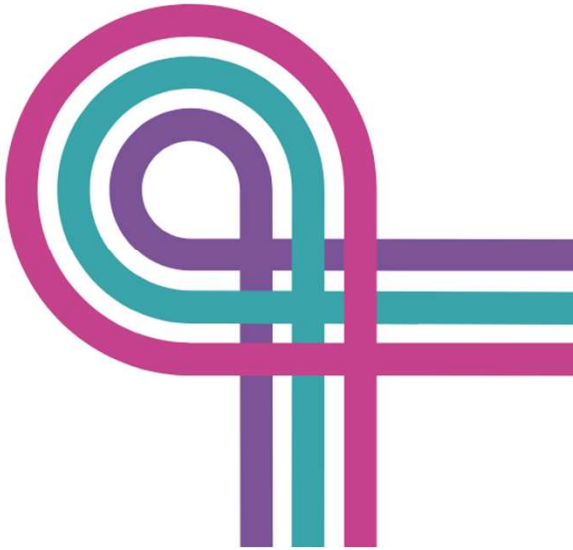
Cyberbiosecurity: A Unique Marriage of Biosecurity and Information Systems

Julianne L. Baron, PhD, CPH, RBP
Professional Certification in Biorisk Management (IFBA)
Professional Certification in Cyberbiosecurity (IFBA)
Certified in Cybersecurity (ISC2)
Justin R. Krehel, MBA

Science and Safety Consulting

Learning Objectives

- Recognize the types of cyberthreats that exist for research and biomedical laboratories
- Identify existing federal guidance documents addressing cybersecurity that can be applied to research and biomedical laboratories
- Explain basic access restriction, vulnerability, and data accessibility cyberbiosecurity needs to organizational IT staff



Research Assets

Research Assets

- What material / information do you think is important to protect within your organization?
- What systems or devices are connected to the network?
  - Are they connected to the public Internet?
- Who might benefit from having access to your materials or data?
  - Both legitimate and illegitimate
- What regulatory requirements apply to controlling access to data and systems? (PHI, PII, FSAP, etc.)

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

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.

Cyberthreats & Risks

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

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

Personal information of thousands of Idaho National Laboratory employees leaked online

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

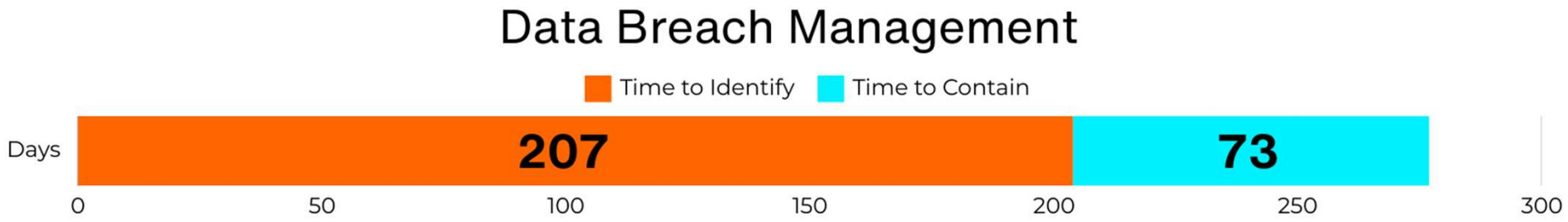
Molecular Pathology Laboratory Network, Inc. Reports Healthcare Data Breach Impacting Patients' PHI

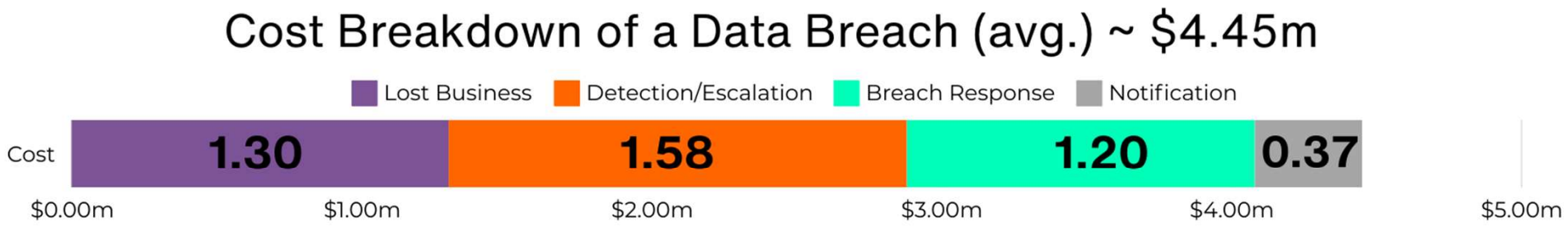
Email Breach at CSI Laboratories Impacts Almost 245,000 Patients

