Chapter 6
Cybersecurity and Cyberbiosecurity Insider Threat Risk Management

Darrell Norman Burrell
https://orcid.org/0000-0002-4675-9544
Marymount University, USA

Calvin Nobles
https://orcid.org/0000-0003-4002-1108
Illinois Institute of Technology, USA

Austin Cusak
Robert Morris University, USA

Laura Ann Jones
https://orcid.org/0000-0002-0299-370X
Capitol Technology University, USA

Jorja B. Wright
https://orcid.org/0000-0002-7028-995X
Capitol Technology University, USA

Horace C. Mingo
https://orcid.org/0000-0002-2395-2990
Marymount University, USA

Jennifer Ferreras-Perez
Marymount University, USA

Katrina Khanta
Marymount University, USA

Philip Shen
Marymount University, USA

Kevin Richardson
https://orcid.org/0009-0002-3212-8669
Edward Waters University, USA

ABSTRACT

This study examines the nature of professionals being insider threats to their own organization, as well as the general increase in harder-to-detect threats coming from an ever-widening acceptance of third-party insiders by organizations that rely on them, such as those in the fields of biomedical sciences, synthetic biology, artificial intelligence, and food production engineering. The current and emerging literature on how individuals are motivated to engage in problematic workplace behaviors as a means of gaining their specific goal or need is examined in this chapter. Following that, the chapter articulates malicious cybersecurity and cyberbiosecurity insider threat indicators and then provides best practices for reducing the risk of these threats in organizations involved in food production engineering, synthetic biology, and artificial intelligence.

DOI: 10.4018/978-1-6684-7207-1.ch006

INTRODUCTION

There is a major connection taking place between the fields of biological science, information technology (IT), and cybersecurity at the present time (Richardson et al., 2019). This convergence is a critical driver in the explosion of biotechnology research and its industrial applications in health care, agriculture, manufacturing, automation, artificial intelligence, and synthetic biology. Other industries that are benefiting from this convergence include manufacturing and artificial intelligence. Creating new creatures via the use of computer programming and other biological principles is the goal of the burgeoning subject of synthetic biology (Richardson et al., 2019). Many diverse market sectors are now exposed to the threats posed by the digital interface as a result of the growing digitalization of information and the procedures for managing biological materials. This is the case since the rate at which biological materials are managed has also increased (Richardson et al., 2019). Players within a single sector lack the agency to manage any challenges, and they are less inclined to collaborate since these convergences are not examined. The term "cyberbiosecurity" refers to an interdisciplinary junction of fields that do not fall under any specific industry (Richardson et al., 2019).

These vulnerabilities can affect biomanufacturing as well as cyber-enabled laboratory equipment and patient-focused systems (Richardson et al., 2019). Protecting computer systems against unauthorized access, theft, or damage to their hardware, software, or information, as well as interference with or diversion of the services such systems are supposed to offer, is what is meant by the phrase "cybersecurity" (Richardson et al., 2019). Important biological material must be shielded from unauthorized use or harm if the goal of biosecurity is to be achieved. Cyberbiosecurity was initially defined by Murch et al. as "developing an understanding of the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life science, cyber, cyber-physical, supply chain and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate, and attribute such threats as it pertains to security." In other words, cyberbiosecurity is "developing an understanding of the vulnerabilities to unwanted surveillance, intrusion To put it another way, the process of "building an awareness of the vulnerabilities to unwanted observation" is what constitutes cyberbiosecurity (Richardson et al., 2019). This field also suffers from the risks of insider threats.

A significant portion of the life sciences sector is comprised of sectors such as biomedical sciences, synthetic biology, artificial intelligence, and food production engineering. It is possible for biotech engineers to find employment in the production of medical equipment, the manufacture of pharmaceutical and medicinal products, research and development, teaching, and a wide variety of other fields that require their technical expertise. Protecting electronic information and assets against unwanted access, use, and disclosure is an important part of cybersecurity in many fields, including healthcare and the biomedical sciences, synthetic biology, artificial intelligence, and food production engineering (Wilder, 2022). The protection of the confidentiality, integrity, and availability of information are the three primary objectives of cybersecurity; yet, the categorization of insiders cannot simply be determined by whether or not a person is currently working (Wilder, 2022). Insiders in healthcare companies need to be investigated through the use of application and data access entitlements. Healthcare and biological sciences, synthetic biology, artificial intelligence, and food production engineering are some of the fields that are being prioritized. Cybersecurity insider risks often include hired and non-employed workers, volunteers, vendor partners, contractors, and even patients who access their personal health information via online portals. These individuals can all pose a risk to an organization's cybersecurity.