CYBERSECURITY
A Board Dilemma

TOBBY
SIMON

Hidden within the dark underbelly of the legendary Trojan Horse, Odysseus and his Greek warriors proved to be the undoing of Troy. Will the World Wide Web and its anonymous residents prove to be the Achilles heel of cyberspace?

The proliferation of global supply chains, increased financial assimilation, expeditious urbanisation, the 'Internet of Things' and its ubiquity have all accelerated worldwide economic growth over the past few decades. Unfortunately, the same developments have also significantly increased our vulnerability to external shocks and global crises. In most developed countries, the digital economy has become the real economy. The Internet and Internet communication technologies (ICT) permeate societies and economies at global and local levels, blurring the line between what is an online activity and what is not. In this context, the issue is no longer about anticipating and preparing for the digitisation of society: it is all about how to harness the benefits of digital economy and generate trust across all sectors.

Hence, in a hyperconnected world, enterprises everywhere from small businesses to the largest, are vulnerable to cyberattacks. Criminals deliver spam, cast phishing attacks, facilitate click-fraud and launch distributed denial of service (DDoS) attacks with high precision. A thriving underground economy fuels the growth of innovative malware and incentivises cyberattacks. The hyper connectivity and the relative anonymity provided by web browsers lowers the risk of detection, and makes cyber espionage activities straightforward and economically attractive to conduct.

Hyperconnectivity is a state of unified communication (UC) in which the traffic-handling capacity and bandwidth of a network always exceeds the demand. The number of communication pathways and nodes is much greater than the number of subscribers. Anonymous web browsing refers to the utilisation of the World Wide Web that hides a user's personally identifiable information from websites visited. Librarians in Massachusetts were reportedly installing Tor software in all their public PCs to anonymise the browsing habits of their patrons. Tor is a computer network run by volunteers worldwide. Before hitting the open Internet, the Tor Browser will connect to several different relays, wiping its tracks each step of the way, making it difficult to figure out where and who you really are. Former Director of Government Communications Headquarters (GCHQ) UK, David Omand states:

> I do not need to remind this audience that as a society we have sold our souls to the Internet. We wanted to exploit its advantages quickly and did; now we are dependent on it; and we have fresh evidence every day of the reckoning to come even as we try to retrofit adequate security.[1]

THE ASYMMETRY

Cyberattacks are asymmetric, continually evolving and becoming more sophisticated, making it difficult for enterprises to stay ahead of the threat. In a battle scenario, the creation and 'massing' of forces is often possible to observe. Such a manoeuvre, involving state-of-the-art weaponry, also needs a high level of expertise that comes from years of education and training. We can trace the kinetic material fairly accurately to its source; and the effects of a kinetic attack unfold over an observable period of time. Defence is possible as long as we are sufficiently diligent and prepared with a response.

The cyber battlefield is quite different because it does not need a factory, a military base or physical material. It does not require the same sort of education, training and experience. All that is required is a computer, an Internet connection, and the time and patience to learn about software, hardware and network vulnerabilities.

Kane Gamble, British teenager and founder of Crackas with Attitude, was 15 years old when he accessed the e-mail accounts of top US intelligence officials, including the head of the

Central Intelligence Agency (CIA), John Brennan. Cyber threats are disproportionate in that the build-up to a confrontation may be undetectable, taking place at lightning speed, and having once occurred, very hard to attribute.

QUANTUM COMPUTING AND ENCRYPTION

In 1980, Paul Benihoff, a scientist from the United States, first proposed a computer based on the principles of quantum mechanics. His idea of this quantum computer was based on Alan Turing's famous theory of computation. In the following years, Nobel prize-winning physicists Richard Feynman and David Deutsch shared insights on how a quantum computer could simulate and reproduce any reliable physical system much faster, and with finite means. In 1994, Peter Shor, a mathematician at Bell Labs, proposed a method for factorising large integers. He used the quantum principles of super position to search for périodicité, which would enable him to perform computations in a few minutes, which would on a classical computer take longer than the age of the Universe.