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

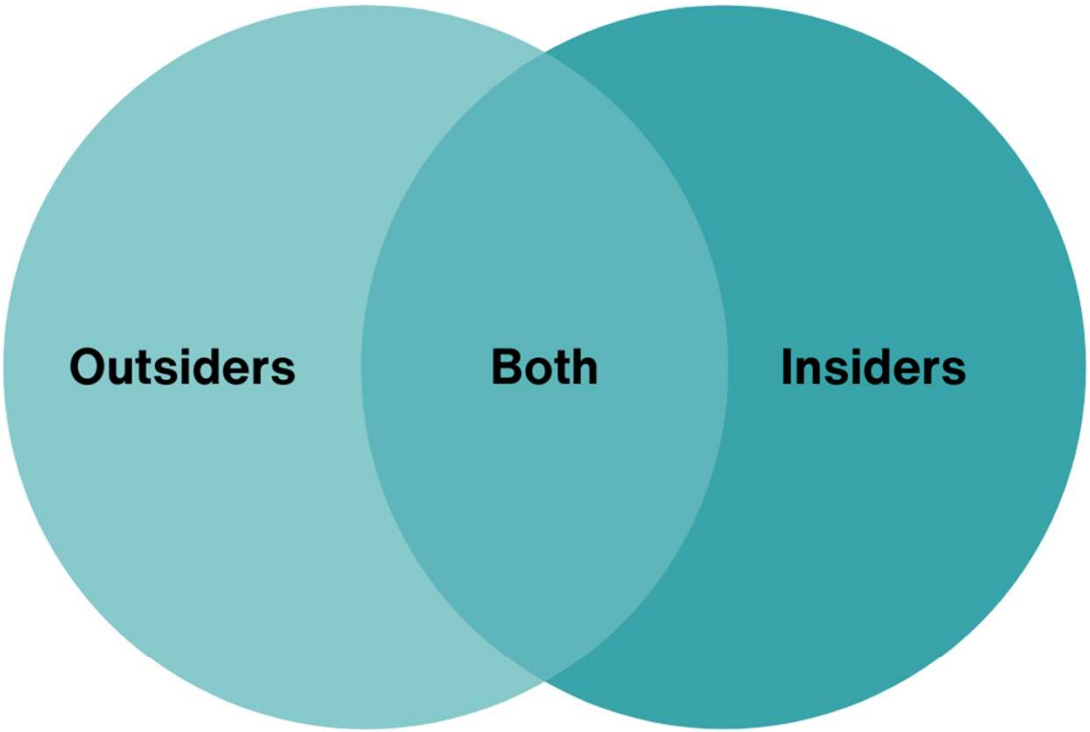




IBM Security, *"Cost of a Data Breach Report"*, 2023

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

Evaluating Data & IT Risks

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

Federal Guidance

Federal Cybersecurity Guidance

- **The NIST Cybersecurity Framework (CSF) 2.0**
- **NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations**
- **Federal Select Agent Program: Information Systems Security Controls Guidance**
- NIST SP 800-30: Guide for Conducting Risk Assessments
- NIST SP 800-37: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-61: Computer Security Incident Handling Guide
- NIST SP 800-66: Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide
- NIST SP 800-82: Guide to Operational Technology (OT) Security
- NIST SP 800-88: Guidelines for Media Sanitization
- NIST SP 800-161: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- NIST IR 8228: Considerations for Managing IoT Cybersecurity and Privacy Risks
- NIST IR 8286A: Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management
- NIST IR 8484: Safeguarding International Science: Research Security Framework
- And many more!

NIST Cybersecurity Framework 2.0

Govern

- Create risk management strategy based on organization
- Identify roles, responsibilities, authorities
- Create policies and implement oversight

Identify

- Identify organizational assets (data, hardware, systems, facilities, personnel)
- Conduct risk assessment
- Identify areas for improvement

Protect

- Use identity management, authentication, access control
- Provide awareness and training
- Protect data in all states and software/hardware
- Protect networks from unauthorized access and threats
- Ensure resilience and availability

Detect

- Continuously monitor systems to identify potential issues
- Investigate anomalies, indicators of compromise, and adverse events

Respond

- Manage identified incidents
- Analyze data about response activities
- report and communicate incidents
- Contain and eradicate incidents

Recover

- Restore systems based on incident recovery plan
- Communicate and coordinate recovery activities

NIST Cybersecurity Framework 2.0: Feb 26 2024

NIST 800-53

Comprehensive document that describes specific security and privacy controls to implement categorized into 20 families by topic.

