

# Revitalizing privacy and trust in a data-driven world

Key findings from The Global State of  
Information Security<sup>®</sup> Survey 2018





Massive data breaches and the constant collection of personal information routinely spur debate on whether privacy, rooted in ancient times, is dead in the digital age. Are we in a post-privacy world? In many ways, it is the wrong question. Privacy, security and trust—all increasingly at risk—are also more vital and intertwined in our data-driven society.

## PwC insights on data privacy and trust

- 1 The challenge for CEOs is going beyond awareness to action
  - 2 Committing to risk management in digital transformation is existential
  - 3 Beyond confidentiality, privacy expectations focus on data use
  - 4 Advanced authentication technology will be a trust builder
  - 5 Even industry titans must boost board involvement
  - 6 More companies should consider hiring a chief privacy officer
  - 7 Lagging businesses in Europe and the Middle East have more work to do
  - 8 The balkanization of the internet will change how companies do business
  - 9 Consumers will vote for responsible innovation and data use with their wallets
-  Next steps for global business leaders

Many organizations worldwide are not doing all they can to protect privacy, according to our 2018 Global State of Information Security® Survey (GSISS). Privacy risk management needs reinvigoration and stronger integration with cybersecurity. Consumers and regulators want this. For CEOs and boards, the existential question is less about the future of privacy and more about the future of their own organization: Will the company muster the will and imagination needed to jolt stalled privacy risk management into action? Will it leverage that momentum and integrate cybersecurity, striving to become a trusted brand for responsible innovation and data usage? Or will it cede its place in the market to more committed competitors?

Drawing on key findings from the 2018 GSISS and beyond, we offer nine insights here on revitalizing privacy and trust in a data-driven world, concluding with next steps for global business leaders.

## 1 The challenge for CEOs is going beyond awareness to action

Senior executives recognize the rising stakes of cyber insecurity. This shows in the findings of our 2018 GSISS, as well as our 21st Global CEO Survey.<sup>1</sup> In the latter, CEOs worldwide identify cyber threats as the business threat of greatest concern. US CEO respondents go further by ranking cyber threats as their greatest overall worry, ahead of over-regulation, geopolitical uncertainty and terrorism. The World Economic Forum's 2018 Global Risks Report ranks both large-scale cyberattacks and major data breaches or fraud among the top five most likely risks in the next decade.<sup>2</sup>

---

1 PwC, [21st Global CEO Survey](#), January 2018.

2 World Economic Forum, [2018 Global Risks Report](#), January 2018.

**44%** say they are creating transparency in the usage and storage of data to a large extent.

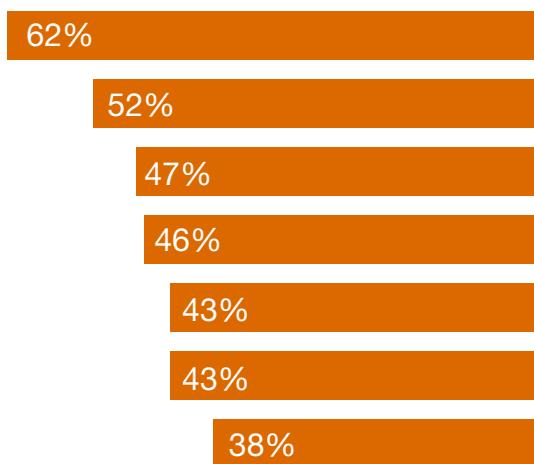


Source: PwC, 21st Global CEO Survey, January 2018.  
Base: 1,293 respondents

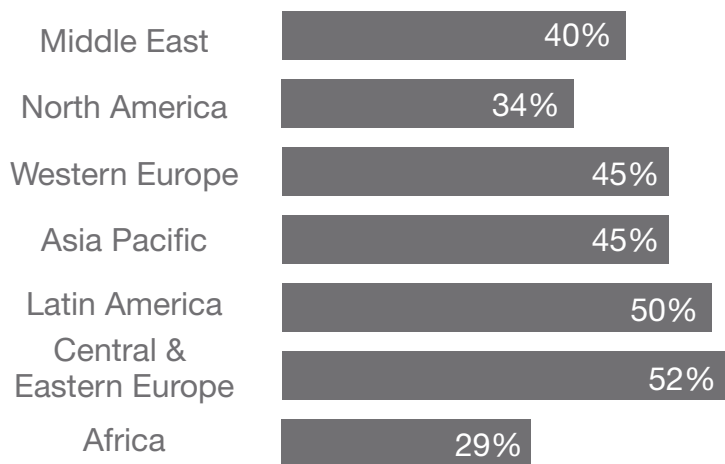
There is some cause for optimism. For instance, 87% of global CEOs say they are investing in cybersecurity to build trust with customers. Nearly as many (81%) say they are creating transparency in the usage and storage of data. Will it be enough? Unfortunately, less than half of CEOs say they are taking these actions “to a large extent.”<sup>3</sup> Further, a third of African CEOs and nearly a quarter of North American CEOs (22%) say they are “not at all” creating transparency in the usage and storage of data.

