T20 INDONESIA 2022 THINK

Policy Brief

THE IMPERATIVE FOR BUILDING AWARENESS, CAPABILITIES, AND COMMITMENT ON CYBERSECURITY

Task Force 2

Meaningful Digital Connectivity, Cyber Security, Empowerment

Kok-Chin Tay, Smart Cities Network
Sam Parmar, Cyfirma

Abstract

COVID-19 has created new challenges for many sectors as they transform and adapt to an operating model in which “working from anywhere” has become the “new normal”. This policy brief aims to recommend policy changes by political leaders to be proactive in the current climate of increased cybersecurity risks to due to this “new normal” and the exponential growth of the IOT.

The proposed approach is to establish a formal cybersecurity policy that is people-centric and enabled by technology. The recommendations are to foster a risk-based methodology and establish processes to minimize cybersecurity risks and data privacy issues among people and critical infrastructure assets.

Challenges

1. Background – The Estimated Trillions of Dollars in Cost of Cybercrime

According to the Gartner Forecast on the Information Security and Risk Management Spending Worldwide Report, annual spending on cybersecurity by organizations is forecast to grow by 12.4% from 2020, reaching US$150.4 Billion in 2021 [1].

However, the estimated costs of the impact of cybercrime increased from US$3 Trillion in 2015 to US$6 Trillion in 2021, with a projected estimated increase to US$11 Trillion by 2025. These estimates are found in Cybersecurity Ventures publication [2], "Cyberwarfare in the C-Suite 2021 Report," but are not limited to them. The figure below shows the detailed costs of cybercrime according to security expert Cyfirma.

COVID-19 and the exponential growth of sensor networks have catalyzed a digital revolution worldwide. Smartphones, tablets, and other handheld devices have now become the keys to the city, putting instant information about transit, traffic, health services, safety alerts, and community news into millions of hands.

However, in doing so, governments and organizations that monitor these infrastructures have more grounds to cover. Public, private and open sectors are all involved; unfortunately, there is no defined framework to address the risks and subsequent protection needed to safeguard the critical assets against those risks.

2. COVID-19 – Business Not as Usual

The COVID-19 pandemic catalyzed a digital revolution worldwide. It will and has certainly changed the way we work and interact with each other. Digital adoption and online interactions have skyrocketed since the beginning of the pandemic in early 2020.

According to a study by McKinsey & Company [3], businesses have surprised themselves with the speed and success of their digital initiatives in response to COVID-19. On average, digital offerings have leapfrogged seven years of progress in a matter of months.

Similarly, tech giant Microsoft claimed that its customers, which include top IT and government organizations, have had "two years' worth of digital transformation done in just two months."

However, this unprecedented uptake of technology, although feasible and friendly, was adopted hastily, simply because there was no time to use "secure, configure, test, and deploy strategy" for IT Admins of organizations. This has left security holes that have certainly increased the risks for individuals, businesses, communities, and the government agencies alike.

Cybercriminals have taken advantage of this sudden change in work culture and the corresponding change in the corporate technological infrastructure, which can now be penetrated with more ways than previously known to steal confidential information, intellectual property, and/or demand ransom, among other activities.

We have discovered a 600% increase in cybercrime in our survey even a year after the onset of COVID-19—that is, in 2021—and predict that cyberattacks will hit a new high in the year ahead.

3. Exponential Growth of Sensor Networks (IoT and IIoT)

Digitalization will harness technologies such as 5G, Internet of Things (IoT), autonomous vehicles, critical infrastructure, Artificial Intelligence (AI), Industry 4.0, cryptocurrency, cloud, virtual augmented reality (VR/AR), and drones.

The widespread adoption of the Internet of Things (IoT) and Industrial Internet of Things (IIoT) in particular is a use case to be watched from close quarters. These connected devices, estimated at 15 billion in 2022, will expectedly grow to 27 billion by 2025, according to CYFIRMA's Predictions [4]. IoT and IIoT are foundations to smart cities projects with direct impact to not just businesses but also billions of citizens.

IIoT, a sub-sector of IoT, facilitates greater connectivity among equipment, software, and employees in an industrial environment. Although the IIoT market is mostly tied to production-based solutions where automation is key to success, IIoT is quickly growing in capabilities and use cases.

The global IIoT market was valued at about $216.13 billion in 2020 and is expected to grow to about $1.1 trillion by 2028, according to Grand View Research.

