IIMC Library Clipping Service Source: News: Online: Forbes India Dated: 14-07-2022

Seven challenges against securing the systemic cyberspace in the industrial IoT age

As organisations in the growing industrial IoT space become increasingly mutually dependent on one another and contribute to growing systemic cyber-risk, here are the seven most important emerging anti-forces they face

BY RANJAN PAL AND BODHIBRATA NAG

It has been widely known for years that the cyber-security business is severely understaffed with respect to the technology it is supposed to protect, both at the level of specialists/experts and across the non-expert workforce.

Every new technology carries the potential to change the existing cyber-risk landscape that business organisations face today. In recent years, one of such new technologies has been the Internet of Things (IoT) which most business industries (service sectors) are increasingly relying upon. More specifically, these customer-facing service sectors—manufacturing, transportation, retail, finance, and energy, among many others—have begun to heavily exploit the opportunities that ubiquitous data-sensing, 5G-driven mobile communications, and rapidly scaled-up automation in IoT-driven control systems bring to derive efficiency, improved customer experience, and new service opportunities. Moreover, the pervasive IoT technology will result in business services that are

hyper-connected and interdependent, operating on sophisticated shared infrastructures and relied on to support critical functions across society and industry.

RSS_On the flip side, the ubiquitous connectivity characteristic of IoT technology is introducing systemic cybersecurity risk in service-networked business supply chains that will only increase over time as the technology matures and becomes widely adopted. This is primarily due to three key features. First, the sheer scale of the IoT-connected service world will rapidly expand the cyber-attack surface, with an increased risk to confidentiality, integrity, and availability of digital assets. Second, IoT-driven smart societies are woven through complex interdependencies between business and government organisations, supply chains, sectors, and individuals that open up channels for cascading cyber risk. Finally, most of this interdependent IoT-driven smart society shares communication and computing resources through the cloud, internet service providers, and hardware/software product vendors. This creates a correlated cyber-attack surface that increases both the chances of attack and the potential for severe systemic impact causing cyber-security compromises.

As organisations in the growing industrial IoT space become increasingly mutually dependent on one another and contribute to growing systemic cyber-risk, they can no longer consider their capabilities to ensure cybersecurity and resilience. One should consider the cyber-resilience of the entire networked ecosystem. It is, therefore in the interests of the ecosystem stakeholders to join hands to ensure that the basic minimum cyber-assurance standards are met in this ecosystem. And that risk aggregation can be identified and monitored within end-to-end services and supply chains as well as shared infrastructures. The basic prerequisite is to pinpoint the most important challenges working against striving for the minimum cyber-assurance thresholds.

We set out in this article to identify and lay down the seven most important emerging anti-forces (challenges) against securing this modern and rapidly expanding systemic IoT-driven industrial cyberspace upon which current business sectors are increasingly relying.

1. WIDENING GAP IN NEEDED CYBERSECURITY RESOURCES:

It has been widely known for years that the cyber-security business is severely understaffed concerning the technology it is supposed to protect, both at the level of specialists/experts and across the non-expert workforce. This trend is only going to increase with rapid technological innovation. Unless education, training, and the socio-economic importance of cybersecurity are accelerated significantly in society, and among corporation employees, business organisations are always going to fall behind in securing applications and services driven by state-of-the-art technology. Moreover, a general lack of minimum required level of cyber literacy among leaders (C-suite) and innovators has overshadowed the importance/appreciation of a high financial budget that always needs to be allocated to hire the best cyber-security staff in quality and quantity.

2. THE FRAGMENTATION OF CYBER-GOVERNANCE:

The systemic and interdependent service network ecosystem is growing at an odd time when the global governance of cyberspace is weak. A siloed approach is the status quo for the applicability of technical standards and cyber-governance principles, with incompatible security-compliance requirements and not enough communication between the jurisdictional and sectoral siloes across businesses and nation-states. This lack of communication is often rooted in geopolitical divergence and protectionist stances within the siloes. The overall fragmented cyber-governance will adversely affect the ecosystem's cyber-security strength.

