McKinsey & Company

Public and Social Sector Practice

Follow the leaders: How governments can combat intensifying cybersecurity risks

It is undoubtedly challenging to craft and execute a national cybersecurity strategy. Our research reveals common elements of successful strategies.

by Ankit Fadia, Mahir Nayfeh, and John Noble

September 2020

Against a backdrop of escalating geopolitical and geo-economic tensions, one of the biggest threats nations face today is from state-sponsored cyber warfare. From election interference to the alleged attempted theft of sensitive COVID-19 vaccine research to power-supply cutoffs for nearly a quarter-million people, state-sponsored cyberattacks are infiltrating the critical infrastructure of countries around the world.

Not just state actors but also nonstate actors today have more technical prowess, motivation, and financial resources than ever before to carry out disruptive attacks on a country's critical infrastructure. Any attack on critical infrastructure in one sector of a country can lead to disruption in other sectors as well. An attack on a country's telecommunications , for example, may disrupt electronic payments.

But this is just part of the problem. Today, individuals and businesses are more dependent than ever on digital connectivity in virtually every aspect of their existence. Most people cannot imagine going even a few hours without access to the internet. Globally, an estimated 127 new devices connect to the internet every second.[1] Any disruption in digital connectivity is considered an obstacle in the path of progress.

Owing to the COVID-19 pandemic, our dependence on all matters digital has increased dramatically. With remote working having become integral to our economies and the medical response, the rising dependence of citizens and businesses on everything digital is only going to continue.

With every new device, user, and business that connects to the internet, however, the threat of cyberattacks increases. If a government cannot provide secure and trusted digital connectivity, societies can't prosper and economies won't thrive.

As a result, more than 100 governments have developed national cybersecurity defense strategies to combat the cybersecurity risks that their citizens, businesses, and critical infrastructure face. To help up-and-coming governments, we studied and benchmarked the cybersecurity strategies of 11 nations (see sidebar, "About the research").

While countries have taken a wide variety of approaches to cybersecurity defense, we have identified five common elements of successful national strategies. We explore those strategies in this article. The dangers relating to cybersecurity are constantly evolving, and the stakes are high. Governments that focus their efforts in these five places might be in a better position to prevent cyberattacks, mitigate their damage, and better protect their citizens, businesses, and critical infrastructure.

[1] Mark Patel, Jason Shangkuan, and Christopher Thomas, "What's new with the Internet of Things?," May 10, 2017, McKinsey.com.

About the research

No government can eliminate all possible threats. But some have excelled in creating, implementing, and refining national cybersecurity defense strategies. We identified those governments based on these two criteria:

1. Global Cybersecurity Index (GCI) rank. The International Telecommunication Union publishes the GCI, which "measures the commitment of countries to cybersecurity at a global level—to raise awareness of the importance and different dimensions of the issue."[1] To qualify for our study, countries needed to be ranked in the GCI's top 30 in 2018. Many experts believe that the GCI's methodology has room for improvement. Still, it is the only global index measuring cybersecurity maturity of countries that has gained traction

[1] Global Cybersecurity Index, International Telecommunication Union, itu.int.

About the research (continued)

and is actively used by several countries to measure their own progress.

2. Network Readiness Index (NRI) rank. Published by the Portulans Institute, the NRI assesses the progress and readiness of technology adoption in countries around the world in terms of technology, people, governance, and impact. To qualify for our study, countries needed to be ranked in the top 30 of the NRI.[2]

Together, these criteria help to identify nations that are combating cybersecurity risks through comprehensive efforts at a national level. We are not evaluating the countries on their performance but choosing a few that might have lessons for other countries around the world. These nations have invested considerable resources to improve their cybersecurity. Based on this methodology, the following countries were included for our benchmarking analysis: Australia, Canada, China, Estonia, France, Germany, Israel, Singapore, South Korea, the United Kingdom, and the United States (exhibit).

We made exceptions for China and Israel. We believe China is a worthy addition given its sheer scale and the progress it has made in digital innovation across sectors in recent years. Similarly, in the past five years, Israel's cybersecurity ecosystem has grown faster than nearly any other in the world. Israel accounts for less than half a percent of global GDP, but in 2018 a whopping $1.2 billion—nearly 20 percent of worldwide venture-capital investment in cybersecurity—went to Israeli cybersecurity start-ups.[3]

[2] Soumitra Dutta and Bruno Lanvin, eds., *The Network Readiness Index 2019: Towards a future-ready society,* Portulans Institute, 2019, networkreadinessindex.org.
[3] Nir Falevich, *Cybersecurity Report 2019: Key Insights into israeli cybersecurity—looking back at 2018, moving into 2019,* Start-Up Nation Central, startupnationcentral.org.

