DAIMLER

German OWASP Day 2016

CarIT Security: Facing Information Security Threats

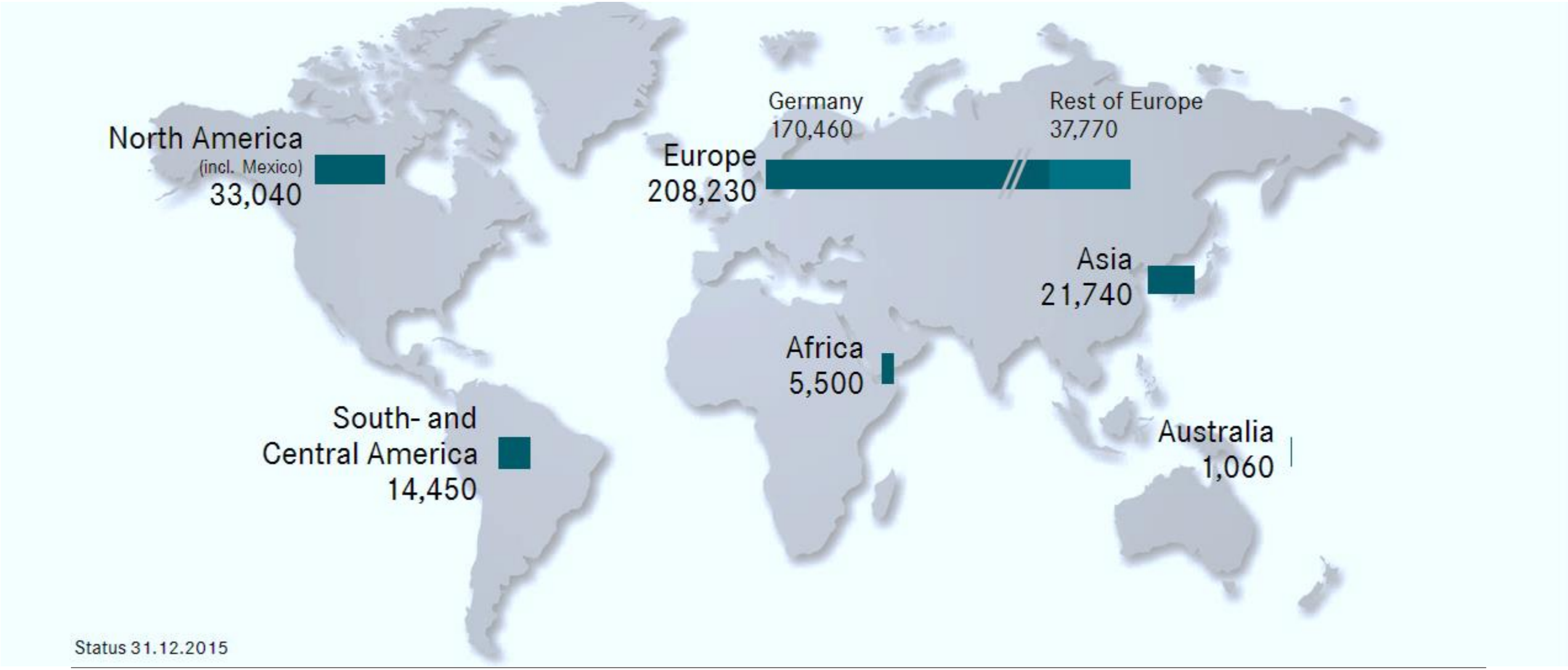
Tobias Millauer

Daimler – Business Units

	Mercedes-Benz Cars	Daimler Trucks	Mercedes-Benz Vans	Daimler Buses	Daimler Financial Services
					
2015					
Revenues	€ 83.8 bn	€ 37.6 bn	€ 11.5 bn	€ 4.1 bn	€ 19.0 bn
Employees	136,941	86,391	22,639	18,147	9,975

MAYBACH
Mercedes me
AMG
smart
FUSO
BHARATBENZ
WESTERN STAR
FREIGHTLINER
Thomas BUILT BUSES
SETRA
moovel
CAR 2GO
mytaxi
Mercedes-Benz Financial Services
Daimler Truck Financial
Mercedes-Benz Bank

