Digital Square on
securing digital health

digital square

The fundamentals of cybersecurity and data privacy

April 20, 2023

USAID
FROM THE AMERICAN PEOPLE

BILL & MELINDA GATES foundation

PATH

Agenda

- CIA Triad
- Consequences of cyber attacks
- Why security is vital for digital health
- Security and data privacy, the difference, and business implications
- The principles of secure development and deployment
- Practical challenges and security approaches and action plans
- The opportunity to put questions throughout

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.

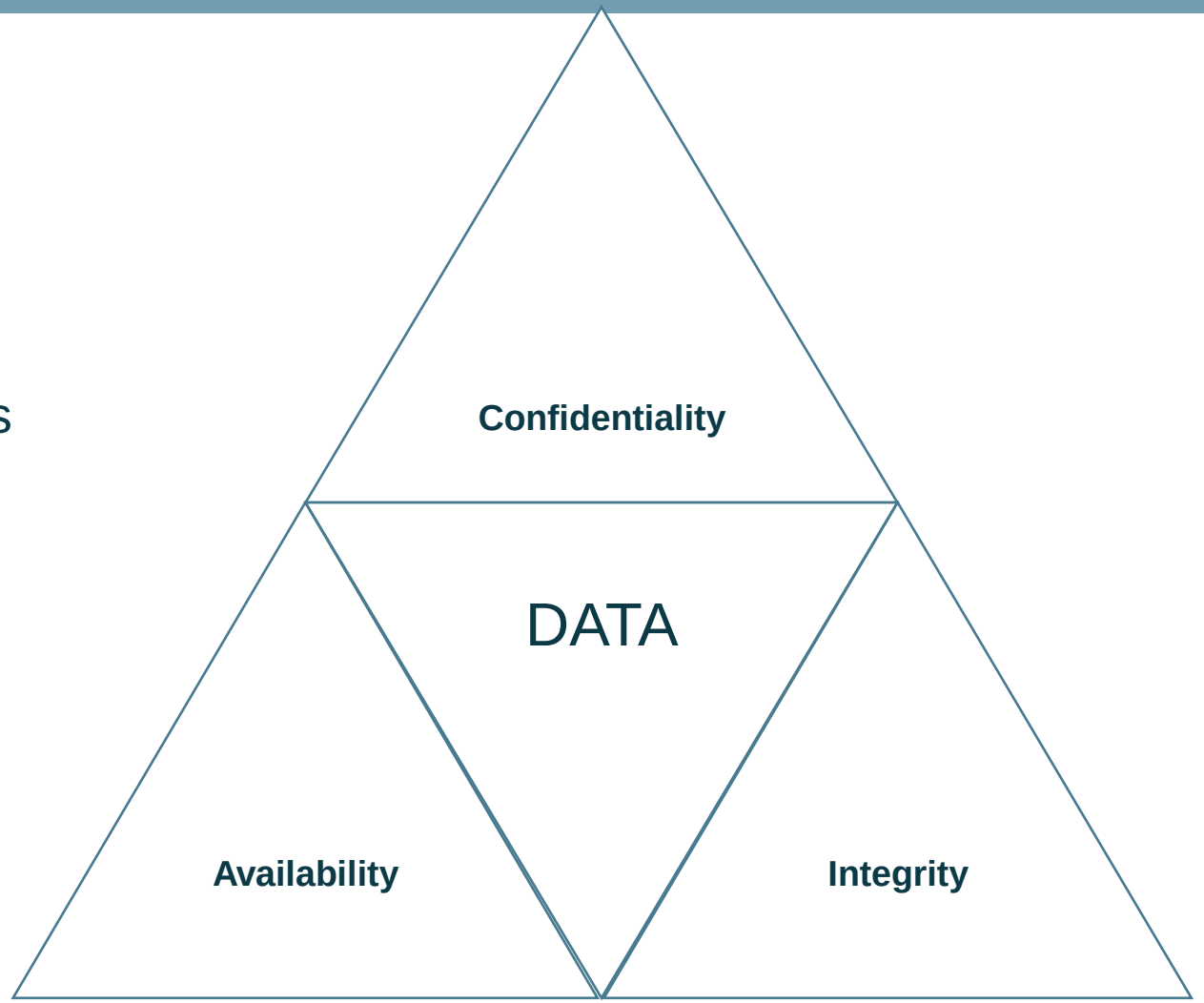
Overall, both cybersecurity and data privacy are essential for protecting sensitive information and ensuring the safety and security of individuals and organizations in today's digital age.

Why Cybersecurity is Important

Cybersecurity is important because it helps protect sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction. Sensitive information can include personal information, financial data, and confidential business information. [1]