3. MISFIT OPERATIONAL AND TECHNOLOGICAL SECURITY TOOLS:

Apart from the just-mentioned cyber-governance non-coordination between relevant siloes, existing operational and technical cyber-security capabilities are well below par to address sophisticated and naive emerging cyber-attacks on new technologies and data formats. This automatically affects the effectiveness of joint policy-driven operations, even in the ideal case if cyber-governance were not to be fragmented. Such (tech-driven) policy operations include

information sharing; collective response; and detection, disruption, and deterrence of cybercrime. The need of the hour is to AI-automate most, if not all, of these operations and execute them in real-time to ensure their dynamic and effective interoperation, at the pace necessary to address emerging cyber-threats.

MISALIGNED CORPORATE INCENTIVES AND INFORMATION ASYMMETRY:

Security is often given a secondary or tertiary consideration in the design process of emerging technology innovations. The age-old proverb "market first, fix later" has continued to hold in the technology industry for decades. Emerging technologies such as IoT devices have been designed and market-deployed widely with minimal security features built-in - too insignificant for the huge space of existing and emerging cyber-attacks they are subject to. This 'market-capturing' design mindset creates a significant negative externality on service supply chains through rare catastrophic events such as the Mirai DDoS attacks executed via IoT devices' compromise, causing global service network ecosystem losses worth billions of dollars. Furthermore, there is the inherent information asymmetry problem, whereby tech innovators are unaware—and at times careless—of the intricate complexity of service supply chains their technology will be part of. They make false assumptions about the existing security inherent in the supply chain ecosystem upon which their solutions are layered, aggravating the chances of major cyber-attacks in such ecosystems.

5. AMBIGUOUS ACCOUNTABILITY:

Taking off from the previous point, while shared service dependence among organisations in a service network might be able to take advantage of cyber-risk diversification benefits to ensure resilience, it can also create ambiguity in the accountability (a result of market competition between the organisations and information asymmetry regarding private intra-organisational security accountability policies) for ensuring this resilience, assuring end-to-end services and shared critical infrastructures. The ambiguity will only grow with the intricacies of the underlying service-networked ecosystem. It will complement the Information asymmetry-driven free-riding effects that drive the sub-optimal level of cyber-resilience in such ecosystems.

6. BELOW-PAR CYBER-THREAT INFORMATION SHARING

cyber-threat information sharing is vital for effective collaborative operational security in systemic supply chain networked environments. By sharing information on (a) the threats targeting these environments and (b) indicators of compromise and responses, organisations in a service network can collectively improve their cyber-resilience capabilities and make it increasingly difficult and costly for malicious cyber actors to launch systemic cyber-attacks. Though currently there exists information sharing and analysis centres (ISACs), they are incapable of meeting the information sharing demands of the intricate service-networked environments. In addition, there is a shortage of technological innovations that can securely and privately communicate high-volume, high-speed cyber-threat information between stakeholders in a supply chain service network.

7. CYBER-INSURANCE CHALLENGES:

It is widely known that cyber-insurance, in principle, has the potential to improve cyber-security. However, systemic cyber-risks in service-networked ecosystems greatly challenge commercial cyber-insurers in primarily multiple different ways when accurately assessing the cyber-risk posture of organisations and effectively underwriting aggregated loss coverage portfolios—both necessary conditions for improving cyber-security. First, an absence of effective regulation regarding the proper language of reporting cyber-breach incidents, in addition to weak cyber-threat information sharing policies, generates asymmetric information barriers when allocating liability among networked stakeholders for cyber-incidents. In addition, in a large-enough service network, the visibility of risk sources is reduced for a cyber-insurance agency—further dampening effective ownership of cyber-risk. Moreover, there is a huge void in the quantitative model space that can accurately estimate (aggregated) cyber-risk in such complex service-networked settings under small amounts of cyber-threat data. Finally, technologies such as driverless cars cross multiple insurance silos. For such emerging technologies, the liability for security and ownership of cyber-risk is blurred among a supply chain of manufacturers and service providers.

In summary, there are hidden and systemic risks inherent in the emerging industrial IoT-driven technology

environment supporting service-networked ecosystems, which will require significant changes to the international and security community response to cybersecurity. Policy interventions are required that incentivise collaboration and accountability for businesses and governments.

Ranjan Pal (MIT, USA & University of Cambridge, UK)
Bodhibrata Nag (Indian Institute of Management Calcutta))

Source: https://www.forbesindia.com/article/iim-calcutta/seven-challenges-against-securing-the-systemic-cyberspace-in-the-industrial-iot-age/78113/1