WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Global Agenda Council on Cybersecurity

April 2016

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

REF 180416

Contents

Executive Summary

Fuelled by billions of users and endless new internet of things devices, we are in the midst of an explosion of hyperconnectivity. This means attackers can now disrupt more people through more devices, and each year there are more breaches, more affected companies and users, and more damage. It is increasingly clear that no one is immune from cyberattacks.

For this reason, it is imperative that the public and private sectors *balance and prioritize* the limited resources available to address cybersecurity challenges. Too often, cultural and financial pressures encourage devaluing investments in cybersecurity. Before those pressures can change, the public and private sectors must better understand the tensions that make it difficult to fully embrace cybersecurity best practices, as well as the obstacles to effective collaboration.

What the Private Sector Should Know About Public Sector Tensions:
Among the many significant challenges that can make it difficult for the public sector to effectively address cybersecurity issues, there are three particularly important hurdles:

1. International fragmentation: Differences in approaches to cybersecurity, 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.
2. International norm-setting: International political differences and country-specific agendas can make it difficult to develop consensus norms regarding cybersecurity let alone enforce those norms consistently and effectively.
3. Roles with respect to the private sector: The varying and sometimes confrontational roles that the public sector must play, spanning regulator to information sharer and collaborator, can create tensions with the private sector that can be counterproductive to trust and cooperation.

What the Public Sector Should Know About Private Sector Tensions:
Similarly, there are many significant challenges that can make it difficult for the private sector to effectively address cybersecurity issues, including two particularly important obstacles:

1. Misalignment of incentives for cybersecurity best practices: Companies often fail to take basic steps to protect their systems and their users because 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.
2. 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.

Additionally, there are obstacles that impede public-private sector collaboration on cybersecurity issues, including trust deficits between the government and 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.

Securing the Future
These powerful tensions within the ecosystem make it clear that systemic changes are necessary to realign approaches to cybersecurity. Although there is no quick fix, there are steps that organizations can take immediately to begin to address cybersecurity challenges. These include:

1. *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.
2. *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.
3. *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.

The public and private sectors acting alone cannot overcome the culture and incentives that make cybersecurity so difficult today. To address these systemic challenges, the public and private sectors must come together in several ways, including:

4. *Blended governance approaches:* The public and

private sectors must explore new ways of collaboration that would leverage the perspectives of governments, companies, civil society and academia.

5. *Careful government interventions:* The public and private sectors must collaboratively construct effective regulations and frameworks that address cybersecurity needs without hampering innovation or diminishing trust.
6. *Independent security organizations:* Independent organizations can reward implementation of best practices and create high-information consumers.
7. *Holistic cybersecurity education:* More holistic educational programmes can provide cybersecurity professionals with a range of necessary skills beyond the purely technical.

There is no silver bullet for cybersecurity, but that does not mean the problems are intractable. Instead, it means that careful collaboration between the public and private sectors is necessary to address these complex challenges in an ongoing and comprehensive manner.

1. Introduction

The Global Agenda Council on Cybersecurity, one of the World Economic Forum's 80 Global Agenda Councils, was formed to explore and develop practical solutions to the challenging questions on changing cybersecurity trends and emerging new challenges. Cybersecurity can no longer be left to IT departments and security groups within companies. It is an issue that requires engagement at the highest levels of both industry and government.

The council's members include cybersecurity experts, policy-makers, business executives, civil society representatives and academics. Over the course of several meetings, these experts have identified and debated some of the central issues, challenges and opportunities relating to cybersecurity. This report synthesizes several of the ideas expressed at these meetings.

Cybersecurity has already become a critical issue across business, industry, government and civil society; it will only grow more urgent as the online world becomes a central and underlying component of the physical world. As of the end of 2015, 3.2 billion people are connected to the internet in some form, including 2 billion from developing countries. And this is growing at a rapid pace. From 2000 to 2015, the global internet penetration rate grew from 6.5% to 43%.[1] Those people, and the many more who join each year, rely on the internet for their jobs, commerce, culture and communications. And they are connected by more than just PCs and mobile devices; increasingly, everyday products and core infrastructure – including refrigerators, thermostats, the electrical grid and aircraft engines – rely on embedded computers and network connections. As society and industry become more dependent on these internet-connected devices, the significance of cybersecurity increases as well.

The public and private sectors each face difficult and unique challenges in balancing their varied roles and responsibilities, and prioritizing their limited financial, time and human resources. Too often, members of the public sector fail to appreciate the complexity of the challenges that the private sector faces and vice versa. These misunderstandings can inhibit effective collaboration and partnerships. This report tries to break through those barriers to build a foundation in which collaboration can thrive.

There are no easy solutions, but the good news is that there are things the private sector can do right now to address these cybersecurity challenges. By following and implementing cyber hygiene and best practices, companies can make an immediate and positive difference. However, without cooperation between the public and private sectors, such measures will be inadequate. 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. But together with the public sector, these challenges can be addressed. Through the use of new multistakeholder processes, as part of blended governance frameworks, public-private partnerships can begin to change the culture and incentives of security best practices, create frameworks for collaboratively constructing effective cybersecurity regulations and tools without hampering innovation or diminishing trust, and support the creation of independent security organizations that enable well-informed consumers.

The World Economic Forum possesses a unique ability to focus the attention of decision-makers at the highest levels of both the public and private sectors, and to harness their energies in devising creative and effective solutions. In that way, the Forum is the ideal institution to address cybersecurity issues. The Global Agenda Council on Cybersecurity, as well as the Forum's Future of the Internet Initiative's Cyber Crime project, present unique opportunities for exploring innovative solutions to a complex and ever-evolving problem. As described below, advancing cybersecurity will require multistakeholder collaboration and international cooperation. The World Economic Forum's Global Agenda Council on Cybersecurity is proud to be a contributor to that effort.

2. Emerging Trends

Many public and private sector decision-makers intuitively appreciate that cybersecurity is an important consideration. But less clear are the tectonic shifts pushing the issue to the fore. Although there are many factors that contribute to cybersecurity's increasing saliency, three are worth identifying here: (1) the shift toward cloud services and more devices' built-in Internet connectivity; (2) the increased prevalence, severity, and fallout from data breaches, and (3) the inability of security to keep pace with technological development.

A. Increased Reliance on Internet-Connected Devices and Services

Key takeaway: The internet of things and cloud computing are creating new opportunities for vulnerabilities and crime while simultaneously expanding the potential devastation of such attacks.

Decreasing costs of hardware, software and internet connections, combined with greater bandwidth capacity, are enabling companies to put internet connections into previously unconnected devices,[2] while making users more reliant on data centres and cloud computing.[3] Taken together, these two trends have enabled rapid changes in the capabilities of software, products and services. But they have also opened new opportunities for crime and espionage, and simultaneously expanded the potential devastation of such attacks.

Cheaper and faster technology is making cloud computing increasingly technically and economically viable. The cost of digital storage has plunged from $300,000 per gigabyte of data in 1981 to $0.03 per gigabyte in 2014.[4] Files that would have taken days to download over a 28.8 kbps dial-up connection can be transferred in minutes or seconds over today's broadband connections. These changes have enabled an array of new services that move many aspects of computing, including data storage and analysis, to remote systems that provide access and computational power to users on an as-needed and aggregated basis. Companies are no longer required to build their own network infrastructure; companies can instead use infinitely scalable cloud computing to rent remote storage and processing capabilities and easily scale up their resources as they grow. In fact, major internet companies such as Dropbox, Netflix and Pinterest do just that – they have built entire platforms on server infrastructure rented from other companies. Consumers benefit from cloud computing as well, using online services to store, access, synchronize and share files, photos and other digital assets.

As cloud computing has become more common, the centralization of services and the explosion of internet of things (IoT) devices has created a hyperconnectivity that creates new challenges for cybersecurity:

1. *Centralization of services:* Cloud computing has unburdened smaller companies from the need to invest in infrastructure, which has decentralized and democratized opportunities for smaller companies to deploy innovative services. But this has also led to centralization at the infrastructure level on to a handful of platforms. Only a few companies have the resources to build and deploy the massive data centres necessary for modern internet services. For that reason, a large portion of internet data and traffic is managed by a concentrated pool of companies including Amazon, Microsoft, Google, Rackspace and IBM. This centralization presents both challenges and opportunities; these large data centres are often better equipped to maintain their services to defend against attacks than the average small company but they also present more tempting targets for attackers.
2. *Expansion of connected devices:* The transfer of services and data to the cloud has also enabled the rapid adoption of interconnected devices, including both mobile devices and IoT. Increasingly, individuals are relying on mobile devices for internet connectivity. Mobile broadband (i.e., 3G and 4G connections) penetration has reached 47% worldwide and is estimated to grow to 70% by 2020,[5] enabling new online services such as mobile banking in sub-Saharan Africa.[6] Additionally, the cloud has enabled an array of internet-connected physical objects (IoT) ranging from critical infrastructure to personal devices. These objects have the ability to generate data through a variety of sensors and then process and store that data in the cloud. Some estimate that by 2020, there will be 25 billion connected "things" in use,[7] most with durability, latency, enrolment, vulnerability, authentication and privacy challenges.

Taken together, this hyperconnectivity of services and products has greatly increased the ability of attackers to reach more users through more devices. Every new connected device introduces another potential entry point to the network, increasing the overall attack surface. Cloud computing and IoT are forecast to create unprecedented opportunities for improving lives and enabling innovation. Unfortunately, they also invite a new set of cybersecurity challenges.

Cloud computing service providers' incentives may not always align with greater investments in cybersecurity, or they may simply lack the necessary expertise. Many companies that have marketed conventional industrial machines or non-computerized appliances or services are now grappling with complex security issues. For example, car manufacturers, consumer appliance manufacturers, livery services and industrial equipment manufacturers are facing many of the same challenges that have traditionally been considered "computer" problems. The universe of devices connected to the internet is vast, and developers and manufacturers bring different corporate cultures, experiences and expertise when designing the security of their products. And for some, that experience and expertise is limited.

B. Breaches and Vulnerabilities Are Increasing in Frequency and Severity

Key takeaway: Attacks are inevitable. Over the past year, major entities from nearly every sector have suffered significant attacks and the commoditization of exploits and vulnerabilities will only enable more attacks.

The number and severity of breaches continue to rise. According to one report, there were 1,540 breach incidents in 2014, affecting over 1 billion records – a dramatic increase from 1,056 incidents affecting 575 million records in 2013.[8] Cybersecurity is a challenge for entities both large and small, sophisticated and not. A recent study conducted for the UK government found that 90% of large businesses and 74% of small businesses had suffered a data breach over the past year, both increases over the previous year.[9]

Over the past couple of years, breaches have affected some of the most important industries worldwide – including finance, healthcare, entertainment – and governments. In mid-2014, a small team of criminals infiltrated JP Morgan Chase's computer system to steal the personal information of 83 million individuals and small businesses as part of a securities fraud scheme.[10] In early 2015, attackers used a variety of exploits to steal 80 million social security records and other personal data from the US health insurance company Anthem. And in October 2015, police arrested two teenagers for stealing bank and personal information of up to 4 million customers from the UK telecoms company TalkTalk.[11]

Government systems have also been the target of attacks. For example, in January 2014 it was revealed that an employee of the Korea Credit Bureau had stolen the personal credit card data of 20 million South Koreans and sold the information to marketing firms.[12] In June 2015, the United States Office of Personnel Management discovered a year-long intrusion into its systems. The attack compromised the records of over 21 million current and former US government employees, including social security numbers, sensitive background-check records and even fingerprints.[13] While the attacks were originally believed to have originated from nation-state sponsored adversaries, the Chinese government recently arrested several criminal hackers who allegedly conducted the attack.[14]

Sony Pictures suffered a crippling attack in late 2014, suspected to be the work of hackers tied to a nation-state government. The hackers, allegedly motivated by the pending release of the Sony film, The Interview, stole and then released large files including unreleased movies and scripts, internal financial reports, employee health information, and a trove of publicly embarrassing internal emails. The attack crippled Sony's systems, including: "The telephone directory vanished. Voicemail was offline. Computers became bricks. Internet access on the lot was shuttered. The cafeteria became cash-only. Contracts – and the templates those contracts were based on – disappeared."[15]

These examples make apparent that there is no single cybersecurity threat or adversary. Instead, threats take many forms. Attackers can be nation-states or affiliated hacking groups; they can be criminals, or a disgruntled employee. Attackers can be motivated by political or commercial gain. They can take advantage of human mistakes, technical vulnerabilities, or a combination of these. They can use any of the high-profile vulnerabilities that have been found in popular user software such as Flash, critical security protocol toolkits like OpenSSL (e.g., Heartbleed), and mobile device operating systems like Android (e.g., Stagefright).