Exhibit

The cybersecurity strategies of 11 leading benchmark countries from around the world were analyzed.

Benchmark countries	GCI 2018 (score, rank)[1]	NRI 2019 (score, rank)[2]
Australia	0.890, #10	74.80, #13
Canada	0.892, #9	74.72, #14
China	0.828, #27	57.63, #41
Estonia	0.905, #5	69.30, #23
France	0.918, #3	73.42, #18
Germany	0.849, #22	78.23, #9
Israel	0.783, #39	70.86, #22
Singapore	0.898, #6	82.13, #2
South Korea	0.873, #15	73.84, #17
United Kingdom	0.931, #1	77.73, #10
United States	0.926, #2	80.32, #8

[1] *The Global Cybersecurity Index 2018* (GCI) is a composite index produced, analyzed, and published by the International Telecommunication Union to measure the commitment of countries to cybersecurity in order to raise cybersecurity awareness.
[2] *The Network Readiness Index 2019* (NRI), published by the Portulans Institute, maps the network-based readiness landscape of 121 economies based on their performances across 62 indicators across four pillars: technology, people, governance, and impact.

Principal elements of a comprehensive national cybersecurity strategy

These are the five elements of successful national cybersecurity strategies:

— A dedicated national cybersecurity agency (NCA)

— A National Critical Infrastructure Protection program

— A national incident response and recovery plan

— Defined laws pertaining to all cybercrimes

— A vibrant cybersecurity ecosystem

Dedicated national cybersecurity agency

Best-in-class countries give a single entity—usually referred to as a national cybersecurity agency—the overall responsibility of defining and driving the cybersecurity agenda of the entire country. This involves developing a cohesive national cybersecurity strategy with a portfolio of initiatives, among them protecting the critical infrastructure of the country, mobilizing the response to cyber incidents, defining cybersecurity standards, improving the cyber awareness of citizens, and developing the cybersecurity capabilities of professionals.

Fulfilling these responsibilities requires the NCA to have adequate in-house technical skills and expertise. To fill any capability gaps, the NCA typically partners with and mobilizes other government entities as well as the private sector. The United Kingdom's National Cybersecurity Agency, for instance, works closely with other government entities, such as the Department for Digital, Culture, Media & Sport, to improve capabilities of the cybersecurity professionals in the country.

When setting up an NCA, countries can consider design choices, such as:

— Should the agency reside within a defense and intelligence entity or within a civilian body?

— What level in the government does the agency report to?

— What is the scope of the agency's control and oversight (for example, does it focus only on critical infrastructure or also on citizens and small and midsize businesses)?

Approaches to these design choices vary even among leading countries but typically reflect a country's political philosophy, federal government structure, maturity of cyber capabilities, and overall cybersecurity aspirations.

National Critical Infrastructure Protection program

If an NCA could only focus on one aspect of cybersecurity, it should be protecting the critical infrastructure of the country. Critical infrastructure is typically the most attractive target for hostile state actors. Disruption to critical infrastructure can have an impact on the economy, business confidence, society, and even overall national security. Critical infrastructure typically consists of both information technology and operational technology, which makes it harder and more complicated to protect. Our study found that the best-in-class National Critical Infrastructure Protection programs focus on the following three success factors:

Prioritized critical sectors and assets. A country typically determines whether a sector is critical based on how significant a role it plays in ensuring the health of the economy, well-being of the society, and national security of the country. For example, the European Union's Network and Information Security (NIS) directive considers energy, transport, digital infrastructure, healthcare, and water critical sectors to protect. Our global benchmark analysis of 11 countries reveals that the majority of those countries have identified 11 critical sectors, ranging from energy (oil, gas, and nuclear power) to healthcare and emergency services.

Typically, an NCA works with the regulator of each critical sector to prepare criteria for what should constitute critical assets in that sector. For example, in the United Kingdom, the Department for Business, Energy & Industrial Strategy considers any company that supplies electricity to more than 250,000 final customers to be critical.

Globally recognized cybersecurity standards to protect critical assets. Best-in-class countries recommend that organizations in critical sectors comply with globally recognized cybersecurity standards, such as the ones defined in the US National Institute of Standards and Technology's Cybersecurity Framework. Employing a globally accepted standard makes it easier for organizations to comply since it's likely that their cybersecurity teams are already familiar with it. Similarly, the European Union's NIS directive aims to achieve a common, high level of network- and information-systems security across all critical-sector entities in EU countries.