CIA triad

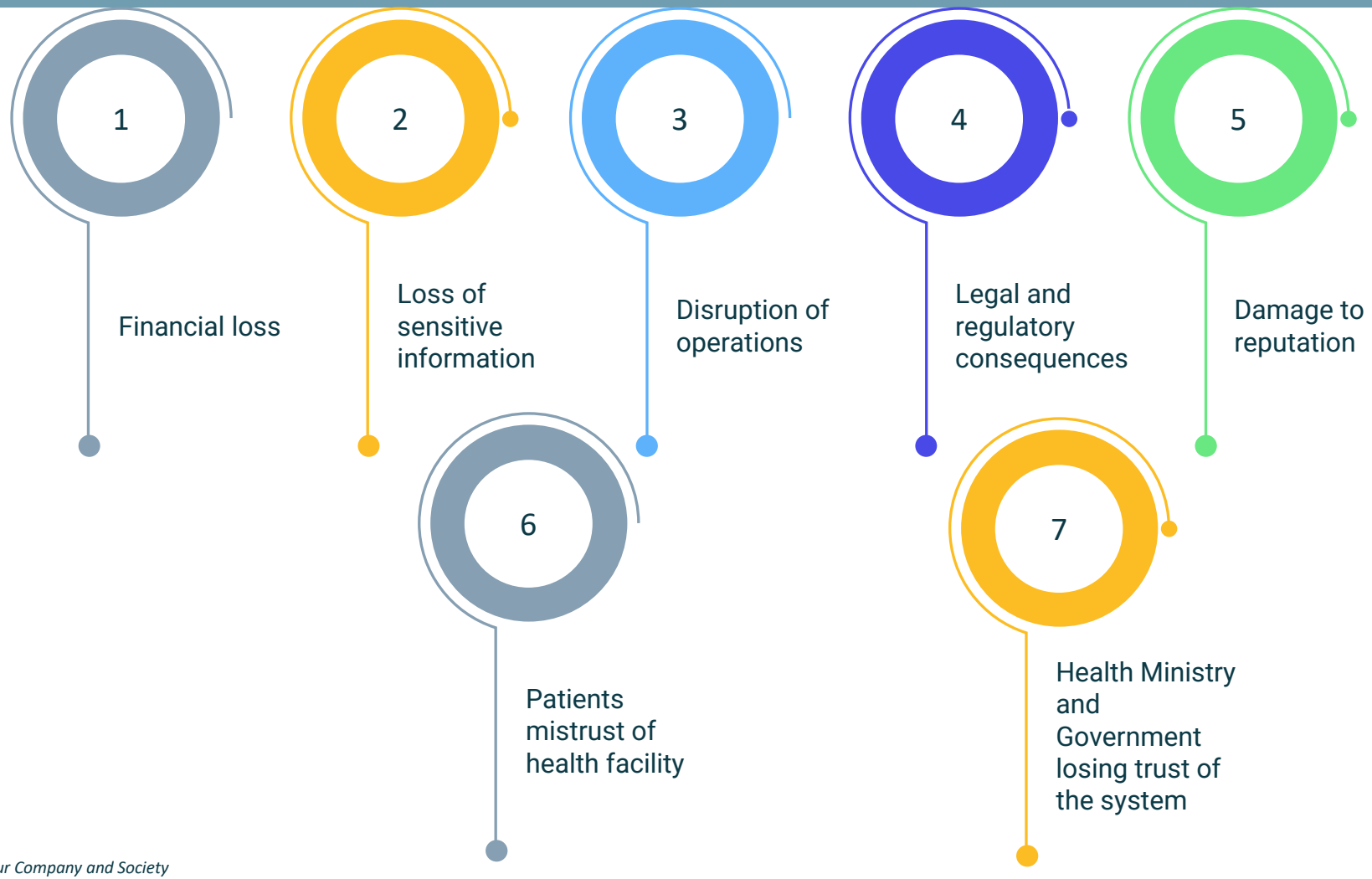
- Confidentiality
  - Ensuring that information is not made available or disclosed to unauthorised individuals, entities, or processes
- Integrity
  - Protecting the accuracy and completeness of assets
- Availability
  - Property of being accessible and usable upon demand by an authorised entity
- Non-repudiation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



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.

Consequences of cyber attacks



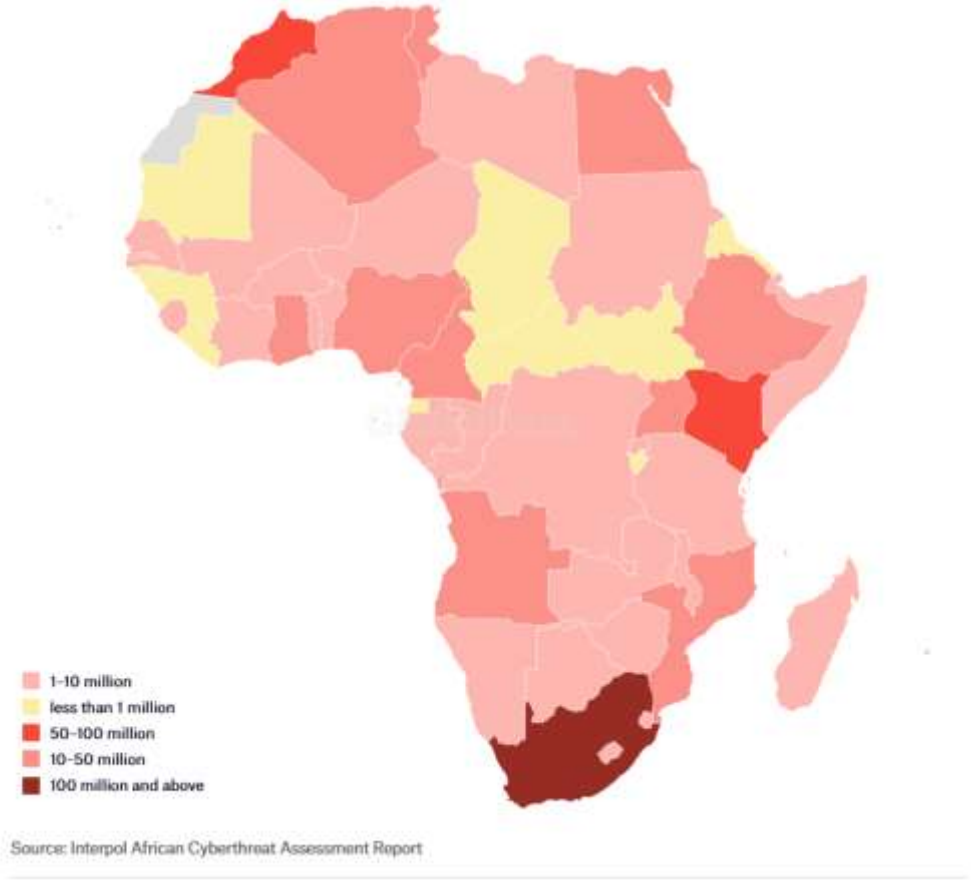
2Solving Cyber Risk: Protecting Your Company and Society
Andrew Coburn, Eireann Leverett, Gordon Woo · 2018

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

Africa overall cyber threat detection 2020 - Feb 2021



6 investmentmonitor.ai
https://www.investmentmonitor.ai/features/africa-cyber-crime-threat-digitalisation/

