Chapter 48
Cyber Resilience for the Internet of Things

Marcus Tanque
Independent Researcher, USA

Harry J. Foxwell
George Mason University, USA

ABSTRACT

This chapter examines and explains cyber resilience, internet of things, software-defined networking, fog computing, cloud computing, and related areas. Organizations develop these technologies in tandem with cyber resilience best practices, such as processes and standards. Cyber resilience is at the intersection of cyber security and business resilience. Its core capabilities encompass integrated strategic policies, processes, architectures, and frameworks. Governments and industries often align defensive and resilient capabilities, to address security and network vulnerability breaches through strategic management processes.

INTRODUCTION

Cyber resilience architectures and frameworks involve security models, procedures and practices. Industry develops solutions architecture and methods with greater capabilities to measure, evaluate, withstand, resist, mitigate, monitor, recover and protect critical infrastructure systems from cyber-attacks. These perspectives comprise (operational security, defensive and reactive functions) focused on deterring cyber-attacks or disruptive events (NIST, 2014). Besides this chapter lays emphasis on cyber resilience, the future direction of cyber resilience capabilities and Internet of Things (IoT) solutions. Additionally, the authors analyze how global organizations may benefit and learn from past and recent technology problems, to enhance the advance of IoT infrastructure data-sharing and provisioning (EU, 2011). This study also emphasizes technological solutions, progressions and capabilities; specifically, speed, volume, security and user's privacy for sustaining consumers and organizations' commonplace requirements (Cyber Resilience, 2016).

DOI: 10.4018/978-1-5225-8897-9.ch048

On global organizations' critical infrastructures cyber-attackers have steadily increased over the course of years (Cyber Resilience, 2016). As such, governments and high-tech companies continue to develop cyber resilience solutions, policies, methods, trials and standards, to satisfy business and management practices (EU, 2011). Human occurrences and natural tragedies generally originate deliberate cyber-attacks—this includes both intended/inadvertent events. Every perspective being presented in this article further exemplifies authors' useful, sound and real-world expertise. Similarly, the authors put emphasis on specific areas involving cyber resilience and IoT capabilities. To further explain, the background section delivers decades of empirical technology knowledge base. This includes domains supplementing cyber resilience capabilities, and how bad actors 'adversaries' may maximize every opportunity presented to indiscriminately launch cyber-attacks against planned or target of opportunities within the infrastructure. The contextual section also evaluates events, methods and concerts for progressing an organization's all-inclusive business objectives.

BACKGROUND

In the present decade, cyber resilience solutions have played a vital role in protecting organization's infrastructures. This includes spanning organization's ability to in tandem deliver predictable results aimed at decreasing adversative, circumstantial and consequential cyber activities—merging policy and security capabilities, such as information security, business continuity operations and structural resilience. Thus, the advent of cyber resilience capabilities has evolved extending from significant technology and security elements, to contemporary business processes. Such cyber activities can be viewed as security components that span availability, integrity and confidentiality (AIC).

Today AIC triad serves as an epitome for supporting an organization's organizational policies. Similarly, these security elements continue to play a considerable role in the global enterprise's environment. These processes are designed to support IT systems, data and services as well as ensuring IoT systems are capable of withstanding active or future threats. The next section discusses the evolution, impact and future trends affecting cyber resilience, IoT systems and relatively other infrastructure areas.

EVOLUTION, IMPACT AND FUTURE TRENDS

For many years, organizations have advanced from implementing cyber resilience capabilities. For instance, opponents could take advantage of avantgarde and custom-tailored solutions, to launch cyber-attacks, which may often be successful (McCarthy, Collard, & Johnson, 2017). The advent of modern-day distributed computing solutions comprises (Cyber Resilience, 2016): mobile access, cloud computing and IoT systems (EY, 2015). Often cyber-attacks are deliberate or planned—strategic cyber-attacks typically occur when security analysts or specialists, fail to update software or conduct network vulnerability scanning on system(s). The authors describe cybersecurity a method comprising procedures, measures and technologies. These services are developed to provide continuing protection of organization's security capabilities. Similarly, these methods stem from protecting businesses' IoT infrastructure resources; core systems, networks and technologies. Yet, cyber resilience covers (policy, processes, procedures and infrastructure). These mechanisms include cyber security and business resilience among others (McCarthy et al, 2017).