Technical Note

One Health: Safeguarding Biosecurity and Cyberbiosecurity in Toxin and Venom Research Laboratories

Subhash Janardhan Bhore *

Posted Date: 4 September 2023

doi: 10.20944/preprints202309.0184.v1

Keywords: biosecurity; cyberbiosecurity; one health; toxins; venom

Technical Note

One Health: Safeguarding Biosecurity and Cyberbiosecurity in Toxin and Venom Research Laboratories

Subhash Janardhan Bhore [1,2]

[1] Department of Biotechnology, Faculty of Applied Sciences, AIMST University, Bedong-Semeling Road, 08100 Bedong, Semeling, Kedah Darul Aman, Malaysia; subhash@aimst.edu.my or subhashbhore@gmail.com

[2] The National Coalition of Independent Scholars, 125 Putney Road, Brattleboro, Vermont 05301, USA.

Abstract: Training researchers and stakeholders is crucial to mitigate the risks associated with toxins and venom. By sharing knowledge on the responsible use of toxins, venoms, chemicals, and data from biosecurity and cyberbiosecurity perspectives, we empower laboratorians to make informed choices. We need to remember that cultivating a culture of sustainable biosafety and biosecurity is vital for one health. This technical note highlights the essence of safeguarding biosecurity and cyberbiosecurity in toxin and venom research laboratories workshop designed and implemented to boost biosecurity.

Keywords: biosecurity; cyberbiosecurity; one health; toxins; venom

Introduction

In the intricate web of life, organisms have evolved various defense mechanisms to ensure their survival. Among these adaptations, toxins and venoms play a crucial role. Research on toxins and venoms is essential to understand more about them and explore the possibilities of using them for therapeutic applications [1–5]. However, toxins and venoms from research laboratories could be misused by nefarious actors [6–9]. Hence, for biological risk (biorisk) mitigation from one health perspective, the best practices of biosecurity and cyberbiosecurity should be in place at all toxin and venom research laboratories. The concept of one health recognizes the interconnectedness of human, animal, and environmental health.

A specially designed three-day training (workshop) on safeguarding biosecurity and cyberbiosecurity in toxin and venom research laboratories was jointly organized by the Health Security Partners (HSP), USA, the Malaysian Society for Toxicology (MySOT), Malaysia, and other partners with the support of the Biosecurity Engagement Program (BEP), USA. Twenty-seven researchers from Malaysia, Singapore, and Thailand who work with toxins and animal venoms participated in the workshop. The workshop was conducted on May 24-26, 2023, at Royal Plaza on Scotts, Singapore.

The workshop's primary objective was to increase researchers' understanding of the crucial significance of maintaining biosecurity and cyberbiosecurity in laboratories dedicated to toxin and venom research. During the workshop, eleven subject matter experts (SMEs) deliberated on several issues, including the dual-use nature of toxin research, physical and personnel biosecurity methods to protect laboratories, best practices in cybersecurity to protect data from increasing cyberattacks, know-your-collaborator tools to screen collaborators or funders looking to conduct joint research, share strains and data, or requests to present findings at a conference, and importance of protecting toxins and venom, and the best practices to protect biosecurity-sensitive materials, equipment, data, technologies, and expertise from the toxin and venom research facilities. Some highlights of the workshop are reported in this paper.

 doi:10.20944/preprints202309.0184.v1

Highlights from the Workshop

During the opening remarks, a representative from BEP (USA) highlighted that the BEP is fully committed to engaging scientists and combating biological threats worldwide by assisting in improving biosecurity, bioprotection, and pathogen surveillance. BEP delegate also emphasized that all stakeholders must work together to build sustainable capacity in biosecurity, disease surveillance, and scientific investigation.

Because of the physical properties of biological toxins and easy accessibility, biotoxins (aka zootoxins) have become attractive targets of nefarious actors [10]. While discussing toxins and venoms research from a national security perspective, an SME highlighted that tight regulation is essential, as a tiny amount of toxins could kill millions and millions of people. SME also underlined that synthetic biology and biotechnology tools could be misused for the large-scale production of toxins, to make them more lethal, or to create a novel toxin. Toxins and venoms could be purchased or stolen from research laboratories or vendors or made in the do-it-yourself (DIY) laboratory – SME accentuated.

