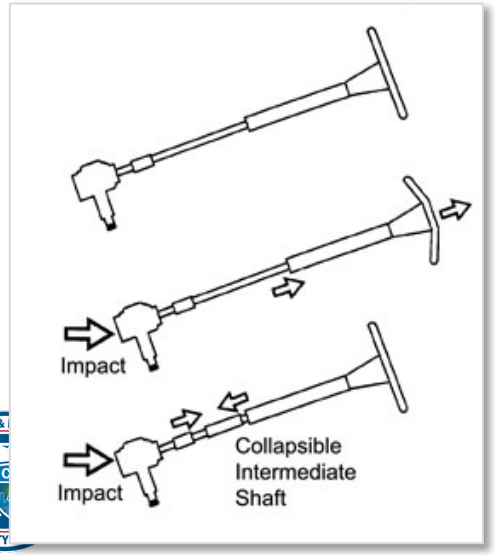
Underlying principles

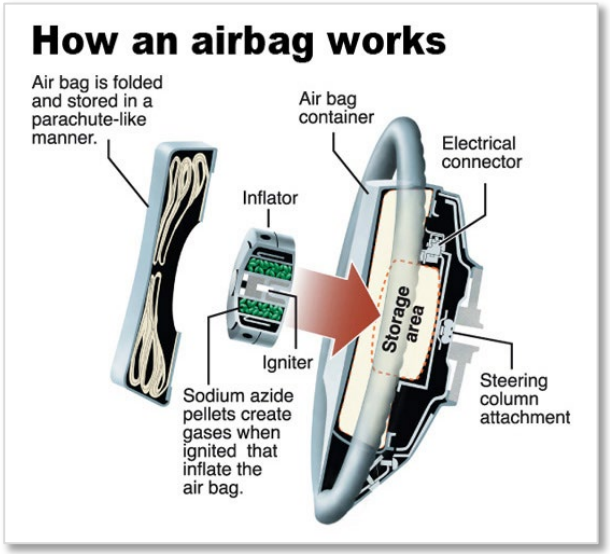
3 Principles

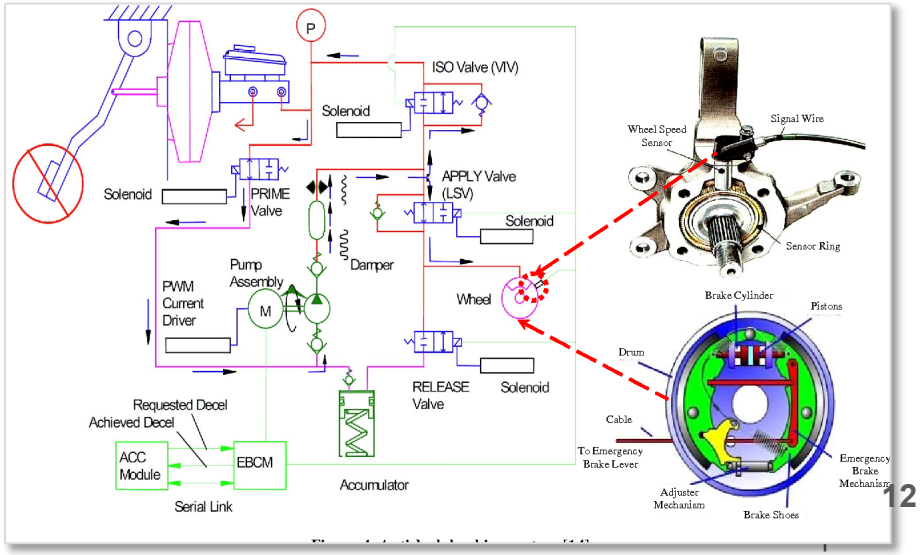
1. Manufacturers should take ownership of the security **outcomes** for their customers. The burden of safety should never fall solely upon the customer.
2. Manufacturers should embrace radical **transparency** and accountability.
3. Manufacturers should build **organization structure** and leadership to ensure safety is built in.

