Laboratory Biorisk Assessments: Considerations for Incorporating Cyberbiosecurity

Julianne L. Baron, PhD, CPH, RBP (ABSA), CC
Professional Certification in Biorisk Management (IFBA)
Professional Certification in Cyberbiosecurity (IFBA)
Certified in Cybersecurity (ISC2)

Science and Safety Consulting

What is Cyberbiosecurity?

- **Cybersecurity** - protection of networks, devices, and data from unauthorized access, theft or damage of physical and data assets, and disruption of services or systems

- **Laboratory Biosecurity** - protection of biological material, technology, or research-related information from loss, theft, or deliberate misuse

- **Cyberphysical Security** - protection of network systems and devices that interact with physical input and output

Murch et al. (2018). Front. Bioeng. Biotechnol. 6:39.

Lab Attacks in the News

1.3 Million-Record Database of Netherlands COVID-19 Testing Lab Exposed Online

Clinical test data of 2.5 million people stolen from biotech company Enzo Biochem

LifeLabs pays ransom after massive data breach affecting up to 15 million Canadians

Nationwide Laboratory Services Ransomware Attack Affects 33,000 Patients

Personal information of thousands of Idaho National Laboratory employees leaked online

UnitedHealth confirms ransomware gang behind Change Healthcare hack amid ongoing pharmacy outages

Johnson Controls Ransomware Attack: Data Theft Confirmed, Cost Exceeds $27 Million

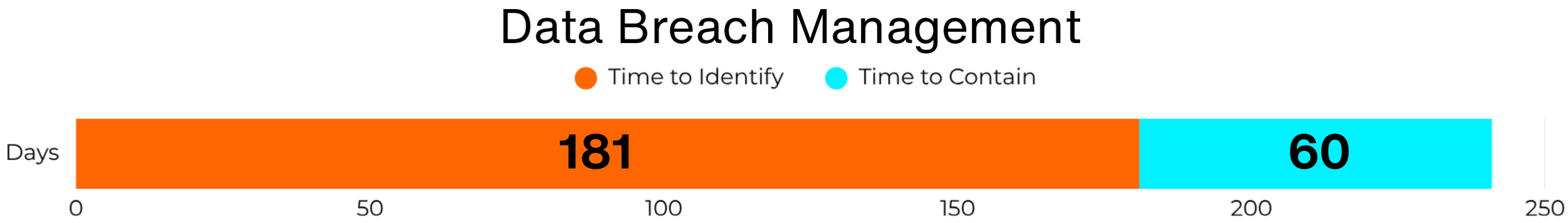
Molecular Pathology Laboratory Network, Inc. Reports Healthcare Data Breach Impacting Patients' PHI

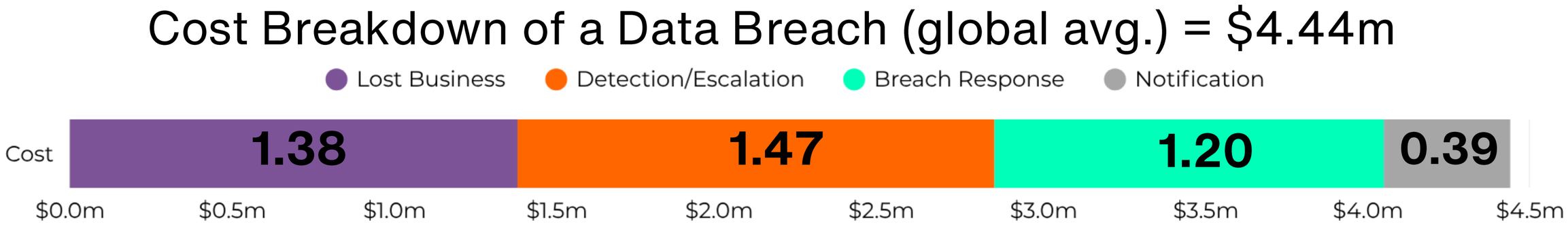
Email Breach at CSI Laboratories Impacts Almost 245,000 Patients