While deliberating dual-use materials, expertise, data, and equipment protection needs, an SME highlighted that United States Government policy for oversight of life sciences dual-use research of concern and policy for institutional oversight of life sciences dual-use research of concern could serve as a model for national oversight and institutional oversight, respectively. For assessing and managing risks associated with toxins and venoms, SME suggested that researchers and stakeholders from toxins and venom research laboratories should have answers to basic questions such as: Could this research yield information that could be intentionally misused to threaten public health, safety, and security? What is the nature of the threat and potential consequences? What is the likelihood that harm can be done? Do the potential risks outweigh the potential benefits?

During deliberating the dual-use material potential of various toxins and venoms, an SME pointed out that biological toxins (biotoxins) and venoms are the potential tools for bioterrorism. SME also highlighted that the main objective of dual-use research governance is to reduce accidents and incidents and enable their early detection and response, which could reduce future opportunities for misuse of research, tools, and knowledge without hindering the benefits of life science research.

Venom research is essential to understand venom evolution, its ecological impact, how venoms work, and search for novel biomolecules that could serve as precursors in developing new drugs and therapeutic applications. One of the SMEs shared a comprehensive overview of snake venom research in Malaysia and highlighted that snake venom research is essential for the benefit of humanity, as it facilitates the development of innovative treatments (e.g., synthetic antibodies, broad-spectrum antivenoms, small molecule inhibitors), diagnostic tools, and new therapeutic agents (e.g., anticancer, anticoagulant, antiplatelet, antiinfective, analgesics, antihypertensive, heart failure, etc.). During the deliberations, the participants learned the importance of protecting venom, cDNA/DNA clones, plasmid DNA, gene expression cassettes, and disposal of biowaste and biosecurity-sensitive materials from the venom research facilities.

Pore-forming toxins (PFTs) are a class of proteins produced by various bacteria, fungi, and other organisms [11]. PFTs can cause tissue damage, organ failure, and even systemic effects. Not all PFTs are harmful to humans; however, dangerous PFTs could be misused by nefarious actors. An SME shared a comprehensive overview of the PFTs family, including Anthrax toxin (*Bacillus anthracis*), lota toxin (*Clostridium perfringens*), Tc toxin (*Photorhabdus luminescens*), VCC toxin (*Vibrio cholerae*), and **α**-Hemolysin (*Staphylococcus aureus*), and highlighted that understanding the mechanisms and effects of these toxins is crucial for developing strategies to prevent and treat associated illnesses and to mitigate the biosecurity risks.

To inculcate the importance of identifying and mitigating insider and outsider threats, an SME discussed toxin scenario-based case studies and highlighted the importance of laboratory biosecurity oversight in protecting biotoxins (e.g., Botulinum, Mycotoxins, Saxitoxin, Neosaxitoxin, Abrin, Ricin, etc.) and venoms (aka zootoxins) to mitigate the risks. SME also stated that timely identification of the gaps in toxins and venom research laboratories' biosecurity program would help avoid disasters.

 doi:10.20944/preprints202309.0184.v1

Through scenario-based discussions, participants learned to identify the common gaps in laboratory biosecurity risk management and recognized the biosecurity threats from toxins and venoms.

In order to mitigate the biosecurity risks at toxins and venom (as well as other life sciences) research facilities, all laboratorians must be familiar with the eight pillars of biosecurity. While deliberating about how to secure toxins and venom-related dual-use materials, expertise, data, and equipment, an SME highlighted that by adhering to the eight pillars of biosecurity (biosecurity awareness, personnel reliability, physical security, material control and accountability, transport security, information security, emergency response, and management), we could strengthen our preparedness, response capabilities, and resilience in the face of biosecurity threats. From one health perspective, the SME also highlighted the importance of biosecurity best practices in safeguarding dual-use biological materials, equipment, and knowledge.

While sharing thoughts on the responsibility of scientists working with dual-use materials, an SME highlighted that researchers working with dual-use materials have a special responsibility to ensure the ethical and responsible use of their research and knowledge. Dual-use materials imply substances, technologies, data, or knowledge that can have both beneficial and potentially harmful applications. It is vital for researchers to recognize the potential risks associated with toxins, venoms, and their work and take appropriate measures to minimize associated biosecurity risks – participants learned.

