The journey to digital trust

Digital businesses that lead in safety, security, reliability, privacy and data ethics will be the titans of tomorrow. It is a journey worth taking.

Fall 2018

pwc.at/digital-trust-insights

Introducing Digital Trust Insights

For 20 years, leaders have turned to PwC's Global State of Information Security® Survey (GSISS) as a trusted resource to navigate the cyber risk landscape. Over time, that landscape has evolved to be less about "information security" and more about managing digital risk. As cybersecurity, privacy and data ethics become increasingly intertwined, organizations need a central place to turn for authoritative data and actionable advice. That is why we are rebooting GSISS to create Digital Trust Insights. This new platform will explore how to build confidence in the readiness of people, processes and technologies to meet tomorrow's challenges.

If the lifeblood of the digital economy is data, its heart is digital trust—the level of confidence in people, processes, and technology to build a secure digital world. Companies, regulators, and consumers need new mechanisms to build that confidence as they address emerging challenges in business, risk management, and compliance. It's telling that the United Nations is convening a forum on the internet's role in widening distrust among people.[1] An essay in *The Economist* predicted 2018 "will be remembered as the year that privacy law finally started catching up to the Internet."[2] Imagine what it would mean for businesses to begin a new legacy of building digital trust in 2019. At PwC, we believe next year will be pivotal as organizations start laying that foundation. Companies that show the connected world how to lead in safety, security, reliability, privacy, and data ethics will be the titans of tomorrow. It is a journey worth taking.

Our inaugural PwC Digital Trust Insights survey asked 3,000 business leaders worldwide about the readiness of their organizations to address digital business, risk management and compliance challenges. We have identified 10 major opportunities for improvement around people, processes and technology. These are based on survey findings from companies of all sizes worldwide, as well as medium and large businesses in key sectors such as financial services; healthcare; industrial products; consumer products; technology, media, and telecommunications (TMT); and energy, mining, and utilities. We have also included actionable advice to help business leaders seize the opportunities in ways that could help redefine their business.

1. United Nations, Cybersecurity and Fake News to Dominate List of Concerns at Internet Governance Forum, October 2018.
2. The Economist, Toward defining privacy expectations in an age of oversharing, Aug. 16, 2018.

People

Tomorrow's transformation starts with people

1. Engage security experts at the start of digital transformations

Companies everywhere are pursuing digital transformation projects—putting emerging technology into action while aiming to solve problems, create unique experiences, and accelerate business performance.[3] It's no secret that sprawling connectivity among personal devices, governments, businesses, and industrial equipment is fueling exponential growth in cyber and privacy risks.[4] Nine in ten of our survey respondents at companies executing digital transformation projects say they include security and privacy personnel as stakeholders and proactively manage cyber and privacy risks by design in the project plan and budget. But only 53% say that proactive risk management measures are baked into the project "fully from the start."[5] That percentage is relatively higher in the financial services, health, and TMT sectors and relatively lower in consumer markets, among respondents from medium and large companies. But there is no monopoly here on the opportunity for improvement. Businesses worldwide can do better.

91%
of enterprise-wide digital transformation include security and/or privacy personnel as stakeholders
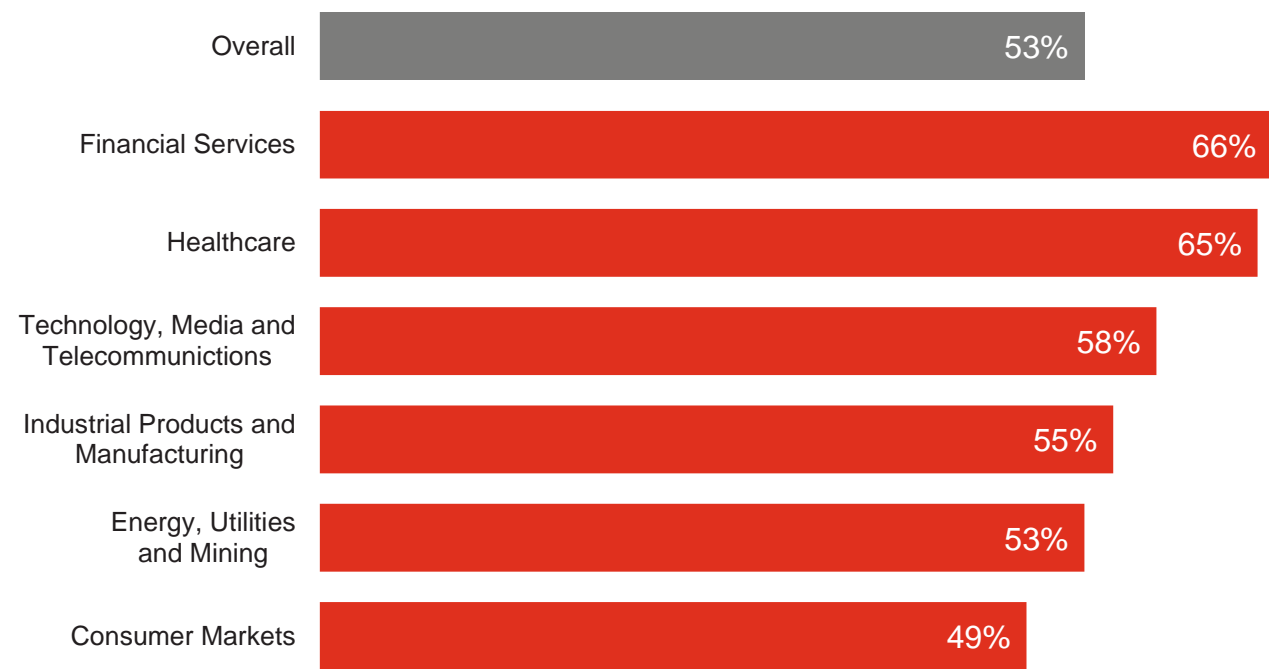
53%
include proactive management of cyber and privacy risks by design in the project plan and budget "fully from the start"