23andMe confirms hackers stole ancestry data on 6.9 million users

HACKERS ARE SELLING ACCESS TO BIOCHEMICAL SYSTEMS AT OXFORD UNIVERSITY LAB

Time Is (Loss Of) Money





Brazil lowest cost at $1.22m USD | USA highest cost at $10.22m USD

IBM Security, *"Cost of a Data Breach Report"*, 2025

Protecting Your Assets

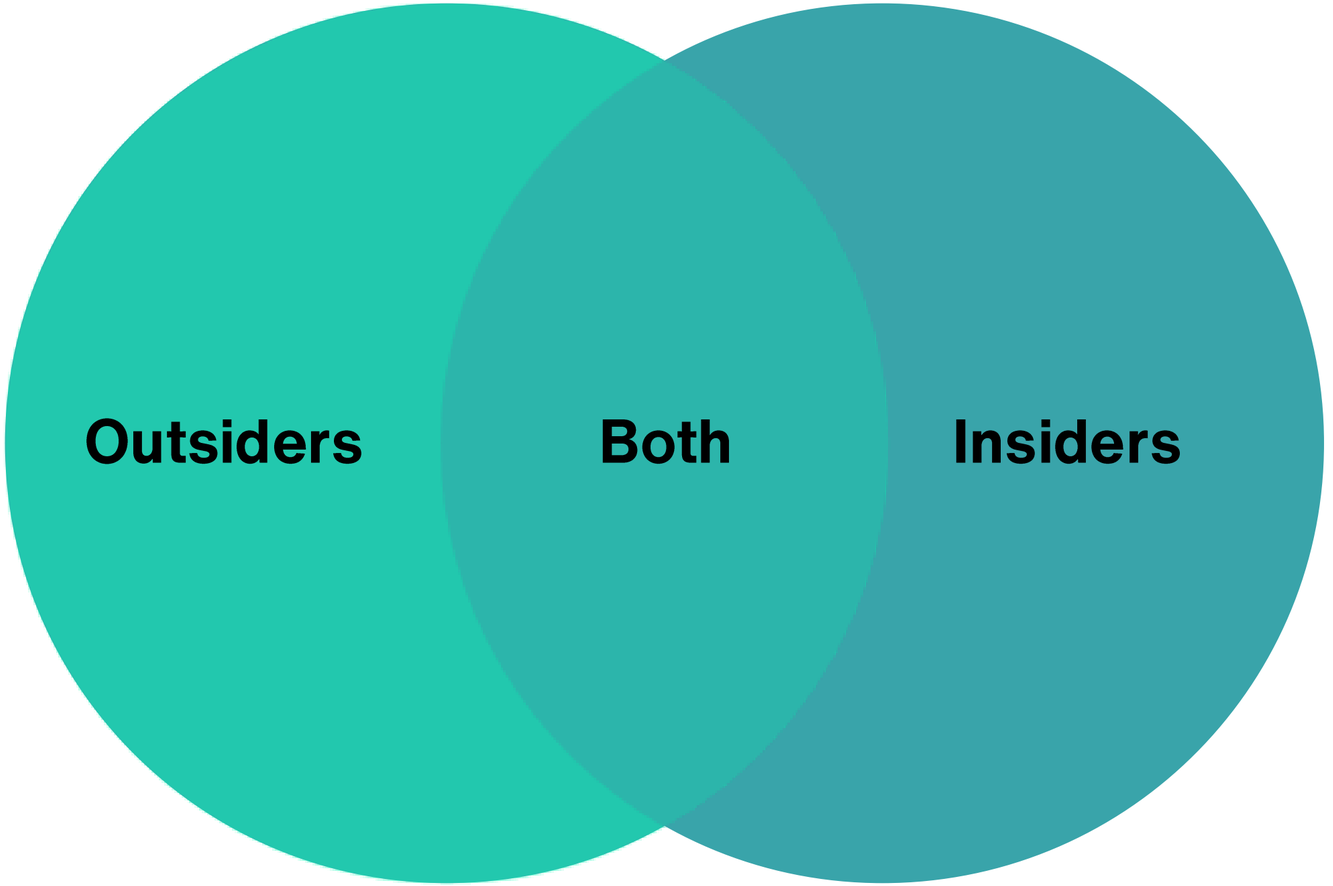
- Biological samples and agents
- Biological and chemical reagents
- Genetic sequences
- Bioinformatics pipelines
- Laboratory equipment