To ensure appropriate measures are in place, life sciences research organizations must have an

Insider Threat Program. In this line, during deliberations on identifying and preventing insider threats, an SME highlighted that we should not ignore insider threats, as legitimate access to materials, equipment, and information could be misused to cause damage or harm to staff, the organization, or the community. SME also stated that personal risk factors (e.g., conscience, connections, ego, financial, ideology, lifestyle, nationalism, etc.), work-related risk factors (e.g., performance, violations, security weakness, etc.), and targeting risk factors (e.g., foreign travel, exposure, knowledge, and access, etc.) must be considered while identifying and preventing insider threat. Troubled insiders tend to behave in ways that can give cause for concern; hence, understanding behavioral queues is essential to identifying insider threats – workshop participants learned.

From a biosecurity perspective, identifying and preventing the exploitation of research collaboration is crucial. In this line, during deliberation on how to identify and prevent exploitation of research collaboration, one of the SMEs highlighted that establishing clear expectations, promoting open communication, and addressing potential issues early on help in protecting researchers and their organizations. SME also highlighted that meticulous due diligence (DD) and know-your-customer (KYC) best practices help in identifying red flags to avoid exploitation by nefarious actors or their proxies.

Physical security and access control are crucial for protecting toxins, venoms, biological agents, and biosecurity-sensitive material, equipment, and knowledge from laboratories for several reasons. In this line, an SME discussed the importance of physical security and access control and highlighted that physical security and access control are critical components in ensuring the safe handling, storage, and protection of valuable assets, including toxins, venoms, and biological agents.

A meticulously maintained inventory of organizations' valuable assets is crucial to mitigate biosecurity risks. Inventory encompasses the assortment of merchandise or substances an organization maintains, encompassing toxins, venoms, biological agents, chemicals, and infective or toxic materials such as tissues, tissue extracts, and DNA/RNA/protein samples. One of the SMEs highlighted that inventory, material accountability, and information security are essential for every life sciences research organization to ensure biosecurity. SME underlined the importance of recognizing no one-size-fits-all, considering the operating environment (e.g., the chain of custody, fieldwork, physical security), involving IT and security teams to advise, evaluating the needs and feasibility of the organization’s goals, and observing odd behaviours of laboratorians and stakeholders.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 September 2023 doi:10.20944/preprints202309.0184.v1

Prevention is always better than cure. In this line, robust preventive measures (deter, detect, delay) are always better than reactive measures (respond, recover) to mitigate biosecurity risks. However, we need to remember that adversaries have the means, motives, and capabilities to cause harm. Therefore, life sciences research organizations' emergency response teams (ERT) should be competent and well-equipped. During deliberation on emergency and incident response, an SME highlighted that the red teaming exercise is very helpful in identifying if there are any biosecurity vulnerabilities in the organization. Red teaming exercise could be used to discover weaknesses in development and testing processes, assess internal employees' awareness about information security, understand the impact of a security breach, and test the information environment, team's incident response capabilities, security controls, and organization's ability to protect critical assets from real-world attacks – participants learned.

Life sciences research organizations and researchers started recognizing the importance of cyberbiosecurity [12], as it addresses the emerging threats [13] and vulnerabilities associated with the increasing use of digital systems, data [14], and biotechnologies [15]. During the deliberation on the best practices in cybersecurity to protect data in research laboratories, an SME highlighted that a breach in cybersecurity could have substantial adverse impacts on the supply chain, one health, safety, environment, quality, regulatory (or legal) system, economy, and reputation of organizations or countries. SME also underlined the importance of data flow analysis to identify and document life sciences research organizations' requirements, data sources, manual dependencies, processes, and data. SME stated the importance of understanding - Who will access the data? What activities will be performed on the data? What are the access rights defined? How will data flow? Where is the data stored? What are the security controls? During the discussions, participants also learned the importance of identifying and controlling data egress points (Table 1) to mitigate the organization's cyberbiosecurity risks.

Table 1. Data egress point controls to mitigate cyberbiosecurity risks.

