Digital Square on
securing digital health

digital square

# Data Privacy and Security Guidance for digital health decisionmakers

USAID
FROM THE AMERICAN PEOPLE

BILL & MELINDA GATES foundation

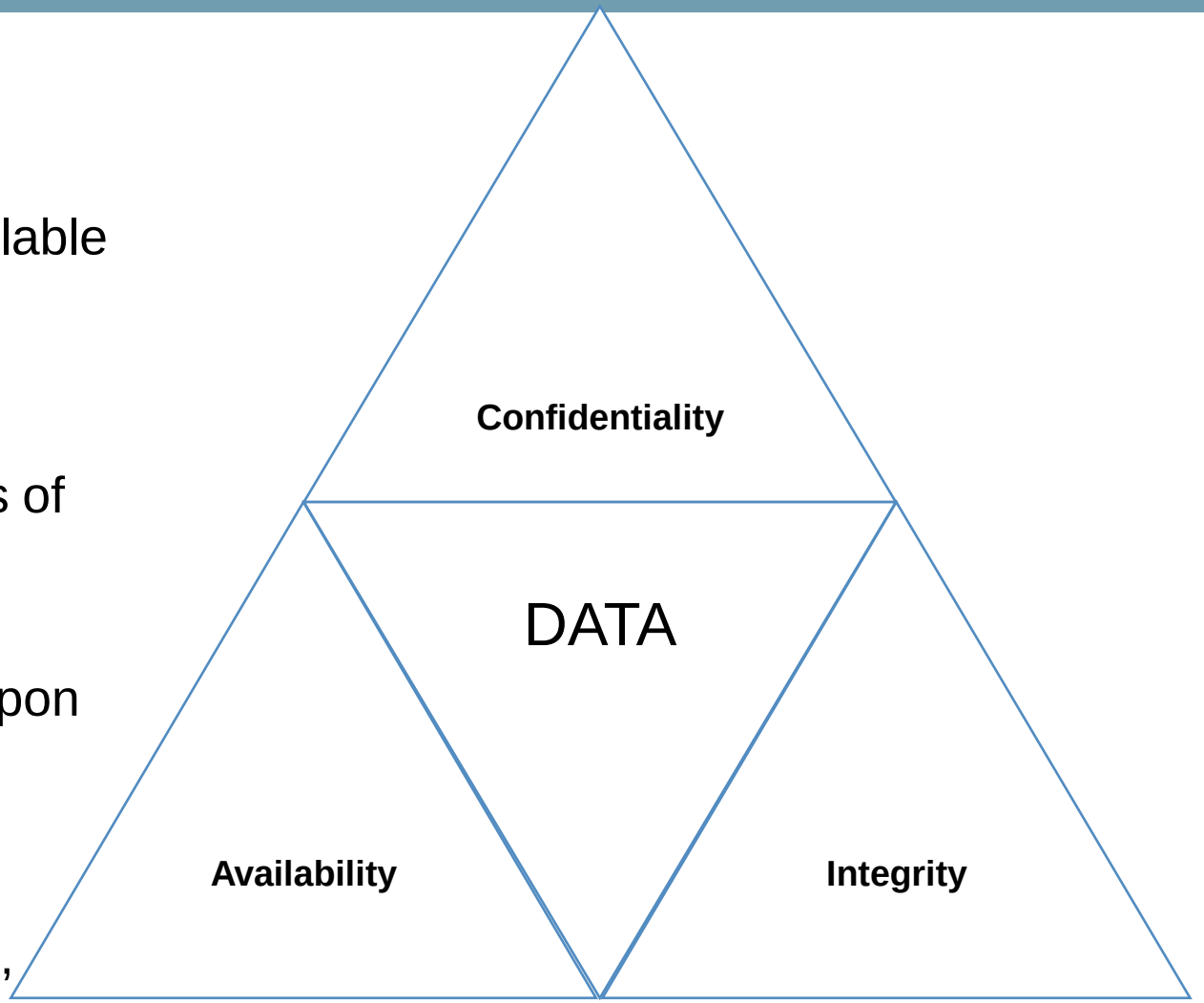
PATH

# Agenda

- Overview of cybersecurity for decisionmakers, risks and consequences
- The true cost of cybersecurity; financial and reputational benefits
- Legal and regulatory landscape of cybersecurity
- Organizational security awareness, training and learning
- Types of cyber stacks, real-life examples and impact
- Best practices and industry standards

# CIA Triad

- Confidentiality
  - Ensuring that information is not made available or disclosed to unauthorised individuals, entities, or processes
- Integrity
  - Protecting the accuracy and completeness of assets
- Availability
  - Property of being accessible and usable upon demand by an authorised entity
- Non-repudiation
  - Subjects cannot deny creating, writing or modifying data, Software, hardware, email, etc.



# Cybersecurity & Data Privacy

Cybersecurity and data privacy are two related but distinct concepts that are essential for protecting sensitive information and ensuring the safety and security of individuals and organizations.

Effective cybersecurity measures are essential for protecting personal information and other sensitive data from cyber attacks and data breaches. Similarly, robust data privacy policies are critical for ensuring that personal information is collected, stored, and used in a secure and responsible manner.

Overall, both cybersecurity and data privacy are essential for protecting sensitive information and ensuring the safety and security of individuals and organizations in today's digital age.

# Privacy and Security in Healthcare

Foundational truths

- Healthcare is highly regulated worldwide as is the protection of personal data
- All stakeholders in health care need to apply a reasonable standard of care and due diligence to safeguard patient information
- We also need to comply with fast evolving regulatory environment
- Privacy and security are important to everyone involved in healthcare

**Privacy:** Involves controlling access to personal information and a control a person can have over information discovery and sharing

**Security:** It is administrative, technical and physical mechanism that protects information from unauthorized access, alteration, and physical mechanism that protects information from unauthorized access, alteration, and loss