- Knowledge and procedures
- Research data
- Clinical trials data
- Intellectual property
- Trade secrets

- Client information
- CRM data
- Ordering information
- Credit card data

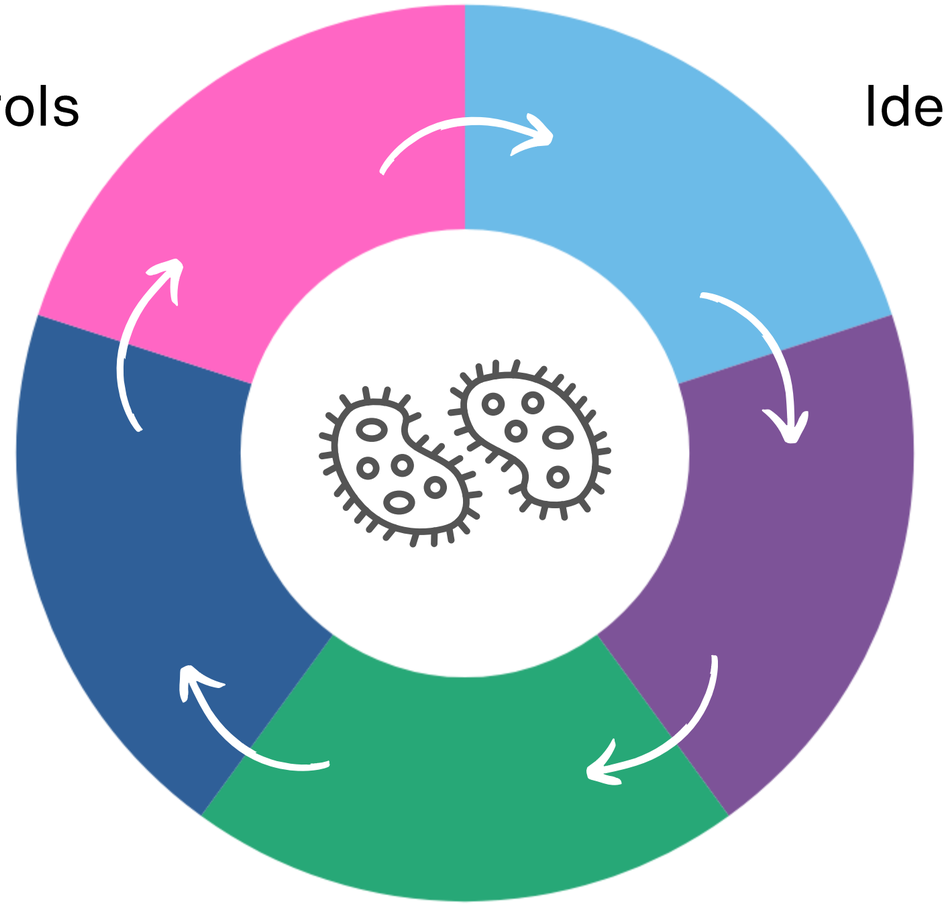
Cyberthreat Sources

- Hostile cyber or physical attacks
- Human errors (intentional or unintentional)
- Structural failures (hardware, software, environmental controls)
- Natural and man-made disasters, accidents, failures



