Opinion
Volume 15:2, 2022

Journal of Computer Science & Systems Biology

ISSN: 0974-7230 Open Access

Role of Cyber Security in Informative Science

Elisha Stewart*

Department of Information Science, University of Bergen, Norway

Introduction

Cyber security is the use of technologies, processes, and controls to defend against cyberattacks on systems, networks, programmes, devices, and data. Its goal is to reduce the risk of cyberattacks and to protect against unauthorised use of systems, networks, and technologies. Cyber security is the use of technologies, processes, and controls to defend against cyberattacks on systems, networks, programmes, devices, and data. Its goal is to reduce the risk of cyberattacks and to protect against unauthorised use of systems, networks, and technologies [1].

Oversight of cyber security risks is becoming more difficult as a result of new regulations and reporting requirements. Management must assure the board that its cyber risk strategies will reduce the risk of attacks while also limiting financial and operational impacts. Because SCADA (supervisory control and data acquisition) systems frequently rely on older software, critical infrastructure organisations are frequently more vulnerable to attack than others. The NIS Regulations apply to operators of essential services in the UK's energy, transport, health, water, and digital infrastructure sectors, as well as digital service providers .The Regulations, among other things, require organisations to implement appropriate technical and organisational measures to manage their security risks [1,2].

Description

Addressing vulnerabilities in your operating systems and network architecture, such as servers and hosts, firewalls and wireless access points, and network protocols, is part of network security. Because a square is a quadrilateral with four right angles, every square IS a rectangle. Similarly, cybersecurity, like physical security and information security, falls under the IT security umbrella. However, not every rectangle is a square because the definition of a square requires all sides to be the same length. The point is that not all IT security measures qualify as cybersecurity because cybersecurity has its own set of assets to safeguard [2,3].

James Stanger, Chief Technology Evangelist, defines cybersecurity as "focusing on protecting electronic assets – including internet, WAN, and LAN resources – used to store and transmit that information." Convenience is one of the many benefits of living in a world where every device is connected. It's incredibly simple to use your smartphone or device to conduct business, manage your social calendar, shop, and make appointments. That's why many of us have adopted it as second nature.

However, the convenience of connected data also means that threats from bad actors can cause significant damage. Cybersecurity initiatives are critical to safeguarding our data and, by extension, our way of life. IT professionals can focus on process when employees outside of the IT department are trained. The methods used by cybersecurity professionals to protect sensitive data are multifaceted. In short, these IT professionals are responsible for detecting and identifying threats, protecting information, responding to incidents, and recovering from them [3-5].

Conclusion

Putting processes in place not only ensures that each of these buckets is constantly monitored, but if a cybersecurity attack occurs, referring to a well documented process can save your company time, money, and the trust of its most valuable asset your customers. Once you've established frameworks and processes, it's time to consider the tools you'll need to begin implementation. When it comes to your toolbox, technology has two meanings: the technology you'll use to prevent and combat cybersecurity attacks, such as DNS filtering, malware protection, antivirus software, firewalls, and email security solutions. Computers, smart devices, routers, networks, and the cloud are examples of technology that requires your protection.

References

1. Glynn, Shawn M., Gita Taasoobshirazi and Peggy Brickman. "Science motivation questionnaire: Construct validation with nonscience majors." *J Res Sci Teach* 46 (2009): 127-146.
2. Deci, Edward L. and Richard M. Ryan. "The" what" and" why" of goal pursuits: Human needs and the self-determination of behavior." *Psychol Inq* 11 (2000): 227-268.
3. Burrows, Andrea C. and Mike Borowczak. "Computer science and engineering: Utilizing action research and lesson study." *Educ Action Res* 27 (2019): 631-646.
4. Burkam, David T., Valerie E. Lee and Becky A. Smerdon. "Gender and science learning early in high school: Subject matter and laboratory experiences." *Am Educ Res J* 34 (1997): 297-331.
5. Giannakos, Michail N., Ilias O. Pappas and Letizia Jaccheri, et al. "Understanding student retention in computer science education: The role of environment, gains, barriers and usefulness." *Educ Inf Technol* 22 (2017): 2365-2382.

How to cite this article: Stewart, Elisha. "Role of Cyber Security in Informative Science." J Comput Sci Syst Biol 15 (2022):401.

***Address for Correspondence:** Elisha Stewart, Department of Information Science, University of Bergen, Norway, E-mail: ElishaStewart50@gmail.com*

Received 07-Feb-2022, Manuscript No.Jcsb-22-58226; **Editor assigned:** 09-Feb-2022, Pre QC No. P-58226; **Reviewed**: 23-Feb-2022, QC No. 58226; **Revised:** 28-Feb-2022, Manuscript No. R-58226; **Published:** 07-Mar-2022, DOI: 10.37421/jcsb.2022.15.401