Quantum computing is a game-changing technology for cybersecurity because of its inherent speed boost that can be used to solve complex mathematical problems. Digital computers run on data that is encoded to the binary system, where the state of any single bit can only be 0 or 1. Quantum goes beyond binary by virtue of a qubit's ability to reside in more than one of two positions. A qubit can represent simultaneously a quantum state made up of two or more values called a superposition. In simple terms, a qubit's superposition provides more computing power in the same space.

Michele Mosca, deputy director of the Institute for Quantum Computing at the University of Waterloo, Ontario, has estimated that there is a one-in-seven chance that some fundamental public-key crypto will be broken by quantum by 2026, and a one-in-two chance of the same by 2031. Thus, any nation that is able to position itself as a pioneer in quantum computing will be in an advantageous position to access information from across the world while safeguarding its own data.

This opens up the possibility of malicious actors taking advantage of the system, and the various vulnerabilities. Imagine a system that can break through any encryption. The question

then arises as to why traditional computers are more vulnerable. Quantum computers can conduct complex processes and calculations at extraordinary speeds that are beyond the grasp of an advanced supercomputer. While we can use the power of quantum computing to build more complex protection layers, we cannot preclude the fact that it could also harm hackers. In the majority of attacks, the adversary targets the user and social engineering plays a large part, if not larger, than the technical expertise. As long as humans can be persuaded to part with a secret in appropriate circumstances, all cryptography in the world is vulnerable.

THE THREAT

Contrary to what is generally perceived, cyber threats today go well beyond network security. Network security is essentially the process of taking physical and software preventive measures to protect the underlying network infrastructure from unauthorised access, misuse, malfunction, modification or improper disclosure, thereby creating a secure platform for computers, users and programmes to perform their permitted critical functions within a *secure environment*.

From here on, hackers will launch increasingly focused attacks on everything from critical infrastructure to medical devices. The spiralling number of connected devices, or the Internet of Things, presents a unique opportunity for hackers to increase their surface area of attack. Going forward, smartphones present the biggest risk category because of the sheer number in use and multiple vectors of attack, including malicious apps and web browsing. Headless worms, machine-to-machine attacks, jail breaking, ghost ware and two-faced malware would constitute some of the biggest cybersecurity threats. We shall soon see 'headless worms'—malicious code targeting 'headless devices', such as smartwatches, smartphones and medical hardware. The growing reliance on virtualisation and both private and hybrid Clouds will make attacks on Cloud and Cloud infrastructure more fruitful for cybercriminals. Mobile devices running on compromised apps will provide a way for hackers to remotely attack private and public Clouds, and access corporate networks. Ghost ware are those malware designed to penetrate networks, steal information and then cover up tracks, making it extremely difficult for companies

to track exactly how much data has been compromised, and hinders the ability of law enforcement to prosecute criminals.

For key stakeholders in the cybersecurity narrative it then becomes absolutely essential to determine the security of the *entire ecosystem*. The results of a two-year research project conducted by Synergia Foundation, a Bangalore-based strategic do-tank, showed that the maximum surface area for networks in the cyber security narrative is at best 16 to 18 per cent. This means that even if a company is able to theoretically secure its networks 100 per cent, it may still be hugely vulnerable by more than 80 per cent.