Source: Fall 2018 Digital Trust Insights, PwC
Base: 3,000 respondents

---

3. More than half of respondents (55%) say their company is engaged in an enterprise-wide digital transformation project. The projects are even more prevalent at companies valued at $100 million or more in key sectors such as technology, media and telecommunications (86%) and financial services (81%).

4. European Political Strategy Centre, State of the Union 2018: Our Destiny in Our Hands, Sept. 13, 2018.

5. The figure a bit lower for small business (48%) and medium-sized businesses (also 48%) and a bit higher for large businesses (63%).

The percentage of medium and large firms asserting risks are managed 'fully from the start' varies by sector

Sector	Percentage
Overall	53%
Financial Services	66%
Healthcare	65%
Technology, Media and Telecommunictions	58%
Industrial Products and Manufacturing	55%
Energy, Utilities and Mining	53%
Consumer Markets	49%

q1060: Earlier you said that your company is currently involved in an enterprise-wide digital transformation project. To what extent is proactive management of cyber and privacy risks included by design in the project plan?

Source: Fall 2018 Digital Trust Insights, PwC
Base: 3,000 respondents

Actionable advice for business leaders

- Include cybersecurity and privacy personnel in digital transformation projects from day one—and evaluate whether they have the right skills aligned to design, build, and sustain digital transformation initiatives, or if external resources are needed.

- Network with industry peers who have gone through similar transformation projects to learn lessons, including which skills their peers placed for successful completion.

- Connect with stakeholders from leading technology firms to learn from their transformation endeavors.
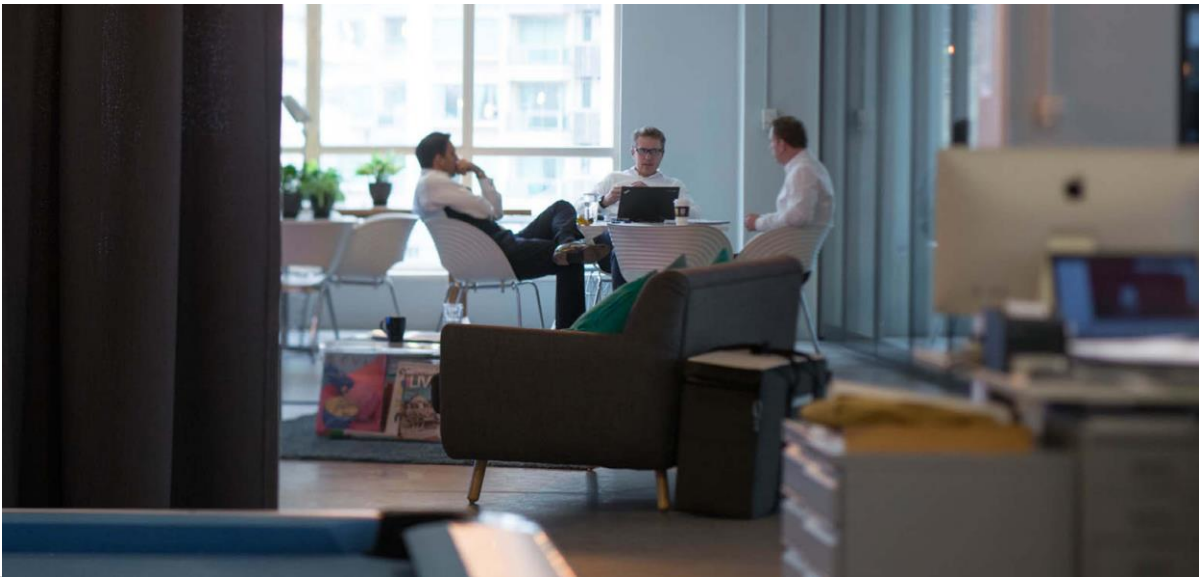
2. Upgrade your talent and leadership team

