Deep Science Publishing
https://doi.org/10.70593/978-93-49910-67-6_10

Chapter 10: Ensuring cybersecurity and data privacy in expanding digital infrastructure ecosystems

10.1. Introduction

The growth in interconnected Digital Infrastructure Ecosystems (DIE's) which facilitate information exchange is coupled with a corresponding increase in vulnerability to cyber threats. To protect against cyber threats to individuals and business processes, one must protect not only the information's confidentiality, integrity, and availability (CIA), but also accountability and assurance (AA) — both essential to the proper functioning of dependent processes, and of a DIE itself, comprised of many Link/Message Exchanges

Fig 10.1: Ensuring Cybersecurity and Data Privacy in Expanding Digital Infrastructure Ecosystems

upon which these dependent processes rely. Traditional laws and cybersecurity frameworks center solely on the CIA triad to protect the Exchange messages themselves. Consequently, organizations do not effectively ensure the quality of their Link/Messages Exchanges, exposing themselves and their information to threats of manipulation. Even risk-based best practice regulatory schemes consider only the potential for loss or misuse and not the potential for deliberate uncertainty of a DE's Link/Message Exchanges. Ensuring Cybersecurity and Data Privacy in Expanding Digital Infrastructure Ecosystems is challenging. This essay reviews the inadequacies of CIA-centric InfoSec, Privacy, and Accuracy regulations. We finally suggest an innovative supervisory control approach to adequately LTC for DIE Assurance and Confidentiality (Katal et al., 2013; Hashem et al., 2015; Chen et al., 2019).

The nature of DIE threats requires that organizations transition towards a supervisory trusted computing paradigm for Trust and Privacy over the LINK/MESSAGE Exchanges within DIE. Trust is a qualia — an intrinsic manner of trusting perception — that is not communicable through authorized Trust Assignments. Therefore, TA's can neither facilitate nor ensure the Transactions or Exchanges that constitute Governance within the Transaction-based Modeling Architecture do not experience Trust Bubbles or Trust Gaps. However, the success of Transactional Models (T's) exposed to TA's depends solely upon the Acting Trustor, the enacted TA's, and the entity upon which the TA is imposed — i.e. the Acted Trustor from which Assurance is sought.Historically, cybersecurity has emerged in the United States as a national priority after the discovery of the possible exploitation by opportunistic and determined individuals and organizations and even hostile states of defects in mapped implemented protocols and functions of computers that are connected to or linked by the network. But it is only after the release of the computer worm called “Morris” that cybersecurity gained practical visibility as such (Zaharia et al., 2016; Mehmood et al., 2017).

10.2. Understanding Cybersecurity

The term cybersecurity has been defined in many different ways. These range from simple definition such as “the system, function and effect of information assurance in the use of a networked computer or computer systems” to a more elaborate description of the effect of cybersecurity (“functional capability to preserve the availability, integrity and confidentiality of the information of a system”) to a higher abstraction level definition (“the property of a networked computer or computer system that is set to preserve the availability, integrity and confidentiality of the information of the computer or computer system”) to another definition concerned with security management (“discipline resulting from the practice of information assurance in the use of a networked computer or computer systems”). To complete this non-exhaustive collection

of definitions and in order to stress the similarity and distinction between cybersecurity and information assurance, we will quote the definition on information assurance in the cybersecurity lexicon. Cybersecurity has originated as a means to achieve information assurance in networked information subsystems.

