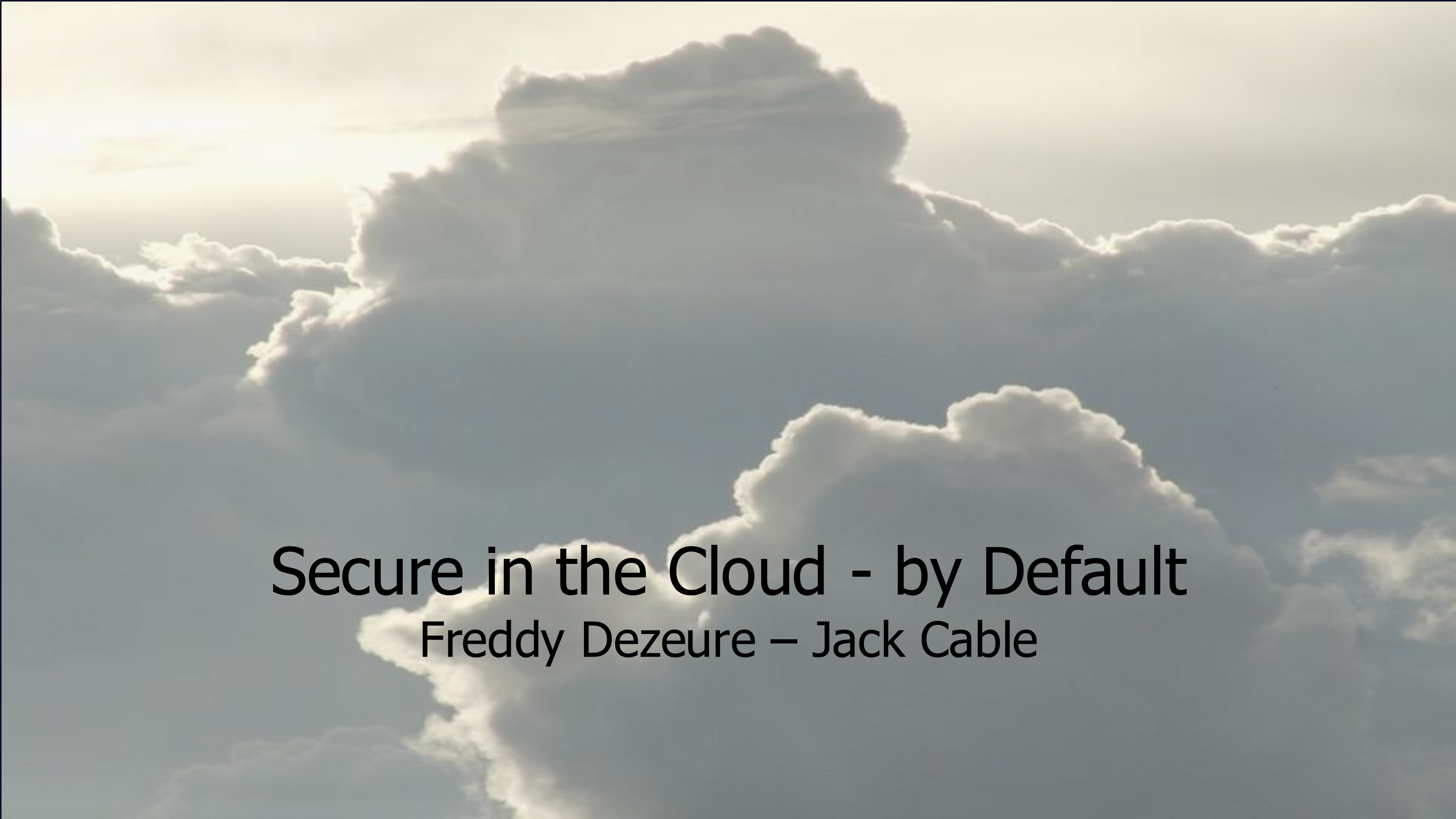


Secure in the Cloud - by Default

Freddy Dezeure – Jack Cable

Who Are We?