Without the right team in place, managing risks around security, privacy and ethics becomes a much steeper climb. Key roles such as chief information security officer, chief security officer, chief privacy officer, chief risk officer and chief data officer are often absent at many companies, according to our findings.

Less than half of respondents are very comfortable their company has adequately identified the executives responsible for cybersecurity (39%) and privacy (40%). About the same percentage (38%) are very comfortable with the sufficiency of their cybersecurity and privacy workforce. Only a third say their organizational structure and workforce is fully ready to meet recent and emerging requirements for cybersecurity, data privacy, and data-use governance.

Actionable advice for business leaders

- Commit to putting the right roles and talent in place, with clearly defined responsibilities, to comprehensively address cybersecurity, privacy and data ethics challenges.
- Conduct an organizational risk assessment to identify and address talent and skill gaps.

3. Raise workforce awareness and accountability

Many businesses could do more to raise employee awareness and accountability around cybersecurity and privacy. Only 34% of respondents say their company has an employee security awareness training program. Only 31% say their company requires employee training on privacy policy and practices.

### Actionable advice for business leaders

- Prioritize raising workforce awareness about cybersecurity and privacy to support business objectives. Use messaging that avoids invoking security fatigue and is memorable enough to influence behavior when busy employees later face phishing schemes and other sophisticated threats.
- Establish corporate policies governing access to IT assets and data. Enforce the policies at all levels of the company to drive accountability for cybersecurity and privacy.

Process

Evolving processes into new trust mechanisms

## 4. Improve communications and engagement with the board of directors

Most respondents responsible for communicating with the board on cyber and privacy risks say that their company has provided the board with strategies for cybersecurity 80%) and privacy (83%), Many of these same businesses, however, may have doubts or concerns around their internal reporting on cybersecurity and privacy metrics. Only 27% of respondents say they are very comfortable that the board is receiving adequate reporting on metrics for cyber and privacy risk management.[6]

80%
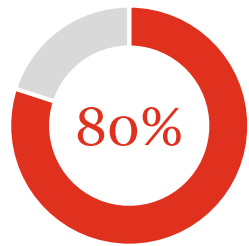
say the board has been provided a cyber risk management strategy

83%
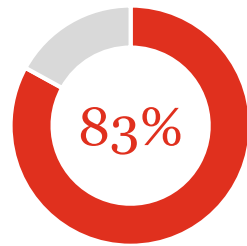
say the board has been provided a privacy risk management strategy

27%
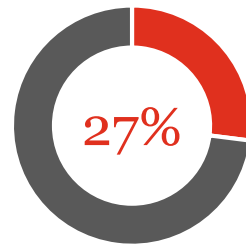
say they are "very comfortable" the board is getting adequate reporting on metrics on cyber and privacy risk management

Source: Fall 2018 Digital Trust Insights, PwC
Base: 3,000 respondents

Actionable advice for business leaders

• Know that the types of measures (implementation, effectiveness/efficiency, and impact) that are obtainable and useful for performance improvement depend on the maturity of the security program and how controls are being implemented.[7] Start with what you can measure today and create a plan to add more sophisticated metrics over time. Also, metrics must address the needs of the stakeholder audience. The board might want metrics on the business impact of security activities—for example, impact of security spending on overall risk posture, cost of addressing a security event, or impact of security efforts on public trust.

• Communicate to the board how external factors—threats, third-party risk and regulations—affect overall risk posture and effectiveness of risk reduction activities.

• Improve the CISO's engagement with board members using these five tips.

6. Also 27% say they are somewhat comfortable, 17% neutral, and 29% uncomfortable to some degree.

7. For additional information, see National Institute of Standards and Technology, Special Publication 800-55 – Performance Measurement Guide for Information Security, July 2008.