**Privacy** is *what* we protect. **Security** is *how* we protect it.

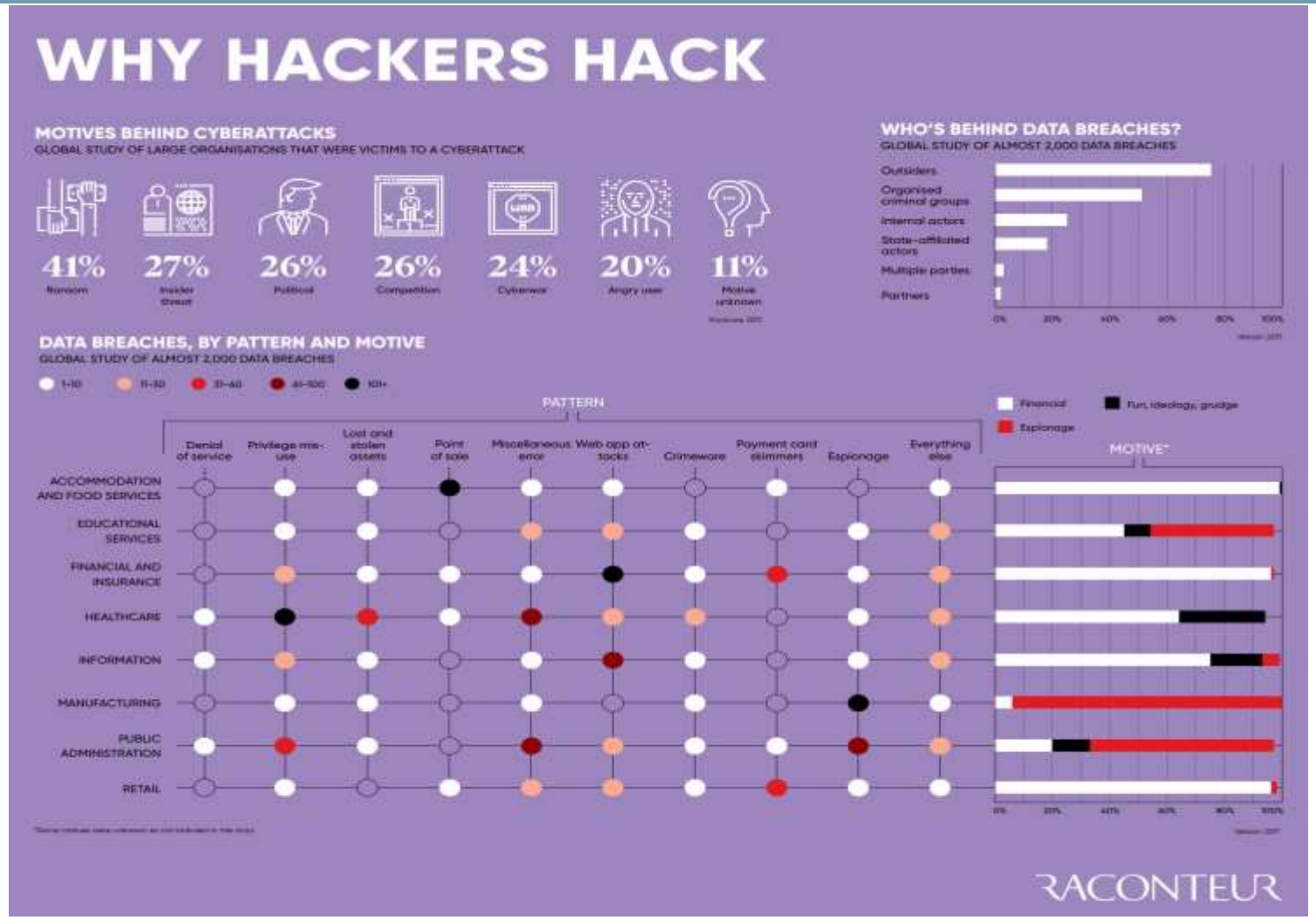
# Complexity of a modern business

- Email
- Mobile devices
- Corporate website
- Social media
- Ecommerce systems
- Online banking
- BYOD and office policy
- Network management
- Backup and remote access

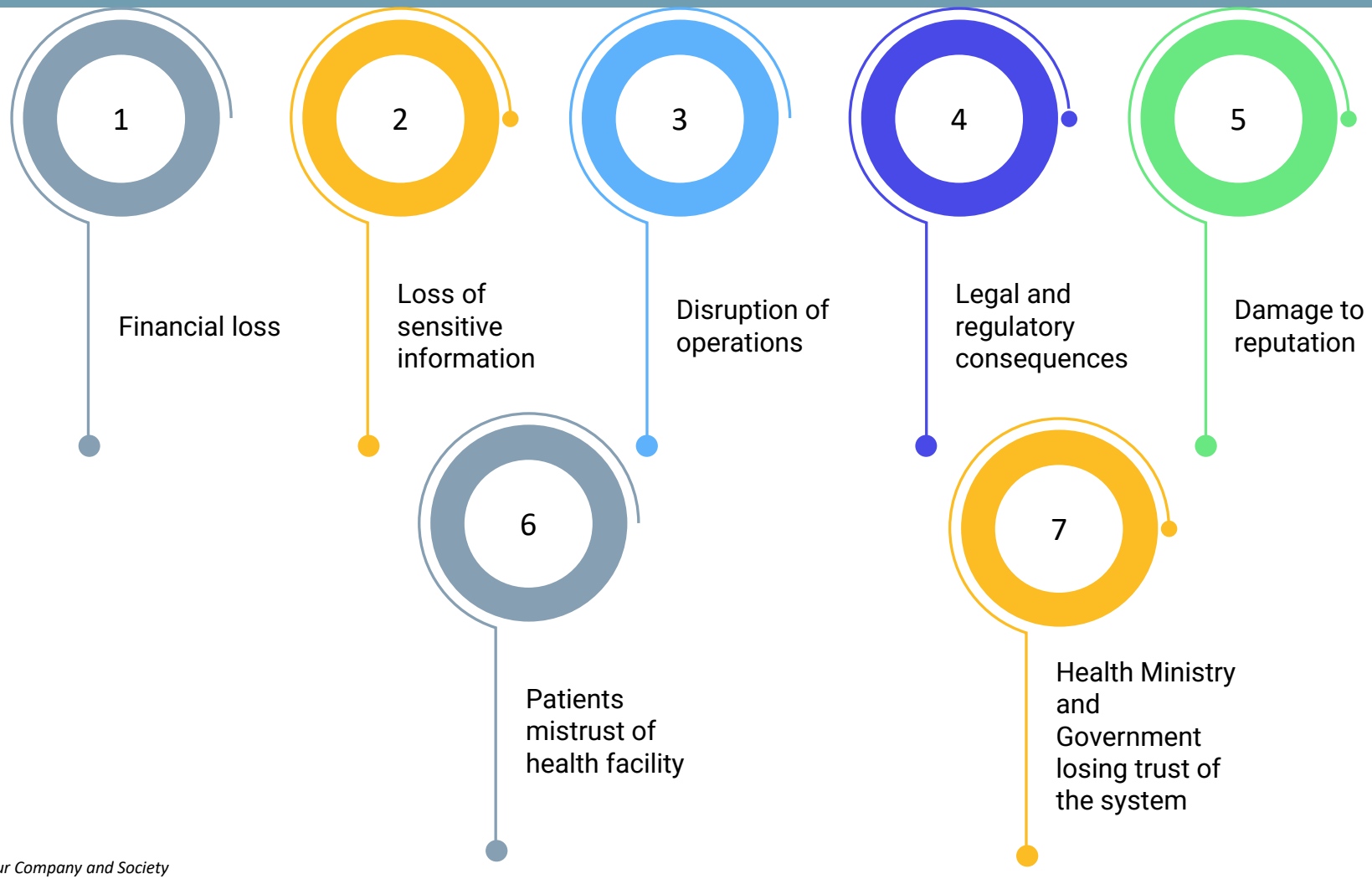
# Cyber Attacks

**Cyber attacks** are malicious attempts to exploit vulnerabilities in a computer system, network, or application to gain unauthorized access, steal data, or cause damage