Access Control

Awareness and Training

Audit and Accountability

Assessment, Authorization, and Monitoring

Configuration Management

Contingency Planning

Identification and Authentication

Incident Response

Maintenance

Media Protection

Physical and Environmental Protection

Planning

Program Management

Personnel Security

PII Processing and Transparency

Risk Assessment

System and Services Acquisition

System and Communications Protection

System and Information Integrity

Supply Chain Risk Management

NIST SP 800-53 rev 5: Sept 2020

Federal Select Agent Program

"Information Systems Security Controls Guidance"- provides information for regulated organizations to protect networks, computers, programs, and data from unwanted and deliberate intrusions.

Application Security
Firewalls and antivirus
Patching/backups

Incident Response
Policies to respond to risks and attacks

Awareness and Training
Mitigating insider threats and avoiding compromise

Information Security
Access authentication
Data storage devices

Network Security
Logical and physical separation

Industrial Control Systems
Protect ICS (HVAC, water, etc.) against attacks

Select Agents: Information Systems Security Controls Guidance; March 2017

Common Exposure Points

Cyberthreats & Vulnerabilities

There are many cyberthreats that can impact organizations. We will briefly touch on three and best practices to mitigate these risks.

Phishing

Phishing is an attempt to trick people into sharing sensitive information or personal data via fraudulent emails, text messages, phone calls or web sites

Unauthorized Access

What are some data access principles to prevent unauthorized access, how can access controls minimize risk, and the “CIA” triad of information security

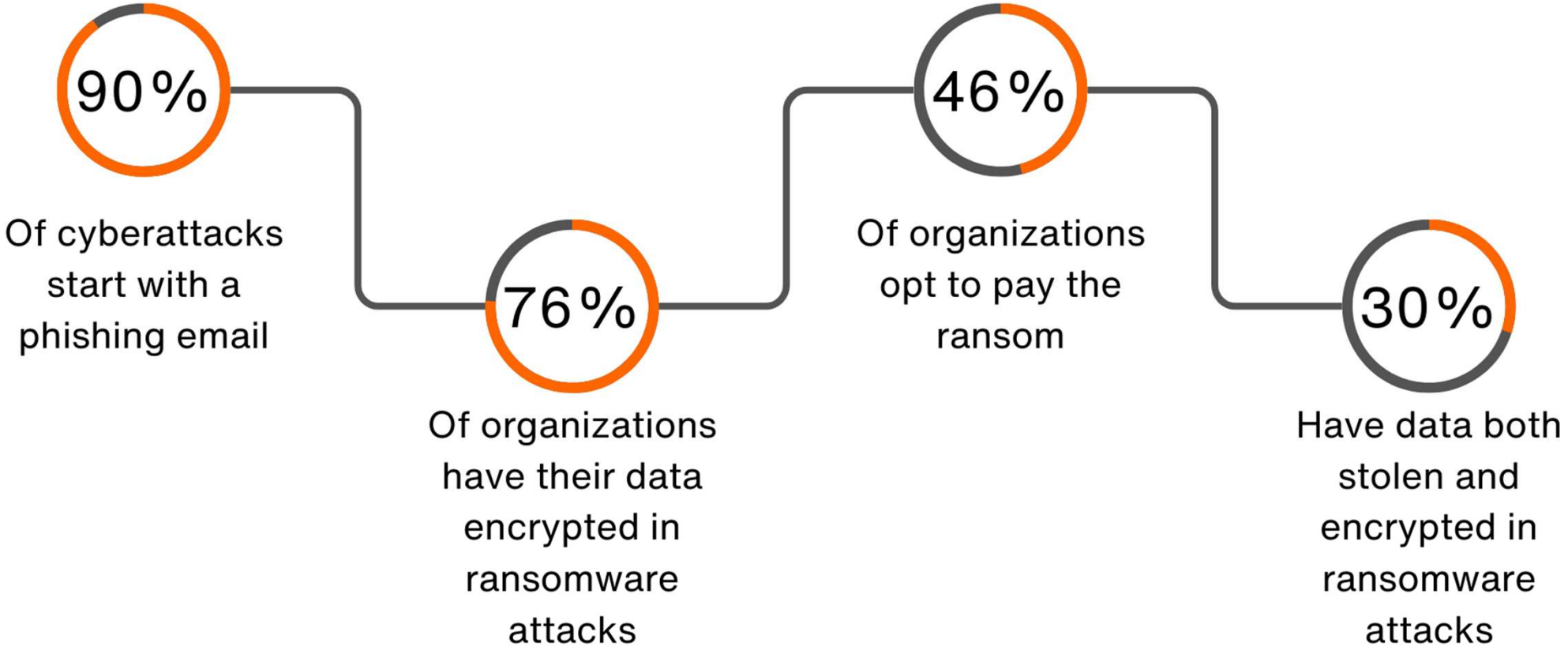
IoT Device Risk

Explore IoT devices and why their proliferation matters to businesses and laboratories, and discuss common device risks, and consider how to help mitigate the risk

