NYU STERN

Center for Sustainable Business

Investing in Cybersecurity in the Auto Industry: Proposed Benefits & Monetization Methods

November 2025



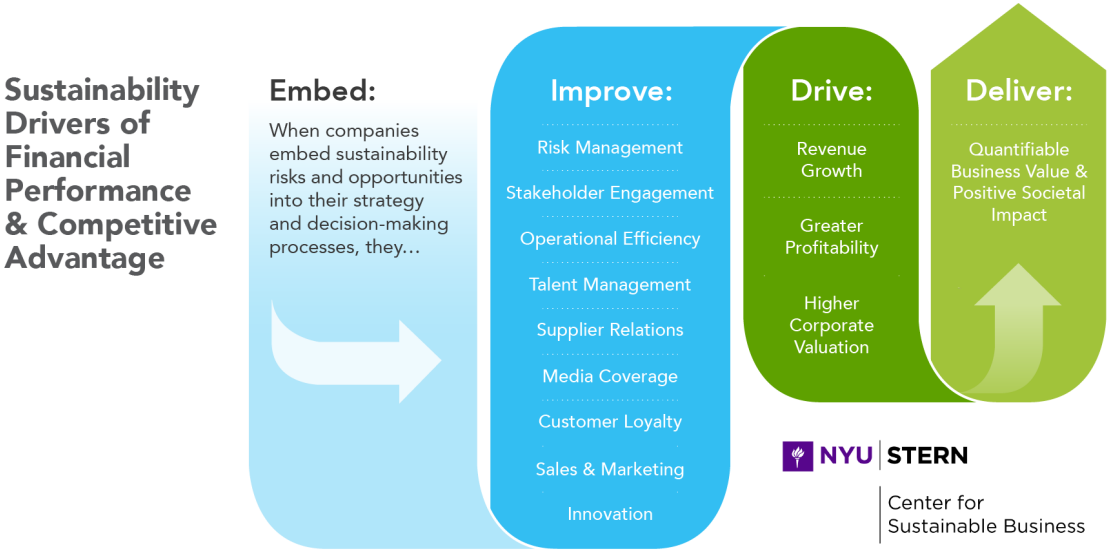
© 2025, New York University. Leonard N. Stern School of Business, Center for Sustainable Business. All rights reserved.

Disclaimer

DISCLAIMER: This tool is provided by NYU Stern Center for Sustainable Business for informational and educational purposes only. It is not to be used for commercial use except through prior written agreement. While every effort has been made to ensure the accuracy and reliability of the data and calculations contained within this tool, NYU Stern Center for Sustainable Business makes no warranties, express or implied, regarding its completeness, accuracy, or fitness for a particular purpose. Users assume full responsibility for any decisions made based on the outputs of this tool. New York University and its affiliates, faculty, staff, and students shall not be liable for any direct, indirect, incidental, or consequential damages arising from the use of this tool. This tool is provided “as is” and may be subject to updates or modifications without notice. Users must cite NYU Stern CSB when using the tool and references to ROSI™ materials. Users should verify all results independently and consult with appropriate professionals before relying on the data and results provided. By using this tool, you acknowledge and agree to these terms.

ROSI™ Framework

Return on Sustainability Investment (ROSI™) Framework



By embedding ESG risk and opportunities within core business strategy, the return on sustainable investment can be quantified, delivering the possibility of both financial value and positive societal impact.

Overview of Auto Industry Framework

NYU Stern CSB is developing a ROSI™ framework for the auto industry with publicly available monetization tools to help the industry understand where and how sustainability can unlock financial value.