Security by Design

- Is a *business* goal of top *business leaders* and not delegated to tech teams
- Security is a formally stated goal *before* the design process begins
- Requires real tradeoffs, like changing programming languages
- Can't be bolted on later. Think: collapsible steering columns, airbags, ABS







Costs of lack of safety by design

EMPI

TAKE THE TWIST OUT OF THOSE SWING AXLES

EMPI CAMBER COMPENSATOR®
Probably the best single suspension modification you can make on a Corvair, Volkswagen, Tempest, or other swing axle rear end is the addition of a Camber Compensator®.
The Camber Compensator® links both half axles into a fully integrated spring suspension system that keeps both wheels working when cornering or driving in gusty winds.
This specially designed heavy-duty transverse spring linkage shackles to the axles just behind the wheel hubs, with a center pivot point at the differential housing. The stabilizing effect of this simple modification is literally amazing. Cornering loads are shared by both wheels. The result is improved handling and road holding stability, particularly at speed.
Kits come complete with all fittings and hardware. **$19.95** and **$24.95.**

EMPI TRACK-TRU SWAY BARS
These new anti-sway bars are second generation improvements over earlier models. They have been extensively tested at Riverside International Raceway and have an even higher degree of stability than their quite successful forebears. These new models are husky enough to withstand the rigors and extreme stresses of race competition.
The TRACK-TRU front bar will add considerably to the safety and driving ease of any Chevy II, Volkswagen or Corvair passenger car or truck. It will improve steering and reduce the effect of crosswinds.
TRACK-TRU bars are cad plated for rust protection. The installation is quite a calm affair, requiring no welding or cutting. The kit comes complete with everything you need except manpower.
$17.95 and **$19.95.**

EMPI CAMBER COMPENSATOR®
☐ Corvair passenger cars and trucks, Porsche 1957-61 and Tempest passenger cars.....**$24.95**
☐ All VW cars, trucks, Ghias thru '63, plus Renaults '57-'62.....**$19.95**
☐ Porsche 1956-57.....**$21.95**
EMPI TRACK-TRU front anti-sway bars.
☐ All Corvairs, Chevy IIs, and VW trucks and station wagons.....**$19.95**
☐ All VW passenger cars.....**$17.95**
Be sure to state year, make and model. Enclose full amount with your order and **EMPI** will pay shipping anywhere in the continental U.S. Californians add 4% tax.

EMPI

SEE YOUR DEALER
OR ORDER DIRECT
P. O. BOX 668, RIVERSIDE 4, CALIFORNIA

JUNE 1963 7

Camber Compensator for your lovely Corvair

- "…keeps both wheels working when cornering or driving in gusty winds"
- "The result is improved handling and road holding stability, particularly at speed"

