

Bold steps to manage geopolitical threats

How businesses can proactively address the cyber-risks of escalating political turmoil



*Key findings from
The Global State of
Information Security[®]
Survey 2017*

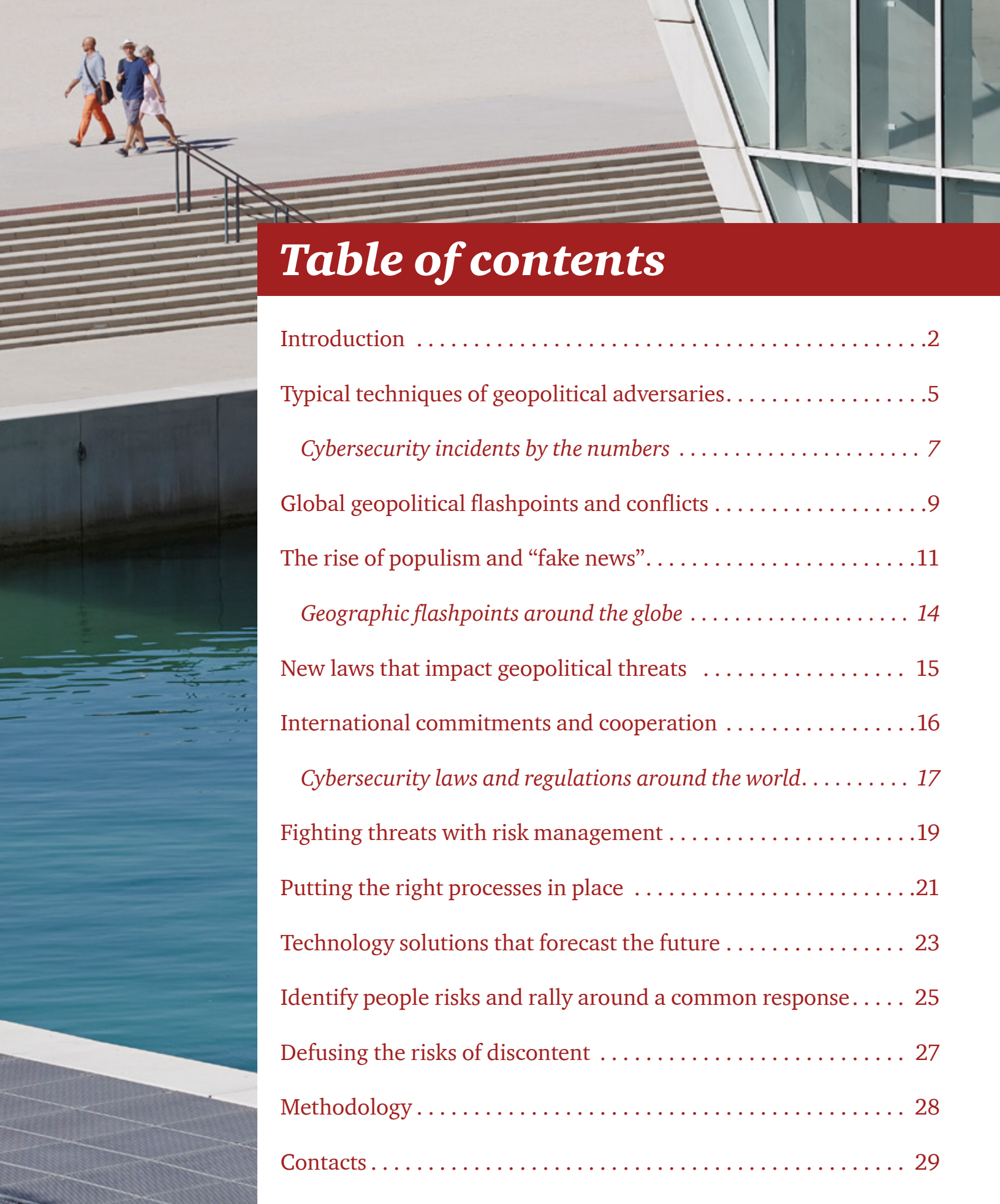
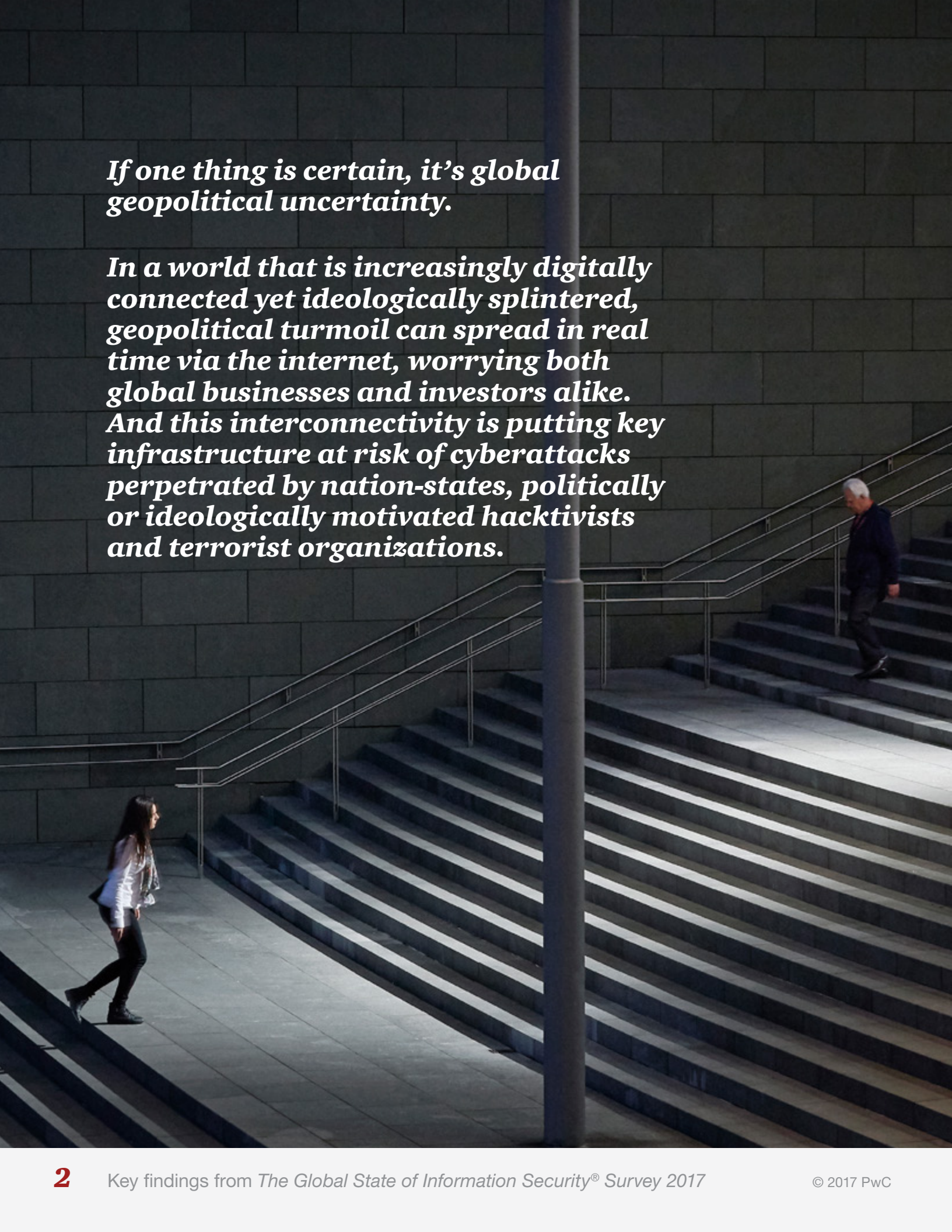