NIST Special Publication 800-30 Rev 1

Biorisk Assessment Cycle



IT Systems Risk Assessment Cycle

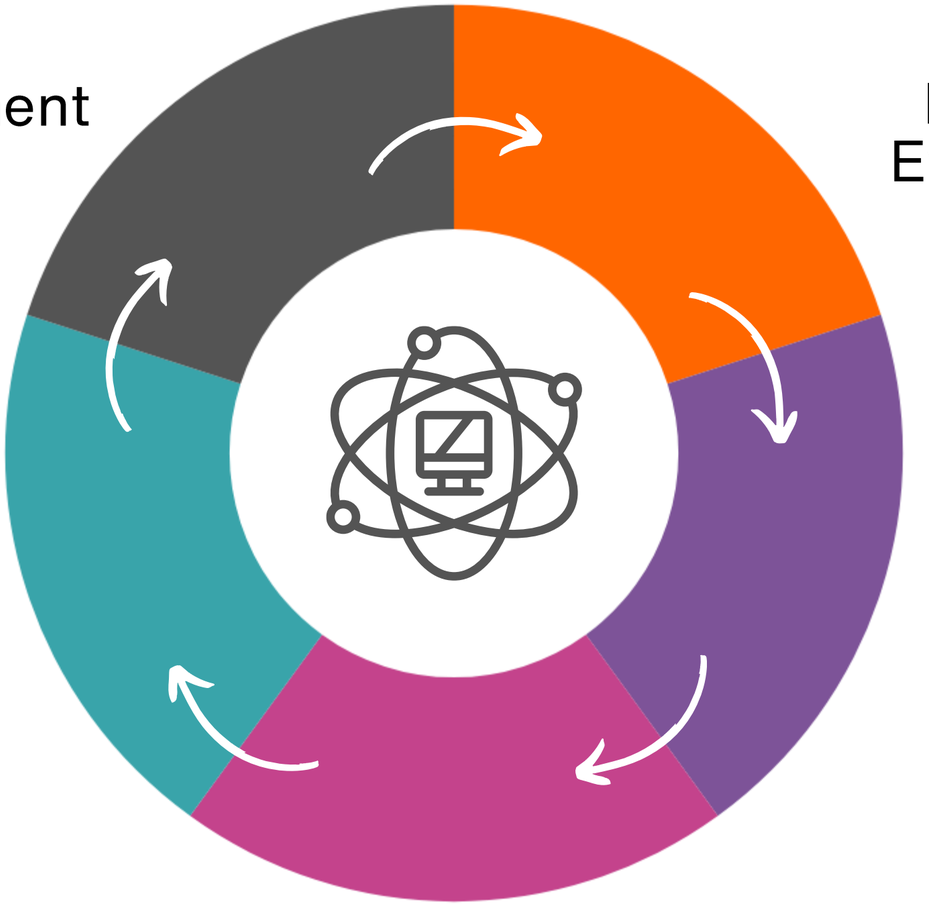
Identify Threat Sources, Events, and Vulnerabilities

