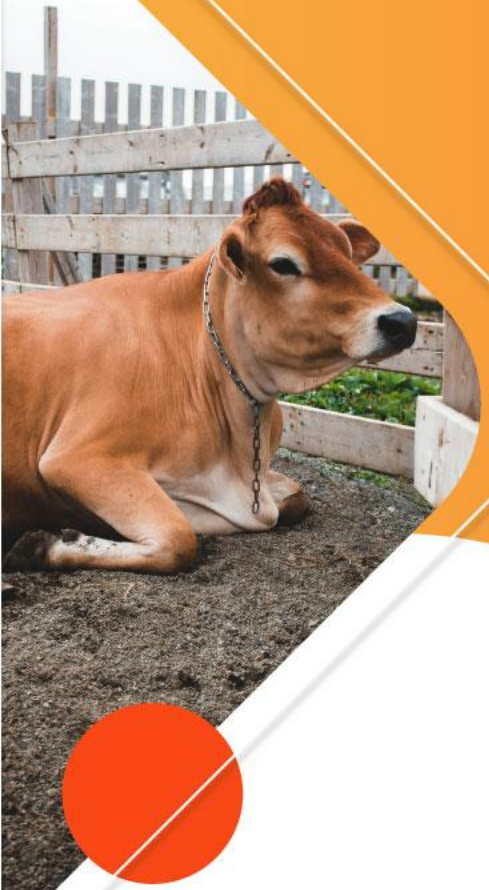
World Organisation for Animal Health

Regional Training Seminar for WOAH National Focal Points for Veterinary Laboratories (cycle III)

8 - 10 July 2025, Gaborone, Botswana



Co-funded by the European Union

Counter Proliferation & Arms Control Centre

CyberBiosecurity

Dr. Kennedy Chepukosi

CyberBiosecurity Expert
IFBA-Certified (BRM, Biosecurity, BRA & CyberBiosecurity)
Lecturer, Technical University of Kenya

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

What networked devices/equipment do you have in your organization?

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Does your organization have any of these?

- Incident response plan
- Bring your own device policy (BYOD)
- Laboratory Information Management System (LIMS)

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Ever heard of (or use) any of these?

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Outline

- Case studies
- What is CyberBiosecurity?
- Foundations of CyberBiosecurity
- Threat Landscape
- CyberBiosecurity vulnerabilities in the laboratory
- CyberBiosecurity Risks to Materials, Data, Lab Workers, Animals & the Environment
- Developing Cybersecurity Training Programs & Fostering Awareness

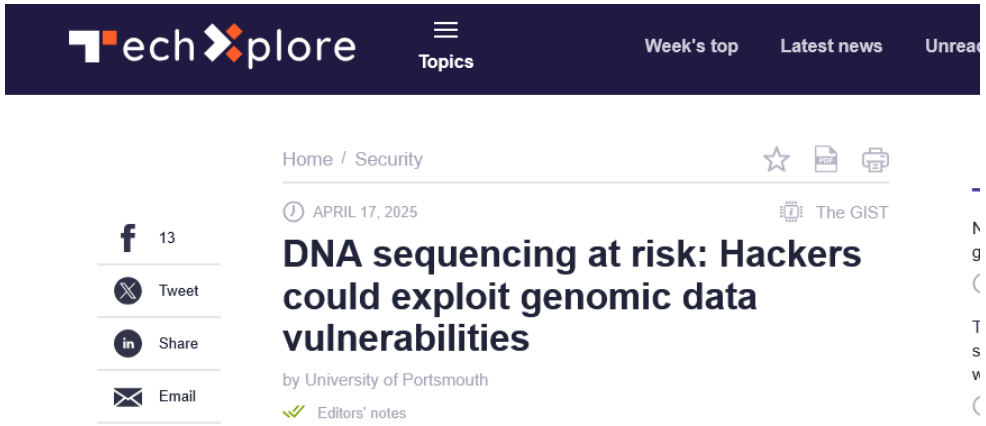
Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Case studies

SCIENCE

These Scientists Took Over a Computer by Encoding Malware in DNA

There's no immediate threat, but as sequencing becomes more commonplace, researchers face security risks.