10.2.1. Definition and Importance

Cybersecurity describes the processes, technology, and practices designed to protect computer systems and networks from damage, theft, or unauthorized access. To be effective, these protective measures must safeguard not only the devices and networks that make up an information technology system, but also the data that resides on or moves through these devices and networks. Cybersecurity is increasingly critical for individuals, businesses, and government agencies as the number of attack vectors associated with computer systems expands. Cyberthreats and attacks may target mobile devices, cloud computing environments, websites, email accounts, and social media platforms, as well as the networks and systems that run industrial applications and critical infrastructure. A successful cybersecurity process appropriately protects the privacy of users, as well as the integrity and availability of information and systems. To achieve this goal, cybersecurity programs must remain in existence even as threats evolve and grow, as evidenced by the recent rise in widespread cybercriminal attacks on essential internet services and a whole galaxy of increasingly sophisticated malware and ransomware threats. Cybersecurity programs must enlist defense measures that go beyond user education and training, as well as risk assessment and mitigation processes that work at the individual system and network level, to identify a broad range of potential attacks and risks. Cybersecurity is also about increasing an organization’s overall security posture, with strong access control measures and monitoring processes that log all access events, and incident response planning and exercise processes that ensure rapid recovery from an actual cyber event. Cybersecurity draws from fields such as computer science, information technology, and information assurance to create a comprehensive defense against today’s wide range of digital threats.

10.2.2. Historical Context

The term "cybersecurity" appears to have first been used in 1989 in a report that stated: "As we enter the 1990s, we increasingly depend upon computer systems for our economic and physical health, and the security of these systems is equally important. The term 'cybersecurity' refers to the measures and controls that ensure confidentiality, integrity, and availability of our information and computer systems." The report highlighted the increasing dependence of business, commercial, and government

functions on cyberinfrastructure, how this was creating expanded vulnerabilities to malfeasance and accidental actions to undermine such systems, and that information security had become a discipline in its own right. The report also noted that such systems formed the "very infrastructure of the economy," and how undermining the security and safety of those systems would greatly impact the economy more broadly.

The term became more widely used in the 1990s, including in a publication that defined cybersecurity as the "ability to protect or defend the use of cyberspace from cyber attacks." It is now widely used to refer to the many aspects of protecting networks, devices, programs, and data from potential cyber threats. Central to its importance, for both governments and private enterprise, is that information systems are fundamental to the functioning and operation of a wide variety of services, products, and sectors, including the economy more broadly. Simply stated, ensuring the security of these systems helps ensure trust and confidence in the services and products that depend on those systems and in the users of those services.

10.3. Data Privacy Fundamentals

Key Concepts Data privacy addresses the proper handling of sensitive data by organizations, businesses, and governments in the data lifecycle – from collection and storage to processing and sharing, analysis, and ultimately destruction. Personal data is any information that relates to an identified or identifiable individual, while sensitive information includes not only sensitive personal data but also confidential business information such as trade secrets. By preventing unauthorized use or sharing of sensitive data, data privacy aims to uphold an individual's right to control how their data is used. Important principles of data privacy include transparency, choice, and data minimization.

Several key technologies help support data privacy. Data masking obscures specific data elements within a database table or cell, and data tokenization replaces sensitive data elements with non-sensitive equivalents, known as tokens. Data loss prevention technology is designed to prevent data breaches while data discovery catalogues data locations and enables organizations to classify data according to its level of sensitivity and corporate policies. Data encryption uses mathematical algorithms to scramble data in a way that can only be deciphered via a decryption key.

Legislation and Compliance Most data privacy requirements in the United States come from sector-specific and state-level regulations rather than a single comprehensive federal law. In 1996, Congress passed the Health Insurance Portability and Accountability Act, which requires organizations in the healthcare sector to protect patient information and follow certain protocols for data sharing. The Children's Online

Privacy Protection Act was enacted in 1998 and requires websites, apps, and other services that are directed to children under the age of 13 to obtain parental approval to collect personal information from children before such data can be collected. In 2003,