Based on research, experience, and engagement with industry leaders, we have identified the following sustainability strategies* used by the industry to include in the framework:

- Mitigate & Adapt to Climate Change
- Waste Management
- Water Management
- Chemical Management
- Support Electrification Ecosystem
- Circularity
- Cybersecurity
- Sustainable Sourcing
- Driver Safety
- Supplier and Employee Well-Being

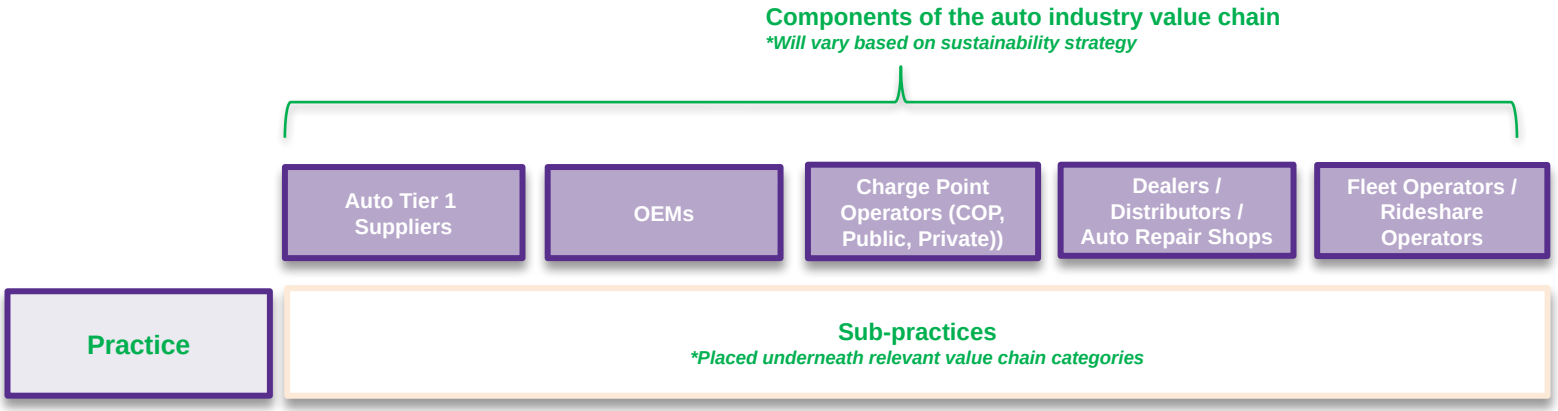
Identified Sustainability Practices and Sub-Practices

Framework Layout

Through our research, we identified key sustainability practices and sub-practices that auto industry value chains are using to achieve their sustainability goals.

- **Each practice is broken into sub-practices, which are mapped to the relevant components of the value chain (and excluded where not applicable).**
- **Benefits are mapped to sub practices, with some benefits appearing across multiple practices.**
- **Specific compliance or enforcement policies are not listed in this framework, except for the new Cross Border Adjustment Mechanism regulations.**

The diagram below illustrates the framework applied for each strategy in the following slides



NYU STERN

Center for
Sustainable Business

Investing in Cybersecurity

Investing in Cybersecurity

	Auto Tier 1 Suppliers	OEMs	Charge Point Operators	Dealers / Distributors / Auto Repair Operations	Fleet Operators / Rideshare Operators
Improve Governance and Oversight to Protect Employee and Consumer Data, and Operating Systems from Cyber Attacks	Implement strong governance responsible for cyber security (such as board level committee responsible for monitoring and promoting data privacy protection programs and compliance with at least one director with cyber security expertise, and senior level executive operations, tech or legal)				
	Align internal controls with NIST and ISO 27001 standards				
	Establish robust risk assessment processes (such as inventory of digital assets; monitoring and updates to security controls, anti-virus software, detective systems and access controls; incident response protocols, regular testing and updates) Establish policies to protect driver data and to meet regulatory requirements				
	Training and awareness on cybersecurity and data-ethics programs for employees				
Strengthen Vehicle and Product Security	Integrate security by design principles across vehicle software and digital platforms				
	Conduct independent penetration testing and vulnerability assessments				

Investing in Cybersecurity (continued)

