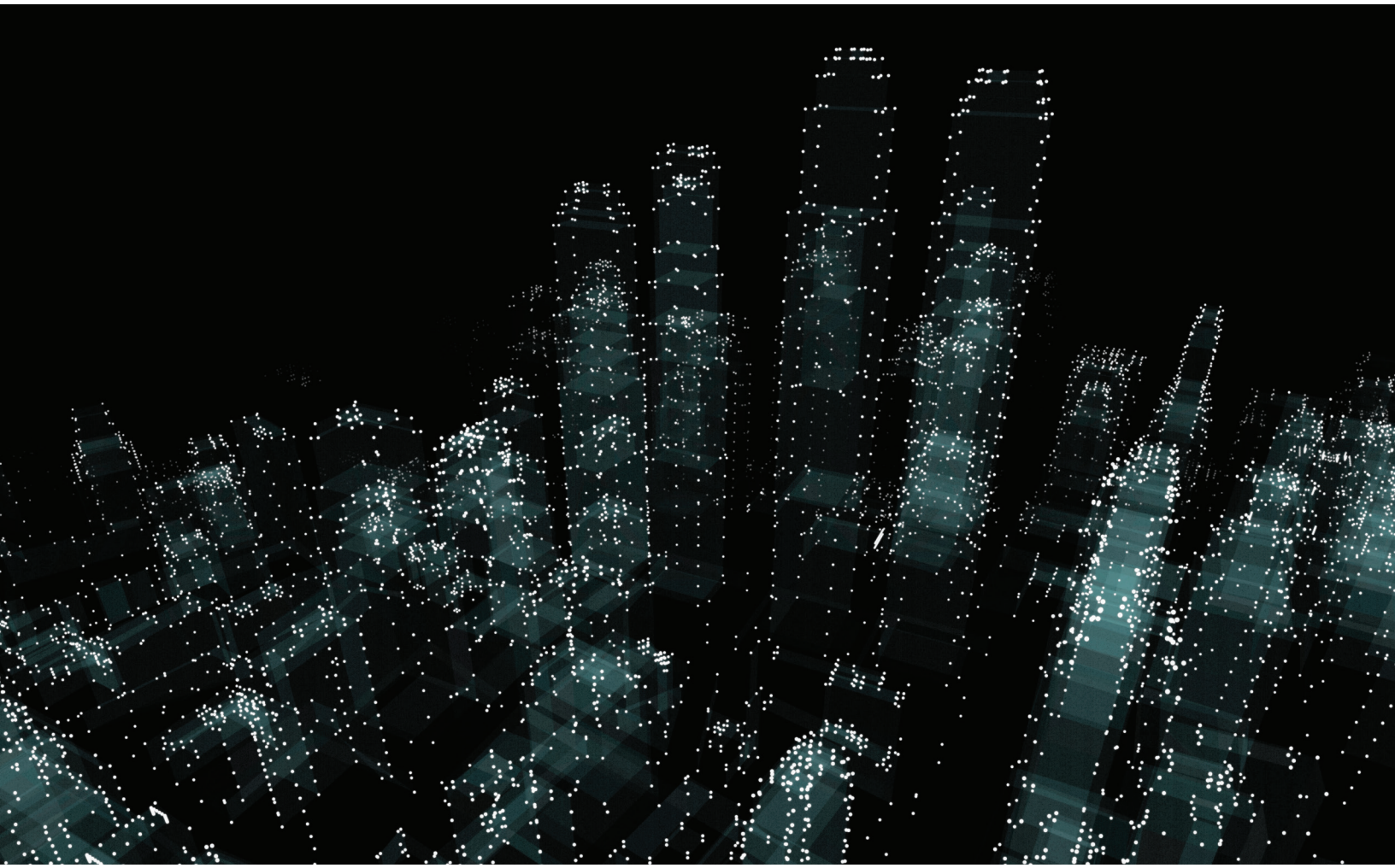
McKinsey&Company

Asking the right questions to define government's role in cybersecurity

There is no one-size-fits-all approach for governments to manage cybersecurity. But asking some key questions can help leaders get started.

