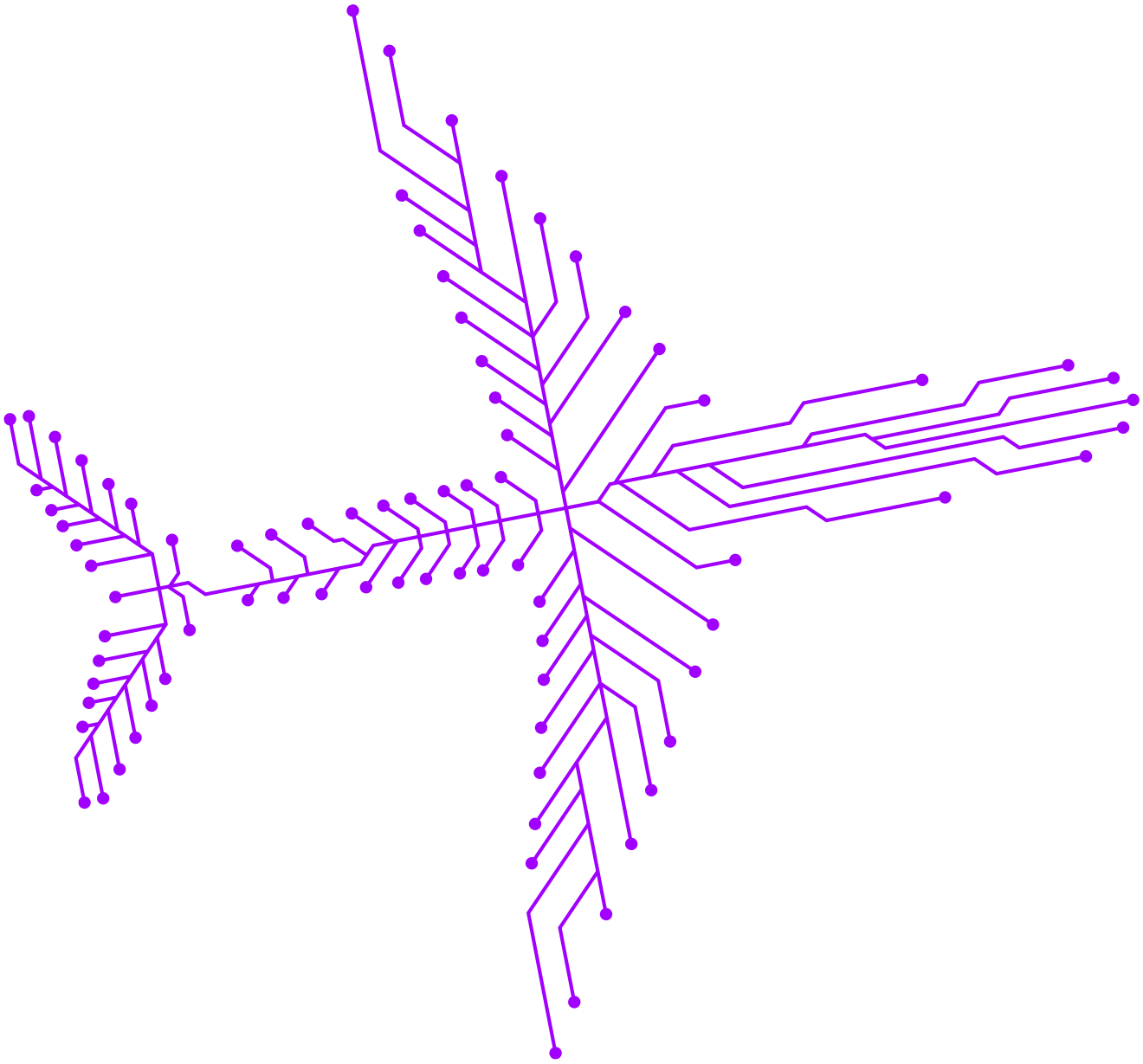
accentureconsulting



SECURING THE DIGITAL SKY

CYBER RESILIENCE IN AEROSPACE AND DEFENSE

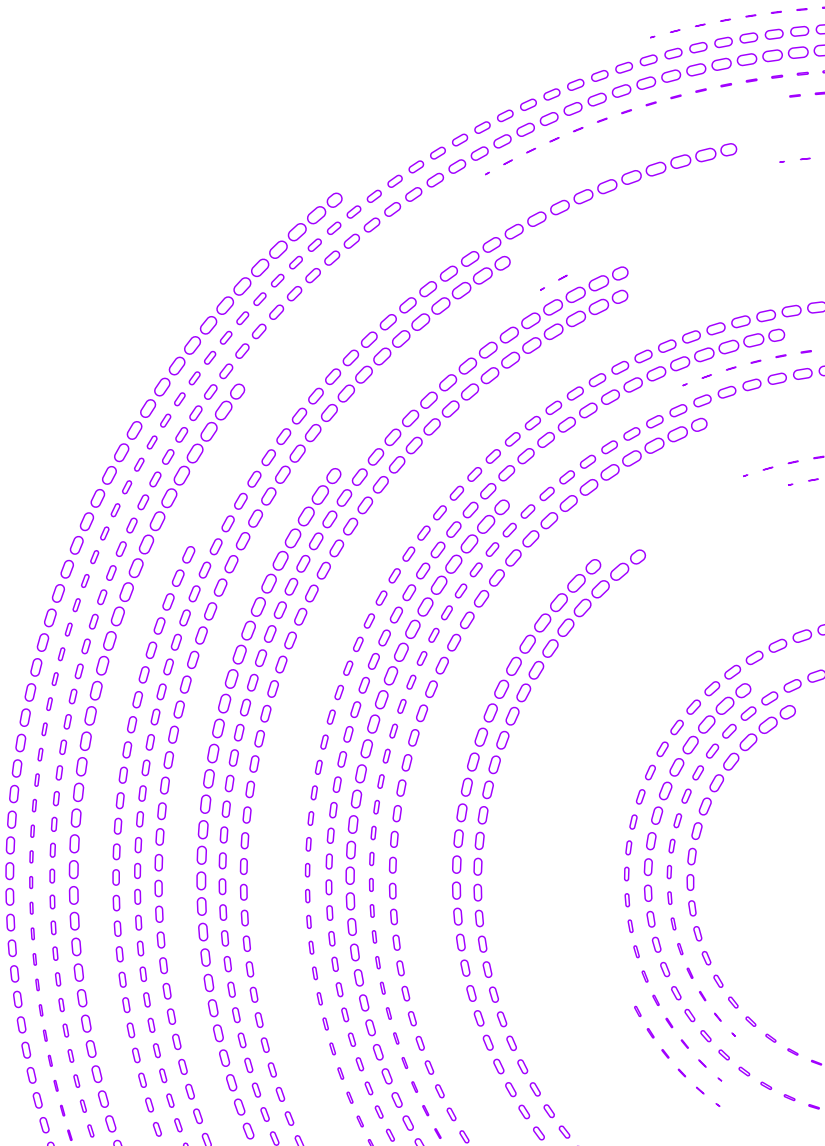
WHY AEROSPACE AND DEFENSE COMPANIES MUST PUT CYBER RESILIENCE AT THE HEART OF DIGITAL TRANSFORMATION