Determine Likelihood, Impact, and Risk

Communicate Risk Assessment Results

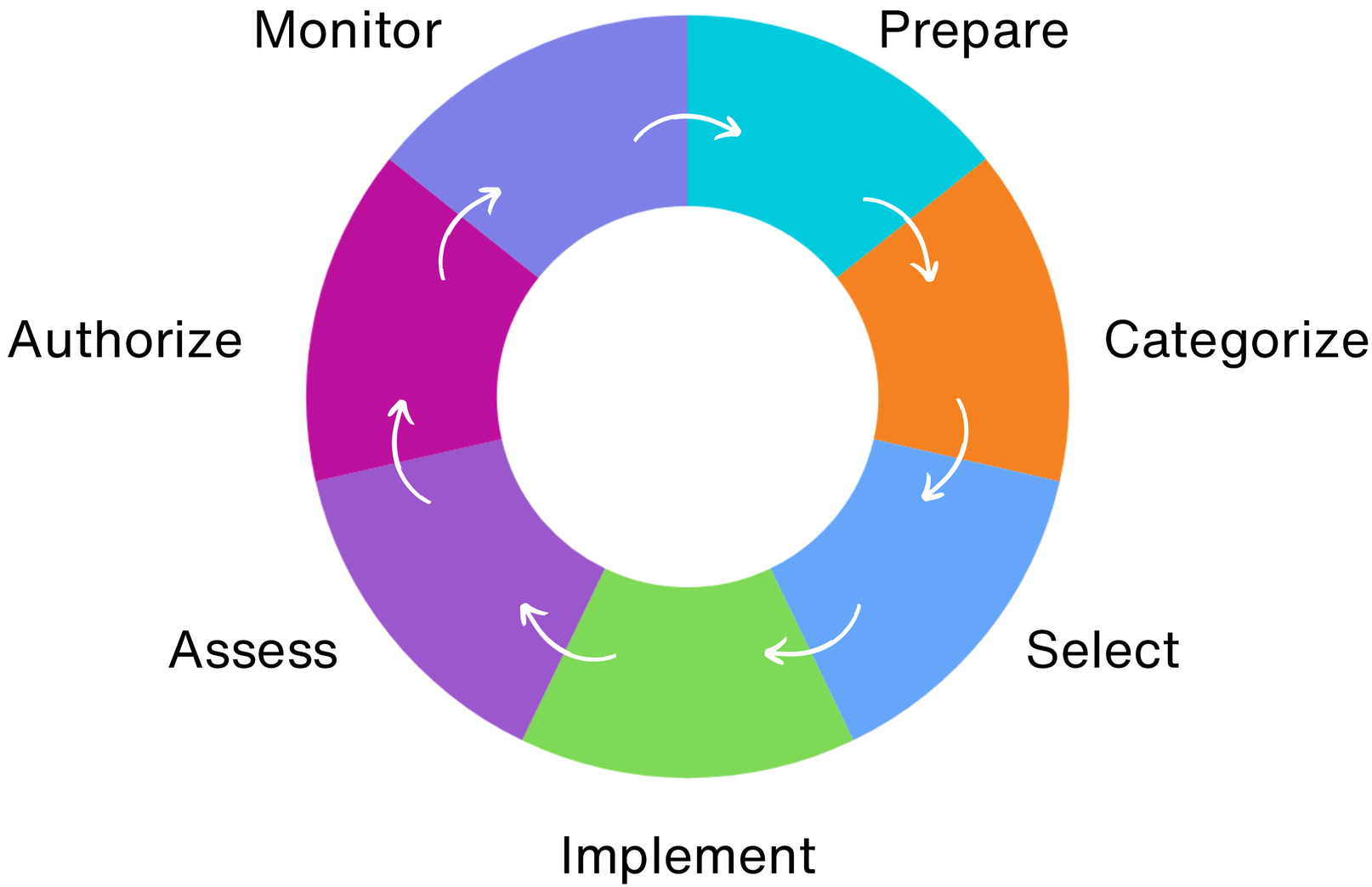
Monitor Risk Factors

Update Risk Assessment



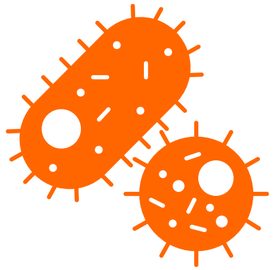
NIST Special Publication 800-30 Rev 1

NIST Risk Management Framework



NIST Risk Management Framework

Evaluating Biological Hazards



Agent Hazards

- Routes of transmission
- Pathogenicity
- Communicability
- Genetic modification
- Resistance to treatment
- Environmental stability
- Exotic vs. endemic
- Regulatory requirements

Agent Handling

- Aerosol generation
- Use of sharps
- Use of animals
- High concentration
- Large volume
- Transporting agents
- Shipping agents
- Use of containment devices
- Appropriate PPE

Personnel

- Education
- Training
- Hands-on experience
- Familiarity with SOPs
- Familiarity with SMP
- Willingness to follow SOPs
- Personal health status
- Stress and workload