Table of contents

Introduction	2
Typical techniques of geopolitical adversaries.....	5
<i>Cybersecurity incidents by the numbers</i>	7
Global geopolitical flashpoints and conflicts	9
The rise of populism and “fake news”.....	11
<i>Geographic flashpoints around the globe</i>	14
New laws that impact geopolitical threats	15
International commitments and cooperation	16
<i>Cybersecurity laws and regulations around the world.</i>	17
Fighting threats with risk management	19
Putting the right processes in place	21
Technology solutions that forecast the future	23
Identify people risks and rally around a common response.....	25
Defusing the risks of discontent	27
Methodology	28
Contacts	29



If one thing is certain, it's global geopolitical uncertainty.

In a world that is increasingly digitally connected yet ideologically splintered, geopolitical turmoil can spread in real time via the internet, worrying both global businesses and investors alike. And this interconnectivity is putting key infrastructure at risk of cyberattacks perpetrated by nation-states, politically or ideologically motivated hacktivists and terrorist organizations.

Business executives are clearly worried: Almost three-quarters (74%) of respondents to PwC's 20th Annual Global CEO Survey said they are concerned that geopolitical uncertainties could impact their growth prospects. Further, more than two-thirds (68%) said that social instability could throttle growth.¹

They have good cause for concern. State-sponsored cyberattacks have more than doubled over the past three years, while incidents perpetrated by activists and hacktivists increased 83%, according to findings from The Global State of Information Security[®] Survey 2017.² While less prevalent, security incidents attributed to terrorists climbed 24% over the past three years.

140% 
Increase in incidents attributed to foreign nation-states over the past three years

PwC, CIO and CSO, *The Global State of Information Security[®] Survey 2017*, October 5, 2016

Further, the number of governments developing offensive cyberweapons is expanding to include smaller nations, a point underscored in the 2017 edition of the World Economic Forum Global Risks Report.³ And the reported theft and leaking of US National Security Agency (NSA) hacking tools shows that highly sophisticated capabilities can sometimes fall into the hands of malicious hackers.⁴ The exploits used to distribute the recent WannaCry ransomware attack, for instance, were reportedly among the NSA tools leaked to the world in April 2017 by an anonymous group called Shadow Brokers.⁵

1 PwC, *20th Annual Global CEO Survey*, January 2017

2 PwC, CIO and CSO, *The Global State of Information Security[®] Survey 2017*, October 2016

3 *Global Risks Report 2017, 12th Edition*, World Economic Forum, Switzerland, 2017

4 The New York Times, *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool*, May 12, 2017

5 The New York Times, *In Computer Attacks, Clues Point to Frequent Culprit: North Korea*, May 15, 2017

“Geopolitical risks and threats are extremely important today and we believe they will remain important for years to come,” said David Burg, PwC’s Global Cybersecurity and Privacy Advisory Leader. *“Smart companies must be aware of geopolitical threats as they make decisions about how to minimize cybersecurity risks, or accept the risks of doing business in a particular part of the world. Responsible companies are investing the time to study this issue and then designing programs that are fit for purpose to address today’s very real risks.”*

Managing this matrix of threats is an enormously complicated proposition, however, because cyberattacks are often intangible in nature and political turmoil can be difficult to predict. Compounding the matter is the formidable technical acumen of state-affiliated threat actors (as well as non-state actors), which has outstripped many organizations’ technological abilities to defend themselves.



Typical techniques of geopolitical adversaries

A typical attack starts with a targeted phishing campaign that covertly installs malicious software on computers when users click a file attachment or website URL. Once implanted, the malware moves laterally across networks and erases its tracks, making this type of incursion extremely difficult to identify.