# WHY THEY HACK



# Consequences of cyber attacks




*2Solving Cyber Risk: Protecting Your Company and Society*
*Andrew Coburn, Eireann Leverett, Gordon Woo · 2018*

# Elements of Risk

What are the **threats**?
What are the **vulnerabilities**?
What is the **likelihood** of a threat exploiting a vulnerability?
What would be the **impact** of this to your business?

# Points to look into

# What are you protecting?

To practice cybersecurity risk management, you can start with these steps:

1. Identify your business' assets
2. Identify the value of these assets
3. Document the impact to your business of loss or damage to the assets
4. Identify likelihood of loss or harm
5. Prioritize your mitigation activities accordingly

# 1. Identify Your Business Assets

List the types of information, processes, important people and technology your business relies upon

- Customer info
- Key employees
- Banking info
- Manufacturing Process
- Proprietary technology

Also consider critical business processes like sales and budgeting.

# 1. Identify Your Business Assets on the Worksheet (cont.)

- In column 1 of the worksheet, list the assets (e.g., information, people, processes, or technology) that are most important to your business
- Add more rows, if needed

| Asset |
| --- |
| Patient health information |
| Devices storing patient information (laptops, server in closet, mobile devices) |
| Processing patient claims to insurance |
| Receiving payments from insurance and patients |
| 3rd party email provider |

# 2. Identify the Value of the Assets

Go through each asset type you identified and ask these questions:

- What would happen to my business if this asset was made public?
- What would happen to my business if this asset was damaged or inaccurate?
- What would happen to my business if I/my customers couldn't access this asset?

# 2. Identify the Asset Values on the Worksheet (cont.)

- Pick an asset value scale that works for you (e.g., low, medium, high or a numerical range like 1-5)

| Asset | Value of the Asset |
|---|---|
| Patient health information | High, due to regulations |
| Devices storing patient information (laptops, server in closet, mobile devices) | Medium |
| Processing patient claims to insurance | High |
| Receiving payments from insurance and patients | High |
| 3rd party email provider | Medium |

# 3. Document the Impact to your Business of Loss/Damage to the Assets

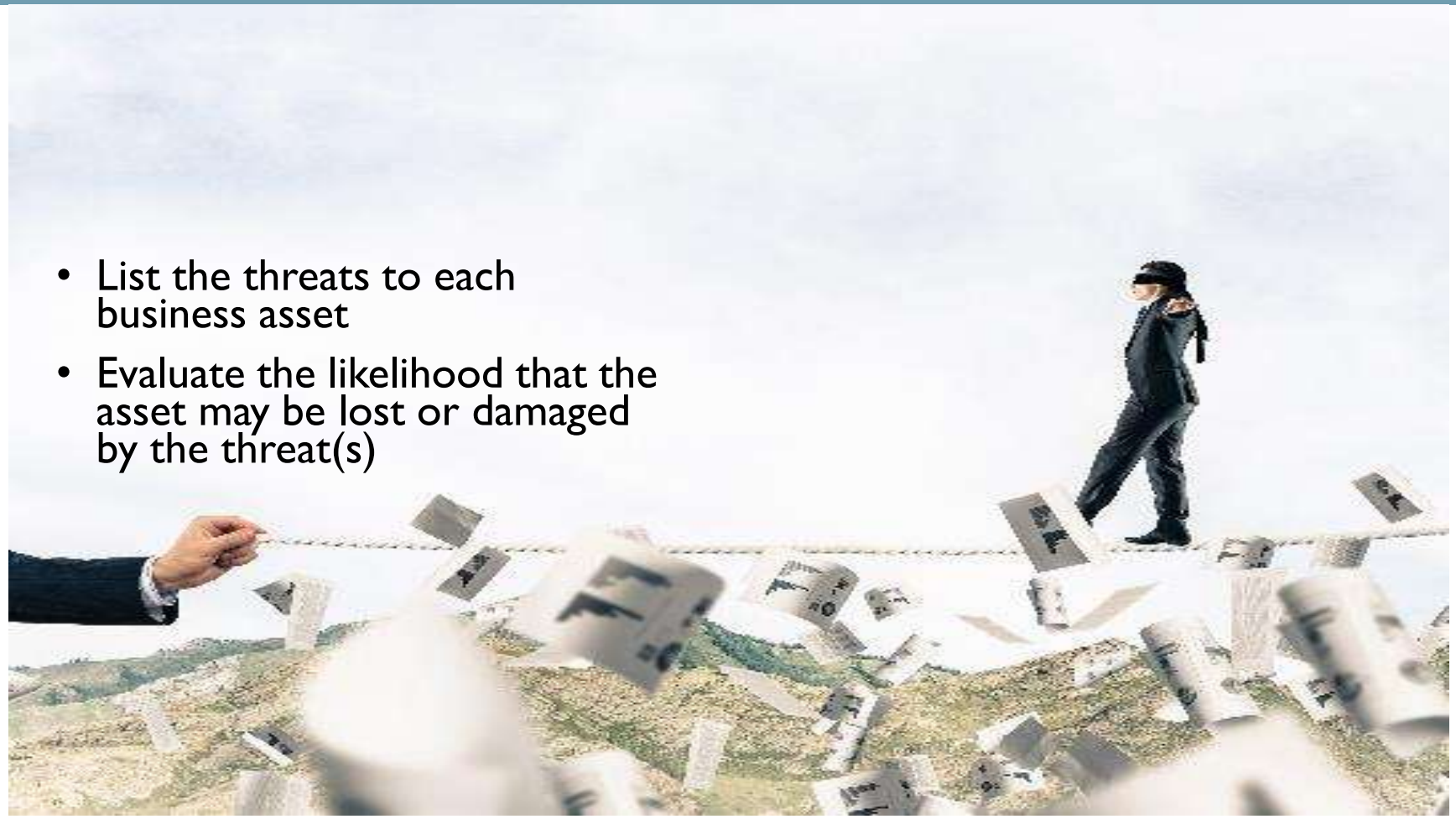
- Consider the impact to your business if each asset were lost, damaged, or reduced in value (e.g., intellectual property revealed to competitors)
- This impact may differ from the asset value determined in step 2.