## CEOs worldwide have room to grow on cybersecurity and privacy

CEOs who say they are building trust with customers by investing in cybersecurity to large extent



CEOs who say they are building trust with customers by increasing transparency in data use and storage to large extent



Source: PwC, 21st Global CEO Survey, January 2018.

Base: Middle East respondents (52); North America (148); Western Europe (274); Asia Pacific (464), Latin America (136), Central & Eastern Europe (139), Africa (80)

<sup>3</sup> 47% of global CEOs say they are investing in cybersecurity to a large extent and 44% say they are to a large extent creating transparency in the usage and storage of data.

## Many businesses are still beginners at data-use governance

Only about half of respondents have put key measures in place



Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018.  
Base: 9,500 respondents

## 2 Committing to risk management in digital transformation is existential

Digital technologies are changing how society consumes, transacts, interacts, organizes and works in ways that current metrics don't fully capture.<sup>4</sup> The estimated amount of data that will be created and copied annually in 2025 is mind-boggling.<sup>5</sup> However, our 2018 GSISS results, based on responses from 9,500 executives in 122 countries and territories, show that many companies are still beginners in data-use governance.

Strengthening cybersecurity “at all levels—from those who collect data to those who transmit it, process it, store it, and use it—will be crucial” for personal data protection, according to the European Commission’s in-house think tank.<sup>6</sup> However, as many as 44% of 2018 GSISS respondents say they lack an overall information security strategy.<sup>7</sup> And executives are concerned about lagging skills in cybersecurity and privacy, according to our 2017 Global

4 US Commerce Department, [First Report of the Digital Economy Board of Advisors](#), December 2016.

5 The Economist, [Data is giving rise to a new economy](#), May 6, 2017. The article reports a prediction by a market-research firm (IDC) that the data created and copied annually “will reach 180 zettabytes (180 followed by 21 zeros) in 2025.

6 European Political Strategy Centre, [Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level](#), May 2017.

7 PwC, [Strengthening digital society against cyber shocks](#), Oct. 18, 2017.

Digital IQ<sup>®</sup> Survey.<sup>8</sup> In today's world, the old habit of moving to technology innovation before thinking through the issues and risks can have unprecedented consequences for businesses. "There are very few companies that are building cyber and privacy risk management into their digital transformation correctly," says Sean Joyce, PwC's US Cybersecurity and Privacy Leader. "The winners of the future are going to be the ones that from the design phase all the way to production build in that risk management—it's a brand-defining opportunity."

*"There are very few companies that are building cyber and privacy risk management into their digital transformation correctly."*

– Sean Joyce, PwC's US Cybersecurity and Privacy Leader

### 3 Beyond confidentiality, privacy expectations focus on data use

With confidentiality increasingly in jeopardy, data privacy is becoming more about controlling how data is used, while cybersecurity is focusing more on preventing data manipulation and destruction that could undermine trusted systems.<sup>9</sup> The Sheltered Harbor initiative in the financial sector, for instance, has developed standards to help banks recover and restore account data in the event of a major cyberattack.<sup>10</sup>

<sup>8</sup> PwC, [2017 Global Digital IQ<sup>®</sup> Survey](#), February 2017.

<sup>9</sup> Dan Geer, [closing keynote at SOURCE](#), Boston, April 27, 2017. The speech states in part, "Amongst the classic triad of confidentiality, integrity, and availability, we have heretofore prioritized confidentiality, especially in the military sector. That will not be the case going forward. In the civilian sector, integrity will supplant confidentiality as the highest goal of cybersecurity. In the military sector, weapons against integrity already far surpass weapons against confidentiality."

<sup>10</sup> PwC, [Strengthening digital society against cyber shocks](#), Oct. 18, 2017.



Consumers, however, have relatively low confidence that companies will use personal data in a responsible way. In PwC’s 2017 US Consumer Intelligence Series survey, only 25% of consumers say they believe most companies handle sensitive personal data responsibly.<sup>11</sup> The risk that personal data might be misused is Europeans’ top worry about online banking and e-commerce, according to a 2017 European Union public opinion survey on cybersecurity.<sup>12</sup>

The US National Institute of Standards and Technology’s goals for privacy engineering—a nascent branch of systems engineering focused on developing privacy solutions—initially included confidentiality.<sup>13</sup> But this goal soon changed to “disassociability”—enabling transactions not associated with a person’s identity—which is related to cryptography and the principle of data minimization.<sup>14</sup> The European Union’s General Data Protection Regulation (GDPR) calls for privacy by design, including data minimization, and says companies may need to pseudonymize or encrypt personal data. This all underscores the need for corporate governance over the management, protection and use of data.

