gg-group.com

ONE FRAMEWORK TO RULE THEM ALL

Boris Orbach | Head of Global Information Security

Gebauer & Griller Kabelwerke GmbH

Boris Orbach

Background

- Creating and implementing cyber security strategies and programs
- Managing cyber security governance, risk and compliance
- Expertise in security frameworks (NIST, CIS, OWASP)
- Leading security certifications (TISAX, ISO 27xxx, PCI DSS, SOC½)
- Performing technical audits, pentests and hands-on operations

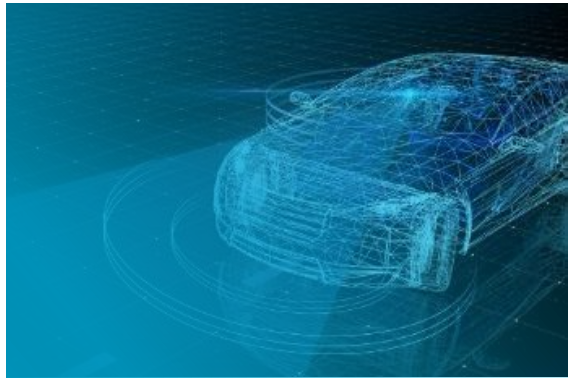
- 2019-today – CISO
- 2017-2019 – Information Security Architect / vCISO
- 2015-2017 – IT Security Project Manager / Team Leader
- 2010-2015 – IT Risk Consultant / IT Auditor / IT Security Consultant
- 2006-2010 – NOC Analyst / Undergraduate Teaching Assistant / System Administrator

- $(ISC)^2$ CISSP, CCSP
- ISACA CISA, CDPSE, CSX-P
- M.Sc. Cybersecurity (in process)

Overview

Gebauer & Griller

One of the energy and data transmission leaders for the automotive and industrial sectors.



Automotive Industry

Integration of advanced technologies creates new security vulnerabilities.

Security compliance comes to protect against evolving threats.

Cybersecurity Requirements

Growing regulatory demands: NIS 2, UNECE WP.29, TISAX, ISO/SAE 21434, etc.

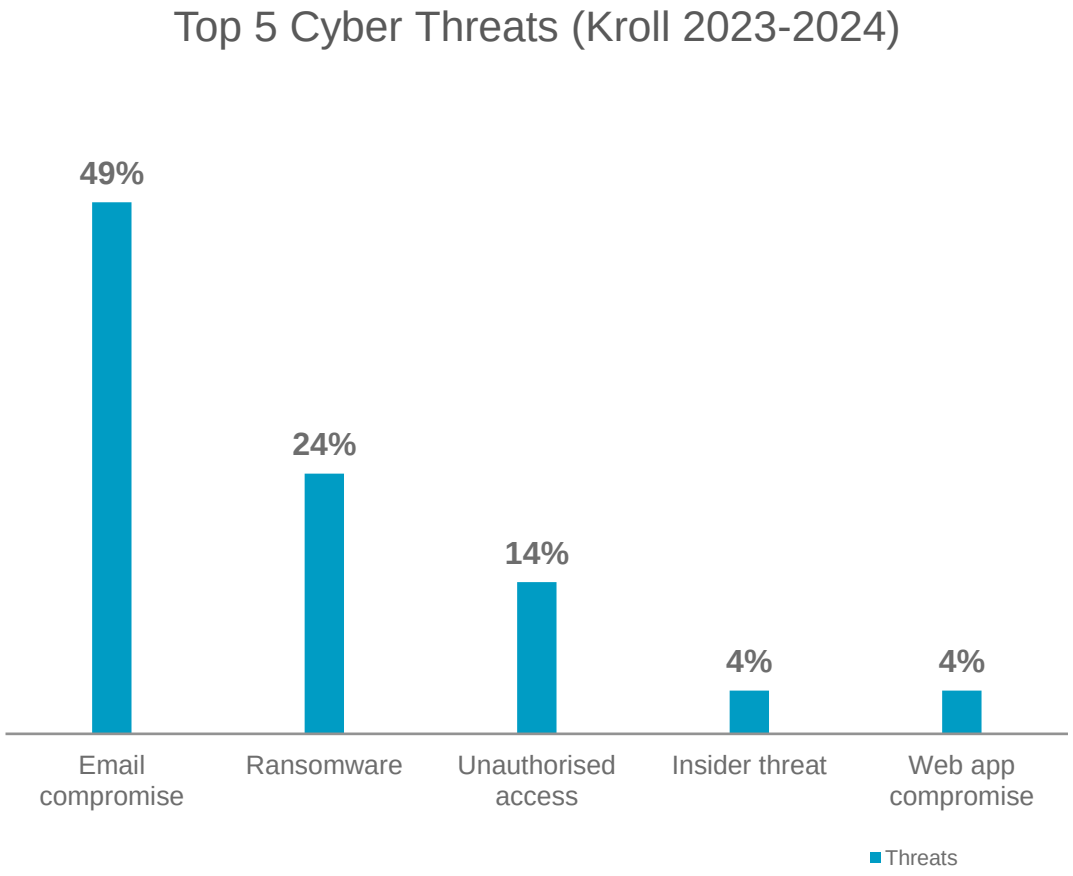
OEMs impose standards for supply chain protection.