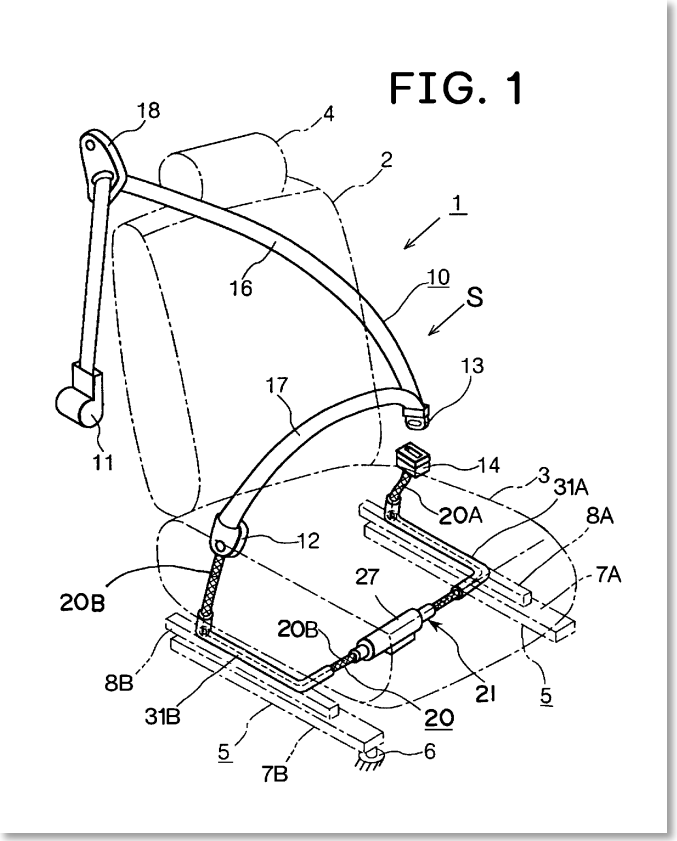
Examples of Secure by Design

- Memory-safe programming languages
- Secure hardware foundation
- Secure software components
- Parametrized queries
- SBOMs
- Vulnerability disclosure policies w/ legal safe harbor
- *And more…*