As connectivity innovations—such as multi-cloud environments, edge computing, and 5G networks—become more widespread and accessible, we should expect to see more applications of IIoT across global industrial markets.

However, this hyper-connected environment will subject governments and businesses to further cybersecurity risks as it will correspondingly open new avenues for cybercriminals. Thus, there is an urgent need to include all IoT and IIoT products and services into the overall technology infrastructure of the organization with requisite security measures in place.

Proposals for G20

Against the backdrop of heightened cybersecurity threats and risks, governments have a significant role to play in ensuring that businesses can operate without the constant fear of cyberattacks. Regulatory environment can be improved to build cyber resiliency.

Step 1 – Formalize Cybersecurity Policies by the Political Leadership

Cybersecurity policies and organizational preparedness are still lacking and have repeatedly been highlighted by various law enforcement agencies around the globe.

Formulation of policies and the training of staff and individuals require specific actions by governmental and business leaders, which again require the inclusion of educational activities from the ground-up level. However, all these require time and effort, and it is thus desirable that the Taskforce 2 of T20 implement the policies recommended in this paper.

Organizations need to ensure they are focusing on getting the basics right when it comes to cyber hygiene. What does that mean?

1. They need to first identify and classify critical assets in their jurisdiction. Once classified, a risk-based approach should then be designed or graded for all the cyber controls associated to these critical assets.
2. Governments need to make mandatory arrangements and provide recurring training and guidance to staff on cyber hygiene.
3. Understanding the attack surface and current cyber hygiene standards and configurations across the external digital foot print of the respective organization.
4. Finding security gaps, naming the biggest vulnerable areas in the entire digital supply chain, and addressing them.
5. Ensuring visibility and setting appropriate detection controls in place so that threats can be detected at a very early stage if not before their occurrence itself.
6. Issuing a proactive notification in case of a data breach or credential leak and having an incident response playbook ready so that response to such an incident is lightning quick, which may also help limit attacks.
7. Establishing a minimum risk maturity score for every asset/institution, probably depending on its size and domain, in order to allow it to do business. This is a long-term approach and will require an extensive study and involvement of all SMEs concerned.

Step 2 – The Imperative for Systematic Execution

So, how can this be done?

1. **Attack Vector Assessments:** Every company, business, and organization has its own exposed threat landscape that depends upon various factors. Attack vectors also differ. Thus, it is necessary to have a 360- degree view into your threat surface, where attack vector assessments can act as a turning stone. These assessments will uncover new attack surfaces as businesses adopt new digital formats and build further supplier-partner-customer connectivity. This should be undertaken at least once a year.

2. **Mandatory Risk and Vulnerability Assessment:** This needs to be undertaken at least bi-annually when it comes to larger enterprises and on a monthly or quarterly basis for small to medium-sized enterprises. This will help identify threats early and remediation can take place to close any cybersecurity gaps.

3. **Continuous Monitoring and Visibility:** Cybersecurity incidents can happen on Christmas Day, at 3:00 a.m., in the middle of conventions, or while you are having a cup of coffee in bed. With these kinds of demands, a Security Operations Center (SOC) needs to be designed to detect and immediately respond to imminent threats at a nascent stage.

   There must be continuous monitoring so that defenders are aware of the new devices and technologies joining and being adopted into the ecosystem. A full visibility on the external threat landscape to understand threat actors, motives, campaigns and methods will be essential to ensure cyber adversaries do not gain access in the first place.

4. **Mandatory Cyber Incident Reporting:** One action to take would be to make cyber incident reporting mandatory. Incident reporting encourages a culture of cybersecurity. It streamlines the process to prevent incidents from becoming a serious attack, enforces security policies, prevents or minimizes monetary losses, and also helps maintain regulatory compliances such as ISO27001/2, GDPR, among others.

   Additionally, this will create a body of researched data which can then provide insights on threats to the nation and inform the government on strategies to undertake to strengthen the nation's cyber posture.

5. **Bug Bounty Program:** A cyber reward culture can also be cultivated where the discovery of bugs and vulnerabilities are rewarded. This effort uplifts the cybersecurity community and promotes a culture of knowledge sharing and collaboration among the cybersecurity community and the entire public sector.