Ransomware attack hits German pharmaceutical wholesaler, disrupts medicine supplies

AEP, a German pharmaceutical wholesaler based in Bavaria, said it was hit by a ransomware attack that could disrupt the supply of medicine to thousands of pharmacies.

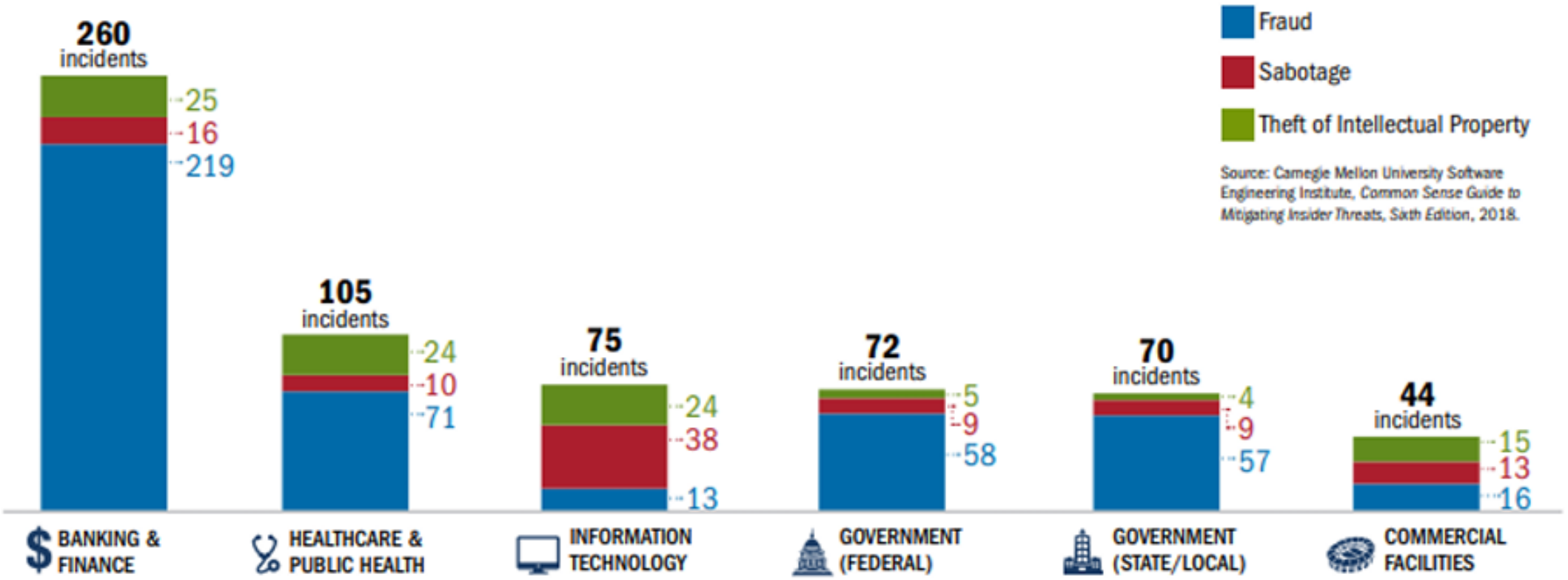
Cyberattack on UK's CVS Group disrupts veterinary operations

By Bill Toulas

April 8, 2024 10:45 AM 0

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

What Sectors are targeted?



Carnegie Mellon University Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats*, Sixth Edition.

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

What is CyberBiosecurity?