5. Tie security to business goals

As corporate leaders aggressively adopt technology-driven business models, cybersecurity programs are increasingly misaligned with the business. Only 23% say they plan to invest over the next year in aligning business objectives with information security strategy.[8]

Actionable advice for business leaders

Companies can make progress by focusing on areas such as the following:

- Embedding cybersecurity into new products and/or services

- Conducting risk, regulatory and compliance assessments

- Conducting cybersecurity framework assessments that align business imperatives to cybersecurity controls

- Refreshing cybersecurity strategies and plans

6. Build lasting trust around data

As the amount of data in the world soars, more companies could be at risk of crossing ethical red lines as they pursue new ways to monetize it. Among businesses worth $100 million or more, only about half say they are making large investments in data governance, in creating transparency in the use and storage of data and toward increasing the control individuals have over their data. And many medium and large businesses in key sectors are not "very comfortable" they have identified their most valuable and sensitive digital assets.[9] Not surprisingly, the percentage of respondents who are very comfortable they have identified such assets (40%) is close to the share who say their company has a program for doing so (43%).

Actionable advice for business leaders

- Implement data-governance programs that determine not only where sensitive data lives, but also the value to the business and how to protect it.

- Manage risks for the whole data lifecycle, including creation, storage, using, sharing, archiving, and destruction.

---

8. Among medium and large businesses in key industries, the statistic is a bit higher in sectors such as TMT (37%) and industrial products (32%).

9. Depending on the sector, it might be half or less that feel that confident. In addition, a sizeable number say they are "moderately comfortable."

7. Boost cyber resilience

Cyber resilience includes the agility of both defense and recovery capabilities. Resilient systems help companies to sustain operations when possible amid cyberattacks, and to rapidly recover in the event of disruption. This is critical because the crippling or halting of operations can lead directly to financial losses that often exceed, and mount more quickly, than those from data exposure. And the importance of maintaining data integrity will only grow as companies make more data-driven decisions with the aid of artificial intelligence.[10]

Only about half of medium and large businesses in key sectors say they are building resilience to cyberattacks and other disruptive events to a large extent. And fewer than half of them say they are very comfortable their company has adequately tested its resistance to cyberattacks.

Actionable advice for business leaders

- Develop an understanding of the risk appetite around core business practices. Take into account the potentially differing views of stakeholders such as the chief financial officer, the chief operating officer, the chief information officer, and other executives focused on security, privacy, and risk.

- Use leading approaches to cyber resilience. They include the development and assessment of plans designed to address risk-appetite concerns in an evolving threat landscape. They also include the constant monitoring of technology infrastructure to enable high availability, disaster recovery, and data integrity.