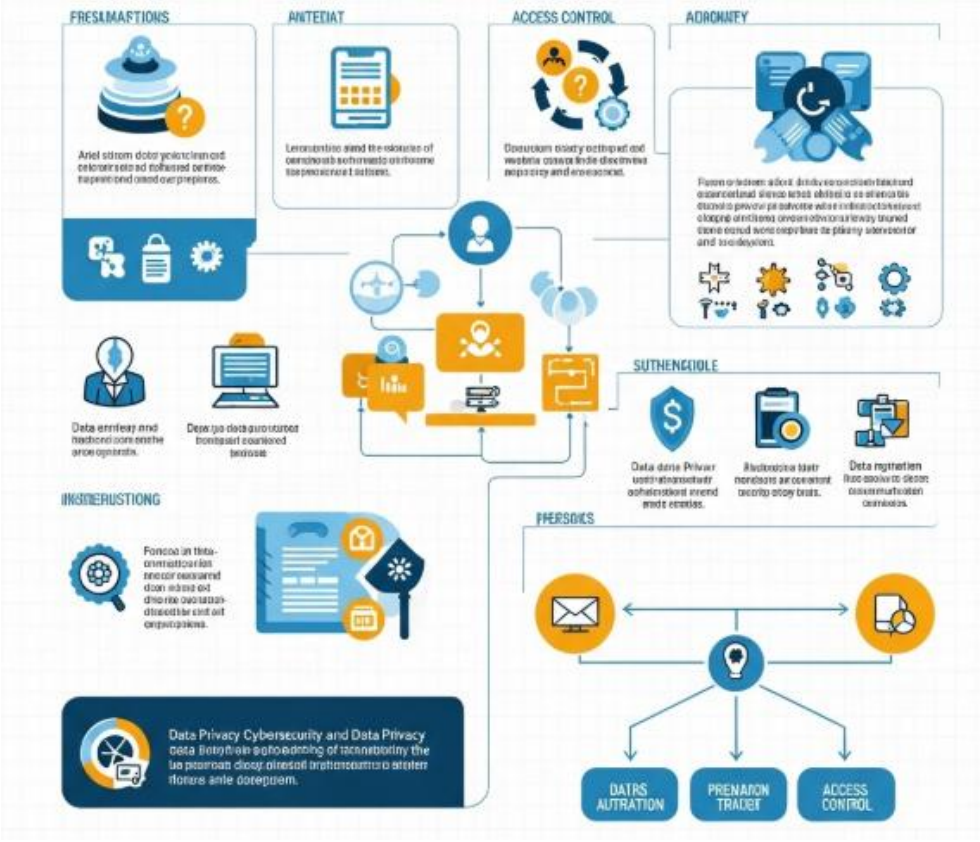

Fig 10.2: Fundamentals of Ensuring Cybersecurity

the Federal Trade Commission imposed certain requirements on financial institutions via the Gramm-Leach-Bliley Act on how they should gather and protect customer data.In addition, in the United States, the Federal Trade Commission Act prohibits unfair or deceptive acts or practices and mandates clear disclosures before acquiring and using personal data. Federal laws govern telecommunications, wire and electronic communications, and computer security; protect sensitive information about children; prohibit information discrimination for loans, employment, or insurance; apply when there is a breach of data involving sensitive information; prohibit harm to individuals such as through stalking or harassment; impose retention requirements; and require sharing of information with law enforcement. A key element of effective cybersecurity is adhering to best practices established by sectoral experts. These best practices complement legal requirements.

10.3.1. Key Concepts

Fulfilling individual rights and organizational obligations around data processing are key pillars of data privacy. Organizations have privacy obligations, such as the creation of accountability programs, defining the roles and responsibilities of staff who process data, implementing and documenting necessary training, informing and communicating with appropriate stakeholders and individuals, maintaining records of data processing activities, conducting necessary data privacy impact assessments, developing communication protocols for dealing with inquiries and complaints, and/or reviewing supplier and vendor relationships to ensure that they share responsibility for safeguarding individual rights. Violations may be met with civil and, increasingly, confidential municipal complaint systems, and in some cases the principle of private action may apply. In addition, appropriate compensation systems for affected individuals may be initiated and civil and possible criminal penalties applied by organizations and public or expert authorities.

For individuals, the data subject basic rights on which the requirements of data privacy are based include the right to be informed; the right to access; the right to rectification; the right to erasure; the right to restrict processing; the right to data portability; and the right to object. Although actual individual data subject rights can differ between jurisdictions and treaties, the Ideal Data Subject Rights suggest a comprehensive synthesis of data subject guarantees, and anchored in data privacy ordinances, specifically treaty-based international guarantees, and the corresponding national Data Protection Authorities and their legal cases or guidance documents.