---

11 PwC, [Consumer Intelligence Series: Protect.me](#), November 2017.

12 European Commission, [Special Eurobarometer 464a, Europeans’ attitudes towards cyber security](#), September 2017.

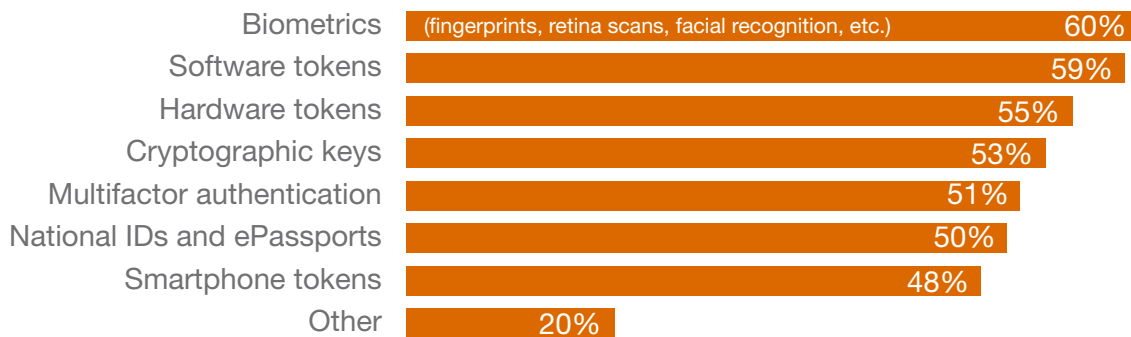
13 Inside Cybersecurity, [NIST’s draft privacy-engineering concepts avoid defining privacy](#), Oct. 3, 2014.

14 NIST Interagency/Internal Report (NISTIR) - 8062, [An Introduction to Privacy Engineering and Risk Management in Federal Information Systems](#), January 2017. The other two goals are predictability and manageability.

## 4 Advanced authentication technology will be a trust builder

The July 2017 G20 summit declaration stressed the need for “trust in digital technologies.”<sup>15</sup> We expect emerging improvements in authentication technology, including biometrics and encryption, to increasingly help business leaders build trusted networks. In the 2018 GSISS, half of respondents say the use of advanced authentication has improved customer and business partner confidence in the organization’s information security and privacy capabilities. In addition, 48% say advanced authentication has helped reduce fraud, and 41% say it has improved the customer experience. Further, 46% say they plan to boost investment in biometrics and advanced authentication this year. Simply using biometrics, however, creates its own exposure to privacy regulation and public concern as it relates to companies needing to track biometric information. And relying on knowledge-based authentication—when users provide a mother’s maiden name, for instance—potentially leaves an organization vulnerable to attack if the knowledge is stolen in a separate breach.<sup>16</sup>

### Companies are adopting advanced authentication technologies



Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018.  
Base: 9,500 respondents

We also expect increased pressure on industry to encrypt data for protection, which will drive related investments. Among financial sector respondents, 46% say they plan to increase investment in encryption this year.

<sup>15</sup> G20 Leaders’ Declaration, [Shaping an interconnected world](#), July 2017.

<sup>16</sup> PwC, [2018 Global Economic Crime and Fraud Survey](#), February 2018, predicts cybercrime will be the most disruptive fraud for organizations in the next 24 months.

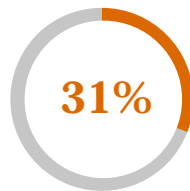


5

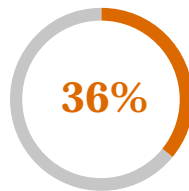
## Even industry titans must boost board involvement

Organizations of all sizes should boost the engagement of corporate boards in the oversight of cyber and privacy risk management. Less than a third of 2018 GSISS respondents say their corporate board directly participates in a review of current security and privacy risks. For organizations worth more than \$25 billion the figure is only a bit higher. Without a solid understanding of the risks, boards are not well positioned to exercise their oversight responsibilities for data protection and privacy matters. In addition, most US corporate directors are not very confident that their company’s data security and privacy program is comprehensive and that the company has identified its most valuable and sensitive digital assets, according to our 2017 Annual Corporate Directors Survey.<sup>17</sup>

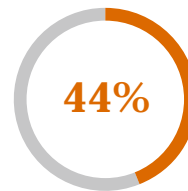
### Board involvement has significant room to grow



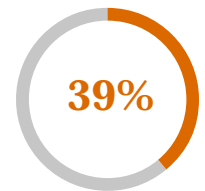
Say their corporate board directly participates in a review of current security and privacy risks\*



Of organizations worth more than \$25 billion say their corporate board directly participates in a review of current security and privacy risks\*\*



Of directors are very confident their company has a comprehensive program to address data security and privacy\*\*\*



Are very confident their company has identified its most valuable and sensitive digital assets\*\*\*

\* Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018. Base: 9,500 respondents  
\*\* Base: 435 respondents

\*\*\* Source: PwC, 2017 US Annual Corporate Directors Survey. Base: 842–849 respondents

17 PwC, [2017 Annual Corporate Directors Survey](#), October 2018.

## 6 More companies should consider hiring a chief privacy officer

About two-thirds of respondents worldwide say their organization has put a chief privacy officer (CPO) or similar executive in charge of privacy. This is even more common among the largest organizations. For institutions worth \$10 billion or more, at least 79% of respondents say their organization has such an executive in place. For organizations worth between \$15 billion and \$25 billion, it is 81%.