Security by Default

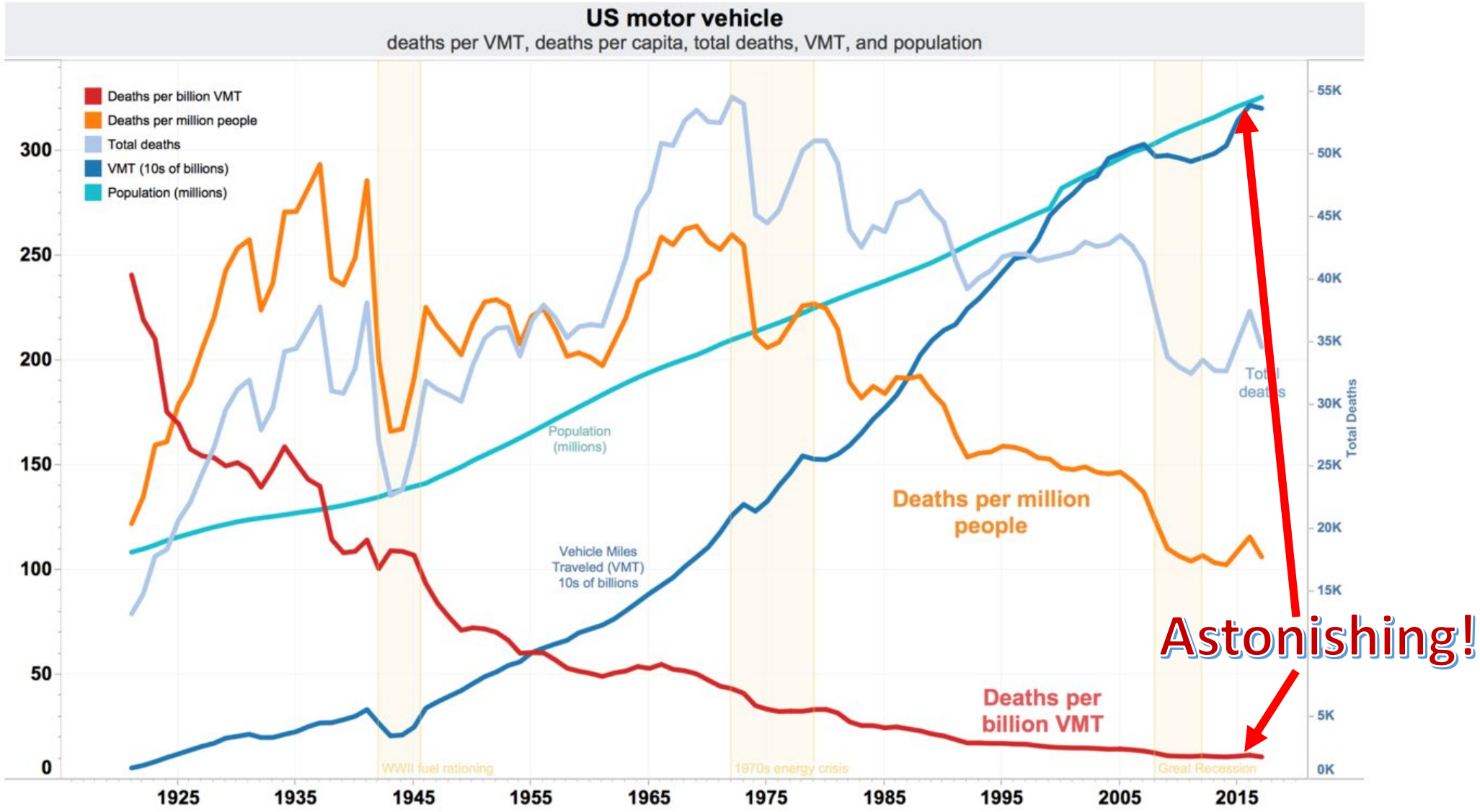
Security by Default

- Secure configs are the baselines out of the box
- Keeping configs secure should be the responsibility of the manufacturer
- Strong nudges to be more secure, like MFA
- Transform “hardening guides” into “loosening guides”
- Requires no new licenses or costs
- Comes in every product, like seatbelts
  (that used to be an up-charge)



Examples of Secure by Default

- Eliminating default passwords
- Single sign-on at no additional cost
- High-quality audit logs at no extra charge
- Reducing “hardening guide” size
- Security setting user experience
- *And more…*


US motor vehicle
deaths per VMT, deaths per capita, total deaths, VMT, and population
Deaths per billion VMT
Deaths per million people
Total deaths
VMT (10s of billions)
Population (millions)
300
250
200
150
100
50
0
55K
50K
45K
40K
35K
30K
25K
20K
15K
5K
0K
Total Deaths
Population (millions)
Vehicle Miles Traveled (VMT) 10s of billions
Deaths per million people
Deaths per billion VMT
Astonishing!
WWII fuel rationing
1970s energy crisis
Great Recession
1925
1935
1945
1955
1965
1975
1985
1995
2005
2015

Where is the best CVE analysis?

- Why is there a difference between the memory safety numbers that manufacturers self-report, and what is in the CVE database?
- What if a car manufacturer's internal numbers were different from the NHTSA's public numbers?

https://www.cvedetails.com/

CVE Details

The ultimate security vulnerability datasource

Log In Register **Take a third party risk management course for FREE**

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles

CVSS Score Distribution For Top 50 Vendors By Total Number Of "Distinct" Vulnerabilities

	Vendor Name	Number of Total Vulnerabilities	# Of Vulnerabilities									Weighted Average
			0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+	
1	Microsoft	9285	481	111	635	250	1728	986	947	1916	40	2191	6.70
2	Oracle	9023	246	148	442	569	2675	2520	1017	772	42	592	5.80
3	Google	8157	836	55	738	100	1984	691	1243	1338	37	1135	6.00
4	Debian	7980	278	94	444	214	2213	1573	1576	1263	24	301	6.00
5	Apple	5981	284	58	396	55	1146	716	1554	786	17	1019	6.60
6	IBM	5609	186	64	370	987	1489	1049	550	539	27	398	5.60
7	Redhat	4801	162	72	358	222	1311	817	752	736	16	355	6.00
8	Cisco	4380	114	6	96	193	961	912	565	987	47	499	6.60
9	Fedoraproject	4373	422	37	210	126	1222	863	903	481	14	95	5.50
10	Canonical	3895	5	56	256	133	1215	681	576	680	10	283	6.20
11	Linux	3097	205	106	476	85	921	164	232	767	10	131	5.50
12	Opensuse	3066	7	47	194	108	834	597	561	402	5	311	6.30
13	Mozilla	2507	155	12	78	8	541	442	321	400	1	549	6.70
14	Netapp	1903	114	26	118	72	688	405	258	191	7	24	5.40
15	Apache	1883	153	11	45	45	441	581	203	305	6	93	5.90
16	HP	1839	12	11	70	44	299	263	136	400	20	584	7.40
17	SUN	1530	3	26	98	44	290	271	108	404	3	283	6.80
18	Adobe	1483	75		19	16	240	146	97	96	4	790	7.90
19	Jenkins	1362	172	1	58	199	554	150	190	26	1	11	4.80
20	SAP	1236	97	3	31	73	378	289	178	124	3	60	5.60
21	Suse	997	16	19	81	20	210	121	128	173		229	6.70
22	GNU	964	28	12	53	33	258	208	180	153	2	37	6.00
23	Siemens	931	85	5	37	31	180	203	234	116	9	31	5.80

The Goal

How can CVE allow determining authoritative root causes of vulnerabilities?