# 3. Document the Impact to your Business of Loss/Damage to the Assets (cont.)

- Pick an impact value scale that works for you (e.g., low, medium, high)
- Consider if any business processes have manual backup methods

| Asset | Value of the Asset | Impact of Loss/ Damage to the Asset |
|---|---|---|
| Patient health information | High, due to regulations | High |
| Devices storing patient information (laptops, server in closet, mobile devices) | Medium | High |
| Processing patient claims to insurance | High | Medium (can institute manual processes temporarily) |
| Receiving payments from insurance and patients | High | High |
| 3rd party email provider | Medium | Medium |

# 4. Identify likelihood of loss or damage to the asset



# 4. Identify likelihood of loss or damage to the asset (cont.)

| Asset | Value of the Asset | Impact of Loss/ Damage to the Asset | Threats to the Asset | Likelihood of Loss/Damage to the Asset |
|---|---|---|---|---|
| Patient health information | High, due to regulations | High | Hackers, ransomware | Medium |
| Devices storing patient information (laptops, server in closet, mobile devices) | Medium | High | Thieves, malware, phishing | Low |
| Processing patient claims to insurance | High | Medium **(can institute manual processes temporarily)** | Denial of service, hackers | Low |
| Receiving payments from insurance and patients | High | High | Denial of service, hackers | Low |
| 3rd party email provider | Medium | Medium | Phishing, malware | Medium |

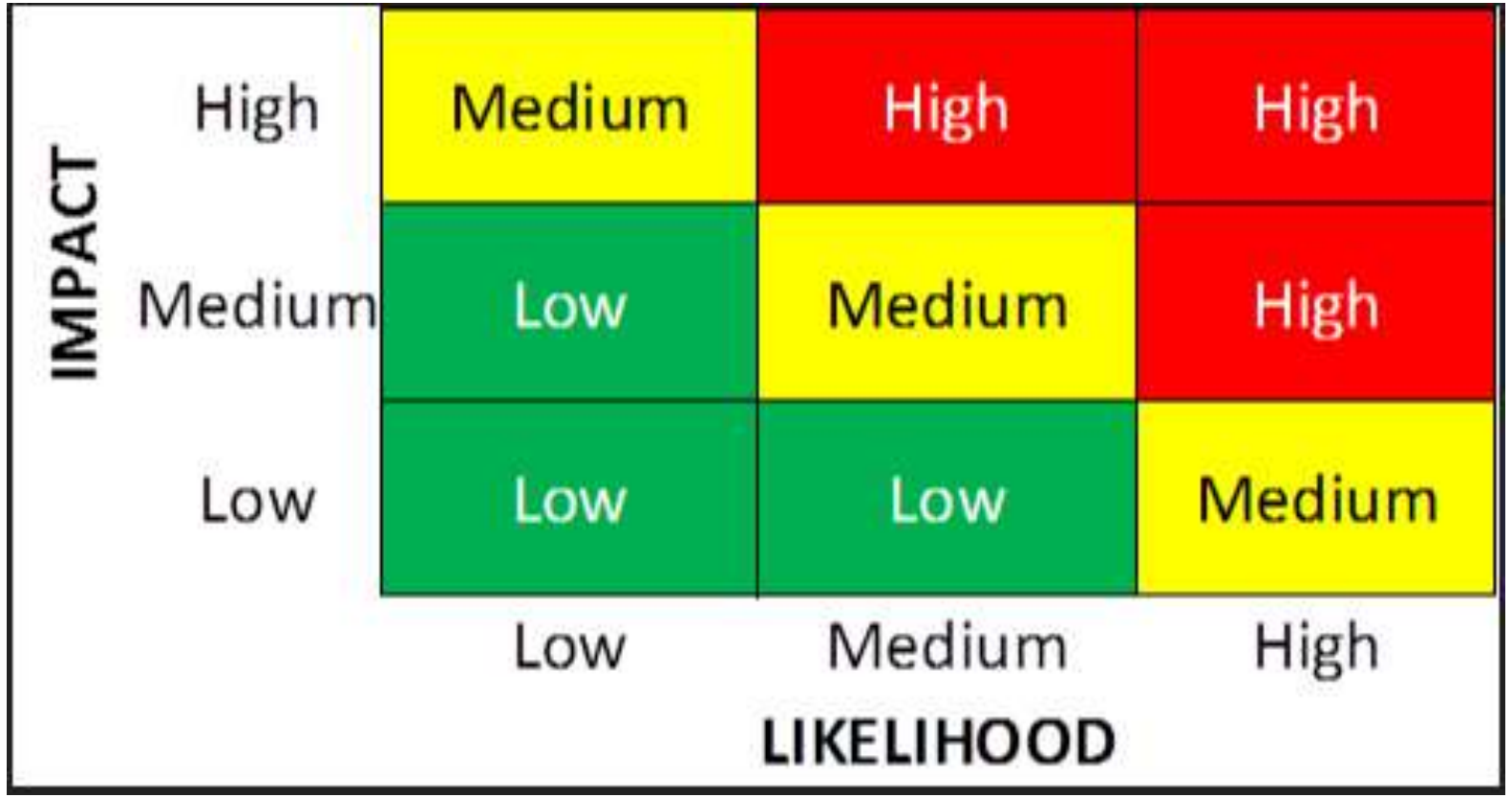
# 5. Identify Priorities and Potential Solutions

- Compare your impact and likelihood scores. Assets with high impact and/or likelihood scores should be assigned top priorities.
- Identify your priorities.
- Identify potential solutions.
- Develop a plan, including funding, to implement the solutions.

