INNOVATING AT SPEED AND SCALE WITH IMPLICIT SECURITY TECHNOLOGY VISION
Continuous innovation through emerging technology adoption.

It is mandatory for companies now that digital is everywhere. In fact, more than three-quarters of executives (76 percent) believe that the stakes for innovation have never been higher—and getting it right will require new ways of innovating.¹

But how can your enterprise be at the forefront of technology adoption to drive growth—and do it securely? What will create this engine for continuous innovation, especially as competition swirls from both startups and ambitious peer companies? And why is the timing for innovation so vital now as global businesses face economic uncertainty?

Answers to these questions emerge through Accenture’s pioneering cyber research, in which we have identified an elite subgroup of global enterprises that are innovating securely for competitive differentiation. We call these the “alpha innovators.”

Our most significant findings? These alpha innovators—all major household or industrial name brands—are making big plays with artificial intelligence (AI), fifth-generation wireless technology (5G), quantum computing and extended reality (XR). They are not only investing heavily and simultaneously in three or more of these emerging technologies for business growth, but also collaborating with Security executives from day one and throughout the adoption journey. As a result, they are better prepared to maintain their leadership in the marketplace through innovation outcomes, such as top-line revenues, cost savings, market capture and new services.

In other words, these alpha innovators are doing innovation right—at speed and scale with implicit Security.

Using our data-driven insights, your company can align this approach with your Business and Security goals to help design a unique Innovation DNA that functions as a core part of the enterprise, rather than as an ad-hoc activity.²
Contents

Core report based on survey findings

4 Meet the alpha innovators
6 Understanding the big-picture context
18 Power plays of the alpha innovators
   20 Multi-pronged strategy
   22 Risk mindset
   26 Borderless collaboration
   28 Culture of innovation
   30 Defense in depth
35 Recommendations to align power plays
39 Survey methodology

Emerging technology sidebars

12 AI Security: Expanded approaches
16 5G features escalate security
24 Quantum computing introduces security “zingers”
32 Importance of securing XR
Meet the alpha innovators

In conducting our cyber research, Accenture surveyed Business and Security executives, most of which were C-level, from global companies across multiple industries with $5 billion+ in revenues.

Already high performers, these enterprises understand that future growth depends on continuous innovation with disruptive technologies. Therefore, Accenture’s objective was to determine what approaches and best practices are differentiating them from the competition and why. (To learn more about our online survey methodology and panel of executives, see description at end of document.)

What emerged through our analysis was a notable innovation divide among the surveyed set. Most importantly, we identified an elite subgroup (28 percent) of enterprises—or what Accenture is calling the “alpha innovators”—that are adopting early and going big with powerful plays to achieve growth. (Note: We are calling the remaining 72 percent the “followers.”)

These alpha innovators are actively exploring and applying multiple emerging technologies and investing heavily to integrate them across the business. Additionally, they show a more mature approach to AI, 5G, Quantum and XR, especially in terms of understanding how to secure the technologies and how to engage collaboratively with Security executives.

This ability to be ahead of the curve is more critical than ever. Given global events, companies must work swiftly to be resilient in the market, outmaneuver uncertainty and shape the future. Now that digital is everywhere, people increasingly expect new services and solutions to fully address Security and data privacy. Companies that deliver on these expectations will likely increase business ecosystem and customer confidence in adopting new products and services fueled by emerging technology.

Bottom line, the alpha innovators exhibit both the appetite for continuous innovation and the Security acumen to do it in a risk-managed way at speed and scale. Thus, they are the ones to emulate.
With further analysis, Accenture identified the five “power plays” that alpha innovators are doing right in terms of a multi-pronged strategy—investing at scale now across all four emerging technologies; risk mindset—assessing the Security risk fully; behavior of borderless collaboration—working across all aspects of the enterprise for agility; culture of innovation—creating an internal and external ethos; and defense in depth—applying a range of protective and detective security controls and models for emerging technologies.

Specifically, we focused our study on looking at how the alpha innovators bring innovation into their lifecycle to drive business growth and scale their approaches. This included how they engage across the organization to innovate, think about collaboration, demonstrate agility and apply Security practices to de-risk technology adoption. From this analysis, we also ascertained how these attributes are building trust with customers, employees, ecosystem partners and governments—in ways that balance the business value being delivered with people’s values, an important distinction in the post-digital era.

Since collaboration inside and outside the enterprise is essential for success, we present some survey results from a dual perspective across the C-suite—from both the Business side (Chief Information Officer, Chief Innovation Officer, Chief Strategy Officer, Chief Technology Officer and Business Unit/Line of Business Lead) and the Security side (Chief Risk Officer, Chief Cyber Security Officer, Chief Information Security Officer (CISO). This provides a richer picture of organizational behavior and perceptions, while revealing a point-counterpoint view of what is and is not working with emerging technology adoption. (Note: For the remainder of the report, we will use CXO to refer to all Business respondents and CISO for all Security respondents.)

In the following sections, we first review the insights derived from the overall data set to establish context for the characteristics of the surveyed enterprises. Then, we drill down into the differentiating traits of the alpha innovators, namely the five “power plays” that set them apart from the “followers.” To supplement these data insights, we include four emerging technology sidebars with Accenture’s perspectives on securing AI, 5G, Quantum and XR. Finally, we offer key takeaways to help companies achieve their innovation objectives regardless of their position on the continuous innovation journey.
Starting with the whole data set, our research shows that all survey respondents see the enormous opportunities availed through emerging technologies to impact business growth. As such, they are confidently incorporating adoption planning into their strategies for AI (at 87 percent), 5G (79 percent), Quantum (63 percent) and XR (58 percent). All surveyed enterprises are also taking steps to be their own disruptors. They are not waiting idly for the competition to define the market; instead they are pursuing emerging technology initiatives internally and externally to maintain their leadership positions in the marketplace and achieve competitive advantage now.

As shown in Figure 1 (left-hand chart), most respondents (i.e., 30+55=85 percent overall; 28+62=90 percent of the alpha innovators) identify as first or early adopters of emerging technologies and believe they are prepared for adoption. This result also provides evidence of a marked gap between perception and reality; in other words, a disparity between self-identifying as an early adopter and setting the strategic course to actually perform as an early adopter.
Figure 1: Most respondents say they are rapidly adopting emerging technologies and relying on a comprehensive operational approach; however, actions speak louder than words.