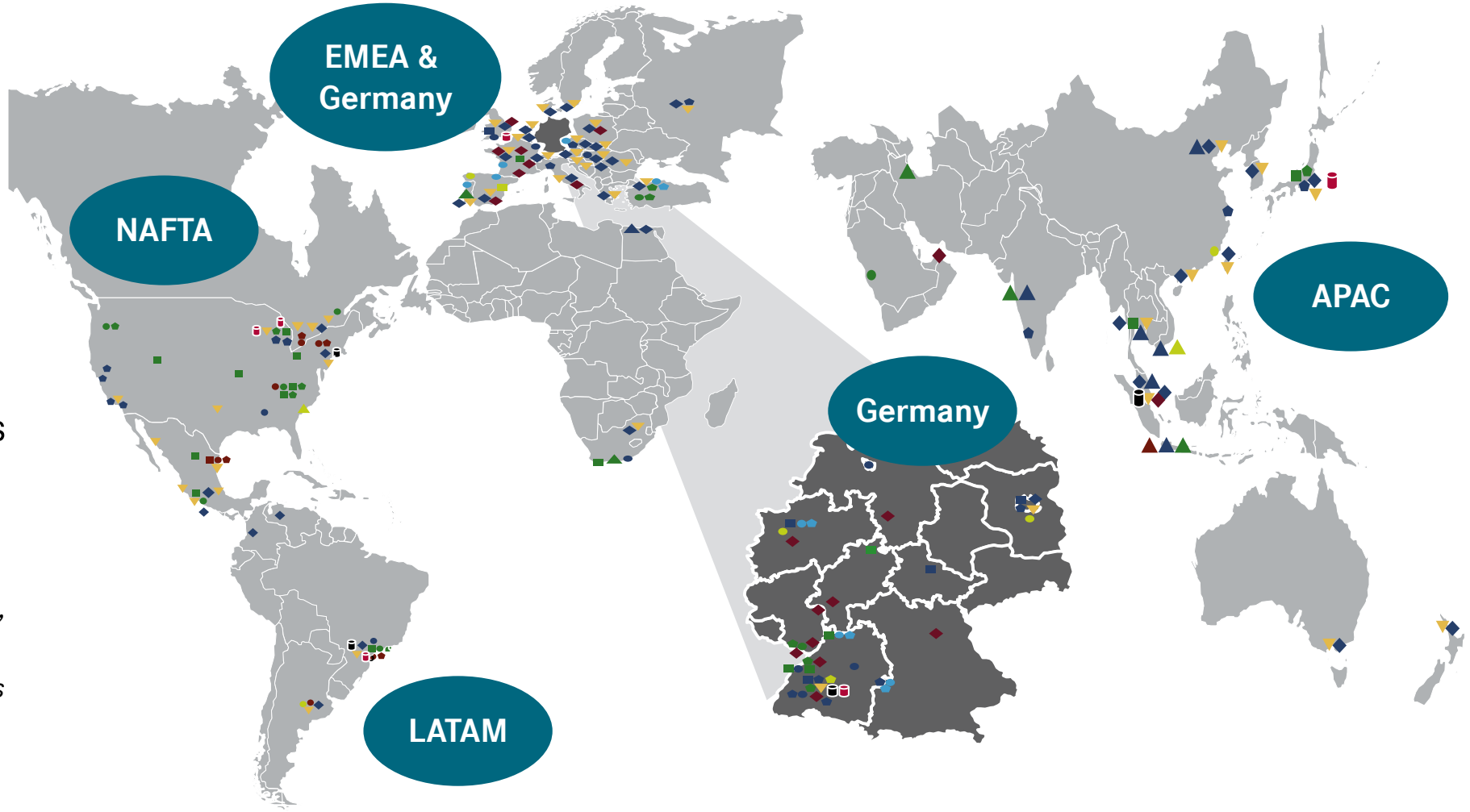
Daimler – 284,000 employees worldwide



Daimler – IT: 24x7x365

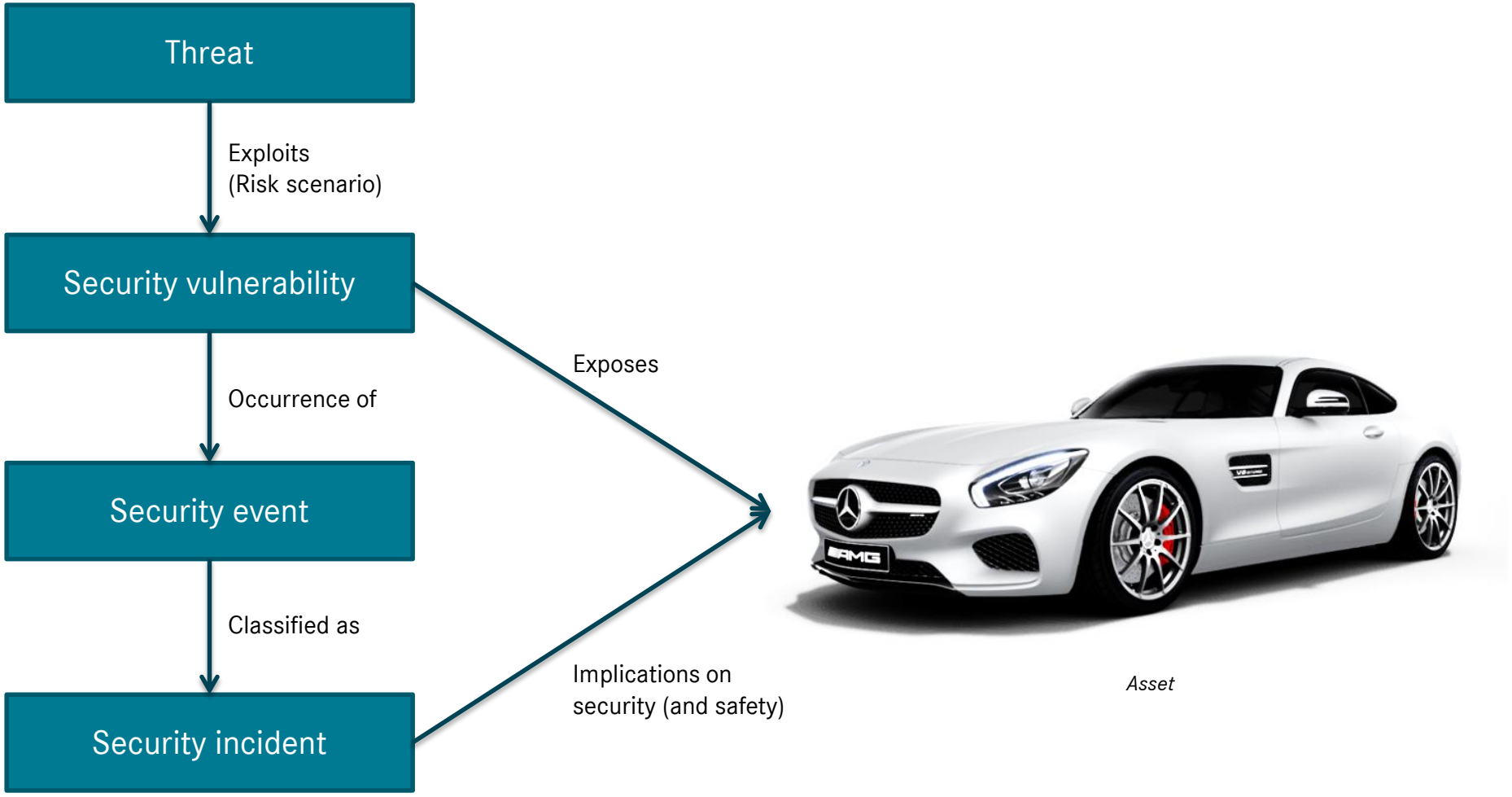
- Present on 6 continents
- More than 500 sites cross linked
- IT services for 284.000 employees
- 9.136 locations in focus