Aerospace and defense companies recognize they need to move faster towards the digital future. They must adopt technologies such as cloud and robotic process automation (RPA) to improve operating and business models that drive top and bottom line improvements. However, some are not prepared to address the cyber risks that accompany transformation to a connected, data-driven future enterprise. To be cyber resilient, organizations need to infuse security into everything they do—and every new thing they are preparing to do—along with ensuring that their partners' and suppliers' security also meets the right standard.

When everything is digital, everything is at risk

Aerospace and defense companies are betting on a shift to modernize their tech-enabled business and operating models in the expectation that their investments will deliver bottom-line savings and top-line growth, while also complying with new regulations. They are moving towards building an enterprise that relies upon constant, intimate digital connections with suppliers, partners and customers to stay relevant and competitive, and uses intelligent technologies in all its business operations.

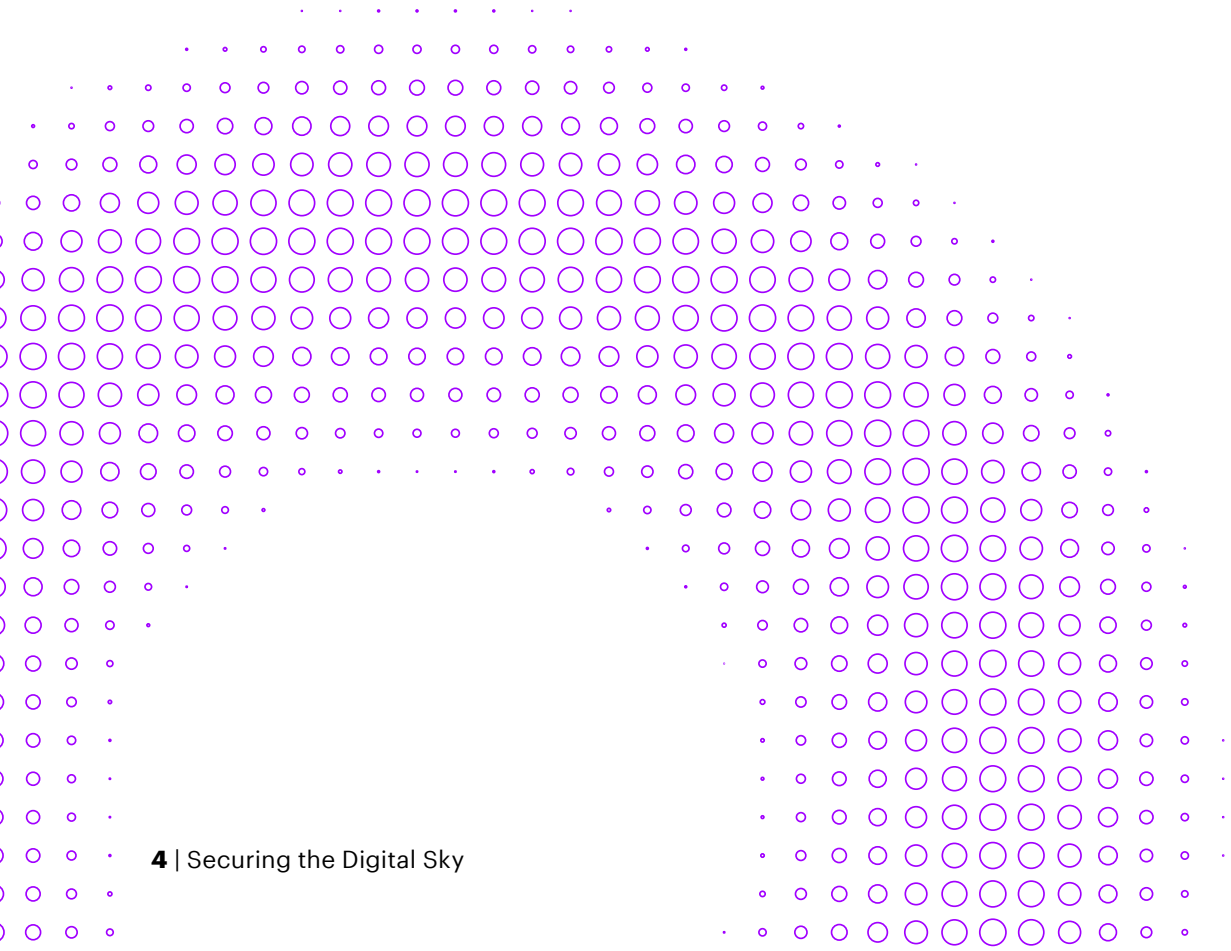
But these connected, intelligent and autonomous enterprises come with additional cyber risk. Our survey of aerospace and defense executives, including Chief Information Security Officers (CISO)[1], shows that 75% believe cybersecurity risks will grow substantially in the next few years as they adopt new and enhanced business technologies. Risks to the business include halting business operations as a result of outages, the loss of sensitive data (e.g. intellectual property, controlled information and personally identifiable information) owing to security breaches.