**2/3** say their organization has put a chief privacy officer or similar executive in charge of privacy.



Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018, October 18, 2017  
Base: 9,500 respondents

Respondents from organizations worth more than \$25 billion also appear to be outperforming other organizations in adopting limits on data collection, retention and access; maintaining an accurate data inventory; requiring training on privacy policy and practices; conducting compliance audits of third parties; and requiring third parties to comply with privacy policies. However, as many as one-third of respondents from the organizations with the most resources have yet to take these key actions.

### Businesses worth + \$25 billion are better at data-use governance

But a third of these industry titans have not yet taken key actions



Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018.  
Base: 407 respondents



## 7 Lagging businesses in Europe and the Middle East have more work to do

Businesses in Europe and the Middle East generally lag behind those in Asia, North America and South America in developing an overall information security strategy and implementing data-use governance practices, according to 2018 GSISS findings.<sup>18</sup> The data dovetails with the European Political Strategy Centre’s conclusion that Europe is “insufficiently prepared” for cyber risks,<sup>19</sup> as well as PwC’s previous finding that Middle East companies often have a “false sense” of cybersecurity.<sup>20</sup>

### Regional rankings show Asia and North America leading in key practices

Overall security strategy	Requires employee training on privacy	Accurate inventory of personal data	Limits data collection, retention and access	Audits compliance by third parties	Requires compliance by third parties
Asia 59%	N. America 58%	Asia 55%	Asia 53%	S. America 50%	S. America 50%
N. America 59%	Asia 57%	N. America 53%	N. America 53%	Asia 49%	N. America 47%
S. America 54%	S. America 50%	S. America 52%	S. America 47%	N. America 47%	Asia 47%
Europe 52%	Europe 47%	Europe 47%	Europe 44%	Europe 42%	Europe 44%
Middle East 31%	Middle East 29%	Middle East 20%	Middle East 19%	Middle East 26%	Middle East 26%

Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018.  
 Base: North America respondents (3,175), South America (1,261), Europe (2,416), Asia (1,585) and Middle East (94).

18 However, 64% of UK respondents say they have an overall information security strategy. Also, among UK respondents, the percentages for adopting data-use governance measures compare favorably with the results for organizations worldwide. For instance, 60% of UK respondents say they have an accurate data inventory.

19 European Political Strategy Centre, [Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level](#), May 2017.

20 PwC, [A false sense of security? Cybersecurity in the Middle East](#), March 2016.

**32%**  
say they started  
a GDPR assessment as  
of spring 2017.



Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018, October 18, 2017  
Base: 9,500 respondents

The EU's General Data Protection Regulation (GDPR), which applies to any organization that does business in the EU, will go into effect in May 2018. Some 2018 GSISS respondents say they were already making preparations for GDPR as of spring 2017—a year before the compliance deadline. About one third of respondents had started a GDPR assessment, for example, and this figure was a bit higher in Asia (37%) than elsewhere. In our latest GDPR pulse survey of 300 executives at US, UK and Japanese businesses, most respondents say GDPR preparations remain in the assessment and operationalizing phases, which suggests little progress across regions.<sup>21</sup>

The EU's Directive on Security of Network and Information Systems (NIS directive), which aims to boost cyber resilience, also goes into effect in May 2018. Businesses identified by member states as operators of essential services (critical infrastructure), as well as digital service providers (search engines, cloud computing services and online marketplaces), face new requirements under the directive for security and for reporting incidents to national authorities. As with GDPR, companies could face serious consequences for noncompliance.<sup>22</sup> “CEOs should see GDPR and the NIS directive not as compliance drills but rather as strategic opportunities to align their business for success in a data-driven world,” says Grant Waterfall, PwC's Europe, Middle East and Africa Cybersecurity and Privacy Leader. “In addition, companies should be reaching out to regulators to build relationships and lines of communication before compliance deadlines arrive.”

## **8** The balkanization of the internet will change how companies do business

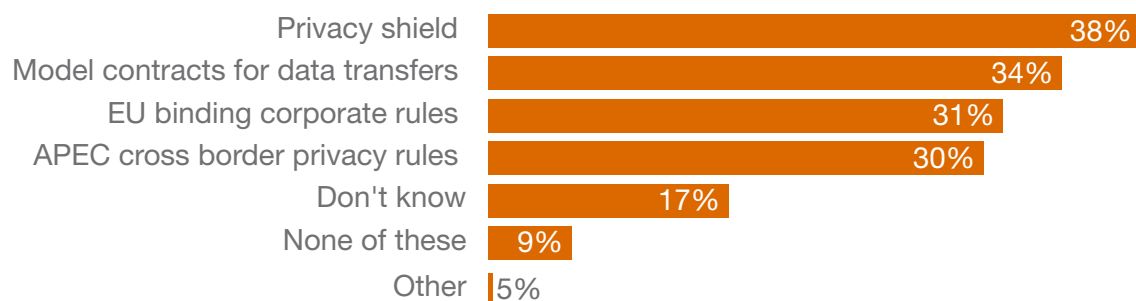
How companies address GDPR and other regulations such as China's new cybersecurity law and Russia's privacy law may have long-term implications. A recent forecast by the US National

<sup>21</sup> PwC, [Corporate GDPR preparations to stretch past May 2018](#), February 2018.