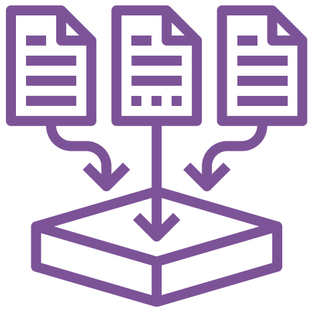
Equipment & Facilities

- HVAC systems
  - Directional airflow
  - HEPA filters
- Maintenance of equipment
- Availability of containment devices (BSC, rotors, etc.)
- Protection of PPE
- Laboratory layout

Evaluating Data & IT Hazards

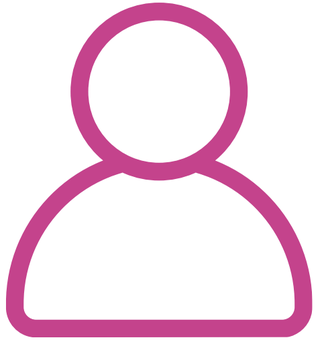
Data Classification

- Is data public or private?
- What type of data is it?
  - Proprietary / IP
  - Confidential
  - PII / PHI / credit card
- Is data encrypted or password protected?
- How valuable is data?



Data Handling

- Who can access?
  - Access controls
- Who should access?
  - Internal use or shared?
  - Who can share and how?
- Where is the data located?
  - Paper, local computer, cloud, server?



Personnel

- Education
- Training
- Hands-on experience
- Familiarity with data security practices
- Willingness to follow data security practices
- Stress and workload

Equipment & Facilities

- Firewall / VPN
- Internal (private) cloud
- External cloud (MS, AWS)
  - Public, private, hybrid?
- Multi-factor authentication / tokens
- Patching and updates
- Longevity of systems
- File storage structure

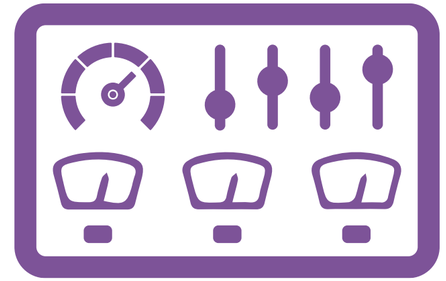
Cyberbiosecurity-Related Controls

Where can / do we incorporate cyberbiosecurity into our engineering controls?

Physical Access Control

- Badge / card readers
- Biometric devices
- PINs
- Electronic freezer locks
- Tokens / PIV cards
- Intrusion detection systems

Industrial Control Systems



- **ICS:** Systems that monitor and control industrial processes and infrastructure (including HVAC, water, wastewater access control, cameras, power, etc.)
- Building Automation Systems (BAS) or Building Management Systems (BMS) are a type of ICS

Cyberbiosecurity-Related Controls

Where can / do we incorporate cyberbiosecurity into our administrative or work practice controls?

Awareness Training

- Inform lab staff about the value of their research assets and potential insider threats to not only specimen but data
- Incorporate common lab-related phishing scams into training
- Stress the need for staff to identify and report IoT and other connected devices

Data Access Control

- Configure systems and physical spaces with least privilege access
- Restrict use of personal devices (phone, laptop) to access lab data
- Protect systems and devices with credentials that include multi-factor authentication

Incident Response

- Discuss potential physical security and cybersecurity incidents (loss of credentials / passwords, data breach, security alarms, etc.) and incorporate into incident response procedures
- Conduct annual drills that include cyber- incidents

Conclusions: A Call For Collaboration

Labs Can Be Vulnerable

Laboratories and other types of research and medical environments can be vulnerable to cyber threats

Lab Assets Are Valuable

These environments contain both biological materials **and** data / records that are valuable to cyber criminals

Terminology Differs

IT and biorisk management professionals may describe hazards and the risk assessment process differently

Collaboration Is Needed

Understanding existing cyber-related risk mitigation controls that are already used is a great place to start to bridge the communication gap

Questions?

Julianne L. Baron, PhD, CPH, RBP (ABSA), CC
Professional Certification in Biorisk Management (IFBA)
Professional Certification in Cyberbiosecurity (IFBA)
Certified in Cybersecurity (ISC2)

Julianne@scienceandsafetyconsulting.com

Science and Safety Consulting