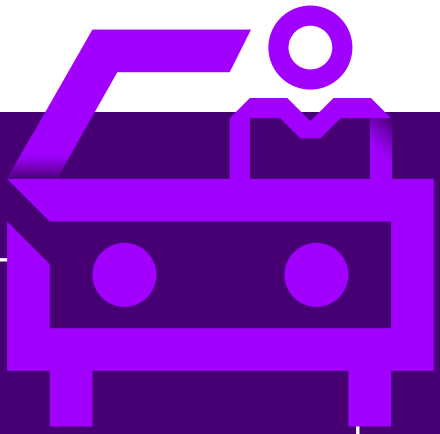
accentureconsulting

SECURITY IN THE DRIVER'S SEAT

ACHIEVING CYBER RESILIENCE IN THE AUTOMOTIVE INDUSTRY

Scaling up security

No industry is safe from the threat of cyberattacks—automotive companies on average had 160 targeted attacks last year, a fact compounded by a complex business model that involves dealing with legacy systems, a vast supplier delivery network and new data demands. As the world becomes more connected, Chief Information Security Officers (CISOs) in the automotive industry are faced with today's challenges around protecting their critical IT and manufacturing systems from cyberattacks. They must also manage tomorrow's threats that arise as a result of a broad ecosystem of relationships and the growing tsunami of data. Such actions change the scope of the CISO role—from tech-savvy specialist to business-outcome-focused advisor. To make this transition, CISOs must not only collaborate with the digital officer and digital marketing teams, but also be equipped with the insight and foresight needed to counteract cyber threats and accelerate competitive edge.



81% **of automotive executives are confident that they can quickly recover manufacturing operations in the event of a cyberattack; yet out of 33 cybersecurity capabilities, automotive is high-performing in just 18.**

2/3 **of automotive executives surveyed have experienced security incidents that involve their customers' personally identifiable information (64%) and their manufacturing industrial control systems (63%).**

Business-first security

CISOs need to evolve their role to become business enablers, guardians of cybersecurity strategies that protect critical assets and operations, even as organizations transform to become more competitive and drive growth. Organizations must handle upcoming threats posed by connected environments, broader ecosystems and the expanded use of data in all aspects of the business. In short, the security team must be front and center of any strategic plans.

Cybersecurity budget authorization rests at the highest levels of the organization; even more automotive than global respondents say it is with the Board of Directors.

30%
automotive respondents

27%
global respondents

Actions automotive manufacturers can take to reshape traditional operations and deal with the next wave of cyber threats include:

Secure operational technology environments

Safeguard the supply chain

Shift from product-oriented to customer-centric business

Secure operational technology environments

In a digital world, manufacturing environments are open to new threats. CISOs need to expand their scope of responsibility beyond information technology (IT) environments. As operational technology (OT) environments become more connected, they also become more vulnerable. For instance, when NotPetya struck, the malware spread from the servers of a Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations and causing an estimated US$10 billion of damages.[1] Similarly, the malware WannaCry forced more than one automotive manufacturer to temporarily idle some of their European plants and even shut down one automaker's production plant. Security must be seamless and universally applied across the enterprise, because decision making that is not rooted in sustainable security planning and practices can have a major impact on the business, reputation and market share of automotive companies.

As the automotive industry embraces the Industrial Internet of Things (IIoT), OT environments are under attack—the impact is being felt in areas such as process control devices or manufacturing lines through robotic control units. Such threats are challenging the industry from an organizational and technological perspective.

Protecting intellectual property and preventing production downtimes are key priorities for any automotive manufacturer. Security objectives need to focus on three areas:

Availability: Interruption can be disastrous in a production environment. A just-in-time production system can incur significant financial damage immediately if availability is not managed properly.

Integrity: Targeted attacks on data integrity in production plants have the potential to prompt far-reaching call back initiatives for automotive players.

Confidentiality: Increasing digitalization and regulation demand data protection. Automotive manufacturers that fail to put data protection first risk a loss of customer trust or even hefty fines. They need to account for data protection early in the product lifecycle and balance any restrictions with the need for accessible data in the OT environment.

71%

of automotive executives are less likely to recognize the risks from new business models and the increase in attack surface than global respondents (82%).