### Innovation appetite for adopting emerging technologies
(CXOs and CISOs; n=500)

<table>
<thead>
<tr>
<th>Category</th>
<th>Overall</th>
<th>Alpha Innovators</th>
</tr>
</thead>
<tbody>
<tr>
<td>First adopter</td>
<td>28%</td>
<td>30%</td>
</tr>
<tr>
<td>Early adopter</td>
<td>62%</td>
<td></td>
</tr>
<tr>
<td>Early majority</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>Late majority/Late follower</td>
<td>1%</td>
<td>2%</td>
</tr>
</tbody>
</table>

### Agreement with statements
(CXOs and CISOs; n=500)

<table>
<thead>
<tr>
<th>Category</th>
<th>Overall</th>
<th>Alpha Innovators</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategy/Investment:</strong> We prioritize investments in emerging technologies such as Extended Reality, Artificial Intelligence, 5G and Quantum Computing as much as our current technologies</td>
<td>81%</td>
<td>61%</td>
</tr>
<tr>
<td><strong>People/Internal workforce:</strong> We have the skills we need to secure the adoption of emerging technologies such as Extended Reality, Intelligence, 5G and Quantum Computing</td>
<td>74%</td>
<td>64%</td>
</tr>
<tr>
<td><strong>People/Ecosystem:</strong> We have many/multiple connections with outside organizations with expertise in emerging technologies such as Extended Reality, Artificial Intelligence, 5G and Quantum Computing</td>
<td>82%</td>
<td>65%</td>
</tr>
<tr>
<td><strong>Processes:</strong> We use the lens of emerging technology to review our business processes and this is built into our business strategy</td>
<td>82%</td>
<td>65%</td>
</tr>
</tbody>
</table>
Continuing with the right-hand chart in Figure 1, this preparation translates into the following actions:

**Investment** Prioritizing investments in AI, 5G, Quantum and XR (61 percent overall; 81 percent alpha innovators score themselves as a 4 or a 5 on a five-point scale)

**People** Assessing the internal workforce skillsets needed to secure the technology adoption (64 percent overall; 74 percent alpha innovators)

**Ecosystem** Developing connections with outside organizations that have expertise in the emerging technologies (65 percent overall; 82 percent alpha innovators)

**Processes** Using the lens of emerging technology to review business processes as a core part of the business strategy (65 percent overall; 66 percent alpha innovators).

Generally, this reveals that the surveyed companies have the foresight, operational structure and follow-through for innovation. They are not leaving technology exploration to outside entities—they are taking on the challenge directly and making budgetary decisions to achieve their aims.

But preparation and approach are also where the alpha innovators demonstrate a decisive edge, showing they are twice as likely to take the strategy, people (internal workforce) and process actions to the fullest extent by scoring themselves as 5s on a five-point scale.

Moving to questions about budget (see Figure 2), most of the surveyed companies are already investing or planning to invest in emerging technologies—and within four years, nearly all companies expect to adopt these technologies. What is noteworthy here is the sheer size of these investments: 34 percent of respondents spent more than US $500 million over the past year. Of this, 9 percent spent more than US $1 billion over the past year on disruptive technology adoption.

This finding confirms that enterprises with a continuous innovation agenda are not only investing early, they are investing heavily to achieve speed and scale that drives new growth. It also serves as a signal to every company aspiring to become an innovator: it is critical to reassess your strategy now and recalibrate investments accordingly—or get surpassed by the competition.

34% of respondents spent more than US $500 million investing in emerging technologies over the past year
Figure 2: Respondents are allocating significant budget for emerging technology implementation.

Timing to invest in emerging technologies
(CXOs and CISOs; n=500)

Emerging technology spend (past year)
(CXOs and CISOs; n=500)

- Less than $250 million USD
- Between $250 - $500 million USD
- Between $501 million and $1 billion USD
- Over $1 billion USD

34% Spending > $500m

Percent of respondents (cumulative over time)

AI  5G  Quantum  XR

0%  10%  20%  30%  40%  50%  60%  70%  80%  90%  100%

Already investing <1 year 1-2 years 3-4 years > 4 years

Security Technology Vision | Innovating at Speed and Scale with Implicit Security
But our analysis also shows that emerging technologies pose a major paradigm shift in Security challenges. As shown in Figure 3 (left-hand chart), all respondents believe AI, the most implemented emerging technology to date as indicated in our study, is perceived as the most significant Security risk (45 percent); however, only 31 percent think 5G poses a significant risk and only 28 percent believe the same for Quantum Computing—which are both surprisingly low results. The translation? Even though most C-suite executives are assessing the Security risk of these new technologies, they are underestimating the challenges they pose. (For more information on the specific risks, see sidebars about securing AI, 5G, Quantum and XR.)

Additional analysis shown in Figure 3 (right-hand chart) suggests a gap in the knowledge of the risks these technologies will undoubtedly introduce, reinforcing the need for Business and Security to collaborate in innovation discussions. As companies get farther along in the adoption journey, CISOs have a better risk IQ around what it takes to protect the organization, for example, across the expanded attack surface introduced by AI. In time, we would expect this better understanding of the risks to continue across 5G, Quantum and XR.
Figure 3: C-suite executives generally underestimate the Security risk of emerging technologies; for technologies other than AI, with later adoption, Security risk is underestimated even more so.

### Extent technologies expected to increase level of security risk for enterprises
(CXOs and CISOs; n=500)

<table>
<thead>
<tr>
<th>Technology</th>
<th>CXO</th>
<th>CISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artificial Intelligence</td>
<td>45%</td>
<td>31%</td>
</tr>
<tr>
<td>5G</td>
<td>31%</td>
<td>29%</td>
</tr>
<tr>
<td>Quantum Computing</td>
<td>28%</td>
<td>31%</td>
</tr>
<tr>
<td>Extended Reality</td>
<td>21%</td>
<td>35%</td>
</tr>
</tbody>
</table>

### Technologies imposing significant/moderate risk
(CXOs and CISOs; n=500)

<table>
<thead>
<tr>
<th>Technology</th>
<th>CXO</th>
<th>CISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artificial Intelligence</td>
<td>69%</td>
<td>83%</td>
</tr>
<tr>
<td>5G</td>
<td>61%</td>
<td>55%</td>
</tr>
<tr>
<td>Quantum Computing</td>
<td>61%</td>
<td>58%</td>
</tr>
<tr>
<td>Extended Reality</td>
<td>56%</td>
<td>57%</td>
</tr>
</tbody>
</table>
AI Security: Expanded approaches

As described in Adversarial AI, an Accenture Labs-Cybersecurity point of view, AI presents a new attack surface that enterprises must be ready to defend.

Unlike discretely coded applications, AI behavior is probabilistic; by nature, all conditions and outcomes are not practically demonstrable or known. To be able to trust AI in production, companies should build key Security functions for an analog Security capability.