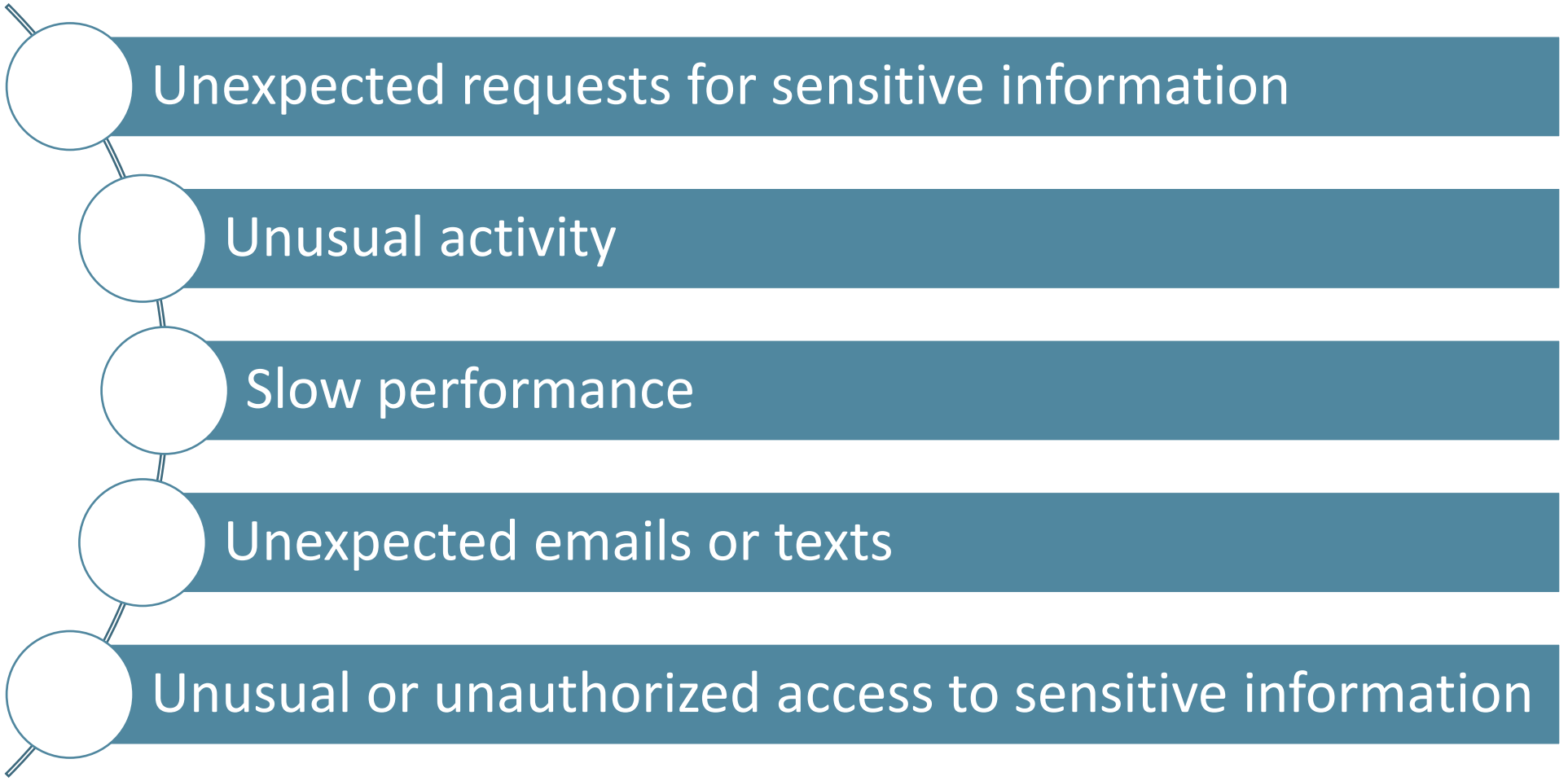
Number of Internet users in Africa

"More than 90% of African businesses are operating without the necessary cyber security protocols in place."
-Interpol African Cyber Threat Assessment Report 2021

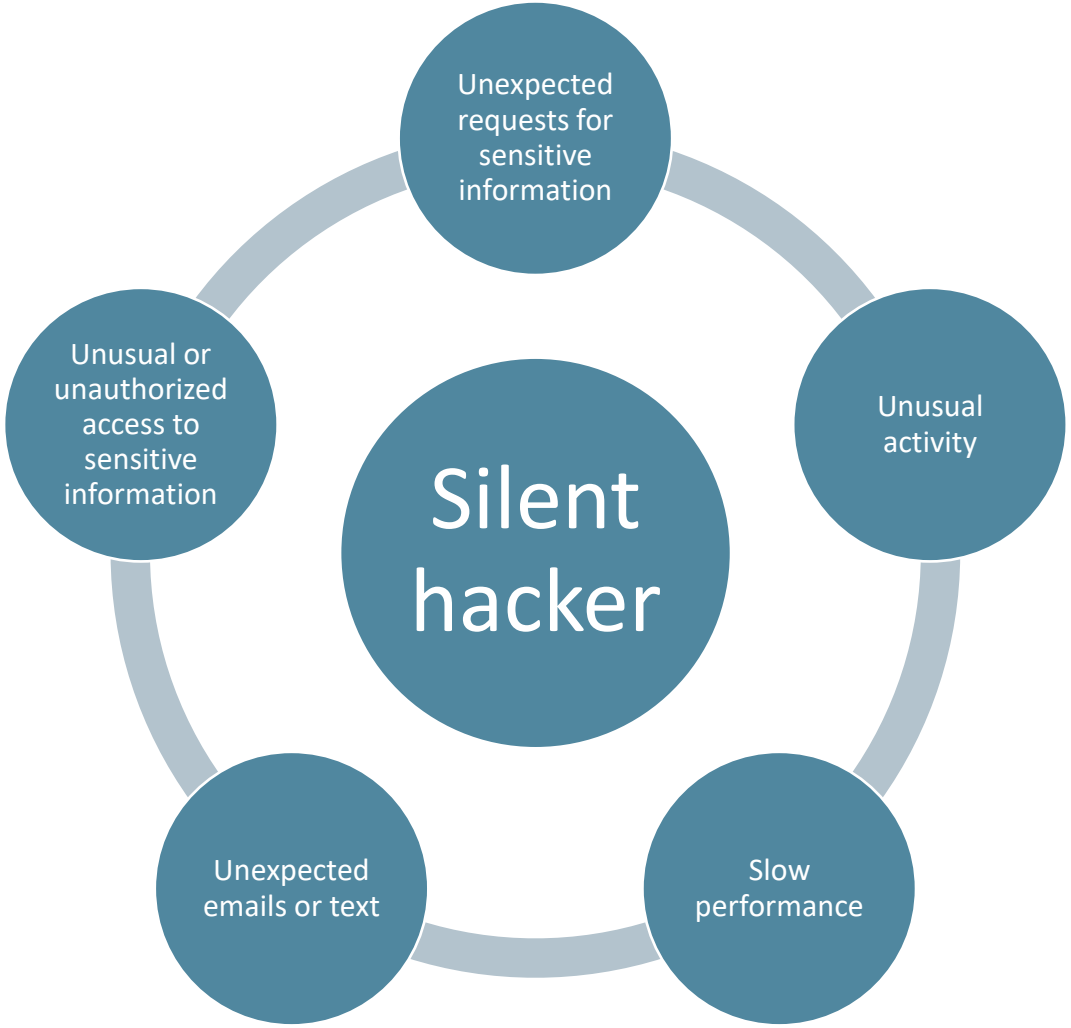
Common types of cyber attacks in health sector

