Abstract – the paper "Human Factors in Biocybersecurity Wargames" emphasizes the need to understand vulnerabilities in the processing of biologics and how they intersect with cyber and cyber-physical systems. This understanding is crucial for ensuring product and brand integrity and protecting those served by these systems. It discusses the growing prominence of biocybersecurity and its importance to bioprocessing in both domestic and international contexts.

I. Introduction

A. *Scope of Bioprocessing:*

- Bioprocessing encompasses the entire lifecycle of biosystems and their components, from initial research to development, manufacturing, and commercialization.
- It significantly contributes to the global economy, with applications in food, fuel, cosmetics, drugs, and green technology.

B. *Vulnerability of Bioprocessing Pipelines:*

- The bioprocessing pipeline is susceptible to attacks at various stages, especially where bioprocessing equipment interfaces with the internet.
- This vulnerability necessitates enhanced scrutiny in the design and monitoring of bioprocessing pipelines to prevent potential disruptions.

C. *Role of Information Technology (IT):*

- Progress in bioprocessing is increasingly dependent on automation and advanced algorithmic processes, which require substantial IT engagement.
- IT spending is substantial and growing, paralleling the growth in bioprocessing.

D. *Open-Source Methodologies and Digital Growth:*

- The adoption of open-source methodologies has led to significant growth in communication and digital technology development worldwide.
- This growth is further accelerated by advancements in biological computing and storage technologies.

E. *Need for New Expertise:*

- The integration of biocomputing, bioprocessing, and storage technologies will necessitate new expertise in both operation and defense.
- Basic data and process protection measures remain crucial despite technological advancements.

F. *Importance of Wargames:*

- To manage and secure connected bioprocessing infrastructure, IT teams must employ wargames to simulate and address potential risks.
- These simulations are essential for preparing organizations to handle vulnerabilities in their bioprocessing pipelines.

II. Importance of Emphasizing the Bio Component in Biocybersecurity

A. *Evolution of Biological Processes:*

- Biological processes are no longer just the result of data processing. They are now integral to various functions such as interlocks (e.g., retina and fingerprint scanners), decision-making (e.g., health monitors), and even data processing techniques themselves (e.g., biocomputing).

B. *Biological Phenomena in Cybersecurity:*

- In biocybersecurity, biological phenomena can serve as interlocks and facilitatory steps within cybersecurity systems. This integration introduces numerous potential targets for exploitation, from simple organism behaviors to the properties of organic compounds.

C. *Monitoring and Targeting:*

- The transport of biomolecules within or between organisms can be precisely monitored, and specific genes can be targeted. This can be done on both macro and microscales, requiring creativity but offering potentially profitable outcomes.

D. *Predictive Analysis:*

- Insurance companies might use genomic data to set rates based on projected diseases, although current tools are flawed. However, the predictive power of these tools is expected to improve over time.

E. *Biocomputing and Bioprocessing:*

- As bioprocessing infrastructure increasingly relies on biocomputing, societies will need to examine biological systems similarly to how they examine digital systems.
- DNA can be used to encode weapons to attack machinery interfacing with bioprocessing pipelines or as a means of smuggling.

F. *Need for Rigorous Examination:*

- A lack of rigorous design and protocol can be disastrous for an organization. Therefore, teams are encouraged to

thoroughly examine their bioprocessing pipelines to identify and mitigate vulnerabilities.

III. WarGame Simulation

A. Preliminary Steps

- **Selection**: Appoint a facilitator knowledgeable in cybersecurity and interpersonal skills to run the activity.
- **Review**: Review current security procedures and evaluate participation, such as unsecured devices or poor password practices.

B. Step 1 - Training

- Divide into "data defenders" and "data hackers" teams.
- The hacker identifies a vulnerability, and the defender finds a way to patch it (e.g., malicious USB drives and disabling USB ports).
- Switch roles and partners every 5-10 minutes.

C. Step 2 - Group Ideation

- Defenders envision strategies to protect against vulnerabilities.
- Hackers devise exploits targeting the facility's vulnerabilities.
- Allow sufficient time for ideation using materials like whiteboards and sticky notes.

D. Step 3 - WarGame

- The hacker group announces an exploit plan.
- The defender group responds with a mitigation strategy.
- This response continues until an impasse or time limit.
- The activity should be recorded for analysis of weaknesses and potential security improvements.

IV. Discussion

A. Common Exploitations Identified:

- **Inefficiency and Exploitations of Security Theater**: Security measures that are more for show than actual protection can be inefficient and exploitable.
- **Security Implications of Underpaid or Unpaid Workers**: Workers who are not adequately compensated may pose security risks.
- **Miscommunications of Conventional Security Threats**: There are often miscommunications regarding traditional security threats.
- **Lack of Knowledge of Novel Threats**: Staff may lack awareness of new and emerging threats.

B. Knowledge Gaps:

- There are considerable gaps in knowledge among staff in firms involved in bioprocessing operations. This highlights the need for continuous education and training.

C. Importance of Switching Roles and Staying Updated:

- Participants in wargames should switch roles and stay updated on new trends in biocybersecurity, cybersecurity, and biosecurity. This is crucial as developments in these fields may not always overlap.

D. Frequency and Variation of Wargames:

- It should be conducted frequently to keep staff practiced and aware of potential dangers. The style and order of wargaming can be varied to meet organizational needs.

E. Exploration of Complex Scenarios:

- It is suggested to explore wargames involving multiple opposing groups, such as state-level actors, corporate actors, internal actors, and ethical hackers. This can provide a more comprehensive understanding of potential security dynamics.

F. Shared Destiny of IT and Bioprocessing:

- The discussion emphasizes that IT and bioprocessing are increasingly interconnected. Both mental and physical operations should reflect this shared destiny to ensure optimal security.

V. Importance and Conclusion

- **Fast-Paced Development**: The rapid advancements in biology and bioprocessing necessitate continuous and collaborative security efforts.
- **Diverse Requirements and Tools**: Different laboratories have varying requirements, tools, cyber-physical interactions, and workarounds, which influence their specific security needs.
- **Vulnerability of Lower Funded Labs**: Labs with less funding are more susceptible to conventional penetration methods due to limited resources.
- **Targeting of Well-Funded Labs**: Labs with substantial funding may be specifically targeted due to their valuable assets and research.
- **Incomplete Supply Chains**: research facilities do not have a complete end-to-end supply chain, making them vulnerable to exploitation at various interaction points.
- **Need for Comprehensive Security**: Achieving comprehensive security coverage requires representation and collaboration from all invested groups within the facility.