Mary Calam, David Chinn, Jonathan Fantini Porter, and John Noble



SEPTEMBER 2018 • PUBLIC SECTOR

Government leaders are increasingly aware that promoting prosperity and protecting national security includes providing cybersecurity. That means demonstrating that a nation, state, region, or city is a safe place to live and do business online. And it includes deterring cyberattacks, preventing cyber-related crime, and protecting critical national infrastructure while also maintaining an environment that makes technological progress easy.

It is a tall order. National security and criminality are different—and multifaceted—in the digital arena. Tools developed by governments to provide security are seized, weaponized, and proliferated by criminals as soon as they are released. Malware-development utilities are available on the dark web, enabling criminal activity even by those with only basic digital skills. Cyberthreats cross national boundaries, with victims in one jurisdiction and perpetrators in another—often among nations that don't agree on a common philosophy of governing the internet. And complicating it all, criminal offences vary, legal assistance arrangements are too slow, and operating models for day-to-day policing are optimized for crimes committed by local offenders.[1] Even relatively low-level threats can have impact on a vast scale.

Each country is addressing the challenge in its own way, just as companies tackle the issue individually. Approaches vary even among leading countries identified by the Global Cybersecurity Index, an initiative of the United Nations International Telecommunications Union. Differences typically reflect political and legal philosophy, federal or national government structures, and how far government powers are devolved to state or local authorities. They also reflect public awareness and how broadly countries define national security—as well as technical capabilities among policy makers. Despite such differences, our work with public- and private-sector organizations suggests a series of questions government leaders can ask to assess how prepared they are.

Who is accountable?

An effective national cybersecurity ecosystem crosses traditional institutional boundaries and includes a wide range of departments, agencies, and functions, both military and civilian. Many countries have yet to clarify who is accountable across all dimensions of cybersecurity or to impose a single governance structure. That lack of clarity can result in a confused response to crises and inefficient use of limited resources.

In our experience, a single organization should have overall responsibility for cybersecurity, bringing operational activity and policy together with clear governance arrangements and a single stream of funding. Particularly when responding to a cyberattack, clarity of leadership and decision making is vital to ensure the correct balance among helping victims recover quickly, taking measures to protect others (by increasing resilience and attacking the source of the attack), and performing a criminal investigation of those responsible. While some national and state governments have consolidated accountabilities into a clear structure, such as Estonia's Cyber Security Council, or have well-established and tested crisis-response mechanisms that they have adapted for use in cyberevents, as in Sweden, many others do not.

Key skills are often in short supply. Knowledge of the threat, resources, and authority to make decisions may all sit in different places across government. This reduces operational effectiveness and can also result in weak legislation, bad policy, and lack of investment. Some countries are starting to address these challenges. Germany, for example, has strengthened its Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) to lead its national cybersecurity strategy and establish shared cybersecurity services for government.

The United Kingdom's National Cyber Security Centre (NCSC) is also widely cited as a model for

government-level cybersecurity. It brings together analysis, assessment, and crisis response to provide advice to critical national infrastructure organizations, businesses more broadly, and the public (exhibit). Its operating model involves both access to highly sensitive intelligence and dissemination of public information. And it brings together cybersecurity experts from government and the private sector in a single body.

Questions governments can ask include the following:

- Are lines of accountability and remits clear—both for policy and for crisis response?
- Is it clear how government priorities are decided and communicated?
- Is there a coherent, cross-government strategy? Is it reviewed and refreshed regularly?
- What performance metrics does the government have for the strategy? How are they monitored?
- What information does the government publish about progress on cybersecurity?
- Do the responsible parts of government come together regularly to agree on plans and review progress?

Exhibit

The National Cyber Security Centre leads the UK government's cybersecurity work.

