Written by Toomas Hendrik Ilves

Few things in the world seem to progress faster than technology. But despite technology's inexorable march forward, security almost always seems to be a generation behind. As society and industry become more dependent on internet-connected devices, and the online world becomes a central and underlying component of the physical world, the significance of cybersecurity increases commensurately. No longer can security be left to IT departments and security groups within companies. Rather, it requires engagement at the highest levels of both industry and government.

The private sector on its own cannot create a culture that emphasizes security practices, realign financial incentives that reward speed over security, or mend trust deficits with the public sector. However, together with the public sector, these challenges can be addressed to change the culture and incentives of security best practices.

Before that can happen, though, we must recognize that there are significant challenges that can make it difficult for the public sector to effectively address cyber security issues. Three particularly important issues stand out:

International fragmentation: Differences in approaches to cyber security, data jurisdiction, and legal enforcement (not to mention culture, language and politics) across jurisdictional and territorial boundaries can make it hard to effectively prevent, investigate, and prosecute cyberattacks.

International norm-setting: International political differences and country-specific agendas can make it difficult to develop a consensus when it comes to the norms around cybersecurity, let alone enforce those norms consistently and effectively.

Roles with respect to the private sector: The varying and sometimes confrontational roles that the public sector must play – from regulator to information sharer and collaborator – can create tensions with the private sector that can be counterproductive to trust and cooperation.

Similarly, there are numerous challenges that can make it difficult for the private sector to effectively address cybersecurity issues, including two particularly important obstacles:

Misalignment of incentives for cybersecurity best practices: Companies often fail to take basic steps to protect their systems and their users. Companies are placed in the difficult position of balancing the market pressures of rapid innovation against sustained investments in cybersecurity, which may raise costs or delay delivery of products to market.

Ecosystem complexities: Today's software and hardware environments are increasingly complex ecosystems populated by a network of interacting devices, networks, people and organizations. This means cybersecurity solutions often require the voluntary engagement, cooperation and investments of many independent entities, while the incentives and mechanisms for taking such actions are distributed inconsistently across the ecosystem.

For example, if a significant vulnerability in common and free software is disclosed, every device using that software should be patched as soon as possible. Even if the patch is available immediately, nobody can force updates by individual server owners, and unsecure devices remain available for a long time.

Additionally, there are obstacles that impede public-private sector collaboration on cybersecurity issues, including trust deficits between the government and the private sector, the challenge of maximizing the effectiveness of government interventions while balancing security objectives with fast-paced innovation, and the weakness of existing information-sharing frameworks.

The need for change

These powerful tensions within the ecosystem make it clear that systemic changes are necessary to realign approaches to cybersecurity. The public and private sectors must come together in several ways, for example through blended governance approaches or holistic cybersecurity education.

They should collaboratively construct effective regulations and frameworks that address cybersecurity needs without hampering innovation or diminishing trust. Blended or collaborative governance allows the public and private sector to address cybersecurity threats together. For example, in the energy sector, dissident groups or terrorist organizations continue to seek ways to cause disruption, and the blended governance approach of tight collaboration between public and private entities is the best solutions to defend the critical infrastructure.

Similar collaboration should apply for education, as the private and public sectors together bridge the knowledge gap for both technical and non-technical employees.

Acting now

There are steps that both the private and public sector can take right now to begin to address cybersecurity challenges. These include:

Adopting best practices and cyber hygiene: An important first step is developing policies and procedures that include regularly validating approved hardware and authorized software, establishing security system configurations, timely patching of applications and operating systems, controlling and auditing user privileges, and educating users.

Improved authentication: Organizations must move beyond insecure passwords to mechanisms such as two-factor authentication and continuous authentication technology, which will become increasingly important as more devices connect to our networks.

Preparing for attacks: It is critical that organizations take steps to prepare for eventual attacks, including enhancing forensic capabilities, developing business continuity plans, and developing plans for regaining user trust.

Even if there is no silver bullet for cybersecurity, that does not mean the problems are intractable.

With the world more digitally interconnected than ever before, cybersecurity in the Fourth Industrial Revolution will face critical challenges and opportunities. Only collaborative efforts to make more innovative and strategic frameworks between governments, companies, civil society and academia will better secure our digital ecosystem. More specifically, cooperation between public and private sectors has a significant role to play in the evolution of a secure future.

This article was based on the findings of a report by the Global Agenda Council on Cybersecurity, available here .

Original article on the World Economic Forum webpage .