Consider the breach of the US Office of Personnel Management (OPM).⁶ In March 2014, the OPM was alerted to an intrusion that began four months earlier when a hacker obtained the credentials of a third-party contractor to breach the network, install malware and create a network backdoor. Despite efforts to neutralize the attack, a series of breaches eventually resulted in exfiltration of personnel files of 4.2 million former and current government employees, as well as security background clearance information on 21.5 million individuals. On January 11, 2017, during his first press conference as president-elect, US President Donald J. Trump said that China carried out the OPM attack.⁷ But while US government officials and cybersecurity experts also believe that China was behind the breach, the US has not publicly issued a definitive attribution report for the hack. It can be difficult for governments to definitively attribute the source of a cyberattack without releasing classified information.⁸

6 US House of Representatives Committee on Oversight and Government Reform, [The OPM Data Breach](#), September 7, 2016

7 The New York Times, [Donald Trump's News Conference: Full Transcript and Video](#), January 11, 2017

8 The New York Times, [Hacking Linked to China Exposes Millions of U.S. Workers](#), June 4, 2015

“Geopolitical risks and threats are extremely important today and we believe they will remain important for years to come,” said David Burg, PwC’s Global Cybersecurity and Privacy Advisory Leader.

Another common tactic is the use of increasingly powerful distributed denial of service (DDoS) techniques by politically motivated hacktivists to embarrass or disrupt the operations of businesses and governments. The scale and brute force of DDoS attacks has intensified over the past year. In early 2016, a DDoS assault on the BBC's website peaked at a blistering 600Gbps.⁹ Just eight months later, the French internet hosting firm OVH reported an attack that topped 1Tbps.¹⁰

As political and economic uncertainties deepen across the globe, managing geopolitical threats is becoming a serious business risk that should be top of mind among executives and Boards of Directors.

This is the fourth in a four-part series on key findings from The Global State of Information Security® Survey 2017. The first two installments, [Moving forward with cybersecurity and privacy](#) and [Toward new possibilities in threat management](#), explored how digital businesses are adopting new cybersecurity technologies and processes and how they are addressing threats. The third paper, [Uncovering the potential of the Internet of Things](#), discusses cybersecurity issues for this emerging platform.

⁹ CSO, [DDoS Attack on BBC May Have Been the Biggest in History](#), January 8, 2016

¹⁰ Forbes, [How Hacked Cameras Are Helping Launch the Biggest Attacks the Internet Has Ever Seen](#), September 25, 2016



Take a look at our interactive timeline.

Connecting the dots: A timeline of technologies, threats and regulations that redefined cybersecurity and privacy

Cybersecurity incidents by the numbers

Incidents attributed to sophisticated threat actors by region

	North America	South America	Europe	Asia Pacific	Middle East & Africa
Activists/hacktivists	17%	17%	21%	21%	18%
Foreign nation-states	9%	9%	10%	10%	7%
Terrorists	8%	11%	11%	10%	14%

Source: The Global State of Information Security® Survey 2017

The frequency of detected incidents attributed to highly skilled malefactors is, for the most part, similar across geographic regions. Growth patterns of compromises across geographies and industries, however, suggest new fault lines in the geopolitical landscape.

Compared with other regions, fewer respondents from Middle East and Africa reported incidents attributed to nation-states. But within the region, compromises ascribed to nation-states soared 166% in 2016 over the year before. That's not entirely surprising, given the high incidence of geopolitical strife in the region. The Middle East and Africa also reported the biggest increase in attacks by hacktivists.

Europe reported a sharp (26%) year-over-year surge in attacks by nation-states and a 22% jump in incidents attributed to hacktivists. In North America, incidents ascribed to nation-states dipped slightly, while activity by hacktivists notched up (7%). South American respondents reported a double-digit rise in nation-states compromises.

Incidents attributed to sophisticated threat actors by industry

Activists/ hacktivists	Telecommunications 24%	Automotive 23%	Financial services 21%
Foreign nation-states	Entertainment & media 17%	Oil & gas 13%	Utilities 13%
Terrorists	Aerospace & defense 15%	Utilities 14%	Technology 12%

Source: The Global State of Information Security® Survey 2017

Any business in any industry is vulnerable to geopolitical threats. Across industries, nation-state incidents are highest in the entertainment/media and oil/gas industries. Telecommunications, automotive and financial services respondents are most likely to report incidents attributed to activists/hacktivists. And incidents ascribed to terrorists are most often reported by aerospace, defense and utilities companies.



Global geopolitical flashpoints and conflicts

Political rifts are broadening around the globe, stoking the potential for dangerous consequences in cyberspace and the physical world. Governments generally consider state-on-state cyber espionage for national security purposes to be within international norms. There is no global consensus, however, on rules governing conflict in cyberspace. Countries of various sizes, meanwhile, are increasingly acquiring offensive cyber capabilities as a means for advancing geopolitical objectives. In addition, some such capabilities have been stolen and leaked. As sophisticated hacking tools proliferate, a range of state, non-state and criminal actors operating in the shadows around the world are becoming more capable of posing geopolitical threats. Potential intersections of geopolitical tensions and cyber risks can be found worldwide. (See chart, Geographic flashpoints around the globe, page 14)

In November 2015, the G-20 backed voluntary norms of behavior in cyberspace, including the protection of critical infrastructure. Since then, however, a United Nations effort has been unable to reach consensus on the applicability of certain international law.¹¹ Cyberattacks, meanwhile, have already resulted in physical damage to critical infrastructure. The first known cyberattack to take down a power grid was in December 2015, when hackers infiltrated and took control of Ukraine's power distribution systems, cutting electricity to 230,000 residents. Power was restored within hours, but the operations of the distribution systems were impacted for several months.¹² Ukraine accused Russia of conducting the cyberattack, but the Kremlin denied involvement.