Freddy Dezeure

Independent Strategic Advisor

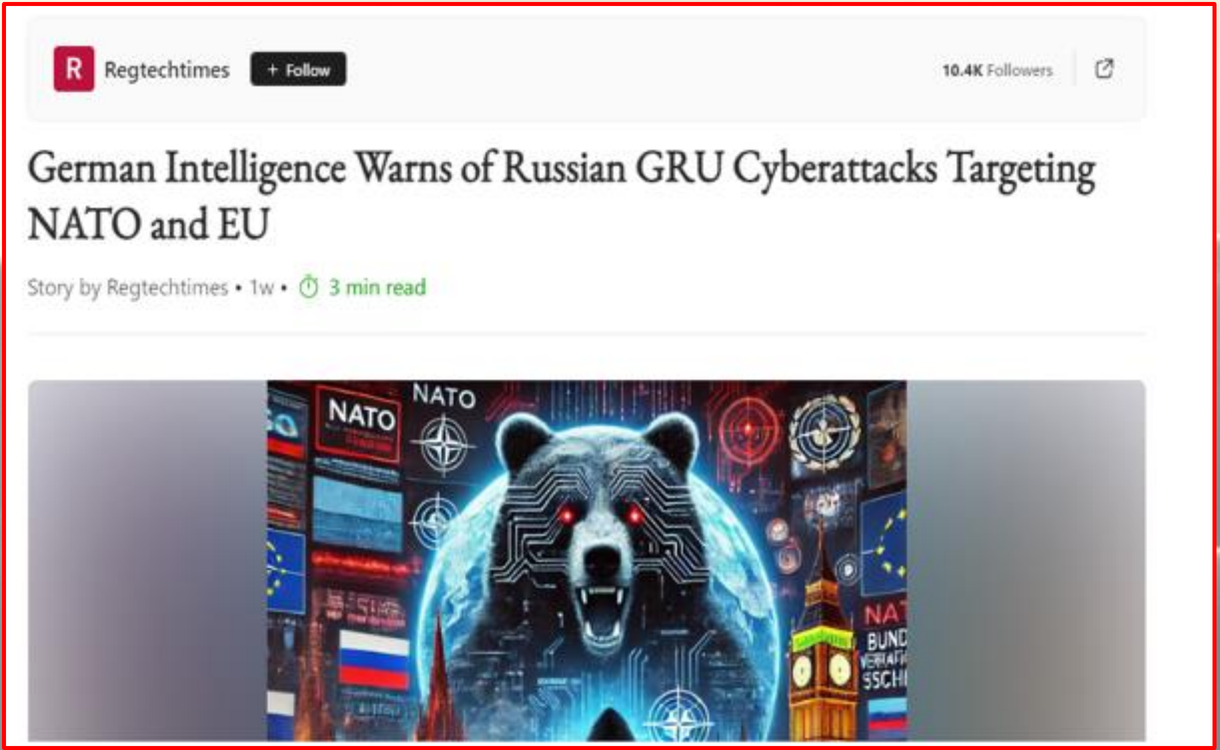
CERT-EU founder

Jack Cable

Senior Technical Advisor

U.S. Cybersecurity & Infrastructure Security Agency (CISA)

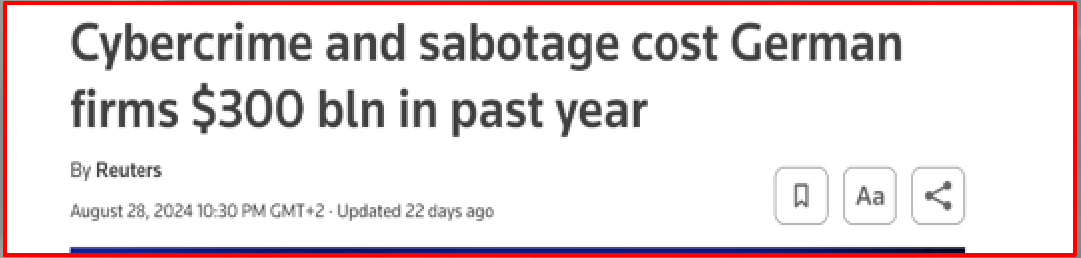
Sept. 2024



German Intelligence Warns of Russian GRU Cyberattacks Targeting NATO and EU

Story by Regtechtimes • 1w • 3 min read

August 2024



Cybercrime and sabotage cost German firms $300 bln in past year

By Reuters

August 28, 2024 10:30 PM GMT+2 · Updated 22 days ago

Managing the world’s infrastructure

Cloud (IAAS): 70% market share

Office automation (SAAS): 100% market share

CapEx: 100 $bn/year (2024)