Regulations Challenges

Unique challenge to manage multiple overlapping regulations and customer-specific demands.

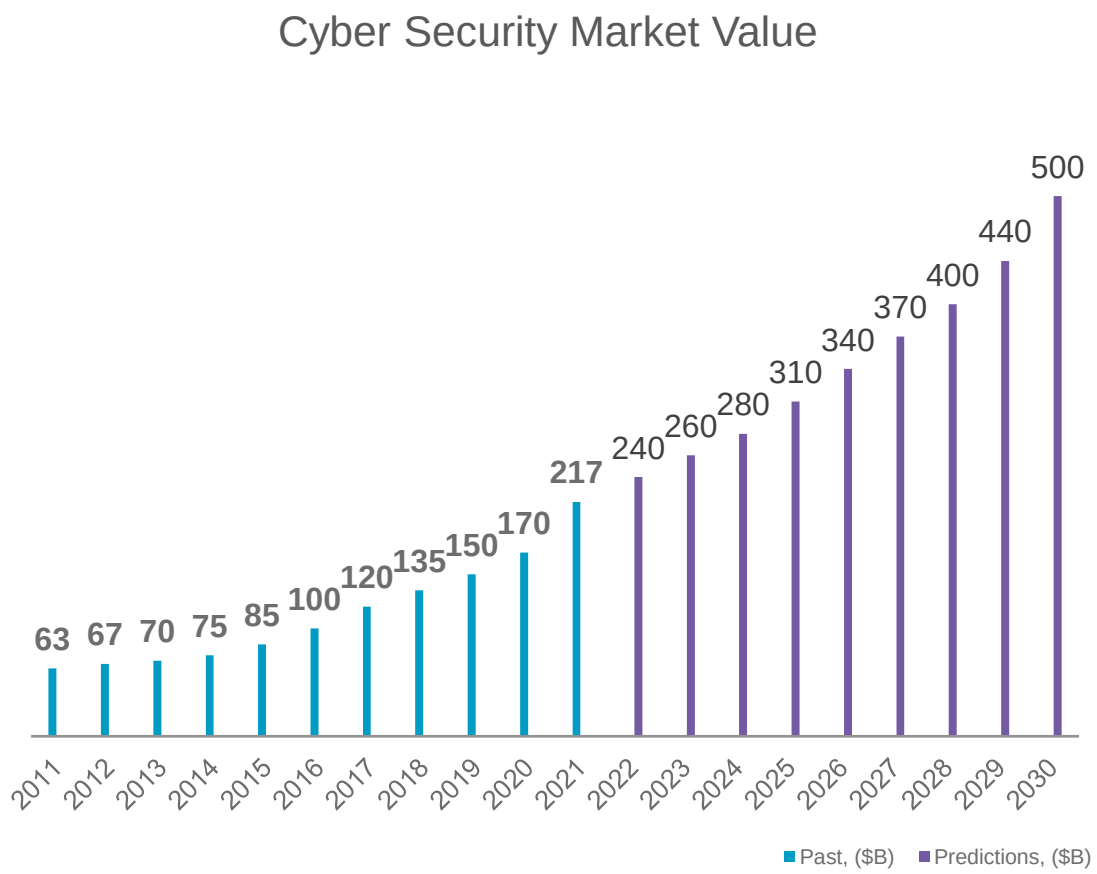
Cyber Security in Manufacturing

- Most important causes of security incidents in manufacturing systems:
  - Outdated Systems and Software / Unpatched Vulnerabilities
  - Supply Chain Vulnerabilities / Insecure Remote Access
  - Inadequate Employee Training and Awareness
  - Insufficient Network Segmentation
  - Weak Authentication Mechanisms
  - Unmanaged and unsecured devices (“Shadow OT”)
  - Misconfigured Systems and Devices



