CEOs face test of resilience in 2019 as geopolitical cyber activity picks up

Geopolitical cyber activity is heating up, increasing the costs for businesses and nations. Resilience could set your organization apart at a time like this.

Here's what you need to know and do now.

March 2019

pwc

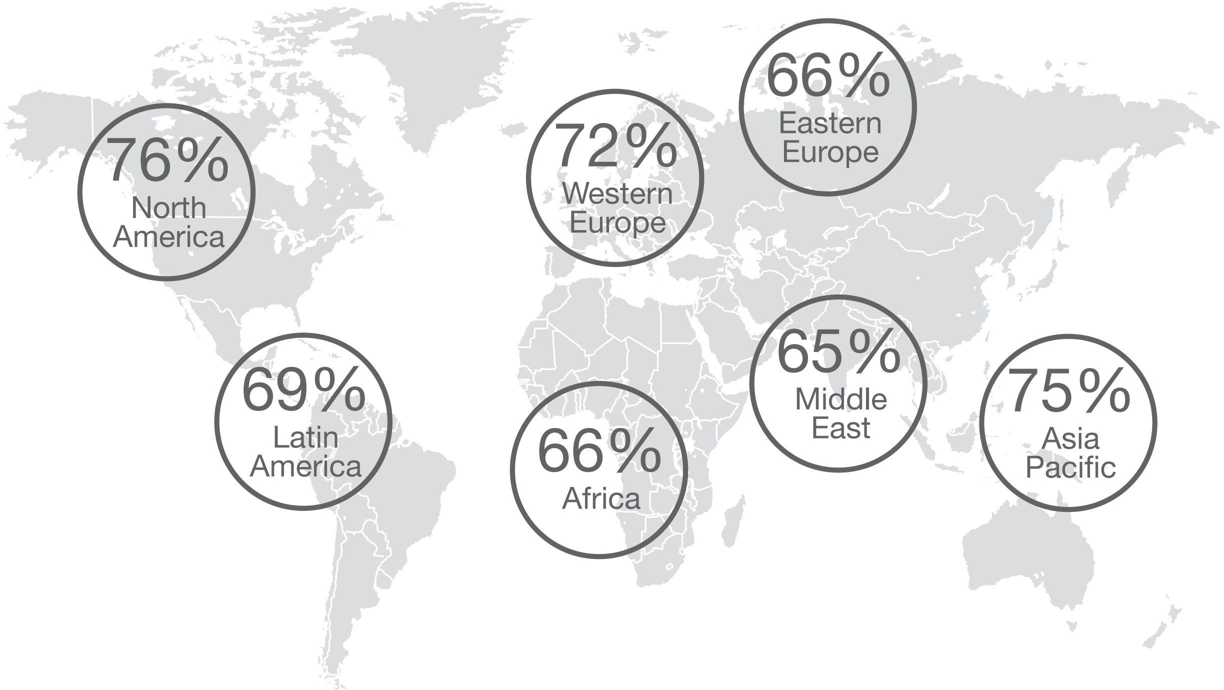
pwc.com/us/CEOresilience

There is a powerful and mysterious threat keeping business leaders awake at night: geopolitical cyber activity. Almost three quarters of CEOs who participated in PwC's 22nd Annual Global CEO Survey say their company may be affected by geopolitical cyber activity. And yet only 15% strongly assert their company is cyber resilient.

State and non-state actors are honing cyber weapons into cheap but effective—and unpredictable—geopolitical instruments.[1] Criminal threats like "ransomware," for example, are being refashioned into agents of chaos.[2] A sure way to hurt a country is to attack its economy and business. The power of these threats may not be obvious when headlines first report their awkward names, like WannaCry and NotPetya, but it is clear from the aftermath. NotPetya amounted to the most costly and destructive cyberattack in history, according to the White House. There is no telling how long that record will stand, but it is surely temporary. A recent study pegs the cost of a global ransomware cyberattack in a severe hypothetical scenario at $193 billion (compared to NotPetya's estimated cost of $10 billion).[3]

72% of CEOs worldwide say their company may be affected by geopolitical cyber activity.