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

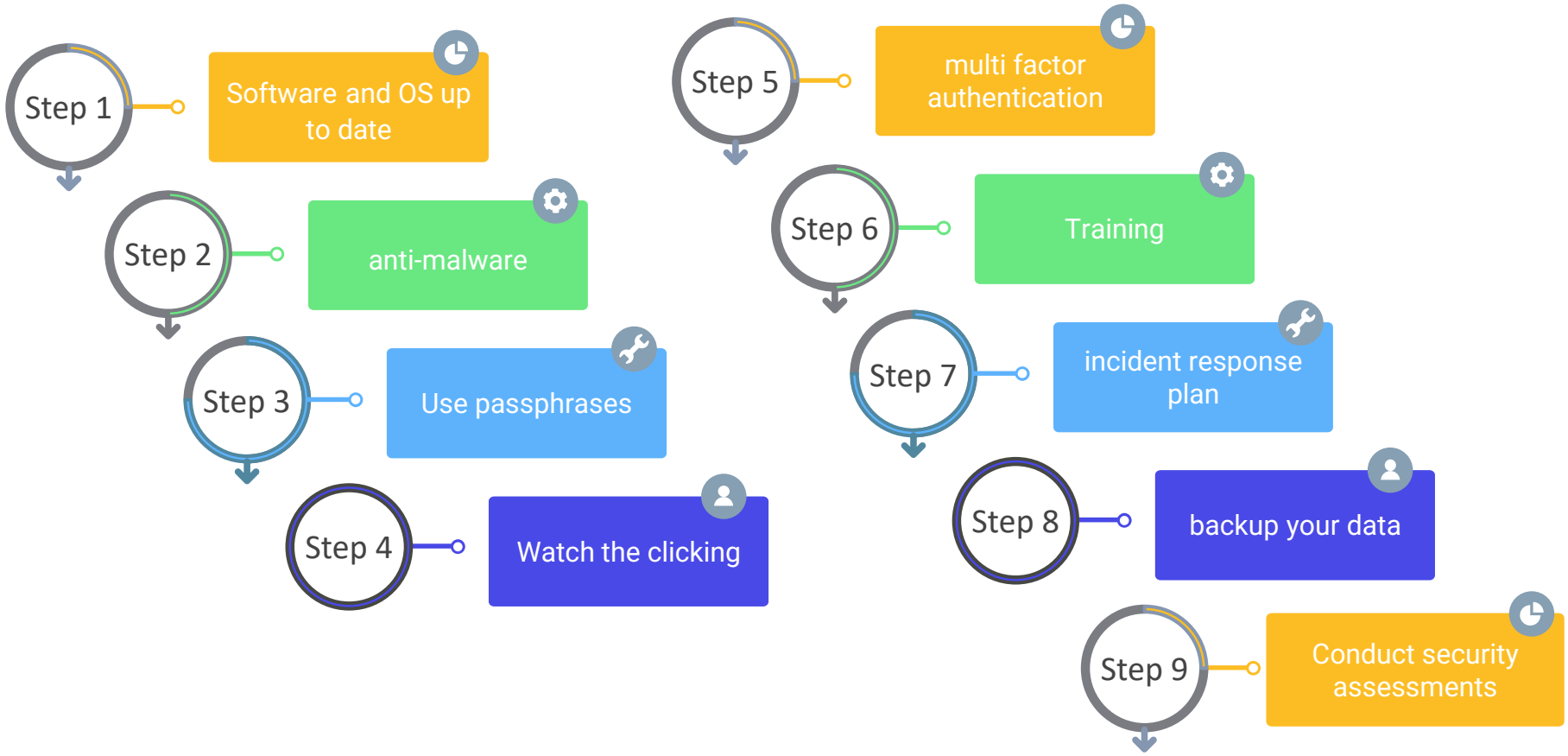
Recognizing a cyberattack (IoC)



Recognizing a cyberattack (IoC)



Best practices for protection against cyberattacks



Cybersecurity in the Digital Age: Tools, Techniques, & Best Practices
Gregory A. Garrett, 2018

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

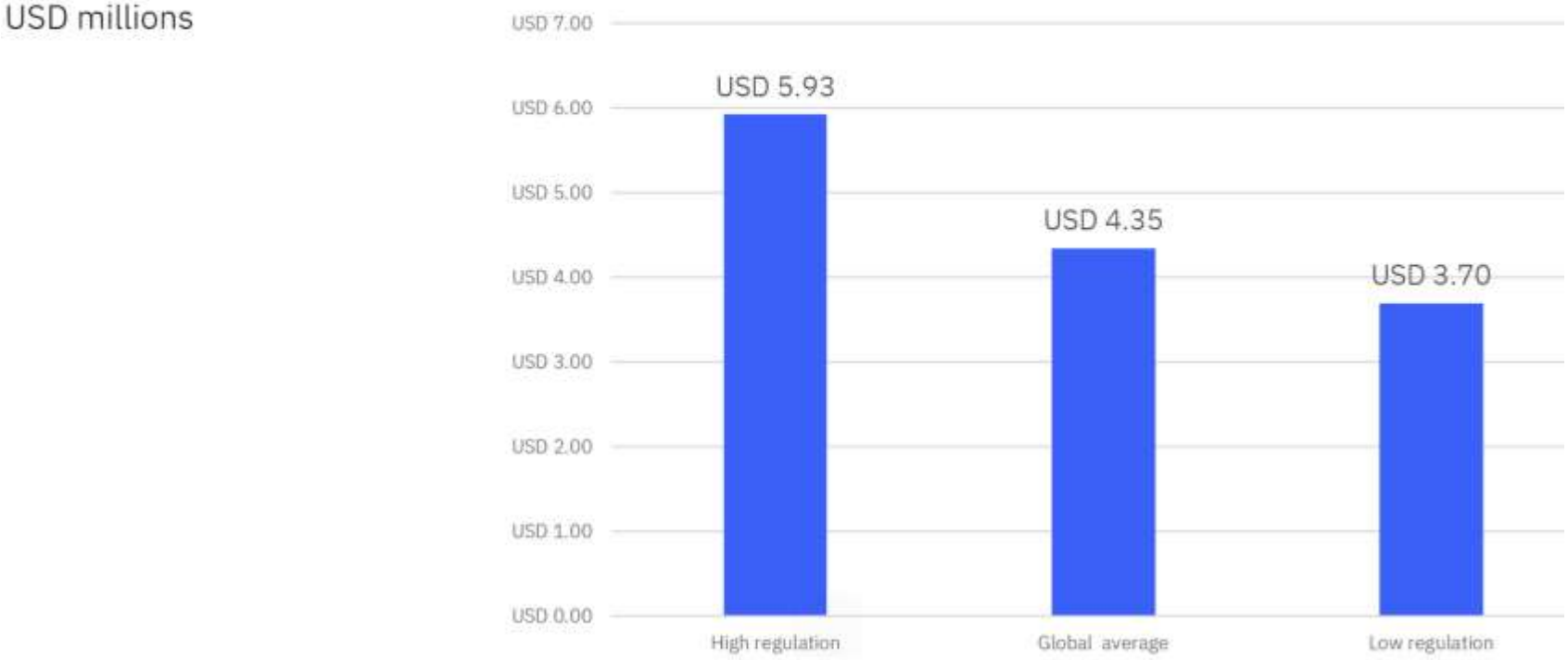
Privacy: Involves controlling access to personal information and a control a person can have over information discovery and sharing