The future is arriving now, along with more cyber risk

Virtually everything that makes the future business more efficient, faster-moving and more competitive, involves some type of digital system or network connection that is open to the introduction of corrupting elements and is vulnerable to security incidents. Both the data and the programs that provide intelligence, for example, can be hacked. As they operate in a highly regulated industry, the theft of sensitive data is a key area of concern for aerospace and defense executives. What's more, the integration of operational technologies (OT) in aerospace manufacturing and production has made companies particularly vulnerable to cyber threats.

As many companies have learned the hard way, breaches of customers' sensitive proprietary and personally identifiable information can not only disrupt business, but also destroy the trust essential to retain customers, both B2B and consumer, in the new world of digital business.



CONNECTED
Always on, always vulnerable

The future aerospace and defense business relies on 24/7 connectivity to carry out internal processes, work with partners and reach customers. Companies are linked electronically across value and supply chains—increasingly over wireless networks—and over long distances. In addition, with the increased use of the Internet of Things (IoT), companies are also using digital connections to retrieve data and manage equipment in the physical world. In our survey, respondents cited several types of technology-related connections that they believe will raise cyber risk as they are more widely adopted (See Figure 1).

Topping the list is Artificial Intelligence (AI), which 84% of respondents said will increase cyber risk moderately or significantly. In aerospace manufacturing, companies are using AI to analyze production data from their factories and predict variations in manufacturing processes, which could enable them to tackle production issues. AI is also being utilized to improve operational efficiency for airline fleets by predicting in-service equipment failures.

Following AI on the list are mobile computing and IoT, which were cited by 82% and 80% of respondents, respectively, as posing a growing cyber risk. With the implementation of cloud-based solutions, airlines and maintenance, repair and overhaul providers (MROs) are embracing digital transformation by using mobile devices or tablets that eliminate the need for managing on-premise technology or hardware.

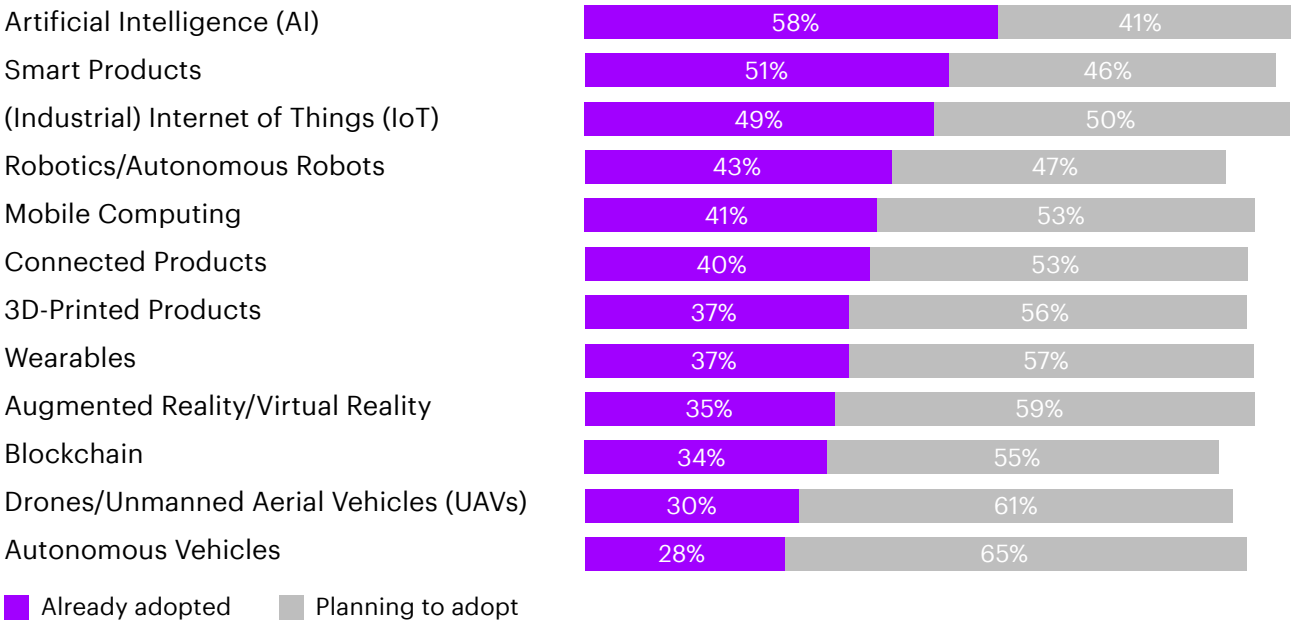
Increasingly, companies rely on the cloud for greater flexibility in IT operations and to access specialized services, such as AI analysis. Cloud computing is also operating behind the scenes in many smartphone apps to perform the data crunching that a phone can't, creating another potential vulnerability in the Bring Your Own Device (BYOD) virtual work environment.

IoT has special significance in MRO as sensors, which help in gathering data effectively to perform predictive maintenance, are being deployed on engines, fuselage, landing gear and other aircraft systems. The IoT is also being used extensively in supply chains to increase operational efficiencies, manage and track assets and monitor vital processes. Top executives are also greatly concerned about the potential dangers of sharing data with third parties. In our survey, 69% of respondents said they expect data exchanges with strategic partners and other third parties to increase cyber risk and 89% anticipate that the number of third parties and strategic partners in their ecosystems will increase in the next three years. In short, delivering products and services that are "uncompromised" is a key challenge that aerospace and defense companies face today and will continue to face in the future.