---

10. Read the April 2018 Forrester report, The Future Of Cybersecurity And Privacy: Defeat The Data Economy's Demons, for more on this subject.
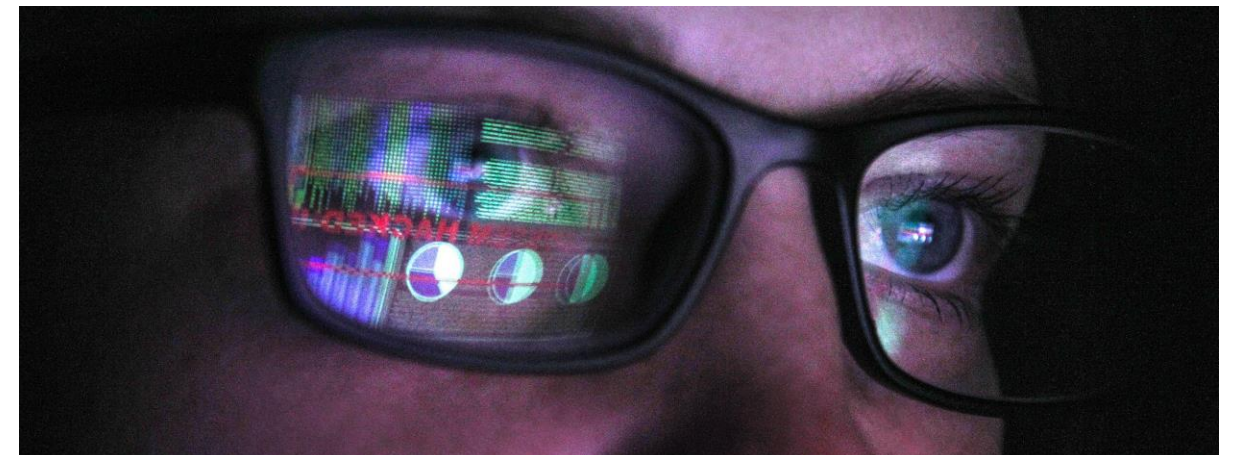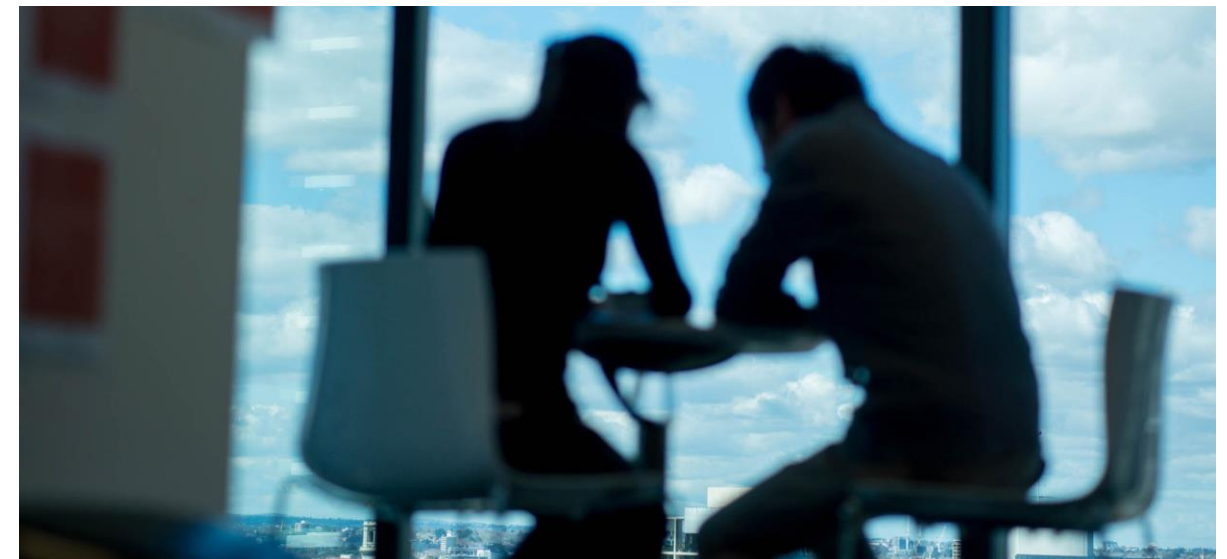
8. Know thy enemies

Cyber threat concerns vary by industry and company size. Over the last year, for instance, concerns about state-sponsored hackers increased most in financial services 33%), while anxiety about cybercriminals spiked in consumer markets (50%) and the biggest rise in unease about industrial espionage was in the TMT sector (51%), according to respondents from medium and large businesses. Only 31% of respondents worldwide, however, say they are very comfortable their company has identified those parties who might attack its digital assets.

Our findings also show relatively large companies are more concerned about insider threats than are small businesses. Among companies of all sizes, the net increase in concern around insider threats in consumer markets is merely 9%. But for medium and large companies in consumer markets, the statistic exceeds 30%. Concern about insider threats has grown more modestly among health-services respondents from the same size companies, however, despite Verizon's 2018 Data Breach Investigation Report finding about the health sector's insider-threat problem.[11]

Actionable advice for business leaders

- Use cyber threat intelligence and insider threat programs to inform security activities and risk assessments and support related investment decisions.

- Study your risk and threat landscape; apply threat intelligence to your risk scenarios; develop a threat-intelligence program and function; and use leading tools to make the intelligence actionable.

---

11. Verizon, 2018 Data Breach Investigation Report, 2018. The report states, "The Healthcare industry has the dubious distinction of being the only vertical that has a greater insider threat (when looking at breaches) than it does an external threat. This somewhat bleak finding is linked closely to the fact that there is a large amount of both errors and employee misuse in this vertical."

9. Be proactive in compliance

Respondents say the top digital compliance and ethics challenges worldwide include staying aware of the latest regulatory developments (41%); complying with current regulations (37%); and preparing for future regulations (34%). Brazil's data protection law is a recent example of new legislation. Perhaps the most well known example is the European Union's General Data Protection Regulation (GDPR), which went into effect in May 2018. Fewer than half of companies worth $100 million or more say they are fully ready to comply with GDPR.

Among US respondents, confidence about the readiness to comply with the California Consumer Privacy Act—which goes into effect in 2020—varies by sector: TMT companies are the most confident and health companies are the least confident. Three quarters of respondents in China say they are entirely ready to comply with China's cybersecurity law, but far fewer respondents in other countries assert the same.