Responsibilities:

- Protect the UK's critical services from cyberattack.
- Manage major cybersecurity incidents.
- Improve the underlying security of the UK internet through technological improvement and advice to citizens and organizations.

Sample functions:

- Develops knowledge and distills insight on cybersecurity into practical guidance for public consumption.
- Responds to cybersecurity incidents to reduce the harm they cause to people and organizations.
- Applies industry and academic expertise to build capability in the cybersecurity system.
- Secures public- and private-sector networks.
- Provides a single point of contact for government agencies, departments, and organizations of all sizes.
- Collaborates with law-enforcement, defense, intelligence, and security agencies and international partners.

Source: National Cyber Security Centre, ncsc.gov.uk

How centralized should you be?

Some countries have consolidated their audit and regulation functions in a centralized agency. Japan, for example, has its Cyber Security Strategic Headquarters, and Romania has its Association for Information Security Assurance. Others, such as India, have dispersed audit functions across multiple bodies. Both models can work, but as India's *National Information Security Policy and Guidelines* illustrates, a decentralized model—in this case, ministries are tasked to self-audit and bring in external auditors—requires clear national guidelines and standards. Israel's benchmarking and accreditation arrangements have also been key to raising standards across all sectors.

At the very least, governments can insist on reporting of cyberevents by victims and on sharing of vulnerabilities by suppliers into a single reporting, analysis, assessment, and response hub. In Germany, for example, federal legislators have sought to amend the law to require companies to register any cyberincidents in which they are a victim. Australia introduced a notifiable-data-breaches

scheme in 2017, making it a legal requirement to notify affected individuals and the Office of the Australian Information Commissioner of serious data breaches.[2] Ideally, governments will also make it easy for citizens and businesses to report such breaches through an automated platform to facilitate responses, advice, and feedback. Such platforms will also increase transparency around threats and steps to mitigate them.

Sectoral regulators have a more significant role to play in raising cybersecurity standards than has perhaps been recognized. There are moves toward a more regional approach to regulation, reflecting the cross-border digital world: for example, the EU Commission's proposals to develop a regionwide framework of cybersecurity standards.

Questions governments can ask include the following:

- To what extent do data protection and privacy regulations reflect the challenges of the digital age?
- How coherent is the approach to cyberregulation across different sectors of the economy and the wider information and communications technology supply chain? What advice does the government provide?
- Does the criminal law adequately address offenses committed online?
- How closely have policies and regulation been developed in partnership with private-sector operators who will be impacted?

How can you work with the private sector?

Governments do not have a monopoly on (or even the largest role in) cybersecurity. Open and trusting relationships with the private sector and academia are essential. Governments need commercial organizations to put more emphasis on cybersecurity, particularly as many companies operate across shared digital platforms. When companies and academic institutions have more knowledge, expertise, and capability, governments can work with them to develop the knowledge and tools needed to strengthen the ecosystem.

Many attacks could be prevented by basic security precautions and maintaining up-to-date patches, yet relatively few countries have invested significantly in education or training programs. One that has is Israel. Its investment in cybersecurity and integration of it into the educational curriculum, its extracurricular activities for high-school students, and its national military service have created a thriving, globally competitive, professional cybersecurity market. The Israeli government has also worked with the private sector, both to build capability and awareness and to grow the economy through the cybersecurity sector—by investing in R&D, for example.

Another example is Singapore, in which the National Cybersecurity R&D Programme supports public–private research partnerships. These are funded by $190 million Singapore dollars ($137.85 million) in the national strategy for developing research and the creation of the National Cybersecurity R&D Laboratory at the National University of Singapore.

And working with industry is also key to the United Kingdom's NCSC, where sharing of information and expertise includes a unique collaboration between a highly classified intelligence organization and the private sector. Its Cyber Essentials framework is a unified tool for assessing and guiding the development of cybersecurity for private-sector companies. Any company bidding for government contracts must confirm that it is compliant with the scheme. In conjunction with the Centre for the Protection of the National Infrastructure, NCSC also accredits companies under the government's cyberincident-response scheme as providers of technical-mitigation services.