The first step is to divide the task into two parts: the creation of AI models and the usage of them. In creation mode, your company must protect both the data needed to train the AI and the environment where it is been created. In usage mode, the data in motion needs to be protected prior to reaching the AI for decision making and again must not be manipulated on the return. In many AI systems, distributed or federated training is mandatory. This is because the data cannot be harvested into one location—either for technical reasons or for intellectual property protection and regulations. Therefore, companies will also need to insert secured federated learning for collaboration between parties.

Another important area is to translate and expand secure development operations (DevSecOps) practices to protect AI throughout the lifecycle, a machine learning DevSecOps. Unfortunately, there is no silver bullet to defend against AI manipulations, so it will be necessary to use layered capabilities to reduce risk in AI-driven business processes. This means taking common Security functions and controls (e.g., input sanitization, application hardening and Security analytics) and formalizing their machine learning equivalents—across data integrity and veracity checks, input pre-processors, resilience design, and manipulation detection and response capabilities.
Every business process will differ in terms of critical functionality and overhead tolerance. Companies will need to perform a threat modeling exercise for each process and curate individual defenses in order to maintain the core business function. It is also helpful to keep a library of repeatable defenses for different scenarios, making it easier for data scientists (who are not Security specialists) to protect business processes.

Emerging research has demonstrated that machine learning models have unique Security and privacy issues once in production.\(^3\) If a model is exposed to external inputs, it is at risk for model extraction—a method for reverse engineering the model and generating a surrogate model that reproduces the functionality of the original model. This has obvious implications for intellectual property confidentiality, plus surrogate models can be used to increase the efficiency of model manipulation attacks. According to related research, adversaries can also conduct inference attacks on the model to learn about the training data set, which could contain sensitive or regulated personally identifiable information.\(^4\)

To defend against model extraction and privacy attacks, you need to think carefully about the models exposed externally, as well as the necessary controls to secure those models. Some controls are easy to implement such as rate limitations or usage thresholds; however, some models may require more sophisticated defenses, including abnormal usage analytics and web API Security. Keep in mind that weaknesses may also relate to the nature of the machine learning model, itself.

In many cases, companies use AI models that are provided as a service, which should trigger the hygiene and Security controls expected in cloud service environments. Nonetheless, you still need to pay attention to the providence of these models and data. Open sourced or externally generated models and data provide compelling attack vectors into organizations. This is because attackers do not have to bypass internal Security controls to manipulate the data/models and insert unintended behavior. Be sure to validate anything procured externally—looking for new data or model poisoning attempts to manipulate model behavior—before applying it to business processes.

Lastly, your company will need different Security capabilities to validate AI models, data sets and model behavior and understand the strength of the model before deploying into production environments. These Security capabilities will span the ML pipeline—from augmentation/modification of the raw dataset, to model design and training, to sample/model interaction analysis. Once again, every ML process will differ in functionality and overhead tolerance, so it will be necessary to build threat models for each process and have methods for different scenarios to ensure data integrity and model strength.
The theme of underestimation continues as C-suite executives overall underrate the extent and timing of what they need to do to secure these technologies and when. For example, as shown in Figure 4A, when asked how their organizations are planning to build the expertise needed to support the emerging technologies, most said they would train existing employees (77 percent), collaborate or partner with organizations that have the expertise (73 percent), hire new talent (73 percent) and acquire new businesses or start-ups (49 percent).

While these are all viable approaches, especially when done concurrently, both CXOs and CISOs are still underestimating the time it takes to upskill professionals to the appropriate level. Online learning platforms can help employees gain basic proficiency in securing a technology; however, achieving expertise and full competency will most likely take years of education combined with practical experience.

What’s more, respondents assume there will be ample talent with AI, 5G, Quantum and XR skillsets available for hire, but the reality is a shortage of these skills in the marketplace.

To compound the issue, finding security talent with these emerging technology skills will be even harder. Given these factors, it is important that companies strengthen their ecosystem collaboration with proven third parties and talent acquisition plans now, in order to ramp up the necessary security skills and security alliances as quickly as possible.

Likewise, CISOs universally underestimated when they need to start planning to secure these emerging technologies (see Figure 4B). Only half (55 percent) are actively planning to secure AI today and the numbers decline from there with 5G (36 percent), XR (32 percent) and Quantum (29 percent).
What’s apparent is a general lack of understanding and potentially a lack of urgency about the security risks—an oversight that could have profound effects on both the innovation and growth potential of these enterprises.

In our assessment, the understanding of the security risks increases as these companies move forward on the adoption curve. Early in adoption, there is knowledge about the security risks to the enterprise. Further into adoption, we see much more comprehension and engagement from teams working to secure the technology and actively manage risks.
5G features escalate security risks

As more enterprises transition to 5G technology applications, both service providers and service consumers will have to take 5G Security issues and potential implications into consideration.

Challenges your company could face can be categorized into three groups:

1) Security issues carried over from previous generations of telecommunication protocols and standards that were not resolved in 5G, such as lack of authentication functions.

2) New Security issues that arise from 5G technology through features, including virtualization that expands the attack surface and hyper-accurate location tracking that may increase privacy issues for users.

3) Security concerns from the increased volume and speed of the network, such as a surge in video and remote computing of AI; more frequent video communication and XR usage will introduce new image and video-based vulnerabilities.

Like the growth of cloud services, 5G has the potential to create shadow networks that operate outside of the knowledge and management of the enterprise. As companies learned early in the journey to cloud, they must manage enablement and bring rogue instances into the enterprise fold of controls.

Additional lessons learned from the technology supply chain can also apply in the 5G realm, such as ensuring device integrity throughout the entire spectrum—hardware, firmware and applications. Since 5G inherits the weaknesses of HTTP, XML and TLS protocols, the attack surface at the edge can expand with IT/OT convergence to include a range of devices with increasing levels of intelligence, including autonomous machines and robotics. And now the stakes are even higher with the migration to a remote workforce, as people complete work from anywhere using laptops, tablets and mobile phones. As a result, companies must carefully consider which processes and data are moved to a wide spectrum of end devices and what level of trust is needed in each.

By design, 5G networks bring together multiple heterogeneous networks and technologies, which will likely create new complexity and costs for network monitoring and Security management. Device registration must include authentication to manage the attack surface of the enterprise. Without it, message integrity and user identity cannot be assured.
Likewise, the number of devices that can be connected to the network and request different types of services (e.g., low latency vs. high reliability) exposes the network to jamming, denial of service and other performance-targeting attacks. In addition, any new or adjusted configuration of the network as a service, based on a request from the network tenant, are provisioned automatically to achieve high availability and robust operation. Validating and testing these configurations in a continuous integration/continuous delivery mode requires managing Security risks in the development and staging phases as well.