**Sample Priority Structure**

**High:** Implement immediate resolution.
**Medium:** Schedule a resolution.
**Low:** Schedule a resolution.

# 5. Prioritize Assets - Risk Matrix



# 5. Prioritize Asset Protection

| Asset | Value of the Asset | Impact of Loss/ Damage to the Asset | Threats to the Asset | Likelihood of Loss/Damage to the Asset | Prioritization of Protection to the Asset |
|---|---|---|---|---|---|
| Patient health information | High, due to regulations | High | Hackers, ransomware | Medium | High |
| Devices storing patient information (laptops, server in closet, mobile devices) | Medium | High | Thieves, malware, phishing | Low | Low |
| Processing patient claims to insurance | High | Medium **(can institute manual processes temporarily)** | Denial of service, hackers | Low | Low |
| Receiving payments from insurance and patients | High | High | Denial of service, hackers | Low | Low |
| 3rd party email provider | Medium | Medium | Phishing, malware | Medium | Medium |

# Regulations And Frameworks

General Data Protection Regulations (GDPR)

Health Insurance Portability and Accountability Act (HIPAA)

Payment Card Industry Data Security Standards (PCI DSS)

The Federal Risk and Authorization Management Program (FedRAMP)

The Cybersecurity Information Sharing Act (CISA)

Data Protection Act (DPA)

California Consumer Privacy Act (CCPA)

International Standard Organization (ISO)

Cybersecurity Maturity Model Certification (CMMC)

Protection of Personal Information Act (POPI Act)

NIST Cybersecurity Framework (CSF)

# Why regulations?

Cybersecurity
Regulation
Functions

# Identify


**Develop organizational understanding** to manage cybersecurity risk to systems, assets, data, and capabilities.

# Protect


**Develop and implement the appropriate safeguards** to ensure delivery of services.

# Detect


Develop and implement the appropriate activities to **identify the occurrence of a cybersecurity event.**

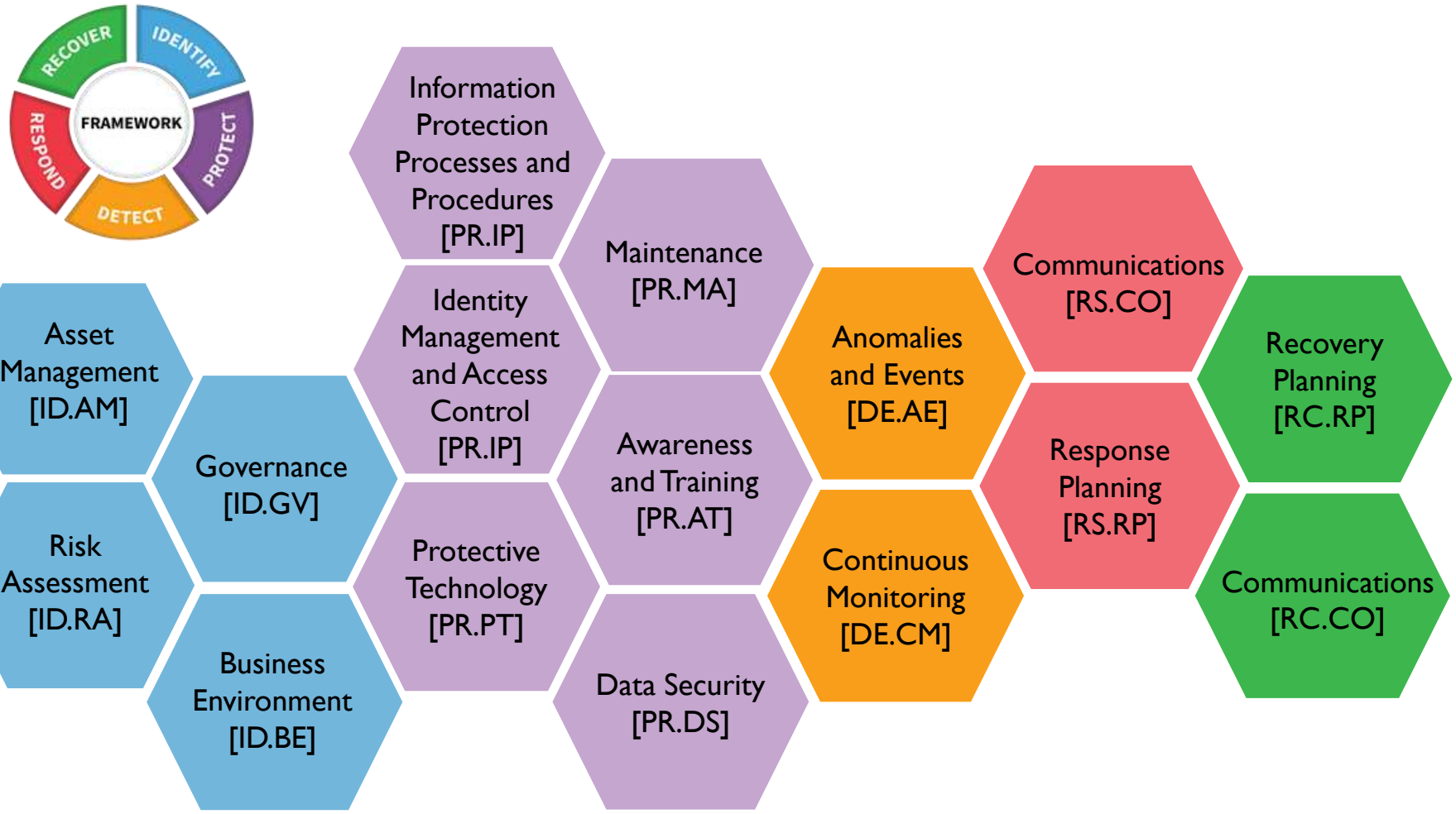
# Respond


Develop and implement the appropriate activities to **take action regarding a detected cybersecurity event.**

# Recover


Develop and implement the appropriate activities to maintain plans for **resilience and to restore any capabilities or services** that were impaired due to a cybersecurity event.