In some regions, the figure is even higher.



Source: PwC's 22nd Annual Global CEO Survey
Base: All respondents 1,378

[1] European Political Strategy Centre, Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level, May 2017.
[2] Cambridge Centre for Risk Studies, 2018; Global Risk Index 2019 Executive Summary, Cambridge Centre for Risk Studies, University of Cambridge. Ransomware attacks are "increasingly being used for strategic and political reasons rather than financial gain," report states.
[3] Cambridge Centre for Risk Studies, Lloyd's of London and Nanyang Technological University, Bashe attack: Global infection by contagious malware, 2019.

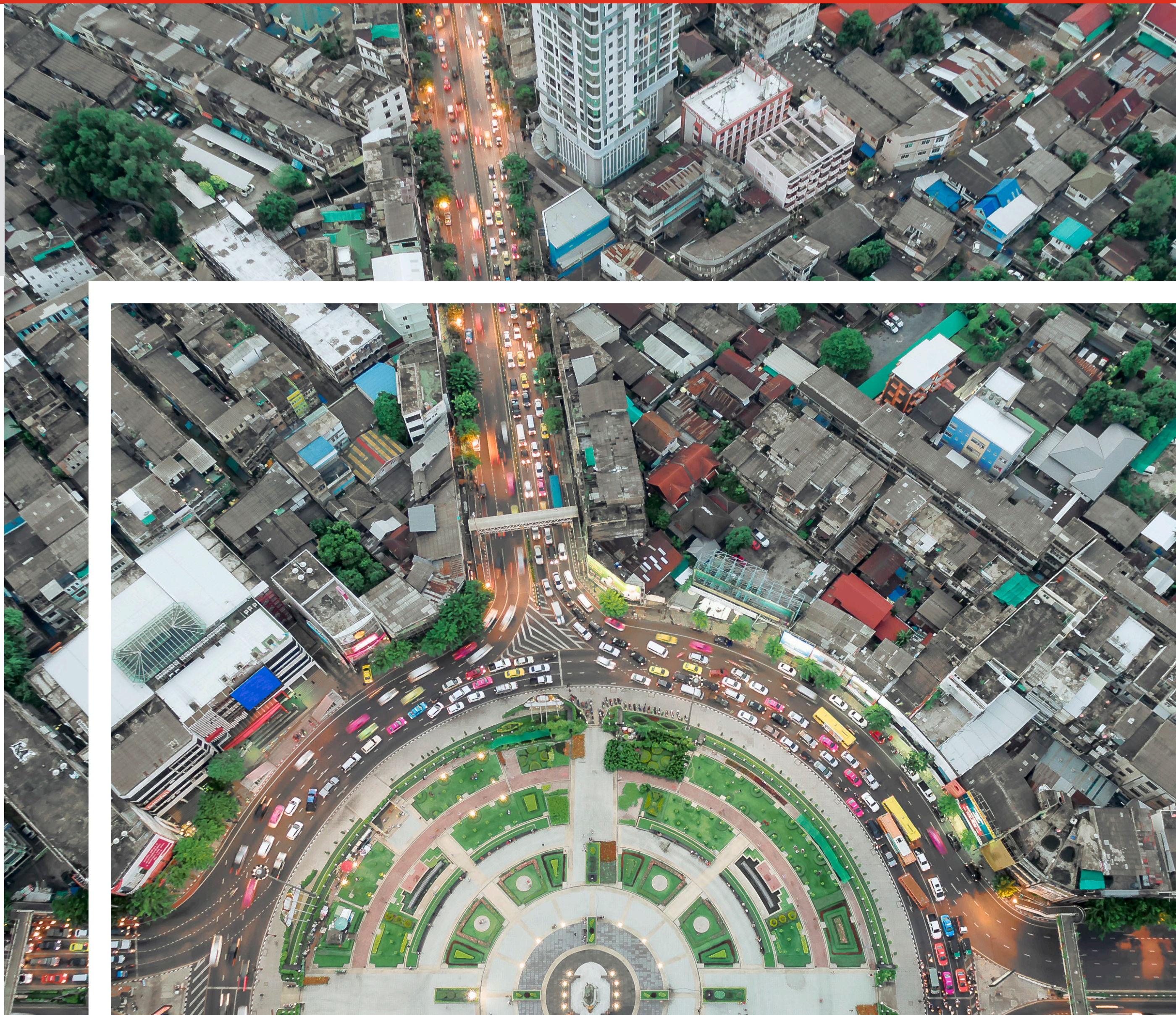
How your digital resilience could be tested in 2019