Actionable advice for business leaders

- Focus more on identifying new and emerging legislation, rules and implementation guidance.

- Use an integrated compliance approach instead of siloed efforts. In other words, businesses operating across different jurisdictions should comply with the highest standard. The boundaries of such an approach should be the sum of all the rules.
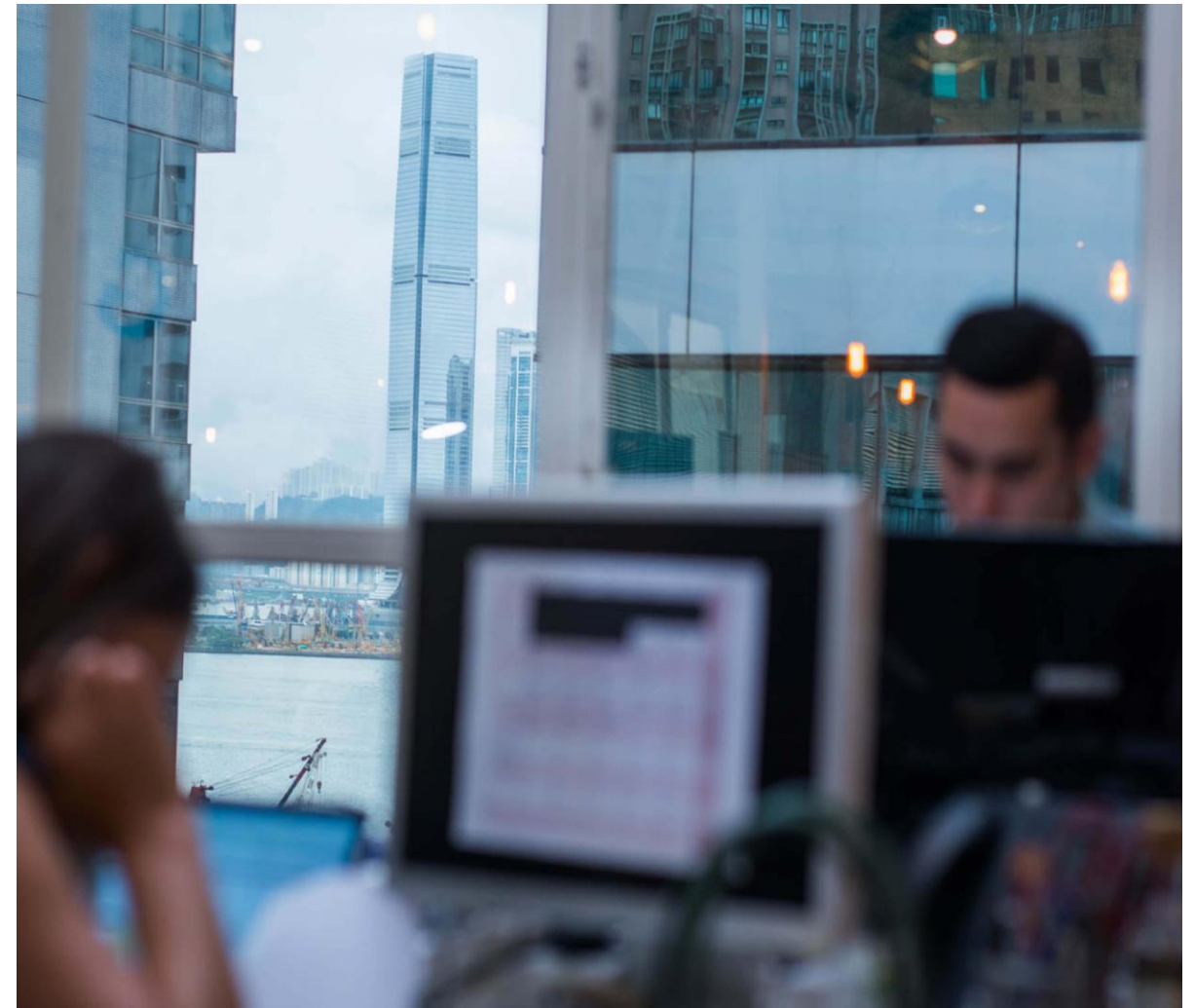
Technology

Accelerating controls for emerging technology

## 10. Keep pace with innovation

Explosive growth in technology and data over the next decade will obliterate barriers between cyber, physical, and virtual worlds, ratcheting up the complexity and scale of cyber and privacy risk management worldwide. Digital data and devices will be embedded more in critical infrastructure, in consumer products, in vehicles, in daily life, and even in humans, in "a world in which the physical, cyber and virtual merge."[12] Data collection will be more pervasive than ever as the internet of things (IoT)[13] spreads like ivy—and hackers will be drawn to its vines like birds to berries.