Phishing and Ransomware

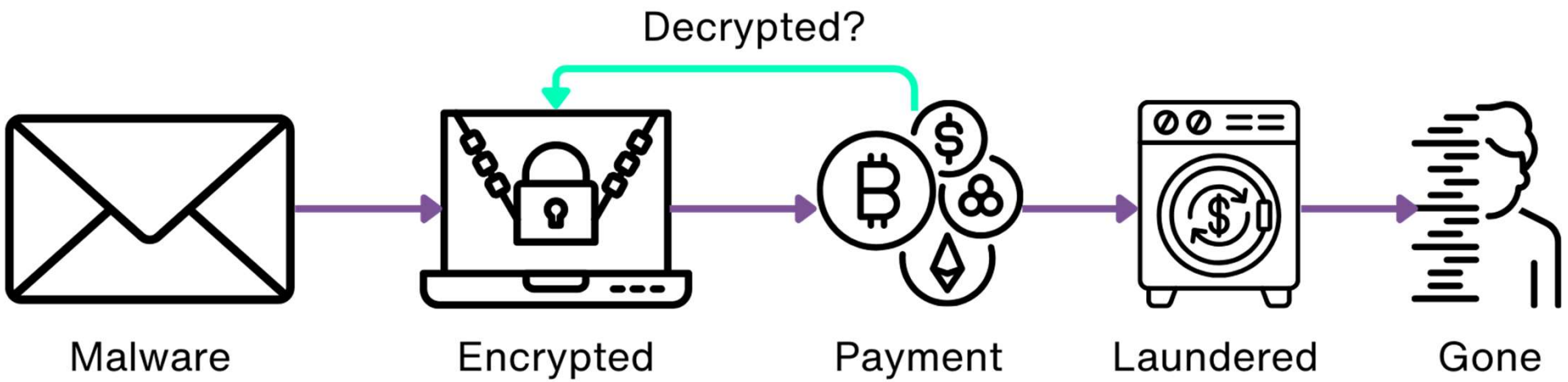
Phishing: Data Dangers

Note - the source report was built on information from 5400 mid-sized businesses sized 100-5000 people across the globe, and gathered via opt-in survey. There are variations in these numbers dependent on respondents and targeted audience.



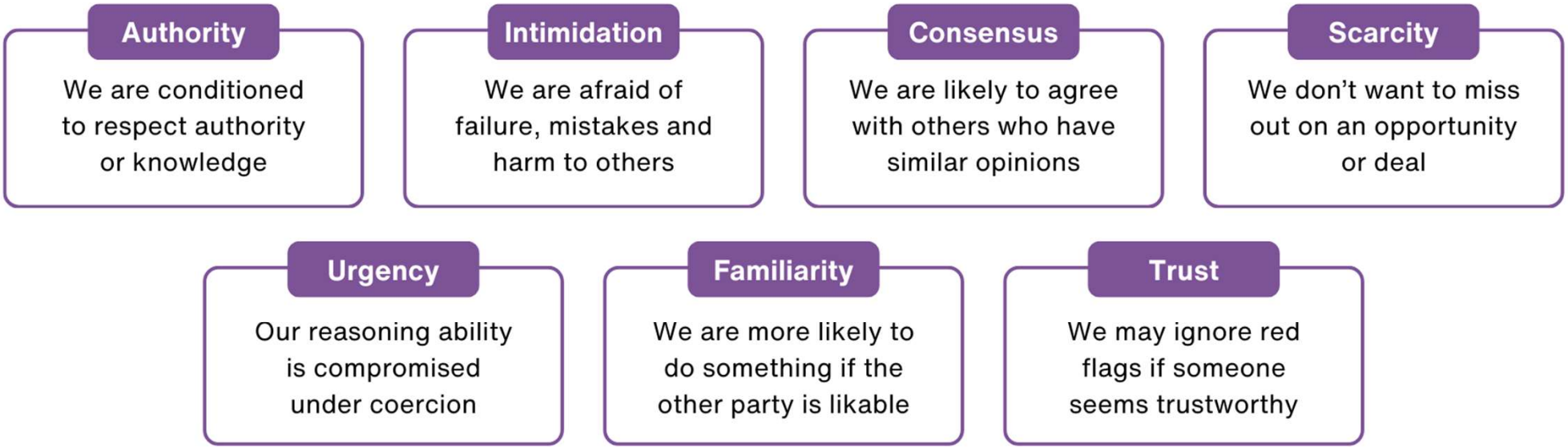
Sophos Ltd. *"The State of Ransomware 2023"*, 2023
Cisco, *"Cyber Security Threat Trends"*, 2021