¹¹ US State Department, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, June 23, 2017

¹² Wired, *Inside the cunning, unprecedented attack on Ukraine's power grid*, March 3, 2016

The United States has reportedly used cyber operations in an attempt to undermine North Korea's efforts to develop intercontinental ballistic missiles.¹³ North Korea's recent testing of ballistic missiles has escalated tensions between Pyongyang and Washington, and has strained accords with other Asian nations.

Last year, South Korea accused North Korea of a number of serious cyberattacks that it said compromised smartphones of government officials, breached 160 companies and government agencies, and leaked military intelligence.¹⁴

In neighboring China, relations with the US initially faltered after the administration of President Trump signaled that it would take a more aggressive approach to economic and political policies with China. More recently, however, the Trump administration has tentatively offered China more favorable trade policies in exchange for applying economic pressure on North Korea in a bid to curb its nuclear program.¹⁵ China, for its part, is asserting a bolder stance on territorial disputes in the South China Sea.

In Brazil, political and economic issues have given rise to new waves of hacktivist activity. Last summer, the loose-knit hacking collective known as Anonymous Brasil launched #OpOlympicHacking, an attack on the Olympic Games in Rio de Janeiro that took down several government websites.¹⁶ The hacktivist group was also behind hacking activity supporting the anti-austerity movement in December 2016.

And then there's the continuing escalation of Islamist terrorism fomented by social media and the internet. Extremist groups continue to leverage tools such as social media, locked cellphones and encrypted communications channels to coordinate attacks, disseminate propaganda and share information. The perpetrators of the 2015 Paris attacks, for instance, used an encrypted messaging app to coordinate assaults that killed 130 people.¹⁷

¹³ The New York Times, [Trump Inherits a Secret Cyberwar Against North Korean Missiles](#), March 4, 2017

¹⁴ Flashpoint, [Business Risk Intelligence—Decision Report](#), January 11, 2017

¹⁵ The New York Times, [Why Trump's Budding Bromance With Xi Is Doomed](#), May 3, 2017

¹⁶ RSA, [Major Events and Hacktivist #OpOlympicHacking](#), August 20, 2017

¹⁷ The Washington Post, [The 'app of choice' for jihadists: ISIS seizes on Internet tool to promote terror](#), December 23, 2016

The rise of populism and “fake news”

Over the past year, numerous political movements have crystallized into new threats. Chief among them: a wave of populism that is polarizing democratic societies across the globe.

This current of populism is already producing worrisome consequences. It is eroding international cooperation and catalyzing unilateral economic policies and mutual suspicions of countries around the world, according to a report by the World Economic Forum.¹⁸

Among Western nations, the UK’s decision to leave the European Union (Brexit), the election of US President Trump and a rejection of constitutional reforms in Italy represented significant victories for populists and supporters of deglobalization. This movement is not limited to the West, however. Populism is also escalating in nations like Turkey and the Philippines.^{19,20}

In the US, it remains unclear to what extent the Trump administration’s protectionist economic policies might impact cybersecurity. Although President Trump has emphasized an “America first” stance on business interests, eschewing a global approach that has dominated economic policy for decades, the White House has also included in its executive order on cybersecurity²¹ a section underscoring the importance of international cooperation and calling for the development of a related US engagement strategy.

Regarding the Middle East, President Trump has said he intends to take a hard line against Iran and may attempt to renegotiate the Iran nuclear accord. Already, the US has imposed new sanctions against Iran in response to a ballistic missile test.²² It is arguable that sanctions, as well as the increasingly contentious relationship between the Washington and Tehran, could trigger retaliatory cyberattacks.

¹⁸ *Global Risks Report 2017, 12th Edition*, World Economic Forum, Switzerland, 2017

¹⁹ The New York Times, *Turkey’s Populists See an Unlikely Ally*, November 16, 2016

²⁰ The Diplomat, *The Global Populist Surge Is More Than a Western Story—Just Look at Asia*, December 10, 2016

²¹ The White House Office of the Press Secretary, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017

²² Bloomberg, *Iran Avoids Taking Trump Bait to Collapse Nuclear Deal*, February 5, 2017

Perhaps the most striking—and certainly unexpected—development over the past year are reports of state-backed interference with foreign political processes via cyber operations. In 2016, hackers infiltrated the computers of the US Democratic National Committee (DNC) and leaked more than 19,000 email messages that included sensitive information about the presidential campaign.²³ US officials have accused Russia of orchestrating the hack to interfere with the US presidential election, a matter the Federal Bureau of Investigation (FBI) is investigating.²⁴ Russia denied any state role in the hack although officials stated that “patriotically minded” private Russian hackers could have been involved.²⁵ The Kremlin has also previously accused other countries of using cyberattacks to influence Russian affairs.²⁶

More recently, cybercriminals hacked the computer systems of French presidential candidate Emmanuel Macron and leaked “massive” amounts of campaign documents 36 hours before voting began. The hacking operation had little impact on the election outcome, however, because France prohibits media coverage of elections 44 hours before polls close. US security officials have implicated Russia in the hacking.²⁷ French officials, however, have not publicly attributed the source of the attack. The head of the French government’s cybersecurity agency has noted the hackers used a generic, simple approach that does not rule out the possibility of state involvement but “means that we can imagine that it was a person who did this alone. They could be in any country.”²⁸

23 The Washington Post, [Wikileaks posts nearly 20,000 Hacked DNC Emails Online](#), July 22, 2016

24 The Washington Post, [Full transcript: FBI Director James Comey testifies on Russian interference in 2016 election](#), March 20, 2017

25 The New York Times, [Maybe Private Russian Hackers Meddled in Election, Putin Says](#), June 1, 2017

26 Los Angeles Times, [Russia’s answer to charges of meddling in U.S. elections: You’re messing with ours, too](#), June 23, 2017

27 AP News, [US watched Russia hack French systems during election](#), May 10, 2017

28 CBS/Associated Press, [French security chief warns of risk for “permanent war” in cyberspace](#), June 1, 2107

The maneuver against the US election also introduced a new phrase into the political lexicon: “fake news,” a strategy to disseminate spurious and highly partisan online articles via social media to influence understanding of current events.