Step 3 – The ABC Methodology for Cybersecurity

Cybersecurity is a complex and sophisticated subject. It can only be understood when you get the basics right. In this policy brief, we propose the "ABC" methodology of understanding cybersecurity:

A. Awareness of Cybersecurity

The proliferation of Industry 4.0, which includes the billions of IoT devices, has only raised the spectre of cybersecurity, making governments, business communities, and end users extra cautious of the risks and exposures of the digital world and the repercussions that it holds.

For this, we recommend the adoption of the following policies:

1. Mandatory cyber threat monitoring to ensure businesses are kept abreast of their external threat landscape and always understand their digital risk posture at real-time or near real-time.

2. Mandatory training and certification for all government employees, updated annually to remain in sync with the latest technologies and the corresponding threats.

3. All businesses that require handling of consumer/customer details should have qualified security personnel who are familiar with all the cybersecurity threats associated to the respective domain.

4. Irrespective of the grade or the hierarchy of a user in a particular organization, all users should be given mandatory basic cybersecurity education offered by experts.

5. Regulatory controls for listed companies should include mandatory cyber hygiene. This refers to ensuring listed companies who are accountable to shareholders and the general public, and follow a set of guidelines on how they should handle data, protect their

corporate digital assets, manage third-party cyber risk, and build cyber awareness amongst their workforce.

B. Building Capabilities and Capacities

We recommend the following policies to be adopted in order to develop capabilities and capacities to address the cybersecurity risks, threats, and ensure data privacy:

1. **Be Proactive** – Move from the common event-driven and reactive cybersecurity approach to intelligence-driven predictive approach aimed at strengthening cyber posture management.

2. **Conduct Regular Training** – Educating employees to be wary of unsolicited emails or social media posts which contain attachments can go a long way. But this needs to be done by providing routine training and conducting tests that would rate and improve their cyber awareness understanding.

3. **Integrate Cybersecurity into the Business Objectives and Processes** – This means from the time a business or organization makes a market entry, adoption of new technology and innovation should have cybersecurity assessment in place. This leads to the adoption of cybersecurity awareness within the organization and among the employees.

4. **Plan and Conduct Periodic Red Team Exercises** – One of the least performed yet highly effective capability that any organization can have is having a red team that can perform periodic offensive tests and help measure the effectiveness of the people, processes, and security technologies used to define the entire ecology of that organization.

5. **Get foundational controls and capabilities right** – Ensure visibility, monitoring, perimeter defenses are in sync and there is a dynamic/agile way of managing cybersecurity to counter the fast-evolving threat landscape.

6. **Use AI/ML** - Automate and orchestrate workflows and playbooks to help with rapid discovery and response.

Building Capabilities Idea #1 - Building a Human Firewall

Like COVID-19, the pandemic of cybersecurity threats has now become an endemic and no one's data is safe anymore. Organizations are always at risk of being attacked from the external threat landscape; and they are probably, if not equally, at a higher risk of threats from within the organization as well. An organization's security can be easily crashed by an employee or human error, where careless or ignorant staff members are currently the second assured cause of a serious security breach, according to several studies.

Organizations can therefore not afford to overlook the primary significance of training its employees of the threats and best practices to encounter cybersecurity. So, how well is your organization or employee equipped against highly skilled criminals, malicious hackers or nations that aim to steal data or any other valuable information or service?

A survey, State of IT Security 2019, shows that email security and employee training are the top challenges faced by information technology (IT) security professionals. Despite firewalls and other security software, employees are still the most common entry points for phishers. For a company with more employees, equally, the entry points increase and likewise, it implies an increase in "phish" in the sea.

Building Capabilities Idea #2 - Topics for Capacity Building via Training

Cybersecurity training needs to be mandatorily provided to help all employees protect themselves and the company against cyberattacks and threats. Training empowers employees with an up-to-date know-how to recognize and mitigate a cyber threat. By making employees able to identify and eliminate cyber threats, you are strengthening the most vulnerable link in the chain.

With the current IT infrastructure, most hackers use artificial intelligence nowadays. Systems are manipulated such that most breaches involve some kind of human error. Organizations should therefore train their employees to avoid attack from social engineering to protect their fundamental resources for conducting business and flawlessly interact with customers.

Simple and repetitive tasks can be modelled into automated systems. Nevertheless, people will always be behind the operation of any automated task and on the end of every email, chat session or a phone call. People, therefore, present the concept of "human factor" in the crosshairs or cyber attackers. The only defense against such attacks is by education or in other terms, by providing employees with security awareness training.