Beyond that, few countries have made efforts to improve cybersecurity in small and medium-size businesses. These are likely to have the least resources and knowledge to build their own cybersecurity. Cybersecurity vulnerabilities in these companies can reduce their own economic value. But they can also be a weak link for bigger firms, creating vulnerabilities as they provide goods and services, including to governments.

Questions governments can ask include the following:

- To what extent does the government sponsor or invest in cybersecurity R&D?
- To what extent does the government support cybersecurity training, education, and awareness-raising for businesses, those in work, those in education, and those in the general population?
- Does the government engage the private sector or academia in its cybersecurity work? How effective are these partnerships?
- Does the government provide a platform for information sharing among organizations?
- What guidance on cybersecurity does the government provide to private-sector companies? How clear and coherent is that government advice to multiple stakeholders outside the government?

Are you operationally ready?

Countries vary dramatically in their ability to deal with cyberattacks and how they manage crises. It is often unclear how citizens and businesses should report cyberattacks or seek help. That confusion results in chronic underreporting and makes it hard to know the true scale of the problem and to build understanding to prevent future attacks.

To make matters worse, few countries yet have a workforce with sufficient cybersecurity skills to match demand. A study of the global information security workforce estimates that the world will fall 1.8 million short of the number of cyberskilled individuals needed by 2022.[3] Those who do have the relevant skills command premium salaries. And what cybersecurity skills others have are often concentrated in small pockets, such as in the intelligence agencies, and not available to governments more broadly. Most governments would do well to invest now in recruitment and training and to adopt more flexible approaches to recruitment and retention from outside traditional sources of talent. For the short term, consolidating existing scarce resources into a single place, as the United Kingdom's NCSC has done, can boost the value of available expertise, bringing the most highly skilled cyberexperts together as a single, government resource.

Some governments are taking a proactive stance on cyberdefense. From 2009, for example, the Australian government consolidated the internet gateways of various departments into seven certified "lead-agency gateways." These provide an initial foundation for consistent cybersecurity and a reduced attack surface.[4] The UK government launched a suite of initiatives in 2017 known as Active Cyber Defence, designed to "protect the majority of people in the UK from the majority of the harm caused by the majority of attacks, the majority of the time." As a result, UK-hosted phishing attacks fell by about 20 percent in the 18 months prior to February 2018, even as global volume itself rose by nearly 50 percent.[5]

Law-enforcement capabilities are often the least effective part of a government's response. Law-enforcement agencies spend up to 95 percent[6] of their budgets on staff, allowing only limited investment in technology. Staffing models are often highly traditional, making it more difficult to bring new technical skills into the organization at the scale and pace needed to address the volume of business that is cybercrime. Criminal-investigation

techniques, such as seizure of company servers in evidence, can hinder recovery from attack.

Questions governments can ask include the following:

- What are the emergency-response arrangements for a major cyberattack?
- Is there a national emergency-response team? Are there emergency-response teams for key sectors?
- What arrangements are there for the sharing of information to prevent and respond to a cyberattack? Are there clear reporting mechanisms for alerting the authorities to a cyberattack? What happens when a report is received?
- How often are response arrangements tested and exercised?
- How will the government ensure rapid recovery from a cyberattack?
- Which agency or agencies have responsibility for investigation of cyberattacks and online crime? What capabilities and capacity do those agencies have?
- What capabilities and capacity does the government have to gather intelligence on cyberthreats, assess them, and disseminate the analyses in a way that shapes action?

Where is multinational cooperation possible?