# Follow regulation

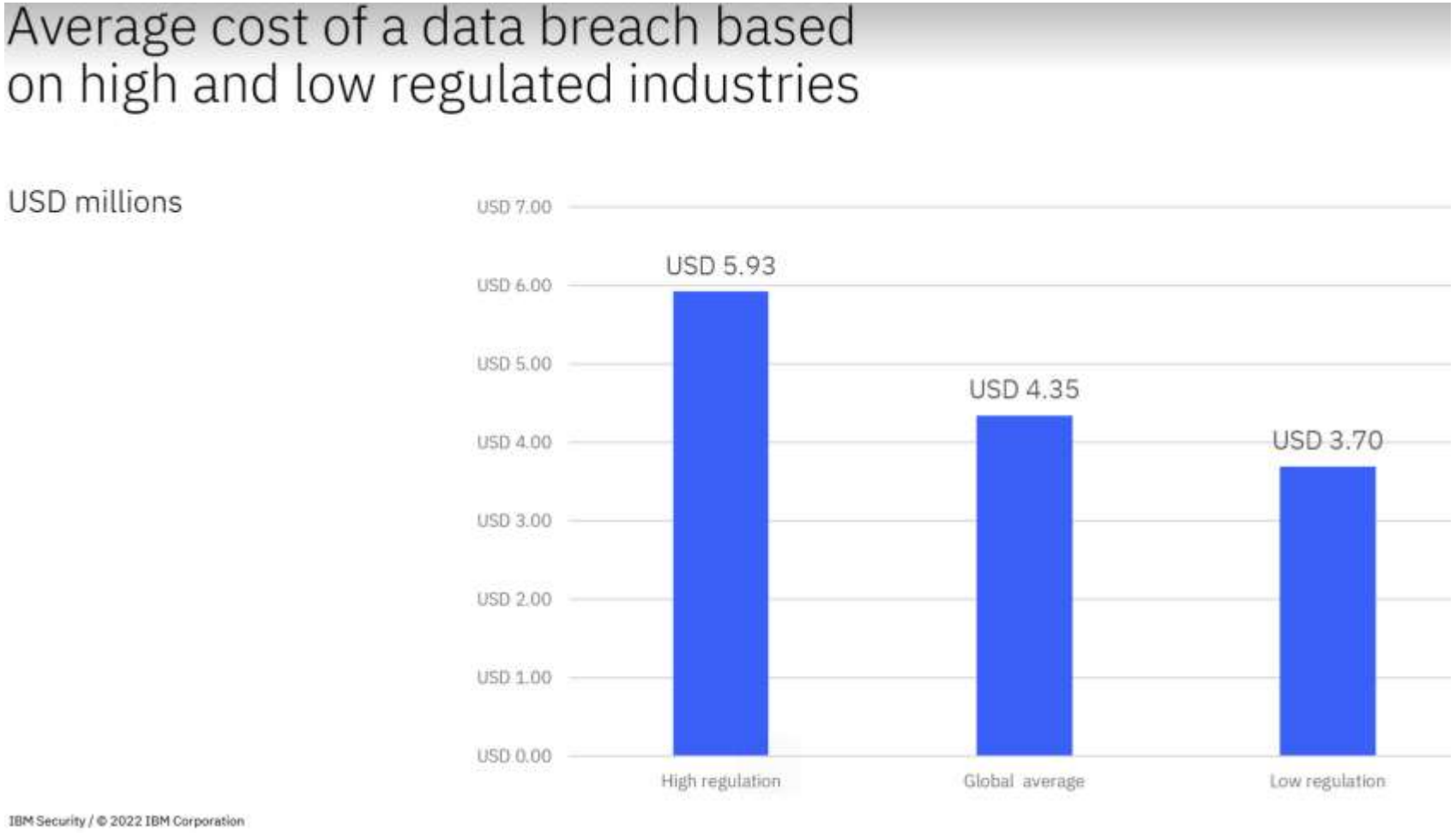


# The healthcare industry is particularly vulnerable to cyber attacks due to the sensitive nature of the information it handles

It is essential for healthcare organizations to be aware of cyber attacks and take steps to prevent them, such as regularly updating software and security systems, providing employee training on cybersecurity best practices, and having a plan in place for responding to cyber attacks if they occur.

cost of a breach in the healthcare **$10.10M**
Average total cost of a breach in the healthcare industry

# Regulated industries also see long tail of costs that accumulate down the line

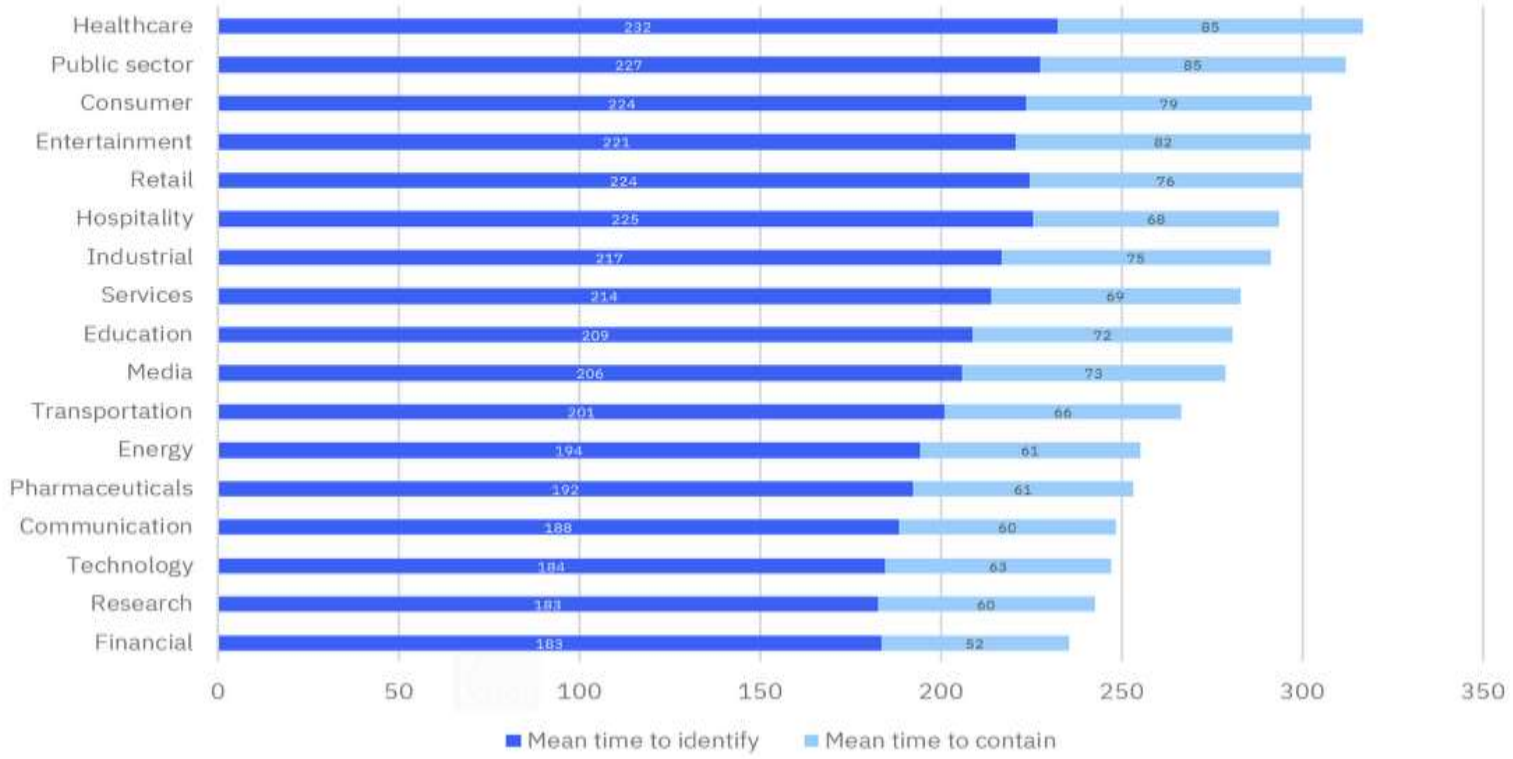


# Common types of cyber attacks in health sector

- Ransomware attacks
- Phishing attacks
- Distributed Denial of Service (DDoS) attacks
- Malware attacks
- Insider threats
- Social engineering attacks