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.

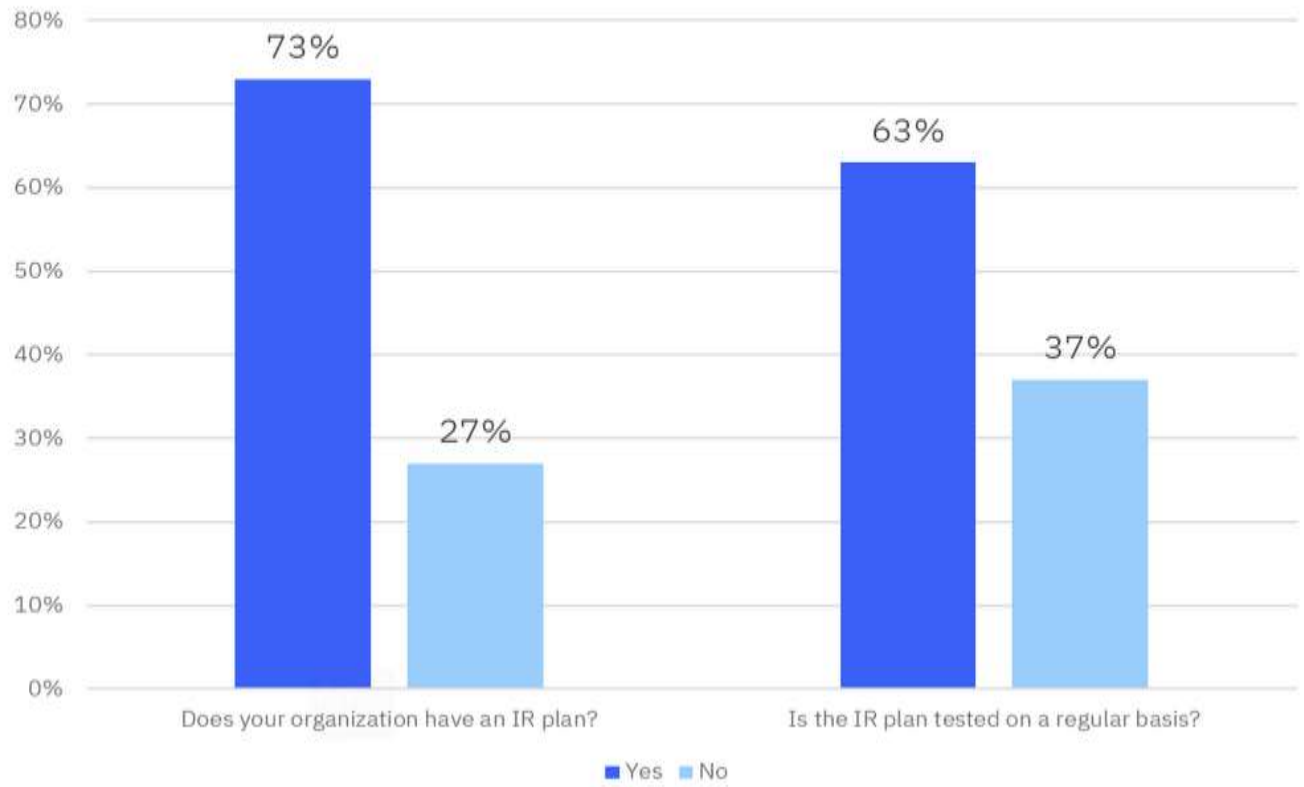
Regulated industries also see long tail of costs that accumulate down the line