Robust governance mechanism. In many countries, tension exists between the regulating entity and the enforcement entity. This is the reason why it is critical to the success of the National Critical Infrastructure Protection program that a robust governance mechanism be in place between the NCA, which formulates the strategy, governance, and technical standards of a country's overall National Critical Infrastructure Protection program, and the sector regulators, which are responsible for creating awareness about and enforcing the cybersecurity standards in their respective sectors.

To meet the unique needs of specific sectors, regulators in some countries may recommend additional sector-specific cybersecurity standards as well. In the United States, to secure credit-card transactions and related personally identifiable data, all companies that handle card payments must comply with the Payment Card Industry Data Security Standard. To ensure compliance, sector committees typically audit sectoral entities on a periodic basis and may choose to apply incentives or penalties.

National incident response and recovery plan

Cyberattacks are inevitable, so every government needs to develop a national incident response and recovery plan to mitigate the effects of cyber incidents and improve recovery time. Our study found that the best-in-class plans focus on six important elements:

Clearly defined reporting procedure for citizens and businesses. Best-in-class countries clearly define to whom their citizens and businesses should report cyber incidents. For example, in the United Kingdom, the National Cyber Security Centre (NCSC) is a single point of contact for all businesses—and, increasingly, citizens—to report cyber incidents. In the back end, it is critical to build a centralized repository across government entities that captures data related to all cyber incidents in the country. This will enable governments to gather insights and intelligence and respond more effectively to cyber incidents.

Active monitoring for cyberthreats. In addition to passively recording all reported cybercrimes, governments must actively monitor the internet for cyberthreats. For example, 24 hours a day, seven days a week, the US National Security Operations Center monitors security threats entering the United States and combines network patterns with existing national-security intelligence to assess threats.

Multiple sources of threat intelligence. To supplement traditional sources of threat intelligence, best-in-class governments establish additional channels. For instance, in 2013 the United Kingdom launched the Cyber Security Information Sharing Partnership, which features a platform where the government and the private sector can share threat intelligence quickly and confidentially.

Proactive efforts to combat cyberthreats. Best-in-class countries use data from both active and passive sources to initiate actions to combat cyberthreats facing the country. For example, the NCSC in the United Kingdom launched the Active Cyber Defence initiative to tackle cyberthreats in an automated and scalable manner. If a threat such

as malicious content is detected on a website, the NCSC proactively blocks it across the entire country and works with the hosting company to take it down.

Standardized severity-assessment matrix. The benchmark countries classify each cyber incident based on its severity in terms of loss of life, national security, public confidence, type of victim, and interdependence, among other dimensions. The hacking of a major bank may be classified as a high-severity incident, while the hacking of a small business may be classified as a low-severity incident. A standardized matrix provides all incident respondents with a common language for cyber incidents of different severity levels.

Robust mobilization plan to respond effectively to cyber incidents. In conjunction with the severity-assessment matrix, each country should develop a robust mobilization plan that defines which government entities should respond to a cyber incident and what role each should play. The responding agencies typically vary depending on the severity level of the incident. In the event of a low-severity incident, such as a small enterprise being hacked, the local police might respond and the NCA might share guidance on its portal for the benefit of other small and midsize enterprises. However, in the event of a national emergency, such as the targeting of a power grid, multiple government entities are expected to respond—including the police, energy-sector regulators, intelligence agencies, and the NCA itself. Depending on the consequences of the attack, there may also be a requirement for political leadership.

Framework of cybersecurity laws

As governments develop cybersecurity laws to prevent, investigate, and take actions against cybercrimes, they should focus on two success factors:

Robust substantive and procedural cybersecurity laws. Governments need to decide which aspects of cybersecurity they want to legislate and which aspects they want to provide guidance on without necessarily imposing any legal penalties. One good option while developing national cybersecurity laws is to embrace the guidelines laid out by the Budapest Convention—an international treaty governing cyberlaws agreed upon by more than 60 countries.

The Budapest Convention recommends that countries enact two categories of laws: substantive and procedural. Substantive laws define different types of possible cybercrimes—including copyright infringement, computer-related fraud, child pornography, and violations of network security—and the corresponding punishment. The procedural laws define the authority and responsibilities each country must keep in mind while implementing the laws. Both substantive and procedural laws need to be refreshed regularly to keep up to date with the ever-changing landscape of cybercrime.

International cooperation and collaboration. The transnational nature of cybercrime makes it critical for governments to participate in global forums, establish intelligence- and threat-sharing partnerships with other countries, and collaborate on preventing and investigating cybercrimes.