<sup>22</sup> UK government press release, [Government acts to protect essential services from cyber attack: Britain's most critical industries are being warned to boost cyber security or face hefty fines](#), Jan. 28, 2018.

Intelligence Council predicts the world's increased reliance on data “will require establishing clear limits and standards on data ownership, data privacy and protection, cross-border data flows and cybersecurity that could become increasingly important points of domestic and international policy conflict.”<sup>23</sup> Increasing regulation in this arena is more than likely.

## Which approaches are organizations taking for cross-border data flow?



Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018.  
Base: 9,500 respondents

Countries such as China have begun requiring companies to maintain data and application software within geographical boundaries where the businesses are operating.<sup>24</sup> The balkanization of the internet will change how companies do business. This will likely reduce efficiency and, in a macro way, have some effect on the global economy. Emerging approaches to cross-border data flows, nascent privacy rules and expanding regulation on data use worldwide all add up to an increasingly challenging path for companies to navigate toward success in the global digital economy. “Companies must watch not only emerging laws but also related implementation guidance, which can differ in important ways,” says Paul O’Rourke, PwC’s Asia Pacific Cybersecurity and Privacy Leader. “For instance, draft April 2017 cross-border data flow guidance for China’s cybersecurity law proposed new language calling for all network operators to comply.”

<sup>23</sup> US National Intelligence Council, [Global Trends: Paradox of Progress](#), January 2017. It also states that “conflicting pressures on balancing privacy and security interests will have far-reaching consequences for governance, economic competitiveness, and social cohesion.”

<sup>24</sup> PwC, [Top Policy Trends of 2018](#), January 2018.



## 9 Consumers will vote for responsible innovation and data use with their wallets

Data is driving the global economy in extraordinary ways that could transform society and expand prosperity. Technology is integral to everyday life, and viewed as helpful by many people. In our 2017 US Consumer Intelligence Series survey, respondents identified future scenarios they would consider most acceptable. At the top of the list is the use of Global Positioning System technology to let consumers locate lost or stolen devices. Next on the list is the use of comprehensive health records to identify a health condition before symptoms show, and the use of smart-home technology to control temperature and electrical systems to save money and resources while residents are away.

Consumers do put a monetary value on privacy—but context matters. It may seem paradoxical when consumers voice privacy concerns while still providing personal data online, but this does not mean consumers do not value privacy, Alessandro Acquisti, Professor of Information Technology and Public Policy at Carnegie Mellon University's H. John Heinz III College, noted last fall at PwC's Privacy Retreat.<sup>25</sup> He said research suggests that privacy preferences are shaped by context as opposed to being absolute.

In our 2017 US Consumer Intelligence Series survey, consumers say the biggest threats to consumer privacy protection include hackers and the emergence of new technologies such as artificial intelligence, machine learning and the internet of things (IoT).<sup>26</sup>

<sup>25</sup> PwC, [What CEOs need to know about privacy ethics, economics and risks](#), 2018.

<sup>26</sup> PwC, [Consumer Intelligence Series: Protect.me](#), November 2017.

PwC believes that in 2018 organizations will face growing pressure from end users and regulators to deploy AI that makes decisions in an explainable, transparent and mathematically provable way.<sup>27</sup> Robust governance and a new operating model could help AI reach its full potential.<sup>28</sup> “Market adoption of AI solutions will depend on end-user confidence that they—and not the machines—are in control of their information and their life choices,” says Jay Cline, PwC’s US Privacy Leader.

We also believe consumers will pay more for technology products that are designed with security and privacy in mind. In a 2017 EU public opinion survey, most respondents (61%) say they consider security and privacy features when choosing an information technology product and more than one quarter (27%) say they are ready to pay more for better security and privacy features.<sup>29</sup> The latter figure is notably higher in some EU countries, the same survey finds.<sup>30</sup> Consumer interest in data privacy is reportedly growing in China.<sup>31</sup> In addition, a 2017 PwC survey found 75% of US consumers surveyed were willing to pay more for extra security for smart home devices—if given the opportunity.<sup>32</sup> Consumers often do not have that option, however, because many IoT devices are cheaply produced with essentially no security or privacy protections. That needs to change.

---

27 PwC, [2018 AI predictions](#), January 2018.

28 PwC, [Accelerating innovation: How to build trust and confidence in AI](#), 2017.

29 European Commission, Special Eurobarometer 460, [Attitudes towards the impact of digitisation and automation on daily life](#), May 2017.

30 The percentage saying they would pay more is even higher in Denmark (44%), Germany (43%), Ireland and Cyprus (both 37%), and the United Kingdom (36%), among other EU countries, according to the same survey.