Microsoft

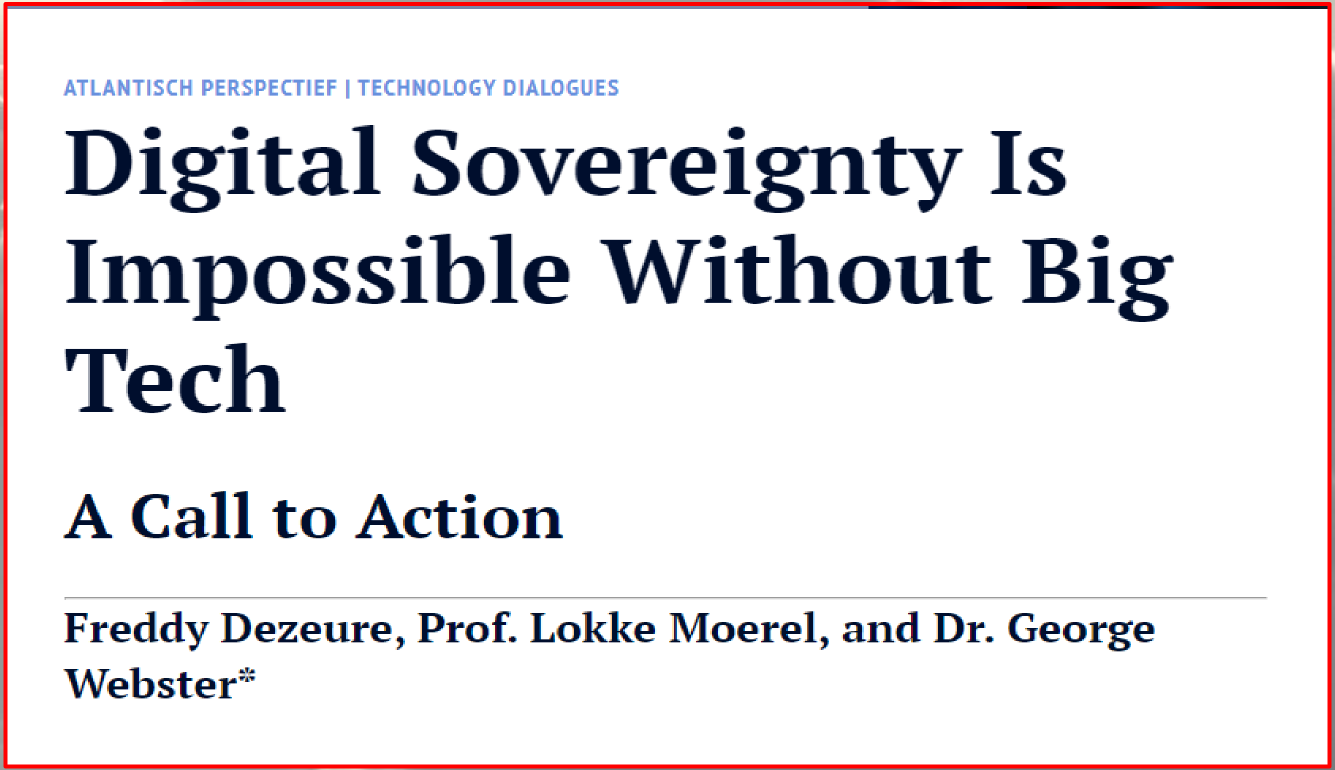
aws

Google Cloud

[Gartner Says Worldwide IaaS Public Cloud Services Revenue Grew 16.2% in 2023]

[Tech giants pour billions into cloud capacity in AI push]

Dec. 2023



ATLANTISCH PERSPECTIEF | TECHNOLOGY DIALOGUES

Digital Sovereignty Is Impossible Without Big Tech

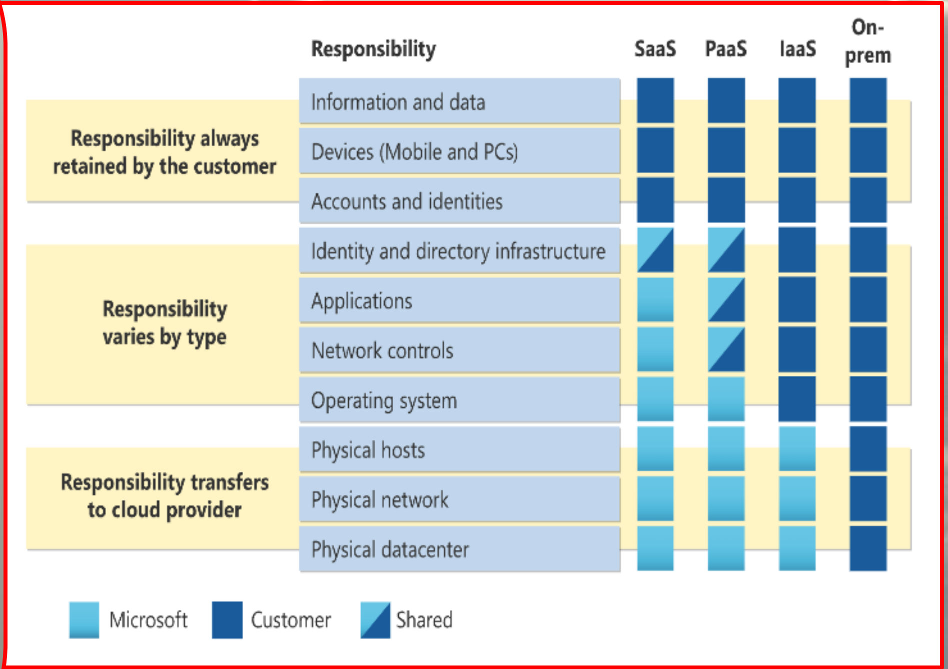
A Call to Action

Freddy Dezeure, Prof. Lokke Moerel, and Dr. George Webster*

What is the issue?

"Shared Responsibility Model"

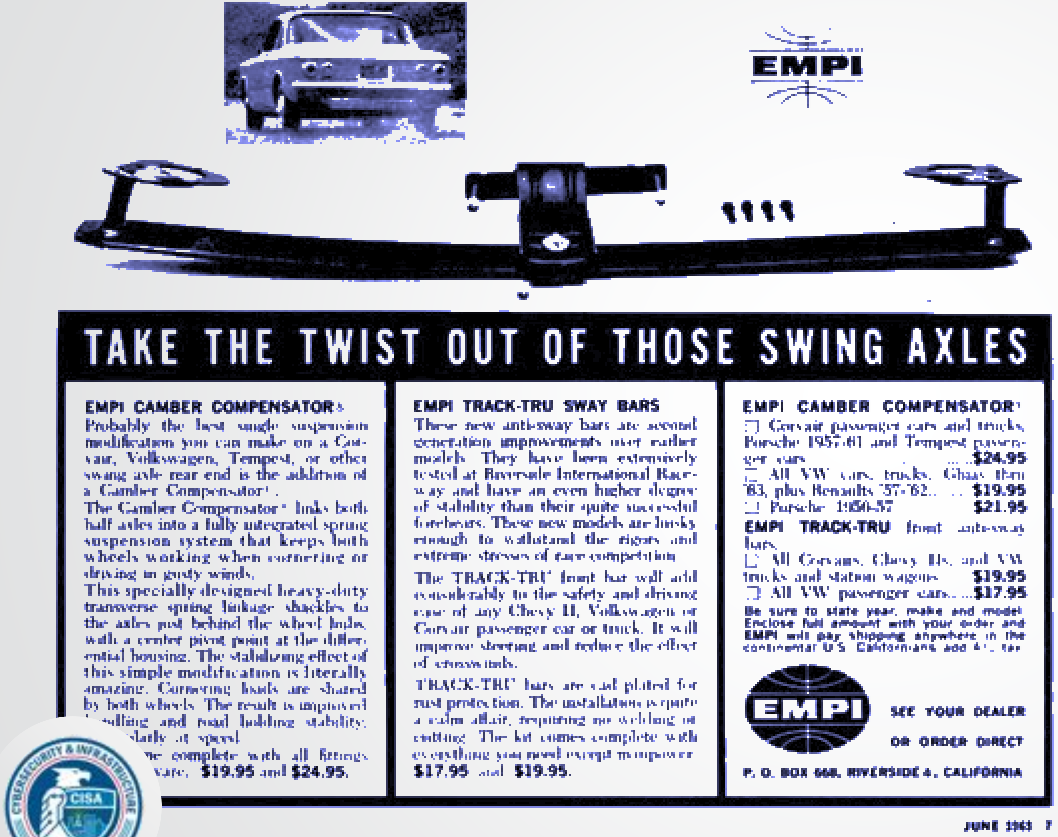
- CSPs rely on customers to implement secure settings
- Customers lack capacity and expertise
- Most organizations are not / will never be secure
- Thriving economy of criminals hacking our infrastructure and vendors promising to protect it