It is difficult to measure the costs of such attacks. Many estimates exist, and while the exact amounts may not be accurate or useful, they underscore the potential severity. For example, IBM and the Ponemon Institute estimate that the average consolidated cost of a data breach is $3.79 million.[16] By contrast, the 2014 Verizon Breach Investigation Report suggests a range of costs, depending on the number of stolen records; while a breach of 100 records is estimated to cost a company anywhere from $1,000 to over $500,000, a breach of 100 million records could cost between $400,000 to just under $200 million. [17] Highly regulated industries, such as healthcare, education and finance, may have even higher data breach costs.

Not only is no one immune from these high-cost attacks, but it is becoming easier to obtain the tools necessary to perpetrate them. Lucrative grey and black marketplaces for selling hacking tools, software vulnerabilities and exploits – particularly coveted zero-day exploits – facilitate and enable attacks. The increasing availability of the tools required for a successful cyberattack has increased both the number and sophistication of attacks,[18] and developments like machine learning, which will lead to attacks that rapidly evolve, will only increase sophistication of attacks in the future. Cyber criminals have evolved from discrete, ad hoc networks of individuals to a highly organized system of financially driven criminal enterprises around the globe. And this commoditization of cyber offensive tools will continue to enable the growth of cyberattacks.

C. Business and Technology Developments Outpace Security Improvements

Key takeaway: The speed and pace at which new products *and services are being developed outpaces the ability and/ or willingness of companies to address cybersecurity risks.*

The growing threat of attacks is compounded by the fact that the speed and pace of development for new products and services outpace companies' abilities to respond to cybersecurity threats. For many companies, security considerations are secondary as they balance the market pressure for rapid innovation against investments in cybersecurity. Emphasizing cybersecurity may not lead to immediate or measurable impacts on earnings or might delay bringing products to market. For that reason, it is easy for executives and board members to view investments in cybersecurity as a waste of money or, worse, a waste of critical time. Even seemingly small tasks such as rolling out and installing updates and patches can take a long time. In some cases, patches may break core product functionality or prove too expensive and might be forgone entirely. The 2015 Verizon Breach Investigation Report, for example, noted that "99.9% of the exploited vulnerabilities had been compromised more than a year after" the vulnerability had first been publicly disclosed and a patch made available. More often than not, critical product updates remain unapplied well after vulnerabilities have been discovered.[19]

The pace of technical development also makes it hard for institutions and individuals to make informed purchasing decisions. The technical complexity of cybersecurity is only one piece of that information gap. Some of the same factors that enable the fast pace of innovation also create barriers to informed purchasing with respect to cybersecurity, including:

- Lower barriers to market entry: Developing new online tools and services might have previously required companies to invest heavily in capital expenditures, including servers and other network infrastructure. Now companies can rent infinitely scalable architecture, lowering the initial investment costs and making it easier for anyone to enter the market, no matter what their competence.
- Ease of becoming a developer: Big software companies like Microsoft and Google have extensive hiring, training and quality-assurance programmes, which can help ensure (although by no means guarantee) that end products reflect expertise in cybersecurity. Now, however, app stores like those found on the Android and iOS ecosystems have lowered the bar for becoming a developer and distributor. These developers may have neither the knowledge and experience to address cybersecurity issues nor the resources to respond to issues when they arise.
- Fewer signalling devices and less accountability: With new market entrants emerging daily, it is harder for consumers to rely on brand name as a proxy for quality. Where a brand name company might face market pressures to address cybersecurity lapses in its products, there is no guarantee that a new start-up will even exist in six months, let alone respond to issues. This can make it harder for consumers to identify quality apps and hold developers accountable when issues arise.[20]

Collectively, these changes in the marketplace can increase the cybersecurity risks faced by consumers and users of products and services by making it harder for them to properly assess the associated risk of new tools and services.

3. Current Tensions and Considerations

These emerging trends create a complicated and quickly evolving cybersecurity landscape. Both governments and companies struggle with unique challenges as they try to *balance and prioritize* resources and responsibilities. Too often, for the public and private sectors, security is an afterthought. Simple steps, like cyber hygiene and adopting best practices, remain undone because of cultural and financial pressures that allocate financial, time and human resources to other priorities. While the public and private sectors could begin to address these challenges together, often they fail to appreciate the difficult tensions they each face. Before the public and private sectors can effectively collaborate on cybersecurity, they must better understand the tensions and considerations that shape their respective approaches to cybersecurity.

A. What the Private Sector Should Know About Public Sector Tensions

Key takeaway: The public sector must simultaneously play a multitude of roles with respect to cybersecurity, which can create conflicts, confusion and distrust. Governments face significant challenges as they attempt to balance those roles while navigating complex relationships with national, regional and global stakeholders.

It is important for the private sector to keep in mind that any single government or agency can be playing one or many roles in the cybersecurity ecosystem. And in playing each of these roles, the government may have different, or even competing, interests and objectives. These roles can include:

- Governments as defenders – governments strive to protect their citizens from harm, which may include promoting cybersecurity best practices, aggregating intelligence, or even engaging in offensive operations that weaken the cybersecurity of other countries.
- Governments as users – governments rely on effective cybersecurity to defend their own systems.
- Governments as regulators – acting through their legislative, judicial, regulatory branches, governments regulate to implement policy through the rule of law.
- Governments as stakeholders – acting through a variety of bilateral and multilateral negotiations and agreements, governments establish international law or norms to govern cybersecurity.
- Governments as coordinators – governments coordinating public and private initiatives, through standard-setting processes, and by facilitating the sharing of information between private and public stakeholders.
- Governments as promoters – governments actively promoting cybersecurity and the local companies that enable it through endorsement, funding and incubation programmes.
- Governments as researchers – governments conducting or funding research on technical or societal issues related to cybersecurity.
- Governments as service providers – governments providing cybersecurity (or information relating to it) for use by other government agencies or the public.
- Governments as educators – governments educating both citizens and the private sector about the importance of and approaches to cybersecurity.[21]

In playing these various roles, each important in their own way, governments are continually switching from one role to the next, as they rebalance, reprioritize and reshape their objectives. This can create shifting, challenging and even confusing relationships with stakeholders and the private sector. For example, in the course of responding to and investigating cybersecurity incidents, governments must balance cross-border cooperation while resolving conflicting national laws and jurisdictional claims, and protecting their own national interests. At the international level, governments must balance multilateral cooperation with unilateral action as they encounter a messy and evolving set of global norms. And in the course of pursuing national security, governments struggle to find the right balance of cooperation and coordination with the private sector, as well as the right balance between government's offensive and defensive roles.

1. International Fragmentation

Key takeaway: Fragmentation, both legal and technical, has complicated government efforts at responding to, investigating and prosecuting cybersecurity incidents. Outdated and inadequate bilateral and multilateral mechanisms have necessitated striking a difficult balance between cooperation and confrontation at the international level.

Government efforts at addressing cybersecurity are often complicated by the legal and technical fragmentation of the internet. The internet is not an international network, but a transnational one. For that reason, responding to and investigating cybersecurity incidents requires, among other things, coordination across territorial and jurisdictional boundaries. However, legal fragmentation has been a

significant obstacle to international cooperation. This legal fragmentation emerges from differences across jurisdictional and territorial boundaries in approaches to cybersecurity, along with differences in culture, language and politics.

In cybersecurity investigations, governments must carefully balance claims of "data sovereignty", which refers to the tricky questions relating to assertions of jurisdiction over data as it is stored within, and transits across, national boundaries. Any country physically involved in the processing, storage or transmission (origination, destination, or intermediary) of data could be said to have a jurisdictional claim over data. Governments must carefully navigate these complex, and often competing, set of assertions in order to obtain data necessary to an investigation.

When governments try to resolve these jurisdictional questions, it can lead to tensions with other nations and with private sector companies. For example, in December 2013, as part of a federal narcotics investigation, the United States government was trying to obtain access to a particular customer's emails that were stored at a Microsoft data centre in Dublin, Ireland. One option for the US government would have been to exercise the Mutual Legal Assistance Treaty (MLAT) process, a system of bilateral and multilateral agreements by which nation states commit to assisting one another in criminal investigations and prosecutions. In complex international investigations into cybersecurity incidents, such cross-national cooperation is often necessary and is an increasingly important part of investigations. According to estimates from the US Department of Justice, over the past decade the number of MLAT requests to the US increased by 60%, with computer records requests increasing tenfold.[22]

However, as a mechanism for addressing cybersecurity, the MLAT process has, in practice, proven difficult and frustrating for law enforcement. Many of the MLAT agreements were drafted before the globalization of data and, as a result, investigators are often waiting months for responses to MLAT requests. Cybersecurity incidents require quick responses because digital evidence can quickly disappear, which makes it difficult for governments to rely on MLATs in these circumstances. For those reasons, in the Dublin case the US government instead served a warrant on Microsoft, claiming that the US had jurisdiction over the data because Microsoft is a US company. Microsoft opposed the warrant, asserting that the US government's jurisdiction did not reach data stored exclusively in another country. This is just one example of the difficult choices governments must make in balancing cooperation and confrontation in cybersecurity investigations.

Additionally, governments face a feedback loop that encourages greater levels of fragmentation. Governments often invoke the challenges of addressing cybersecurity issues as a reason for increasing fragmentation, which, in turn, only makes it harder to address cybersecurity. Several countries, including China,[23] Russia[24] and Brazil,[25] have proposed or enacted data localization laws to stop one kind of cybersecurity threat (nation-state surveillance) even though it may complicate addressing other cybersecurity threats.

Similarly, in response to concerns about US surveillance, the European Court of Justice struck down the "Safe Harbor" data-transfer provision of the 1995 Data Protection Directive in October 2015. The Safe Harbor rule had permitted companies outside the EU to store and process the data of Europeans, as long as they self-certified their ability to adequately protect that data. In response to the court's decision, the EU and US announced a new framework for transatlantic data flow. This new agreement – the EU-US Privacy Shield – includes a requirement that American companies wishing to import data from Europe meet new obligations on how personal data is processed and individual rights are guaranteed. In addition, the EU-US Privacy Shield includes limitations, safeguards and oversight mechanisms protecting the rights of EU citizens during US government law enforcement and national security investigations. The EU-US Privacy Shield also provides for mechanisms for EU citizens to seek redress for violations of the agreement and for annual reviews of the agreement.[26] Although the EU-US Privacy Shield must still be adopted, the entire affair highlights the risk of greater fragmentation through conflicts over data sovereignty.

2. National Security and International Norms

Key takeaway: The development of norms can lag substantially behind technological developments. And even when norms are established, they can be applied inconsistently.

It is important for the private sector to keep in mind that governments operate in an international arena where they are continually constrained by norms of behavior. These norms can be an effective way to counteract fragmentation through shared understandings and agreements for addressing cybersecurity challenges. Through mechanisms, ranging from legal treaties to non-binding statements, informal customs and principles, governments have increasingly sought to establish international norms and agreements on investigations into cybercrimes and acceptable practices relating to cyber activities. However, the development of norms also poses challenges for governments as they must often act to address new cybersecurity threats well before norms are established and must carefully choose when to adhere to norms and when those norms interfere with their national laws and interests.

There have been several recent, and largely successful, attempts at addressing aspects of cybersecurity through norms. However, these efforts also highlight many of the challenges for governments. For example, in 2001, the Council of Europe adopted the Budapest Convention on Cybercrime. The convention aimed to facilitate detection, investigation and prosecution domestically and internationally by increasing international cooperation. The Budapest Convention currently has 54 signatories, with 47 of those having ratified the convention. While considered a success in many respects, it also demonstrates some of the challenges of norm-setting, including:

– *Delays:* Nearly half of the ratifying countries took a decade or longer to complete ratification.

– *Lack of Uniformity:* The Budapest Convention, while not limited to European countries, remains a primarily European agreement, with many significant stakeholders around the world actively in opposition.
– *Narrow scope:* The convention, by design, only touches on a small aspect of cybersecurity; attempts to expand the convention to other topics have so far had only limited success.
– *Conflicts of laws:* Several countries have struggled with fully implementing the convention due to constitutional or statutory conflicts, particularly those relating to different conceptions of privacy and free speech.
– *Slow to update:* Nearly 15 years old, the convention has been criticized for not keeping pace with technological change and evolving needs.[27]

A more recent effort at international cooperation and norm setting is the United Nation's 2014-2015 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of National Security (UNGGE), composed of representatives from 20 nations. The UNGGE released a report in July 2015, which built on previous efforts from 2010 and 2013. The report detailed existing and potential threats to information security, the possible cooperative measures to address them, including norms, rules or principles of responsible behaviour for states, and suggested various confidence-building measures to strengthen telecommunication and global information system security. That experts from 20 nations developed a consensus report on cybersecurity represents a positive turn towards establishing norms with respect to cyberspace. And although questions remain about the ultimate enforceability of the agreement, it remains a positive sign for the development of cybersecurity norms.

3. Cooperation with the Private Sector

Key takeaway: The public sector faces a difficult challenge of balancing the need to access information for investigations with the security of communications, privacy rights and commercial interests.

