Building a national cybersecurity agency

Microsoft Policy Papers

Addressing cybersecurity challenges at the national level

Cybersecurity has become a national priority for the majority of countries around the world and rightly so. Over the last two decades, billions have benefited from economic and social opportunities driven by the exponential growth and rapid adoption of ICT. That same development has, however, also given rise to new cyber-threats, from fraud and theft of intellectual property or personal data, to the disruption of services, and even destruction of property.

Today, many governments are working to adopt, review, or implement national cybersecurity strategies, policies, laws, regulations or other national approaches, with countless other efforts taking place at sectoral, state, city or other levels. To support the implementation of these, countries have considered the development of a central cybersecurity agency or a similar body to help manage their efforts.

However, developing effective approaches to tackling cybersecurity at national level isn't easy, especially if they are going to have widespread or long-lasting effects. The task of such agencies is complex; not just because of the pervasiveness of computing today, but because of the legacy of pre-cyber policy-making and regulation. Effectively, cybersecurity is one of the first policy areas that challenges traditional governance structures and policy-making. National cybersecurity approaches need to tackle a great deal, from promoting online safety and protecting government services and critical infrastructures, to engaging internationally to tackle global threats. These topics cut across an unprecedented range of traditional government departments, from defense and foreign affairs, to education and finance.

Moreover, governments are particularly dependent on the private sector when it comes to dealing with cybersecurity. The majority of online infrastructure is owned and operated by the private sector, which therefore holds much of the information related to cybersecurity threats. As a result, the effectiveness of national cybersecurity approaches often hinges on how successfully and how extensively the private sector is involved in awareness raising, information exchange, and policy development.

What makes a successful national cybersecurity agency?

Allowing for many different forms that a national cybersecurity agency can take, our experiences of working with governments around the world indicate that there are some particularly effective approaches to structuring them. These include approaches to how they are structured operationally, how their roles are viewed, and which responsibilities they are assigned. The five recommendations for structuring an effective national cybersecurity agency are:

1. Appoint a single national cybersecurity agency: A single agency dedicated to managing cybersecurity at the national level can be an effective way for managing the security of civilian agencies, critical infrastructure protection and national level incident response. While cybersecurity concerns are likely to cut across many "traditional" government agency policy areas, such as justice, treasury, defense, or foreign affairs, having a centralized authority will help establish a horizontal baseline of cybersecurity best practices which the different sector-specific verticals can build off.
2. Provide the national cybersecurity agency with a clear mandate: Any national cybersecurity agency will be expected to navigate a complex environment that spans other government departments, national legislatures, established regulatory authorities, civil society groups, the general public, public and private sector organizations, and international partners. It is therefore important that all stakeholders have a clear expectation of what the mandate of the national cybersecurity agency is, so they know what to expect and who to talk to.

3. Ensure the national cybersecurity agency has appropriate statutory powers: Currently, most national cybersecurity agencies are established not by statute but by the delegation of existing powers by other parts of government. We anticipate that this approach will need to change with the passage of comprehensive cybersecurity laws. The delegation of existing powers, which may be subject to multiple underlying regulations, may not be sufficient to provide the national cybersecurity agency with all of the powers it requires to effectively carry out its new functions.
4. Implement a five-part organizational structure: This five-part structure we propose allows for a multifaceted interaction across internal government and regulatory stakeholders and external stakeholders from the public and private sectors, as well as the international arena. In particular it addresses one of the core challenges governments have faced: how to reconcile mandatory reporting of cyber-incidents, with the voluntary and bi-directional exchange of information about cyber-threats:
    - The Policy and planning unit should lead the nation's development, coordination, alignment, and integration of cybersecurity policies, strategies and plans.
    - The Outreach and partnership unit should lead and manage relationships and interfaces across the government and with other nations, institutions, and the private sector.
    - The Communications unit should coordinate regulatory and non-regulatory communication, including messages, documents and publications, and statements to all stakeholders on behalf of the national cybersecurity agency.
    - The Operations unit should be tasked with ensuring effective coordination and deployment in response to cyber threats, effectively acting as a CERT.
    - The Regulatory unit should be responsible for overseeing compliance with cybersecurity regulations, including developing guidance, and collaborating with other units to update regulatory obligations.
5. Expect to evolve and adapt: Given the pace of technology development the unavoidability of change will require the agency to evolve and adapt over time if it is to continue to fulfill its mandate. We recommend regular processes are established to review agency performance and the nature of the changes taking place in the wider "cyberworld". Emerging best practices and newly established standards or baselines should be studied and most importantly, both the agency's private sector and civil society partners should be involved in the discussions.

A strong national cybersecurity agency can help governments manage all the different aspects of cybersecurity governance. Drawing on the five recommendations made in this paper, it can engage (within government itself, across the broader domestic context, and with other jurisdictions) and it can keep up to date with developments and adapt accordingly. Given clear ownership and power across the various functional areas it is expected to oversee, and equipped with the necessary capabilities and resources, a national cybersecurity agency can deliver not only for those who make the policy but also for those who take the policy, be they critical infrastructure providers, businesses, public sector organizations or even other regulators.