	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	□	◩	■	■
	Network controls	□	◩	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◩ Shared

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA



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 [illegible]ndling and road holding stability, [illegible]larly at speed. [illegible]me complete with all fittings [illegible]ware. **$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 1950-57 **$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

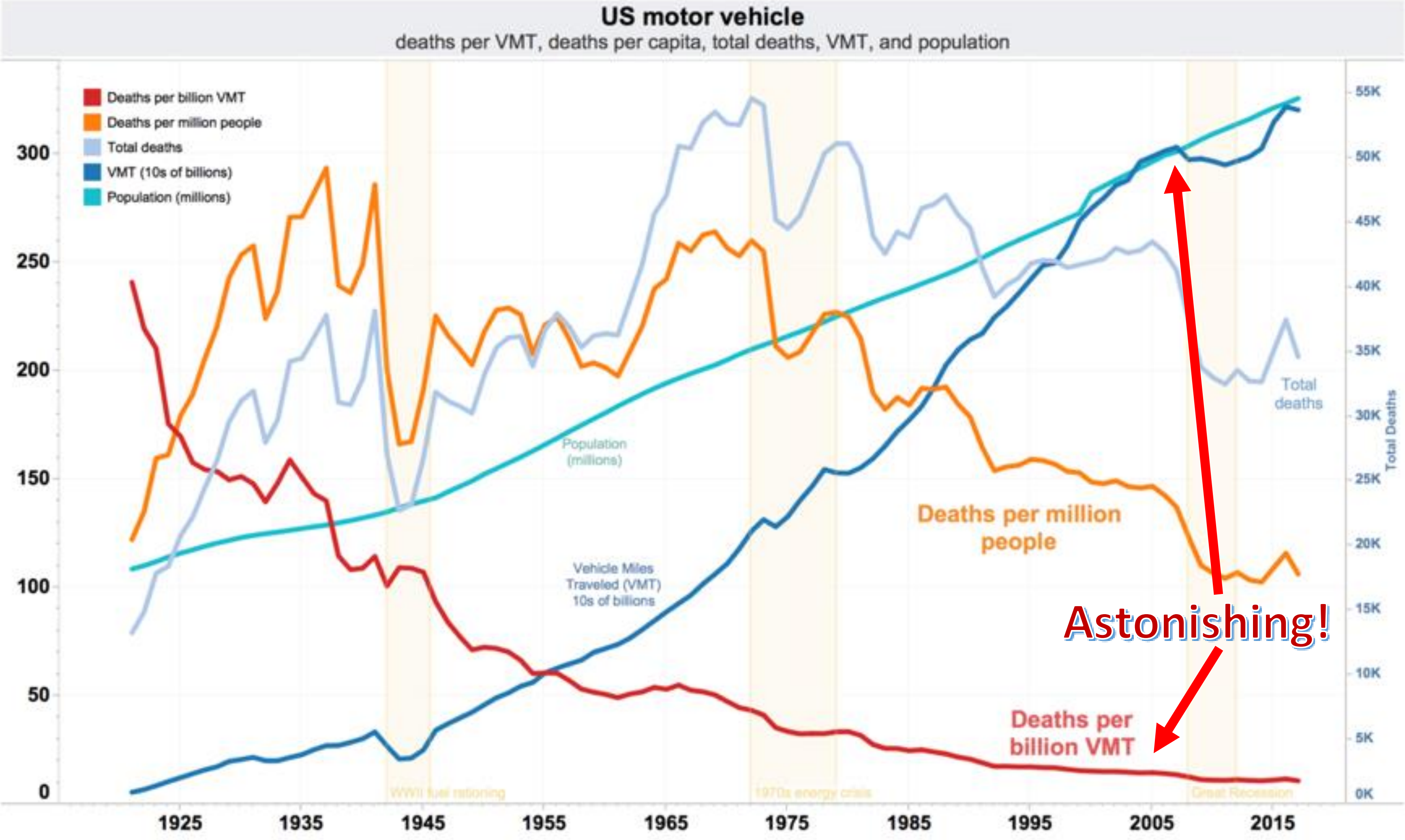
OR ORDER DIRECT

P. O. BOX 668, RIVERSIDE 4, CALIFORNIA

> *…keeps both wheels working when cornering or driving in gusty winds*

> *The result is improved handling and road holding stability, particularly at speed*