Governments play many roles and sometimes these roles can conflict, creating confusion and challenges for the private sector. Nowhere is that tension more apparent than the current global debates about the proper limits of governmental authority in accessing digital communications. Within the past year, conflicts over the use of encryption in communication devices and services have taken centre stage, often throwing into tension governments' roles as defenders, promoters, users and regulators. This debate has focused on both encryption of the devices that prevent anyone other than the owner from reading data stored on the device, and end-to-end encryption of communications. End-to-end encryption refers to the exchange of data over a communication channel that is completely encrypted from the sender to the intended receiver, meaning that anyone intercepting or passing the data, including service providers, law enforcement and intelligence agencies, cannot access the contents of the communication.

Over the past two years, several companies announced the availability of device and end-to-end encryption in their products. In 2014, Apple announced that iOS 8's iMessage would encrypt communications end-to-end and that iPhones would be encrypted by default.[28] Shortly after, Google followed suit by announcing that Android Lollipop would encrypt user data in certain messaging applications by default.[29] In November 2014, popular instant messaging service WhatsApp, currently owned by Facebook, announced it would support an end-to-end encryption protocol called TextSecure.[30] In March 2015, Yahoo introduced an extension that encrypted messages in Yahoo Mail.[31]

This trend towards greater encryption in consumer-grade software and devices has created a difficult challenge for governments, which must balance national security and law enforcement demands for additional information and the need for security in devices to prevent crime and fraud. Around the world, states have taken different regulatory approaches to this challenge. In the United Kingdom, for example, proposed legislation could potentially ban the use of the end-to-end communications in applications including WhatsApp, iMessage and Snapchat.[32] Similarly, the use of encryption in consumer messaging applications continues to be hotly debated in places like the US and France, particularly after the coordinated attacks in Paris in November 2015 and increased attention to the threat from groups such as ISIS.[33]

B. What the Public Sector Should Know About Private Sector Tensions

It is important for the public sector to understand that the private sector often fails to adequately address cybersecurity not because of a lack of solutions. In many cases, implementing those solutions may come at the cost of added expenses, reduced shareholder gains, delayed product releases, or impaired user experiences. There is no shortage of accepted best practices that companies could implement that would reduce the risk of attacks and the harms that would come from those attacks. For example, there are best practices relating to general corporate security, including the Center for Internet Security's (CIS) set of Critical Security Controls for effective cyber defence.[34] And there are best practices relating to network security management, including the ISO 27001, the International Organization of Standardization's (ISO) exhaustive set of security standards for an Information Security Management System (ISMS).[35] And there are best practices relating to cloud security more generally, such as recommendations from the Cloud Security Alliance,[36] and best practices for cloud security on specific platforms, such as the best practices for Amazon's Web Services.[37] Government agencies have also made available sets of best practices, including the Australian Signals Directorate's list of 35 cybersecurity steps[38] and the UK's "10 steps to cybersecurity", covering issues such as user privileges, system configuration, malware prevention and user education.[39]

Additionally, there are known best practices with respect to authentication. Understanding whether a user has the proper credentials and authority to access a service, system, device or network can be critical to ensuring cybersecurity. There is increasing recognition that passwords alone are an insufficient form of authentication. Here, too, there are acknowledged approaches to improving authentication, including biometrics, or two-factor identification, which combines something you know (e.g., a password) with a physical object (e.g., an item unique to the user such as a mobile phone, ID-card etc.).

There is no shortage of best practices and implementing them would have measureable results. The Australian Signals Directorate estimates that 85% of the attacks it observes could be mitigated by simply following four basic steps, including patching applications and patching operating systems.[40] And yet, although many of these best practices are known to mitigate a significant number of cybersecurity risks, many enterprises in the private sector, both large and small, fail to take these steps. In some cases, the limitation is a lack of awareness about available best practices. In many other cases, the obstacle for companies is in balancing the financial, time and human resources that such changes would require against the competitive market pressures that demand quick profits and rapid innovation.

1. Resources and Knowledge Gaps

Key takeaway: Companies face challenging questions about prioritizing the application of financial, time and human resources, necessitating difficult trade-offs between investments in new products and features, securing their own systems, securing end-user systems and data, and securing legacy products, all within a market that rewards rapid innovation and being first to market.

As seen above, there are many best practices and standards that companies could follow for addressing cybersecurity issues within their systems and products. However, on the whole, even with the increase in high-profile breaches, there are still many companies that simply take inadequate steps to secure either their own systems or their users' data, or both. One reason for this gap between concept and implementation is that companies have limited financial, time and human resources and they face many pressures to prioritize issues other than cybersecurity.

Companies often have to balance the market pressures of rapid innovation and shareholder returns with ensuring security. Investments in security can prevent significant losses but may not generate positive returns on investment in the short term when compared to the potential returns from investments in innovation and future product development.[41] Additionally, the market stresses rapid product development and often rewards those first to market. In such an environment, it is easy for cybersecurity to become a secondary priority to be addressed only after the product is developed.

Even in the wake of incidents, companies can place a low emphasis on security. For example, in 2011, Sony's PlayStation Network was hacked, exposing the personal information of 77 million accounts.[42] Despite having already suffered a significant breach, when Sony Pictures – another Sony subsidiary – was hacked in 2014, only 11 of Sony's 7000 employees were assigned to the company's information security team.[43] In a 2007 interview with *CIO Magazine*, Jason Spaltro – then executive director of information security at Sony – stated that the low value placed on security was a "valid business decision to accept the risk" of a security breach, and that investing $10 million to avoid $1 million of penalties was not something he would do.[44]

Even companies seeking to invest in their human resources often face a systemic resource gap: a lack of trained cybersecurity specialists. A 2015 report from Cisco estimated that there were 1 million unfilled cybersecurity jobs.[45] In actuality, the knowledge gap is even greater because the Cisco figure counts only the demand for full-time *technical* cybersecurity specialists, and does not consider the impact of cybersecurity on numerous *non-technical* positions. The employees in these non-technical positions, despite a lack of cybersecurity training, are often asked to address cybersecurity challenges. These challenges can include addressing the businesses risks of cybersecurity threats, determining the interaction between physical security and cybersecurity, planning for public responses after a data breach, managing cybersecurity specialists, or engaging with government agencies following a serious cyberattack. Considering that any computer-using employee is a potential cybersecurity risk or a part of the response, a lack of basic cybersecurity training contributes to the expanding knowledge gap.

In general, companies have limited time and resources. They frequently must make a difficult set of balancing decisions prioritizing where those limited resources can be best utilized. Even when putting resources into cybersecurity, companies must balance between dedicating resources to the security of their own systems and dedicating resources to securing end-user products. While large companies may have more resources, they also may face additional challenges and costs of coordinating across various silos within the company. By contrast, smaller companies may not have the financial or human resources capacity for addressing the multitude of complex cybersecurity challenges.

Companies must also make difficult choices in prioritizing the vulnerabilities they choose to patch. For example, companies must decide how much of their limited security budgets should be spent on buying vulnerabilities from security researchers. The vulnerabilities marketplace has become increasingly lucrative, which makes it increasingly expensive for companies to keep vulnerabilities out of the hands of criminals. Some companies have created bug-bounty programmes as a means of participating in that marketplace, but many companies' bounties are not competitive with what governments or criminals might pay for a vulnerability or an exploit. Even when companies know of the vulnerabilities, whether purchased or not, there are more than can possibly be fixed. Companies must allocate their limited resources and choose which bugs and vulnerabilities to address, while risking leaving gaps for attackers to exploit.

Additionally, not every industry has a culture and an upgrade cycle that is compatible with the fast pace of development in the technology and software industries. In some industries, seemingly small changes like a software upgrade might trigger unacceptably large costs. For example, certain utility operators in the US typically depend on their industrial control system software to last for 10 to 15 years, and many of those companies are still using Windows XP on their critical infrastructure. This poses a significant cybersecurity issue as Microsoft ended support for Windows XP in 2014. The industry, however, is locked into this outdated software because the tight integration between the management systems and the software means it would cost more than $100 million and would take several years for them to upgrade to newer systems.[46]

The example of Windows XP in utilities is emblematic of a larger challenge: software and hardware vendors often cannot force their customers to upgrade and secure their systems. Once products are in the hands of customers, product updates can be impossible to fully implement. For example, in May 2015, a vulnerability was found to likely affect millions of routers due to a specific component, NetUSB, that many manufacturers had used in their routers. This vulnerability would allow an attacker to wipe or compromise a router, and potentially install malware to spy on the users, or even compromise the entire network. Patches for the issue were deployed inconsistently. In some cases, the owner of the router might not understand the problem or know how to apply the patch. In other cases, just like with the utilities, the patch or update could cause unacceptable disruptions for the end-users. Even well-intentioned companies can sometimes find that the resources required to provide cybersecurity updates would far outstrip their ability to deliver them.

Finally, resource allocation can be a challenge when it involves allocating resources across companies and industries. In these circumstances, companies and sectors may not be able to agree on who should bear the costs of addressing certain risks. For example, in the US, many retail companies who use point-of-sale terminals have not moved to more secure chip systems for credit card transactions and continue to rely on antiquated and vulnerable magnetic strip technology. This is in large part because the retail companies are not eager to shoulder the cost of upgraded point-of-sale terminals even if it leaves customers insecure.[47]

2. Ecosystem Management Challenges

Key takeaway: Companies face difficult challenges in effectively addressing cybersecurity issues where solutions must be implemented by several independent actors who own and manage different parts of an interoperable system, and where a single product is the result of several components made by different companies or even different silos within the same company.

Software and hardware environments are increasingly complicated ecosystems populated by a complex community of interacting devices, networks, people and organizations. Because no single company can maintain and control every aspect of the ecosystem, trust and cooperation are essential. Companies face challenges in managing these ecosystems both where the ecosystem is the product of many different actors and companies deploying interoperable systems, and in situations where a single product is made up of components from different companies or even different silos within the same company.

Interoperable system complexity:
Highly interoperable systems can create rich ecosystems of services and devices, but they can also create cybersecurity challenges. Without a single point of control over the ecosystem, cybersecurity challenges can be addressed only through a combination of trust and voluntary cooperation between each participant. As the complexity of the ecosystem increases, so, too, do the costs of coordination and the risk of mismatched incentives. These challenges have been apparent in Google's Android mobile operating system, where the lack of central control has led to several cybersecurity breakdowns. Google provides Android as open-source software, and it has gained significant market share, installed on an estimated 80% of smartphones.[48] Although Google maintains the core code, the ecosystem as a whole involves the participation of hundreds of handset manufacturers and carriers which can customize the operating system before loading it on their devices or deploying it on their networks.

Google cannot push security updates directly to end users. Instead, it can take months for users to receive updates to Android, if at all. That delay is because handset manufacturers must first test the update to ensure it is compatible with their devices. Then the wireless carriers must also test each new update. And both the handset manufacturers and the carriers might have modified the Android code or created their own apps, and each new update from Google might require extensive revisions to that custom code, further compounding the delays. For these reasons, wireless service providers and device manufacturers often delay or forgo significant operating system updates to avoid the cost in financial, time and human resources that these updates require. As a result, many older Android smartphones never receive security and feature updates from Google. As of December 2015, only 29.5% of Android devices run the year-old Lollipop version and only 0.5% are running the newest Marshmallow version.[49] By contrast, Apple has much more control over the software that runs on its devices, a model that allows the company to release updates directly to users. Consequently, 70% of iOS devices are using Apple's latest operating system.[50]

This challenge of updating Android devices became a significant security liability when researchers discovered Stagefright in July 2015, which was a major exploit that allowed an attacker to take over a victim's device through a simple SMS message or audio file.[51] When discovered, Google moved quickly to issue a patch to the software. However, the Android device ecosystem took months to propagate out the fix and some older devices were never patched. In response to this security failure, several companies within the Android ecosystem have pledged to change their processes to provide monthly patches.[52]

A similar ecosystem challenge was the Heartbleed vulnerability, which was disclosed in April 2014 and was believed to affect 17% (about half a million) of the internet's secure web servers.[53] The bug compromised any secure connection that utilized OpenSSL, allowing attackers to eavesdrop on communications, steal data directly from services and users, and impersonate services and users. Although a patch for OpenSSL was made available quickly, there was no central point of control that could force updates; individual server owners were responsible for applying the patch to their systems. Some owners patched their servers quickly and others took months.

Single product complexity:
Ecosystem issues can also affect the cybersecurity of a single product. Today's complex devices often rely on the integration of technology from many suppliers. These relationships rely on trust – most companies lack the time, money and resources to check the source code or the design specifications of every component sourced from others. Companies must trust that their vendors and suppliers live up to their security assurances.

The 2015 hack of a Chrysler Jeep Cherokee showed how difficult it can be to secure products made from components from a variety of suppliers and vendors. The Jeep entertainment system utilized Uconnect, a third-party application that connected to the internet. Using Uconnect's IP address, hackers were able to gain access to the Jeep from a remote laptop miles away and seize control of the car's dashboard, steering, braking and transmission functions.[54] In this case, manufacturing a complex product like a car requires trusting that all of the components, when placed together, will not create cascading vulnerabilities. Although companies can conduct supplier and vendor audits or use other controls to try to catch vulnerabilities, that may delay and significantly increase the costs and complexities of developing new products.