"It is Nexus between Biology and Cybersecurity"

- *Computers can be compromised by encoding malware in DNA sequences*
- **Biological threats** can be **synthesized** using publicly **available data**
- **Trust within the biotechnology** community creates vulnerabilities at the interface between cyberspace and biology
- **Awareness is a prerequisite to managing these risks**

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Foundations of CyberBiosecurity

- Multidisciplinary
- Associated with potentially significant impacts to the bioeconomy
- Addresses the *malicious destruction, misuse, or exploitation of valuable information, processes, and material*
- Requires an **understanding of both life science and the digital worlds**

"[…] emerging hybridized discipline at the interface of cybersecurity, cyber-physical security and biosecurity."

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Threat Landscape

Cyberbiosecurity by the Numbers

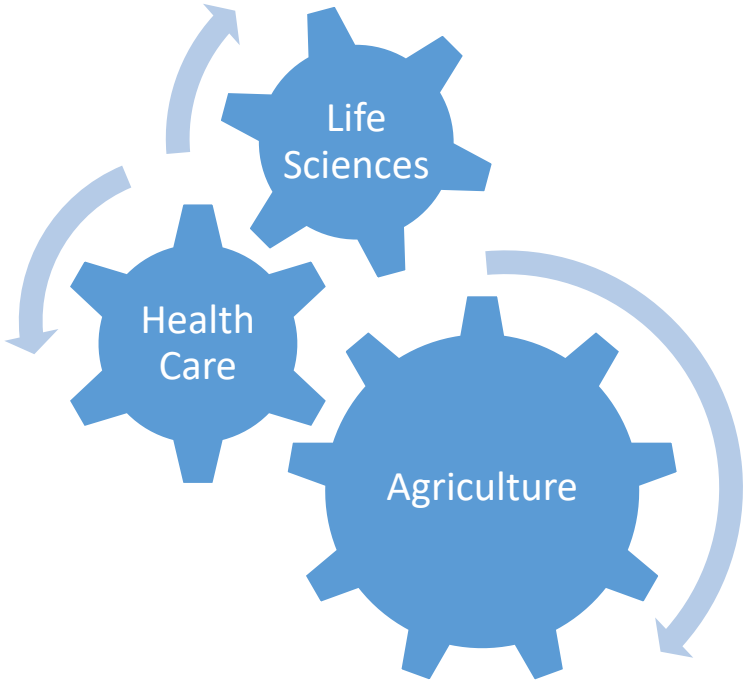
- Ransomware attacks succeed every **40 seconds**, with an attempt every **11 seconds** (DataProt).
- **53%** of connected healthcare devices at risk of a cybersecurity attack (Cynerio).
  - Most vulnerable are IV pumps and VOIP systems

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

CyberBiosecurity – Risks to the Bioeconomy

Threats to the Bioeconomy

- Disrupted growth and innovation
- Theft, loss, or disruption of IP and data
- Misuse of products and organizations



Impacts from Realized Risk

- Employment
- Supply chain
- Transportation
- Trade
- Security
- Cybersecurity

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

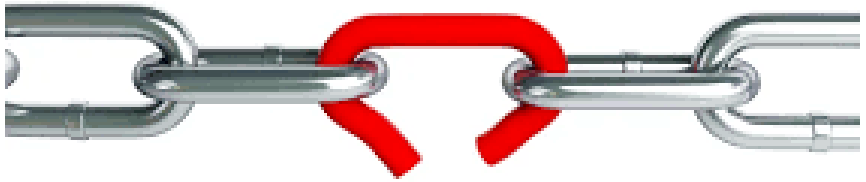
Sectors of concern

- Life sciences
  - Research
    - Sequencing
    - Laboratory Information Management Systems (LIMS)
  - Diagnostics
    - Patient information
    - Epidemiologic data
  - Non-traditional laboratory environments
- Biomanufacturing
- Biomedical sciences
- Biotechnology
- Synthetic biology