Average cost of a data breach based on high and low regulated industries



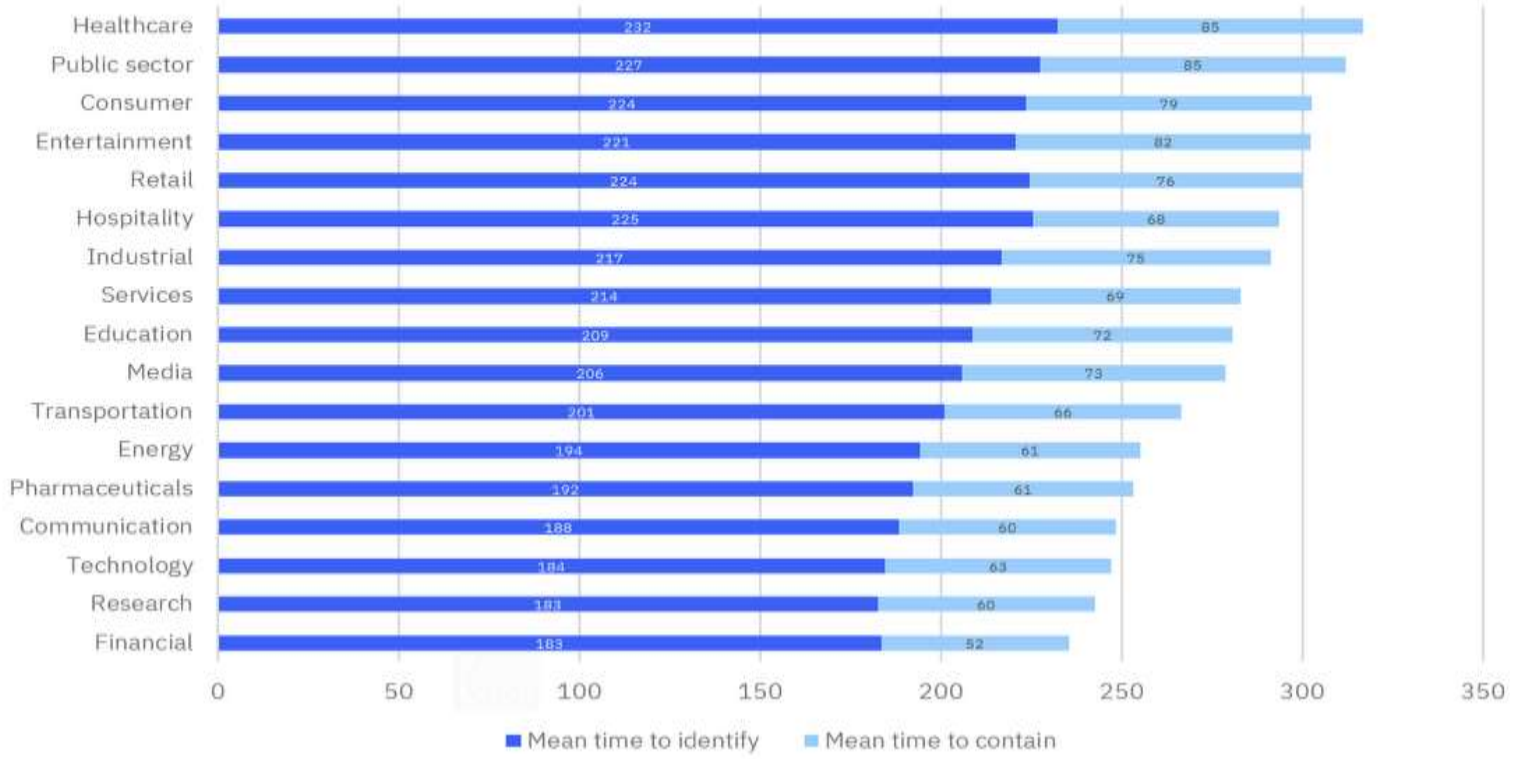
Incident response plan

Does your organization have an incident response (IR) plan and is it tested?



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

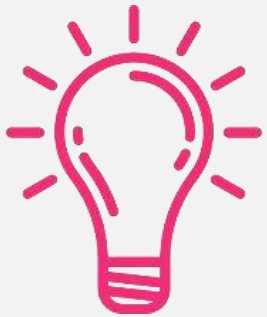
Cybersecurity and Data Privacy

digital square

Cybersecurity vs data privacy

Cybersecurity

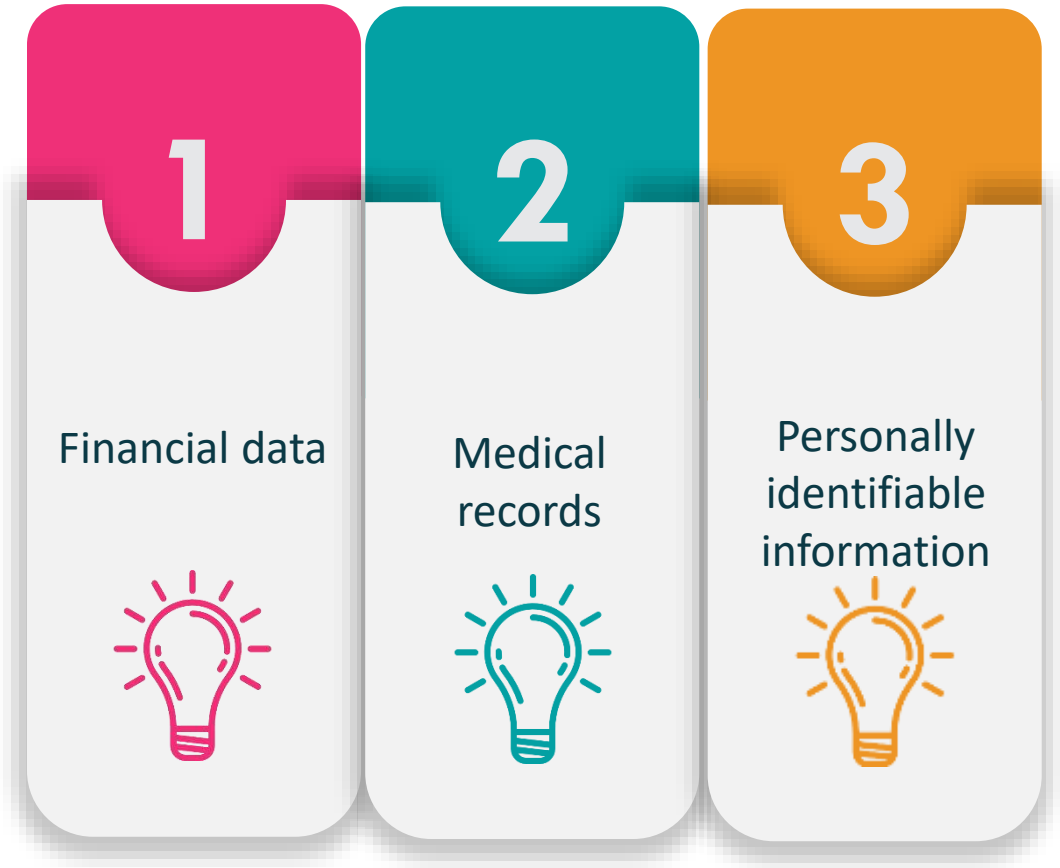
is focused on protecting digital assets and infrastructure