  41 Daimler group branches,
  61 production locations,
  9.034 distribution locations

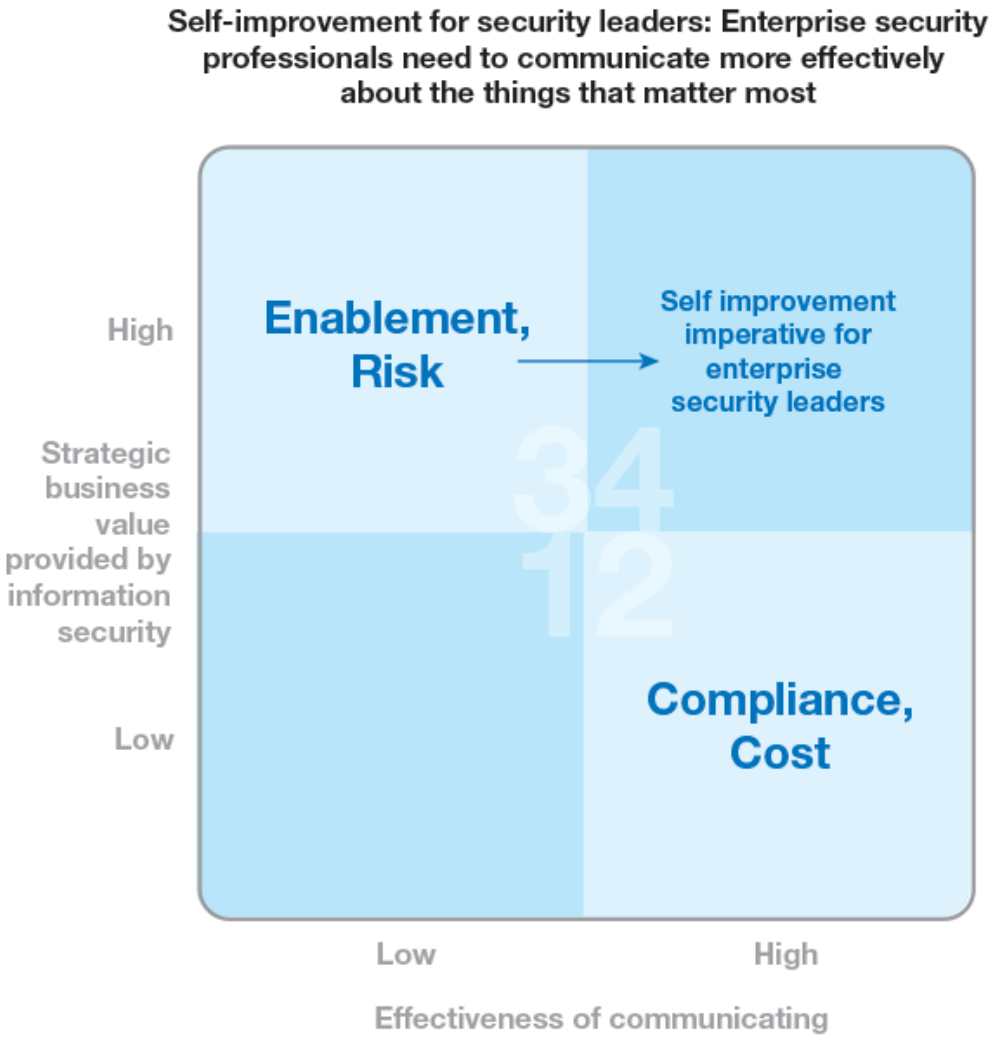


The Connected Car

The relationship of objects in a security chain



Self-improvement for security leaders

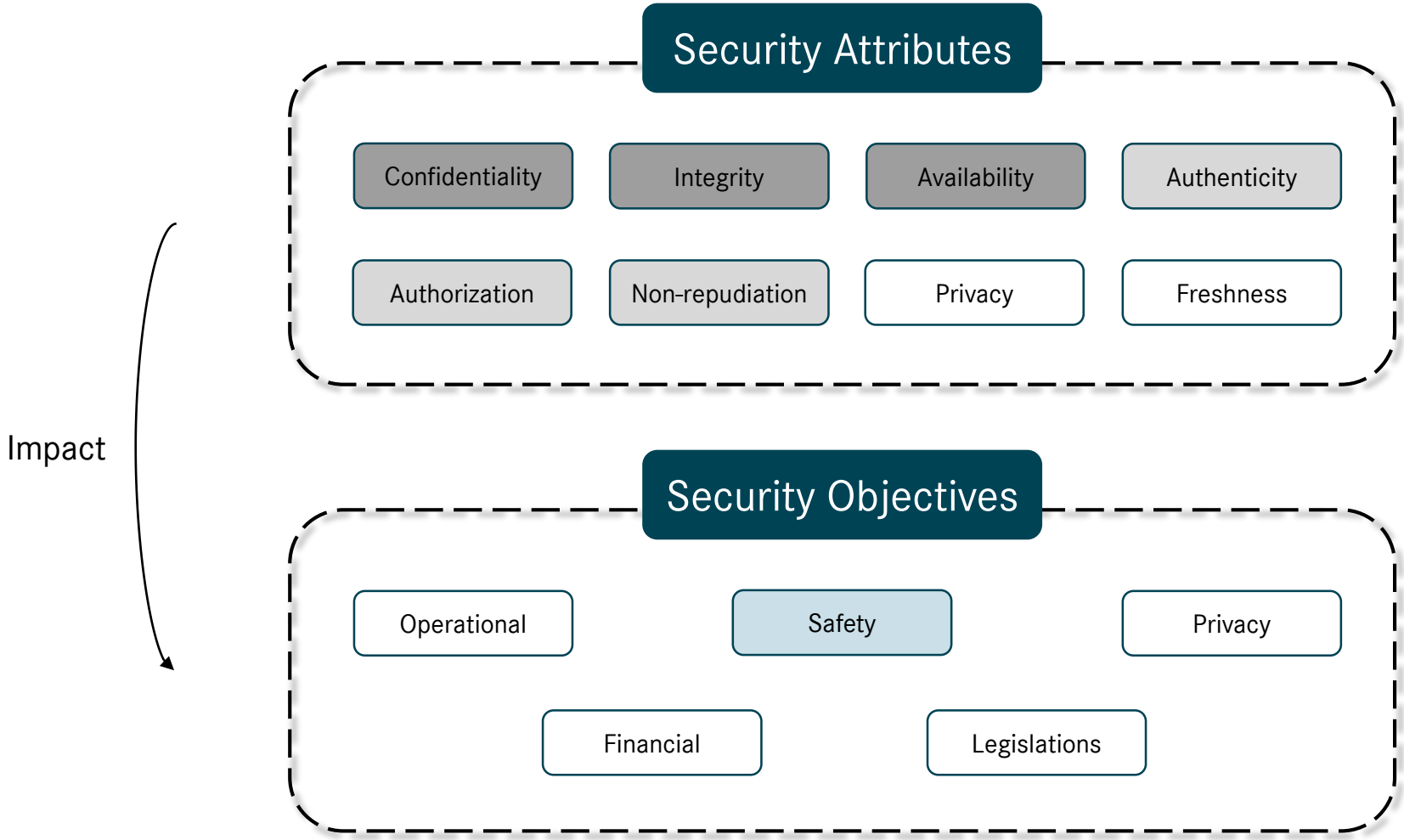


https://securityintelligence.com/self-improvement-agenda-for-cisos-what-is-top-of-mind-for-2015/

STRIDE Threat Model

S – Spoofing	Authentication
T – Tampering	Integrity
R – Repudiation	Non-Repudiation
I – Information disclosure	Confidentiality
D – Denial of service	Availability
E – Elevation of privilege	Authorization

HEAVENS Security Model



https://www.sp.se/en/index/research/dependable_systems/heavens/sidor/default.aspx

STRIDE Threat Model + HEAVENS Security Model

S – Spoofing	Authentication, *Freshness*
T – Tampering	Integrity
R – Repudiation	Non-Repudiation, *Freshness*
I – Information disclosure	Confidentiality, *Privacy*
D – Denial of service	Availability
E – Elevation of privilege	Authorization

https://www.sp.se/en/index/research/dependable_systems/heavens/sidor/default.aspx

Vehicle Cybersecurity

NHTSA

- **Protective/preventive measures and techniques**
  These measures, such as isolation of safety-critical control systems networks or encryption, implement hardware and software solutions that lower the likelihood of a successful hack and diminish the potential impact of a successful hack.
- **Real-time intrusion (hacking) detection measures**
  These measures continually monitor signatures of potential intrusions in the electronic system architecture.
- **Real-time response methods**
  These measures mitigate the potential adverse effects of a successful hack, preserving the driver's ability to control the vehicle.
- **Assessment of solutions**
  This involves methods such as information sharing and analysis of a hack by affected parties, development of a fix, and dissemination of the fix to all relevant stakeholders.