Topics to cover in employees' cybersecurity and awareness program are:

- Different and latest forms of cyber threats.
- Password security.

- Identifications and reporting of cyber threats.
- Email, internet, and social media policies and safe usage terms.
- Best practices for a safe cyber usage.

Building Capabilities Idea #3 – The Use of Artificial Intelligence and Automation

Artificial intelligence is a two-edged sword that hackers might employ as a security solution or as a weapon. AI comprises the creation of programs and systems that can exhibit human-like characteristics. The ability to adapt to a specific environment or respond intelligently to a circumstance is one of the traits. Artificial intelligence (AI) has been widely used in cybersecurity solutions, but hackers are also using it to create sophisticated malware and carry out stealth assaults.

AI can be used to execute intelligent attacks that can multiply over a system or network. Smart malware can exploit unmitigated vulnerabilities leading to a full-fledged attack. If an intelligent attack comes across a patched vulnerability, it can adapt to try different ways to attack to achieve its objective.

Artificial intelligence (AI) can be used to construct malware that can imitate trusted system components and be employed in stealth assaults. Cyber criminals, for example, utilize AI-enabled malware to understand an organization's compute environment, patch update lifecycle, types of communication protocols. As a result, hackers can carry out undetectable assaults by blending into a company's security environment.

Changing malware behaviour can be hard to rein in. "Multimorphic" malware is fast becoming a reality. State-sponsored threat actor groups are developing malware that cannot be easily detected. This type of "multimorphic" malware can switch seamlessly across stages of a cyberattack, such as reconnaissance, exploit, and exfiltration. Deciphering the actual behavior path of such malware will be difficult as it utilizes complex obfuscation techniques based on selected inputs derived from the target's unique characteristics. It would be hard to identify this type of malware as there is no historical behavior to track.

To counter these sorts of AI-powered cyberattacks, organizations would need to move away from an "event-centric" cyber defense strategy to an "intelligence-led" approach. In the latter, defenders would gather insights to cyberattacks at the early planning stage and take appropriate action to remediate security gaps. This proactive method requires cybersecurity to utilize predictive capabilities—being aware of cyberattack campaigns at the stage of planning and reconnaissance and not at the stage of weaponization and exploit.

Due to the resource crunch for cyber security expertise, AI-enabled tools and platforms will allow automation to detect and prevent cyber attacks based on the roles defined. This means

such machine-based execution of actions can automatically detect, investigate, and remediate cyberthreats with or without human intervention. It would subsequently prioritize alerts as they emerge, and perform automated incident response.

C. Commitment by Leaders

To minimize the disastrous consequences of cybersecurity breaches, it is imperative for the political leaders of each country to seriously consider the real threats and risks of cybersecurity for government agencies, the business community, and the population at large.

We recommend that the political leadership commit to an Action Plan to address the Cybersecurity threats by formalizing an Inter-Ministerial Taskforce for the CyberSecurity policies and supporting infrastructure.

We also recommend the following specific action items for all the ministries and agencies:

1. **Formulate a Cybersecurity Policy Handbook** – This will help all government ministries, and businesses to remain in-sync and even be controlled by a singular cybersecurity agency.
2. **Establish Cybersecurity Sub-Taskforces in each of the ministry and agency** – Develop a taskforce that will be led by a qualified professional and will be supported by representatives from all departments to ensure compliance to the cybersecurity policy.
3. **Monitor and Assess Cyberthreats on a regular basis** – all the Cybersecurity taskforces will be mandated to report their assessment of the Cyberthreats of their ministries or departments on a regular basis. It will be consolidated at the Inter-Ministerial Committee to evaluate the overall situation for the city or country.

CONCLUSION

This policy brief highlights the importance of critical paths towards a more protected world against the real threats of cyberattacks and cybercrimes targeting governments, business communities, and society at large. Key takeaways from our paper include:

1. There is an imperative for governments around the world to proactively establish national policies with respect to Cybersecurity and form a decentralized network of Task Forces to implement these policies.
2. We propose the “ABC” approach for such implementation in a proactive manner:
    - Awareness – assist the various Task Forces of the various vulnerabilities of the organizations and types of cyberattacks and crimes.
    - Building Capabilities – provide different kinds of training and workshops, incorporating artificial intelligence and automation in these programs.