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

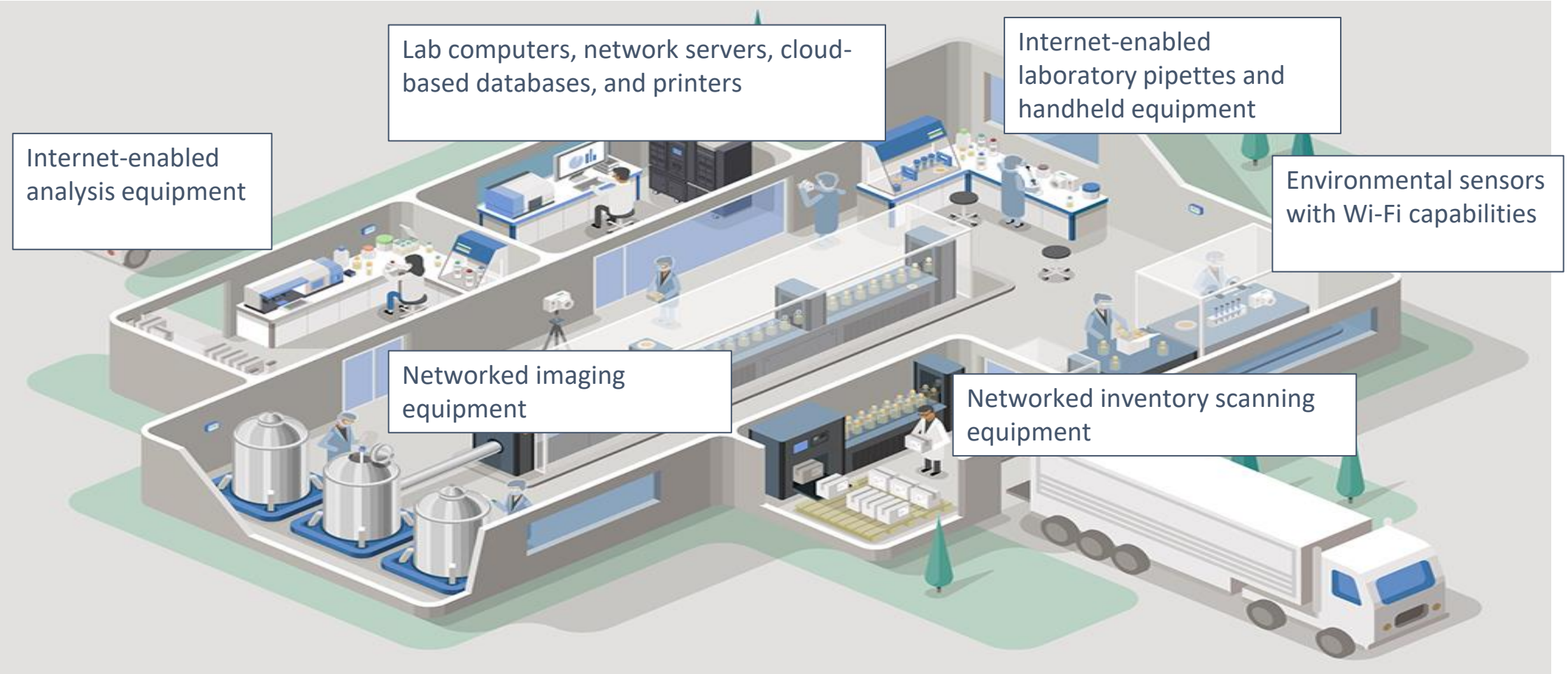
CyberBiosecurity vulnerabilities in the laboratory

- *"A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate the system security policy."*



Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Where are the vulnerable points?



Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Common equipment as attack vectors

All-in-one networked printers

Cameras and Surveillance

Freezer/Refrigerator Temperature Monitors

VoIP Phones

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Interconnected equipment and the IOT

Lab equipment as new vectors for cyberbiosecurity attacks

- **Interconnected devices** and sensors can be targeted by adversaries
- “Smart” technology, thermal cyclers, incubators, freezers, environmental sensors…

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Cyber-Physical vulnerabilities

- Access control systems
- Cameras and surveillance equipment
- Air handling / differential pressure systems
- Animal cage controls and containment systems

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Cyber-Material vulnerabilities

- Schedules/patterns for operations
- Digital maintenance order requests and schedules
- Biological waste streams and schedules
- Environmental monitors
- Inventory management systems and acquisition management

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Cyber-Transport vulnerabilities

- Record-keeping systems
- Chain-of-custody
- Transit control procedures
- Transport information and incident response planning

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Cyber-Personnel vulnerabilities

- Personnel access to data/ systems
- Training and competency
- Personal devices

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

CyberBiosecurity Risks to Materials, Data, Lab Workers, Animals & the Environment

What is a Biological Risk?

- *"The **probability** that a particular adverse event [e.g., accidental infection or unauthorized access, loss, theft, misuse, diversion or intentional release], possibly leading to harm, will occur."*

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

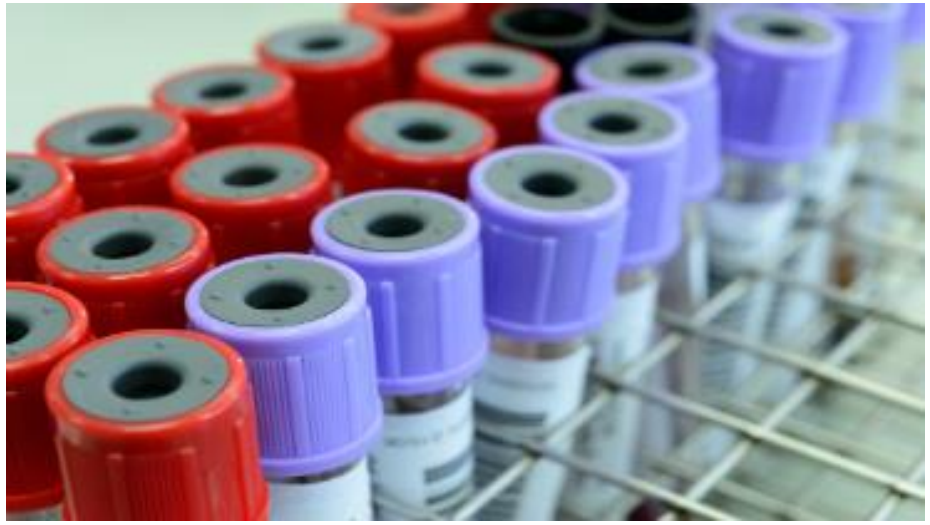
CyberBiosecurity Risks

- Integrity of materials
- Integrity of data and patient information
- Worker safety
- **Laboratory animals**

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Risk to integrity of materials

- Altering DNA/RNA sequences
- Disrupting material storage conditions
- Altering reaction parameters
- Decreasing integrity of resultant work and publications



Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Risk to integrity of data

- Altering, deleting, withholding, or generating uncontrolled data
- Releasing confidential data
- Creating malicious data that damages equipment or networks
- Data theft, misuse, violation of intellectual property
- Alteration of epidemiologic information
- Patient data and medical history

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Risk to Laboratory workers

- Compromised lab containment
  - Reversing containment airflow
  - Compromising intrusion detection measures
- Theft or ransom of medical information
- Compromising laboratory equipment to create operational hazards

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Risk to laboratory animals

- Disruption of **digitized monitoring equipment** (e.g., compromised animal cages or physical containment system)
- Alteration of animal housing conditions
  - Temperature
  - Air quality
  - Noise levels
- Adulteration or interruption of supply chain for animal feed, bedding, supplies, e.t.c

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

CyberBiosecurity Risk and Threat Assessment

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Framework of Risk and Threat assessment

Ground-up laboratory assessment

- What equipment do I have, and which of it is IoT-enabled?
- What are my assets?
- Which of my assets are valuable to adversaries, and how are they protected?
- What are my lab's threats, vulnerabilities, and potential risks?
- What can I do to mitigate risks?
- How can I measure the effectiveness of my mitigation strategy?
- How do I respond in the event of a successful or unsuccessful attack?
- How often should I revisit my mitigation protocols?