Data Privacy

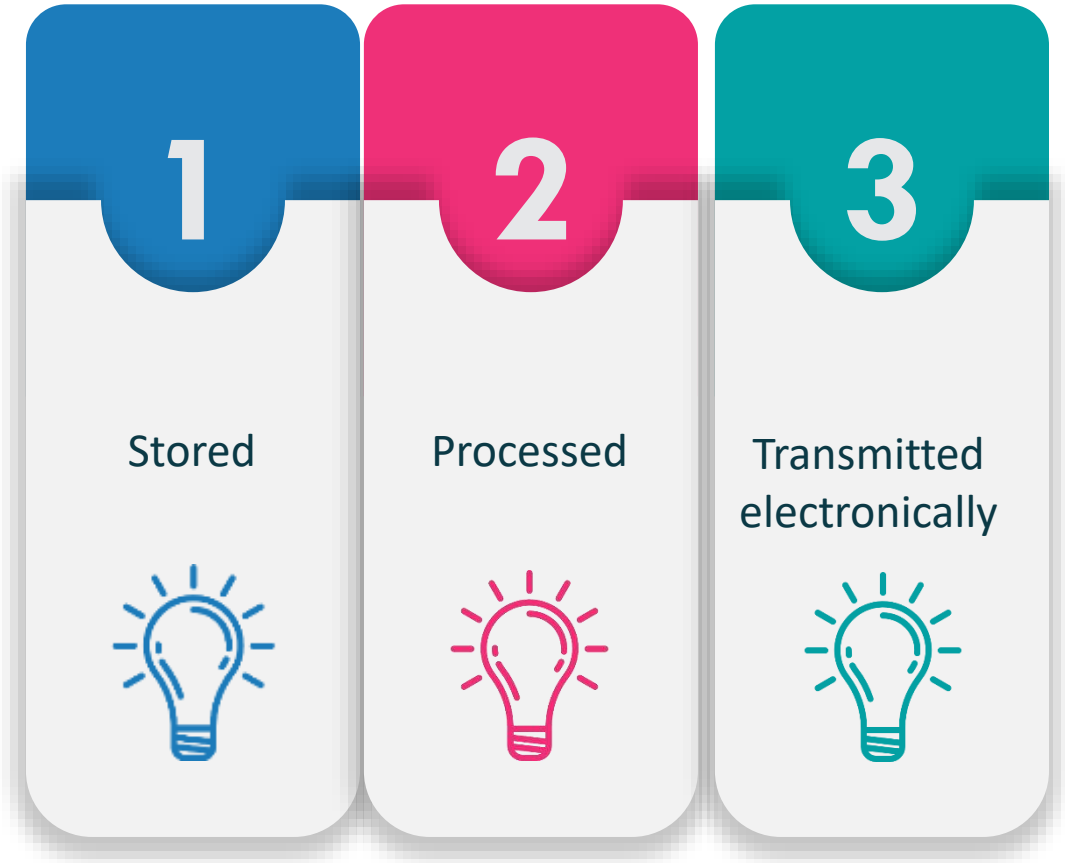
is concerned with safeguarding personal data and ensuring privacy rights

Data privacy: measures ensures personal information such as:

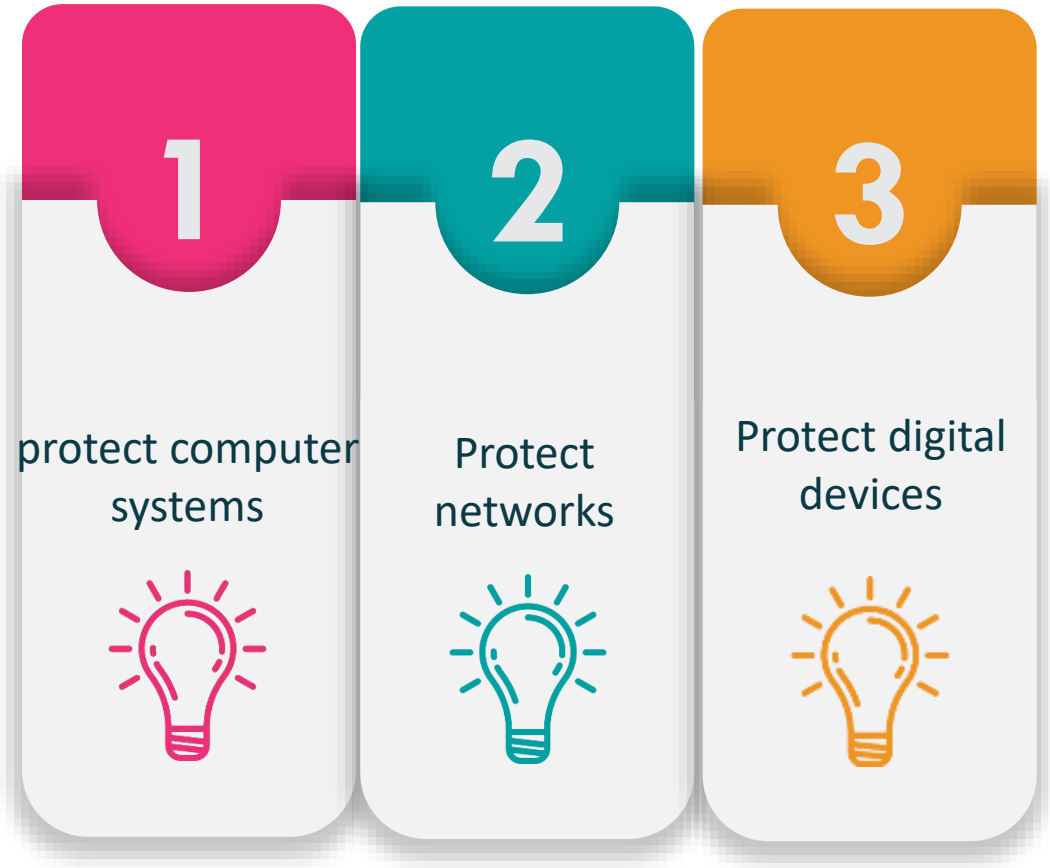


Kept private and secure from unauthorized access or use

Data privacy: protection of sensitive or confidential information



Cybersecurity refers to the measures that:



Cybersecurity measures prevent:

Secure software development, implementation and deployment

digital square

Secure software development and DevSecOps

Secure software development is an approach to creating software that prioritizes security throughout the entire development process.

DevSecOps is a methodology that emphasizes the collaboration and integration of security into the DevOps process. This approach involves building security into the software development process from the outset rather than treating it as an afterthought.