One of the advances in 5G is seamless handover at speed. To achieve this, however, organizations should enable quick roaming and simplified identity management, which in turn can increase the exposure of the connection to man-in-the-middle attacks.

Lastly, the consumer-friendly features proposed by 5G technology and devices, such as location-based or API services, directly targets the user privacy offered by organizations. In response, companies should reinforce and expand privacy protocols to cover this broader range of services.
Power plays of the alpha innovators

As we looked deeper into the full set of global high-performing companies, our cyber-research findings reveal an innovation divide—between the preparedness and actions of the elite subgroup of alpha innovators (28 percent of companies surveyed) and the remaining followers in terms of a multi-pronged strategy, risk mindset, borderless collaboration, culture of innovation and defense in depth.

The alpha innovators are doing something exceptional and, in the process, creating an advanced playbook. They are achieving continuous innovation at speed and scale with implicit Security. They are innovating securely for competitive differentiation and future growth. And they are making the moves for scale, taking the significant steps and embedding the distinctive Security capabilities across the business for long-term success.

The most striking result from our findings about the alpha innovators? In order to innovate at scale and speed with emerging technology, collaboration with the CISO is essential (see Figure 5). Early adoption and major investments are not enough. True success requires significant CISO engagement and cyber risk management expertise from the beginning and throughout the day-to-day innovation journey, which includes having the right mindset, behaviors and culture to make it happen.
To be poised for successful and secure emerging technology adoption, your company should follow this advanced playbook, which is distilled into these five power plays:

#1 Multi-Pronged Strategy
#2 Risk Mindset
#3 Borderless Collaboration
#4 Culture Of Innovation
#5 Defense In Depth

Companies planning to innovate for growth should take heed: The Security decisions your company makes today will determine which side of the innovation divide you land on. Security investment protects overall innovation investment and the resultant return on investment. Thus, preparation has never been more critical. Collaboration is front and center. Whether maintaining your enterprise’s position as an alpha innovator or aspiring to make the leap into this category, it will take bold action and ongoing commitment to achieve while building your unique Innovation DNA.

Figure 5: Alpha innovators are much more likely to collaborate with the CISO to fully address Security challenges of emerging technology adoption.

<table>
<thead>
<tr>
<th>Security Technology Vision Index (CXOs and CISOs; n=500)</th>
<th>Collaborate</th>
<th>Support CISO inclusion</th>
<th>Adopt cybersecurity mindset</th>
<th>Commit resources</th>
<th>Invest early</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alpha Innovators</td>
<td>81%</td>
<td>59%</td>
<td>78%</td>
<td>51%</td>
<td>100%</td>
</tr>
<tr>
<td>Followers</td>
<td>70%</td>
<td>49%</td>
<td>68%</td>
<td>32%</td>
<td></td>
</tr>
</tbody>
</table>

Security Technology Vision | Innovating at Speed and Scale with Implicit Security  |

#TECHVISION2020
Multi-Pronged Strategy: Invest at scale now across all four emerging technologies

The alpha innovators, the 28 percent of the companies surveyed, are already investing in at least three of the four emerging technologies: AI, 5G, Quantum and XR.

Naturally, those investing in at least three technologies are investing significantly more than the remaining set—at a rate of 51 percent investing more than US$500 million. And the pinnacle of the alpha innovators—the top 6 percent—are going even bigger by actively investing in implementing all four technologies now (see Figure 6).

Figure 6: Alpha innovators are adopting emerging technologies more rapidly and committing to at least three of the four technologies today.

<table>
<thead>
<tr>
<th>Organizations investing in emerging technologies (AI, 5G, Quantum, Extended Reality) (CXOs and CISOs; n=500)</th>
<th>Percent of IT budget dedicated to emerging technologies (CISOs; n=250)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investing in less than 3 (Followers)</td>
<td>Alpha Innovators</td>
</tr>
<tr>
<td>Investing in 3 or more (Alpha Innovators)</td>
<td>More than $500m</td>
</tr>
<tr>
<td>72%</td>
<td>49%</td>
</tr>
<tr>
<td>28%</td>
<td>51%</td>
</tr>
</tbody>
</table>

Followers

| 71% | 29% |

More than $500m

$500m or less
Homing in on the Security spend in the alpha innovators set, CISOs are allocating more than one quarter of their budgets to secure emerging technology (see Figure 7). Overall, our survey respondents say their companies have an average of nearly $235 million of IT budget dedicated to emerging technologies. This is a substantial amount and a clear indicator of the deep, action-oriented commitment they have to achieving innovation, which includes investing in the necessary Security tools, dedicating the appropriate number of people to secure networks, applications, data and access control for these new technologies; up-skilling people with the new level of Security skills required; and supplementing where needed by building ecosystem partnerships with third-party providers.

Figure 7: Alpha innovators are allocating significantly more of their IT budget for emerging technology implementation.

28% of companies surveyed are already investing in at least three of the four emerging technologies.

Percent of IT budget dedicated to emerging technologies
(CISOs; n=250)

- 1% – 20%: 19% Alpha Innovators, 45% Followers
- 21% – 40%: 36% Alpha Innovators, 42% Followers
- > 40%: 25% Alpha Innovators, 14% Followers
Continuous innovation through emerging technology adoption requires a comprehensive view of Security—and a plan to de-risk emerging technology adoption from day one.

Across the alpha innovators, all C-suite executives are significantly more aware of the magnitude and implication of the Security risks of implementing AI, 5G, Quantum and XR. This means that both CXOs and CISOs at these companies have essentially institutionalized a shared understanding and ownership of that risk.

As shown in Figure 8, however, there is a marked difference of perceived risk by technology type. While the overall risk assessment for 5G, Quantum and XR is still lower than expected among all respondents, what we find particularly interesting is the comparison between the alpha innovators vs. the followers. On one hand, the finding shows that almost everyone is assessing the risk of each technology more accurately when further along in the adoption cycle. But what sets the alpha innovators apart is the ability to assess the risk better earlier in the adoption cycle, which reduces risk earlier, protecting the innovation investment and reducing overall lifecycle development costs.
Figure 8: Perception of Security risk varies by type of technology and where companies are in the adoption cycle.

