Feature

Developing a Common Understanding of Cybersecurity

Deepak Rout, CISM, CRISC, CISSP, has more than 20 years of professional experience in technology management and leadership roles. He is currently the leader of the IT consulting practice for the global management consulting firm Protiviti and is focused on providing customised solutions and services to clients to meet their business challenges in the cybersecurity, IT risk, governance and compliance domains. Prior to pursuing a consulting career, Rout spent most of his career as a practitioner in several industry sectors in the areas of technology strategy, business process management, risk management, information security architecture and operations, governance and compliance, strategic cost reduction, and talent transformation.

Cybersecurity is frequently discussed, but the meaning and scope of the term have not been consistent. There is even disagreement on how the term is spelt. It is referred to as 'cyber security' and 'cybersecurity'.

Semantics often get in the way of common understanding. The impact of semantic confusion can be extreme when the subject under consideration is critical to business.

Whatever the spelling and meaning, there is concurrence that cybersecurity matters pose significant risk to governments, industry sectors and the general public. An entire industry exists to meet the perceived need around managing related risk, and it is valued at more than US $160 billion.[1] There is also a consensus that cybersecurity is closely related to the domain of information security.[2] Therefore, professionals working in information security and related domains would benefit from an understanding of the meaning and scope of cybersecurity.

ORIGINS OF CYBER

The word 'cyber' has Greek roots roughly meaning one who guides a boat, such as a pilot or rudder operator. Plato adapted this word to mean something along the lines of governance and associated it with government control, as governments steer society. In the 20th century, American mathematician and philosopher Norbert Wiener foresaw the rise of sophisticated robots, which would need artificial intelligence to control their actions. Wiener coined the word 'cybernetics', borrowing from Greek roots to refer to intelligent controllers, and he indicated that they would be difficult to design and build. Weiner retained the connection between technological control and governance. Speculative fiction novelist William Gibson foresaw the space of virtual interactions in his 1984 novel *Neuromancer* and coined this 'cyberspace', borrowing the prefix 'cyber' from Wiener. Many adopters of the early Internet were fans of Gibson's work, so cyberspace became a standard name for the place users went when on the Internet. Gibson's usage, however, eliminated the context of governance in the word cyber, as the Internet is inherently not amenable to central control systems.

Meanwhile, security experts had already settled on the term 'information security' to mean securing of information and digital systems, and it was considered synonymous with 'computer security' and 'network security'. The British Standards Institute (BSI) published the first set of standards around information security, namely BS 7799, in 1995.[3] These standards were later incorporated into the global standards from the International Organization for Standardization (ISO), namely ISO 27000. The current standards of information security are ISO/IEC 27001-2, updated in 2013.[4]

It is interesting that cybersecurity gained attention when the useful term information security already existed for the same thing. There is no clear research establishing why this is so, but it is attributable to a combination of military influence, marketing hype and societal acceptance. As digital technology became vital for business and governments, the military started preparing to defend national interests around this area. Because conventional military thinking is based on the defense and attack of some kind of space (e.g., terrain, aerospace), cyberspace became a useful reference to the digital domain. Hence, securing cyberspace became cybersecurity. In addition to many defense measures, cybersecurity also came with some offence measures as well.

The term cyber has found easy acceptance with the media and, through them, with society in general. While information security sounded formal and demanded a deeper understanding of technology aspects, cybersecurity connected well with science fiction and popular imagination, as it struck a chord with business leaders and industry experts in increasingly digital global commerce. It is no surprise then that the accepted semantics

were quick to overflow into other areas (e.g., cybercriminals, cyberattacks, cyberwar, cyberdefence, cyberdiplomacy).

Interestingly, with leading global governments increasing their cybersecurity capabilities designed to exert control and exercise governance on cyberspace, cybersecurity has come full circle with regard to the meaning of cyber, implying Wiener's vision of technocratic control and Plato's vision of government control.

