www.pwc.com/gsiss

Cybersecurity and Privacy

Strengthening digital society against cyber shocks

Key findings from The Global State of Information Security® Survey 2018

pwc

Table of contents

Massive cybersecurity breaches have become almost commonplace, regularly grabbing headlines that alarm consumers and leaders. But for all of the attention such incidents have attracted in recent years, many organizations worldwide still struggle to comprehend and manage emerging cyber risks in an increasingly complex digital society. As our reliance on data and interconnectivity swells, developing resilience to withstand cyber shocks—that is, large-scale events with cascading disruptive consequences—has never been more important.

There have been no reported deaths from cyberattacks and relatively little destruction.[1] But the disruptive power of cyberattacks is increasingly clear, particularly in geopolitical threats. For example, a December 2015 cyberattack in Turkey impacted networks used by the country's banks, media, and government.[2] Later that month, the first known cyberattack to take down a power grid targeted Ukraine's power distribution systems, cutting electricity to 230,000 residents.[3] That attack also targeted the country's phone system, preventing customers from reporting outages and thereby hindering power-restoration efforts.[4] In June 2017, the Petya cyberattack, aimed at Ukrainian computers, disrupted business operations across the globe. Massive data breach risks are raising concerns about the power of cyberattacks to ripple through the global economy.[5]

Anticipated results of a successful cyberattack against automation and/or robotics systems

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

1 The Cipher Brief, Cyber Deterrence Is Working – So Far, July 23, 2017
2 Harvard University Belfer Center for Science and International Affairs, Too Connected To Fail, May 2017
3 Wired, Inside the cunning, unprecedented hack on Ukraine's power grid, March 3, 2016
4 US Homeland Security Advisory Council, Final Report of the Cybersecurity Subcommittee: Part I - Incident Response, June 2016
5 The Wall Street Journal, The Morning Download, Sept. 11, 2017

Executives worldwide acknowledge the increasingly high stakes of cyber insecurity. In our 2018 Global State of Information Security Survey® (GSISS), leaders of organizations that use automation or robotics indicate their awareness of the potentially significant fallout of cyberattacks. Forty percent of survey respondents cite the disruption of operations as the biggest potential consequence of a cyberattack, 39% cite the compromise of sensitive data, 32% cite harm to product quality, 29% cite damage to physical property, and 22% cite harm to human life.

"Many organizations need to evaluate their digital risk and focus on building resilience for the inevitable."
– Sean Joyce, US Cybersecurity and Privacy Leader, PwC

Yet despite this awareness, many companies at risk of cyberattacks remain unprepared to deal with them. Forty-four percent of the 9,500 executives in 122 countries surveyed by the 2018 GSISS say they do not have an overall information security strategy. Forty-eight percent say they do not have an employee security awareness training program, and 54% say they do not have an incident-response process. "Many organizations need to evaluate their digital risk and focus on building resilience for the inevitable," said Sean Joyce, PwC's US Cybersecurity and Privacy Leader.

Business leaders are not well served by cybersecurity commentary that veers into either hyperbole about "cyber armageddon" or the countervailing viewpoint that most cyber threats are mundane. Much more productive would be a robust global conversation that gives business leaders actionable advice to build resilience against cyber shocks. In this paper—the first in our series on the key findings of the 2018 GSISS—we attempt to do just that.

How cyber interdependence drives global risk

According to the World Economic Forum (WEF), the rising cyber interdependence of infrastructure networks is one of the world's top risk drivers. The WEF 2017 Global Risks Report found that cyberattacks, software glitches, and other factors could spark systemic failures that "cascade across networks and affect society in unanticipated ways."[6]

The US National Intelligence Council's recent global trends report similarly cautioned that society faces "imminent" risk of cyber disruption—potentially on a massive scale with "lethal consequences"—due to the vulnerability of critical infrastructure.[7] Case studies of non-cyber disasters have shown that cascading events often begin with the loss of power—and many systems are impacted instantaneously or within one day, meaning there is generally precious little time to address the initial problem before it cascades.[8] Interdependencies between critical and non-critical networks often go unnoticed until trouble strikes.[9]

Many people worldwide—particularly in Japan, the United States, Germany, the United Kingdom, and South Korea—are concerned about cyberattacks from other countries.[10] Tools for conducting cyberattacks are proliferating worldwide. Smaller nations are aiming to develop capabilities like those used by larger countries. And the leaking of US National Security Agency (NSA) hacking tools has made highly sophisticated capabilities available to malicious hackers.[11] When cyberattacks occur, most victimized companies say they cannot clearly identify the culprits. In our 2018 GSISS, only 39% of survey respondents say they are very confident in their attribution capabilities.