Other industries have undergone **radical** transformations to prioritize safety & security



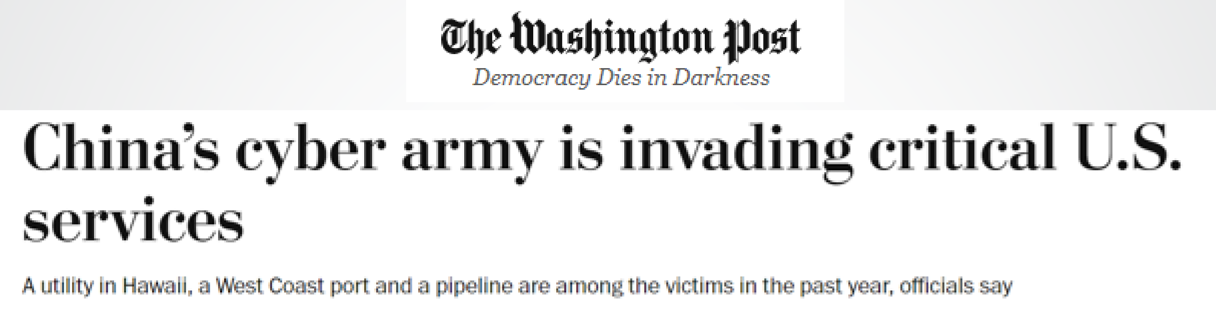
US motor vehicle

deaths per VMT, deaths per capita, total deaths, VMT, and population

Astonishing!

How does the software industry stack up?

Basic, preventable classes of vulnerabilities are causing significant harm

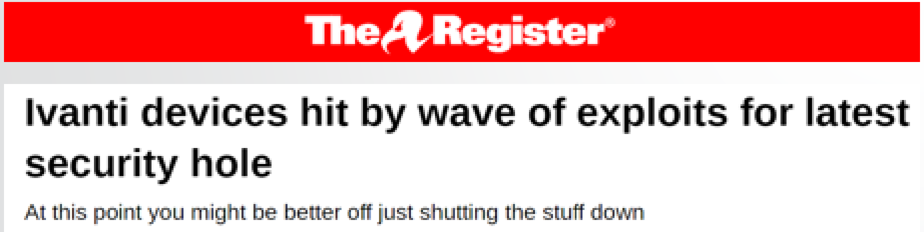


The Washington Post

Democracy Dies in Darkness

China’s cyber army is invading critical U.S. services

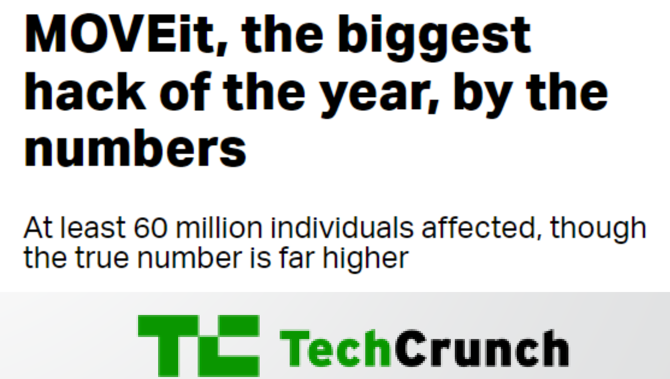
A utility in Hawaii, a West Coast port and a pipeline are among the victims in the past year, officials say



The Register®

Ivanti devices hit by wave of exploits for latest security hole

At this point you might be better off just shutting the stuff down



MOVEit, the biggest hack of the year, by the numbers

At least 60 million individuals affected, though the true number is far higher

TechCrunch

THE BURDEN FALLS ON END USERS

SECURITY PRODUCTS

LOGS

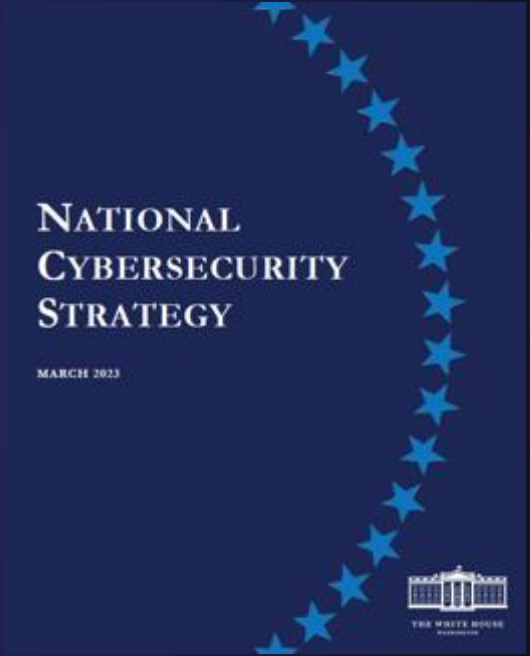
PATCHES

IAM

GUIDES

U.S. National Cybersecurity Strategy

"We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organizations that are **most capable** and **best-positioned** to reduce risks for all of us."



NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE

WASHINGTON

CISA's Secure by Design Whitepaper

SECURE BY DESIGN

SHIFTING THE BALANCE OF CYBERSECURITY RISK:

PRINCIPLES AND APPROACHES FOR SECURE BY DESIGN SOFTWARE

CISA
ASD
ACSC
Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
National Cyber Security Centre
National Cyber Security Centre
CSIRTAmericas Network
NISC
CSA SINGAPORE
certnz
NSM NORWEGIAN NATIONAL CYBER SECURITY CENTRE
National Cyber and Information Security Agency
KISA KOREA INTERNET & SECURITY AGENCY
JPCERT CC

SECURE BY DESIGN PRINCIPLES

1. Take ownership of customer security outcomes

2. Radical transparency and accountability

3. Lead from the top

SECURE BY DESIGN

PLEDGE

GOALS

MULTIFACTOR AUTHENTICATION (MFA)

DEFAULT PASSWORDS

REDUCING ENTIRE CLASSES OF VULNERABILITY

SECURITY PATCHES

VULNERABILITY DISCLOSURE POLICY

COMMON VULNERABILITIES AND EXPOSURES (CVE)

EVIDENCE OF INTRUSIONS

A call to action

Improving the world's cyber resilience, at scale
Implementing baseline security by default

Freddy Dezeure, Prof. Lokke Moerel, and Dr. George Webster

https://www.researchgate.net/publication/378213351_Improving_the_world's_cyber_resilience_at_scale_Implementing_baseline_security_by_default

Vendor guidance

https://learn.microsoft.com/en-us/microsoft-365/security/
https://www.microsoft.com/en-us/security
https://aws.amazon.com/security/
https://cloud.google.com/security
https://workspace.google.com/security/

Government guidance

SCuBA

FedRAMP

CyberFundamentals

ASD's Blueprint for Secure Cloud

Community guidance

CCM™
Cloud Controls Matrix

CIS Controls

CLOUD PROFILE

Financial Services Sector Coordinating Council
[illegible]

FS-ISAC

Principles for Financial Institutions' Security and Resilience in Cloud Service Environments

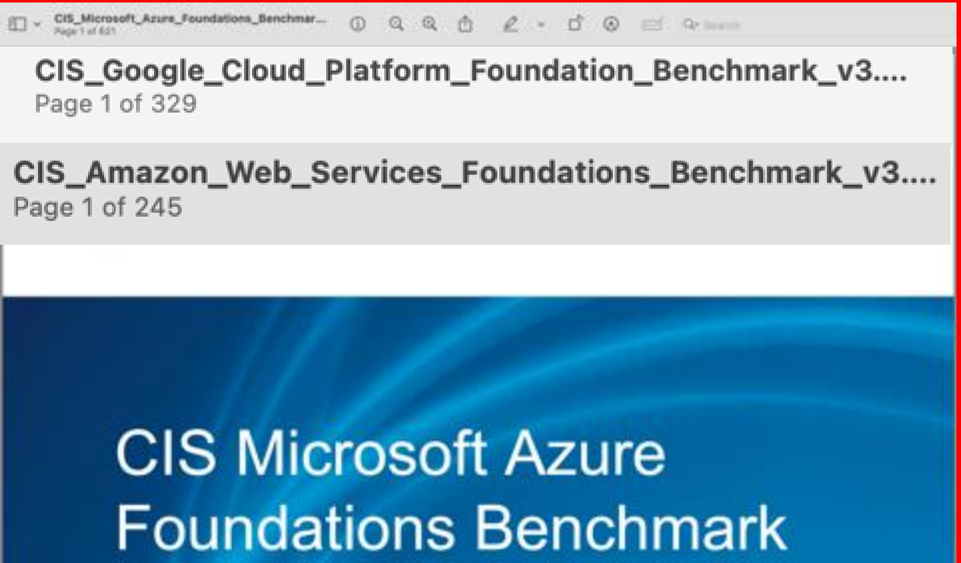
Users

Individual efforts to harden infrastructure:
- Internal expertise
- Paid vendor support
- Specialised consultancy

Vendor guidance

https://learn.microsoft.com/en-us/microsoft-365/security/
https://www.microsoft.com/en-us/security
https://aws.amazon.com/security/
https://cloud.google.com/security
https://workspace.google.com/security/