	Auto Tier 1 Suppliers	OEMs	Charge Point Operators	Dealers / Distributors / Auto Repair Operations	Fleet Operators / Rideshare Operators
Strengthen Supply Chain Security and Operational Resilience	Establish strong vendor management practices (such as vetting processes, security assessments, security requirements and incident response protocols in contracts) including compliance with ISO/SAE 21434 and UNECE WP.29				
	Conduct regular third party cyber risk assessments and collaborate on corrective actions				
	Identify protocols for detecting threats and responses including driver notifications				
Safeguard Driver Privacy and Data Protection	Provide transparent privacy notices and obtain explicit consent for data use				
	Implement practices to protect vehicles from hackers (such as encryption on key fob radio frequencies, onboard systems, secure logins and passwords, multi-factor authentication and biometrics, and VPN)				

NYU STERN

Center for
Sustainable Business

Monetization Approach

Investing in Cybersecurity

Overview of Sustainability Strategy and Relevant Value Drivers

Sustainability Strategy Definition

Cyber Security

Auto industry companies are strengthening cybersecurity by enhancing governance, policies, frameworks and practices, and vendor management to protect employee, consumer, and operational data. Investments focus on secure software development to protect vehicle systems and connected infrastructure, real-time threat detection, encryption, and workforce training, Companies are also implementing stronger policies to safeguard driver information, ensure regulatory compliance, and maintain customer trust.

The following slides focus on the benefits and relevant value drivers derived from the *Cyber Security* strategy

Relevant Value Drivers	**Benefits that…**
Risk Management (RM)	Encourage risk mitigation and resilience within the value chain
Operational Efficiency (OE)	Optimize corporate and supply chain efficiencies to lower cost and increase profits
Customer Loyalty (CL)	Attract an increasing community of conscious buyers & consumers, while reducing retention costs

Investing in Cybersecurity

Overview of Sustainability Strategy and Relevant Value Drivers (continued)

The following slides focus on the benefits and relevant value drivers derived from the *Cyber Security* strategy

Value Drivers not Captured in this Strategy

Stakeholder Engagement (SE)	Improve goodwill among the broader stakeholder community (i.e. investors, NGOs)
Talent Management (TM)	Attract and retain high-quality internal talent
Supplier Relations (SR)	Improve upon the relationships between the company and its suppliers
Media Coverage (MC)	Increase a company's media presence with the development of traditional and social media content
Innovation (IN)	Create new revenue streams using sustainable business models
Sales and Marketing (SM)	Increase volume of sales through brand and marketing policies

Investing in Protecting from Cyber Attacks

Overview of Benefits and Monetization Methods

OE	RM	SR
SM	SE	MC
CL	TM	IN

value Drivers based on color coding illustrated on previous slides

Practice	Sub-Practice*	Proposed Benefits	Value Drivers	Suggested Monetization Methods
Improve Governance & Oversight to Protect Employee/ Consumer Data & Operating Systems from Cyber Attacks	Implement strong governance responsible for cyber security (such as board level committee responsible for monitoring and promoting data privacy protection programs and compliance with at least one director with cyber security expertise, and senior level executive- operations, tech or legal) Align internal controls with NIST and ISO 27001 standards Establish robust risk assessment processes (such as inventory of digital assets; monitoring and updates to security controls, anti-virus software, detective systems and access controls; incident response protocols, regular testing and updates) Establish policies to protect driver data and to meet regulatory requirements	Avoidance of **fines and legal actions** due to data breaches	RM OE	Assess the probability and average cost (fines, administrative costs, cost of production delays, legal/PR expenses) of a regulatory violation based on historical data or relevant proxies. Estimate the reduction in probability of a violation due to implementing the changes (improved employee and consumer cybersecurity data and operating system policies, processes, and practices; and vendor management practices). Multiply the probability reduction by the average costs to quantify the benefit
		Mitigates **reputation risk** and related costs (such as revenue loss from cyber risk scandals, PR expenses, etc.)	RM	Assess the costs related to reputational scandals using historical information or comparable proxies. Cost assessment may include potential sales impact, and legal or management time costs associated with legal action against the company (use historical data from past lawsuits, and/or publicly available data on settlement costs. If no historical data exists, determine a range of potential costs via the legal and communications teams). Estimate the reduced probability of a scandal after implementing cyber security practices and multiply by the costs to quantify the benefit
		Avoid **other costs** related to data breaches (such as management time, ransom demands, and potential sales losses)	OE	Calculate the savings in other costs (i.e labor, maintenance & repairs, loss of sales, employee related downtime) related to identified practices, governance and/or process change implementation less any implementation costs to quantify the benefit

*Each Sub-Practice has the potential to drive all benefits.