Ransomware: A Roadmap

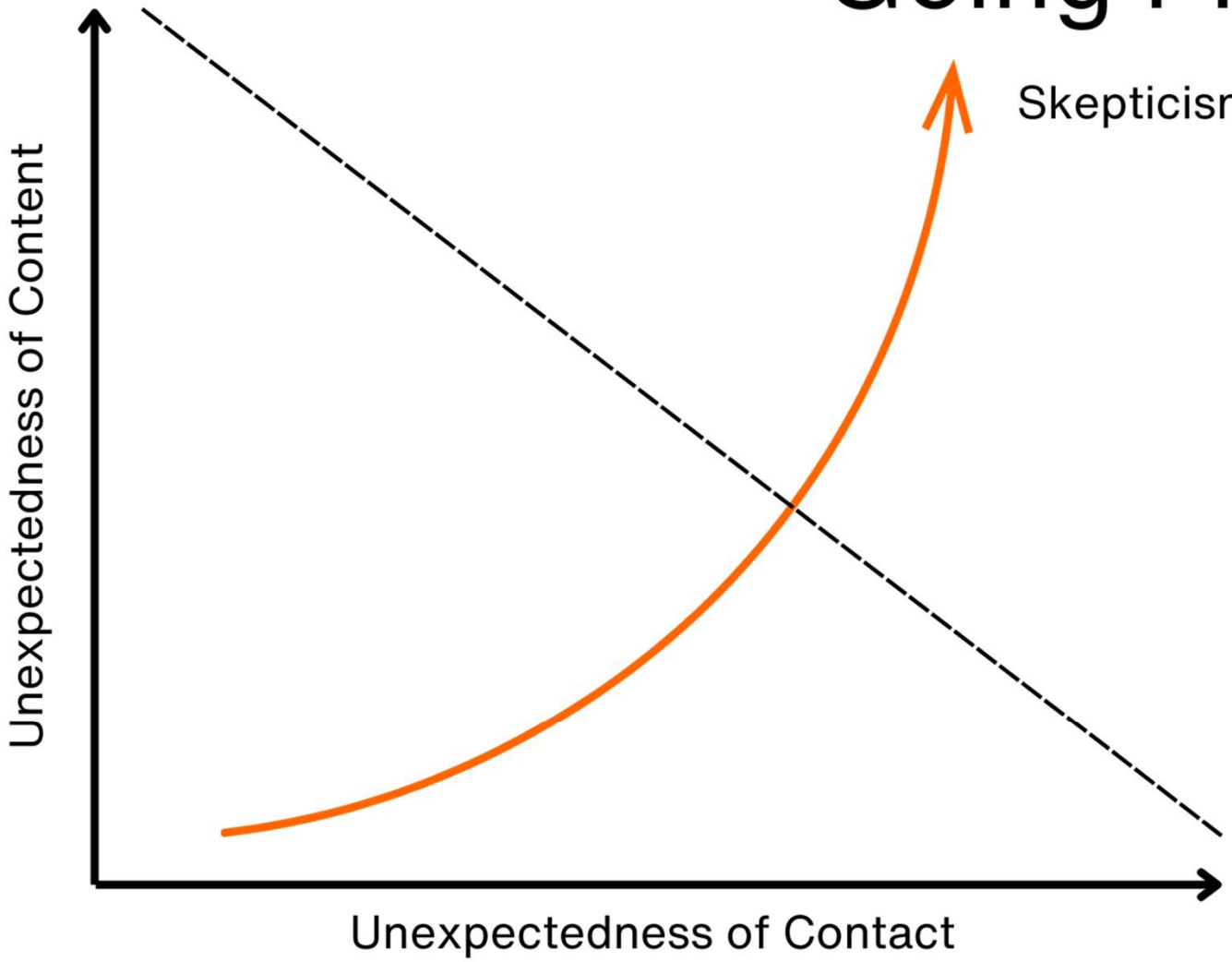


Situational Awareness

Most (phishing, ransomware, scam) threats carry a key set of characteristics in common to lead someone to act against their best interests



Going Phishing



Access Control

The Three Data Principles

We need to know the data we are working with to be reliable, good data that has not been unknowingly interacted with.

Confidentiality

How can it be assured this data has not been viewed or intercepted by parties who should not have access?

Integrity

How can it be assured this data hasn't been altered unknowingly from the intended content?