Government guidance



CIS_Google_Cloud_Platform_Foundation_Benchmark_v3....
Page 1 of 329

CIS_Amazon_Web_Services_Foundations_Benchmark_v3....
Page 1 of 245

CIS Microsoft Azure
Foundations Benchmark

Users

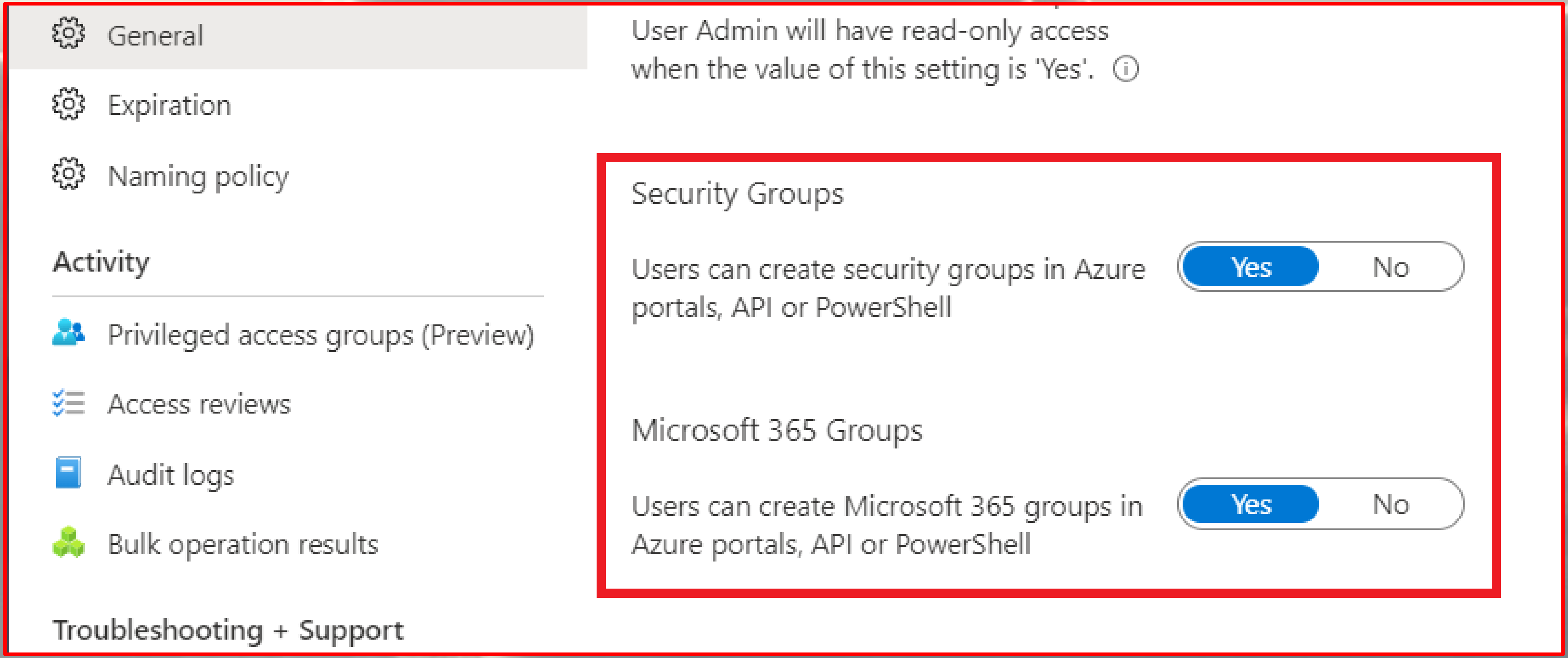
Individual efforts to harden infrastructure:
- Internal expertise
- Paid vendor support
- Specialised consultancy

Example lack of SbD

Recent Red Team findings

- Ensure 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'
- Ensure That 'Users Can Register Applications' Is Set to 'No'
- Ensure 'User consent for applications' is set to 'Do not allow user consent’ or Ensure 'User consent for applications' Is Set To 'Allow for Verified Publishers'
- Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes'
- Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No’

Recent Red Team



User Admin will have read-only access when the value of this setting is 'Yes'.

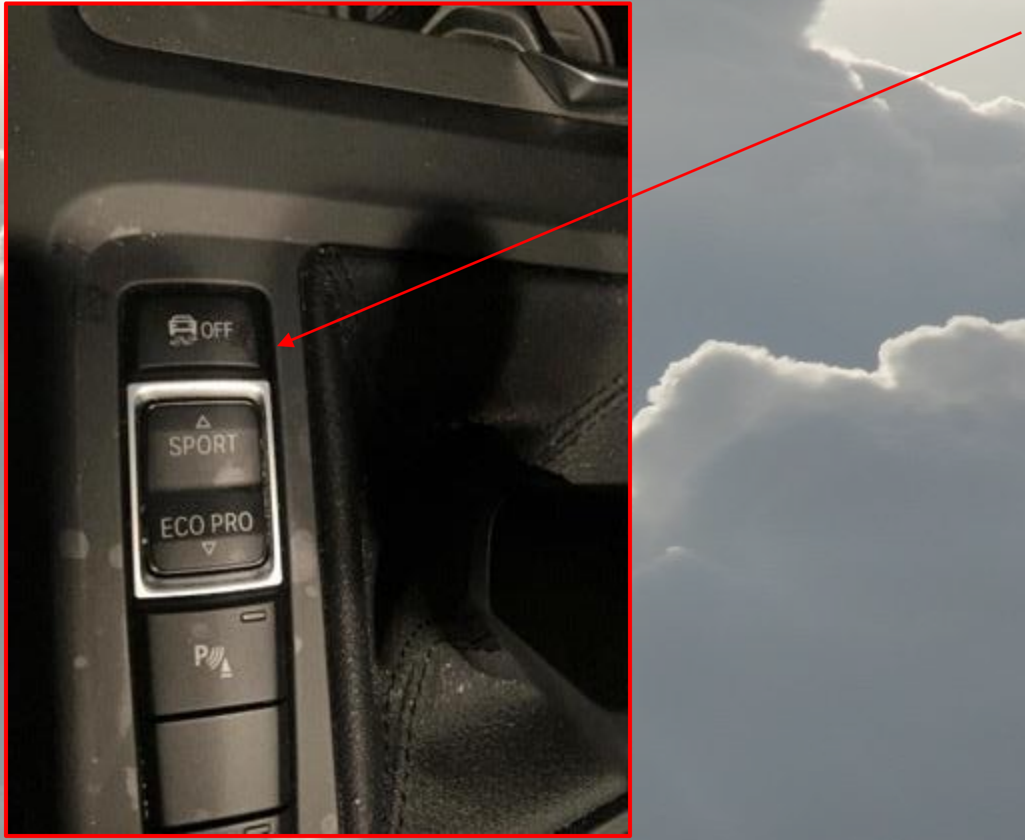
Security Groups

Users can create security groups in Azure portals, API or PowerShell [✓ Yes] No

Microsoft 365 Groups

Users can create Microsoft 365 groups in Azure portals, API or PowerShell [✓ Yes] No