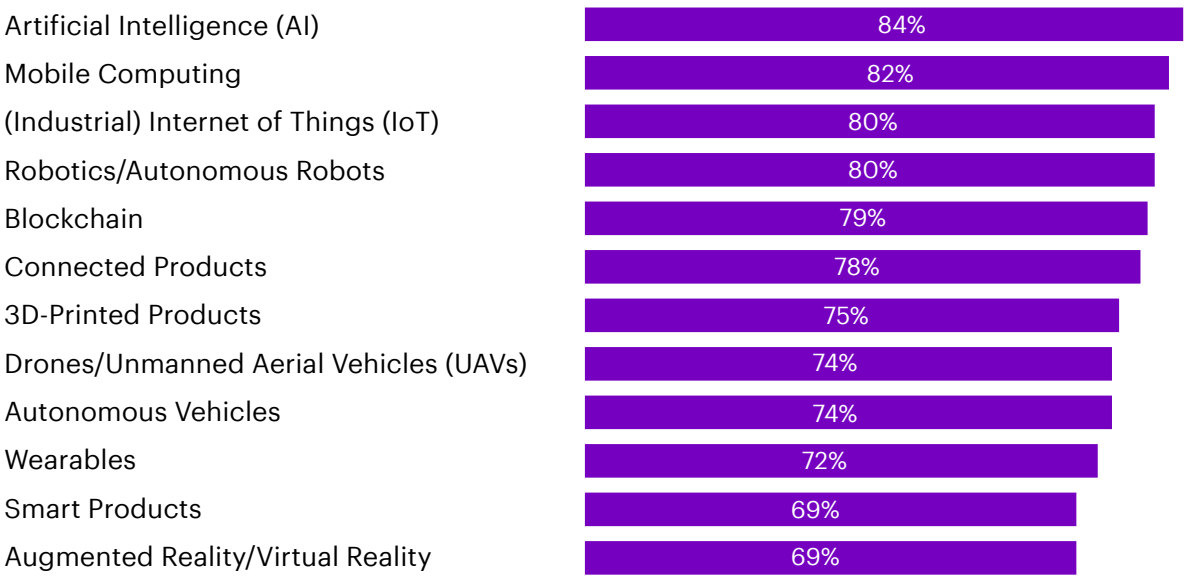
Companies also expect to make and sell many more connected aircraft products and solutions—ranging from wearable devices to next-generation avionics and inflight connectivity solutions. These products introduce potentially catastrophic cyber risks—expanding the risk from potential loss of life and physical disruptions to monetary and reputational loss.

Figure 1: Technology adoption and anticipated cybersecurity risk

New and emerging technologies that aerospace and defense companies have adopted or planning to adopt.



% of respondents stating that the technology will moderately or significantly affect the cybersecurity risk on aerospace and defense enterprises



INTELLIGENT
More data, more risk

Intelligent systems use a combination of advanced technologies, such as AI and large data sets, to take on tasks once performed by humans, as well as doing things that humans cannot easily do. Today, intelligent systems enable any business to acquire the analytical sophistication that was once the preserve of the few large organizations that could hire armies of data scientists. Using machine learning, for example, a visual processing program can teach itself how to sort parts on an assembly line or "listen" to a caller and answer customer service questions. In management, intelligent systems are helping companies make data-driven decisions. Companies represented in our survey are aware of the risks that they are assuming with the wider use of intelligent technologies: 70% of executives agree that the use of customer data significantly or moderately increases their company's risk exposure.

Given the intersection of AI, machine learning and big data within businesses, both security and data privacy protection will become stretched as risk increases. Protecting larger amounts and new kinds of sensitive data is a major concern for executives. 86% of respondents say the amount of sensitive or confidential data exchanged with ecosystem partners will increase or significantly increase in the next three years.

Companies collect more information about customers and in many more categories than ever—demographics, finances, buying histories and lifestyles—to craft the customized offers and superior customer experiences that can stimulate incremental sales and build loyalty. For example, to boost their ancillary revenues airlines are harnessing predictive analytics and machine learning to provide personalized offers to their customers. If such data is stolen or abused, companies know that they could suffer severe damage to their business, including financial loss, fines and reputational loss.

AUTONOMOUS
Self-directing systems need protection

For example, autonomous machines are deployed on the Boeing 777X airliner and Lockheed Martin F-35 fighter jet production lines. 86% of respondents say robotics will be a growing source of cyber risk. These autonomous machines could possibly be targeted by malicious hackers intending to gain access to the system's controller software, making changes to their actions that result in unsafe products. For example, Boeing's manufacturing plant had been affected by a ransomware attack last year, compromising a few computer systems affecting the 777 assembly line.[2]

In the back office, autonomous systems are multiplying as robotic process automation is introduced to save time and costs, along with improved quality, by standardizing and streamlining a wide range of business processes. It involves machine-to-machine communication, such as automatically generating an order in a supplier's computer when the procurement system signals that inventory is running low.

Today's security strategies are winning—the last war

Companies are making gains against cybercrime. According to the 2018 Accenture State of Cyber Resilience Report, companies across all surveyed industries have reduced the rate of successful cyberattacks from 30% to 13% as the number of targeted attacks more than doubled in 2018.[3] As impressive as this progress seems, most of the victories are related to known threats on existing systems. Aerospace and defense companies are more concerned about some of the unknown threats, such as nation states hacking into their systems and embedding hidden malware or exploits. Meanwhile, the future is already arriving and introducing new threats. Companies have yet to develop a broad perspective of these new cyber risks, nor have they developed the responses and remediation plans they need to operate in the new environment. In short, we are winning yesterday's war, but we are not building adequate protection against the risks created by the connected, intelligent and autonomous systems of the future business.

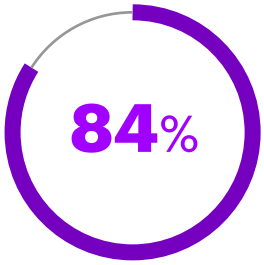
Today's security approach will not be enough to win tomorrow's battles. In most companies, security remains a separate function dedicated to shielding core IT systems and sensitive data from external entities and threats.