Investing in Protecting from Cyber Attacks (continued)

Overview of Benefits and Monetization Methods

Practice	Sub-Practice*	Proposed Benefits	Value Drivers		Suggested Monetization Methods
Improve Governance & Oversight to Protect Employee/ Consumer Data & Operating Systems from Cyber Attacks	Implement strong governance responsible for cyber security (such as board level committee responsible for monitoring and promoting data privacy protection programs and compliance with at least one director with cyber security expertise, and senior level executive- operations, tech or legal) Align internal controls with NIST and ISO 27001 standards Establish robust risk assessment processes (such as inventory of digital assets; monitoring and updates to security controls, anti-virus software, detective systems and access controls; incident response protocols, regular testing and updates) Establish policies to protect driver data and to meet regulatory requirements	Avoid **operation disruption** and associated costs	OE		Calculate the number and average cost of historical disruptions related to noncompliance or cyber security events. Estimate the reduction in likelihood of an event due to the practice, governance or process implemented and multiply by average costs to quantify the benefit
		Improves upstream or downstream **vendor and supplier relationships**	SR	OE	Measure the impact of supplier collaboration on vendor management and contract administration costs (legal costs, accounts payables staffing), working capital, and inventory management (improved delivery times, lower buffer stock). And measure the impact of cyber security management practices on costs associated with operations, legal/PR, manufacturing, etc. to quantify the benefit
	Training and awareness programs for employees	Improve **employee relations** leading to increased employee engagement	TM	OE	Measure impact on employee engagement - on productivity (revenue per employee, profit per employee, cost per day) and/or the ability to attract and retain the best talent (turnover, % of high performers) to quantify the benefits. See Employee Wellbeing Monetization Tool for suggested metrics

*Each Sub-Practice has the potential to drive all benefits.

Investing in Vehicle System Protections

Overview of Benefits and Monetization Methods

Practice	Sub-Practice*	Proposed Benefits	Value Drivers	Suggested Monetization Methods
Strengthen Vehicle and Product Security	Integrate security by design principles across vehicle software and digital platforms _____ Conduct independent penetration testing and vulnerability assessments	Increases **customer loyalty** by safeguarding their data	CL	Calculate the additional volumes of business that can be earned from existing and/or new customers driven by practice changes, increased protocols and training. Multiply by incremental volumes by an average sales price to calculate the total $ value and apply an average margin % (that may include the impact of additional costs) to quantify the benefit
		Avoid **other costs** due to data breaches (such as management time, ransom demands, and potential sales losses)	OE	Calculate the savings in other costs (i.e labor, maintenance & repairs, loss of sales, employee related downtime) related to identified practices, protocols, training and/or process change implementation less any implementation costs to quantify the benefit
		Avoidance of **fines and legal actions** due to data breaches	RM	Assess the probability and average cost (fines, administrative costs, cost of production delays, legal/PR expenses) of a regulatory violation based on historical data or relevant proxies. Estimate the reduction in probability of a violation due to implementing the changes (vehicle safety technologies, policies, and practices). Multiply the probability reduction by the average costs to quantify the benefit
		Mitigates **reputation risk** and related costs (such as revenue loss from cyber risk scandals, PR expenses, etc.)	RM	Assess the costs related to reputational scandals using historical information or comparable proxies. Cost assessment may include potential sales impact, and legal or management time costs associated with legal action against the company (use historical data from past lawsuits, and/or publicly available data on settlement costs. If no historical data exists, determine a range of potential costs via the legal and communications teams). Estimate the reduced probability of a scandal after implementing the vehicle safety technologies, policies and practices and multiply by the costs to quantify the benefit

*Each Sub-Practice has the potential to drive all benefits.