Cybersecurity Best Practices for Modern Vehicles

NHTSA

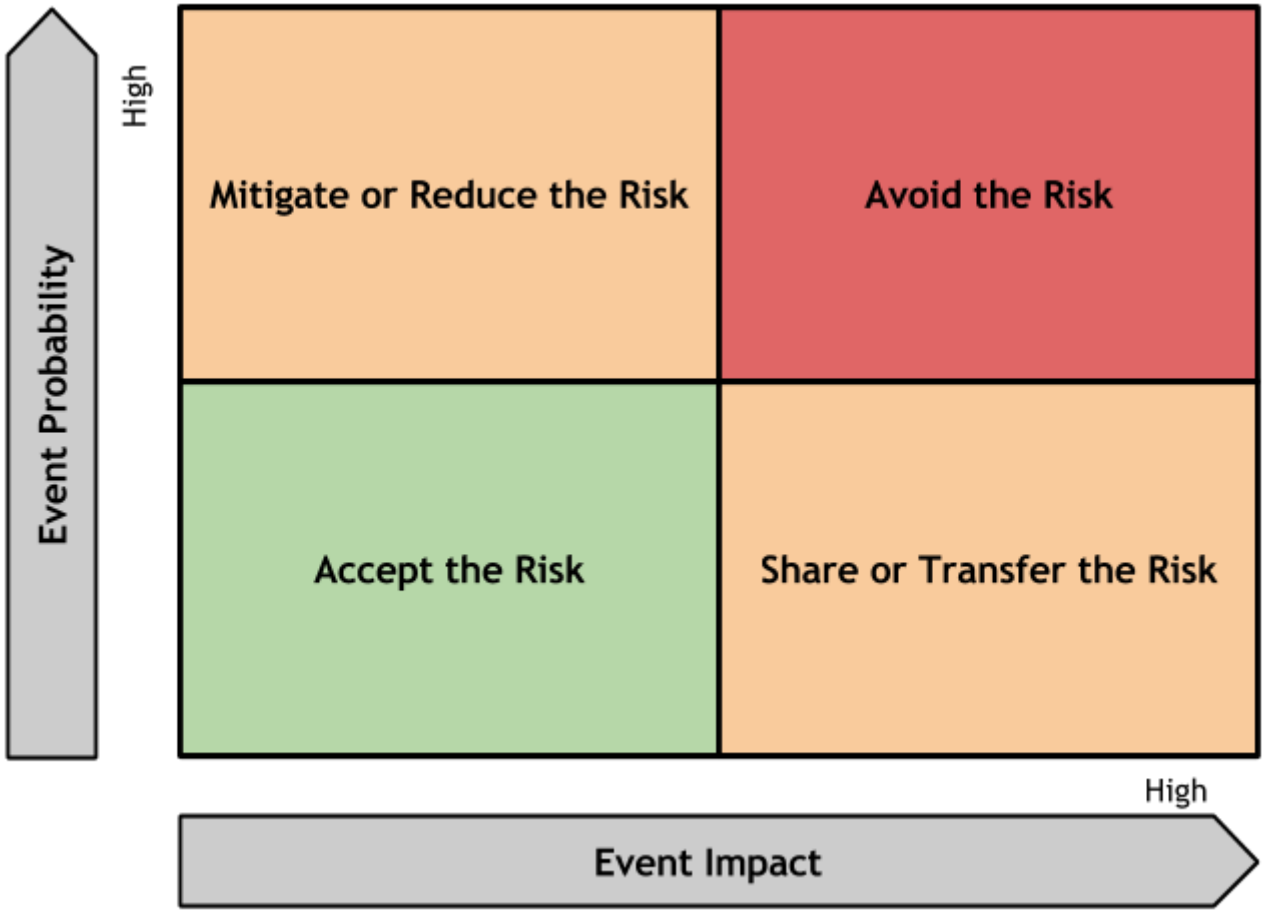
- Vehicle Development Process With Explicit Cybersecurity Considerations
- Vulnerability Reporting/Disclosure Policy
- Vulnerability / Exploit / Incident Response Process
- Self-Auditing (Risk Assessments, Penetration Tests, Organizational Decisions)
- Fundamental Vehicle Cybersecurity Protections (see Details)
- Leadership Priority on Product Cybersecurity

E-Safety Vehicle Intrusion Protected Applications

Security threat severity class	Aspects of security threats			
	Safety	**Privacy**	**Financial**	**Operational**
0	No injuries.	No authorized access to data.	No financial loss.	No impact on operational performance.
1	Light or moderate injuries.	Anonymous data only (no specific driver of vehicle data)	Low-level loss.	Impact not discernible to driver.
2	Severe injuries. / Light/moderate injuries for multiple vehicles	Identification of vehicle or driver. / Anonymous data for multiple vehicles.	Moderate loss. / Low losses for multiple vehicles.	Driver aware of performance degradation. / Indiscernible impacts for multiple vehicles.
3	Life threatening or fatal injuries. / Serve injuries for multiple vehicles.	Driver or vehicle tracking. Identification of driver or vehicle, for multiple vehicles.	Heavy loss. / Moderate losses for multiple vehicles.	Significant impact on performance. / Noticeable impact for multiple vehicles.
4	Life threatening or fatal injuries for multiple vehicles.	Driver or vehicle tracking for multiple vehicles.	Heavy losses for multiple vehicles	Significant impact for multiple vehicles.