6 World Economic Forum, 2017 Global Risks Report, January 2017
7 US National Intelligence Council, Global Trends: Paradox of Progress, January 2017
8 CascEff, Cascading effects: What are they and how do they affect society? July 31, 2017
9 Internet outages after the Sept. 11, 2001, terrorist attacks were caused by a chain of events: lack of electric power required a major data center to use backup generators that relied on fuel; poor air quality in the city due to the attack hindered data-center cooling, hastening fuel consumption; normal fuel delivery was blocked by emergency traffic limits; and without fuel, the generators could not function. See Harvard University Belfer Center for Science and International Affairs, Too Connected To Fail, May 2017
10 The Pew Research Center, Spring 2017 Global Attitudes Survey, August 2017
11 PwC, Bold Steps to Manage Geopolitical Cyber Threats, 2017

39% say they are very confident in their cyberattack attribution capabilities.

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

The soaring production of insecure internet-of-things (IoT) devices is creating widespread cybersecurity vulnerabilities.[12] Rising threats to data integrity could undermine trusted systems and cause physical harm by damaging critical infrastructure.[13]

In May 2017, G-7 leaders pledged to work together and with other partners to tackle cyberattacks and mitigate their impact on critical infrastructure and society. Two months later, G-20 leaders reiterated the need for cybersecurity and trust in digital technologies. The task ahead is huge. As the United Nations' International Telecommunication Union wrote in its 2017 Global Cybersecurity Index report, global interconnectivity could expose "anything and everything" to cyber risks and "everything from national critical infrastructure to our basic human rights can be compromised."[14]

There is a wide disparity in cybersecurity preparedness among countries around the world—both "between and within regions," according to the UN's 2017 Global Cybersecurity Index.[15] The UN found that only 38% of member states have a published cybersecurity strategy, and only 11% have a dedicated standalone strategy. Only 12% have a cybersecurity strategy in development. Although 61% of member states have an emergency response team with national responsibility, only 21% of states publish metrics on cybersecurity incidents.

12 PwC, Uncovering the Potential of the Internet of Things, 2017

13 Then-US Director of National Intelligence James Clapper told Congress in 2016, "Future cyber operations will almost certainly include an increased emphasis on changing or manipulating data to compromise its integrity (i.e., accuracy and reliability) to affect decision-making, reduce trust in systems, or cause adverse physical effects. Broader adoption of IoT devices and AI—in settings such as public utilities and health care—will only exacerbate these potential effects."

14 United Nations International Telecommunication Union, Global Cybersecurity Index report, 2017

15 The report ranked Singapore, the United States, Malaysia, Oman, Estonia, Mauritius, Australia, France, Georgia, and Canada as the most committed member states.

In our 2018 GSISS, we found that the frequency of organizations possessing an overall cybersecurity strategy is particularly high in Japan (72%), where cyberattacks are seen as the leading national security threat[16], and Malaysia (74%), which scored very well in the UN cybersecurity index. Both countries are in East Asia and the Pacific, a region where the World Economic Forum says cyberattacks are among the top five business risks.[17]

High preparedness does not necessarily mean low risk. The UN's 2017 Global Cybersecurity Index ranked the United States among the member states most committed to cybersecurity, second only to Singapore. But US infrastructure is still vulnerable to what the World Economic Forum deems the No. 1 business risk in North America: "large-scale cyberattacks or malware causing large economic damages, geopolitical tensions, or widespread loss of trust in the internet."[18] The US Department of Homeland Security has identified more than 60 entities in US critical infrastructure where damage, caused by a single cyber incident, could reasonably result in $50 billion in economic damages, or 2,500 immediate deaths, or a severe degradation of US national defense.[19]

For many people, the risk is real. A Pew Research Center survey found that a substantial majority of Americans expect major cyberattacks in the next five years on US public infrastructure or banking and financial systems. Most information security professionals believe that US critical infrastructure will suffer a cyberattack within the next two years.[20]

16 The Pew Research Center, Spring 2017 Global Attitudes Survey, August 2017
17 World Economic Forum, 2017 Global Risks Report shareable infographics, January 2017
18 World Economic Forum, 2017 Global Risks Report, January 2017
19 "Additional views" statement by Sen. Susan Collins (R-ME) in US Senate Report 114-32, April 15, 2015
20 Black Hat, The 2017 Black Hat Attendee Survey: Portrait of an Imminent Cyberthreat, July 2017

This underscores the need for all organizations, no matter how prepared they think they might be, to verify whether strategic cybersecurity goals are being executed. The White House's National Infrastructure Advisory Council wrote in an August 2017 report that many US infrastructure companies are not practicing basic cyber hygiene despite the availability of effective tools and practices.[21] In fact, the report's authors note, many companies are unaware of available federal tools for scanning, detecting, mitigating, and defending against cyber threats.