Investing in Supply Chain Security & Operational Resilience

Overview of Benefits and Monetization Methods

Practice	Sub-Practice*	Proposed Benefits	Value Drivers	Suggested Monetization Methods
Strengthen Supply Chain Security and Operational Resilience	Establish strong vendor management practices (such as vetting processes, security assessments, security requirements and incident response protocols in contracts) including compliance with ISO/SAE 21434 and UNECE WP.29) Conduct regular third party cyber risk assessments and collaborate on corrective actions Identify protocols for detecting threats and responses including driver notifications	Avoid **operational disruption** and associated costs	OE	Calculate the number and average cost of historical disruptions related to noncompliance or cyber security events. Estimate the reduction in likelihood of an event due to the practice, governance or process implemented and multiply by average costs to quantify the benefit
		Avoidance of **fines and legal actions** due to data breaches	RM	Assess the probability and average cost (fines, administrative costs, cost of production delays, legal/PR expenses) of a regulatory violation based on historical data or relevant proxies. Estimate the reduction in probability of a violation due to implementing the changes (vehicle safety technologies, policies, and practices). Multiply the probability reduction by the average costs to quantify the benefit
		Avoid **other costs** due to data breaches (such as management time, ransom demands, and potential sales losses)	OE	Calculate the savings in other costs (i.e labor, maintenance & repairs, loss of sales, employee related downtime) related to identified practices, protocols, training and/or process change implementation less any implementation costs to quantify the benefit
		Mitigates **reputation risk** and related costs (such as revenue loss from cyber risk scandals, PR expenses, etc.)	RM	Assess the costs related to reputational scandals using historical information or comparable proxies. Cost assessment may include potential sales impact, and legal or management time costs associated with legal action against the company (use historical data from past lawsuits, and/or publicly available data on settlement costs. If no historical data exists, determine a range of potential costs via the legal and communications teams). Estimate the reduced probability of a scandal after implementing the vehicle safety technologies, policies and practices and multiply by the costs to quantify the benefit

*Each Sub-Practice has the potential to drive all benefits.

Investing in Vehicle System Protections

Overview of Benefits and Monetization Methods

Practice	Sub-Practice*	Proposed Benefits	Value Drivers	Suggested Monetization Methods
Safeguard Driver Privacy and Data Protection	Provide transparent privacy notices and obtaining explicit consent for data use Implement practices to protect vehicles from hackers (such as encryption on key fob radio frequencies, onboard systems, secure logins and passwords, multi-factor authentication and biometrics, and VPN)	Avoidance of **fines and legal actions** due to data breaches	RM	Assess the probability and average cost (fines, administrative costs, cost of production delays, legal/PR expenses) of a regulatory violation based on historical data or relevant proxies. Estimate the reduction in probability of a violation due to implementing the changes (improved driver safeguard policies and practices, improved customer communication/ transparency/ permissions). Multiply the probability reduction by the average costs to quantify the benefit
		Mitigates **reputation risk** and related costs (such as revenue loss from cyber risk scandals, PR expenses, etc.)	RM	Assess the costs related to reputational scandals using historical information or comparable proxies. Cost assessment may include potential sales impact, and legal or management time costs associated with legal action against the company (use historical data from past lawsuits, and/or publicly available data on settlement costs. If no historical data exists, determine a range of potential costs via the legal and communications teams). Estimate the reduced probability of a scandal after implementing the driver safeguarding policies and practices and multiply by the costs to quantify the benefit
		Increases **customer loyalty** by safeguarding their data	CL	Calculate the additional volumes of business that can be earned from existing and/or new customers driven by practice changes. Multiply by incremental volumes by an average sales price to calculate the total $ value and apply an average margin % (that may include the impact of additional costs) to quantify the benefit

*Each Sub-Practice has the potential to drive all benefits.



Center for
Sustainable Business