Not surprisingly, most respondents (81%) say IoT is critical to at least some of their business. Only 39%, however, say they are very confident they are
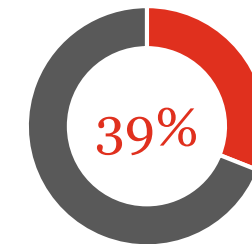
building sufficient "digital trust" controls— security, privacy and data ethics—into their adoption of IoT. (An additional 30% say they are "somewhat confident.")

In addition, only 30% list IoT security among the safeguards they plan to invest in this year.[14] IoT devices interact with the physical world in novel ways. These devices often cannot be accessed, managed or monitored like other information technology and they sometimes require additional cybersecurity and privacy controls.[15]
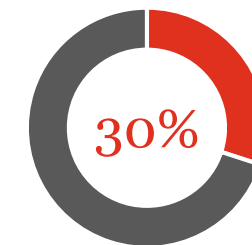
Survey respondents have even less confidence in the sufficiency of their digital trust controls for other emerging technologies such as artificial intelligence (AI).
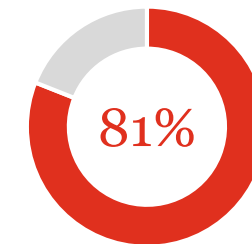
81% say IoT is "critical" to at least some of their business

39% are "very comfortable" they are building sufficient digital trust controls into adoption of IoT

30% say they plan to invest in IoT security over the next 12 months

---

12. US National Security Telecommunications Advisory Committee, Report to the President on Emerging Technologies Strategic Vision, July 14, 2017.
13. The internet of things (IoT) is a network of physical objects—devices, vehicles, appliances—embedded with sensors, software, network connectivity, and computing capability enabling them to collect, exchange, and act on data, usually without human intervention.
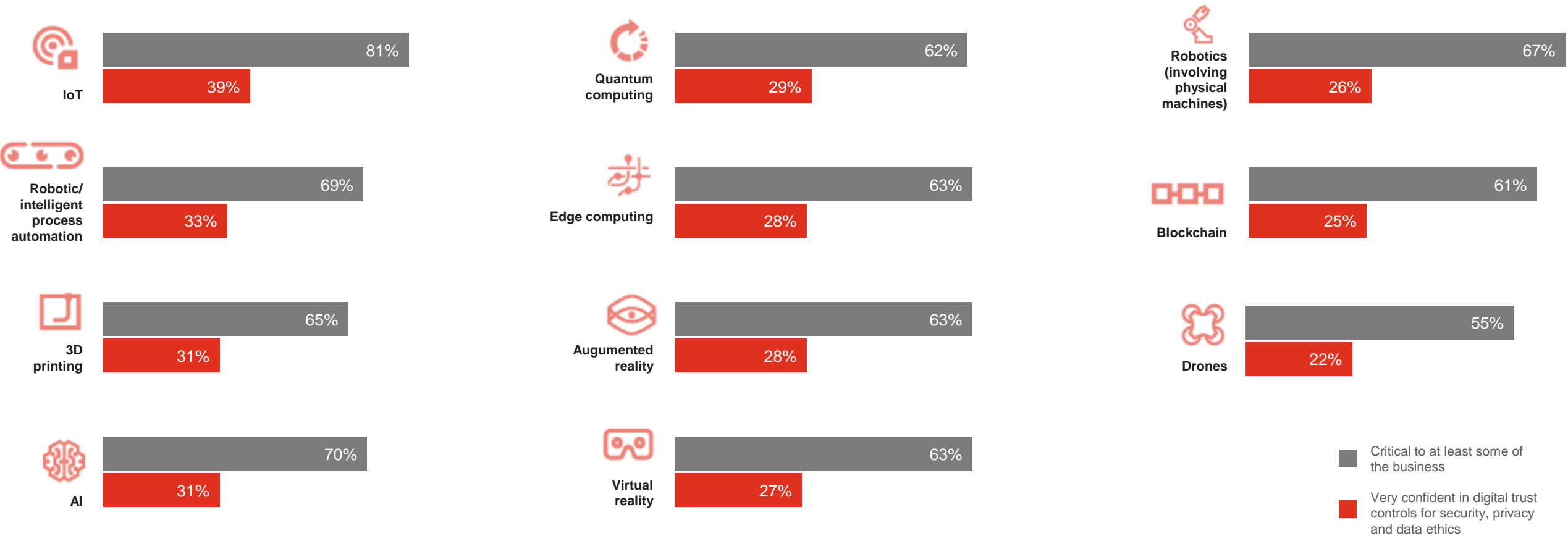14. Among medium and large businesses, IoT security is the top security investment priority cited by health and consumer markets respondents.
15. NIST, NISTIR 8228 (DRAFT): Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, September 2018.