Resilience: The cyber-shock absorber businesses need

"Tomorrow's successful states," the US National Intelligence Council wrote in 2017, "will probably be those that invest in infrastructure, knowledge, and relationships resilient to shock—whether economic, environmental, societal, or cyber." The same idea applies to tomorrow's successful companies—those that are resilient will be best positioned to sustain operations, build trust with customers, and achieve high economic performance. So how can organizations achieve the toughness required to absorb the disruption caused by a cyberattack? The results of our 2018 GSISS suggest some answers.

Leaders must assume greater responsibility for building cyber resilience. In the private sector, those driving business results must also be held accountable for the associated risks of doing business. Boards must exercise effective oversight and proactive risk management. Strategies for business continuity, succession planning, strategic alignment, and data analytics are key. Yet the 2018 GSISS found that most corporate boards are not proactively shaping their companies' security strategies or investment plans.

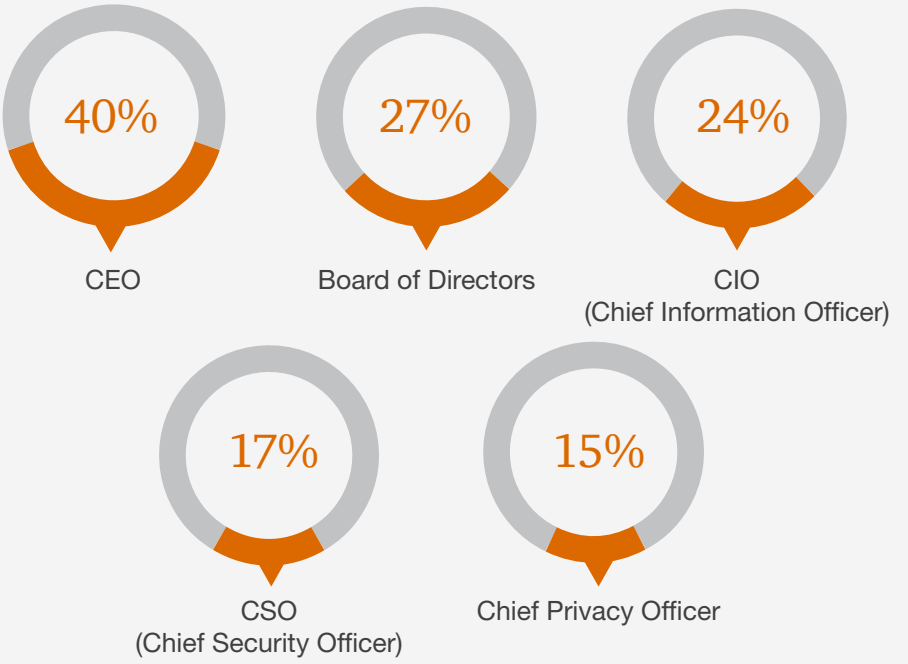
21 National Infrastructure Advisory Council, Securing Cyber Assets, August 2017

Only 44% of GSISS respondents say their corporate boards actively participate in their companies' overall security strategy. "Many boards still see it as an IT problem," said Matt Olsen, co-founder and president of business development and strategy for IronNet Cybersecurity and former head of the US National Counterterrorism Center. According to the National Association of Corporate Directors' 2016-2017 surveys of public- and private-company directors, few board members feel very confident that their companies are properly secured against cyberattacks.[22] Often a result of boards' lack of involvement in security measures, such doubt should come as no surprise. Just under half of all GSISS respondents agree that risk alone drives security spending. About 30% disagree, and the remainder are on the fence.

Most GSISS respondents (66%) say their organizations' security spending is aligned with the revenues of each line of business, but a sizeable remainder (34%) say that is not the case or they are not sure. The chief information security officer (CISO) is increasingly important. According to the 2018 GSISS, it is more common for a company's CISO or chief security officer to report directly to the CEO or the board of directors than to the chief information officer. "The CISO must help the board understand where the company stands in providing cybersecurity for the company networks," said Keith Alexander, the founder and CEO of IronNet Cybersecurity, who formerly led US Cyber Command and the National Security Agency as a four-star general. "The information provided should include any cyberattacks that have occurred, as well as shortfalls in training, equipment, and tools in the cyber domain. The CISO must highlight shortfalls so the board can execute their responsibilities in understanding and addressing risks facing the company."