31 The Economist, [In China, consumers are becoming more anxious about data privacy](#), Jan. 25, 2018.

32 PwC, [Smart home, seamless life: Unlocking a culture of convenience](#), January 2017.



## Next steps for global business leaders

**The C-suite must own management of digital risk:** Cybersecurity, privacy and trust are increasingly intertwined within and outside the organization. CEOs must lead and not simply delegate data protection and privacy issues to others who are not fully responsible for driving the business and setting the risk appetite. To support CEO decision-making, the chief privacy officer should have a seat at the table. In addition, increasing communication with the board on these matters should be a priority. Further, CEOs must lead development of the resilience needed to sustain operations in the event of disruptive cyberattacks. Updating business continuity strategies, for instance, is important for maintaining access to accurate data in a crisis. Organizations should also leverage the World Economic Forum's principles for cyber resilience.<sup>33</sup>

**Engage your board:** Boards as a whole—not merely individual directors—should continuously arm themselves with better knowledge about the C-suite's plans to address emerging risks to data protection and privacy. This requires a sustained commitment to board education. Our primers on [How your board can be effective in overseeing cyber risk](#) and [Five questions boards should ask about data privacy](#) can provide a starting point. For example,

more boards should be asking whether their company's plans for adopting new technologies and data analytics are in sync with emerging global privacy regulations.

**Prioritize data-use governance:** Using data in more innovative ways opens the door to both more opportunities and more risks. Businesses should balance data use with strong protection and detection controls. Understanding the most common risks—including lack of awareness about data collection and retention activities, for example—is a starting point for developing a data-use governance framework. For more information, see [Monetizing data while respecting privacy](#), [Responsibly leveraging data in the marketplace](#), and [Strategically managing emerging cyber risks](#).

**View GDPR as an opportunity:** Business leaders should see GDPR as an opportunity to align their organizations to where they need to be for future success, not merely for compliance but rather for strategic risk management. Companies should take the initiative to engage with European regulators, maintain focus after the deadline because peak enforcement may not happen this year, and be mindful that ambitious law firms could act as de facto enforcement agents by pursuing GDPR-related litigation in civil courts. For more information, see [our research and insights](#).

<sup>33</sup> WEF, [Advancing Cyber Resilience: Principles and Tools for Boards](#), Jan. 18, 2017.



**Consider the risks of regulation abroad in a strategic context:** The balkanization of the internet could mean more companies will face pressure from foreign governments to provide access to sensitive intellectual property such as source code. Decisions about how to respond to such pressure should be informed by consideration of the cyber, privacy and trust risks that could arise from disclosing such sensitive information to foreign government officials.

**Champion responsible innovation:** Industry should support and participate in the development of emerging standards, as well as nascent efforts to build ties between privacy and technology professionals,<sup>34</sup> which could help put privacy principles into practice and provide consumers with smarter devices designed with cybersecurity and privacy in mind. Further,

by embedding cyber and privacy risk management in digital transformation efforts, corporate leaders can better align their organizations to withstand disruptive cyber threats, sustain operations, bolster the brand and business, build trust with consumers and gain competitive advantage.

Companies that seize the opportunity to manage data protection and privacy risks are expected to be better positioned to thrive in the data-driven economy and build resilience in digital society. Businesses that rush to transform digitally without building in security and privacy are on the path to obsolescence. In our next paper on the key findings of our 2018 Global State of Information Security® Survey, we'll explore themes related to the future of cybersecurity.