10.3.2. Legislation and Compliance

In jurisdictions where data protection laws do exist, digital infrastructure technologies must be designed and operated to meet legal compliance. These legal regimes differ in many important ways, notably the breadth of confidentiality protections, the range of entities covered by the laws, the types of data and the purposes for which data may be used, the data subject rights guaranteed, and the nature and severity of consequences for violations. Especially important for the success of a U.S. data privacy system, which is subject to less data subject control than other systems, are public company disclosure of privacy gain or loss, remediation of privacy losses, shareholder litigation, and authority over U.S. tracking of browsing behavior and changes in data privacy without informing data subjects. Globally, digital infrastructure technologies should not be used for "public" or "common good" purposes – such as safety, security, municipal services, economic development, health care, education – in countries where such uses violate the Constitution or laws. Even when not explicitly addressed, the Fundamental Principles of Information Privacy: collection limitation, data quality, purpose specification, statutory

protection, security safeguards, openness, individual participation, accountability, and public awareness should guide conduct.

10.4. Digital Infrastructure Ecosystems

Digital Infrastructure Ecosystems extend beyond the unique components of trusted networks, trusted computing, distributed ledger, trusted services, and trusted marketplace. Digital Infrastructure Ecosystems provide a service framework for trusted digital infrastructure services. Digital Infrastructure Ecosystems are complex, multi-stakeholder collaborative structures made up of diverse public and private entities that need to work together to provide security. In the digital communication context, infrastructures consist of satellites, terrestrial lines, base stations, routers, switches, and devices. But the Digital Infrastructure Ecosystems' depth and breadth go beyond the technical hardware that facilitates the layer of digital services accessible to users. Digital Information Ecosystems include the physical cybersecurity resources as well as the vendors that make and integrate these components, cybersecurity service providers, and the solution vendors at the application level shielding user and critical infrastructure data, identities, and assets from thievery and manipulation, as well as thwarting hostile attacks designed to damage the operations of critical infrastructure or induce denial of service. Digital Infrastructure Ecosystems are reliant on local, state, and federal government investment in cybersecurity and the educated and certified cybersecurity workforce needed to successfully manage, assimilate, implement, and operate the tools that enable happy and safe digital experiences and relationships. The Digital Infrastructure Ecosystems' trusted components and business models also draw heavily from trust principles found in other aspects of safety and security within the communities broadly divided into safety, security, and health, such as transportation industry regulatory frameworks, inspection, and licensing, and public telecommunications regulatory models.

10.4.1. Components of Digital Infrastructure

Digital infrastructure is defined as an asset that supports rapid digitalization with a suite of basic services and leading-edge technologies for e-Government services, the digital economy, and digital society. Digital infrastructure is a new but emerging concept driven partly by the emergence of digital economies, e-Government services, and digital urbanization. Digital infrastructure has three characteristics which describe its key components, i.e., it is not just about physical computing equipment but networks and digital services that can be rapidly scaled; it supports difficult-to-qualify but necessary borderless public good services; and, it provides backbone services that permit and

induce the fast replication of country services and eliminate inefficiencies in terms of investments by other parties. Digital infrastructure allows for faster but economically efficient country transformation into digital economies, digital societies, and smart cities. Therefore, digital infrastructure becomes a suite of core services that allow for economy-wide digitization and create an enabling environment for spurring private-sector investment in constructing digital economy digital services.

Digital infrastructure comprises both physical and non-physical components. Physical components include computer processing systems, data storage components, physical networks, border gateways, and hardware shipping logistics. Non-physical components include globally familiar access services such as cloud computing, data storage, artificial intelligence as a service, Big Data analytics, data security, machine-to-machine communications, and related borderless professional technical services. Digital infrastructure serves as the backbone for the multitude of private digital economy services providing digitalization through mobile apps in financial services, health services, entertainment, retail, education, travel, and hospitality, distribution logistics, manufacturing, and other related technical and business consulting services.