Vibrant cybersecurity ecosystem

Without help from citizens, professionals, and private-sector organizations, a government alone will not have the scale to improve the overall cybersecurity of its entire country. Best-in-class governments enable cybersecurity companies to thrive, develop the capabilities of cybersecurity professionals, and raise citizens' cyber awareness by focusing on three priorities:

Vibrant ecosystem of cybersecurity companies and entrepreneurs. Best-in-class countries have a vibrant ecosystem of accredited cybersecurity service providers, training providers, and entrepreneurs. Such an accreditation program not only pushes companies to improve their overall service but also helps customers differentiate between genuine and fly-by-night providers. For example, the United Kingdom's NCSC runs accreditation programs to certify cybersecurity consultancies, training providers, and professionals in the country. To expand its cybersecurity private sector, Israel's National Cyber Directorate has invested heavily in the

past decade in supporting education, research and development, and innovation in various cybersecurity fields—with impressive results (exhibit).

National cybersecurity workforce. A study of the global information-security workforce estimated that the world will fall 1.8 million short of the number of cyber-skilled individuals needed by 2022.[2] This means that governments need to proactively train, upskill, and refresh the cyber capabilities of professionals throughout both the public and private sectors. This is typically done using a combination of these models:

– *Partnering with formal educational institutions.* In the United Kingdom, the NCSC has certified 24 master's degrees, three integrated master's degrees, and five bachelor's degrees in cybersecurity from 23 universities as part of its program to recognize high-quality courses. In the United States, since its inception in 2001, the CyberCorps Scholarship for Service program has had approximately

[2] "Global cybersecurity workforce shortage to reach 1.8 million as threats loom larger and stakes rise higher," (ISC)², June 7, 2017, isc2.org.

Exhibit

Israel has a formidable cybersecurity ecosystem.

Supporting entities	National Cyber Agency National Cyber Directorate National Innovation Agency	Ministry of Economy Office of the Chief Scientist
Major initiatives	**Business support**	Developed initiative to promote cybersecurity companies in country and also facilitate funding for companies
	Innovation	Set up dedicated cybernetics and cybersecurity facility to promote innovation in cybersecurity; bring together academia, private-sector enterprises, and defense forces
	Education	Launched national program to increase number of cybersecurity professionals in country by coordinating cybersecurity and other tech-related educational curricula to promote skilled talent pool in economy
	Financing access	Established dedicated ~$25 million funding program to encourage research and development activity in cybersecurity companies in 2015

Observed impact[1]	~450	~$1.2 billion	~$418 million	~$6 million	~20%
	Active cybersecurity companies in 2018	Investments in cybersecurity sector in 2018	Total value of exits in 2018[2]	Median size of investment rounds in cybersecurity in 2018	Share of global venture-capital investments in cybersecurity in 2018

[1] Based on data in Nir Falevich, *Cybersecurity Report 2019: Key insights into Israeli cybersecurity—looking back at 2018, moving into 2019*, Start-Up Nation Central, startupnationcentral.org.
[2] Based on value of six out of 12 exits (first-time deals, including initial public offerings, and buyouts) that were disclosed in 2018.
Source: Israel Ministry of Foreign Affairs; Start-Up Nation Central; McKinsey analysis

3,600 graduates find placements in more than 140 government entities. Today, there are approximately 70 active institutions that participate in the CyberCorps scholarship program.

– *Establishing a central training portal.* The US Department of Homeland Security provides free online cybersecurity training to federal, state, and local government employees and contractors through its Federal Virtual Training Environment portal.

– *Leveraging private-sector training providers.* Many countries, such as Israel, provide incentives to attract global private-sector training companies to set up centers and offer courses.

In addition to these three models of workforce development, best-in-class countries connect with students when they are young and encourage them to pursue a career in cybersecurity. For example, the NCSC's CyberFirst program aims to help young people explore their passion for cybersecurity through competitions, courses, and apprenticeships.

Cyber-aware citizens. The role of an NCA is to ensure that citizens are receiving consistent and clear guidance on how to combat cyberrisks. The UK government runs the Cyber Aware campaign to help individuals, families, and smaller organizations by providing simple guides on topics ranging from staying secure online to protecting data and devices.

While the world's best NCAs have comprehensive strategies, it is not possible for a single organization to deliver all the components of a strategy on its own. Partnerships that involve other players in the cybersecurity ecosystem—including those in the private sector, academia, and other public-sector areas, both local and international—are essential to combat the cybersecurity risks of a country.

Beyond governments and across borders, the digital age connects us all. The security of all users—and the well-being of societies and economies around the world—depends on a concentrated effort to thwart the increasingly costly and threatening cyberrisks that undermine the world order. To protect this interconnected world, countries can establish national cybersecurity agencies and strategies based on lessons gleaned from the experience of many countries over several decades.

Ankit Fadia is an associate partner in McKinsey's Dubai office, **Mahir Nayfeh** is a partner in the Abu Dhabi office, and **John Noble** is an external adviser to McKinsey.