Tighter collaboration between or within companies may help to address these ecosystem challenges, but more often than not, company cultures prevent open communication about systems and designs. Within companies, for both competitive and institutional reasons, stovepiping is common within divisions. Although this data siloing can protect product secrecy and trade secrets, it can also prevent collaboration and information sharing. Similar concerns may prevent companies that collaborate on products with suppliers and vendors from sharing critical information. In all cases, these communication gaps may contribute to cybersecurity issues in complex ecosystems.

C. Broader Ecosystem Tensions and Considerations

Key takeaway: Effective collaboration between the public and private sectors requires that they recognize and address the obstacles and limitations to collaboration, including their lack of trust, and difficulties in lawmaking and enforcement, and obstacles to research and information sharing.

It is not enough for the public and private sectors to understand the challenges they face. It is also important for them to recognize and address the challenges and limitations of any efforts at collaboration. Collaboration may not be easy, but it is essential for addressing many cybersecurity issues because the internet is a transnational system spanning jurisdictional boundaries and public and private systems.

Many cybersecurity challenges affect both the public and private sectors and benefit from the expertise and perspectives across governments, companies, academic institutions, industry experts and the general public. Collaboration is critical for five reasons:

1. *Technical gaps:* The private sector controls many of the critical systems and resources that comprise the internet.
2. *Talent gaps:* The private sector captures a stronger current of technical talent and expertise.
3. *Information gaps:* The public sector has greater access to national and international threat information.
4. *Enforcement gaps:* The public sector is better positioned to investigate and prosecute cybercrime and enable cooperation between companies that otherwise might be impeded by concerns over competition and reputation.
5. *Development gaps:* Partnerships can build bridges between mature and developing industries and countries, facilitating knowledge and information sharing.

The public and private sectors are intentionally distinct and their differences are important. However, those same differences can also make partnerships difficult. One of the main challenges to partnerships has been the trust deficit that has grown between public and private entities, particularly after recent revelations about surveillance.

The lack of trust is not the only obstacle to collaboration in the cybersecurity ecosystem. The public and private sectors can attempt to collaborate through information sharing, the creation of standards, incident response, security research and more. However, each of these collaborative approaches requires balancing the multifaceted roles that both public and private sector entities play. For example, governments play dual roles as both regulator and collaborator with the private sector. Similarly, companies within an industry play dual roles of both competitors and partners in addressing cybersecurity issues. These multifaceted roles and relationships create tensions and obstacles for effective collaboration.

1. Trust Deficits Between Companies and Governments

Key takeaway: As a result of a backlash to government surveillance, companies are hesitant to collaborate with governments due to fear of negative perceptions, loss of business and liability risks from divulging private information, colluding with competitors, or exposing themselves to additional penalties.

One of the most significant obstacles to building and maintaining effective partnerships between the public and private sectors is the fundamental lack of trust that emerged after the Snowden leaks in 2013. In response to revelations about government surveillance, several major technology companies, including Apple, Facebook, Google, Twitter and Microsoft, expressed concerns over publicly collaborating with government actors. These companies and others have worked together to publicly protest government surveillance and lobby for surveillance reform.

Companies have been particularly hesitant to collaborate with the US government because of the potentially negative financial impacts. Distrust of US government policies and statements regarding surveillance have led several non-US companies and foreign governments to be suspicious of any company that might be aiding intelligence collection. Some analysts have estimated that the Snowden leaks in particular will cost major US technology companies billions of dollars in lost sales.[55] These factors push companies to distance themselves from the negative perceptions of a tight collaboration with government, creating a cold climate in public-private relations.[56]

The debates about the use of end-to-end encryption highlight this lack of trust between the public and private sectors. Because technology companies have been leery of voluntarily cooperating with law enforcement agencies, several government leaders from around the world, including Prime Minister David Cameron of the UK and leaders in China, have sought the legal authority to compel access to online communications for lawful investigations.[57] The public and private sectors have struggled to agree on what is feasible. For example, NSA Director Admiral Michael Rogers proposed that technology companies implement certain technical changes to encryption that would enable government access, such as so-called "golden keys".[58] In response, members of the security technologists and the private sector have claimed such solutions would introduce new vulnerabilities, threaten economic competitiveness and weaken existing security measures.[59]

An additional trust issue is that companies fear sharing information with governments and other companies may expose them to liability, either for divulging private information, inadvertently revealing information that subjects them to regulation or sanction by other government entities, or for antitrust violations for colluding with competitors.

Overcoming these trust deficits is necessary for collaboratively addressing cybersecurity challenges. However, there are other significant obstacles to collaboration between the public and private sectors. The tools that the public and private sectors can use for collaboration each come with their own challenges. As will become apparent, trust (or a lack thereof) is an element of many of those challenges as well.

2. Standards, Regulation and Enforcement

Key takeaway: The public and private sectors, when collaborating in standard-setting, lawmaking and legal enforcement, must find the right balance between government interventions and innovation, and between deliberative legal processes and the need for quick resolutions.

The public and private sectors can and do collaborate on cybersecurity issues through standard-setting, lawmaking (encompassing both legislation and regulation) and legal enforcement. However, when collaborating in any of these ways, it can be difficult for the public and private sectors to find the right balance between government interventions and innovation, and between deliberative legal processes and the need for quick resolutions. This difficulty is apparent in some of the ways in which they collaborate:

Standard-setting: The creation and adoption of standards can help identify best practices, create shared norms, and enable interoperability across complex systems – all crucial to cybersecurity. Collaboration in standard setting can enable the development of norms that reflect diverse perspectives and offer unique solutions to difficult cybersecurity challenges. However, standard-setting has many challenges of its own:

- *Speed:* Standard-setting institutions are slow-moving and often fail to keep pace with technical innovation, a particular problem when trying to address quickly developing cybersecurity threats. By the time a standard is finalized, it may be out of date and fail to fully address emerging issues.
- *Compatibility:* Products that were designed and deployed before or even during the standard-setting process may be incompatible with subsequent standards and impossible or difficult to update.
- *Universality:* Standards benefit from network effects. However, there are a variety of coalitions and institutions that are developing alternative or competing standards for addressing cybersecurity issues. This leaves many standards without a critical mass of adoption and creates a fragmentation that undermines effectiveness.

Lawmaking: The creation of legislation and regulation is another opportunity for public and private sector collaboration. In some cases, lawmaking can be more effective than standards because it offers a mechanism for compelling compliance and uniformity with cybersecurity practices when the market might otherwise be fractured and uncoordinated. For example, several pieces of cybersecurity legislation have been proposed including the recently enacted US Cybersecurity Information Sharing Act (CISA) of 2015, which could stimulate collaboration that would not otherwise occur. Collaboration in the legislative and regulatory processes helps address the public sector's lack of technical and industry knowledge. But lawmaking, like standard-setting, can be ill-equipped at addressing the fast-moving cybersecurity environment. Lawmaking processes can be slow and difficult, and the current political environment in the US has made it difficult to enact legislation.

Enforcement: Legal enforcement of cybersecurity issues is another avenue for public and private sector collaboration. Investigations of cyberattacks, for example, often require

such collaboration. However, as described previously, such collaboration requires a difficult balance between public and private interests.

In all of these examples of standard-setting, lawmaking and enforcement, it can be very difficult for the public and private sectors to balance the different roles they must play at different times. For example, sometimes governments act as a defender of cybersecurity and sometimes governments seek to exploit cybersecurity vulnerabilities. Choosing the correct times and places to play those roles can be difficult, and a trust deficit can exacerbate the problem. For instance, documents from the Snowden revelations indicated that when participating in a public-private process for establishing a new standard for random-number key generations, the NSA championed one in particular – the Dual_EC_DRBG generator. Documents from Snowden indicate that the NSA had used the standard-setting process to urge adoption of a standard that it could break, damaging trust and complicating its role in future collaborations.[60] By contrast, there are times when the public sector in its enforcement role can help companies respond to and recover from attacks in ways that would have been impossible without government assistance. In these circumstances, collaboration can help build trust and confidence in their partnerships.

Case Study – Enforcement in Action: Cybercrime

At the World Economic Forum, there are efforts under way to improve collaboration between the public and private sectors in improving the investigation and prosecution of cybercrimes. The Future of the Internet Initiative's Cybercrime Project, an effort complimentary to this Global Agenda Council, recognizes that meaningful and effective approaches to combating cybercrime require close collaboration between the public and private sectors. In an effort to foster that collaboration, the Cybercrime Project has identified several recommendations for effective public-private partnerships:[61]

1. Public and private sectors should share more information related to cyber threats, vulnerability and consequences.
2. Public and private sectors should work to create new platforms, strengthen existing platforms and coordinate these platforms to increase information-sharing and improve investigations and prosecutions.
3. Public and private sectors should cooperate to encourage and advance wider adoption of the Budapest Convention on Cybercrime, or, of the principles it promotes.
4. Public and private sectors should work to build trust and discuss contentious topics related to cybercrime, such as encryption, cloud servers, data access and protection of privacy, to find appropriate solutions.
5. Public and private sectors can engage in other initiatives aimed at reducing cybercrime.

3. Knowledge and Information Sharing

Key takeaway: Knowledge and information sharing is a critical tool in addressing cybersecurity challenges and, by definition, it requires participation from both the public and private sector. However, trust deficits, secrecy obligations, ineffective frameworks for sharing and liability risks all constrain and limit sharing.

Information and knowledge are key currencies in cybersecurity, as they are critical to both prevention and response, including:

- *Balancing resources:* The public and private sectors have different perspectives, skill sets and time horizons, and information sharing is critical to addressing the complete array of cybersecurity challenges. The government is in a unique position to think about long-term threats and the types of actors who are capable of carrying them out, as well as to aggregate information from a variety of sources. By contrast, the private sector is in a unique position to implement and respond to many security threats.
- *Building expertise:* Not only do the public and private sectors have different perspectives and expertise, but they have different levels of maturity and experience. Fostering a knowledge exchange from governments and companies with experience addressing cybersecurity issues to those without those experiences is important for sharing best practices and preventing cybersecurity breaches. In fact, cybersecurity knowledge sharing has been identified as a central component of sustainable development more broadly.[62]
- *Attribution:* After an attack, identifying who caused an incident and how is critical for patching vulnerabilities and deterring future incidents. In attributing incidents, sometimes, private and public entities receive an overwhelming amount of complex, difficult-to-decipher information. Other times they receive too little information. In either case, both sectors receive only one perspective, necessitating information sharing for proper attribution. On several occasions, companies and governments have made mistakes in attributing attacks, often due to bad or insufficient information sharing.

Information and knowledge sharing is an important form of collaboration, but it faces many challenges. The most significant is the trust deficit described above, which creates resistance to collaboration of any kind, and concern about the accuracy of any information that is shared. In addition to the trust deficit, several other challenges exist, including:

- *Secrecy obligations:* Governments must balance their obligations with respect to secrecy in national security, intelligence and grand jury information with the need for bi-directional information sharing. Government secrecy obligations can restrict the extent and depth to which governments can share information with the private sector. For companies, these secrecy issues raise the concern that information sharing flows in one direction – from companies to governments, with limited reciprocity.

– *Institutional reforms:* Certain organizations exist to help facilitate open information sharing, such as the National Cyber Security and Communications Integration Center (NCCIC)[63] in the US and the Cyber Security Information Sharing Partnership (CISP)[64] in the UK. However, many of these institutional initiatives are created within silos, without input from other stakeholders, or as "quick fixes" to fill gaps temporarily. They often place an emphasis on some aspects of reorganization, such as agency-to-agency coordination, over other issues like improving existing communication with the private sector. For that reason, there is significant scepticism over whether these reforms will be successful, whether they address the correct issues, and whether they serve the best interests of the private sector and the public at large.
– *Liability risks:* Companies fear they may be held liable either by directly revealing information that violates a statute, or indirectly by revealing information that leads to liability for unrelated offences. For example, a well-intentioned disclosure to one government entity might subject those records to public records requests, which may in turn lead to further investigations by a different government agency or civil lawsuits. To address this issue, in the US, for example, the Cyber Security Information Sharing Act (CISA) contains a strong liability safe harbour that immunizes companies from private rights of action and regulatory enforcement actions that arise from certain types of information sharing. While the law has been criticized for a lack of user privacy protections and limitations on the downstream use of the disclosures, public and private stakeholder groups will have voluntary tools and standards for sharing information and protecting privacy.[65]

Knowledge and information sharing is a key tool in addressing cybersecurity challenges, and by definition it requires participation by both the public and private sectors. The development of effective laws, regulations and standards, as well as prevention and attribution, all require careful calibration of public and private interests and perspectives. However, in the absence of knowledge and information sharing, that calibration and balancing of interests may be impossible. Unfortunately, there are significant challenges that impede effective knowledge and information challenge.