Today, less than half of cybersecurity budgets fund protection for OT security. Also, standard security strategies focus on detecting threats and minimizing damage, rather than making digital products and processes safer by design and during the development process. Having a robust DevSecOps program can help an organization achieve and maintain compliance while optimizing security. It does this by enabling and delegating responsibility to developers and application administrators to incorporate security measures in the software development lifecycle and beyond.[4]

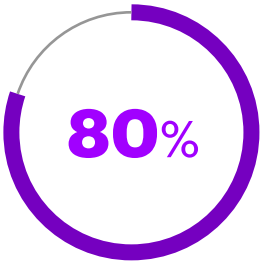
The connected, intelligent, autonomous business needs pervasive cyber resilience—with proven methods for keeping cyberattacks from crippling the business and security integrated into everything the organization does. Security expertise must be dispatched to the front lines and security must be embedded not only in IT, but also in product design, business processes and the daily work of employees. 84% of executives believe that additional security roles are needed to embed cybersecurity outside of the security/IT department (See Figure 2).

Figure 2: Aerospace and defense C-suite perception of security roles in the organization

Add new security roles

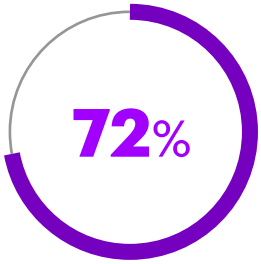


84% of CXOs agree that additional security roles are needed to embed cybersecurity outside of the security/IT department (operational technology, physical security).

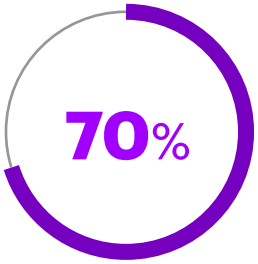


80% of CXOs agree that a C-level role is needed to bridge the CISO and the business to ensure seamless communications and business alignment.

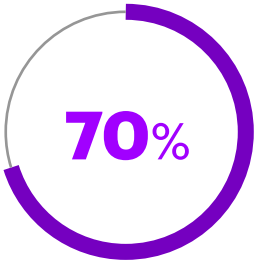
Evolve the Next-Gen CISO role



72% of CXOs agree that the role of the CISO will evolve from being an 'authoritative enforcer' to an 'influencer/ coach' to the rest of the c-suite.



70% of CXO's agree that the CISO will need a seat at the table when discussions about strategy, new businesses and new technology adoption are taking place among business leaders.



70% of CXOs agree that the CISO will need to evolve to be exceedingly business savvy to engage business leaders and be more relevant.

Closing the gap between risk and protection

There is a growing gap between the risks that companies are assuming and their cybersecurity posture. Many aerospace and defense companies are hesitant about adopting emerging technologies owing to the fear and uncertainty of the potential risks. They also tend to have cultures that are typically resistant to change. There is a disparity between what executives say are the emerging areas of concern and the cybersecurity strategies employed to enable protection. For example, while companies say that the growing volume of data exchanged with third parties is a risk, few companies are able to ensure data integrity beyond their own operations: 52% of aerospace and defense companies rely on the protocols of third parties or simply trust them to protect the information that they share.

As Figure 3 illustrates, our survey reflects a consistent pattern of gaps between awareness of growing risks and the protection afforded by current cybersecurity strategies. For example, 75% of companies said cloud services will raise cyber risk, but only 49% said that cloud technology is protected by their cybersecurity strategy. Areas with the largest gaps between risk and protection are APIs, protecting employee performance data and smart products.

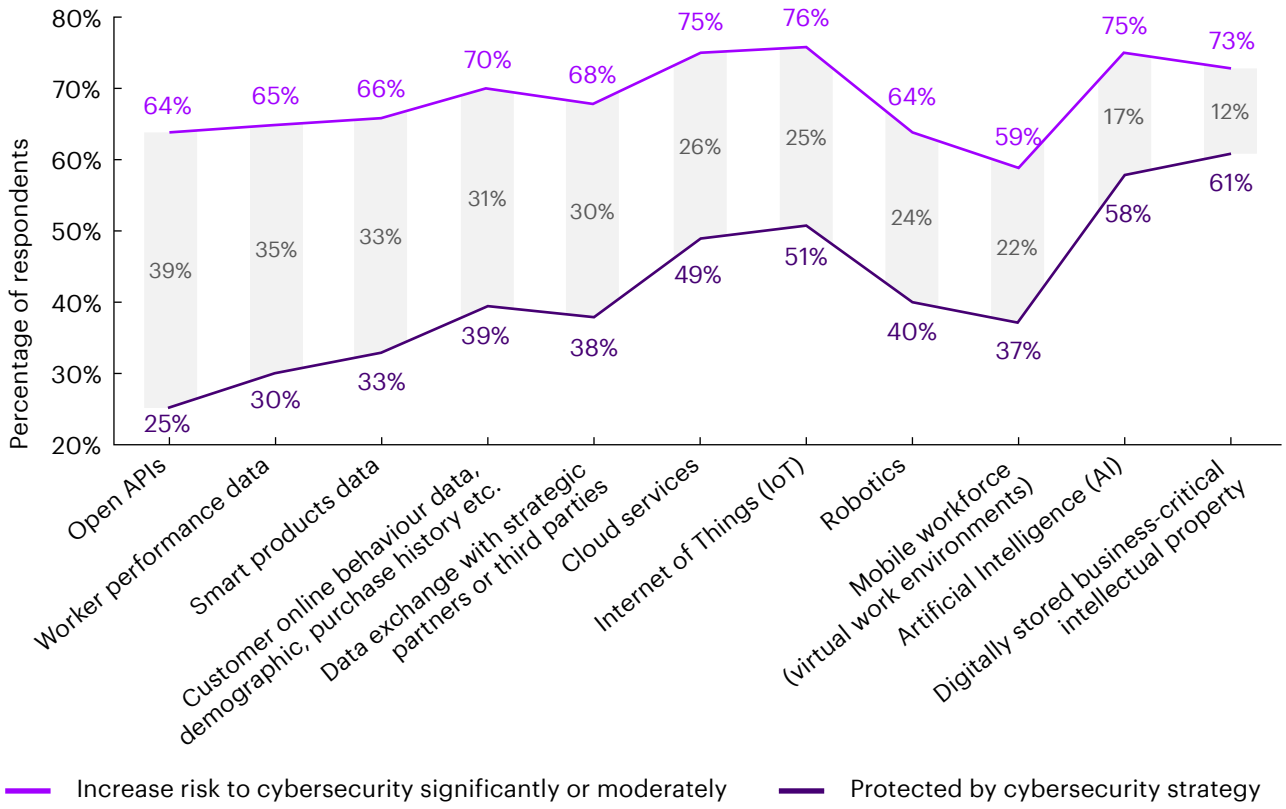
To close the gap between awareness of growing risks and current cybersecurity strategies, companies must update the way they plan and execute cybersecurity.