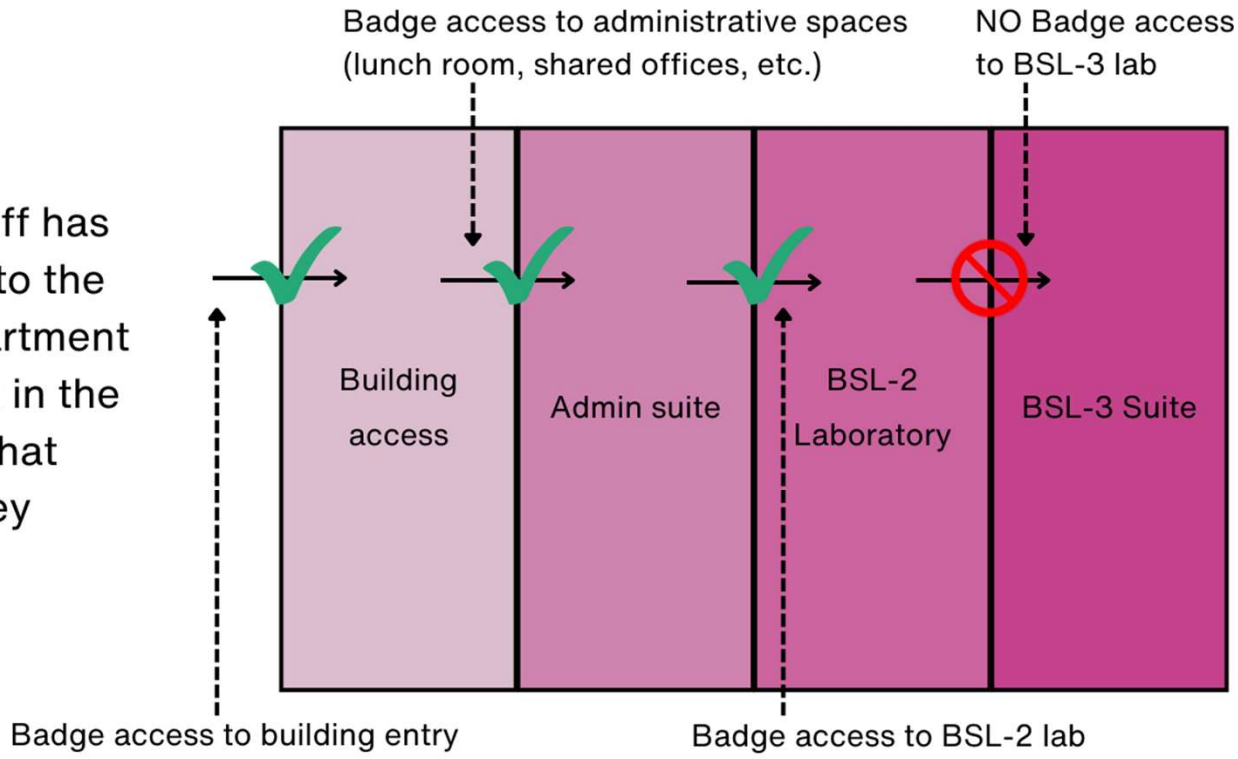
Availability

How can it be assured this is data available for use when it is needed?

Least Privilege Access

Every user of a system, program, or space should operate using the least amount of privilege necessary to complete their job.

A new lab staff has been hired into the virology department who will work in the BSL-2 lab. What access do they need?



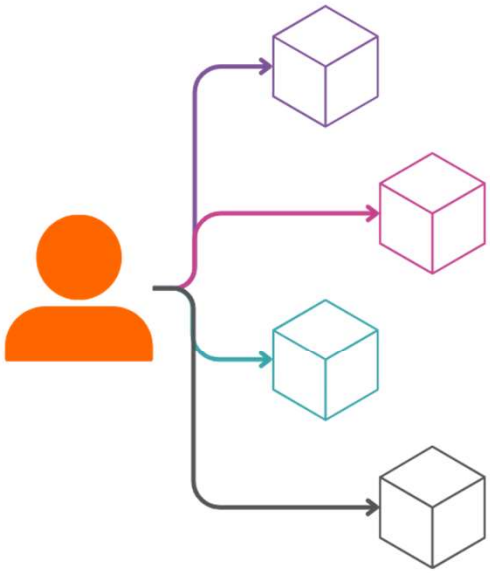
Consider:

- Do they need specific safety training or to be mentored to work in the BSL-2?
- If so, do they really need badge access to the BSL-2 lab at hire?

RBAC - Role Based Access Control

Premise: Don't need it for your role? Don't get access to the information

This is already done at some level without thinking about it



Files necessary to perform role

Collection of shared data which helps perform role

Selected, curated data to fulfill a specific task

Off-limits data

Phrases / Terms

1. Allow list only
2. Deny by default
3. Need to know basis
4. Privileged information

Goal: Limit Unauthorized Access

Network Security & IoT Devices

Network Security and IoT Devices

What is a network? What are Internet of Things (IoT) devices?

Network

At the highest level, a network is a set of computers (or devices) that share resources and allow for file exchange or other network communications over wired or wireless technologies.