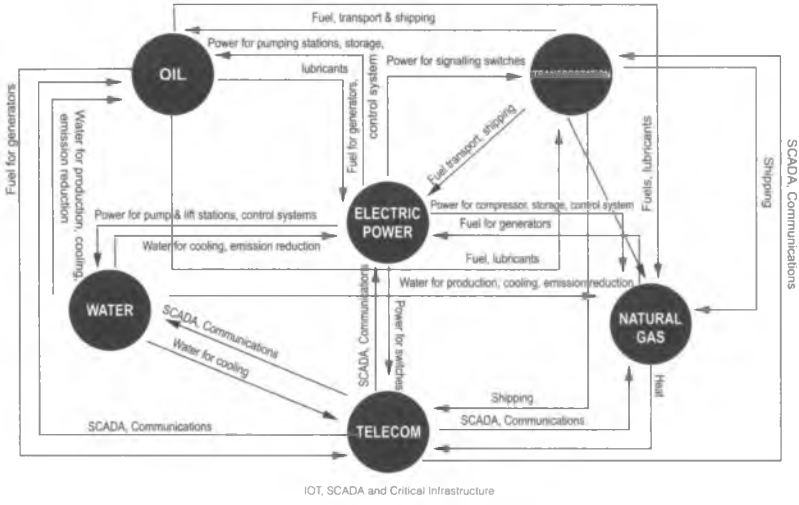
Cyber threats encompass a number of external factors beyond the ambit of networks, including External and Internal Intelligence, Web Intelligence (WEBINT), Human Intelligence (HUMINT), Open Source Intelligence (OSINT), Signal Intelligence (SIGINT), Supply Chain Security and Social Media. The key to an effective deterrence strategy is for an enterprise to get tactical intelligence about possible adversaries and then to develop proactive counter strategies.

It is estimated that more than 60 per cent of threats faced by organisations emanate within the organisation. Information Technology (IT) managers in most instances are adept in understanding technology issues, but may not be equipped to remedy such threats which need interdisciplinary skills, including elements of physical security. This lack of knowledge might inadvertently put an organisation at a strategic disadvantage. A company's top-level management team, including its board, must therefore be equipped with insights, and intelligence and intervention tools to handle such asymmetric threats.

THE CHALLENGE

CRITICAL INFRASTRUCTURE

Industries have now replaced older equipment with hardware and software that are less expensive, much quicker and can seamlessly communicate with the Internet. At the heart of any critical infrastructure is an Industrial Control System (ICS), which includes Supervisory Control and Data Acquisition (SCADA) systems, and Distributed Control Systems (DCS) that monitor processes and control the flow of information. The ICS is a major segment within the operational technology sector. These could be mine-site-conveyor belts, oil-refinery cracking towers, power consumption



Synergia Foundation

on electricity grids, or signals that emanate from information systems. While the widespread use of Cloud computing and the adoption of Internet-of-Things technology has significantly reduced costs, it has also increased cyber vulnerabilities in the ICS.

Critical infrastructure facilities (electricity, oil, gas, water, waste, etc.) rely heavily on electrical, mechanical, hydraulic and other types of equipment. The equipment is further controlled and monitored by systems known as controllers and sensors. These systems are connected to management systems, together forming networks that leverage SCADA and ICS solutions. Both ICS and SCADA enable efficient collection and analyses of data and help automate control of equipment, such as pumps, valves and relays. While their implementation is proprietary, SCADA controllers are essentially small computers. They use standard computer elements, such as operating systems (often embedded Windows, Unix), software applications, accounts and logins, communication protocols, etc. Consequentially, the challenges associated with vulnerabilities and exploits extend to ICS and SCADA systems, with the additional challenge of such systems operating in environments that can be physically difficult to reach or, in many cases, can never be brought offline.

WannaCry Ransomware was a cyberattack outbreak that targeted machines running the Microsoft Windows operating system.

We all know that it affected companies and individuals in more than 150 countries, including government agencies and multiple large organisations globally.

An examination of the vectors shows: First, the attack on the British National Health Care System (NHS); then on Spain's largest telecommunication company, Telefonica; French car manufacturer, Renault; Russian cell phone operator, MegaFon; US-based Fed Ex; the Ukrainian state power company and Kiev airport; the Chernobyl nuclear power plant; the Ukrainian central bank; the Ukrainian aircraft manufacturer, Antonov; one of the largest shipping companies in the world, Maersk; and, TNT, one of the largest packet forwarders in the world. The attack also extended to Russia's biggest oil producer, Rosneft; and Saint-Gobain, a construction company in France, among others.