For example, 90% of aerospace and defense companies base their cybersecurity investments solely on past and current known risks and security compliance requirements, and do not consider future business needs in the investment plan for cybersecurity. In general, governance is not effectively established to deal with the pervasive risks arising from the future business. Often this responsibility is left to the CISO and the cybersecurity team.

The majority of business unit leaders are not asked to build security into product designs or other offerings. Business unit leaders are accountable for cybersecurity in only 31% of the organizations surveyed. While most companies have hired a CISO or assigned cybersecurity to a C-suite executive, such as a CIO, these leaders often only have limited impact beyond the security organization. For example, nearly half of respondents say the CISO is brought into discussions only after a new business opportunity has been agreed by top management.

Aerospace and defense companies can improve on spreading security knowledge among employees and create a “security-first” culture that will support pervasive cyber resilience. Only half of the respondents said all employees receive cybersecurity training upon joining the organization and then receive regular updates throughout their employment. 52% of CISOs acknowledge that establishing or expanding an insider threat program is a high priority in their role.

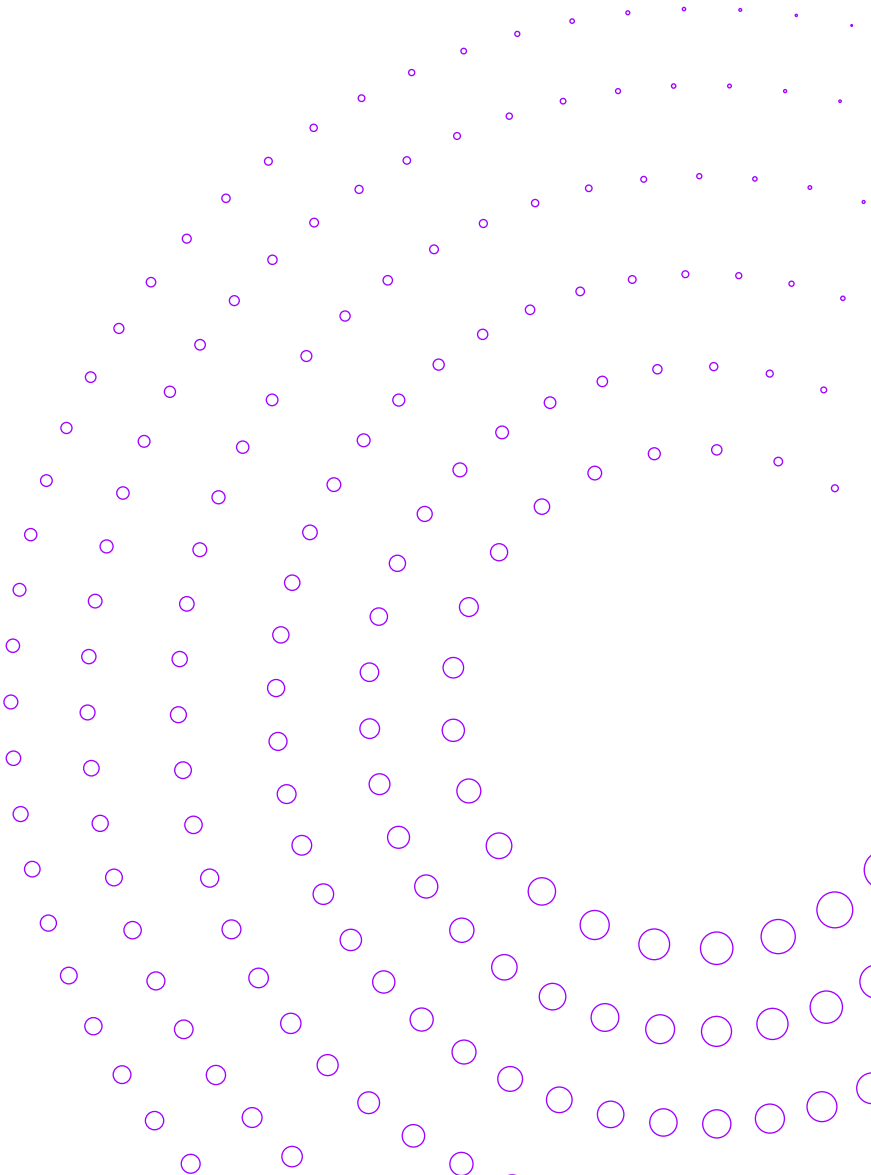
Figure 3: Gap between increased risk and cybersecurity protection



How to protect the future

To make the future business cyber resilient, companies must prepare for the risks that come with new business models and intelligent technologies. Companies not only need to link security with the business, they also need to employ the same intelligent technologies that the business—and the hackers—are using. 80% of respondents expect cybersecurity risks to diminish substantially in the next few years. This reduction is due to new cybersecurity technologies such as hardware authentication, user behavior analytics and deep learning.

To build the pervasive cyber resilience needed for the intelligent enterprise to grow safely, companies need to embed security into everything that CISOs do. They can start by developing a coherent cyber strategy and investment plan that focuses on the key issues of data governance and protection. Companies will need to make structural changes to disperse security within the enterprise and accountability across the organization, their suppliers and partners. They will need to educate the workforce and customers and work with strategic partners, third parties and industry alliances to enhance end-to-end security.