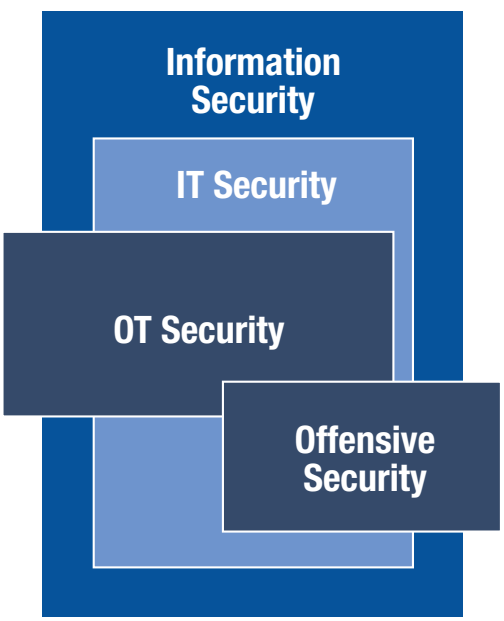
SEARCHING FOR A RELIABLE DEFINITION OF CYBERSECURITY

Having understood the origin of the term, it is essential to get an understanding of the term itself. There are quite a few close variations in the meaning and scope of cybersecurity, and there are some outliers:

- **Dictionary definition:** 'Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack'.[5]
- **General understanding in computer security communities:** Security aspects have always lagged behind functionality in the world of computing. This has been an oft-repeated sequence at all stages of the IT revolution, be it mainframes, personal computers (PCs), Internet, cloud, mobile, social media or cyber. However, the lag time between security and functionality has been narrowing with each stage of technology advancement. Computer security, or IT security, has come to be known as a discipline applied to computing devices such as computers and smart phones, as well as computer networks such as private and public networks, in addition to the Internet.It includes 'all processes and tools by which digital equipment, the information they contain and services provided using them are protected from unintended or unauthorized access, change or destruction'.[6] Computer security has grown in importance due to the increasing reliance on computer systems in most societies. It includes physical security to prevent the theft of equipment and information security to protect the data on that equipment. In recent times, cybersecurity has been synonymously referred to as computer security.
- **Views from technology media:** Several leading technology publishers have tried to define cybersecurity:
  - Tech Target defines it as, 'The body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cybersecurity'.[7]
  - Techopedia defines it as, 'Preventative methods to protect information from being stolen, compromised or attacked in some other way. It requires an understanding of potential information threats, such as viruses and other malicious code'.[8]
- **Definition by industry sectors:** The International Telecommunication Union (ITU) defines cybersecurity as 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets'.[9] Organisation and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of organisation and user assets against relevant security risk factors in the cyberenvironment.
- **Definition by the US government:** The US National Institute of Standards and Technology (NIST) defines cyberspace as a global domain within the information environment consisting of the interdependent network of information systems infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. 'Cyberattack' is defined as an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, maliciously controlling a computing environment/infrastructure, or destroying the integrity of the data, or stealing controlled information. Consequently, cybersecurity is defined as 'the ability to protect or defend the use of cyberspace from cyber attacks'.[10]

- **Definition by research firms:** In June 2013, Gartner acknowledged that there is confusion in the market over how the term should be used and published a research paper to help define cybersecurity. The paper said the 'use of the term 'Cybersecurity' as a synonym for information security or IT security confuses customers and security practitioners, and obscures critical differences between these disciplines'.[11] To help set the record straight, the paper defined the term: 'Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries'.[12] The paper further clarified that 'Cybersecurity is a superset of the practices embodied in IT security, information security, operational technology (OT) security and offensive security'.[13] The paper also provided a graphic to illustrate this (**figure 1**).

Figure 1—Components of Cybersecurity



Source: Gartner, June 2013. Reprinted with permission.

Gartner advises that 'Security leaders should use the term "Cybersecurity" to designate only security practices related to the combination of offensive and defensive actions involving or relying upon information technology and/or operational technology environments and systems.'

The Gartner definition encompasses all of the definitions suggested by industry bodies, professional organisations and government agencies. It also clearly outlines the components of cybersecurity and sets them in context with an illustration. However, it underlines an offensive element that may not apply to entities other than government organisations with specific authorised mandates. Moreover, engaging in such measures would amount to infringement on laws in most parts of the democratic world. For the purposes of understanding and implementing cybersecurity measures at an enterprise or entity level, the Gartner model is suitable; however, nongovernmental organisations should apply it without the offensive security measures. This does not alter the definition of cybersecurity as such; rather, it limits the applicability or scope of cybersecurity for enterprises.

IS IT CYBERSECURITY OR CYBER SECURITY?