10.4.2. Trends in Digital Expansion

An estimated 24 trillion devices will be connected to the Internet by 2030, the equivalent of 3,000 connections for every person on the planet. The 4th Industrial Revolution is spearheading new technologies such as AI, Cyber-Physical Systems, Digital Twins, and the Digitization of everything driving this expansion. Given our increasing reliance on such devices, we must mitigate risks that come with it at every single opportunity and failure to do so creates data privacy and cybersecurity concerns that have led many developed and developing countries to formulate their own legal, compliance, and regulatory frameworks. These new rules are geared at implementing privacy protection mechanisms across all devices or services that we rely on. Among notable mentions, fines ensure data privacy and protection across their customer stores or face hefty fines, which can go up to 20 million Euros or 4% of worldwide turnover associated with the violation. Organizations that send data to countries that lack data privacy or protection regulations are also liable, which has additional ramifications.

Given that Digital Twins are taking center stage in the strategy of many organizations across various industries, we advise organizations to mandatorily undertake risk assessments of the vendor infrastructure within which data would be housed. Third Parties are the single largest threat that exposes organizations to risk. External vendors, including but not limited to Cloud Service Providers, are preferred targets for criminal actors conducting Cyber-Attacks. In addition, with the proliferation of non-personal identifiable information, including customer purchasing patterns, regulations mandate

that companies that transfer such data to another organization for profiling, who do not share any mutual operations on that data, can face hefty fines as well. Third Party Risk Management, therefore, must become an ongoing program for organizations that adopt Digital Twins. The fastest way to achieve this with utmost accuracy and security is to integrate Third Party Risk Management through Digital Twin implementation.

10.5. Threat Landscape

The need for organizations to engage with numerous digital partners is driving the emergence of Digital Ecosystems offering enormous commercial promise. However, along with such Mega-trends affecting the cybersecurity landscape, there's a parallel need for these partnerships working with a growing Digital Infrastructure of Cloud, Mobility, Big Data, and IoT, to factor in associated threats and vulnerabilities. Research's imminent doom threatens organizations of all sizes and types; some predictions put the estimated damages from cyber-crime at over USD 6 trillion. In this scenario, cybersecurity attacks and attempts are predicted to increase exponentially over the coming years alongside increasing levels of sophistication and bandwidth of cyber-adhere, with hundreds of billions of records predicted to be stolen over similar timeframes. Before organizations get mired in creeping paralysis from the Cybersecurity FUD Factor, it's appropriate to contextualize the nature of Cyber Threats in order to help shore up Digital Infrastructure used in Digital Ecosystems. To a certain extent, such threats are dependent upon the motivations of cyber-attackers ranging from quest for financial gain, pursuit of ideological agendas and inflicting reputational damage, nation-state sponsored cyber-warfare and cyber-espionage, to threats of cyber-terrorism with the agenda of creating panic or compromising critical infrastructure.

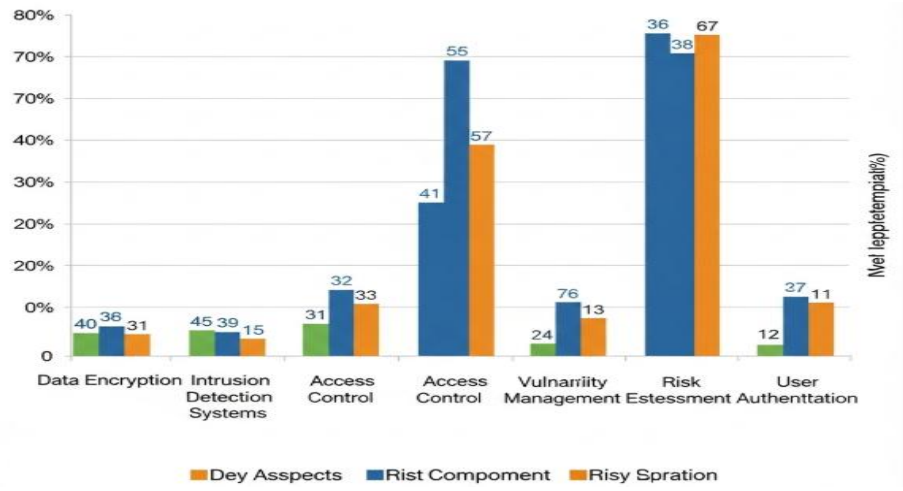

Fig 10.3: Cybersecurity and Data Privacy in Expanding Digital Infrastructure

Cyber-attacks differ not only in their motivations but also along a wider range of characteristics including the deployment of malware, attacks using social engineering to compromise systems, and breaches involving extortion like Ransomware. Apart from these cyber-defenses, advocates of Deception Technology point to the possibility of deploying decoys and lures during the design phase to draw in attackers and trick them into defeating bogus systems thereby offering organizations an opportunity to learn indicators of compromises and detect future attempts to exploit vulnerabilities.