22 Only 5% of public-company directors and 4% of private-company directors said they were "very confident." Most said they were only "moderately confident" (42% of public-company directors and 39% of private-company directors), according to survey data included in the National Association of Corporate Directors' 2017 Cyber-Risk Oversight Handbook

To whom does the CISO, CSO, or equivalent senior information security executive directly report?



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

Organizations must dig deeper to uncover risks. Achieving greater cyber resilience as a society and within organizations will require a more concerted effort to uncover and manage new risks inherent in emerging technologies. Organizations must have the right leadership and processes in place to drive the security measures required by digital advancements. Many businesses are just beginning this journey.

For example, relatively few respondents say their organizations plan to assess IoT risks across the business ecosystem. The ownership of responsibility for IoT security varies depending on the organization—29% say the duty belongs to the CISO, while others point to the engineering staff (20%) or the chief risk officer (17%). Cybersecurity executives, meanwhile, are still absent in many organizations. Only about half (52%) of respondents say

34%

say their organizations plan to assess IoT risks across the business ecosystem.

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

their organizations employ a CISO; 45% say they employ a chief security officer; and 47% say they employ dedicated security personnel to support internal business operations. Many organizations could manage cyber risks more proactively. Only half of respondents say their organizations conduct background checks. Many key processes for uncovering cyber risks in business systems—including penetration tests, threat assessments, active monitoring of information security, and intelligence and vulnerability assessments—have been adopted by less than half of survey respondents.

Greater information sharing and coordination among stakeholders is needed. Only 58% of respondents say they formally collaborate with others in their industry, including competitors, to improve security and reduce the potential for future risks. Trusted, timely, actionable information about cyber threats is a critical enabler for rapid-response capabilities that support resilience. Across organizations, sectors, countries, and regions, building the capability to withstand cyber shocks is a team effort, the effectiveness of which will be diminished without greater and more significant participation.

It is important for the information shared to be actionable. Among GSISS respondents who participate in collaboration, only half say their efforts have led to sharing and receiving more actionable information from their industry peers.

Only half of respondents say their organizations conduct background checks.

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

Next steps for global business leaders

C-suites must lead the charge—and boards must be engaged. Senior leaders driving the business must take ownership of building cyber resilience. Establishing a top-down strategy to manage cyber and privacy risks across the enterprise is essential. Resilience must be integrated into business operations. A company's risk management strategy should be informed by a solid understanding of the cyber threats facing the organization and an awareness of which key assets require the greatest protection. There should be a coherent risk appetite framework. Leadership must drive the development of a cyber risk management culture at all levels of the organization.

Pursue resilience as a path to rewards—not merely to avoid risk. Achieving greater risk resilience is a pathway to stronger, long-term economic performance. For example, the companies that built business-continuity management procedures into their enterprise risk management programs before the 2011 Japanese tsunami were able to resume operations faster than their competitors—allowing them to capture market share after the disaster.[23] Governments worldwide have long-term economic and national security interests in developing and disseminating useful practices and technologies to advance resilience in key sectors.

23 PwC, Building a Risk Resilient Organisation, 2012

Purposefully collaborate and leverage lessons learned. Industry and government leaders must work across organizational, sectoral, and national borders to identify, map, and test cyber-dependency and interconnectivity risks as well as surge resilience and risk-management. Leaders must also work together to tackle the thorny problems of accountability, liability, responsibility, consequence management, and norms. To do so, organizations should capitalize on available insights:

- Seek lessons in disaster-response case studies. For example, a 2016 study of the key underlying factors that made power restoration so effective after Superstorm Sandy found that such factors were lacking in the realm of cybersecurity. The study proposes potential ways to build an "all-hazards" system intended to address unique challenges associated with cyberattacks.[24]
- The National Association of Corporate Directors' "2017 Cyber-Risk Oversight Handbook" stresses that board members "need to ensure that management is fully engaged in making the organization's systems as resilient as economically feasible."[25] Cyber resilience principles issued by the World Economic Forum for boards in January 2017 are among the tools available.
- Developers of critical systems should design them to fail "as predictably and gracefully as possible," as advocated in a 2014 Center for a New American Security report.[26]
- Emerging guidelines from the Information Sharing and Analysis Organization (ISAO) standards body could help stakeholders across the economy more effectively share cyber threat information and lessons learned.