Here are three ways in which your resilience could be tested this year—and beyond.

1.
Digital daggers

Rising tensions among the world's major powers could embolden geopolitical actors in the shadows of cyberspace. Large majorities of respondents to the World Economic Forum's latest annual survey on global risks anticipate "political confrontations between major powers" (85%), cyber-enabled data theft (82%) and cyberattacks that disrupt operations and infrastructure (80%) in 2019.

Don't expect any declarations of "cyberwar"—this isn't about large-scale conflict. Think instead of digital "cloak and dagger." Without warning, lurking adversaries can unsheath concealed, silent weapons to undermine economies, critical infrastructure, and public trust in vital systems. These insidious attempts at "punishment, subversion, or coercion" pose the greatest risk to cyber stability.[4] Your company could be targeted if it owns or operates critical infrastructure, or it could be affected if those on which it relies are attacked. If your operations are disrupted, you may not only incur financial losses but also encounter challenges with insurance claims. The cloak-and-dagger nature of cyberattacks may spur some insurers to deny coverage based on an act-of-war exclusion.



[4] Strategic Studies Quarterly, Confidence Building Measures for the Cyber Domain, vol. 12, no. 3, 2018, pp. 10–49.

2. Cyber deterrence

Policymakers are experimenting with stronger measures to fend off cyberattacks. The European Union is considering plans for cyber sanctions, a tool previously used by the US government. The Trump administration's new cyber strategy, meanwhile, puts greater emphasis on US government offensive cyber operations, including threats to punish actors who dare target US critical infrastructure. To set clear red lines for "cyber deterrence," US officials may cite a new list of the most strategic risks to US critical infrastructure this year.

Although US "cyber deterrence" policy has moved from theory to practice, it is still in its infancy and being evaluated by Congress. Some industry leaders support the strategy's more proactive use of US government cyber capabilities to defend critical infrastructure. Critics of the strategy worry increased offensive hacking could spur adversaries to respond in kind. Researchers in this camp are developing a framework to help industry assess whether the new strategy deters or incites adversaries.

3. Greater accountability for resilience

Companies face rising expectations from governments to boost their resilience in the interest of national security. In the US, homeland security officials are creating new risk-management mechanisms to work with facilities deemed to be the "crown jewels" of critical infrastructure. Meanwhile in the European Union, a directive that went into effect in 2018 requires providers of essential services to be resilient to cyberattacks. It's the first time the EU has legislated on cybersecurity. Related UK guidance puts a new onus on companies to use lessons learned from incidents to update and retest response plans as needed. Other government agencies, including the Monetary Authority of Singapore, are also developing new requirements for cyber resilience.

Shoring up digital resilience

A PwC study of hundreds of incidents involving cyber and operational failures has identified the common root cause in most cases: the dependence on a highly **siloed** and **reactive** approach to digital resilience.

Businesses cannot count on an inconsistent web of solutions, policies, and procedures in a crisis, certainly not when attacks are becoming more sophisticated and the window for the right response is getting shorter. An organization cannot protect what matters most based on an ad-hoc inventory of digital assets. And if it doesn't understand the interdependencies that underpin its business operations—for example, across its supply chain—it cannot mitigate the risks.