10.5.1. Types of Cyber Threats

Threats exploit vulnerabilities in hardware and software, organizations, sectors, environments, and geographies for attacks that could have significant impacts. Major types include viruses, worms, Trojans, ransomware, denial-of-service attacks, phishing, and advanced persistent threats.

Viruses are programs that clandestinely attach themselves to other executable files and self-replicate. They can create unforeseen impacts on systems by corrupting data, reformatting the user's hard drive, shifting the system to run illegitimate scripts, or even erasing system files, and can travel stealthily between computers by replicating themselves. Worms are independent programs that replicate themselves across networks to fill up caches and network bandwidth. Frequently, they encrypt files on one's computer or network, rendering them inaccessible until demands for ransom are met. They can also execute denial-of-service attacks against a victim's public IP address. Often used in DoS attacks, detection and prevention of attacks resulting from worms are crucial to maintaining network performance.

Trojans are programs that mislead users about their true intent to gain unauthorized access to user systems. After installation, Trojans create a backdoor to allow attackers to exploit victims' systems remotely, allowing attackers to access users' data. Once installed, it may steal and send data, download other malicious programs, act as a keylogger, alter or stop firewall configurations, modify browser settings, and/or capture screenshots. A variant of Trojans, called rootkits, allow attackers to create a back door system to maintain unauthorized access and control over a victim's computer. They can gain administrator privileges by transcending the normal level of security. Although commonly used for spying, sampling user infrastructure data, and stealing sensitive information like login credentials and key certifications, rootkits can be deployed for more dangerous goals, like credential requests, machine reconfiguration, or system control. Using methods of stealthing, these programs can conceal their presence by destroying or replacing files related to detection and deletion.

10.5.2. Emerging Threats in Digital Ecosystems

Cyber-attacks have been evolving continuously. The rapid anniversary of new technology, services and capabilities in the connected world has expanded the attack surface – both in terms of numbers and types of assets connected, and in the diversification of threats. Adversaries are now more capable, better organized, and more creative. They are deploying the same technologies that are used to expand services to execute effective attacks at minimal cost. Many new technologies are being created that are at first too difficult for adversaries to exploit – it will be many years still before the AI-based attack tools can be created that can fully exploit the high-performance computing environments that talented individuals and organizations are developing. The next decade will almost certainly see attackers having more access to sophisticated tools that can exploit vulnerabilities at scale.

The proliferation of industries being transformed by services and connect, coupled with the vast populations of users connected with devices – both managed and unmanaged – is further complicating risk management. Attacks are occurring in all sectors across the economy at an accelerated rate – attacks not only on corporations, but state, local and tribal governments; nonprofit and charitable organizations; and other critical infrastructure component operators – with increasingly damaging impacts. Malware-based threats are a fact of life found in all areas of the economy, internationally. The motivations of the actors vary widely based on their goals, but the tools to implement many of their threats are largely the same, and reducing the burden of risk is a common goal at all levels of activity.

10.6. Risk Management Strategies

Organizations looking to implement digital infrastructure must carefully evaluate it across multiple criteria before making any investment or commitment. For new and existing assets, risk management strategies are often defined using qualitative tools, which involve tabulating factors such as likelihood and cost, risk matrices, or similar frameworks. Additionally, quantitative techniques are used to implement modeling and simulation approaches that yield optimal solutions. Networks that are redundant and standardized have been shown to have increased resiliency and lower LCC, and emerging strategies focus on collaborative, crowd-sourcing models that permit a progress report approach, such that risks can be dealt with as they arise.