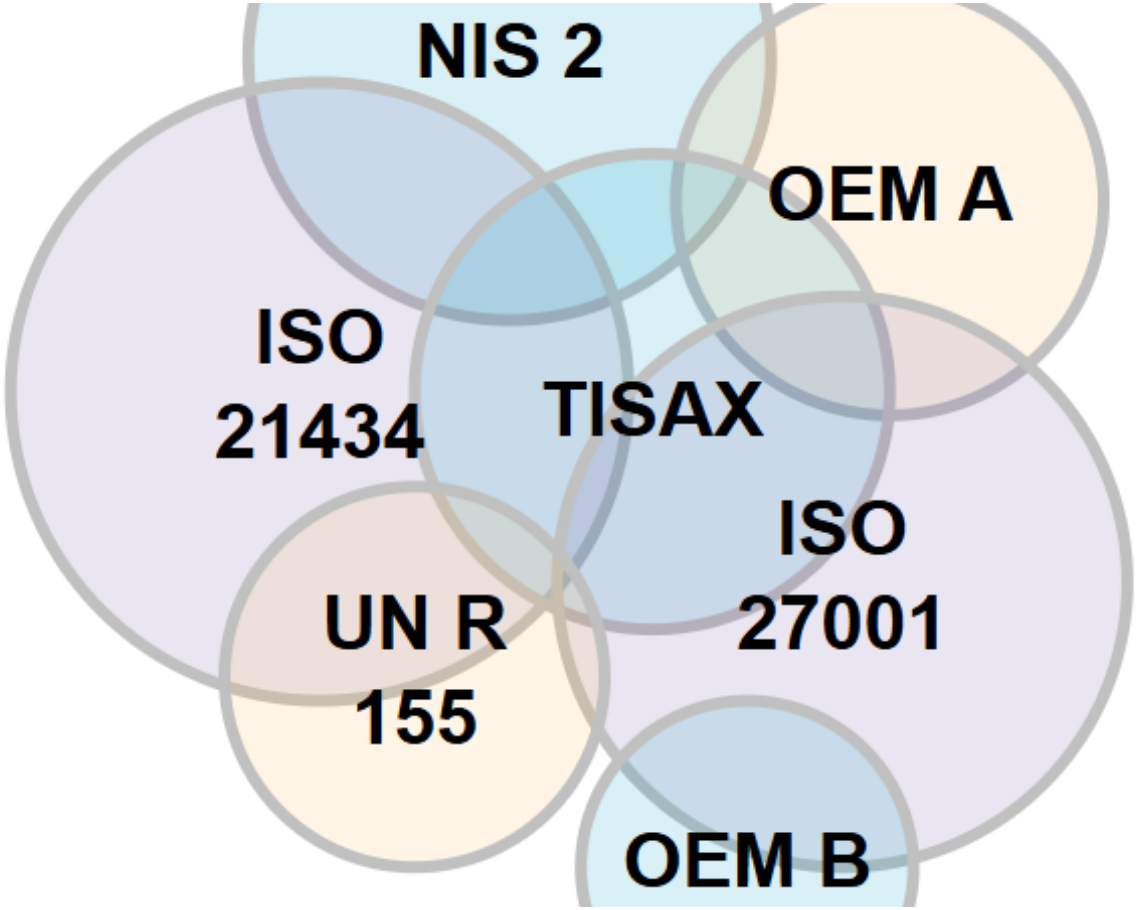
Cyber Security Market

- Significant growth in cybersecurity in recent years:
  - Rising adoption of digital technologies and digital transformation across industries
  - Increasing frequency, sophistication, and impact of materialised cyber threats:
    - 2022 – Toyota (automotive manufacturer) $300M
    - 2023 – Yanfeng (automotive parts) $300M
  - Multiple technologies require complex cyber security measures for protection
  - Growth in security solutions to counter increasing sophisticated cyberattacks



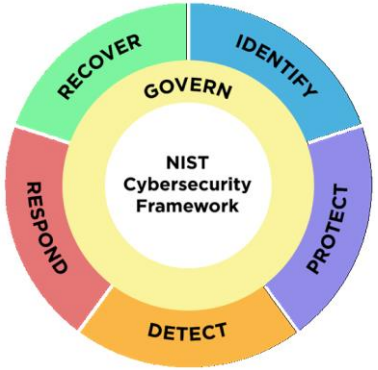
Cyber Security Regulations Challenges

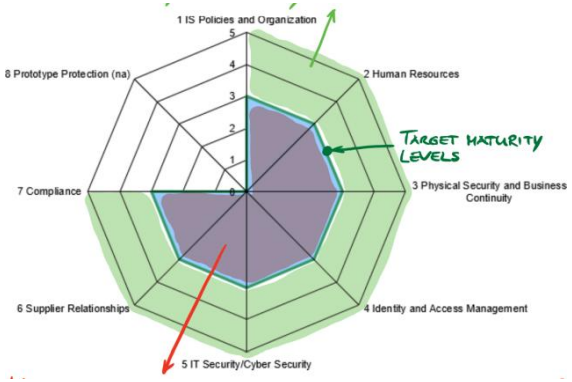
- Complexity of compliance requirements:
  - Overlapping security regulations
  - Customer-specific demands
- Resource intensiveness:
  - Financial costs
  - Human resources
  - Operational disruptions
- Risk of non-compliance:
  - Legal and financial repercussions
  - Damage to reputation and loss of customer trust

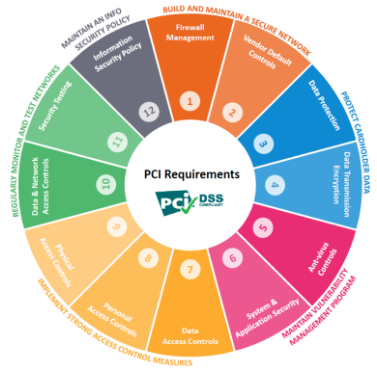


Core Framework

What to choose?







NIST CSF 2.0 (6->107)

Govern

Identify

Protect

etc.

ISO/IEC 27002:2022 (4->93)

Organizational controls

People controls

Physical controls

Technological controls

TISAX (9->79)

IS Policies and Organization

Human Resources

Physical Security

etc.

PCI DSS (6/12->259)

Secure Network and Systems

Data Protection

Vulnerability Management

etc.

Practical Approach

Key Components

- Core structure:
  - NIST CSF Core Functions –> GG Security Functions
  - NIST CSF Core Categories –> GG Security Domains
  - NIST CSF Core Subcategories –> GG Security Topics
- Compliance mapping
- Security risks
- Ongoing activities
- Security controls

GG SECURITY FUNCTION	NIST CORE FUNCTION	GG SECURITY DOMAIN	GG SECURITY TOPIC
Maintain Actual Security Organization	**GOVERN**	**Cybersecurity Organization**	1
			Organization
			Responsibilities
			Shared Responsibilities
			Policies
Manage Security Risks	**IDENTIFY**	**Cybersecurity Risk Management**	2
			Methodology
			Asset Management
			Risk Assessments
			Risk Map / Register
			Cyber Insurance
Ensure Compliance Requirements		**Cybersecurity Assessments**	3
			Compliance Management
			External Audits
			Internal Audits
			Penetration Testing
			Network Assessments
			System Assessments
			Application Assessments