---

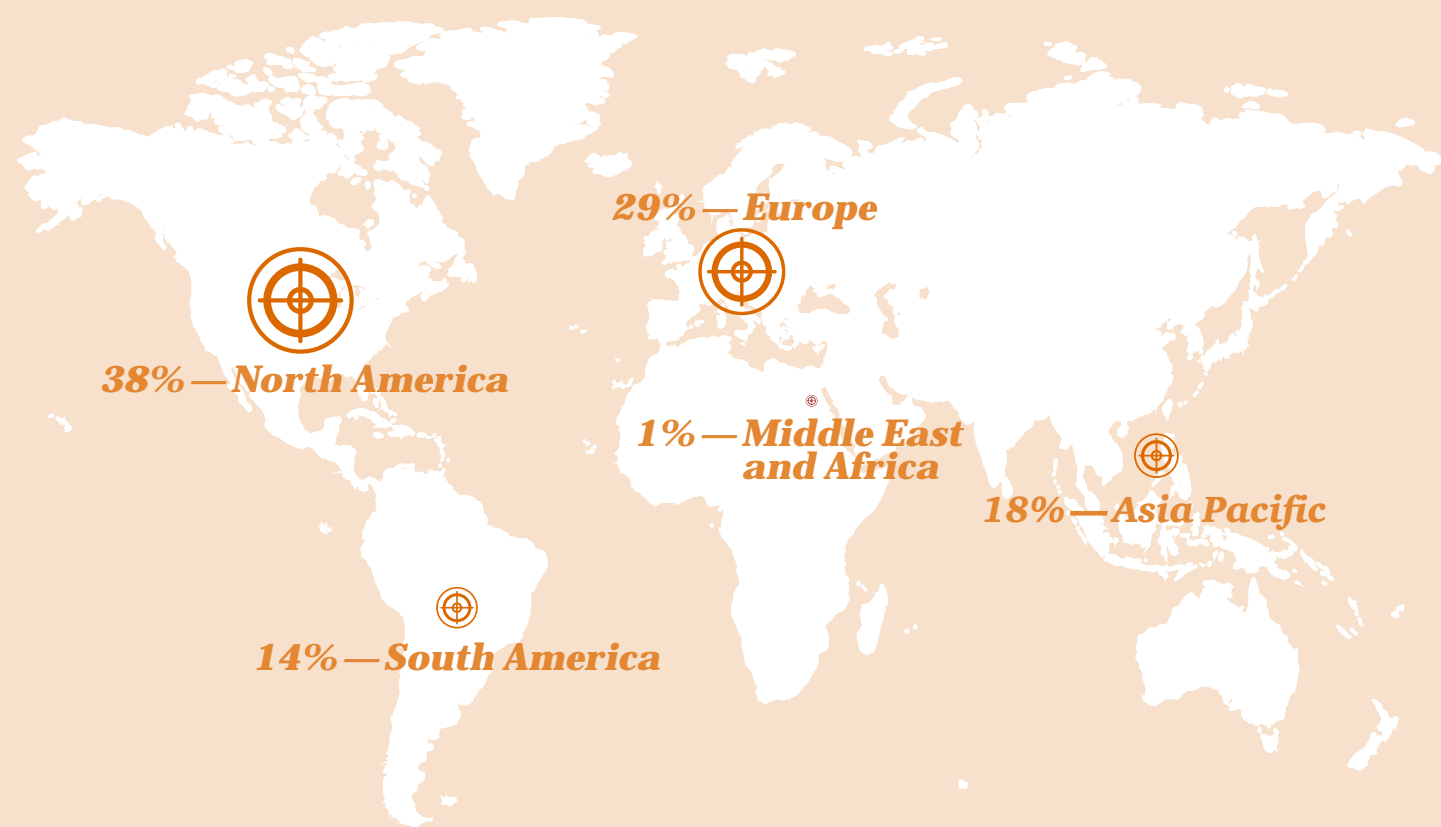
<sup>34</sup> NIST, [Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1](#), Dec. 5, 2017, includes a section on privacy engineering.

# Methodology

*The Global State of Information Security® Survey 2018* is a worldwide study by PwC, CIO and CSO. It was conducted online from April 24, 2017 to May 26, 2017. Readers of CIO and CSO and clients of PwC from around the globe were invited via email to participate in the survey.

The results discussed in this report are based on responses of more than 9,500 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices from more than 122 countries and territories.

Thirty-eight percent of survey respondents are from North America, 29% from Europe, 18% from Asia Pacific, 14% from South America and 1% from the Middle East and Africa.



The margin of error is less than 1%; numbers may not add to 100% due to rounding. All figures and graphics in this report were sourced from survey results.