The transnational nature of cyberattacks means that even effective state or national coordination might not be sufficient. Mutual legal-assistance treaties were constructed for the predigital age, and mechanisms are too slow to keep pace with investigation of online crime. In 2013, a UN report on cybercrime estimated that mutual legal assistance took 150 days on average.[7]

Differences in political and ideological positions might make further progress on establishing international norms for the internet impossible. Instead, norms agreed by coalitions—such as the Tallinn Manual, sponsored initially by NATO—might emerge to shape responses to state-based attacks. Bilateral partnerships between other states, such as the one between the Czech Republic and Israel that focuses on the protection of critical assets and encourages private-sector innovation, are also developing. And a proposal before the European Parliament would strengthen its Agency for Network and Information Security in leading the union's cybersecurity efforts, including by having the agency act as a coordination hub for crises.

Questions governments can ask include the following:

- In which international forums on cybersecurity does the government participate?
- What arrangements with other nations do the government have to share information, best practices, or alerts?
- Does the government collaborate with other governments to prevent or investigate cybercrime? How effectively does it use mutual-legal-assistance mechanisms for cybercrime?

How have you defined critical national infrastructure?

If governments address no other aspect of cybersecurity, they must protect critical infrastructure. Many, such as the United States, have started to address cybersecurity from this perspective.[8]

What exactly constitutes critical infrastructure and the proper role of government in protecting it is not universally agreed upon. Some countries, such as France and Israel, have a centralized, regulatory approach toward companies perceived as critical. Both have legislation defining what is critical and related obligations. France formally designates both

public and private companies as critical operators, which must then meet a range of specified security requirements—and it defines the category broadly to include more than 250 public and private operating companies across 12 sectors.[9] Others, such as Switzerland, are more decentralized. In the United States, the Department of Homeland Security coordinates a national infrastructure-protection plan and requires sector-specific agencies to develop sector-specific plans. The Office of Infrastructure Protection offers tools and training for companies that are considered critical infrastructure. In the Czech Republic, the implementation of a cybersecurity legal framework has facilitated a more directive approach.

The digital world extends the definition of critical national infrastructure, lengthening the list of sectors and activities that are essential to the smooth functioning of the economy. Companies within those sectors might also have critical dependencies on other organizations, themselves outside the definition of critical national infrastructure. Yet few countries have domestic hardware and software industries of any scale, leaving them potentially vulnerable to cyberattack through foreign-owned infrastructure. Government decisions about inward investment might increasingly have to balance economic advantage with cybersecurity considerations.

Questions governments can ask include the following:

- Is there an agreed-upon definition of the critical national infrastructure?
- By what means does the government ensure the cybersecurity of critical infrastructure?
- How does the government support the companies and organizations it defines as critical?
- How does the government ensure compliance with security standards? How is that compliance measured?
- Is there a mechanism to ensure that cybersecurity is taken into account when considering major foreign-investment propositions?

Government's role in cybersecurity will only grow as the global demand and dependency on the internet and internet-connected devices continue to increase. With increasing threats and fewer opportunities to fail, governments must rise to the challenge to protect both national security and economic prosperity.

[1] *Real lives, real crimes: A study of digital crime and policing*, Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, December 2015, justiceinspectorates.gov.uk.

[2] "Notifiable data breaches scheme," Office of the Australian Information Commissioner, oaic.gov.au.

[3] *2017 Global Information Security Workforce Study*, Center for Cyber Safety and Education, iamcybersafe.org.

[4] "ASD certified gateways," Australian Signals Directorate, February 2017, acsc.gov.au.

[5] Ian Levy, "Active Cyber Defence – one year on," NCSC, February 5, 2018, ncsc.gov.uk.

[6] Review of published police-department budgets.

[7] "The mutual legal assistance problem explained," blog entry by Gail Kent, February 23, 2015, cyberlaw.stanford.edu.

[8] Interview with Daniel Prieto, former director of cybersecurity and technology, US National Security Council.

[9] *The critical infrastructure protection in France*, Secrétariat Général de la Défense et de la Sécurité Nationale, January 2017, sgdsn.gouv.fr.

Mary Calam is a senior expert in McKinsey's London office, where **David Chinn** is a senior partner and **John Noble** is an external advisor, and **Jonathan Fantini Porter** is a specialist in the Washington, DC, office.

Designed by Global Editorial Services.