4. Securing the Future

With so many difficult tensions making it hard to address cybersecurity, it is clear that systemic changes are necessary to realign the culture and incentives that shape cybersecurity. This a complex and evolving space and no single solution can adequately address the full spectrum of challenges. However, there are a variety of approaches that can help. What follows is not an exhaustive list but a starting place for how the public and private sectors can begin to change the culture on cybersecurity.

There are steps that companies can and should begin to take right now to improve cybersecurity. We identify below several of these steps. But while they are crucial, they are not sufficient. The private sector cannot address cybersecurity on its own. Changing the underlying market pressures and culture, improving trust with the public sector, and improving public-private information and knowledge sharing, can only be done through collaboration between the public and private sectors. For that reason, the remainder of this report looks at some things the public and private sectors can do to help address these larger structural challenges. These approaches include: (1) the use of blended governance models; (2) the targeted application of limited regulation; (3) the use of independent security organizations to enable informed purchasing; and (4) expanding security professionals' skill sets to encompass critical non-technical skills. While each of these approaches can potentially address some of the cybersecurity challenges, no single recommendation here can change culture and perceptions. Only time, education and communication can realign cultural approaches to cybersecurity.

A. Immediate Steps the Private Sector Can Take to Emphasize Cybersecurity

Key takeaway: It is critical for enterprises across the private sector to implement best practices throughout all operations, and throughout product lifecycles, as a foundational step to greater cybersecurity – a difficult challenge in a market that rewards rapid product development.

The private sector must directly confront the cultural and incentive challenges that make many of the cybersecurity issues so challenging. In short, companies must work to change the default attitudes that exist in order to place a clear and ongoing emphasis on security. Without addressing these cultural and incentive issues, companies will continue to ignore basic security best practices.

For companies, this shift entails emphasizing security throughout the entire product or service lifecycle, including: (1) planning for security early in the product development cycle, (2) taking into account the security of legacy systems, and (3) ensuring resiliency in the event of an attack. For many companies, this lifecycle approach is a significant departure from their current approach to security. In a market that stresses rapid product development and often rewards those first-to-market, there can be enormous pressure to deliver quickly at the expense of investments in cybersecurity. This pressure was evident in Facebook's early motto of "move fast and break things".[66] Importantly, Facebook also shows that companies can adjust their approach, as its motto changed in 2014 to "move fast with stable infrastructure" in order to reflect a commitment to balancing quick innovation with security and stability.[67]

A cultural shift on the part of private sector entities to better address cybersecurity would involve numerous changes, but we identify three in particular as a starting place:

Adoption of best practices: There are basic steps that companies should follow that, although not a complete solution to cybersecurity issues, would have a demonstrable positive impact. Several examples of these are included in the appendix, and include:

- The CIS Critical Security Controls to enhance enterprise cybersecurity defences and incident response[68]
- The Australian Signals Directorate's list of 35 mitigation steps for reducing the risks from targeted computer network attacks, including application whitelisting, applying application and operating system patches, and enforcing a strong password policy[69]
- The UK's "10 steps to cybersecurity" covering topics such as setting user privileges, malware prevention and user education[70]

Improved authentication: Authentication is critically important for cybersecurity, and particularly challenging in the internet of things(IoT). Companies should move beyond insecure passwords to mechanisms such as two-factor authentication or multi-factor authentication that uses other forms of verification like biometric data. Online services could also enable the use of authentication technologies, including fingerprint and iris scanners, voice and facial recognition, and a variety of technologies, such as embedded Secure Elements (eSE), that help verify identities in more secure ways.[71] And companies should explore new methods of continuous authentication that continually reaffirm authentication throughout the time of access –

something that will become increasingly important with the need to continually re-authenticate IoT devices connected to a network or a system.

Preparation for attacks: No one is immune from cyberattacks. It is critical that companies take steps before they are attacked. Most importantly, companies must: (1) examine and enhance their forensic capabilities to determine the scope of an attack, inform affected customers and entities, and assist law enforcement; (2) develop a business continuity plan to determine whether, how and when to continue or resume business operations after an attack; and (3) develop a plan for regaining customer trust after an attack. Waiting to do these things until after an attack has already happened will be too late.

Changing corporate culture on security is not just a one-time thing – it is a commitment that must be made repeatedly over the course of a product or company's lifecycle. Such a cultural shift is not easy, as it requires a significant investment of financial, time and human resources. During the development phase, workers must devote time and effort testing and securing existing features when that effort could be spent iterating new features. Similarly, such an investment must be remade continually over the lifecycle of the product instead of spending time on new products. In order to make this change, companies must find a balance between rapid innovation and ensuring security. Companies must also find a balance between the costs of investing in security and the ultimate cost of their products. Additionally, companies with limited resources must find the right balance between innovating new products sustainably and supporting existing devices in the future. This latter balancing will be particularly challenging in the industrial IoT, where products may be expected to remain both operational and connected for decades.

One reason why companies have not made such a culture change previously is that the financial incentives simply did not support such a change. While some companies, such as Apple, have used their investment in security as a product differentiator in selling their iOS products,[72] they have done so at a price premium, which serves to commoditize and stratify security. Changing these underlying financial incentives is not something the private sector can do on its own, which is why blended governance models that encourage collaboration between the public and private sectors will be critical.

Case Study – Private Sector in Action: Cyber Insurance[73]

Although cyber insurance is frequently mentioned as a mechanism that businesses could use to mitigate cyber threats, the insurance industry has undertaken the barest of beginnings in this space. Insurance companies have to this point demonstrated little native understanding of the cyber risks posed to enterprises, making it difficult for them to offer effective products.

In order to offer useful products, the insurance industry must establish a reliable way to value a company's cyber and cyber-dependent assets, beginning with data, which can include intellectual property, client/customer data and employee data. In the more traditional areas, e.g., fire, auto, home, etc., the insurance industry is the marketplace expert on risk, with centuries of actuarial data on which to base risk-pricing decisions and to guard insurers against accepting more risk than they can effectively cover.

By contrast, for cyber insurance, the risk profile is far less clear, observable and measureable. Standards are fewer and actuarial data hardly exists. Threats also come from every quarter and create unimaginable consequences – for example, when intemperate executive emails are provided to the press – that can cause considerable loss of reputation, customer loyalty and market share. However, no best practice standard exists to guide the insurance industry in gauging risk. Instead, every major insurer uses its own proprietary scheme of varying degrees of sophistication. Many insurance companies seem to treat total revenue as the primary differentiating factor for categorizing cybersecurity risk. In other words, both a small medical office with voluminous files of intimate personal data and an automated car wash chain of equivalent market value with customer financial records are assessed at the same risk level. While both kinds of data are sensitive, the obvious differences in function, business processes, regulatory requirements and risk exposures distinguish the chances or consequences of a cyber event.

Despite these challenges in assessing risk, insurance carriers have begun to heavily promote their cyber insurance products and the current insurance marketplace provides some coverage for certain specific cyber risks, such as a data breach. For cyber insurance to succeed, this model must change. Insurers must take on the challenge of realistically evaluating the cyber risks they are underwriting, including accounting for the unique cyber risk factors of individual enterprises.

B. Blended Governance

Key takeaway: It is necessary to experiment with new paradigms for distributed and collaborative governance that will enable cybersecurity challenges to be addressed jointly by the public and private sectors.

The challenges to cybersecurity underscore again and again the critical need for collaboration between the public and private sectors. However, many of the existing institutions and mechanisms for collaboration are simply inadequate. Particularly when addressing complex and quickly evolving cybersecurity threats, current approaches are often too slow, too inflexible, or too prone to distrust or dysfunction. There are, of course, exceptions, such as governments hiring "technologists-in-residence" to bridge technical gaps, public-private partnerships such as the World Economic Forum facilitating cross-sector relationships, fusion centres to coordinate public and private intelligence sharing, joint research endeavours, and more.[74]

Addressing the next evolution of cybersecurity threats requires exploring new paradigms and institutions that fundamentally retrain and readjust how the public and private sectors collaborate, and build stronger and deeper

connections between them. Such approaches go beyond traditional multistakeholder governance models to build relationships that are flexible and can be adjusted quickly and responsively to address evolving challenges and conflicts.[75] Through working collaboratively to solve pressing problems, such partnerships can even help build reservoirs of trust between the public and private sectors that are currently lacking.

There is no one-size-fits-all model for such collaboration. Instead, effective groups remain sensitive throughout their entire lifecycle to their dynamic contextual and cultural conditions, the availability of support systems and resources, and the opportunities for and trade-offs related to inclusion, transparency and accountability. Most importantly, these groups are instrumental and dynamic, changing over time to adapt to new circumstances and needs, something that is crucial for groups addressing cybersecurity and its evolving threats.

Such blended governance approaches will build important bridges between the private sector and governments and society as a whole. For example, operating with greater input from the private sector will better enable governments to make critical and targeted investments in cybersecurity that will ultimately help change the cultural and financial incentives for cybersecurity. These investments include:

- *Procurement:* Governments can use their procurement powers to help recalibrate private sector approaches to cybersecurity by purchasing from companies that build security into the entire lifecycle of their products and services. Not only would this help change private sector attitudes but it would also improve the security of public sector systems and services.[76]
- *Research:* Governments can fund research into vulnerabilities and cybersecurity, which ultimately makes it easier and less costly for the private sector to commit to best practices and address issues early on in the process.
- *Education:* Governments can educate both the private sector about best practice and users about safe behaviour and cyber hygiene.

Governments have been particularly adept at using education to advance cybersecurity objectives. For example, Germany, Finland, the Republic of Korea, Israel, Estonia and Austria have all developed university programmes in partnership with the private sector to advance cybersecurity research and develop a new generation of experts.[77] Similarly, several countries, including the UK, Germany, and France, have all worked with the private sector to develop educational programmes to help smaller businesses understand cybersecurity threats.[78]

Public-private partnerships with civil society and academia can also help educate consumers about cybersecurity. If consumers are better educated about cybersecurity and understand the basic steps to help ensure their own security, they will be more likely to reflect that knowledge in their purchasing decisions. Consumers who practise cyber hygiene at the personal level and take their own digital security seriously may reward companies that take security seriously when purchasing products. By making security a higher priority in purchasing decisions, consumers will help the private sector view prioritizing cybersecurity as beneficial to their bottom line.

Case Study – Blended Governance in Action: The Energy Sector

The energy sector is often defined by public and private sectors working in close collaboration, making it an ideal place to address cybersecurity through blended governance approaches. The energy sector manages critical infrastructure, making cybersecurity a serious concern. There have already been several high-profile cybersecurity incidents, including:

- The 2010 Stuxnet worm that destroyed nearly one-fifth of Iran's nuclear centrifuges
- The 2011 "Night Dragon" attack that stole sensitive competitive information about oil and gas field bids and operations from international oil companies
- An attack in 2012 on Saudi Arabia's Aramco that damaged 30,000 personal computers in an attempt to halt all oil production.

The threats against the energy sector are only going to get worse. According to the *Wall Street Journal*, "a survey of 625 IT executives in the US, UK, France and Germany by Intel Security and the Aspen Institute found that 48% said they think it's likely there will be a cyberattack on critical infrastructure in the next three years that will result in loss of life." To date, adversaries have generally been state-sponsored, but dissident groups and terrorist organizations continue to seek ways to cause disruption, including attacks on energy infrastructure.

The energy sector is up against two major cyber threats. The first are vulnerabilities in the information technology (IT) enterprise systems. These are vulnerabilities in the commonly used systems and tools that can affect any commercial enterprise. The approaches for addressing these threats, including best practices and cyber hygiene, are well understood.

The energy sector, also faces threats tailored to the unique operational technology (OT) that is critical to energy production and transmission. Refineries, power plants, transmission and distribution grids and pipelines all rely on specific software and other control technologies. The best ways to protect and defend these specialized systems is not nearly as well understood. Additionally, these OT systems are often difficult or expensive to upgrade as they are typically designed to run for decades. Updates or other threat mitigations can require significant coordination between customers, vendors and others.

C. Regulation and Government Leadership

Key takeaway: Carefully tailored government interventions can help tip the scales toward greater cybersecurity, but such actions must be weighed against the potential impact on innovation.

Aside from the financial and educational interventions described above, there are additional steps the public sector can take to bolster cybersecurity practices. Some approaches, while possible, would be unacceptable: establishing a strict liability regime, for example, in which companies are liable for vulnerabilities in their code would certainly incentivize companies to invest in greater cybersecurity, but it would also significantly reduce investments in innovation, make entire industries unprofitable and generally cripple businesses by rendering risk unaffordable. Similarly, mandating back-door access to encrypted devices and communications, while possible, would fundamentally weaken the security afforded by systems with encryption, introducing more risks than security. However, other government interventions can help the private sector find the right balance between cybersecurity and innovation.