# PwC cybersecurity and privacy contacts by country

## **Australia**

### **Richard Bergman**

Partner

richard.bergman@au.pwc.com

### **Steve Ingram**

Partner

steve.ingram@au.pwc.com

### **Andrew Gordon**

Partner

andrew.n.gordon@pwc.com

### **Megan Haas**

Partner

megan.haas@pwc.com

### **Robert Martin**

Partner

robert.w.martin@pwc.com

## **Austria**

### **Christian Kurz**

Senior Manager

christian.kurz@pwc.com

## **Belgium**

### **Pascal Tops**

Partner

pascal.tops@pwc.com

## **Brazil**

### **Edgar D'Andrea**

Partner

edgar.dandrea@br.pwc.com

### **Eduardo Batista**

Partner

eduardo.batista@br.pwc.com

## **Canada**

### **Sajith (Saj) Nair**

Partner

s.nair@ca.pwc.com

### **David Craig**

Partner

david.craig@pwc.com

### **Richard Wilson**

Partner

richard.m.wilson@pwc.com

### **Justin Abel**

Partner

justin.abel@pwc.com

### **Kartik Kannan**

Partner

kartik.kannan@pwc.com

## **China**

### **Ramesh Moosa**

Partner  
ramesh.moosa@cn.pwc.com

### **Kenneth Wong**

Partner  
kenneth.ks.wong@hk.pwc.com

### **Kok Tin Gan**

Partner  
kok.t.gan@hk.pwc.com

### **Marin Ivezic**

Partner  
marin.ivezic@hk.pwc.com

### **Chun Yin Cheung**

Partner  
chun.yin.cheung@cn.pwc.com

### **Lisa Li**

Partner  
lisa.ra.li@cn.pwc.com

### **Samuel Sinn**

Partner  
samuel.sinn@cn.pwc.com

## **Denmark**

### **Christian Kjær**

Partner  
christian.x.kjaer@dk.pwc.com

### **Mads Nørgaard Madsen**

Partner  
mads.norgaard.madsen@dk.pwc.com

## **France**

### **Philippe Trouchaud**

Partner  
philippe.trouchaud@fr.pwc.com

## **Germany**

### **Derk Fischer**

Partner  
derk.fischer@pwc.com

## **India**

### **Sivarama Krishnan**

Partner  
sivarama.krishnan@in.pwc.com

## **Indonesia**

### **Subianto Subianto**

Partner  
subianto.subianto@id.pwc.com

## **Israel**

### **Rafael Maman**

Partner  
rafael.maman@il.pwc.com

## **Italy**

### **Fabio Merello**

Partner  
fabio.merello@it.pwc.com

## **Japan**

### **Yuji Hoshizawa**

Partner  
yuji.hoshizawa@pwc.com

### **Sean King**

Partner  
sean.c.king@pwc.com

### **Naoki Yamamoto**

Partner  
naoki.n.yamamoto@pwc.com

## **Korea**

### **Soyoung Park**

Partner  
s.park@kr.pwc.com

## **Luxembourg**

### **Vincent Villers**

Partner  
vincent.villers@lu.pwc.com

## **Mexico**

### **Fernando Román Sandoval**

Partner  
fernando.roman@mx.pwc.com

### **Yonathan Parada**

Partner  
yonathan.parada@mx.pwc.com

### **Juan Carlos Carrillo**

Director  
carlos.carrillo@mx.pwc.com

## **Middle East**

### **Mike Maddison**

Partner  
mike.maddison@ae.pwc.com

## **Netherlands**

### **Gerwin Naber**

Partner  
gerwin.naber@nl.pwc.com

### **Otto Vermeulen**

Partner  
otto.vermeulen@nl.pwc.com

### **Bram van Tiel**

Director  
bram.van.tiel@nl.pwc.com

## **New Zealand**

### **Adrian van Hest**

Partner  
adrian.p.van.hest@nz.pwc.com

## **Norway**

### **Lars Fjørtoft**

Partner  
lars.fjortoft@pwc.com

### **Eldar Lorezntzen Lillevik**

Director  
eldar.lillevik@pwc.com

## **Poland**

### **Patryk Geborys**

Senior Manager  
patryk.geborys@pwc.com

### **Tomasz Sawiak**

Senior Manager  
tomasz.sawiak@pwc.com

### **Piotr Urban**

Partner  
piotr.urban@pwc.com

## **Singapore**

### **Tan Shong Ye**

Partner  
shong.ye.tan@sg.pwc.com

### **Jimmy Sng**

Partner  
jimmy.sng@sg.pwc.com

### **Paul O'Rourke**

Partner  
paul.m.orourke@sg.pwc.com

## **South Africa**

### **Sidriaan de Villiers**

Partner  
sidriaan.de.villiers@za.pwc.com

### **Elmo Hildebrand**

Director/Partner  
elmo.hildebrand@za.pwc.com

### **Busisiwe Mathe**

Partner/Director  
busisiwe.mathe@za.pwc.com

## **Spain**

### **Javier Urtiaga Baonza**

Partner  
javier.urtiaga@es.pwc.com

### **Jesus Manuel Romero Bartolomé**

Partner  
jesus.romero.bartolome@es.pwc.com

### **Israel Hernández Ortiz**

Partner  
israel.hernandez.ortiz@es.pwc.com

## **Sweden**

### **Martin Allen**

Director  
martin.allen@se.pwc.com

### **Rolf Rosenvinge**

Partner  
rolf.rosenvinge@se.pwc.com

## **Switzerland**

### **Reto Haeni**

Partner  
reto.haeni@ch.pwc.com

## **Turkey**

### **Burak Sadic**

Director  
burak.sadic@tr.pwc.com

## **United Kingdom**

### **Zubin Randeria**

Partner  
zubin.randeria@pwc.com

### **Richard Horne**

Partner  
richard.horne@uk.pwc.com

### **Alex Petsopoulos**

Partner  
alex.petsopoulos@uk.pwc.com

### **Grant Waterfall**

Partner  
grant.r.waterfall@uk.pwc.com

## **United States**

### **Sean Joyce**

Principal  
sean.joyce@pwc.com

### **Jay Cline**

Principal  
jay.cline@pwc.com

### **Joseph Nocera**

Principal  
joseph.nocera@pwc.com

### **Carolyn Holcomb**

Partner  
carolyn.c.holcomb@pwc.com

### **Joe Greene**

Principal  
joe.greene@pwc.com

### **Mark Lobel**

Principal  
mark.a.lobel@pwc.com

### **Prakash Venkata**

Principal  
prakash.venkata@pwc.com

### **Richard Kneeley**

Managing Director  
richard.j.kneeley@pwc.com

### **Shawn Connors**

Principal  
shawn.joseph.connors@pwc.com

**[www.pwc.com/gsis](http://www.pwc.com/gsis)**  
**[www.pwc.com/cybersecurityandprivacy](http://www.pwc.com/cybersecurityandprivacy)**

## ***Contributing author***

Christopher Castelli

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at [www.pwc.com](http://www.pwc.com).

©2018 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

PwC has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated or audited the data to verify the accuracy or completeness of the information. PwC gives no express or implied warranties, including but not limited to any warranties of merchantability or fitness for a particular purpose or use and shall not be liable to any entity or person using this document, or have any liability with respect to this document. This report is for general purposes only, and is not a substitute for consultation with professional advisors.