There is mounting concern that similar campaigns will be launched to tamper with upcoming elections in other European nations. The US government, for its part, last year classified the country’s election system as part of its critical infrastructure.



Geographic flashpoints around the globe

Nation	Issues	Risks
China	Territorial disputes in the South China Sea; protectionist cybersecurity laws; increasing restrictions on foreign companies.	China may take a more aggressive approach to territorial disputes; its new cybersecurity law may introduce new restrictions on foreign businesses.
Iran	Uncertainty about the Joint Comprehensive Plan of Action (Iranian nuclear accord); increasing political friction with the US over Iranian nuclear program and missile testing.	Possible disruption of national critical infrastructures; may introduce new sanctions on entities believed to engage in malicious cyberactivity.
North Korea	Rising attacks against South Korean government, businesses and power companies; launch of ballistic missiles weakens relations with US and Asian nations.	Possible cyberespionage and destructive attacks on businesses and governments; possible escalation of hostilities as a result of missile testing.
Russia	Tensions within region and with Western nations; critical infrastructure cybersecurity; US federal investigation of Russia and US presidential election.	US Secretary of State said in July 2017 that US and Russia need a common framework on how to deal with cyber threats “in terms of how these tools are used to interfere with the internal affairs of countries, but also how these tools are used to threaten infrastructure, how these tools are used from a terrorism standpoint as well.” ²⁹
Syria	Civil war between government and rebels; ISIS stronghold.	Instability may spread to other nations in the region; Islamist political movement may fragment and spread.
United States	Protectionist policies and deglobalization; federal investigation of Russia and US presidential election; critical infrastructure cybersecurity; sanctions against other governments.	In the interest of increasing cyber deterrence, the White House may object more to the behavior of some other nations in cyberspace and may aim to impose costs on adversaries.

²⁹ The White House Office of the Press Secretary, *Press Briefing on the President's Meetings at the G20*, July 7, 2017

New laws that impact geopolitical threats

Geopolitical uncertainty, populist upheavals and financial volatility have given rise to new national and regional data-protection laws across the globe. What we're seeing is an overall move toward increasing data-localization requirements, policies to circumvent encryption and more severe sanctions. (See chart, Cybersecurity laws and regulations around the world, page 17.)

China's National Cybersecurity Law, which reportedly may be fully implemented by 2018, will present new challenges to outside companies that do business within its borders.³⁰ The law will tighten and centralize the flow of internet data and technology equipment, and impose mandatory reviews of computer equipment in sectors that China deems critical infrastructure. Other recent rules require technology companies and financial institutions to store their data in China, submit to security checks and help the government with decryption, if requested.

Similarly, Russia's Yarovaya Law requires that telecommunications and internet providers store communications data within its national borders, as well as help intelligence agencies decode encrypted messaging services.³¹ In the US, Rule 41 gives law-enforcement agencies new investigative power to search multiple computers in multiple districts with a single warrant.³²

Governments are enforcing laws with more unsparing sanctions against nation-states that launch cybersecurity incidents. In the US, for instance, the government responded to Russia's alleged meddling in the presidential election by expelling 35 suspected Russian intelligence operatives from the US and imposing sanctions on Russia's leading intelligence services.³³

³⁰ Reuters, [Amid industry pushback, China offers changes to cyber rules](#), May 19, 2017

³¹ The New York Times, [Russia Moves to Tighten Counterterrorism Law; Rights Activists See Threat to Freedoms](#), June 24, 2016

³² Fortune, [FBI's New Hacking Powers Take Effect This Week](#), November 30, 2016

³³ The New York Times, [Obama Strikes Back at Russia for Election Hacking](#), December 29, 2016

International commitments and cooperation

The news is not all bad, however. While individual nations are cloaking themselves in protectionist ideologies, the Group of 20 international forum is taking a more cooperative stance.

In 2016, the G-20 affirmed its commitment to the free flow of information across borders and reaffirmed voluntary peacetime norms of responsible state behavior in cyberspace and prohibition of industrial cyberespionage.³⁴ The international forum also committed to address cybersecurity risks, threats and vulnerabilities in the digital economy.

“The G-20 agreement is beginning to build some momentum around creating repercussions for countries that commit cyberattacks for economic advantage,” said Burg. “A very powerful step forward would be to put meaningful global enforcement behind this agreement to protect businesses.”

To be clear, state-on-state cyberespionage conducted for national security purposes is ubiquitous, and will likely continue unabated. However, multilateral and bilateral agreements among governments, as well as the continued development and promotion of international norms of behavior in cyberspace, have the potential to reduce cyber-enabled industrial espionage, foster greater stability in cyberspace and reduce the likelihood of destructive cyberattacks against critical infrastructure. Nascent efforts by government officials to develop cyber-deterrence policy approaches, although relatively immature for now, may also promote stability in cyberspace over the long term.