IoT Device

These are physical, embedded devices that interact with the real world in some way and are connected to the Internet. They may be remotely controlled through voice, an “app”, or physically manipulated. They do not typically have end-user accessible software.

IoT Examples

Smart speakers, most TV’s, voice assistants, video game consoles, light bulbs, smart plugs, automobiles, microwaves, refrigerators, dishwashers

Heart rate monitors, water sensors, microscopes, blood bank equipment, incubators

IoT Device Impact & Risks

IoT devices often work with the physical world

- These devices can change physical systems, and that impact needs to be considered
- Requirements to use the device may not align with common cybersecurity or your organizations security posture - such as resilience, network communication requirements, safety, or performance

Many IoT devices cannot be monitored or worked with using standard tools

- May require manual intervention on individual devices for firmware updates, configuring connectivity, specialized software, and you may have difficulty addressing risks with manufacturers and third parties, including remote access or addressing vulnerabilities

The safety posture of these devices may be difficult to bring to an organizational standard

- Organizations may need to determine appropriate controls around these devices in a non-standard manner, and determine what must be done if security guidelines cannot be met

NIST IR 8228

IoT Device Risk Mitigation

Ensure device security

- Prevent the device as much as possible from being compromised to in order to conduct attacks against other devices, inspect other network traffic, or being used as a “home base” to compromise other local devices

Ensure data security

- The confidentiality, integrity, and availability of data used by the device in all forms, whether stored, transmitted, or directly collected should be preserved to prevent compromise

Ensure individuals’ privacy

- Maintain individuals’ privacy and PII data production in other ways beyond the device and data security where possible, such as by limiting data or preventing remote transmission

Downside and Impact

- May cause devices to not function as intended, limit usefulness, or prohibit key features due to security and privacy concerns.