No	Data Egress Points	Controls
1.	Removable media (e.g., USB, CD, etc.)	• Blocking access through domain controller group policies • Mobile device management (MDM) • Host-based data loss prevention (DLP)
2.	Email	• Restricting access to send emails to external domains • Email attachment file type and size restrictions • No web email access is to be granted over the internet • Email access on mobile devices through MDM solution with containerization control • Host-based or network-based DLP
3.	Laptop	• Hard-disk encryption • The solution to wipe data remotely • Data rights management (DRM) • Host-based DLP
4.	Unrestricted internet access	• Uniform resource locator (URL) filtering • Restrict users from connecting to external internet connections or a wireless network (Wi-Fi) • URL filtering for users connecting to the external internet connection
5.	Special internet access	• URL filtering solution to turn off file upload feature • Host-based or network-based DLP

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 September 2023 doi:10.20944/preprints202309.0184.v1

6.	Internet-facing application	• System and application security • Restrict display of personally identifiable information (PII) • Restrict the download of data from the application • Internet protocol (IP)-based access restriction • Host application admin module on different network ports from normal user access port and restrict access to admin module over the internet
7.	Printing	• DRM solution to restrict print rights • Restrict printer access • Implement and monitor secure printing solution • Host-based DLP
8.	Remote privilege user access rights	• Provide remote access through company virtual private network (VPN) connectivity to limited authorized users on company-provided laptops • Restrict privileged user access through a privilege access management (PAM) solution • Provide remote access rights through a company-owned virtual desktop solution (VDS)
9.	Data exchange with the third party	• A signed service agreement with nondisclosure agreement (NDA) clauses, right to audit, and security requirements • Extension of security controls like digital rights management (DRM), remote access through virtual desktop • Third-party risk assessment
10.	Data hosted in the cloud environment	• A signed service agreement with NDA clauses and security requirements • Controlled access to the cloud admin account • Encryption of data stored at rest with key management controls
11.	Data leak through malware	• Restricted internet access • Threat intelligence integrated with URL filtering • Blocking outgoing traffic • Advanced threat protection (ATP)
12.	Taking photos or writing data	• Restrict mobile camera usage in critical work areas • Restrict pen-paper usage in critical work areas
13.	Offsite backup tapes	• Keep all tapes, disks, and other materials in a controlled environment safe from heat, humidity, dust, etc. • Periodically test long-term retention media and migrate it to new media as technology evolves to ensure data recoverability

USB, Universal Serial Bus; *CD*, Compact Disc.

During the guided exercises, participants were able to identify the existing mitigation measures and biosecurity-associated vulnerabilities in inventory control, information control, personnel control, physical security control, transport security control, emergency and incident response, dual-

use research of concern management, and emerging technologies management at their organization. Round table discussions, case studies, lectures, and exercises helped participants to gain knowledge about biosecurity threats associated with toxins and venom (as well as biological agents) research and the challenges posed by nefarious actors.

At the end of the workshop, participants were able to recognize the importance of best practices to deal with the biosecurity and cyberbiosecurity threats associated with toxins and venom research and develop a suitable biosecurity plan to fix the vulnerabilities.

Concluding Remarks

Research on toxins and venom is essential for studying evolution, advancing medicine, understanding nature, developing new drugs, improving agricultural practices, and exploring biotechnological applications. Hence, we need to encourage toxins and venom research, as it has the potential to benefit human health, conservation efforts, and various industries. However, recognizing the interconnectedness of human, animal, and environmental health through the lens of one health is essential in understanding the impact of toxins and venoms. All stakeholders must remember that we cannot afford to ignore the biosecurity and biosafety risks associated with toxins and venoms and their potential misuse by nefarious actors.

By fostering collaborations, promoting and sharing biosecurity best practices, and implementing preventive measures, we can mitigate the risks associated with toxins and venoms. However, it is crucial to remember that not a one-size-fits-all. Every toxin and venom research facility has unique needs and priorities, and laboratory managers and researchers must determine what works best for their situation to mitigate the biosecurity and cyberbiosecurity risks.

Considering the overall discourse, the main insights from the workshop on safeguarding biosecurity and cyberbiosecurity in toxin and venom research laboratories can be summarized as follows:

i. Prevent unauthorized access to hazardous materials to avoid potential risks.
ii. Breaches in biosecurity can jeopardize public health if hazardous materials fall into the wrong hands or are released accidentally.
iii. Laboratory managers and personnel play a vital role in mitigating bioterrorism threats and safeguarding valuable intellectual property.
iv. Address insider threats to prevent unethical practices and unauthorized experimentation.
v. Promote know-your-collaborator/customer and due diligence best practices to protect valuable knowledge and materials.
vi. Biosecurity and biosafety must be overseen together to protect laboratorians, the surrounding community, and the environment.
vii. Establish biosecurity and cyberbiosecurity policies at the facility/organization level.
viii. Ensure proper training for all staff to mitigate biosecurity, cyberbiosecurity, and biosafety risks.
ix. Emphasize cyberbiosecurity to protect valuable assets from data breaches and intellectual property theft.

