JASON R.C. NURSE

CYBER RESILIENCE: WHAT IS IT AND HOW DO WE GET IT?

In today's world, cyber-attacks seem as routine as the common cold. In the security industry, many live by mantras such as, 'it is not a question of if you will be hacked, it is a question of when' and 'assume that you have already been breached.' With these words in mind, the key considerations therefore are: how should organisations respond and what factors are essential to be resilient in the face of a constantly evolving threat landscape.

Our world is driven by technology. It supports personal and organisational interaction and is a core source of innovation, enterprise and defence. The benefits of technology are, however, not without their concerns. One of the largest of these is the prevalence of cyber-attacks and the reality that as digital technologies and cyber-physical systems become more ubiquitous, such attacks can have a much wider reach.

A cyber-attack on an organisation might not only cause a few systems to be offline, it can impact the surrounding supply chain, a government's infrastructure or even lead to a loss of life. As a result of these issues, there has been a significant push for cyber security research and practice to aid in combating the threat. Primarily, this has focused on protective, detective and reactive security measures. If we ascribe to the mantras above, which are held by many security professionals in the field, then reactive security controls and cyber resilience more broadly, is critical to the continuity of an organisation.

CYBER RESILIENCE: WHAT IS IT?

Resilience is the capability to quickly react and recover from challenges or difficulties. Cyber resilience extends the notion of resilience to cyber-related incidents (deliberate attacks or accidental mishaps). It seeks to explore and define ways through which organisations can create systems, business processes and services that are able to rapidly 'bounce back' after a cyber-attack.

This can be taken one step further to regard true cyber resilience as bouncing back to a stronger position than the organisation was in prior to the attack. The idea in this case is that a resilient enterprise would thoroughly investigate the incident and learn from it, and therefore that incident and others like it, would not be successful in the future.

While cyber resilience has been discussed for some time, particularly in the military and Critical National Infrastructure (CNI) domains, there is still not a clear consensus on exactly how to achieve it. What is agreed however, is that there are several key principles which should be adopted and customised to each enterprise's security context. These are Prepare, Absorb, Recover and Adapt.

Preparation is crucial and relates to developing preventative measures and defining an appropriate response plan for a range of potential cyber incidents. In cases where prevention fails, an organisation should seek to *absorb* the attack through layered security approaches which draw on technical, procedural and human elements. Incident *recovery* is responsible for ensuring business and mission continuity during and after an attack. This is the area often most linked to resilience itself, but it is actually only a part of the resilience puzzle. Finally, technology and cyber-attacks change and evolve, so in order for organisations to be cyber resilient they must *adapt* constantly. This will be necessary with consideration of the systems used, the security postures assumed, and in the trial and adoption of new types of security technology (e.g., artificial intelligence in cyber security).

BETTER CYBER RESILIENCE THROUGH AN ENHANCED UNDERSTANDING OF CYBER-HARMS

One current area of research which has a great deal to offer the topic of cyber resilience is that of organisational 'cyber-harms'. The term cyber-harm describes the damage occurring as a result of an attack perpetrated wholly or partially through digital infrastructures, and the data, information, applications and devices that these infrastructures are composed of.

While the notion behind cyber-harm is not new, what is novel is the conceptualisation by new research of the variety of harm types that can arise from a cyber-attack. These have been characterised by way of a taxonomy of cyber-harms, with the five main categories as follows: Physical or Digital harm (e.g., exposure of confidential data), Economic harm (e.g., disrupted missions or operations), Psychological harm (e.g., confusion or anxiety faced by customers or employees), Reputational harm (e.g., damaged defence or enterprise brand) and Social and Societal harm (e.g., negative impact on the nation).

The enhanced understanding of harms that may result from cyber-incidents is extremely valuable because it forces organisations to broaden their thinking on what they need to protect against, and thus better appreciate the comprehensive nature of cyber resilience. Currently, when most organisations reflect on cyber risk and its management, the focus is on direct harms to themselves (e.g., disruption of services) or their customers and suppliers (e.g., loss of confidential or private data). However, the connectivity of modern-day systems means such a limited view is no longer sufficient, given that the harm emerging from cyber-attacks can easily propagate and aggregate.

One interesting case example is the malware and denial-of-service attack on a Ukraine powerplant in December 2015. This was one of the first incidents that demonstrated the importance of incident recovery and resilience in the cyber-physical systems CNI domain. Through a series of carefully crafted attacks, hackers were able to seize direct control of power systems from official operators, and eventually cut power to an estimated 225,000 people in one of the coldest months of the year.

While all of the details of this case have not been revealed, there are undoubtedly questions around the plant's prevention and response defences, as well as whether there was a full consideration of the harms to consumers without power at such a time. A Prepare-Absorb-Recover-Adapt approach that incorporates, and thus reasons about, the full complement of cyber-harms could have helped planning for this case. In particular, it would have supported an adequate scoping of how a malware attack could impact internal and external operations, and how such a vast number of cyber-harms could propagate and mount over short periods of time. Here, harms can be witnessed in not only the internal environment, but psychologically (in terms of individuals who faced hardship) and societal (lack of trust in connected CNI systems). This and similar analyses can be applied across a wide range of current and future cyber-attack cases.

As we look towards creating organisations, infrastructure and systems that can effectively withstand cyber-attacks, cyber resilience will become an even more significant consideration. Any factors that can further inform and enhance the resilience process will provide organisations with a greater advantage in preparing for attacks and recovering quickly when they arise. We believe that cyber-harm is one of such factors and that its integration can provide the pathway for a more holistic form of cyber resilience, where organisations are well-prepared for responding to all types of attacks and harms.

Dr Jason R.C. Nurse is a Lecturer (Assistant Professor) in Cyber Security at the University of Kent and a Visiting Academic at the University of Oxford. His research focuses on organisational cyber security, insider threat, and human aspects of security and trust.