Practical Approach

Key Components

- Core structure
- Compliance mapping:
  - TISAX 6.0.1
  - NIS 2
  - NIST CSF 2.0
  - OEM A
  - etc.
- Security risks
- Ongoing activities
- Security controls

GG SECURITY DOMAIN	GG SECURITY TOPIC	COMPLIANCE			
		TISAX	NIS 2	NIST CSF	OEM A
Cybersecurity Organization	1				
	Organization	1.2.1		ID.BE-1, ID.	1.1, 2.2.1
	Responsibilities	1.2.2		ID.AM-6, ID.	
	Shared Responsibilities	1.2.4		DE.DP-1	
	Policies	1.1.1;5.1.1;8	21.2.a, 21.2.	ID.GV-1	
Cybersecurity Risk Management	2				
	Methodology	1.4.1		ID.GV-4, ID.	1.6.1
	Asset Management	1.3.1;1.3.4	21.2.i	ID.AM-1, ID.	1,4
	Risk Assessments	1.4.1	20,1	ID.RA-5	
	Risk Map / Register	1.4.1		ID.RA-6	
	Cyber Insurance	---			
Cybersecurity Assessments	3				
	Compliance Management	7.1.1		ID.GV-3	1.6, 1.6.4
	External Audits	1.5.2			
	Internal Audits	1.5.1			
	Penetration Testing	1.5.2			
	Network Assessments	5.2.6			
	System Assessments	5.2.6			
	Application Assessments	5.2.6			
Information Protection	11				

Practical Approach

Key Components

- Core structure
- Compliance mapping
- Security risks:
  - Risk details
  - Possible impact
  - Risk owner
  - Inherited/residual risk levels
  - etc.
- Ongoing activities
- Security controls

GG SECURITY DOMAIN	GG SECURITY TOPIC	Location	Risk Details	Impact
Cybersecurity Assessments	3			
	Compliance Management	Global	No visibility over global cc	Inconsistant
	External Audits	Global	Lack of external audits	Low client vi
	Internal Audits	Global	Lack of internal audits	Low internal
	Penetration Testing	Global	Existing security malpract	Existing vuln
	Network Assessments	Global	…	…
	System Assessments	Global	…	…
	Application Assessment	Global	…	…
Information Protection	11			
	Sensitive Information	Global	…	…
	Personal Data	Global	Lack of personal data lab	No label/mar
	Information Classification	Global	Lack of labeling	Uncontrolled
	Data Loss Prevention	Global	Lack of data leak preventi	Data leakage
	Data Encryption	Global	Lack of information encry	May lead to
	Data Integrity	Global	…	…
	Data Destruction	Global	Lack of destruction confir	Misspaceme
	Data Return	Global	Lack of BT overview	Misspaceme
Access Management	12			
	Identification / Authentication Mana	Global	Lack of formal user regist	Company's s
	Federation Management	Global	…	…

Practical Approach

Key Components

- Core structure
- Compliance mapping
- Security risks
- Ongoing activities:
  - Maturity level
  - Topic responsibility
  - Supporting technology
  - Policies and procedures
  - etc.
- Security controls

GG SECURITY DOMAIN	GG SECURITY TOPIC	Maturity Level	Responsibility	Technology	Policies
Access Management	12				
	Identification / Authentication Mana	0_Incomplete	ITI+ITA+ITS	…	Access Con
	Federation Management	1_Performed	ITI+ITS	…	
	Authorization Management	2_Managed	ITI+DO	…	Access Con
	Password Management	3_Established	ITI+ITS	…	Securing IT
	Privileged Access Management	4_Predictable	ITI	…	Access Con
	Accounts / Access Permissions R	5_Optimized	ITI+DO+ITS	…	Access Con
Network Protection	13				
	Secure Architecture	4_Predictable	ITI+ITS	FW, …	Securing IT
	Wireless Access	3_Established	ITI	…	Access Con
	Remote Access	2_Managed	ITI+ME+ITS	…	Global Mobil
Endpoint Protection	14				
	Servers Hardening	1_Performed	ITI+ITS	GPO	Securing IT
	Workstations Hardening	2_Managed	ITI+ITS	GPO	Securing IT
	Administrator Permissions	3_Established	ITI+ITS	GPO	Acceptable U
	Mobile Devices Protection	4_Predictable	ITI+ITS	…	Acceptable U
	Antimalware / EDR / EPP	5_Optimized	ITS+ITI	EDR	Securing IT
Cloud Protection	15				
	Methodology	1_Performed	ITS	…	…
	Cloud Security Baseline	2_Managed	ITS+ITI	…	Access Con