One form of government intervention is through the development of carefully tailored regulations. In fact, there are already several examples of approaches to regulation, addressing several aspects of cybersecurity:

– *Data-breach notifications:* Several countries have regulations that require companies to notify customers after certain kinds of security breaches. In the US, most states have some form of security breach notification law, and in 2015 the White House proposed a national breach notification standard, though it has not yet been enacted.[79] The EU is reaching the final stages of finalizing the new General Data Protection Regulation (GDPR), set to replace the1995 Data Protection Directive, which will include a 72-hour limit for breach notifications.[80]
– *Critical infrastructure:* The EU has established provisional rules compelling critical service companies in the key industries of energy, transport, banking, financial markets, health and water supply to ensure that their digital infrastructure is resilient enough to withstand online attacks.[81] Similarly, the US National Institute of Standards and Technology's (NIST) Cyber Security Framework is designed to help organizations charged with providing the nation's financial, energy, healthcare and other critical systems to better protect their information and physical assets from cyberattack. The order established a process for identifying high-priority infrastructure and required agencies to follow a series of steps to determine the adequacy and ability of the agency to address risk.
– *Information sharing:* The NIST Cyber Security Framework directed the US Secretary of Homeland Security and the Director of National Intelligence to consistently share unclassified reports with the private sector after cyberattacks.

In addition to regulation, governments also can alter behaviour through encouraging the creation and adoption of norms. This can happen at the national, regional or global level:

– *National and regional norms:* Regional and national cybersecurity strategy statements are one mechanism through which governments can reshape norms about cybersecurity, as an articulation of consensus or aspirational principles.[82] Some of these cybersecurity strategies are targeted toward readjusting the way government agencies relate to each other on issues of cybersecurity[83] or toward improving public and private sector information sharing. Others focus on cybersecurity as a component of encouraging innovation, entrepreneurship and commercial exchange. For example, the EU's comprehensive Digital Agenda includes creating public-private partnerships to address cybersecurity as part of a broader agenda of achieving a digital single market in Europe.
– *International norms:* It can be difficult for norms at the international level to reshape behaviour in the absence of enforcement mechanisms. However, political scientist Joseph Nye has argued that even in the absence of enforcement mechanisms, countries can establish effective norms bilaterally or even unilaterally. According to Nye, bilateral agreements that bar states from attacking certain aspects of the civilian cyber infrastructure during peacetime could encourage a norm of self-restraint.[84] In some cases, new norms can even be unilateral. For example, governments may stockpile a certain set of undisclosed vulnerabilities in software for offensive use, leaving software vulnerable to potential attacks were those vulnerabilities to be discovered by another party. A norm of unilaterally disclosing vulnerabilities instead of stockpiling them would serve to disarm any adversaries who had also discovered that weakness. In turn, a new international norm could emerge in which countries disclose rather than stockpile vulnerabilities.

Government interventions, from regulation and norms to authentication, often struggle to match the speed of innovation and the changing security landscape. Another challenge is that there are often tricky jurisdictional issues between a variety of potential government actors. For example, in the US, several government agencies have already attempted to unilaterally expand their authority to cover cybersecurity, including the Federal Trade Commission, the Federal Communications Commission and Department of Homeland Security. For these reasons, blended governance approaches will be critical for helping governments respond quickly, sidestep jurisdictional issues within governments and ensure that government action is informed and balanced by private sector perspectives and expertise. This will be particularly true in order to address the cross-disciplinary nature of cybersecurity in IoT, which will require a combination of skills and expertise to be brought to bear in the regulatory process. Effective government intervention will require a careful balancing between private and public interests and processes, coordination and cooperation between various actors and agencies.

Case Study – Government Leadership in Action: Authentication

One example of where governments can advance cybersecurity is through supporting the creation of effective authentication systems. Governments are already the most important issuer of credentials in the physical world by issuing documents confirming identity, name, citizenship, date of birth and more. Governments can play a similar role in the digital world. The development of effective and efficient digital identity management enables the migration of economic and social interactions online, and strengthens trust-based digital services.

Several countries and regions have already begun enabling the next generation of services through comprehensive national authentication and digital ID systems.

- Estonia: Most notably, in 2002, Estonia became one of the first countries to introduce a comprehensive national ID system.[85] From birth, Estonian citizens are given a digital birth certificate that is linked to an online health insurance account. After citizens turn 15, they apply for an electronic ID card that provides proof of identity and enables access to a wide range of government e-services, from electronic banking and shopping to encrypted email. These digital tools are increasing efficiency and are saving the time-equivalent of one working week per person.[86]
- Japan: After meetings with Estonian leaders, the Japanese government announced its own MyNumber National Identification system, which was launched in January 2016. The government hopes the cards will help streamline information sharing between governmental agencies administering tax, social security and disaster mitigation programmes.[87]
- India: In 2010, India began creation of a database of unique IDs that included the fingerprint and iris scans of all 1.2 billion residents. The country's leaders say the programme can streamline India's current bureaucratic process and help solve development problems by ensuring that the benefits of services like welfare spending reach the intended recipients. The unique identities will also allow a sizable population of poor Indians to access services like banking.[88]
- European Union: The EU encourages European countries to establish digital ID systems and to also accept the digital IDs of other countries. The EU's Digital Agenda for Europe contains rules designed to encourage and support the use of digital IDs for more efficient electronic interactions between businesses, citizens and public authorities.[89]
- United States: Instead of creating a single, national authentication system, the US government announced a partnership with technology companies and civil society to promote the use of multiple-factor authentication and to make it easier for users to enable those protections.[90]

Many of these digital IDs, including those from Estonia[91] and the United Arab Emirates[92], have built-in public key cryptography to help secure online transactions and promote the use of the IDs in non-government applications such as banking and e-commerce. One example of this is public key infrastructure (PKI), which is a system of policies, procedures and software that helps secure data through the use of public and private cryptographic keys, enabling both secure communications and authentication.

National digital ID systems, however, are not without their risks. The systems often create a linked dossier of sensitive information about individuals ranging from voting to health documents to tax issues. Governments must ensure the security of such a vast collection of personal data. Additionally, governments must be transparent with citizens about how such information is to be used, both nationally and internationally. A failure to do either of these things will erode trust in the system.

D. Independent Security Organizations

Key takeaway: Independent security organizations can play a critical educational role, helping transform any consumer (corporate, institutional, or individual) into a high-information purchaser with respect to cybersecurity, which will reward and encourage cybersecurity best practices.

In order to change the culture and incentives relating to cybersecurity, we need both greater transparency and high-information consumers. Independent security organizations can help do both.

Transparency can be a powerful tool for reshaping the culture and incentives on cybersecurity. If companies believe they will not be held liable for producing insecure products or services, they have little incentive to secure their products, particularly if securing the product or services incurs high costs. One way to generate accountability for cybersecurity is through the creation of independent security organizations focused on cybersecurity. Such an organization would test products and services and give them a seal of approval if they meet certain, independently verified, criteria.

Such a mechanism for introducing accountability to product development is not revolutionary. Independent testing laboratories have been used previously to improve the quality of consumer electrical devices. The Underwriters Laboratories (UL) was established in 1894 as a response to the notoriously unsafe consumer electric products available at the time. The UL, as it is known, is now a global safety and certification company that analyses, tests, inspects and validates new products, ensuring they meet a certain uniform level of safety. The UL Certification mark, found on many home electrical appliances, indicates to consumers that the product has been tested and certified. The same kind of approach, a kind of CyberUL, has been suggested for advancing cybersecurity accountability.

Several initiatives are already under way to create various elements of a CyberUL. For example, in October 2015, the noted security expert Peiter Zatko announced plans to create the Cyber Independent Testing Laboratory (Cyber-

ITL).[93] The goal of the Cyber-ITL is to quantify the security hygiene of pieces of software and to help the consumer understand how safe a piece of software is, much in the same way that a nutritional label describes the calories, fat or allergens in food.[94] The hope is that such information will help consumers, governments and businesses identify products with better cybersecurity to make informed decisions. Similarly, the US government recently announced that the Department of Homeland Security would collaborate with UL to develop the Cybersecurity Assurance Program, which will conduct tests on IoT devices to certify their security.

Just as independent product ratings in Consumers Reports help consumers make educated purchasing decisions, so, too, would a CyberUL. Having high-information consumers – across sectors – will enable better decision-making; for example, when agencies or companies are considering purchasing from a vendor, they could consult the reviews of an independent security organization. Not only would this improve the quality of purchasing decisions but it would also incentivize companies to improve their ratings of their products and services.

A CyberUL, however, is unlikely to be able to fully identify and highlight all cybersecurity gaps in every product. Software and network security is extremely complex and context-dependent, and the complexity of IoT devices will only continue to increase as those devices gain more computational power, sensors and network interfaces. In a laboratory environment with a limited amount of time, there are only so many devices and vulnerabilities that can be tested. Furthermore, it is challenging in a laboratory to simulate the real world. For example, it is difficult to simulate attacks by adversaries who may respond in unpredictable ways and it is difficult to recreate the array of interconnected systems may coexist with a device in the real world. For these reasons, CyberUL proposals are unlikely to be a panacea. However, they may still help reward and encourage good cybersecurity practices.

E. Holistic Cybersecurity Education

Key takeaway: The public and private sectors should together build and support educational programmes that bridge the knowledge gap, enabling cybersecurity professionals to address both the technical and non-technical aspects of future cybersecurity challenges and provide basic cybersecurity training to non-technical experts.

Bridging the cybersecurity knowledge gap requires improving the educational programmes for both technical and non-technical employees. For cybersecurity professionals, it is important that educational programmes provide more than just technical education. A recent report of the National Academies noted that the cybersecurity workforce needs a wide variety of non-technical skills, in addition to strong technical training.[95] Non-technical training is critical because much of cybersecurity threat prevention and response is about human behaviour. Adversaries are human and they often seek to exploit human weaknesses in addition to technical weaknesses. And when attacks succeed, they often have significant human impacts. Because cybersecurity is inherently concerned with human behaviour, it is important for cybersecurity professionals to have non-technical training in the behavioral aspects of cybersecurity. Similarly, training in the management aspects of cybersecurity – including economics, anthropology and psychology – can help cybersecurity professionals advocate for resource investments within their organization to overcome the incentive and cultural hurdles that often hinder investments in cybersecurity. Cybersecurity professionals responding to an incident may need to coordinate activities across multiple organizational elements or job functions and interact with vendors, security consultants, law enforcement or other outside actors. These roles require more than pure technical knowledge, necessitating the development of a variety of non-technical skills.

Conversely, non-technical managers and employees increasingly need more training in cybersecurity. Although non-technical employees need not become cybersecurity professionals, they do need a basic foundation of technical knowledge and training. This basic knowledge will help these employees avoid critical security mistakes, ask managers and decision-makers the right cybersecurity questions and generally support realigning the incentives that shape cybersecurity decisions.

The public and private sectors can work to ensure that both technical and non-technical employees are given the skills they need. Currently, this holistic training is difficult to find. For example, university programmes educating cybersecurity specialists are overwhelmingly tilted toward the technical dimensions. To address this, the public and private sectors should collaborate to develop and support programmes that will address these knowledge gaps. Working together, the private sector can identify the cybersecurity skills that technical and non-technical employees need, and the public sector can offer courses through public institutions that develop those skills.

5. Conclusion

The stakes for cybersecurity have never been higher. With increased data centralization in remote data centres, expanding reliance on cloud computing, the explosion of the IoT, and the growth in both the number and severity of cyberattacks, cybersecurity must be addressed throughout business, industry, government and civil society.

The challenge of addressing cybersecurity should not, and cannot, be addressed by the private or public sectors acting alone or independently. Ultimately, actors across sectors, industries, backgrounds and experiences will need to work together in novel ways that may seem difficult given the trust deficits in today's security ecosystem.

There are steps that companies and government can take immediately to reduce the threats, including the implementation of best practices and cyber hygiene. However, it is equally important for the public and private sectors to understand why their counterparts often struggle to take these steps. This report tries to bridge that gap, to help the public and private sectors better understand the systemic challenges each other faces, and then move past those barriers to change. In order to change the culture and incentives that make addressing cybersecurity so difficult, the public and private sectors must work together to rebuild trust, improve communication, knowledge and information sharing, and more.

Cybersecurity is a complex, quickly evolving field, and there is no silver bullet or turnkey solution that will solve all of these challenges today. Moreover, even if there were, there is no guarantee that such solutions would be equally effective against emergent threats. Ultimately, a combination of these potential solutions will need to be applied and adjusted over time to address these significant issues.

Appendix A

Basic Cyber Hygiene

1. Know what is connected to your network
2. Properly configure key security settings
3. Properly manage user accounts and settings to limit unauthorized access
4. Install timely patches to applications and operating systems
5. Automate and monitor the foregoing to keep foundation cybersecurity posture current

Drawn from: Center for Internet Security, Cyber Hygiene Toolkit, https://www.cisecurity.org/cyber-pledge/tools.cfm

Australia's 35 Strategies to Mitigate Targeted Cyber Intrusions

1. Application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs including DLL files, scripts and installers.
2. Patch applications, e.g., Java, PDF viewers, Flash, web browsers and Microsoft Office. Patch or mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.
3. Patch operating system vulnerabilities. Patch or mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system. Avoid Windows XP.
4. Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.