Bearing in mind the importance of safeguarding biosecurity and cyberbiosecurity at life sciences research laboratories, we can and must promote biosecurity best practices to mitigate biorisks and protect human, animal, and environmental health from one health perspective.

Funding Information: The author received no financial support for the research, authorship, and or publication of this article.

Author's Note: The contents of this article manuscript have not been shared or published elsewhere. The MS will be submitted to a suitable journal for its consideration for publication.

Informed Consent Statement: Not applicable as the study not involving humans.

Data Availability Statement: Not applicable.

Acknowledgements: The Health Security Partners (HSP), USA, fully supported the author's participation in the workshop on behalf of the United States Department of State's Biosecurity Engagement Program. Views expressed in this article are of the author and/or the interpretation of subject matter experts' views from the author's personal perspective and do not necessarily the official standpoint of the author's affiliated organizations or organizers of the training program or the United States Government.

Author's Disclosure Statement: The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article. Organizers of the workshop and the author's affiliated organizations had no role in the writing of the manuscript or in the decision to publish this technical note.

References

1. Kayani AMA, Silva MS, Jayasinghe M, *et al*. Therapeutic Efficacy of Botulinum Toxin in Trigeminal Neuralgia. *Cureus* 2022; 14(7):e26856.
2. Yu Y, Yang R, Zhao X, *et al*. Abrin P2 suppresses proliferation and induces apoptosis of colon cancer cells via mitochondrial membrane depolarization and caspase activation. *Acta Biochim Biophys Sin (Shanghai)* 2016; 48(5):420-429.
3. Bortolotti M, Polito L, Bolognesi A. Toxin and Immunotoxin Based Therapeutic Approaches. *Toxins (Basel)*. 2022; 14(1):63.
4. Rodriguez-Morales AJ. Therapeutic uses of botulinum toxin. *Can Fam Physician* 2009; 55(5):514-515.
5. Park SG, Kim H, Jun H, Choi SY, Kim E, Kang S. Directing ricin-based immunotoxins with targeting affibodies and KDEL signal peptide to cancer cells effectively induces apoptosis and tumor suppression. *J Nanobiotechnol* 2022; 20(1):387.
6. Lee YJ, Cowan A, Tankard A. Peptide Toxins as Biothreats and the Potential for AI Systems to Enhance Biosecurity. *Front Bioeng Biotechnol* 2022; 10:860390.
7. Dayan AD. Misuse of 'toxin.' *Clin Med (Lond)*. 2008; 8(2):230.
8. Misuse of botulinum toxin is potentially lethal. *BMJ*. 2006; 333(7580):1212.
9. Bhore, S.J. Countering Biothreats from Low-Effort Toxins: Some Highlights from the Chemical and Biological Investigation, Evidence, and Countermeasures Training. *Preprints.org*. 2023; 2023040815.
10. Pöhlmann C, Elßner T. Multiplex Immunoassay Techniques for On-Site Detection of Security Sensitive Toxins. *Toxins (Basel)*. 2020;12(11):727.
11. Ulhuq FR, Mariano G. Bacterial pore-forming toxins. *Microbiology (Reading)*. 2022; 168(3):001154.
12. Murch RS, So WK, Buchholz WG, Raman S, Peccoud J. Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy. *Front Bioeng Biotechnol* 2018; 6:39.
13. Tracie EB, Tipples G, Kuschak T, Gilmour M. Laboratory response checklist for infectious disease outbreaks-preparedness and response considerations for emerging threats. *Can Commun Dis Rep* 2020; 46(10):311-321.
14. Mocydlarz-Adamcewicz M, Bajsztok B, Filip S, Petera J, Mestan M, Malicki J. Management of Onsite and Remote Communication in Oncology Hospitals: Data Protection in an Era of Rapid Technological Advances. *J Pers Med* 2023; 13(5):761.
15. Bouchaut B, de Vriend H, Asveld L. Uncertainties and uncertain risks of emerging biotechnology applications: A social learning workshop for stakeholder communication. *Front Bioeng Biotechnol* 2022; 10:946526.