The current state of unpreparedness is captured in the sentiments of CEOs and cybersecurity and privacy executives. Only 41% of business leaders are very comfortable their organization is building resilience to cyberattacks to a large extent, according to PwC's Fall 2018 Digital Trust Survey.

Before a crisis threatens to halt your business operations, your organization should have in place the right capabilities to swiftly defend against cyberattacks and recover from any disruption. With the right approach, you can avoid quickly mounting financial losses, build trust in the marketplace and position your company to gain a competitive advantage by bouncing back faster and stronger than your competitors.

only
35%

of business leaders are very comfortable their company has adequately tested its resistance to cyberattacks

only
34%

of business leaders are very comfortable their company has adequately tested its cyber-incident response plan

only
31%

of business leaders are very comfortable their company has identified those parties who might attack the company's digital assets

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

Three steps to take in 2019

To address the effects of geopolitical cyber activity, you should shore up your digital resilience.

1. Assess your digital resilience

Conduct a review of your business architecture to understand how critical processes could be vulnerable to failure—and how they might recover in the event of disruption. Have you minimized single points of failure due to reliance on a single technology or provider? That is just one of many questions you should be asking. Assessing the adequacy of your digital resilience approach against external benchmarks and frameworks can help identify deficiencies and prioritize your triage approach. Your review should also scrutinize crisis-response capabilities.

2. Design resilience into your operations

First, replace your patchwork of solutions, policies and procedures with an integrated approach to designing, assessing and maintaining a digital resilience program.

Next, become proactive instead of reactive. Take a dynamic data-driven approach to developing defensive and recovery capabilities, testing key safeguards, and identifying potential malicious actors. Identify particular elements—including applications, information and networks—that need to be resilient and implement needed improvements. Use leading tools such as the constant monitoring of technology infrastructure to help enable high availability, disaster recovery, and data integrity. And verify with your insurance providers that your policies have high thresholds for triggering the act-of-war exception.