³⁴ The White House, [Fact Sheet: The 2016 G-20 Summit in Hangzhou, China](#), September 5, 2016

Cybersecurity laws and regulations around the world

Nation	Law/regulation	Provisions	Impact
Australia	Australia Privacy Amendment Bill	Establishes mandatory disclosure of data breaches to customers, the government and possibly the media.	May increase complexity of data-breach monitoring and response plans; will require updated data-breach assessment capabilities; will demand more sophisticated data-breach response capabilities.
China	National Cybersecurity Law	Tightens and centralizes flow of internet data and technology equipment; imposes mandatory reviews of computer equipment in certain sectors.	May make it more difficult for companies to do business in China; businesses may be required to help national authorities in investigations; companies may have to reveal source code and other corporate data.
European Union	General Data Protection Regulation (GDPR)	Mandates new data-privacy requirements for companies that do business in the EU. Key requirements include mandatory data-breach notification, the right to be forgotten, data-protection impact assessments and appointment of data protection officers.	Businesses will need to: assess and remediate compliance with GDPR; update data-governance strategies; and implement adequate processes and technologies for maintaining comprehensive data inventories. Businesses that do not comply with GDPR face fines as high as 4% of the company's global annual revenue.

Nation	Law/regulation	Provisions	Impact
Russia	<u>Yarovaya Law</u>	Anti-terrorism law that expands authority of law enforcement agencies; sets new requirements for data collection and storage; expands regulation of “missionary activities.”	May impact privacy and internet freedom; creates complex requirements for data storage; imposes restrictions on free speech.
United Kingdom	<u>Investigatory Powers Act of 2016</u>	Introduces requirements on interception of communications and the acquisition and retention of communications data; gives law enforcement and intelligence agencies new access to data.	Requires web and telecommunications companies to store web-browsing histories for 12 months; gives law enforcement agencies access to the data.
United States	<u>Rule 41</u>	Gives law enforcement agencies the right to search multiple computers in multiple districts with a single warrant; enables government to search computers that conceal their location using proxy computers.	Could expand government surveillance capabilities; enables the government to search thousands of computers with a single warrant.

Fighting threats with risk management

As noted, political events are notoriously difficult, if not impossible, to forecast, particularly in turbulent geographies and governments. This underscores the need for business leaders to develop resilience — the capability to bounce back from events such as cyberattacks. Resilience will be increasingly important for sustaining the operations of critical infrastructure in the future, the US National Intelligence Council noted in a global trends report issued earlier this year.³⁵

Resilient organizations align risk management with strategic planning, establish clearly defined and automated security processes for information technology and use analytics to predict and rapidly respond to attacks. They also develop strategies for business continuity, succession planning, strategic alignment and data analytics.

Further, business leaders should identify known geopolitical threats and treat them as enterprise-wide business risks, just as they would more tangible issues such as financial instability.

³⁵ National Intelligence Council, *Global Trends: Paradox of Progress*, January 2017



“One of the single biggest changes we’ve seen in recent years is nation-state use of sophisticated cyberattack techniques to compete on a geopolitical stage,” said Burg. *“Today, CEOs, Board members and senior executives around the world recognize that taking cybersecurity very seriously is really critical to business strategy.”*

Business leaders should be prepared to assess emerging geopolitical threats, vulnerabilities and potential impacts across a range of potential circumstances specific to their environment and industry. They should also understand that geopolitical threats are not limited to politically “risky” regions or developing economies. The hacks during the 2016 US presidential elections demonstrated that developed nations are also susceptible to geopolitical compromises.

Moreover, risks are not bound by sovereignty or by nation-state. Ubiquitous, fast internet connectivity means that threats are borderless and can exist within, among and between nations.

Consequently, business leaders should be prepared to address risks that are unique to each country in which they operate. The risks of operating in Brazil will be different than risks associated with running a business in China—or the US, for that matter. The motivations and tactics of malicious actors may also be specific to a particular nation, and solid knowledge of these attributes is essential to understanding the threat landscape.

Safeguarding against unpredictable and highly complex threats will require that organizations integrate geopolitical threats into their overall enterprise risk-management program. Some businesses create an interdepartmental committee that works hand in hand with executive leadership to understand potential geopolitical threats and proactively plan responses.

“It’s absolutely essential that businesses bring geopolitical threats into their risk-management program and, when necessary, put them on the Board’s agenda,” said Burg. *“Specifically, they should examine cybersecurity threats of geopolitical instability within the context of their risk-management perspective.”*

Putting the right processes in place

An assessment of geopolitical risks should be considered within the context of the organization's overall cybersecurity risk posture and its individual processes, technologies and personnel capabilities.

First, know your enemies. Start by performing an enterprise-wide cybersecurity-risk analysis assessment that factors in identified or likely geopolitical threats. This assessment should identify critical business processes and assets, map and test threat scenarios to key controls, and align cyber-risk exposures with individual business risk appetites.

It's essential to examine existing networks, applications and operating systems to determine if they are properly updated. From there, businesses should implement a strategy for proactive patch management to help shield the organization from malicious intruders. Updating of internet-connected servers and computers represents a first line of defense that helps eliminate entry points potentially available to hackers.

Another common vulnerability is poorly protected privileged user accounts, which are a tempting vector to adversaries because they can unlock virtually unlimited access to sensitive data, systems and digital assets. In point of fact, Forrester Research estimates that 80% of security breaches involve privileged credentials.³⁶

Basic precautions to protect these accounts include the use of strong passwords that are regularly changed, secure storage of passwords and limited sharing of account credentials among IT administrators. More advanced capabilities can be found in privileged account management solutions, which create a centralized methodology to integrate security controls across the perimeter, network and application security zones.