And how can CVEs become the foundation for tech starting to look like more mature industries?

Questions

E.g., what percent of vulnerabilities in memory unsafe languages are memory related? In memory safe languages?

How does this change over time?

How do different products manage defects?

As it stands

- ~10% of vulnerabilities in the KEV are solely tagged as CWE-20, Improper Input Validation
  - This isn't a root cause
- Automated analysis gap:
  - Automated analysis of the KEV: ~30% of vulnerabilities are memory related (~47% in C/C++)
  - Manual analysis of the KEV: ~40% of vulnerabilities are memory related (~56% in C/C++)

  * This data is not fully representative but gives a rough picture of where we are at.

  Source: Chris Palmer, Taxonomy Of In-The-Wild Exploitation (https://noncombatant.org/2022/04/22/itw-taxonomy/)

Gaps in vendor-reported data

- Significant gaps in vendor-reported data and what can be gleaned from CVE:

Vendor	% Memory safety from CVE data (via CWEs)	% Memory safety from self-reported data	% of CVE records unmappable to CWE
Vendor 1	61%	66%	23%
Vendor 2	50%	70%	15%
Vendor 3	32%	70%	53%

Source: HSSEDI research

CISA's Secure by Design Strategy

- CISA's Secure by Design work involves several workstreams:
  - Establishing CISA's work to advance Secure by Design & Security by Default
  - Collecting data and best practices to understand what "good" looks like
  - Outside engagement to foster tech ecosystem safety:
    - Working with technology manufacturers to incentivize software that is secure by design and secure by default
    - Encouraging organizations to demand more from their technology vendors
    - Working with educators to integrate security into computer science and other technology-related courses
    - Engaging multiple regions and stakeholder communities

Our Next Steps

- The whitepaper is the first iteration of CISA's Secure by Design work. We look to stakeholders to provide feedback & shape our work here.
- Opportunities for feedback:
  - Future iterations of this whitepaper
  - Sector-Specific Cyber Performance Goals
  - Other potential guidance

Your next steps

- Review the whitepaper and linked documentation
- Think about the history of safety in other fields
- Reach out to us & share your input!
- Think about how your work can drive Secure by Design & Secure by Default

For more information:

https://www.cisa.gov/securebydesign

SecureByDesign@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

Secure by design ecosystem

- Manufacturers
- IT/OT/IoT
- Open-source community
- Education (university, and self-taught)
- Customers
  - CIOs
  - Small and Medium Orgs
- Insurance
- Venture Capital firms
- Secure researchers/hackers
- Integrators
- Interagency partners
- IR firms
- Standards bodies
- Regulators/legislators
- Target rich/cyber poor orgs
- ISACs

Shifting the Balance

Product development

Customer deployment

SDLC: Pre-shipment
Preventative, detective controls (ex: code analysis tools)

SDLC: Post-shipment
Reactive controls (ex: fixing bugs detected at customer sites)

Move *existing* costs & risks left

Left of Boom

Hard costs
Security products, staff, SSO tax, insurance, consultants, counsel

Soft Costs
Deploying hardening guides, training staff, patching, adopting CISA CPGs

Right of Boom

Hard costs
Response to incidents (potential and confirmed), IR firms, outside counsel

Soft Costs
Response to incidents (potential and confirmed), managing IR firms & outside counsel, lost executive productivity

National security delta: The sum of individual risks creates an even larger national security risk though supply chain and other connections.

Bottom line: Customers already pay a silent security tax. We want to shift that poorly measured and unevenly distributed tax to the left, reducing the overall costs and risks to customers.

Residual Business Risks
Few can pay all hard and soft costs
➔ Customer loss, reputation, other risks