Identifying Vulnerabilities

Common risk management practice is to define a list of asset classes and identify specific vulnerabilities by class; examples of physical vulnerabilities are available. IT assets can also be mapped to specific policies, and policy violations tracked over time to identify

policy areas that are producing the most violations. Finally, vulnerability scoring systems are available that assign a score for the vulnerability, allowing prioritization of vulnerability discovery to be based on the severity of the vulnerability. Policy-based networks are particularly well suited to dynamic prioritization of vulnerability discovery periods.

Containment and prevention strategies consider not just how to isolate an IT service to protect the organization from the breach, but also how to detect the breach at the earliest possible time in order to minimize damage and time of exposure. Detection capabilities can range from modeling tools that will detect anomalous operating conditions, to dedicated forensic software and expert systems that will identify the breach.

10.6.1. Identifying Vulnerabilities

Digital infrastructure is under continuous threat and cyberspace is fast on its way to becoming lawless to a degree, much like the seas some centuries ago. The rapid expansion of cloud computing, massive data infrastructure, connected devices, and devices that continuously monitor our lives and environment adds an additional challenge in ensuring robust cybersecurity. In the physical world, services on which people are reliant are backed by blocks and blocks of estate in a resilient construction. The management of cybersecurity risk in the digital world offers no such sense of physical bulk. A risk analysis and systematic identification of vulnerabilities is essential in developing appropriate cybersecurity strategies.

Risk management strategies provide a framework to create a more secure cyberspace, become resilient to any future intrusion, and swiftly recover from the impact of a successful intrusion. Risk analysis is a systematic examination of a cybersecurity posture. The risk assessment begins by understanding system-critical assets and building dependency networks around those assets; it then proceeds by connecting potential cybersecurity threats with vulnerabilities, and estimating and prioritizing the potential impacts/costs. Risk management is the set of activities and processes that prepares an organization to understand, predict, and prevent risks and, if any risk event is realized, be able to respond quickly, effectively, and adaptively with the least disruption. The cybersecurity risk assessment addresses the following questions: What is the risk to an organization? What are the vulnerabilities? What would cause the risk to happen? What would be the consequences if the risk occurred? What is the likelihood of occurrence due to the existing safeguards? What is the acceptable level of risk? Which safeguards are needed to reduce the overall risk to an acceptable level? What is the cost of each safeguard? What happens if a risk event does occur?

10.6.2. Mitigation Techniques

Multiple mitigation strategies can reduce the risk of exploitation by an external actor of the vulnerabilities discussed in this section. One classification of mitigation strategies identifies three distinct areas of risk management: prevention, detection, and recovery. Preventive controls focus on earlier phases in the attack lifecycle. Detecting controls can identify additional attempts at exploitation, while recovery helps restore the integrity or availability of the affected asset. The objective is to make sure that attacks do not happen by hardening the systems. In order for these commands to be verifiable, they need to be communicated down through the developer and operator chain to the actual language scripts that form the blocks of configuration code making up the system security structure. Mitigating controls could be employed by businesses to protect sensitive data from the risks discussed in favor of the potential benefits. The remainder and the greater part of this section is dedicated to protection advice for those organizations. Although much of this advice is primarily for Linux systems, it can also apply to Windows.

Perhaps the most obvious mitigating strategy is to simply not use bind9 and let the entire restrictive configuration right out of the box handle the user concern with the potential consequences of allowing this protocol and code package to be in production. This may be the best strategy indeed, because it would eliminate any question of some developer using v8 in a scripting environment. However, if organizations are indeed required to deploy a DNS server to provide both internal and external services, then any messages not crucial to running the DNS management infrastructure should be blocked down at the router level on either side of the network according to which root zone is running on outward-facing devices. These devices should also be patched up with the most current version of bind9 available.