**Extent technologies are expected increase the enterprise’s level of security risk (Significantly/Moderately)**
(CXOs and CISOs; n=500)

<table>
<thead>
<tr>
<th>Technology</th>
<th>Alpha Innovators</th>
<th>Followers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artificial Intelligence</td>
<td>76%</td>
<td>75%</td>
</tr>
<tr>
<td>5G</td>
<td>69%</td>
<td>56%</td>
</tr>
<tr>
<td>Quantum Computing</td>
<td>53%</td>
<td>75%</td>
</tr>
<tr>
<td>Extended Reality</td>
<td>67%</td>
<td>52%</td>
</tr>
</tbody>
</table>

Alpha Innovators

Followers
Quantum computing introduces security “zingers”

Whether your company adopts Quantum computing or not, you need to be ready for the very real threats to the Security of your organization and data.

Accenture covered the initial challenges in our point of view, Cryptography in a Post-Quantum World. Here, we focus on enterprise adoption of Quantum computing capabilities to enable business outcomes, then look at some newer threat considerations.

When investing in Quantum, the first step is determining which kind of “Quantum.” There is no single Quantum computing modality approach (e.g., superconducting circuits, ion traps, photonic, neutral atom, topological fermions and silicon Quantum dots), and a commercial leader has not yet emerged. Making a long-term bet too early in a single Quantum technology could yield shorter-term results. Instead, investments should be made that are portable or agile, in order to avoid vendor lock-in.

Most enterprise-grade Quantum computers will likely be integrated into organizations and clouds as high-performance systems for specialized computations. Safeguarding these Quantum resources against novel attack vectors will require deep Security expertise in threat modeling, Quantum computing and predictive threat intelligence. Taking some lessons from cloud, make sure your third-party Quantum provider has the right Security controls to protect your organization’s Quantum environment, confidentiality, integrity and availability.
The selected company should also harden computing environments and provide federated access controls to minimize the attack surface.

Cloud-based Quantum resources will also have a new architectural element—known as transpilers—that take your company’s code and translate the instructions into microwave signals. Your vendor/partner should be able to offer transparency around the translated instruction set, to ensure that the transpiler is functioning properly and has not been corrupted.

Like 5G, hardware for Quantum-proof encryption could require new lattice-optimized chips and Security modules [e.g., application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs)]. As companies move to Quantum-proof encryption, it is important to source hardware from trusted vendors that are part of the broader ecosystem-led innovation strategy. Geopolitical issues, access to earth metals, competition for talent and intellectual property espionage in Quantum can also factor into these investments.

In terms of Quantum processing, your company should also start preparing now for post-Quantum cryptography (PQC), as scientific improvements are happening more rapidly. Case in point: In late 2019, MIT reported that researchers had found a way to use a Quantum computer with only 20 million physical qubits—not the billion qubits previously thought to be needed—to break 2048-bit RSA integers in just eight hours. Advancements like this accelerate Accenture’s predicted timeline for the inflection point of Quantum to be even sooner than 2025, meaning that companies must work toward achieving Quantum-proof cryptography faster than we previously recommended. Waiting for the final algorithm selection from NIST (expected by 2024) to start planning will likely leave your company exposed.

As for data, strategic choices on what data needs Quantum protection, and which kind of Quantum key distribution (QKD)/Quantum key generation (QKG) technologies to use for future proofing the business against these risks, may have unforeseen consequences. Almost all the PQC algorithms available still rely on flawed pseudo-random number generation (PRNG). This could be an Achilles’ heel for these algorithms, making them vulnerable to lattice-reduction attacks and symmetric key protection vulnerabilities. The best strategy is to adopt new algorithms and standards with agility, such as ISARA or InfoSec Global.

Finally, as your company begins to integrate blockchain and digital ledger technologies (DLT) into the business, the DLT-based services and business processes designed with public/private key infrastructure and legacy hashing algorithms will be at risk to Quantum computers. This is because Quantum is expected to be powerful enough to break and decode the cryptography that supports identification, authorization and encryption services. To prevent this, you will need to re-architect the cryptographic structure of the blockchain to be Quantum resistant against Shor’s and Grover’s Quantum algorithms, as covered by Accenture in-depth in our report, Cryptography in a Post-Quantum World.
When looking at the overall survey feedback from CISOs, we had an interesting finding: Security leaders generally have a rosier perception of their involvement in innovation initiatives than their Business counterparts (see Figure 9, left-hand chart). This gap is further exaggerated once we look at the alpha innovators and followers (see Figure 9, right-hand chart).

Behaviorally, this shows that there may be innovation initiatives in the Business where Security is not yet engaged or the CISO is not yet aware that the initiative is happening. Clearly, there is more work to be done—even at the alpha innovator level—to solidify collaboration across the enterprise, in order to maximize continuous innovation opportunities and increase growth potential.

**Borderless Collaboration:**
Work across all aspects of the enterprise for agility

Figure 9: Collaboration between Business and Security executives is essential for continuous innovation, with the alpha innovators being much more likely to include the CISO from initiative kickoff through completion.

| CISOs included in discussions of emerging technology adoptions (CXOs and CISOs; n=500) |
|---------------------------------|-------------|
| **Always include CISO**         |
| Alpha Innovators                | Followers   |
| CISOs                           | CXOs        |
| 66%                             | 55%         |
| 60%                             | 37%         |
In a separate behavioral result, as shown in Figure 10, Security leaders at alpha innovators are connecting with the Business to do two things simultaneously: to help adopt emerging technologies while aggressively managing risk at the same time. In other words, CISOs are earning their place in innovation discussions by being responsive and agile. They do not put up roadblocks to adoption; instead they are meeting the Business where it is, evolving their Security capability at the same time (59 percent) instead of delaying (18 percent) or preventing (23 percent) adoption. These CISOs work with the Business to enable innovation business outcomes.

This demonstrates not only the growing importance of the CISO role to the success of the innovation agenda, but also the increasing agility that Security must demonstrate. Not surprisingly, CISOs at the alpha innovators believe they have significant influence (91 percent alpha innovators; 78 percent followers) and help the enterprise move ahead with technology implementations confidently, de-risking along the way and adding Security skills to fill the gaps.

Alpha innovators commit to emerging technologies by creating a solid connection between the Business and Security sides. They are also much more likely to have CISOs integral to this process and collaborating in innovation discussions from the start.

While it is difficult to attribute cause, alpha innovators are behaving with more operational maturity, suggesting they may have found a better way to institutionalize innovation and govern their implementation and Security approach.

Figure 10: Collaboration requires agility. Rather than being a roadblock, alpha innovator CISOs evolve their Security capabilities rapidly to support the emerging technology adoption process.