Once organizations have implemented the Top 4 mitigation strategies, first on the computers of users who are most likely to be targeted by cyber intrusions and then on all computers and servers, additional mitigation strategies can be selected to address security gaps until an acceptable level of residual risk is reached.

5. User application configuration hardening, disabling the running of internet-based Java code, untrusted Microsoft Office macros, and undesired web browser and PDF viewer features.
6. Automated dynamic analysis of email and web content run in a sandbox to detect suspicious behavior, including network traffic, new or modified files, or configuration changes.
7. Operating system generic exploit mitigation mechanisms, e.g., Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).
8. Host-based Intrusion Detection/Prevention System to identify anomalous behaviour such as process injection, keystroke logging, driver loading and persistence.
9. Disable local administrator accounts to prevent network propagation using compromised local administration credentials that are shared by several computers.
10. Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication by Microsoft Active Directory.
11. Multi-factor authentication especially implemented for remote access or when the user is about to perform a privileged action or access a sensitive information repository.
12. Software-based application firewall, blocking incoming network traffic that is malicious or otherwise unauthorized, and denying network traffic by default.
13. Software-based application firewall, blocking outgoing network traffic that is not generated by whitelisted applications, and denying network traffic by default.
14. Non-persistent virtualized sandboxed trusted operating environment, hosted outside the organization's internal network, for risk activities such as web browsing.
15. Centralized and time-synchronized logging of successful and failed computer events with automated immediate log analysis, storing logs for at least 18 months.
16. Centralized and time-synchronized logging of allowed and blocked network events with automated immediate log analysis, storing logs for at least 18 months.
17. Email content filtering allowing only business-related attachment types. Preferably analyse/convert/sanitize links, PDF and Microsoft Office attachments.
18. Web content filtering of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.
19. Web domain whitelisting for all domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.
20. Block spoofed emails using Sender ID or Sender Policy Framework (SPF) to check incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organization's domain.
21. Workstation and server configuration management based on a hardened Standard Operating Environment with unrequired functionality disabled, e.g. IPv6, autorun and LanMan.

22. Antivirus software using heuristics and automated internet-based reputation ratings to check a program's prevalence and its digital signature's trustworthiness prior to execution.
23. Deny direct internet access from workstations by using an IPv6-capable firewall to force traffic through a split DNS server, an email server or an authenticated web proxy server.
24. Server application security configuration hardening e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.
25. Enforce a strong passphrase policy covering complexity, length and expiry, and avoiding both passphrase re-use and the use of a single dictionary word.
26. Removable and portable media control as part of a data-loss prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.
27. Restrict access to Server Message Block (SMB) and NetBIOS services running on workstations and on servers where possible.
28. User education, e.g., internet threats and spear-phishing socially-engineered emails. Avoid weak passphrases, passphrase re-use, exposing email addresses and unapproved USB devices.
29. Workstation inspection of Microsoft Office files for potentially malicious abnormalities, e.g., using the Microsoft Office File Validation or Protected View features.
30. Signature-based antivirus software that primarily relies on up-to-date signatures to identify malware. Use gateway and desktop antivirus software from different vendors.
31. TLS encryption between email servers to prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.
32. Block attempts to access web sites by their IP address instead of by their domain name, e.g., implemented using a web proxy server, to force cyber adversaries to obtain a domain name.
33. Network-based Intrusion Detection/Prevention System using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
34. Gateway blacklisting to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous internet users.
35. Capture network traffic to/from internal critical-asset workstations and servers, as well as traffic traversing the network perimeter, to perform post-intrusion analysis.

From: http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf

United Kingdom: Reducing the Cyber Risk in 10 Critical Areas

1. Information risk-management regime
2. Secure configuration
3. Network security
4. Managing user privileges
5. User education and awareness
6. Incident management
7. Malware prevention
8. Monitoring
9. Removable media controls
10. Home and mobile working

From: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf

[1] ICT Data and Statistics Division, International Telecommunications Union, "ICT Facts and Figures: The World in 2015." 2015. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

[2] Koomey, Jonathan. "The Computing Trend That Will Change Everything." *MIT Technology Review*, 9 April 2012. http://www.technologyreview.com/news/427444/the-computing-trend-that-will-change-everything/; Goldman Sachs, "The Internet of Things: Making Sense of the Next Mega-trend." *Global Investment Research*, 3 September 2014. http://www.goldmansachs.com/our-thinking/ages/Internet-of-things/iot-report.pdf.

[3] Armbrust, Michael et al., "Above the Clouds: A Berkeley View of Cloud Computing," *University of California, Berkeley,* 10 February 2009. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf; Naone, Erica. "Conjuring Clouds." *MIT Technology Review*, 23 June 2009. http://www.technologyreview.com/article/413981/conjuring-clouds/.

[4] Komorowski, Matt. "A History of Storage Cost (Update)." *Mkomo*, 9 March 2014. Web. 25 November 2015. http://www.mkomo.com/cost-per-gigabyte-update.

[5] ICT Data and Statistics Division, "ICT Facts and Figures"; GSM Association, "The Mobile Economy Series 2015." 2015. http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf.

[6] Id.

[7] Gartner. Gartner Symposium/ITxpo. "Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015." N.p., 11 November 2014. http://www.gartner.com/newsroom/id/2905717.

[8] Gemalto. "2014 Year of Mega Breaches & Identity Theft." February 2015. http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf.

[9] United Kingdom, Her Majesty's Government. "Information Security Breaches Survey 2015," 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432413/bis-15-303_information_security_breaches_survey_2015-executive-eummary.pdf.

[10] Hackett, Robert. "Arrests Made in Connection with JPMorgan Hack, Report Says." *Technology*. Fortune, 21 July 2015. Web. 25 November 2015. http://fortune.com/2015/07/21/arrests-jpmorgan-chase-hack/.

[11] "Second teenager arrested over TalkTalk data breach." *The Guardian*, 30 October 2015. http://www.theguardian.com/business/2015/oct/30/second-teenager-arrested-over-talktalk-data-breach.

[12] "Credit Card Details on 20 Million South Koreans Stolen - BBC News." *BBC News*. N.p., 20 January 2014. http://www.bbc.com/news/technology-25808189. http://www.bbc.com/news/technology-25808189

[13] US Office of Personnel Management. "Cybersecurity Incidents." Cybersecurity Resource Center. June 2015. https://www.opm.gov/cybersecurity/cybersecurity-incidents.

[14] The identities, and whether the hackers were connected to the Chinese government, is still unclear.
Nakashima, Ellen. "Chinese government has arrested hackers it says breached OPM database." *Washington Post.* 2 December 2015. https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

[15] Hess, Amanda. "Inside the Sony Hack." *Slate*, 22 November 2015 http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html.

[16] Ponemon Institute LLC. "2015 Cost of Data Breach Study: Global Analysis." May 2015. http://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF.

[17] Verizon. "2015 Data Breach Investigations Report." April 2015. http://www.verizonenterprise.com/DBIR/.

[18] Ablon, Lillian et al. "Markets for Cybercrime Tools and Stolen Data." *RAND Corporation*. 2014. https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

[19] Id.

[20] McGoogan, Cara. "Instagram Scam App Stole Passwords from Users." *Wired UK*. 11 November 2015. http://www.wired.co.uk/news/archive/2015-11/11/malware-infected-instagent-pulled-from-app-store.

[21] See Gasser, Urs and David R. O'Brien. "Governments and Cloud Computing: Roles, Approaches, and Policy Considerations." *Berkman Center for Internet & Society,* 17 March 2014. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2410270.

[22] US Department of Justice, "Mutual Legal Assistance Treaty Process Reform." *FY 2015 Budget Request.* 2015 http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

[23] Wong, Gillian. "China to Get Tough on Cybersecurity." *Wall Street Journal*, 9 July 2015. http://www.wsj.com/articles/china-to-get-tough-on-cybersecurity-1436419416.

[24] Gulyaeva, Natalia and Maria Sedykh. "Russia Enacts Data Localization Requirement; New Rules Restricting Online Content Come into Effect." *Chronicle of Data Protection*, 18 July 2014. http://www.hldataprotection.com/2014/07/articles/international-eu-privacy/russia-enacts-new-online-data-laws

[25] Toor, Amar. "Will the Global NSA Backlash Break the Internet?" *The Verge*, 8 November 2013. Web. 25 November 2015. http://www.theverge.com/2013/11/8/5080554/nsa-backlash-brazil-germany-raises-fears-of-Internet-balkanization.

[26] European Commission, "Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-US Privacy Shield" 29 February 2016. http://europa.eu/rapid/press-release_IP-16-433_en.htm?locale=en; European Commission, "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield" 2 February 2016. http://europa.eu/rapid/press-release_IP-16-216_en.htm.

[27] Vatis, Michael A. "The Council of Europe Convention on Cybercrime," *National Academy of Sciences*, 2010. https://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf.

[28] Sanger, David. "Signaling Post-Snowden Era, New iPhone Locks Out NSA," *The New York Times*, 26 September 2014. http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html.

[29] Timberg, Craig. "Newest Androids will join iPhones in offering default encryption, blocking police," *The Washington Post*, 18 September 2015, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

[30] Greenberg, Andy. "Whatsapp Just Switched on End-to-End Encryption for Hundreds of Millions of Users," *Wired*, 18 November 2014, http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.

[31] Stamos, Alex. "User-Focused Security: End-to-End Encryption Extension for Yahoo Mail," *Yahoo Blog*, 15 March 2015, http://yahoo.tumblr.com/post/113708033335/user-focused-security-end-to-end-encryption.

[32] Curtis, Sophie. "Will WhatsApps really be banned in the UK?" *The Telegraph,* 13 July 2015. http://www.telegraph.co.uk/technology/social-media/11736230/Will-WhatsApp-really-be-banned-in-the-UK.html; Lomas, Natasha. "UK Gov't Must Clarify Its Position On End-To-End Encryption, Says Parliamentary Committee." *TechCrunch*, 1 February 2016. http://techcrunch.com/2016/02/01/uk-govt-must-clarify-its-position-on-end-to-end-encryption-says-parliamentary-committee/.

[33] Perlroth, Nicole. "Security Experts Oppose Government Access to Encrypted Communication." *The New York Times*, 7 July 2015. http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html; Sanger, David E., and Nicole Perlroth. "Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks." *The New York Times*. 16 November 2015. Web. 25 November 2015. http://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html?_r=0.

[34] "Welcome to CIS Controls." *Center for Internet Security.* https://www.cisecurity.org/critical-controls.cfm. Several governments and enterprises have identified Critical Security Controls as an important tool for effective cyber defence. *See* National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." Cybersecurity Framework. February 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf; United Kingdom. "Critical Security Controls guidance" Centre for Protection of National Infrastructure http://www.cpni.gov.uk/advice/cyber/Critical-controls; European Union. "Cyber; Critical Security Controls for Effective Cyber Defence." European Telecommunications Standards Institute. May 2015. http://www.etsi.org/deliver/etsi_tr/103300_103399/103305/01.01.01_60/tr_103305v010101p.pdf; Symantec, "Internet Security Threat Report 2015." International Telecommunications Union, 2015. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf; Verizon "2015 Data Breach Investigations Report." 2015. http://www.verizonenterprise.com/DBIR/2015/; Atlantic Council and Zurich Insurance Group. "Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures." Atlantic Council. 2015. http://publications.atlanticcouncil.org/cyberrisks//risk-nexus-september-2015-overcome-by-cyber-risks.pdf. The California State Attorney General recently announced that enterprises not using the Critical Security Controls would be deemed as failing to provide reasonably security, and subject to appropriate legal action. California Dept. of Justice, "California Data Breach Report." Office of Attorney General. February 2016. https://oag.ca.gov/breachreport2016.

[35] "Information Security Management." ISO 27001. International Organization For Standardization, n.d. Web. 25 Nov. 2015. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

[36] "Cloud Security Alliance." *Cloud Security Alliance*. N.p., n.d. Web. 25 November 2015. https://cloudsecurityalliance.org/.

[37] Todorov, Dob, and Yinal Ozkan. "AWS Security Best Practices." Amazon Web Services, November 2013. http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf.

[38] Id.

[39] United Kingdom. Government Communication Headquarters. "10 Critical 10 Steps to Cyber Security." 16 January 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf.

[40] Australia. Australian Signals Directorate. "Strategies to Mitigate Targeted Cyber Intrusions." February 2014. http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf.

[41] Schneier, Bruce. "Security ROI." Web log post. *Schneier on Security*. 2 September 2008. https://www.schneier.com/blog/archives/2008/09/security_roi_1.html.

[42] Hill, Kashmir. "How Do We Deal with Data Breaches?" *Forbes*. 9 May 2011. http://www.forbes.com/sites/kashmirhill/2011/05/09/how-do-we-deal-with-data-breaches/.