1 Make your business leaders 'Resilience Leaders'

Cybersecurity must be woven into corporate strategy, product design, budgets and daily business activities.

A major US ship-building company has created business unit level CISO roles to disperse security expertise throughout the organization.

Include security in business strategy.

Security must be in the room when strategy is being decided and options are being weighed. Our research reveals only 34% of respondents say the aerospace and defense CISO is brought in before a new business is considered. When security is an afterthought or an add-on, the new business will not be truly cyber resilient. The potential ramifications of cybersecurity breaches are on a par with the damage that companies face from other financial and business risks, and should receive the same strategic attention from CEOs and boards.

Extend security responsibility to the frontline.

Our research shows that 82% of respondents agree that cybersecurity staff and activities need to be dispersed throughout the organization, but cybersecurity remains centralized in 79% of companies. 36% of non-CISO executives say business unit leaders are accountable for cybersecurity today and a similar number say business unit leaders should be responsible in the future. Some companies see this as an extra burden, as the business or IT may not have the resources, skills or interest to include security as part of their daily responsibilities.

Make wiser bets on future resilience spending.

Getting protection right for the future business starts with budgets and planning. Today, only one out of ten aerospace and defense companies include assessments of future needs when allocating money for cybersecurity—the rest focus only on known risks. Less than one quarter of the companies have a strategic cybersecurity plan created collaboratively with IT, security and business leaders.

2 Support the security leader as a trusted business enabler

For CISOs to function as sought-after collaborators and trusted partners, they need to work closely with business units to enable the transformation and growth initiatives envisioned by their senior executive leadership.

Upgrade security talent to link with business units.

One approach that reflects the wide-ranging needs of the future business is the creation of a "Chief Digital Trust, Security and Resilience Officer", who can oversee security in the broadest possible context and serve as a bridge between security and business units, as well as to the CEO and Board of Directors. In our research, more than 80% of respondents agreed that a C-level role is needed to bridge the gap between the CISO and the business to ensure seamless communications and business alignment. Nearly half of aerospace and defense CISOs acknowledge that their responsibilities for securing the organization are growing faster than their ability to address security issues. Companies can also consider adding specialized security experts who would work with business units to build security into new offerings, practices and processes.

Provide clear guidance on cyber priorities. When asked what they need to know from the C-suite and board to understand how the business links to their responsibilities, CISOs said the top three priorities included identifying business areas where attacks would cause the greatest business loss, identifying the company's most valuable digital assets and more C-suite attention to cybersecurity matters. Yet, only 46% of executives surveyed said that their cybersecurity policy defines a formal process to identify business-relevant risks and high-value assets.

Redefine measures of success. As the CISO becomes a stronger partner with business leaders, the metrics of cybersecurity success need to expand. 70% of companies said that they use simple pass/fail metrics associated with a compliance audit to measure cyber resilience. Conventional metrics for the CISO and the security team encourage threat detection and response, but metrics need to evolve to capture additional criteria, such as how well the cybersecurity function is protecting the risks associated with future business, or how well it is spreading cyber resilience knowledge to the frontline. Today, more than two-thirds of respondents concede that cybersecurity metrics are too technical for business leaders to understand.

3 Make employees part of the solution

By accident or intent, employees enable many cyberattacks. To reduce breaches and embed cybersecurity into the fabric of the organization, companies must first make clear that employees are accountable for security.

Raytheon conducts an annual "RTN Secure Week" to help its employees increase their cybersecurity awareness. It also offers its employees the opportunity to enhance their cybersecurity skills through a full-time, formal advanced education program called Cyber ELITE.[5]

Only 12% of CISOs said employees are responsible for cybersecurity today. Security experts must not only provide ongoing training and skill reinforcement (with phishing tests, for example), they must also give employees the tools and incentives to assist in defining and addressing risks. To enact an effective insider threat program, an organization's CEO and CIO must rally human resources, learning and development, legal and IT teams to work closely with the security office and business units to develop and implement the necessary measures.

Train and reinforce safe behaviors. Without a security-first mindset, employees will remain the weakest link. New work arrangements—greater use of contractors and remote work—only make the need for employee training more urgent. Yet, training employees to think and act with security in mind is the most underfunded activity in cybersecurity budgets.[6] Companies should focus on a basic training program for all employees including skill-reinforcement activities for qualified employees.

In addition, companies should use technology to reduce the burden of responsibility placed on users. For example, they could harness attribute-based access control rather than depending on users to secure and remember passwords.

Build cybersecurity champions.
Cybersecurity champions can not only act as advocates for security across the organization, they can also provide feedback to the central team on the effectiveness of security programs. Cybersecurity champions should be at all levels and across the organization to include personnel not aligned to the security organization.

Reward "security-first" behaviors.
Reward employees who report malicious activity or criminal colleagues and offer incentives for security advocates. Only 34% of companies offer incentives for business leaders who are committed to cybersecurity. Rewards will help stimulate the desire to improve cybersecurity hygiene. Often, IT and businesses within an organization ignore and delay the implementation of security measures because they fear that they will either slow down or disrupt business functions, e.g. unintentionally blocking or breaking services.

Maintain strong defenses.
Training and reinforcement can reduce the risk of employees accidentally helping cybercriminals. User and entity behavior analytics (UEBA) systems for example, can flag suspicious employee activity, such as unusual file transfers that could indicate criminal intent. However, many aerospace and defense companies face difficulty in implementing UEBA solutions due to their complexity. Data identification, classification, tagging and protection is also a huge gap within aerospace and defense. Companies are starting to look into solutions to address this gap in order to provide the right level of security against the sensitivity of the data they are trying to protect.

4 Be an advocate for customer protection

Companies say that managing customer requirements is the second most urgent priority for their cybersecurity investments, just after their top objective of perceived risk reduction. 70% of respondents expect the use of sensitive or confidential customer information by their companies to increase. Yet, only 51% of respondents say that their customer or partner environments are adequately protected by their current cybersecurity program. But we believe that when it comes to protecting data, companies can go beyond compliance and become advocates for their customers.