The narrative and messaging is quite evident: In a hyper-connected world, an adversary can disrupt an industry or critical infrastructure anywhere around the globe.

SUPPLY CHAIN SECURITY

Global supply chains rely on the rapid and robust dissemination of data among supply chain partners. As a result, security breaches often occur when a criminal compromises a third-party vendor's credentials, which typically include logins, passwords, badges and security access.

The biggest retail attack in the history of the United States was not particularly inventive, nor did it appear destined for success. In the days prior to the attack, hackers installed a malware in Target's security and payment system, designed to steal every credit card used at the company's 1,797 stores across the United States. At the critical moment—when Christmas gifts were being scanned and bagged, and the cashier asked for a swipe—the malware would step in, capture the shopper's credit card number and store it on a Target server commandeered by the hackers. Later, after the hackers had set their traps, they had just one thing to do before starting the attack: plan their escape route. They uploaded exfiltration malware to move stolen credit card numbers first to staging points spread around the United States to cover their tracks, and then to their computers in Russia. The hackers are believed to have used the credentials of a third-party vendor

to infiltrate Target's network, spending weeks on reconnaissance to install a pair of malware programmes. When asked to respond to a list of specific questions about the incident and the company's lack of an immediate response, Target Chairman, President and Chief Executive Officer Gregg Steinhafel issued an e-mail statement that 'Target was certified as meeting the standards for the payment card industry in September 2013'.

Vulnerabilities in the extended supply chain are an existential threat to enterprises. Organisations are outsourcing rapidly to focus on core competencies, to seek out technical innovation and lower cost resources. While the parent company might be resistant to supply chain vulnerability, questions arise as to the security of its subsidiary or partner companies located around the globe.

BANKS AND FINANCIAL INSTITUTIONS

A cyberattack on Bangladesh Bank, the central bank of Bangladesh, resulted in losses of $81 million and prevented another $850 million in transactions from being processed. The adversaries deployed highly sophisticated attack vectors, involving an aggregation of technical skills, and a deep understanding of how Bangladesh Bank communicated with the Society for Worldwide Interbank Financial Telecommunications (SWIFT).

SWIFT is a consortium that operates a trusted and closed computer network for communication between member banks around the world. Hackers used the SWIFT credentials of Bangladesh Bank employees to request the Federal Reserve Bank of New York to transfer nearly $1billion of Bangladesh Bank's funds to accounts in the Philippines, Sri Lanka and other parts of Asia. By targeting the SWIFT network, the hackers undermined a system that was thus far considered flawless.

The biggest emerging threat to financial institutions are the bot attacks whose frequency has increased multiple times in recent times. A worst-case attack scenario could paralyse a bank for days, leading to millions, if not billions, of dollars in lost business. A bot is a programme that functions as a proxy for a user or another programme, or replicates a human activity. On the Internet, the most ubiquitous bots are programmes called 'spiders' or 'crawlers' that access websites and gather their content for search engine indexes.

CONCLUSION

The stakes involved in cyber threats to businesses and governments are growing exponentially, and the ability to compromise information systems is well understood. However, an emerging threat is one that can cause physical harm to systems and persons. This threat has become existential for certain sectors, such as critical infrastructure. The threat was visible in August 2018, when cyber-criminals breached the security of a petrochemical plant in Saudi Arabia with the intent to sabotage. The investigators concluded that the hackers custom-built nearly all their tools, and could do so as they were able to obtain a copy of the critical software from eBay. Cyber threats can cause extensive damage to the legacy of businesses and governments that CEOs and board members of both public utility companies and business enterprises can no longer afford to disregard.

◆

NOTE

1. From an article written by Sir David Omand sent to the author.

◆◆