3. Contribute to global dialogue on resilience and cyber stability

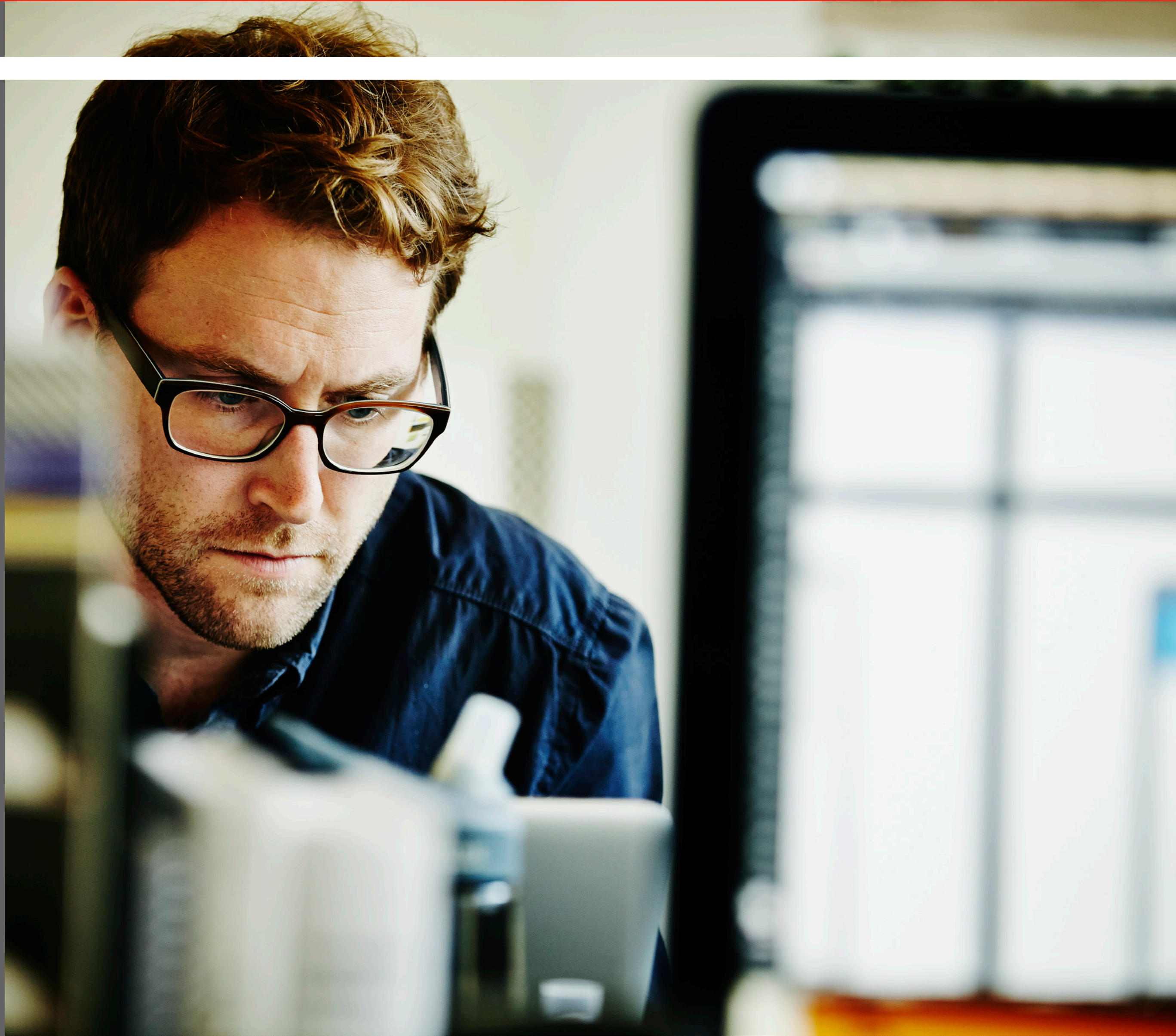
Businesses have a role to play in public-private efforts to build stability in cyberspace. There are concrete things you can do. Your company may be able, for example, to help build a global consensus on key concepts, terms and definitions describing how actors operate in cyberspace.[5] Your organization may possess technical knowhow that could help improve the sharing of cyber threat information through standards and confidence-building measures. You can participate in discussions convened by entities such as the World Economic Forum's Centre for Cybersecurity to turn principles for resilience, security and stability into practice.

[5] Strategic Studies Quarterly, Confidence Building Measures for the Cyber Domain, vol. 12, no. 3, 2018, pp. 10–49.

Your resilience playbook in a nutshell

- In the wider context of a cyber risk management program, assess your business architecture to uncover gaps in digital resilience.
- Apply automation to create an evergreen inventory of key processes and assets and to map dependencies based on network and endpoint data.
- Use scenario planning and information sharing to identify threats and risks.
- Establish a readiness program that uses exercises to support continuous improvements.
- Seek opportunities to contribute to global discussions on resilience and stability in cyberspace.

Cyberattacks are often mounted from places where the line between state and non-state actors is blurry. Growing expertise in both the private and public sectors means no organization, including yours, needs to face these challenges alone. Businesses and governments must start to collaborate in new ways to strengthen national—and global—resiliency.