Thales has combined its capabilities, such as cybersecurity consultancy, secure communications products and technology and operational control services, under a Digital Trust platform, T-SURE, which enables its customers to undertake digital transformation projects in a future proof and resilient manner without compromising their security.[7]

Prepare for new security regulations.
In response to the theft and abuse of customer data, regulators are creating new rules to protect customers, for example, the EU General Data Protection Regulation (GDPR) in Europe and the Defense Federal acquisition regulation supplement (DFARS) in the United States. Non-compliance with these regulations can lead to loss of current and/or future contract awards and subject to contract penalties.[8] One of the main issues for complying with security regulations is having true visibility into the security gaps, status of remediations and current enforcement measures across the supply chain.

Help customers protect themselves.
Companies that make sure customers understand what is happening with their data and teach customers how to protect themselves will be rewarded with customer trust.

5 Think beyond your enterprise to your ecosystem

The future enterprise might conduct business electronically with hundreds or even thousands of suppliers and partners around the world. Any one of these can expose the company to a cyberattack. Only 38% of aerospace and defense companies say that the data they exchange with strategic partners or third parties is adequately protected by their cybersecurity strategy. Hence companies need to work with ecosystem partners to jointly protect their organizations.

Boeing shares threat information with other companies in the industry through the Aviation Information Sharing and Analysis Center (ISAC) as well as with national security agencies.[9]

BAE Systems has launched a cybersecurity intelligence network to address the challenges that companies face in sharing threat intelligence.[10]

Govern and manage ecosystem risks systematically.
Companies can establish formal mechanisms, such as written contracts, as well as informal procedures to develop and maintain secure connectivity with suppliers, partners and other third parties. They need to periodically simulate real-world supply chain attacks that could impact their organizations. And they need to implement a program to assist partners and suppliers in need of support to improve their cyber hygiene.[11]

Participate in the industry's security efforts.
In the next three years, 82% of respondents expect their organizations will work with other companies in their industries to share knowledge, services and products to improve cyber resilience.

The progress on information sharing is also an opportunity to shape participation and development of standards across the organizations within the industry. Our research shows that some are doing this with 62% of companies addressing cybersecurity standards in their collaboration within the community.

Conclusion: Build pervasive cyber resilience

Leaders can ensure the success of the connected, intelligent, autonomous business by making sure that security is a core competency across the organization. If they do this, companies will not only keep the enemy at bay, they will also build trust with customers and partners. By ensuring business processes are more resilient to cyberthreats, they will become stronger competitors. With pervasive cyber resilience, the future business can grow with confidence that cyberattacks will have only minimal impact on their daily operations and reputation.

In particular, managing security across the supply chain needs to be a major focus for organizations conducting business with the government, either directly or indirectly through a defense contractor. Security measures including technical assessments and response/remediation plans must be in place, so that businesses are able to provide evidence to the government that actions have truly been taken to safeguard sensitive information, assets and people.

References

1 2018 State of Cyber Resilience, Accenture, April 2018

2 The Seattle Times (2018), Boeing hit by WannaCry virus from: https://www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/

3 2018 State of Cyber Resilience, Accenture, April 2018

4 Presentation on NIST SP 800-171: Compliance through DevSecOps, Accenture Security

5 Raytheon, Protecting Every Side of Cyber from: https://www.raytheon.com/responsibility/cyber

6 Security Awareness Training Explosion, Cybersecurity Ventures, February 6, 2017

7 Thales Group, Digital Trust from: https://www.thalesgroup.com/en/digital-trust

8 Cybersheath (2018), Understanding DFARS 252.204-7012 and NIST SP 800-171 from: https://www.cybersheath.com/understanding-dfars-252-204-7012-and-nist-sp-800-171/

9 Transportation Research Board, Aviation ISAC from: http://trbcybersecurity.erau.edu/resources/01_14_16_Francy_TRB_Panel_AISAC_FINAL.pdf

10 Bae Systems, The Intelligence Network from: https://content.baesystems.com/theintelligencenetwork/uk

11 Accenture Security Cyber Defense: Supply Chain Defense Services

About the Authors

Kelly Bissell leads Accenture's Global Security business. In this role he spearheads Accenture's commitment to help clients build resilience against cyber risks, accelerate digital business growth and innovate safely.

Ryan LaSalle is Managing Director of Accenture Security—North America. His responsibilities include all aspects of security in North America, helping our clients to become more cyber resilient and giving them the ability to grow with confidence.

Madhu Vazirani is based out of Mumbai office and serves as the APAC Research lead for Financial Services. She regularly conducts strategic analysis on the banking and capital markets industry worldwide and recently also focused on financial inclusion in emerging markets.

Roy Hu is a Principal Director of Accenture Security. He is the Accenture Security Lead for Aerospace and Defense Industry for North America. His responsibilities include managing the security business and providing valued services to aerospace and defense clients.

Aerospace and Defense

John Schmidt
Aerospace and Defense
Global Industry Lead

Marc Gelle
Aerospace and Defense
Europe Industry Lead

Jeffrey Wheless
Aerospace and Defense
Global Research Lead

Anshul Sharma
Aerospace and Defense
Research Associate Manager

About the research

What is a cyber resilient enterprise?

In this study, we define the cyber resilient enterprise as an organization that brings together the capabilities of cybersecurity and business continuity, and has strategies to quickly respond to threats, minimize damage and continue to operate in the face of attack. As a result, the cyber resilient enterprise can proceed with innovation in digital business models, strengthen customer trust and grow with confidence.

About the survey

In early 2018, Accenture Security surveyed 1,460 executives (n=100 for aerospace and defense) to understand the extent to which organizations prioritize security in new business initiatives, whether their security plans address future business needs, what security capabilities they have and their level of internal and external collaboration on security. These executives represent companies with annual revenues of US$1 billion or more from 14 industries and 16 countries across North and South America, Europe and Asia Pacific. Half of respondents were Chief Information Security Officer or equivalent roles, while the remaining half were CEOs and other C-suite executives.

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 477,000 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.

Disclaimer

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

190128