24 The Johns Hopkins University Applied Physics Laboratory LLC, Superstorm Sandy: Implications for Designing A Post-Cyber Attack Power Restoration System, March 2016
25 National Association of Corporate Directors' 2017 Cyber-Risk Oversight Handbook
26 Center for a New American Security, Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies, 2014

- A September 2017 report from The New York Cyber Task Force recommends a variety of cybersecurity approaches to achieve maximum impact at scale for minimum cost. Cloud-based technologies[27] have great potential to improve cybersecurity by providing an architecture and foundation that is secure by design, said Jason Healey, the task force's executive director. "We haven't even begun to see the payoff," Healey said.
- Emerging research could offer new opportunities. In September 2017, for example, the US Department of Energy (DOE) announced an award of more than $20 million to DOE's National Laboratories and partners for the development of cybersecurity tools to boost the resilience and risk management of the US electric grid and oil and gas infrastructure.[28]

Stress-test interdependencies. All key industry sectors across the world would do well to stress-test their interdependencies with simulated cyberattack scenarios designed to inform risk management. Dan Geer, chief information security officer at In-Q-Tel, has advocated developing cybersecurity stress test scenarios aimed at answering the following question: "Can I withstand the failure of others on whom I depend?"[29] A May 2017 study published by Harvard University's Belfer Center for Science and International Affairs endorsed that idea, underscoring the potential value of having regulators in critical infrastructure sectors sponsor or validate such tests.[30]

Voluntary efforts being undertaken now in the financial sector include recent moves by the Financial Services Information Sharing and Analysis Center (FS-ISAC) to establish the Financial Systemic Analysis & Resilience Center (FSARC) and the Global Resilience Federation. Efforts like these could provide relevant cybersecurity models for other sectors. The FS-ISAC is exploring

27 For more discussion on the cloud, see PwC, Moving Forward with Cybersecurity and Privacy, 2017 and New York Cyber Task Force, Building a Defensible Cyberspace, Sept. 28, 2017
28 US Department of Energy, press release, September 2017
29 Dan Geer, For Good Measure: Stress Analysis, login: Volume 39, Number 6, USENIX, December 2014
30 Harvard University Belfer Center for Science and International Affairs, Too Connected To Fail, May 2017

a proof-of-concept approach to building a virtual cyber range designed to enable organizations to conduct simulated, sandboxed cyberattacks that test resilience, said Bill Nelson, the organization's president and CEO. The energy sector conducts a biennial GridEx exercise designed to simulate a cyber/physical attack on the electric grid and other critical infrastructures across North America. "That sort of realistic wargaming—there is no substitute for that," said Matt Olsen of IronNet Cybersecurity.

Focus more on risks involving data manipulation and destruction. In an April 2017 talk, Dan Geer predicted integrity would supplant confidentiality as the most important goal of cybersecurity in the private sector. In the military sector, he added, "weapons against integrity already far surpass weapons against confidentiality."[31] The Sheltered Harbor initiative in the financial sector could offer a model or lessons for other sectors in dealing with these emerging risks. This effort has developed standards to help banks recover and restore account data in the event of a major cyberattack, said Nelson. The National Institute of Standards and Technology's new practice guide, "Data Integrity: Recovering from Ransomware and Other Destructive Events," issued in draft in September 2017[32], provides guidance for effectively recovering from a data-corruption event. Further, the use of blockchain is likely be "particularly relevant when the integrity of transactions or data is critical," as the US National Security Telecommunications Advisory Committee noted earlier this year in a draft report.[33]

The bottom line is that leaders can seize the opportunity now to take meaningful actions designed to bolster the resilience of their organizations, withstand disruptive cyber threats, and build a secure digital society. In the next paper on the key findings of our 2018 Global State of Information Security® Survey, we'll explore related themes on privacy and trust in digital society.