pwc.com/us/CEOresilience

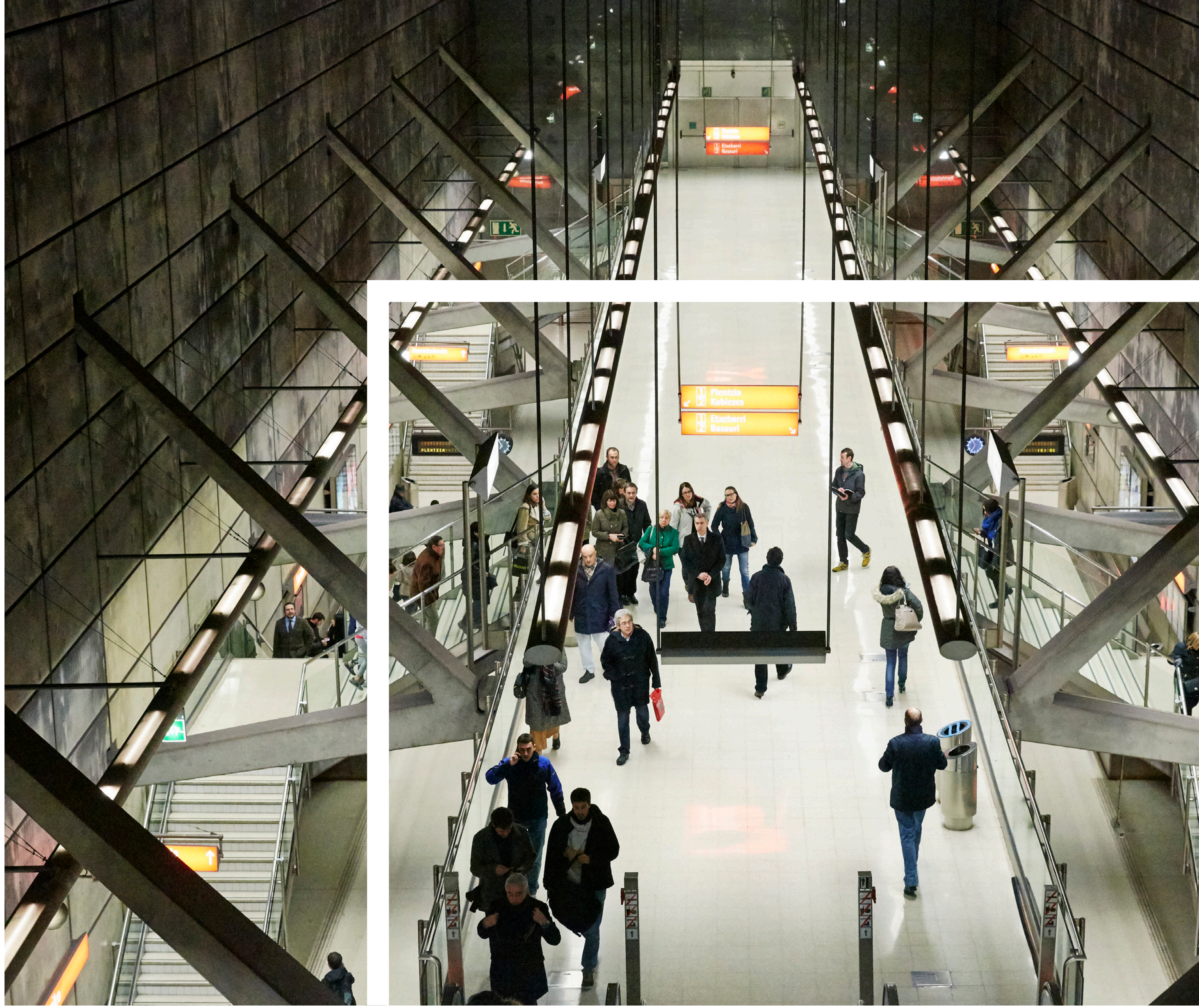
PwC Cybersecurity and Privacy contacts in Spain

Jesús Romero
Socio responsable de Soluciones de Seguridad de Negocio
jesus.romero.bartolome@pwc.com

Javier Urtiaga
Socio responsable de Ciberseguridad-Soluciones de Seguridad de Negocio
javier.urtiaga@pwc.com

Israel Hernández
Socio responsable de Sector Financiero-Soluciones de Seguridad de Negocio
israel.hernandez.ortiz@pwc.com

www.pwc.es/bss



At PwC, our purpose is to build trust in society and solve important problems. PwC is a network of firms in 158 countries with more than 250,000 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/us.