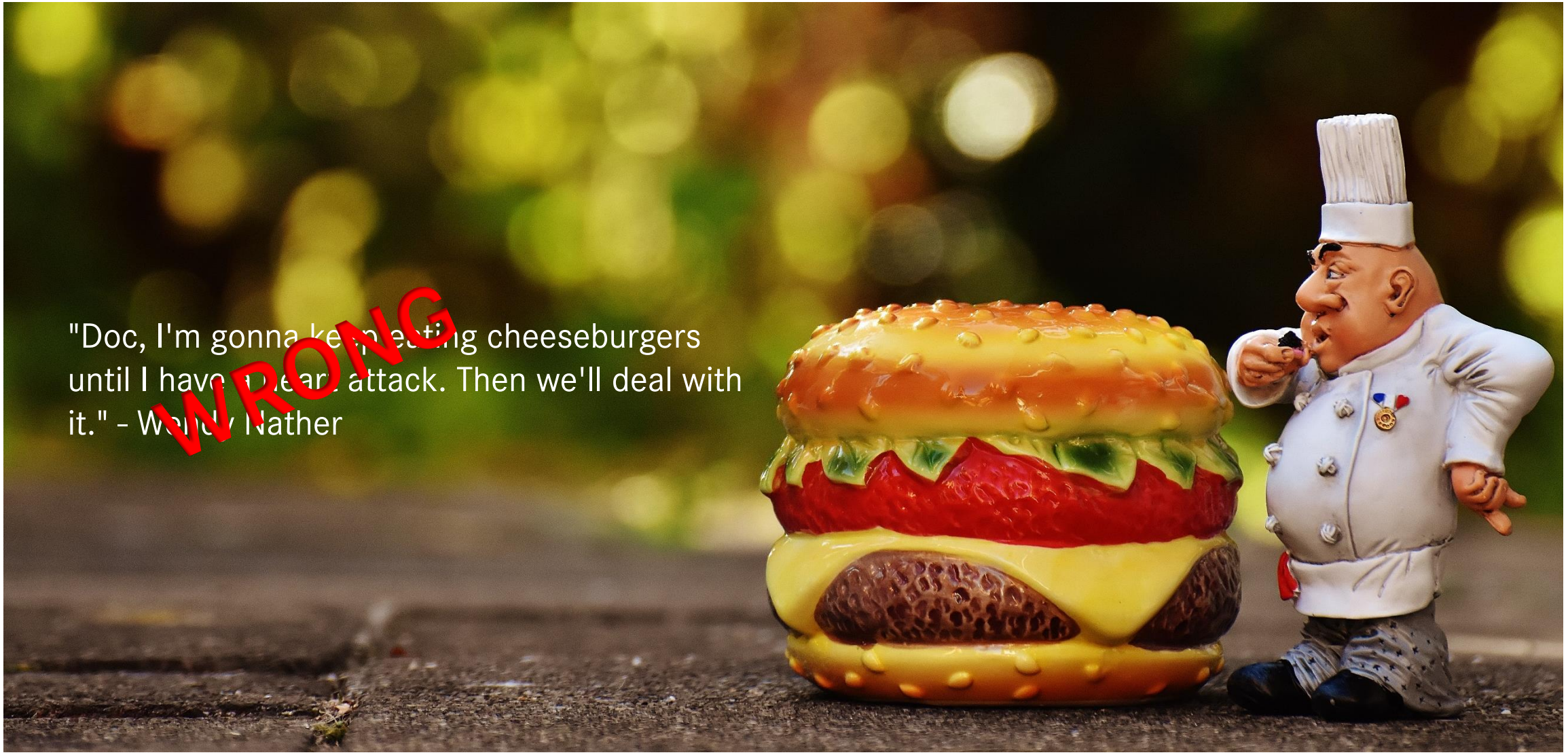
http://www.evita-project.org/

Information Security Risk Management
Treatment Strategy



https://www.owasp.org/images/9/96/ThreatMatrix_medium.png

Information Security Risk Management



DAIMLER

Tobias Millauer

Information Security Architect CarIT

Tel.: +49 176 30945415

Mail: tobias.millauer@daimler.com