10.7. Conclusion

In this article, we cover some fundamental building blocks relevant to securing the ongoing expansion of digital infrastructure and cyberspace ecosystems. The work is focused on applied, pragmatic areas that require wide industry, institutional, and workforce engagement. Working with and deploying cybersecurity and data privacy to the core of the digital infrastructure can help pursue urgent cybersecurity objectives, including restoring the cybersecurity oversight and maintainability that is currently lacking amid the rapid expansion of a very complex cybersecurity and data privacy risk landscape. Significant cybersecurity risks are emerging, not only from continuing traditional digital attacks, but rather from the expansion of the scope and increasing severity of such attacks, in addition to the take-up of more sophisticated and widespread forms of cybercrime and cyberterrorism. These forces can only be met with extraordinary cybersecurity measures. These have long been optimal in the digital

architecture of critical infrastructure owners and service providers. These wide-alonglined risks mean that critical data used in everyday life will be created and consumed, exchanged, processed, stored, analyzed, and erased in far larger volumes, and in far greater situations of cyberspace risk, than ever before. Cybersecurity cyber-physical and cyberspace controls must recognize this reality and balance cybersecurity effectiveness, including reflected in the infrastructure ecosystem interdependencies, resilience in times of incident, and cybersecurity operational burdens.

In the future, it is likely that more enterprises, agencies, and institutions will absorb extended digital infrastructure principles into their cybersecurity and privacy frameworks. They can feasibly do so since the key above principles have been around for over a decade. We will also begin to see mass effects of more enterprise and institutional focus on digital landscape infrastructures that can underpin and secure individual applications in important real-world domains, such as digital trust, digital escrow, digital exchanges, digital security and emergency response.

10.7.1. Future Trends

The meta-trend, Emerging Digital-AI Enabling Ecosystems, is trending rapidly towards pervasive and ubiquitous operation - via such technologies and technology stacks as IoT-Edge-AI for digital infrastructure environments and their infrastructures, within a NaaS-PaaS-XaaS and marketplace-centric Digital-AI Economy, assisted/augmented by the rapid tech trajectory(s) of Generative AI with LLMs and intelligent agents. Yet at the same time, it also represents increasing risk of bad actors mining these very Digital-AI Enabling Ecosystems for threats to Cybersecurity, Data Privacy, Personal Sovereignty, Agency and Tranquility. The increasing coalescence of both these factors - the rapid and ever-expanding facilitation and enablement of Digital -AI Economies via Digital-AI Virtual-Tech Enabling Ecosystems, and the concurrent increasingly expanding area of exposure, risk and vulnerability for The World Within The World - our Digital Lives - is leading towards much more radical innovations and evolutions of Digital Infrastructure, Infrastructure Environments, Intelligent Infrastructure and Intelligent Infrastructure Services. Not just innovations in technology for changing the current landscape of infrastructure - but radical changes to the very fabric of the infrastructure service delivery stack.

The focus here, primarily, has been on Distributed Data-Centric Infrastructure Environments and intelligent services, that are the Digital Infrastructure Enabling foundation of Digital-AI Economy, and Digital Infrastructure-Aware Global Digital Society, based upon the uplift-Catalyst enablers of Metalayer, User Intimacy, Data Economy, Data Sovereignty and Data Tranquility. The service underlays that facilitate and enable new Digital-AI Economy models and Global Online User-Centric Digital

Societal interactions, while addressing the unique Data-Centric security, privacy, sovereignty and tranquility requirements of both Online Users and the Economy At Large. While writing these explorations ideas in bits and bytes, I once more got reminded and reinspired about the many opportunities that lie ahead of us in these transformational areas.

References

Zaharia, M., Chowdhury, M., Das, T., Dave, A., Ma, J., McCauley, M., ... & Stoica, I. (2016). Resilient distributed datasets: A fault-tolerant abstraction for in-memory cluster computing. Communications of the ACM, 59(11), 56–65.

Chen, M., Mao, S., & Liu, Y. (2019). Big data: A survey. Mobile Networks and Applications, 19, 171–209.

Mehmood, R., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., & Guizani, M. (2017). Internet-of-Things-based smart cities: Recent advances and challenges. IEEE Communications Magazine, 55(9), 16–24.

Katal, A., Wazid, M., & Goudar, R. H. (2013). Big data: Issues, challenges, tools and good practices. In 2013 Sixth International Conference on Contemporary Computing (pp. 404–409). IEEE.

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. Information Systems, 47, 98–115.