The convergence of IT and OT requirements highlights dramatic differences between these environments. Security teams are often strangers in OT and operational staff do not have accountability, processes, or the expertise in place to address cybersecurity issues. The average system age in OT is often 15 to 20 years, compared with three to five years in IT. Updates and patching can be infrequent, need to be aligned to limited maintenance windows and carefully managed to prevent operational disruption. Finally, unlike in IT environments, networks in OT environments are often not properly segmented and secured, enabling attackers to move laterally across the environment. As players in the automotive industry prepare to manufacture the future in the same way as other industries, such as General Electric that is building an army of AI-enabled digital twins to make significant operational savings,[2] they need to make sure they do so securely.

Safeguard the supply chain

In addition to internal controls, automotive players have a responsibility to extend security to the ecosystem of partners and suppliers who are integral to their business operations—particularly those that that have access to critical systems and data.

In a highly distributed production environment, some automotive manufacturers are reliant on third parties producing up to 70 percent of their product, and those relationships require transparency and trust. Cars consist of more than 5,000 changeable parts and these variations involve thousands of different external vendors to manufacture them. To supply these variations, the vendors need access to some of the manufacturer's intellectual property (IP), as well as customer data to support customization. Yet, 37 percent of automotive companies said that they do not apply the same security standards to their partners as their own business.[3] Smaller manufacturers and vendors often have security measures that fall far short of what is required to handle supply demands. And in addition to suppliers, unlike in other industries, distribution can involve tens of thousands of dealers and sales representatives, so keeping the network secure from attackers targeting the weakest link is a huge challenge.

In the last five years, there is growing evidence of exploitation taking place. Examples include the remote control of some systems on the driving and parking modes of a specific car model by exploiting weaknesses in the Web browser, and even compromising the car system altogether so that vehicles could be unlocked and their engines started. In July 2018, a security researcher gained access to sensitive corporate documents from nearly all of the major automotive companies that had interacted with a small Canadian company. The breach was not the result of a cyberattack but a flaw in the security basics from the enemy within—inadequate password protection on its internal servers.

50% **of automotive executives rate their third-party cybersecurity high-performing, 9% lower than global respondents.**

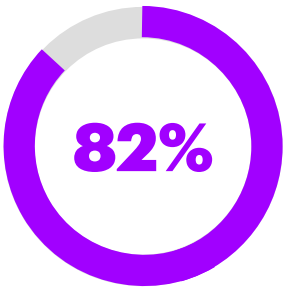
Manufacturers need to turn their attention to their entire supply chain to be confident that the security measures that are applied extend beyond their own four walls. The challenge is not a new one, but with the arrival of shorter development cycles, manufacturers can be tempted to take shortcuts on security. Automotive companies need to establish a safety-by-design culture, adopting Secure Development Lifecycle practices to standardize and embed security processes into all phases while maintaining efficiency. Many leading automotive manufacturers are also looking to their partners to provide up-to-date Secure Sockets Layer (SSL) certificates to prove they are undertaking the necessary security checks. Vendors are increasingly working with managed security partners to meet these obligations and such measures are dictating the pace in the car industry and in other industrial sectors.

Shift from product-oriented to customer-centric business

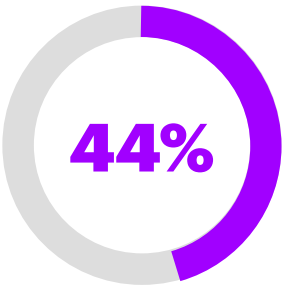
Triggered by new technologies and customer expectations, automotive manufacturers need to think differently about what they are selling and how. Instead of building products, they must address the customer experience. Rather than simply keeping the factory floor lights on, they must manage exponential data growth. Regulatory demands are being met, but trust and transparency is under scrutiny. As with many industries, moving to the cloud and embracing digitization has led to greater volumes of data to manage and exploit.

As they transform from car manufacturer (where value is gained through vehicle sales, financial services and aftersales) to a more customer-centric business as a transportation services provider (where value is achieved through mobility services, connected services, entertainment and car sharing proposals), they will need to employ more robust protection of their customer data.