### How security risk factors into the organization’s decision of whether and when to adopt an emerging technology (CISOs; n=250)

<table>
<thead>
<tr>
<th>Decision</th>
<th>Alpha Innovators</th>
<th>Followers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay adoption in favor of ensuring we can secure an emerging technology</td>
<td>18%</td>
<td>27%</td>
</tr>
<tr>
<td>Prevent adoption if the security risks prove too great</td>
<td>23%</td>
<td>30%</td>
</tr>
<tr>
<td>Adopt while evolving our capability to secure an emerging technology</td>
<td>59%</td>
<td>42%</td>
</tr>
</tbody>
</table>

### Influence CISOs have on the way emerging technologies are adopted in their organization (CISOs; n=250)

<table>
<thead>
<tr>
<th>Influence</th>
<th>Alpha Innovators</th>
<th>Followers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant influence</td>
<td>91%</td>
<td>78%</td>
</tr>
</tbody>
</table>
Continuous innovation requires the right environment to flourish. Data from the alpha innovators shows that they are building a culture of innovation both internally through strategy and workforce skill-building, as well as externally through ecosystem partnerships and acquisitions for Security capability.

CISOs at the alpha innovator organizations realize that the skill sets to secure these technologies will change significantly, and they are committed to addressing this Security skills gap through training initiatives, strategic partnerships with third-party companies across the ecosystem and hiring new talent (see Figure 11). However, Security talent is at a premium in the marketplace and Security-focused training for these technologies is limited. Alpha innovator CISOs recognize they cannot do everything themselves: as part of a broader ecosystem-led innovation approach, they are much more likely to collaborate and integrate with proven third parties that have demonstrated Security expertise.

Figure 11: Alpha innovators are taking several approaches to accessing the requisite Security talent, including external partnerships.

<table>
<thead>
<tr>
<th>Organization plans to secure the expertise to support emerging technologies (Multiple responses) (CXOs and CISOs; n=500)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Train existing employees</td>
</tr>
<tr>
<td>Collaborate/partner with organizations that have the expertise</td>
</tr>
<tr>
<td>Hire new talent</td>
</tr>
<tr>
<td>Acquire new businesses/start-ups</td>
</tr>
</tbody>
</table>
Finally, Figure 12 highlights the equal commitment the Business and Security sides of the alpha innovators have to a culture of innovation. When the historic norm for Business and Security to operate with independent agendas, alpha innovators are different.

They not only align more internal resources to emerging technologies, but also move quickly and respond together to defend and operationalize the implemented technologies. This shows the shared commitment alpha innovator CXOs and CISOs have to achieving growth on the innovation journey.

Figure 12: Alpha innovators demonstrate a shared commitment to a culture of innovation by dedicating more resources to emerging technologies and working together at the same speed and agility.

**Percentage of technology team dedicated to emerging technologies and dedicated/assigned to security and risk**
(CISOs; n=500)

- 1% – 20%: 20% (Followers), 27% (Alpha Innovators)
- 21% – 40%: 25% (Followers), 53% (Alpha Innovators)
- > 40%: 49% (Followers), 27% (Alpha Innovators)

**Percentage of security program focused on emerging technologies (in terms of % of Full Time Employees)**
(CISOs; n=500)

- 1% – 20%: 32% (Followers), 21% (Alpha Innovators)
- 21% – 40%: 30% (Followers), 32% (Alpha Innovators)
- > 40%: 47% (Followers), 38% (Alpha Innovators)
Defense in Depth: Apply range of protective and detective security controls for emerging technologies

Overall, the alpha innovators display the operational maturity through their institutionalized approach to Security governance, controls and data protections to ensure the high bar of continuous innovation.

In other words, they are applying and often developing new controls to create defense in depth around emerging technology implementations at speed and scale.

As many of these emerging technologies are cloud enabled and leveraged as a service, strong cloud security measures are the launch point for the adoption of AI, Quantum and XR services. The many layers of defense in depth required for secure cloud adoption are essential, but quickly followed by bespoke requirements to protect the emerging technology throughout the development and production lifecycle (as highlighted in the four technology sidebars in this report). Inadequate protection throughout the development of new services and offerings with the emerging technology could leave the innovation and the investment exposed to corporate or national espionage or theft. Alpha innovators recognize the need to provide this defense in depth throughout the lifecycle.

With AI, for example, our data shows the alpha innovators, in particular, are using many different controls to secure AI-enabled processes (see Figure 13). Network Security measures top the list at 71 percent; followed by application Security measures at 70 percent; and data validation and sanitization for data fed into models for insights (67 percent).

It is important to note, however, that the threats against AI are advancing rapidly. Thus, we advocate that all companies—both alpha innovators and followers—should expand their methods of protection even further.
This includes securing ecosystem partners that understand how to defend the wider attack surface that AI presents.

Another emerging technology area that has been somewhat overlooked when it comes to Security is XR6, which presents risks relative to cloud, AI and related processes for both enterprise-grade and consumer-facing solutions. Business and Security executives who proactively expand their knowledge of this area will be much better prepared to make fast moves, especially as remote workforce and geographical collaboration needs multiply.

Figure 13: CISOs at alpha innovators are using a variety of measures to protect AI-enabled processes.

<table>
<thead>
<tr>
<th>Measures used to protect Artificial Intelligence enabled processes in the business (CXOs and CISOs, n=500)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network security measures</td>
</tr>
<tr>
<td>Applications security measures</td>
</tr>
<tr>
<td>Data validation and sanitization for data fed into a model (for insights)</td>
</tr>
<tr>
<td>Data validation for training data</td>
</tr>
<tr>
<td>Access control measures for AI models</td>
</tr>
<tr>
<td>Access control measures for training data</td>
</tr>
<tr>
<td>Our AI cloud provider (third party) provides our security</td>
</tr>
</tbody>
</table>

66% 73%
64% 72%
69% 68%
63% 63%
55% 61%
50% 50%
46% 45%

Alpha Innovators
Followers
Importance of securing XR

Extended Reality (XR) refers to the spectrum of experiences that blur the line between the real world and the simulated world, with the two major types being virtual reality and augmented reality.

XR has tremendous potential to deliver information anytime and anywhere in an immersive way through visuals, audio and even olfactory and haptic cues. In enterprise settings, it is used primarily to increase productivity by enabling people to participate in collaborative seminars, meetings, public lectures, professional training, self-guided maintenance, engineering work in the field or for guiding a remote assistant.
Whether your company is going to adopt enterprise or consumer XR solutions, it is important to understand the XR modalities and associated cyber risks. In order of priority, the four missions of an XR system are to:

- **Accurately position the human helmet or manipulated beacons in the six “degrees of freedom” of the space.** This determines where the object is in three-dimensional (3D) space and what direction the object is facing based on local 3D coordinates. Having spatially accurate positioning is key for all XR experiences.