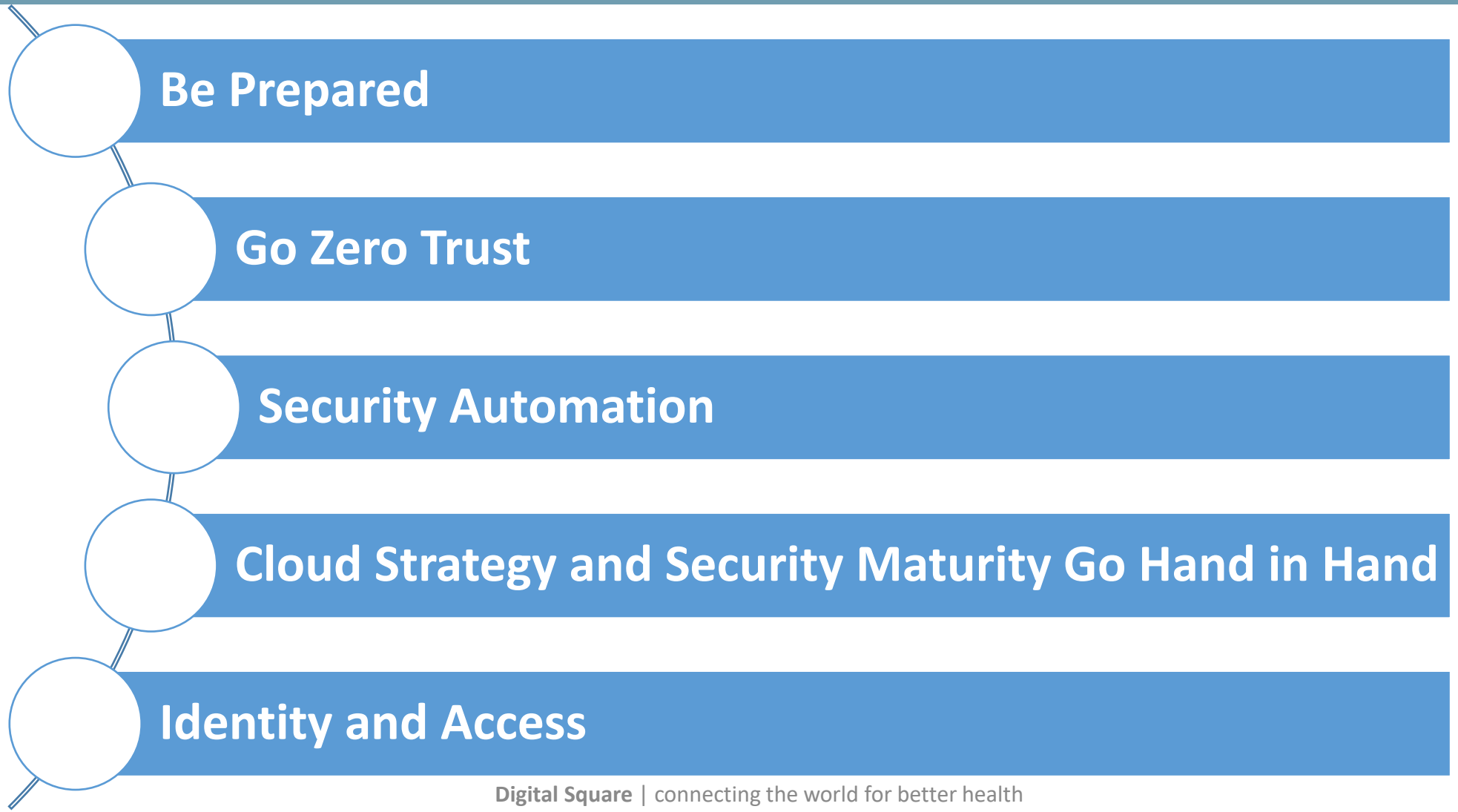
# Days to identify breach

## Average days to identify and contain the data breach by industry




IBM Security / © 2022 IBM Corporation

# Healthy Strategies to Lower Healthcare Breach Costs



# Secure implementation

**Secure implementation** involves the process of ensuring that software and systems are implemented securely to reduce the risk of unauthorized access, data breaches, and cyberattacks

# Security Assessment

digital square

# Security Assessment

**Security assessment** is the process of evaluating the security posture of a system, network, or application to identify potential vulnerabilities and threats:

•Identify assets

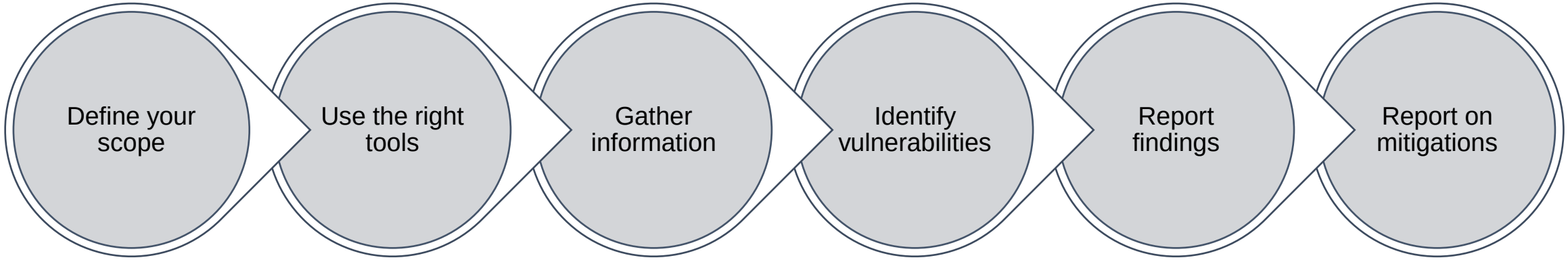
•Threat modeling

•Vulnerability assessment

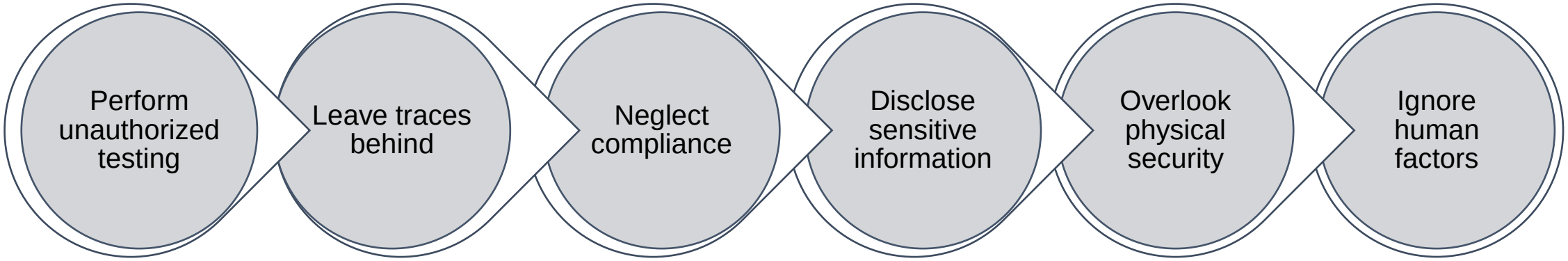
•Penetration testing

•Risk assessment

# How to conduct security assessment



# What to avoid during a security assessment




*Incident Response Planning: Focused Preparation*
*Gabe Smit, Timothy Smit, 2021*