Finally, it's critical to look beyond the individual business ecosystem to understand the potential risks and vulnerabilities of third parties and supply chains. Despite numerous highly public

36 Forrester Research, *The Forrester Wave™: Privileged Identity Management, Q3 2016*, July 8, 2016

breaches that started with compromised third-party credentials, many organizations do not adequately assess their partners' cybersecurity capabilities. This year, for instance, only 49% of GSISS respondents said they require third parties to comply with their privacy policies.

The reason very well may be that developing and implementing third-party risk management programs can be challenging for organizations that lack the right controls, oversight mechanisms and in-house expertise. Complicating the matter are new third-party relationships—such as affiliates that perform shared services, revenue-sharing agreements and roles in the Internet of Things—that may not fit traditional partner profiles. Nonetheless, organizations should take steps to implement a strategy to manage risks throughout the third-party lifecycle, from planning to due diligence, contract negotiation and termination.



Technology solutions that forecast the future

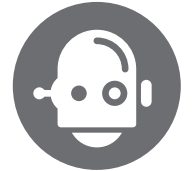
A program to address geopolitical threats won't be successful without sophisticated technologies for monitoring, threat detection and data analytics. These tools, in fact, form the foundation for the next generation of cybersecurity defense: The ability to forecast future events based on very advanced data analytics.

Already, predictive analytics is gaining traction as a means to calculate the probability of threats and take proactive action. Unlike signature-based solutions, which use known cyberattack data, predictive analytics ingests

and analyzes massive volumes of data, then employs self-learning technologies to profile and monitor activity. The ultimate goal of predictive analytics is to forecast terrorist acts, cybersecurity incidents and social upheaval before they occur.

23%

Will invest in artificial intelligence and machine learning in the coming year



PwC, CIO and CSO, *The Global State of Information Security*® Survey 2017, October 5, 2016

“It’s absolutely essential that businesses bring geopolitical threats into their risk-management program and, when necessary, put them on the Board’s agenda,” said Burg.

Similarly, tech-savvy businesses are tapping artificial intelligence (AI) and machine learning technologies that can learn patterns of activities and identify deviations that may signal a breach in progress. Governments, for better or worse, are adopting these technologies to improve surveillance and monitoring for terrorist activities. Despite the fact that AI and machine learning require extensive customization for individual business context, these technologies are gaining momentum: Almost one-quarter (23%) of respondents to PwC's security survey said they plan to invest in AI and machine learning in the coming year.

Another critical technology is encryption of data at rest and in transit. Encryption tools are built on a variety of algorithms, cryptographic strengths and methods. We're seeing that some businesses are adopting application-layer encryption to diminish their attack surface. This approach helps protect data at the points in which applications interact with the network, including in transit across the network, at gateways and at endpoints. Another option is network-based encryption to protect data in transit. This technique applies encryption at the network transfer layer to help safeguard communications between local networks without adding undue complexity.



Identify people risks and rally around a common response

One chink in the armor of cybersecurity programs that's often overlooked is employee training on security best practices. Another is a commitment to an organizational culture of security.

Staff awareness of basic cybersecurity hygiene is particularly vital to deflecting geopolitical risks because threat actors often employ phishing schemes to obtain user credentials and then infiltrate information systems and data. This type of incursion could very likely be defused by training employees on how to recognize and avoid phishing attempts. So it seems counterintuitive that many businesses disregard employee awareness: This year's GSISS study found that almost half (47%) of respondents do not have an employee awareness program in place.



Staff training can also help foster a business-wide culture of security. An organizational commitment to cybersecurity should come from the top, however. It's critical that executive leaders proactively articulate company's commitment to addressing geopolitical conditions and threats. As noted above, the Board should also understand that geopolitical threats constitute significant business risks and should be treated with the same oversight as traditional risks.

Externally, businesses can harness the power of people by sharing intelligence on political threats with business peers, industry groups and government agencies. Specifically, there is much to be gained

from Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs).³⁷ While industry-specific ISACs have been around for decades, the newer ISAOs provide a powerful potential to share threat data at a scale and speed that can significantly disrupt malicious cyberactivity.

51%

Will invest in collaboration among business, digital and IT in the coming year



PwC, CIO and CSO, *The Global State of Information Security*® Survey 2017, October 5, 2016

37 PwC, [Cybersecurity information-sharing hubs: Why C-suites should care about ISAOs](#), April 2016

“One of the single biggest changes we’ve seen in recent years is nation-state use of sophisticated cyberattack techniques to compete on a geopolitical stage,” said Burg. “Today, CEOs, Board members and senior executives around the world recognize that taking cybersecurity very seriously is really critical to business strategy.”

Defusing the risks of discontent

We no longer have to imagine a theoretical world in which geopolitical risks can proliferate across cyberspace and cause significant damage. We now have real-life instances.

Taken together, the volatilities across the global geopolitical landscape and the breakneck pace of technological advances have combined to create myriad new threats that can be quickly delivered across the internet. As nation-states and individual actors continue to test the limits of acceptable behavior in cyberspace, there is a very real possibility that their actions could escalate to the physical realm, including armed conflict.

A risk-based approach to geopolitical uncertainties can help organizations anticipate and manage threats through better visibility into global political activity and how risks might impact individual businesses. It can also assist in proactively monitoring geopolitical situations and implementing a response plan to minimize impacts and losses.