- **Anchor digital objects on the environment space.** In VR, the space is digitized and in AR the space is a see-through camera or lens—and again accurate positioning is critical.

- **Gesture understanding and interaction with the object,** such as pointing a finger at a real or synthetic object.

- **Recognizing the observed information in order to interact with the detected object;** for example, asking “what is this” while pointing to something and having the system recognize the object and answer.

Each XR mode presents related vulnerabilities, especially when the XR content is transferred over the cloud and the AI recognition capabilities are on the cloud-as-a-service as well. These issues include:

- **Location:** tricking the location and positioning system will generate a bias in understanding what is being interacted with and can generate wrongful activation of system. By design XR devices must constantly map the environments in which they operate, so it is necessary to secure stored personal location information.

- **Content masking:** the command “open this valve” may be directed to the wrong object and generate a catastrophic activation. Projected objects and content tampering, where the system transfers data that all is fine, may drive the user to wrongfully activate a certain valve or give a command that interferes with the real system command.

- **AI-trusted recognition:** as the images are transferred to a cloud service for object, voice or gestures recognition, the data can be injected with synthetic information and confuse the response of the AI cloud services.

- **Content of images and environmental sound:** these are a pipe for data leakages, privacy and intellectual property. As the XR system streams video, the stream may be exposed to hackers who can view the entire content. Plus, the video streams and images are stored in cloud repositories, raising questions about location, compliance and regulation constraints.
Since XR is a cloud-supported infrastructure, many of the same multi-tenant and shared environment Security issues will be familiar to companies already managing Security for their cloud environments. Initially, your company will need to implement Security controls for verifying the identity of XR users (who the person is, what kind of XR device is being used and what type of XR service is being accessed via the network), while also developing capabilities for monitoring, detecting and responding to XR-related cyberattacks.

It is also important to assess an XR service provider’s or vendor’s native Security capabilities and privacy controls for providing XR experiences. For example, since XR headsets feature a variety of cameras, people will expect that gathered information is used purely to drive the experience, not track physical motions throughout the day or deny privacy through a first-person view of events. Companies should also be prepared to build supplemental protection on the enterprise side to secure the XR application and associated data and to manage users’ personal data for GDPR compliance, data collection and data usage rights.

Finally, there are Security issues that can lead to liability. For instance, although an AR experience may be designed to guide workers through efficient training, maintenance, assembly, or command and control, the operating system on the devices—like any internet of things (IoT) device or industrial control system—can be compromised and become an entry point to the company network.

Impersonation scams are also as valid in AR and VR systems as they are on web systems. Manipulating the sensors on XR devices for mis-readings could result in negative situations or safety issues, including altering the digital experience or providing uncalibrated information to workers. For example, tampering with the digital side of AR devices, content and recommendations could cause people to perform wrong actions on the physical world (i.e., a hacker inserts incorrect steps into a maintenance procedure, which could later cause a machine to fail). Likewise, in a VR system, human actions performed in real space can be controlled by hackers in virtual space; thus it is imperative to secure the human-environment connection similar to how Security is applied in the automotive industry or robotics.
Recommendations to align power plays

Innovating securely for competitive differentiation is no small feat, especially at the speed and scale of the alpha innovators. Accenture recognizes that your pursuit of the innovation journey and power plays are unique, and each CISO and CXO will need to overcome challenges specific to their company, industry, organizational structure and culture. Nonetheless, given the imperative for growth and demand for innovative solutions, the journey must begin now.
Here are practical steps for CISOs and CXOs to get started and help become successful innovators in partnership:

**CXOs, create an emerging technologies investment plan that ensures Security throughout the lifecycle**

If your company is not already investing US $500 million or more in emerging technologies, how can you possibly get there?

- Start by engaging with a strategic partner that has the insights of a technology vision for the future, an understanding of how emerging tech trends will impact enterprises and the Security capability to deliver.
- Work with a partner that also has a dedicated innovation team to help you identify your unique Innovation DNA to achieve secure growth.
- Develop a strategy to invest in technology innovations that will drive substantial value to the core of the business, not on tangential projects with unclear business impact. Identify innovations that can be applied immediately to generate cost savings, freeing up more budget for emerging technologies investment.
- Most importantly, select a proven partner with expertise in cloud, emerging technology and Security. This trifecta will enable your company to deliver new tech-fueled products and services with built-in privacy, risk management and trust, so you are not wasting your innovation time and money.

**CISOs, take the lead on collaboration to improve company wide understanding of risks**

Does your company work in siloes to achieve growth goals or as “one organization”? Does your company underestimate what it takes to secure investments in emerging technologies and realize expected value?

- Expand your Security agenda to enabling the Business to achieve growth goals securely. Commit to shared success with the Business to earn an active role in the innovation journey.
- Kick-start internal collaboration by reaching across the table to C-suite Business leaders. Make your key performance indicators measure the performance relative to business outcomes. Demonstrate value by showing how Security has accelerated time to market, improved quality, differentiated capability or increased maturity.
- Educate your partners on the threat landscape around innovation and the business. Prepare a threat report or analysis of the enterprise’s strategic initiatives related to emerging technologies. Present risk management strategies that will help mitigate the issues while evolving Security capabilities to match the speed and scale of the change.
- Conduct Security diagnostics to assess the enterprise risks for each emerging technology implementation that is planned or already in motion. Share your knowledge broadly to help Business leaders better understand Security risks.
CISOs and CXOs, refine ecosystem partnerships and commit to skills building

Do you have the strategic relationships and skillsets readily available to manage and secure the emerging technologies?

- Build a partnership evaluation model and examine the range of your ecosystem partnerships across industry, universities, consulting, flexible manufacturing and others. Clarify how and where each brings value.
- Determine which strategic provider(s) has the Security acumen and resources ready and able to supplement your team at scale.
- Assess gaps, investigate alternative companies and confirm which partners will best support your innovation agenda with built-in Security. Share your learnings with partners to align incentives.
- Lead by example and improve your knowledge about managing and securing emerging technology like AI and Quantum through online classes or learning experiences. Invest in expanding this learning framework across your Security team to help upskill employees.

CISOs and CXOs, reassess Security approaches and apply new models to protect upcoming products and services

If your company needs to strengthen Security maturity in one or several areas, where do you begin?