NIST IR 8228

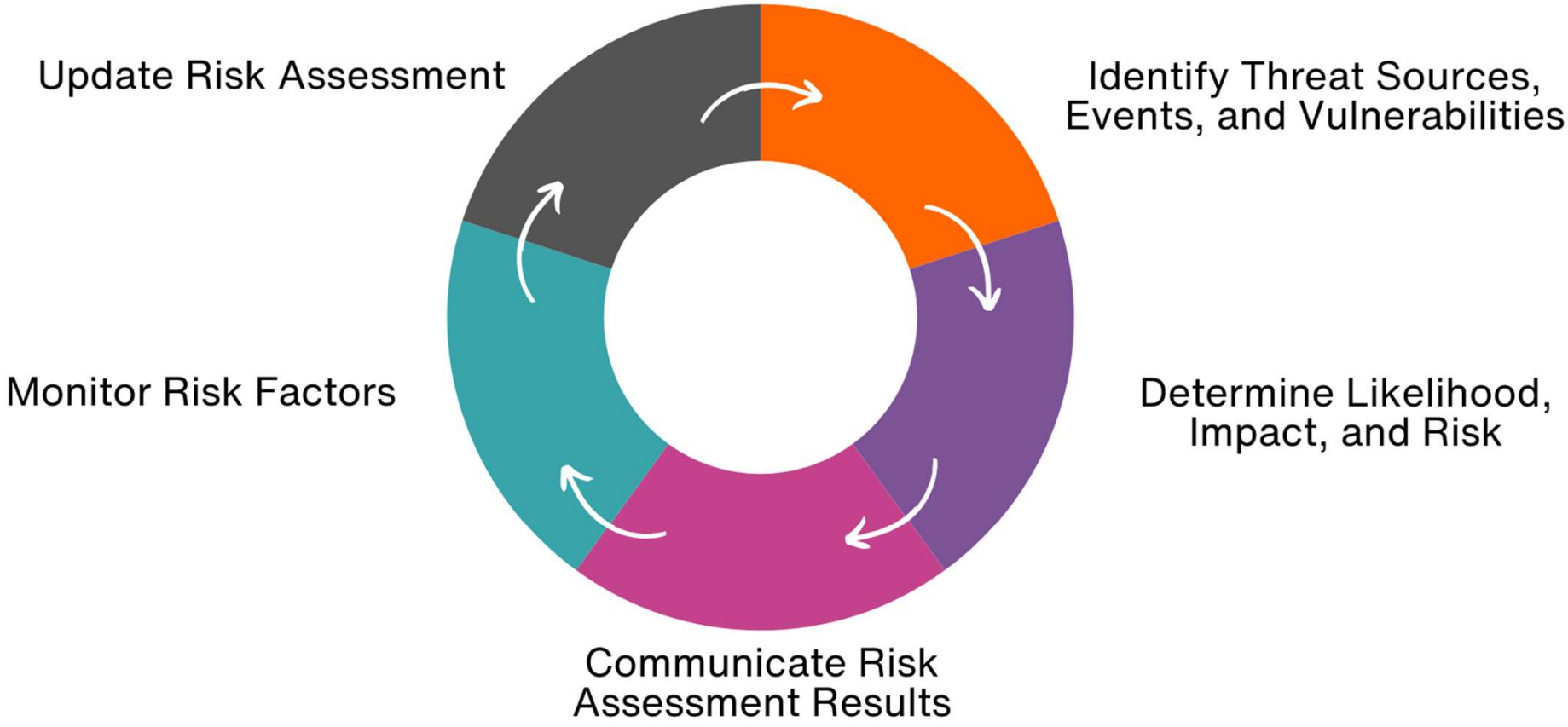
IoT Device - Organizational Policy

	Understand if the device is an IoT device	Can I use a non-IoT device?	Make purchase decisions according to policy. Does your organization have a policy on prohibited or allowed devices? Has a discussion been had on appropriate device use?
	Identify the types of IoT devices	What does each device support?	Do you have an inventory of all devices? What network protocols and ports do the devices use for communication? What vendors, endpoints, or services do they talk to?
	Assess the risk of the device	What is affected by device usage?	Does attaching this device to a particular system cause an outsized risk? Does this device access sensitive data across a network boundary? What if this device fails?
	Determine risk response	How should this risk be managed?	Does this device need to reside on a special network? Is this device acceptable for use? Can policies and firewalls limit the device connectivity? Can the device be hardened?

NIST IR 8228

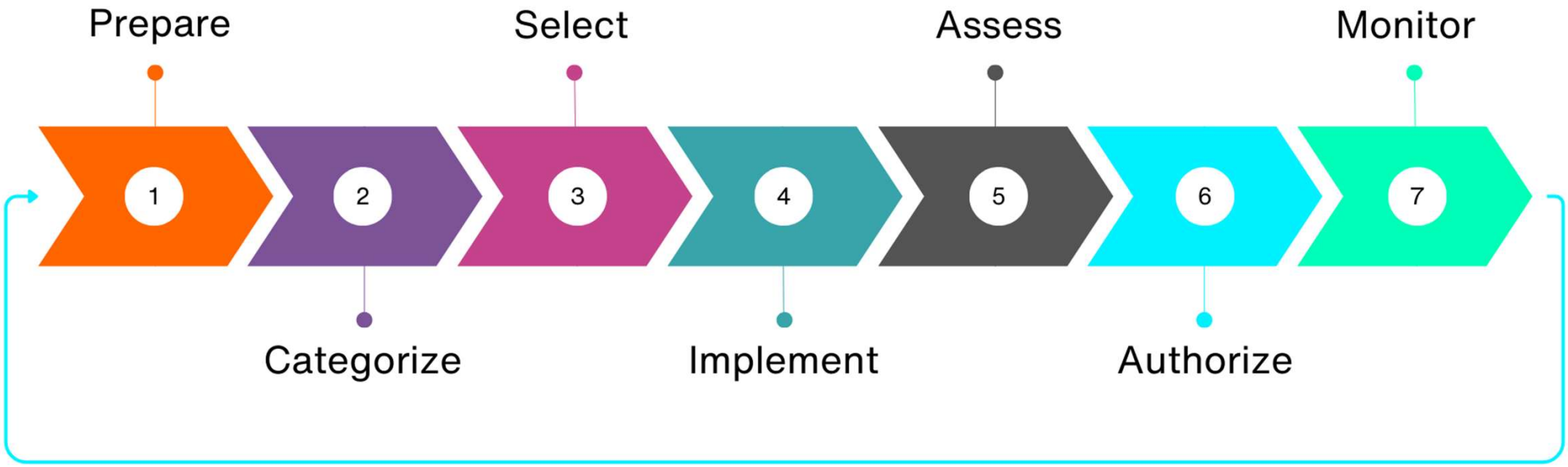
Risk Assessment

IT Systems Risk Assessment Cycle



NIST Special Publication 800-30 Rev 1

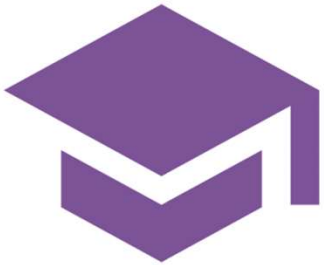
NIST Risk Management Framework



Conclusions

You Are The Weakest Link

Training



Train staff to identify the common signs of threats and how to correctly report them

Access Controls

Limiting access to systems and data can minimize risk of impact and helps control data

Device Security

Understand the full capabilities of devices being purchased and align with organizational policy for maintaining data and device security

Defense In Depth

No individual solution solves all problems. Layered defenses reduce failure risk and create more barriers for exploit