In addition to the multiple definitions of cybersecurity, there are also different ways of spelling the term itself—'cybersecurity' and 'cyber security'.[14] These terms are getting more and more mixed usage lately. There is no recognised authority on the subject *per se*, but guidance can be taken from the Associated Press, the dominant resource when it comes to news copy style, which says it is one word: 'Cyberspace is a term popularized by William Gibson in the novel *Neuromancer* to refer to the digital world of computer networks. It has spawned numerous words with cyber- prefixes,
but try to avoid most of these coinages. When the combining form is used, follow the general rule for prefixes and do not use a hyphen: cyberattack, cyberbullying, cybercafe, cybersecurity. There are some exceptions to the prefix rule, specifically around proper nouns, such as US Cyber Command'.[15] In addition to the Associated Press, most of the sources quoted in the previous definition section use the single-word form.

AN ENTERPRISE-CENTRIC APPROACH TO CYBERSECURITY

There are a few people in the research community who have held out against painting everything cyber, although their ranks are thinning due to the growing global acceptance of the term from governments, industries and the general public. Gartner analysts suggest that many of the activities labelled

cybersecurity are not only not new, but could also be dangerous practices that should not be followed. They suggest that executives need to question the use of cybersecurity budgets before making decisions on the subject.

Gartner analysts recommend that enterprises engage in spending on core operational and procedural security rather than investing significant amounts of money in zero-day vulnerabilities and country watching, sinking huge budgets to deal with advanced threats. Enterprises are advised to concentrate on core infrastructure security, application security and security processes.

CONCLUSION

Security management is a function that is accompanied by expectations of high trust, and it can be bogged down by excessive emphasis on cybersecurity. There is some connection between this hype and the offensive element in the definition of cybersecurity. Thus, by dissociating the offensive element from the definition of cybersecurity, enterprises can avoid the associated hype as well.

All enterprises need to understand their business; document critical information infrastructure; and deploy multilayered protection measures to provide a tiered set of preventive, detective and corrective controls, which define their information security and OT security framework. In doing so, a risk-based approach is an absolute must. In this approach, residual risk, a risk mitigation road map and risk appetite should be clearly understood by security leadership and articulated to executive leadership. There is no room here for hype while developing this understanding, making recommendations for risk mitigation and taking executive decisions.

While offensive measures are out of scope for enterprises, organisations in some critical sectors may need to establish partnerships with suitable government establishments to report cyberattacks, and the concerned government establishment may have the mandate for retaliatory or offensive measures.

ENDNOTES

[1] Sorcher, S.; 'The Race to Build the Silicon Valley of Cybersecurity', *Christian Science Monitor*, 25 March 2015, *http://passcode.csmonitor.com/goldrush*

[2] Tech Target, "Information Security (Infosec)," *https://searchsecurity.techtarget.com/definition/information_security-infosec*

[3] Advanced Information Technology Ltd., "BSS 7799/ISO 17799/ISO 27001 Explained," 2006, *www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0CDMQFjAEahUKEwjs1Li484rIAhWULYgKHRrtDdw&url=http%3A%2F%2Fwww.iso27000info.com%2FDocuments%2FWhat%2520is%2520ISO17799%2520copy%2520version.doc&usg=AFQjCNErA876L1TF-j_FLztn9_eyAH9iGw&sig2=VOQ9QN-RBG2IQ-lFX7iGAA*

[4] International Organization for Standardization, (ISO) and the International Electrotechnical Commission (IEC) "ISO/IEC 27001—Information security management," *www.iso.org/iso/home/standards/management-standards/iso27001.htm*

[5] *Merriam-Webster Dictionary*, 'cybersecurity', *www.merriam-webster.com/dictionary/cybersecurity*

[6] Information Technology Services, "Introduction to Computer Security," University of California Santa Cruz, USA, *https://its.ucsc.edu/security/training/intro.html*

[7] Security Threats and Countermeasures Glossary, 'cybersecurity', *TechTarget*, December 2010, *http://whatis.techtarget.com/definition/cybersecurity*

[8] Techopedia, 'Cybersecurity', *www.techopedia.com/definition/24747/cybersecurity*

[9] ITU Telecommunication Standardization Sector, 'Definition of Cybersecurity', *www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx*

[10] National Institute of Standards and Technology (NIST), *Glossary of Key Information Security Terms*, NISTIR 7298, ed. Richard Kissel, USA, *http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf*

[11] Walls, A.; E. Perkins; J. Weiss; *Definition: Cybersecurity*, Gartner, 7 June 2013, *www.gartner.com/doc/2510116?ref=unauthreader*

[12] *Ibid*.

[13] *Ibid*.

[14] Franscella, J.; 'Cybersecurity vs. Cyber Security: When, Why and How to Use the Term', *InfoSec Island*, 17 July 2013, *http://infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html*

[15] *Ibid*.