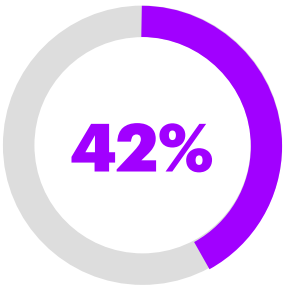
The General Data Protection Regulation (GDPR), launched by the European Union in May 2018, as well as other emerging regional privacy regulations, such as the California Consumer Privacy Act (CCPA), impose significant requirements for automotive companies to protect that data. Data-driven business models open up new digital channels that can collect many different categories of information that fall under GDPR protection requirements, including digital identifiers such as IP addresses, personal data on the driver, and telematics information from vehicles such as location or speed. Understanding what is sensitive or personal can be difficult and there are tighter restrictions around consent and processes that must be in place to ensure these restrictions are met. Detailed records are required around data processing; notifications around data breach have a 72-hour time limit, which may prove difficult to meet in practice. Managing the risk of sensitive data disclosure by third parties, including vendors and dealers, often requires new operational controls to be established. Such requirements, coupled with the prospect of heavy fines for non-compliance, mean that mastering security is vital for the whole business.



of automotive executives are confident that they can protect data privacy and comply with GDPR.



protect customer information as part of their cybersecurity strategy.



protect organization information.

Speed to value

There is little doubt that the automotive industry is under threat—from cyberattacks and the dramatic shifts that are taking place at the heart of how it functions and competes.

CISOs should adapt their role so that they can not only drive forward with confidence, but also accelerate the value their businesses can offer to their customers. Here's how:

01 Address security fundamentals

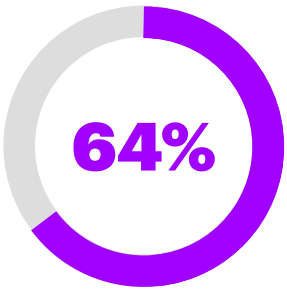
Harden and protect core assets across the entire value chain—including both IT and OT environments—and continue to pressure-test your resilience to manage today's threats. But also keep an eye on the future by automating defenses using breakthrough technologies, intelligence and data to proactively handle future threats.

02 Extend security to the wider ecosystem

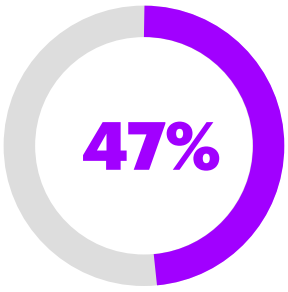
Automotive manufacturers rely on increasingly complex partner ecosystems. Identify weak links and areas of greatest risk among third-party suppliers, manufacturers, and dealers and apply appropriate security controls and governance. Support your ecosystem of vendors to maintain a high standard of mandatory security controls in the wider ecosystem.

03 Create a safety-by-design culture

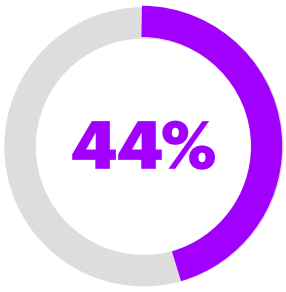
Rethink your approach to security and the role of the CISO. Build on the learnings of the established production environment around car safety. Focus on the creation of a safety culture for cybersecurity efforts, driven by a next-generation CISO who is tech-savvy and business adept.



of automobile executives hold their partners to the same or higher cybersecurity standards as their business, and audit regularly.



recognize they need to improve security monitoring.



recognize they need to improve cyber threat analytics—the "basics" of security programs.

Authors

Uwe Kissmann
Managing Director
Cyber Security Services EMEA
Accenture Security
uwe.kissmann@accenture.com

Axel Schmidt
Senior Managing Director
Global Head of Automotive Industry
Accenture Automotive
axel.schmidt@accenture.com

Contributor

Eliel Mulumba
Security Specialist
Accenture Security
eliel.mulumba@accenture.com

Stay Connected

@AccentureInd
@AccentureConsIt

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 459,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.
Visit us at www.accenture.com.

Notes

Unless otherwise stated, the statistics in this point of view represent automotive respondents in the survey report "Gaining ground on the attacker: 2018 State of Cyber Resilience," Accenture.

References

[1] https://www.wired.com/story/notpetya-cyber attack-ukraine-russia-code-crashed-the-world/

[2] https://www.accenture.com/us-en/insight-ma nufacturing-the-future

[3] https://www.accenture.com/gb-en/insights/s ecurity/cyber-threatscape-report-2018