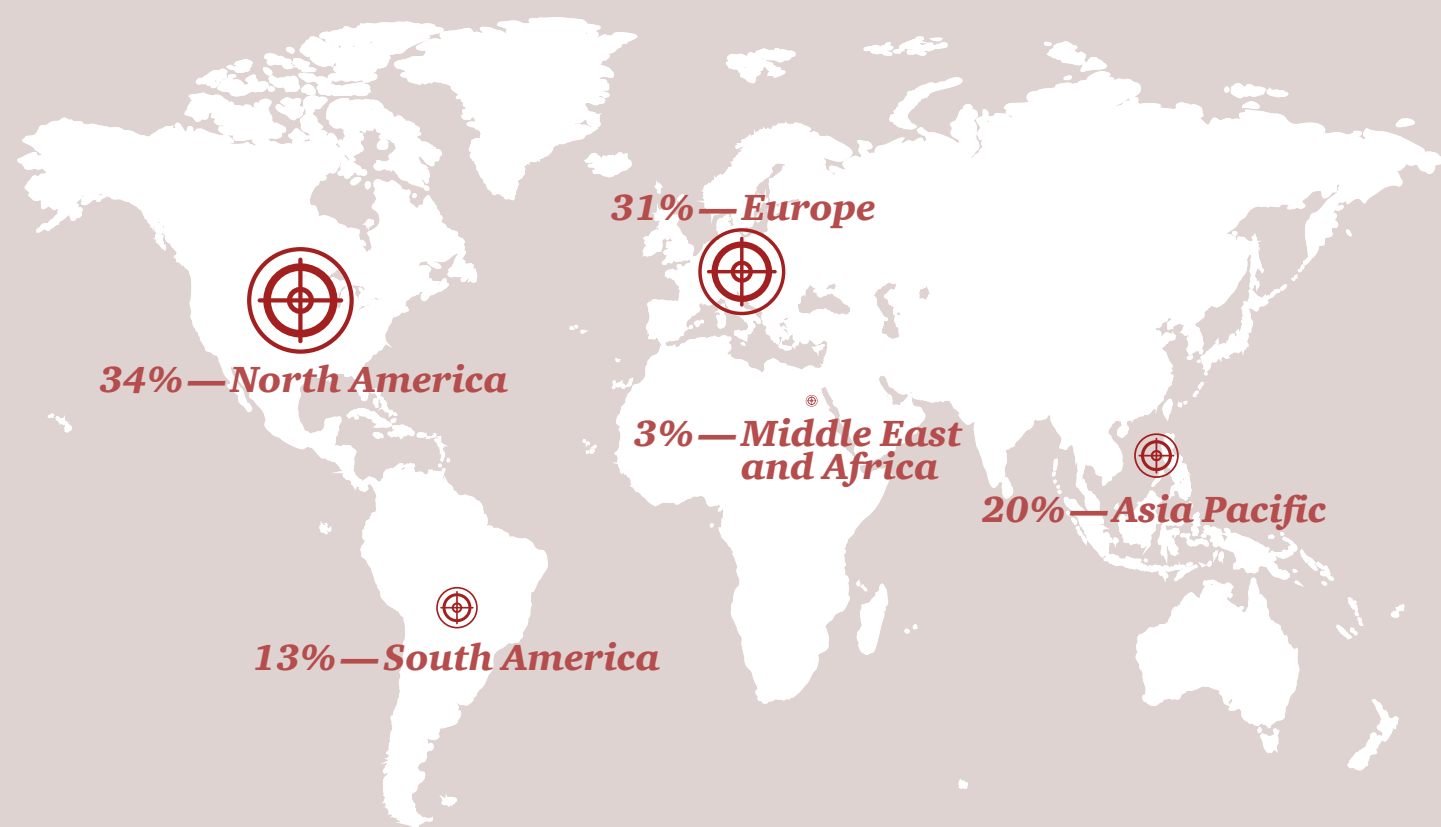
A strategic, carefully considered combination of the right technologies, processes and people skills can help organizations protect themselves by building more resilient cybersecurity capabilities. That, ultimately, can improve trust and create competitive advantages.

Methodology

The Global State of Information Security® Survey 2017 is a worldwide study by PwC, CIO and CSO. It was conducted online from April 4, 2016 to June 3, 2016. 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 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices from more than 133 countries.

Thirty-four percent (34%) of survey respondents are from North America, 31% from Europe, 20% from Asia Pacific, 13% from South America and 3% 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

Andrew Gordon

Partner

andrew.n.gordon@au.pwc.com

Steve Ingram

Partner

steve.ingram@au.pwc.com

Austria

Christian Kurz

Senior Manager

christian.kurz@at.pwc.com

Belgium

Filip De Wolf

Partner

filip.de.wolf@be.pwc.com

Brazil

Edgar D'Andrea

Partner

edgar.dandrea@br.pwc.com

Canada

David Craig

Partner

david.craig@ca.pwc.com

Sajith (Saj) Nair

Partner

s.nair@ca.pwc.com

Richard Wilson

Partner

richard.m.wilson@ca.pwc.com

China

Megan Haas

Partner

megan.l.haas@hk.pwc.com

Ramesh Moosa

Partner

ramesh.moosa@cn.pwc.com

Kenneth Wong

Partner

kenneth.ks.wong@hk.pwc.com

Denmark

Christian Kjær

Director

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@de.pwc.com

India

Sivarama Krishnan

Partner

sivarama.krishnan@in.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 Erik Fjørtoft

Partner

lars.fjortoft@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

Vincent Loy

Partner

vincent.j.loy@sg.pwc.com

Jimmy Sng

Partner

jimmy.sng@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

South East Asia

Jimmy Sng

Partner

jimmy.sng@sg.pwc.com

Spain

Javier Urtiaga Baonza

Partner

javier.urtiaga@es.pwc.com

Elena Maestre

Partner

elena.maestre@es.pwc.com

Sweden

Martin Allen

Director

martin.allen@se.pwc.com

Rolf Rosenvinge

Director

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

Neil Hampson

Partner

neil.r.hampson@uk.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/cybersecurity

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 223,000 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.

©2017 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 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.