# Managing user privileges

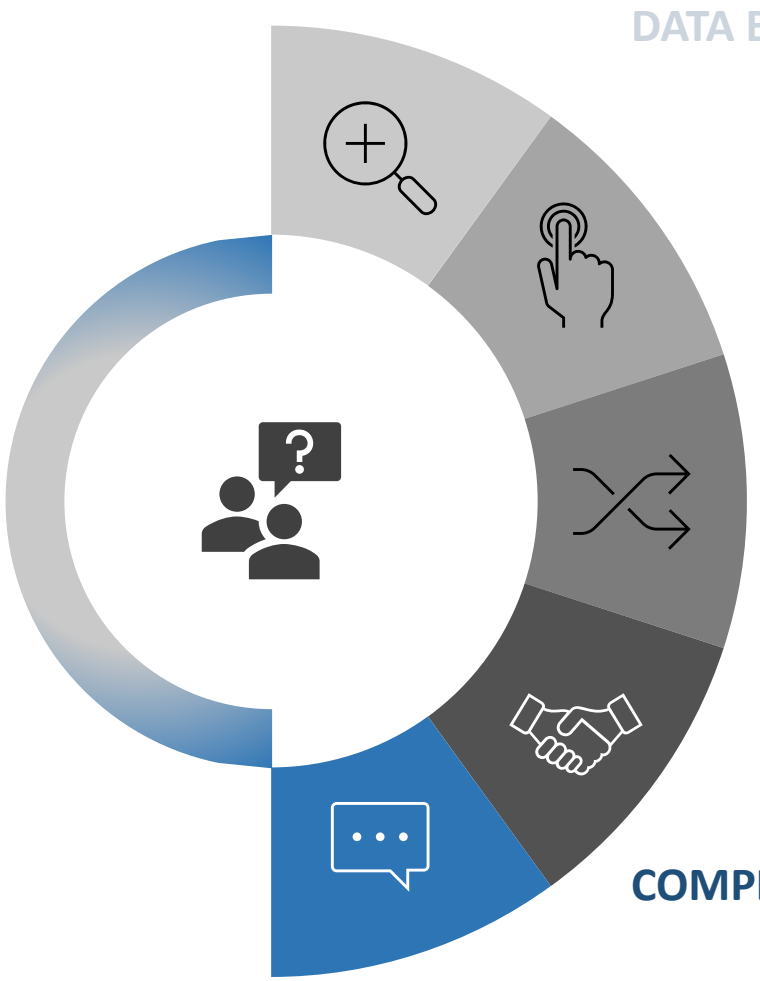
Organisations must create access controls to ensure that employees can only access information that is relevant to their job and based on need to know

# Segregation of duties

a key concept in information security and refers to the practice of dividing responsibilities between different individuals or teams to prevent any one person or group from having too much control or influence over a particular process or system. When it comes to data management, it is important to have a clear segregation of duties between developers and the data management team.

# Third-party security concerns

Third-party security concerns refer to the risks and vulnerabilities associated with the use of external vendors, suppliers, contractors, or other third-party partners who have access to an organization's sensitive data or systems. Third-party security concerns are a major issue for many organizations, as these external partners may not have the same level of security controls and policies in place as the organization itself.



# To address third-party security concerns, organizations should

**CONDUCT THOROUGH RISK ASSESSMENTS**

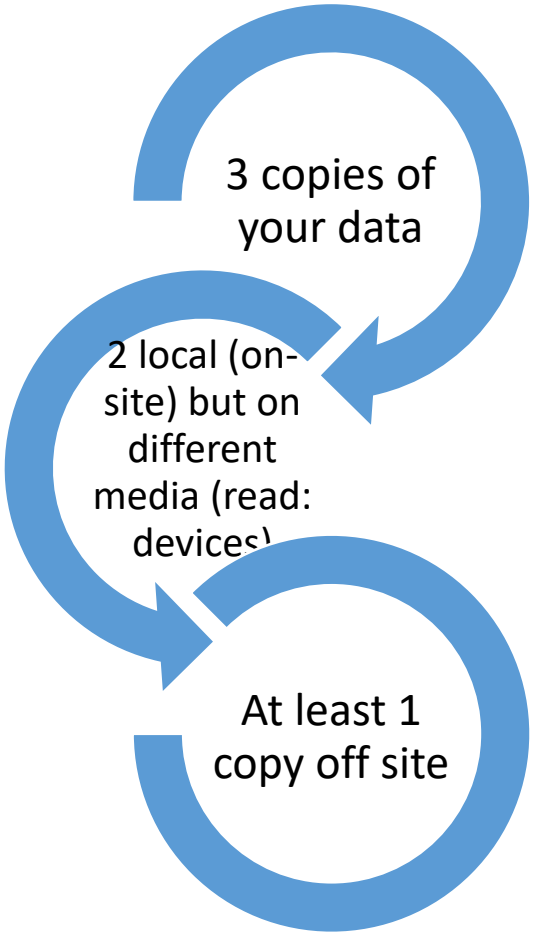
**ESTABLISH CLEAR SECURITY REQUIREMENTS**

**CONDUCT DUE DILIGENCE**

**ESTABLISH SECURITY AND DATA SHARING AGREEMENTS**

**REGULARLY REVIEW AND MONITOR THIRD-PARTY SECURITY**

# 3-2-1 backup strategy



# Q & A

digital square

# Digital Square is supported by:




*Digital Square is a PATH-led initiative funded and designed by the United States Agency for International Development, the Bill & Melinda Gates Foundation, and a consortium of other donors.*

*This presentation was made possible by the generous support of the American people through the United States Agency for International Development. The contents are the responsibility of PATH and do not necessarily reflect the views of USAID or the United States Government.*