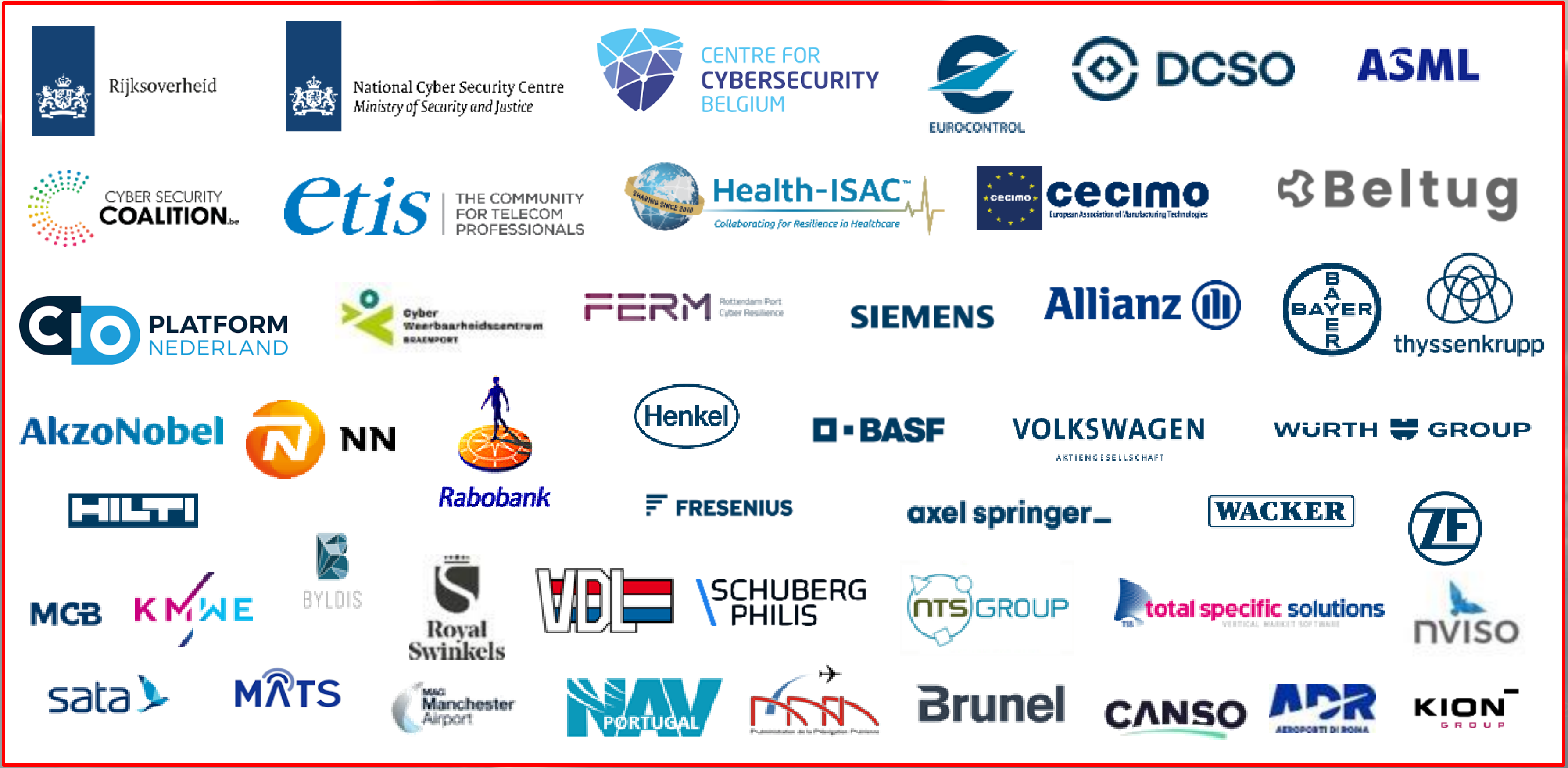
Built-in / opt-out



Tiered approach

- Secure baselines **by default** in the user environment, at no additional cost
- If (1) not possible, implement secure baselines **by workflow**
- If (1) – (2) not possible: offer transparently explained opt-in services (e.g., logging and secure backups)
- Timely warnings if defaults are changed and baseline security is not met
- Higher tiers of protection for specific industries

Community support



An imperfect market

Vendors

- Profit driven
- Organised by product
- Concerned about legal risks
- Lobbying for status quo

Regulators

- Organised by country/sector
- Slow and static
- Lacking skills
- Influenced by lobbyists

Community

- Mostly representing mature organizations
- Lacking resources

Customers

- Focused on convenience, and cost
- Lacking skills
- Dealing with legacy
- Scattered

Next steps