Practical Approach

Key Components

- Core structure
- Compliance mapping
- Security risks
- Ongoing activities
- Security controls:
  - Definition, implementation responsibility, current status
  - Reference to compliance and contractual requirements
  - etc.

GG SECURITY DOMAIN	GG SECURITY TOPIC	Control	Additional remarks / ste
Cloud Protection	15		
	Methodology	…	…
	Cloud Security Baseline	…	…
	Ownership Management	Define the ownership mar	…
Communication Protection	16		
	Secure Browsing	Allow use of engines with	Consider implementation
	Email Security	…	…
	Email Encryption	Emails can be marked as	…
	URL / DNS Filtering	…	…
	USB DoK Protection	USB ports that could be u	…
	Social Networks	…	…
	VoIP	…	…
OT Protection	21		
	Methodology	…	…
	OT Security Baseline	Set priority for processes	…
Secure SDLC	22		
	Security Requirements	…	…
	Secure System Lifecycle	Perform regular patches/	…
	Security Testing	…	…
	Securing Test Data	…	…

Practical Approach

Key Components

- Security awareness training:
  - Onboarding/annual training that covers all security requirements
  - Complementary training for specific groups
  - Monthly newsletter referring to “international days”
  - Monthly complimentary video training
  - Phishing exercises for all employees and specific groups

Year	Month	Date	Released		Loc 1		Loc 2
					Empl	Ext	Empl
2021	January						
2022	January						
2023	January						
2024	January	17.01.2024	Internet Resources Usage	Email Newsletter	v	v	v
		29.01.2024	Data Protection Day	Email Newsletter	v		v
	February	06.02.2024	Safer Internet Day	Email Newsletter	v	v	v
	March	27.03.2024	World Backup Day	Email Newsletter	v	v	v
	April	09.04.2024	Identity Management Day	Email Newsletter	v	v	v
	May	14.05.2024	Fraudulent Payment Emails	Email Newsletter			
		16.05.2024	World Password Day	Email Newsletter	v	v	v
	June	25.06.2024	New Security Awareness Solution	Email Newsletter	v	v	v
		27.06.2024	Deepfake Videos and Calls	Email Newsletter	v	v	v
		28.06.2024	GG Security Awareness Training 1	Full Training	v		v
	July						
	August						
	September	*02.09.2024-*	Physical Security Training	Face-2-Face			
		30.09.2024	Protecting Working Environment	Email Newsletter	v	v	v
		30.09.2024	Protecting Working Environment	Nano Training	v		v
	October	09.10.2024	Fraudulent Payroll Emails	Email Newsletter			
		15.10.2024	Cybersecurity Awareness Month	Email Newsletter	v	v	v

Benefits

- Improved stakeholder trust:
  - Demonstrating a solid commitment to security compliance builds trust with customers, partners, and regulatory bodies
  - Creating a competitive advantage over other suppliers
- Enhanced security posture:
  - Full visibility of all regulatory and customer-specific requirements
  - Comprehensive approach to security
  - Improved risk mitigation
- Scalability and flexibility:
  - Easier to adapt to new requirements without overhauling the entire compliance process
- Operational efficiency:
  - Reduced duplicated efforts and simplified workflows
  - Freed up resources allow to focus on proactive security initiatives
- Cost savings:
  - Lower costs associated with separate compliance systems

Questions?

gg-group.com

Gebauer & Griller Kabelwerke Gesellschaft m.b.H.
Muthgasse 36 | 1190 Wien | Austria

Thank you!