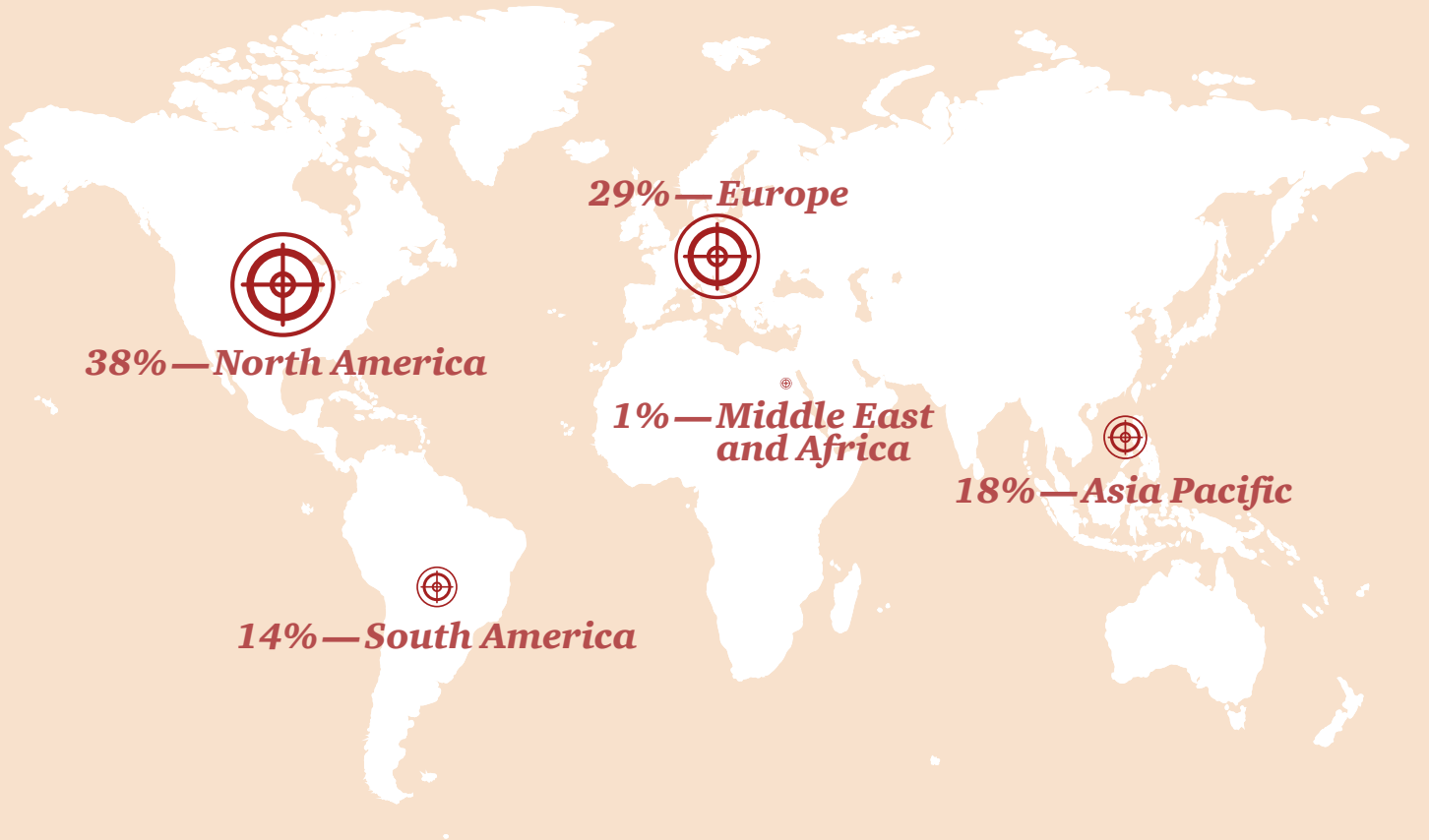
31 Dan Geer, closing keynote at SOURCE, Boston, April 27, 2017
32 US National Institute of Standards and Technology, Data Integrity: Recovering from Ransomware and Other Destructive Events, issued in draft in September 2017
33 US National Security Telecommunications Advisory Committee, Draft Report to the President on Emerging Technologies Strategic Vision, 2017

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.

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

Filip De Wolf
Partner
filip.de.wolf@be.pwc.com

Brazil

Edgar D'Andrea
Partner
edgar.dandrea@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

Rafal Jaczynski
Director
rafal.jaczynski@pl.pwc.com

Jacek Sygutowski
Director
jacek.sygutowski@pl.pwc.com

Piotr Urban
Partner
piotr.urban@pl.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

United States

Sean Joyce
Principal
sean.joyce@pwc.com

David Burg
Principal
david.b.burg@pwc.com

Grant Waterfall
Partner
grant.waterfall@pwc.com

www.pwc.com/gsiss
www.pwc.com/cybersecurityandprivacy

Contributing authors

Christopher Castelli, Barbara Gabriel, Jon Yates,
and Philip Booth

377868-2018