- Take a fresh look at your Security models for the journey to cloud, including how you protect expanding needs for data, internet of things and ecosystem partnerships.
- Increase security risk assessments for innovation adoption and embed Security into the development life cycle through DevSecOps for your company’s integration of AI, 5G, Quantum and XR.
- Invest in the necessary Security tools and dedicate the appropriate number of employees to secure networks, applications, data and access control for emerging technologies.
- Build trust into each product or service using models that protect customers’ data and privacy.
Conclusion

Leaders that take these steps will help Security and Business to work together, building the multi-pronged strategy, risk mindset, borderless collaboration, culture of innovation and defense in depth that support an engine for continuous innovation and a unique Innovation DNA. Do not underestimate what it will take to secure this future. Act accordingly to demonstrate agility: assess early, invest in resources, adopt new Security approaches and de-risk emerging technology adoption on all fronts.

These bold actions and ongoing commitments will help you protect your company’s innovation investments, enabling it to achieve the top-line revenues, cost savings, market capture and new services so necessary for growth.

Empower your company to do innovation securely at speed and scale and join the alpha innovators leading the way.
Survey Methodology

Accenture surveyed 500 respondents from November to December 2019 in 12 industries and eight countries.

A subset of respondent companies was selected based on their avid investment in the four technologies; the criteria was to be investing in at least three of the technologies. This “elite subgroup” represents 28 percent of the total sample, aka the innovation “alpha innovators.”

Title

<table>
<thead>
<tr>
<th>Title Group</th>
<th>Industry</th>
<th>Location &amp; Headquarters</th>
<th>Emerging Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>78 Chief Information Officer (CIO)</td>
<td>40 Automotive</td>
<td>84 Australia</td>
<td>374 I am the decision maker/key advisor in selecting and introducing of emerging technologies in to the business</td>
</tr>
<tr>
<td>19 Chief Innovation Officer</td>
<td>39 Banking</td>
<td>39 Italy</td>
<td>102 I am an advisor to others in selecting and introducing of emerging technologies into the business</td>
</tr>
<tr>
<td>24 Chief Strategy Officer</td>
<td>40 Chemicals</td>
<td>40 Singapore</td>
<td>23 I provide input into the selection and introduction of emerging technologies into the business</td>
</tr>
<tr>
<td>79 Chief Risk Officer (CRO)</td>
<td>50 Communications</td>
<td>17 South Korea</td>
<td>1 I am not involved in the selection or introduction of emerging technologies into the business</td>
</tr>
<tr>
<td>77 Chief Technology Officer (CTO)</td>
<td>46 Energy (Oil &amp; Gas)</td>
<td>46 Spain</td>
<td></td>
</tr>
<tr>
<td>16 Chief (Cyber) Security Officer</td>
<td>50 Healthcare (provider)</td>
<td>3 Switzerland</td>
<td></td>
</tr>
<tr>
<td>155 Chief Information Security Officer (CISO)</td>
<td>50 High Tech</td>
<td>78 United kingdom</td>
<td></td>
</tr>
<tr>
<td>52 Business Unit/ Line of Business Lead</td>
<td>30 Life Sciences (Pharma &amp; Biotech)</td>
<td>193 United States</td>
<td></td>
</tr>
</tbody>
</table>

Revenue

<table>
<thead>
<tr>
<th>Revenue</th>
<th>Title Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5 – 9.9 billion</td>
<td>250 CISO/CSO/CRO</td>
</tr>
<tr>
<td>$10 – $19.9 billion</td>
<td>182 Others</td>
</tr>
<tr>
<td>$20 – 29.9 billion</td>
<td>55 Others</td>
</tr>
<tr>
<td>$30 billion or more</td>
<td>13 Others</td>
</tr>
</tbody>
</table>
The survey was conducted online among a panel of executives.

250
Chief Risk Officer (CRO)
Chief (Cyber) Security Officer
Chief Information Security Officer (CISO) (or equivalent)

250
Chief Information Officer (CIO)
Chief Innovation Officer
Chief Strategy Officer
Chief Technology Officer (CTO)
Business Unit/Line of Business Lead [30 percent max]
References

1 Accenture Technology Vision 2020 survey

2 Innovation DNA is one of five tech trends covered in Accenture Technology Vision 2020, “We, the Post-Digital People: Can your enterprise survive the tech-clash?” Our Innovation DNA trend covers ways businesses can transform how they innovate by focusing on three key building blocks of their company’s innovation DNA: 1) maturing digital technologies, 2) scientific advancements and 3) emerging DARQ technologies. Leaders are weaving these technological building blocks together—with embedded Security—to set a course for their company’s future.

3 https://towardsdatascience.com/how-to-attack-machine-learning-evasion-poisoning-inferencetrojans-backdoors-a7cb5832595c

4 https://www.infoq.com/articles/privacy-attacks-machine-learning-models


Contacts

Lisa O’Connor
Managing Director
Cybersecurity R&D
Accenture Labs
lisa.oconnor@accenture.com

Marc Carrel-Billiard
Senior Managing Director
Technology Innovation Lead
marc.carrel-billiard@accenture.com

Kelly Bissell
Senior Managing Director
Global Lead
Accenture Security
kelly.bissell@accenture.com

Ethan Hadar
Chief Research Officer
Accenture Labs
Europe
ethan.hadar@accenture.com

Lynn LaFiandra
Senior Principal
Accenture Research
lynn.c.lafiandra@accenture.com

Contributors

Malek Ben Salem
Amin Hassanzadeh
Louis DiValentin
Lei Ding
Benjamin McCarty

Ryan LaSalle
Rex Thexton
Neha Joshi
Stirling Goetz
Jacky Fox

Michael Biltz
Ari Bernstein
Mary Hamilton
Matthew Short
About Accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialised capabilities across more than 40 industries—powered by the world’s largest network of Advanced Technology and Intelligent Operations centres. With 513,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at www.accenture.com

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on Twitter @AccentureSecure or visit us at www.accenture.com/security

About Accenture Labs

Accenture Labs incubates and prototypes new concepts through applied R&D projects that are expected to have a significant impact on business and society. Our dedicated team of technologists and researchers work with leaders across the company and external partners to imagine and invent the future.

Accenture Labs is located in seven key research hubs around the world: San Francisco, CA; Sophia Antipolis, France; Washington, D.C.; Shenzhen, China; Bangalore, India; Herzliya, Israel and Dublin, Ireland; and Nano Labs across the globe. The Labs collaborates extensively with Accenture’s network of nearly 400 innovation centers, studios and centers of excellence located in 92 cities and 35 countries globally to deliver cutting edge research, insights and solutions to clients where they operate and live. For more information, please visit www.accenture.com/labs