- Commitment – by the political leadership with funding and resources to support the awareness and capability building of the task forces, business communities, and society at large.

3. We look forward to seeing the adoption of our recommendations among the G20 countries, and globally, and would be most happy to support in taking the next steps further.

References

Gartner, "*Garner forecasts Worldwide Security and Risk Management Spending to exceed $150 Billion in 2021*", https://www.all-about-security.de/english-news/gartner-forecasts-worldwide-security-and-risk-management-spending-to-exceed-150-billion-in-2021, accessed June 2022

Cybersecurity Ventures (2021), "*Cyberwarfare in the C-Suite 2021 Report*"

McKinsey and Company (2022), "*COVID-19: Implications for Business*", April 13, 2022, https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/covid-19-implications-for-business, accessed June 2022

CYFIRMA (2022), "*Cybersecurity Predictions 2022*", https://www.cyfirma.com/cyfirma-cybersecurity-predictions-2022/, accessed June 2022

CYFIRMA (2022), *"The Case of External Threat Landscape Management" https://www.cyfirma.com/the-case-for-external-threat-landscape-management/, accessed June 2022*

ABOUT THE AUTHORS

- Generally acknowledged as a global thought leader for Smart Cities – member of the Advisory Board for ESI Thoughtlab, a think-tank based in Philadelphia, and ASEAN Director of Smart Cities Council, the largest ecosystem of stakeholders in the world with over 600 cities in their network
- Instrumental as a catalyst in getting the Singapore government to launch Smart Nation in 2014. He is the Founding Chairman of Smart Cities Network, a not-for-profit organization incorporated in 2018 and led its strategic partnerships with governments and industry bodies globally, including UN-Habitat.
- Smart City Advisor and Capacity Builder for the Philippines Department of Science and Technology (DOST) and Consulting Expert for the Phnom Penh City Government (Cambodia).
- Smart City Advisor for several companies – developers in Vietnam and Bangladesh, and start-ups based in Singapore and the UK.
- Speaker on topics related to Smart Cities since 2017 and Adjunct Lecturer for several academic institutions in Singapore and Phnom Penh (Cambodia)
- He can be contacted at KC.Tay@SmartCitiesCouncil.com

- Sam is a cybersecurity and technology leader helping organizations craft IT security governance, risk management, compliance, and training strategies.
- Sam has spear-headed cybersecurity strategies for one of the largest mining companies in the world, aligning a 5-year company-wide roadmap with the NIST framework.
- He has also consulted with a myriad of industries ranging from high-tech farming and manufacturing to hospitality and telemedicine. Sam takes pride in seeing the strategies take flight and yielding tangible business outcomes.
- Sam has applied his cybersecurity expertise across both information and operational technologies. Having led cybersecurity projects and seeing to the successful implementation of digital transformation initiatives, Sam now applies his knowledge to helping CYFIRMA's clients solve some of the most pressing security challenges.
- He can be contacted at Sam.Parmar@Cyfirma.com

ABOUT SMART CITIES NETWORK

Smart Cities Network is a global platform for thought leadership, business intelligence, knowledge sharing and creating business opportunities for the smart city global community.

It is a not-for-profit individual membership-based organization, whose members are professionals with expertise in a wide variety of themes, aligned to the various frameworks and digital transformation roadmaps.

Our aim is to develop an ecosystem where thought leaders, innovators, consultants, analyst, networkers, government, private and public organizations can come together to work collaboratively.

Together, we want to build inclusive, sustainable and smart cities that are physically and digitally secure, respectful of our natural environment, improving the quality of lives, developing a competitive economy and aligned to the UN Sustainable Development Goals.

www.smartcitiesnetwork.net

ABOUT CYFIRMA

CYFIRMA is an external threat landscape management platform company. We combine cyber intelligence with attack surface discovery and digital risk protection to deliver predictive, personalized, contextual, outside-in, and multi-layered cyber-intelligence.

We harness our cloud-based AI and ML-powered analytics platform to help organizations proactively identify potential threats at the planning stage of cyberattacks. Our unique approach of providing the hacker's view and deep insights into the external cyber landscape has helped clients prepare for upcoming attacks.

CYFIRMA works with many Fortune 500 companies. The company has offices located in the USA, EU, Japan, Singapore, and India.

www.cyfirma.com