[43] Hill, Kashmir. "Sony Pictures Hack Was a Long Time Coming, Say Former Employees." *Fusion*. N.p., 4 December 2014. http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/.

[44] Id.

[45] Cisco, "Mitigating the Cybersecurity Skills Shortage." 2015 http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf.

[46] King, Rachael. "Windows XP in Utilities Could Mean Big Security Problems." *CIO Journal*. *The Wall Street Journal*, 9 March 2014. http://blogs.wsj.com/cio/2014/03/09/windows-xp-in-utilities-could-mean-big-security-problems/.

[47] Ziobro, Paul, and Robin Sidel. Target Tried Antitheft Cards." *The Wall Street Journal*. 20 January 2014. http://www.wsj.com/news/articles/SB10001424052702304027204579332990728181278.

[48] IDC Research "Worldwide Quarterly Mobile Phone Tracker." 2015. https://www.idc.com/prodserv/smartphone-os-market-share.jsp.

[49] "Dashboards" *Android*. 2015. https://developer.android.com/about/dashboards/index.html.https://developer.android.com/about/dashboards/index.html

[50] Apple "App Store." (accessed 13 December 2015). https://developer.apple.com/support/app-store/.

[51] Z Team. "Experts Found a Unicorn in the Heart of Android." Zimperium Mobile Security, 27 July 2015. https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/.

[52] Dreyfuss, Emily. "Big Android Makers Will Now Push Monthly Security Update." Wired. 6 August 2015. http://www.wired.com/2015/08/google-samsung-lg-roll-regular-android-security-updates/

[53] Schneier, Bruce. "Heartbleed." *Schneier on Security,* 9 April 2014. https://www.schneier.com/blog/archives/2014/04/heartbleed.html.

[54] Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway – With Me In It." *Wired*, 21 July 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[55] Castro, Daniel. "How Much Will PRISM Cost the U.S. Cloud Computing Industry." The Information Technology and Innovation Foundation. August 2013. http://www2.itif.org/2013-cloud-computing-costs.pdf.

[56] Germano, Judith, "Cybersecurity Partnership: A New Era of Public-Private Collaboration." The Center on Law and Security. October 2014. http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf.

[57] Nicole Perlroth, "Security Experts Oppose."

[58] Ellen Nakashima and Barton Gellman. "As encryption spreads, US grapples with clash between privacy and security." *The Washington Post* 10 April 2015. https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html.

[59] Harold Abelson et al. "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications." Computer Science and Artificial Intelligence Laboratory Technical Report https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[60] Perlroth, Nicole, "Government Announces Steps to Restore Confidence on Encryption Standards." *The New York Times.* 10 September 2013. http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/.

[61] World Economic Forum "Recommendations for Public-Private Partnership Against Cybercrime." Cybercrime Project – Future of the Internet Initiative. January 2016. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf.

[62] United Nations "Transforming our world: the 2030 Agenda for Sustainable Development" Sustainable Development Knowledge Platform. 21 October 2015. https://sustainabledevelopment.un.org/post2015/transformingourworld.

[63] US Department of Homeland Security "Information Sharing." http://www.dhs.gov/topic/cybersecurity-information-sharing.

[64] CERT-UK. "Cybersecurity Information Sharing Partnership (CiSP)." https://www.cert.gov.uk/cisp/.

[65] Andy Greenberg and Yael Grauer. "CISA Security Bill Passes Senate with Privacy Flaws Unfixed." *Wired* 27 October 2015. http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/.http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/

[66] Kelly, Samantha Murphy. "Facebook Changes its 'Move Fast and Break Things' Motto." *Mashable*. 30 April 2014. http://mashable.com/2014/04/30/facebooks-new-mantra-move-fast-with-stability/#FWTrQ4zOAsqV.

[67] Id.

[68] "Cyber Hygiene Toolkit." *Center for Internet Security* https://www.cisecurity.org/cyber-pledge/tools.cfm; "About." *Center for Internet Security* http://www.cisecurity.org/about/.

[69] Id.

[70] United Kingdom. Government Communication Headquarters. "10 Critical 10 Steps to Cyber Security."

[71] "FIDO Alliance." *FIDO Alliance Home Comments*. https://fidoalliance.org/.

[72] "iOS Security" *Apple*. Sept. 2015 https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

[73] Analysis based on a forthcoming work by Jane Holl Lute.

[74] One of the newest of these public-private partnerships is the US Commission on Enhancing National Cybersecurity, which is composed of "top strategic, business, and technical thinkers from outside of Government" who will make detailed recommendations to Congress and the President. Fact Sheet: Cybersecurity National Action Plan." Office of the Press Secretary, The White House. 9 February 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[75] Verhulst, Stephen et. al. "Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem." *Centre for International Governance Innovation,* December 2014. https://www.cigionline.org/sites/default/files/gcig_paper_no5.pdf; Gasser, Urs et. al. "Multistakeholder as Governance Groups: Observations from Case Studies" *Berkman Center for Internet & Society,* 14 January 2015 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2549270.

[76] These investments can be substantial; the Obama Administration 2017 budget proposed spending $3.1 billion simply to start modernizing the outdated and difficult to secure IT systems that the government currently uses. Fact Sheet: Cybersecurity National Action Plan." Office of the Press Secretary, The White House. 9 February 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[77] Radunović, Vladimir and Rüfenacht, David. "Cybersecurity Competence Building Trends." November 2015. DiploFoundation http://www.diplomacy.edu.

[78] Id.

[79] US Government "The Personal Data Notification & Protection Act." Press Release. https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

[80] "Interinstitutional File: 2012/0011 (COD)" *Council of the European Union* http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

[81] European Parliament. "MEPs close deal with Council on first ever EU rules on cybersecurity." 12 July 2015. http://www.europarl.europa.eu/news/en/news-room/20151207IPR06449/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity.

[82] *See* World Economic Forum, "Digital Economy and Cyber Security in Latin America and the Caribbean" in Cybersecurity Observatory, "Cybersecurity: Are We Ready in Latin America and the Caribbean?" 2016. https://digital-iadb.leadpages.co/publicacion-cibersecurity/ (noting how regional norms on cyber security can improve cooperation, particularly in responding to cyber threats).

[83] "Cyber Security Strategy," Australian Government, 2011. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/AGCyberSecurityStrategyforwebsite.pdf; "France's Strategy: Information systems defence and security," Agence Nationale de la Sécurité des Systémés d'Information, 2011. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf.

[84] Nye, Joseph. "The World Needs New Norms on Cyberwarfare." *The Washington Post*, 1 October 2015. https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html.

[85] Hammersley, Ben. "Why you should be an e-resident of Estonia." *Wired*, 4 February 2015. http://www.wired.co.uk/magazine/archive/2015/07/features/estonia-e-resident.

[86] "Estonia and Finland become first in the world to digitally sign international agreement." *Estonian World*. 23 December 2013. http://estonianworld.com/technology/estonia-finland-become-first-world-digitally-sign-international-agreement/.

[87] "Japan to implement ID cards following Estonia's example." *Estonian World*. 24 October 2015. http://estonianworld.com/technology/japan-to-implement-id-card-following-estonias-example/.

[88] Sharma, Awol. "India Launches Project to ID 1.2 Billion People." *The Wall Street Journal*. 29 September 2010. http://www.wsj.com/articles/SB10001424052748704652104575493490951809322.

[89] "Trust Services and eID," European Commission, 2015

[90] "Fact Sheet: Cybersecurity National Action Plan." Office of the Press Secretary, The White House. 9 February 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[91] Tamkivi, Sten. "Lessons from the World's Most Tech-Savvy Government," *The Atlantic*, 24 January 2014. http://www.theatlantic.com/international/archive/2014/01/lessons-from-the-worlds-most-tech-savvy-government/283341.

[92] Al-Khouri, Ali M. "PKI in Government Identity Management Systems," *International Journal of Network Security & Its Applications,* 2011. http://arxiv.org/pdf/1105.6357.pdf.

[93] Hesseldahl, Arik. "Famed Security Researcher Mudge Leaves Google." *re/code*. 29 June 2015. http://recode.net/2015/06/29/famed-security-researcher-mudge-leaves-google-for-white-house-gig/.

[94] Knake, Robert. "Q&A with Peiter Zatko (aka Mudge): Setting Up the Cyber Independent Testing Laboratory." *Council on Foreign Relations*. 18 December 2015. http://blogs.cfr.org/cyber/2015/12/18/qa-with-peiter-zatko-aka-mudge-setting-up-the-cyber-independent-testing-laboratory/.

[95] National Research Council, "Professionalizing the Nation's Cybersecurity Workforce: Criteria for Decision-Making, National Academies Press." 2013 http://www.nap.edu/download.php?record_id=18446.

Acknowledgements

Global Agenda Council on Cyber Security

Chair

Toomas Hendrik Ilves	President of Estonia		

Vice-Chair

Jean-Paul Laborde	Assistant Secretary-General and Executive Director, Counter-Terrorism Committee Executive Directorate, United Nations, New York		

Members

Jane Holl Lute	President and Chief Executive Officer	Council on CyberSecurity	USA
Cheri McGuire	Vice-President, Global Government Affairs and Cyber Security Policy	Symantec Corporation	USA
Jeffrey Moss	President	DEF CON	USA
Christophe Nicolas	Senior Vice-President and Founder, Kudelski Security, and Group Chief Information Officer	Kudelski Group	Switzerland
Sundeep Oberoi	Global Head Delivery ESRM	Tata Consultancy Services	India
Troels Oerting Jorgensen	Chief Information Security Officer	Barclays	United Kingdom
Catherine Lotrionte	Assistant Professor of Government and Foreign Service	Georgetown University	USA
Ali Al Masari	Head of Information Protection Department	Saudi Aramco	Saudi Arabia
James Stavridis	Dean, Fletcher School of Law and Diplomacy	Tufts University	USA
Marc Henauer	Head of Reporting and Analysis	Centre for Information Assurance (MELANI)	Switzerland
John Suffolk	President and Global Cyber Security and Privacy Officer	Huawei Technologies	People's Republic of China
William Saito	Special Adviser, Cabinet Office of Japan		

Lee Xiaodong	President and Chief Executive Officer	China Internet Network Information Center	People's Republic of China
Herbert Lin	Senior Research Scholar for Cyber Policy and Security	Stanford University	USA
John Villasenor	Senior Fellow	Brookings Institution	USA
Eugene Kaspersky	Chairman and Chief Executive Officer	Kaspersky Lab	Russian Federation
Nigel Inkster	Director, Transnational Threats and Political Risk	The International Institute for Strategic Studies (IISS)	United Kingdom
Dave DeWalt	Chief Executive Officer and Chairman of the Board	FireEye	USA

When beginning the latest cycle of Global Agenda Councils in 2014, the World Economic Forum recognized the need to address cybersecurity concerns as they relate to an increasingly connected world. Council Chair Toomas Hendrik Ilves and Vice-Chair Jean-Paul Laborde led a diverse group of high-level experts in a series of discussions on the most pressing challenges presented by a full spectrum of cyber-risks. This paper presents a summary of the main themes of the discussions.

We would like to thank three Managing Directors of the World Economic Forum who provided strategic guidance and oversight for our work:

– Richard Samans, Head of the Centre for the Global Agenda
– Jeremy Jurgens, Chief Information and Interaction Officer
– Jean-Luc Vez, Head of Public Security Policy and Security Affairs

We would also like to acknowledge the leaders of the Global Challenge on the Future of the Internet initiative, who provided a broader framework for the work of the council:

– Mark Spelman, Co-Head of the Future of the Internet Initiative
– Alex Wong, Co-Head of the Future of the Internet Initiative
– Alan Marcus, Head of ICT Industries

We would also like to recognize the leadership of the Network of the Global Agenda Councils:

– Stephan Mergenthaler, Head of Knowledge Networks and Analysis
– Liana Melchenko, Practice Lead, Knowledge Networks and Analysis

And, for liaison with universities, we would like to thank Lyuba Spagnoletto, Head of Communities, Knowledge Networks and Analysis.

In addition to those who served on the council, the World Economic Forum wishes to thank the colleagues without whose support, progress would not have been possible:

– Epp Maaten, Adviser on the Information Society of the Foreign Policy Department of Estonia
– Marc Porret, Laila Ezzarqui and Karine Jeannet, from the Office of the Executive Director of the Counter-Terrorism Committee Executive Directorate (CTED) at the United Nations
– Elena Kvochko, Barclays
– Anton Shingarev, Kaspersky Labs

We would like to particularly thank colleagues from the Berkman Center of Internet & Society at Harvard University, who prepared the paper:

– Urs Gasser, Executive Director
– Ryan Budish, Senior Researcher
– David O'Brien, Senior Researcher
– Amar Ashar, General Manager of Special Initiatives

Last but not least, we would like to express our gratitude to all our partners around the world who joined the meetings and calls and provided their input on the paper.

With many thanks,
Danil Kerimi, Joseph Losavio and Alexandra Shaw

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org