Source: Fall 2018 Digital Trust Insights, PwC
Base: 3,000 respondents

Most respondents say emerging technologies are critical for business, but fewer are very confident they have sufficient 'digital trust' controls in place

IoT
- 81%
- 39%

Quantum computing
- 62%
- 29%

Robotics (involving physical machines)
- 67%
- 26%

Robotic/ intelligent process automation
- 69%
- 33%

Edge computing
- 63%
- 28%

Blockchain
- 61%
- 25%

3D printing
- 65%
- 31%

Augumented reality
- 63%
- 28%

Drones
- 55%
- 22%

AI
- 70%
- 31%

Virtual reality
- 63%
- 27%

Legend:
- Critical to at least some of the business
- Very confident in digital trust controls for security, privacy and data ethics

q1010: How important do you expect the following technologies to be to the future success of your business?
q1030: How confident are you that your business is building sufficient 'digital trust' controls into adoption of the following technologies?

Source: Fall 2018 Digital Trust Insights, PwC
Base: 3,000 respondents

Although 70% of respondents say AI is critical to at least some of their business, only 31% are very comfortable they are building sufficient digital trust controls into their adoption of AI. The most effective controls are built during the design and implementation phase.[16] The many possible uses of AI include early identification of potential pandemics, autonomous vehicles, and faster and more efficient cybersecurity.[17] Only 22% of all respondents say they plan over the next year to invest in AI as a security safeguard. However this percentage is higher among medium and large companies in TMT (46%), financial services (40%), and other industries. Such investments could one day transform the role of the CISO[18] and provide ways to defeat otherwise unstoppable AI-powered cyberattacks[19] and deception schemes.[20]

At PwC, we believe companies that commit to building and demonstrating new trust mechanisms in the crucible of today's business, risk management and compliance challenges will likely define tomorrow's digital economy, crowding out less dedicated competitors. It is a journey worth taking.

16. PwC, Accelerating innovation: How to build trust and confidence in AI, 2017.
17. PwC, 2018 AI predictions, January 2018.
18. IDC, IDC FutureScape: Worldwide Security Products and Services 2018 Predictions, IDC #US43159217, October 2017. The report predicts, "By 2020, 50% of security telemetry will be made more useful via the use of machine learning and cognitive software, which will ingest and curate it into actionable and intelligent data at record speed."
19. New York Cyber Task Force, Building a Defensible Cyberspace, Sept. 28, 2017. "It is entirely possible that by 2025 or 2030, a supercomputer-driven attack could overwhelm any traditional cyber defenses on the planet; only a supercomputer-driven defense could react in time," the panel writes, noting this would require handing more power to large corporations and governments.
20. The New York Times, How an AI 'Cat-and-Mouse Game' Generates Believable Fake Photos, Jan. 2, 2018.
21. The Economist, Quantum computers will break the encryption that protects the internet, Oct. 20, 2018.

Actionable advice for business leaders

- Prioritize the development of digital trust controls and security budgets to support business investments and objectives around IoT, AI, and other emerging technologies.

- Stay attuned to emerging IoT security research. For instance, CMU researchers the Risk and Regulatory Services Innovation Center at Carnegie Mellon University sponsored by PwC have been researching the development and design new threat modeling, risk, and maturity assessment frameworks for IoT. Such frameworks could enable organizations to make more informed decisions about which actions and controls to implement for IoT security.

- When creating software, don't just integrate development and operations, but also embed security in the process (DevSecOps).

- Recognize AI will need both more robust governance and a new operating model. See our insights on predictions, building trust and confidence in AI and what it means to open AI's black box.

- Recognize emerging research in quantum computing could have profound implications for cybersecurity and beyond.21 It is not too early to start preparing.

PwC Cybersecurity and Privacy contacts

Georg Beham
Partner, Cybersecurity & Privacy Leader
PwC Österreich

+43 732 611750-19

georg.beham@pwc.com

Contributing author

Christopher Castelli

pwc.at/digital-trust-insights

pwc