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Defining Risks, Threats and Vulnerabilities

Risk is the potential for loss, harm, or damage.

Threat is an activity, deliberate or unintentional, with the potential for causing harm.

Vulnerability is a weakness in a system.

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Defining Risks, Threats and vulnerabilities

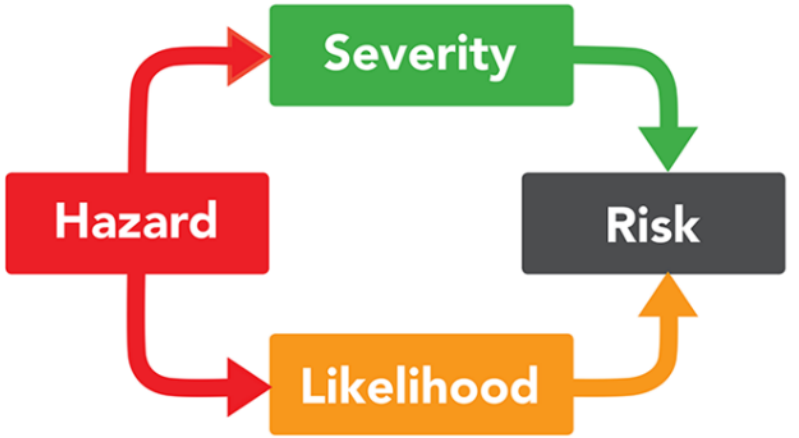
Threat + Vulnerability = Risk

Threat	Vulnerability	Risk
Negligent insider	Poor cybersecurity practices	Data breach

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Conducting Assessment

1. Identify and prioritize biological materials
2. Identify and prioritize the threat
3. Analyze the risk with biosecurity scenarios
4. Develop a Risk Management Program/Plan
5. Re-evaluate regularly



Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Developing Cybersecurity Training Programs & Fostering Awareness

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Communication mechanisms

Know your incident response communication mechanisms…

- Phone
- Email
- Teams / Instant Messaging
- Hotlines or Call Numbers
- Alternate systems

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Training program development

- Identify user groups
- Perform cybersecurity risk assessments
- Assess vulnerabilities and define mitigation strategies
- Competency testing and evaluation
- Iterate as necessary

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Awareness raising

- Culture of security
- Engagement of leadership
  - Impact on the organization
  - Impact on clients and public appearance
  - Impact on reputation

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Best practices for individuals

- Proper device hygiene
- Stewardship of your digital footprint
- Approval processes for new devices
- Supervised integration of new equipment
- Thorough and frequent communication among personnel
- Protect company information and intellectual property

- Use strong, unique passwords
- Regularly update software and systems
- Implement two-factor authentication (2FA)
- Backup important data frequently

https://haveibeenpwned.com/

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

For organizations/Institutions

- Ensure regular pentest services
- Have BYOD policy
- Have a robust incident response plan
- Ensure compliance with cybersecurity framework(s) (NIST 2.0, ISO 27001 & ISO 27002 Frameworks, SOC2 Framework, NERC-CIP Framework, HIPAA Framework, GDPR Framework, FISMA Framework)
- Cybersecurity training programs

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Key Takeaways

✓ **Technology presents significant security vulnerabilities** to the life science enterprise and public health space

✓ **Cybersecurity** and **global health security converge** with increasing digitization of health data and information

✓ **Vulnerabilities pose a threat** to individual organizations' **reputation**, **integrity** and **quality of research data**, intellectual property, and **biological products**

✓ **Exploitation of these vulnerabilities** could easily **compromise public health** and health security

✓ There is an **urgent need to prevent threats** to bioeconomy through integrated efforts

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

“Security of Biological Data and Infrastructure is a Shared Responsibility”

Co-funded by the European Union
Counter Proliferation & Arms Control Centre

Thank You!

Co-funded by the European Union
Counter Proliferation & Arms Control Centre