The eight principles of secure development & deployment

1 **Secure development is everyone's concern**

2 **Keep your security knowledge up-to-date**

3 **Keep your security knowledge up-to-date**

4 **Secure your development environment**

5 **Protect your code repository**

6 **Secure the build and deployment pipeline**

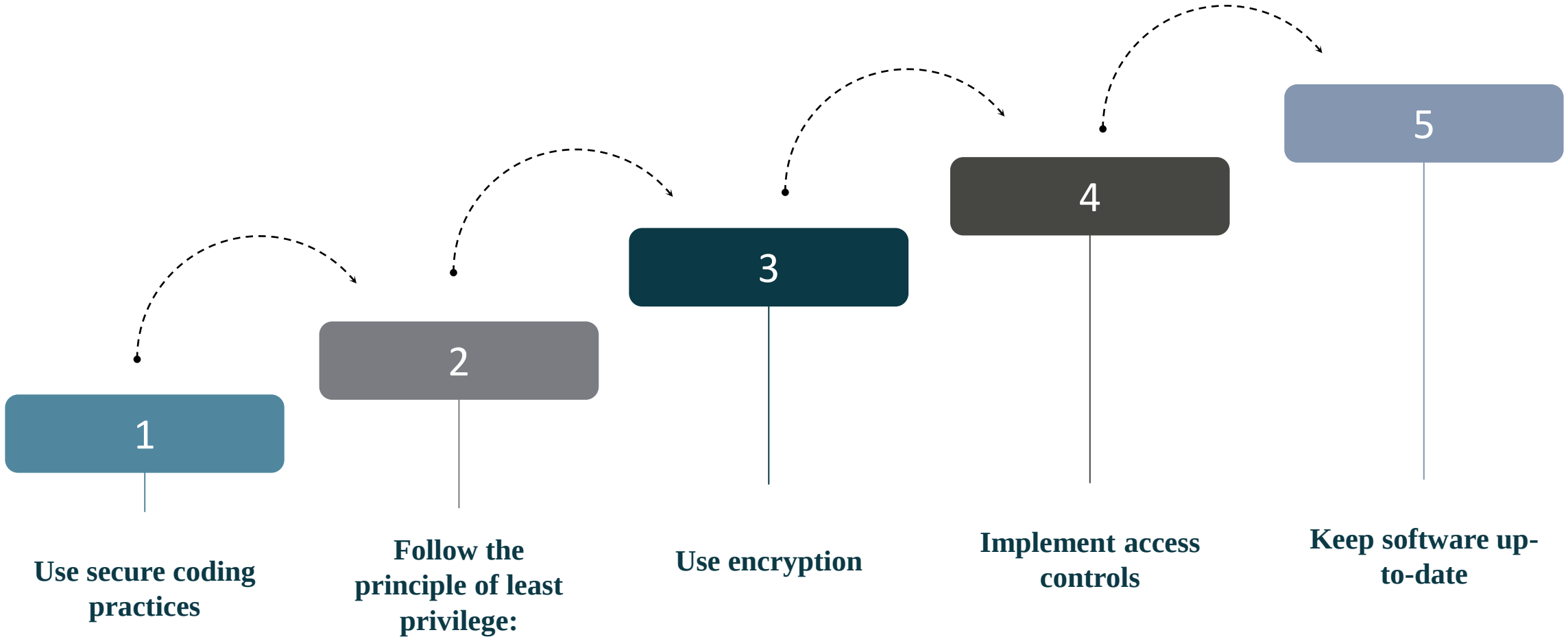
7 **Continually test your security**

8 **Plan for security flaws**

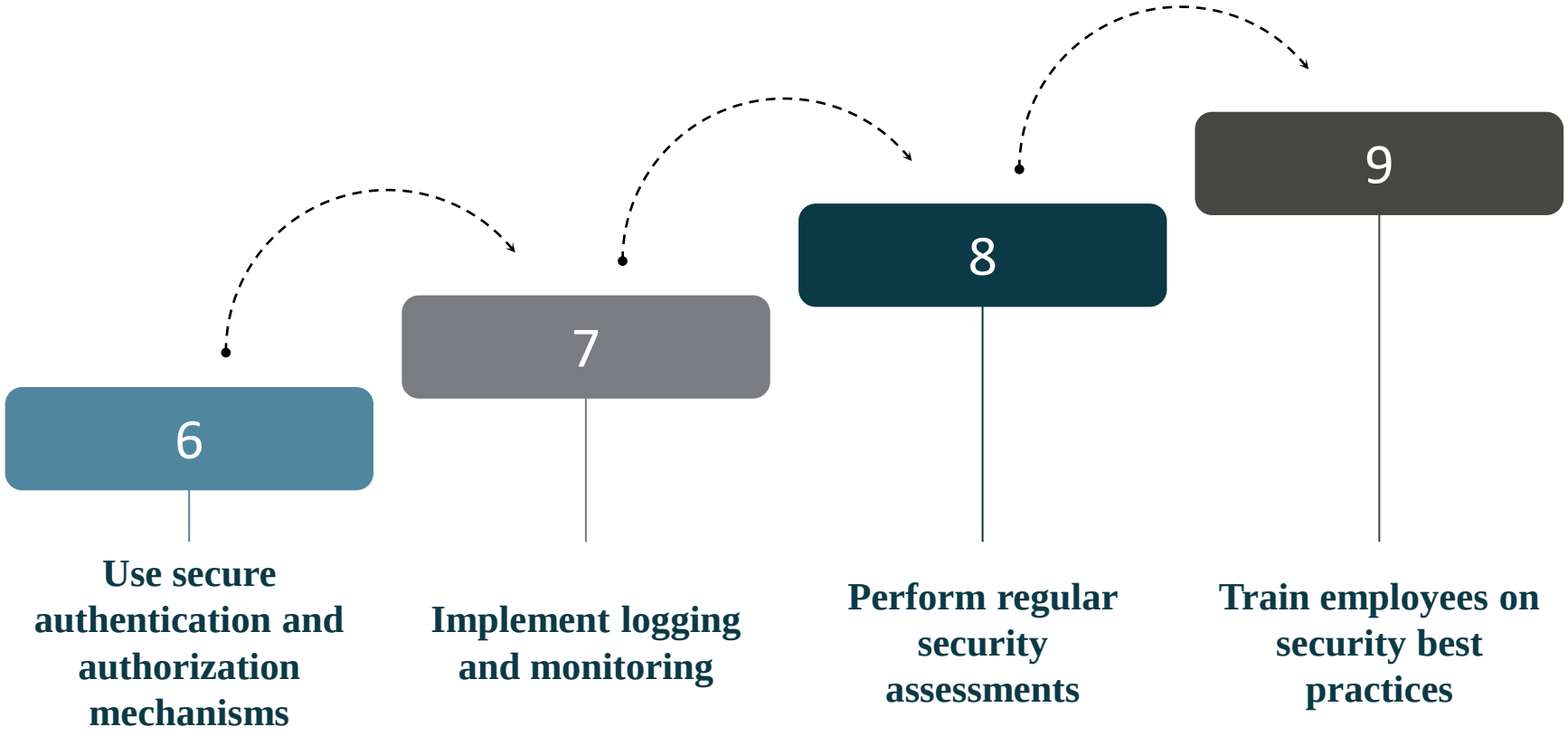
Secure implementation

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.

Best secure implementation practices



Best secure implementation practices (cont)



Security Assessment

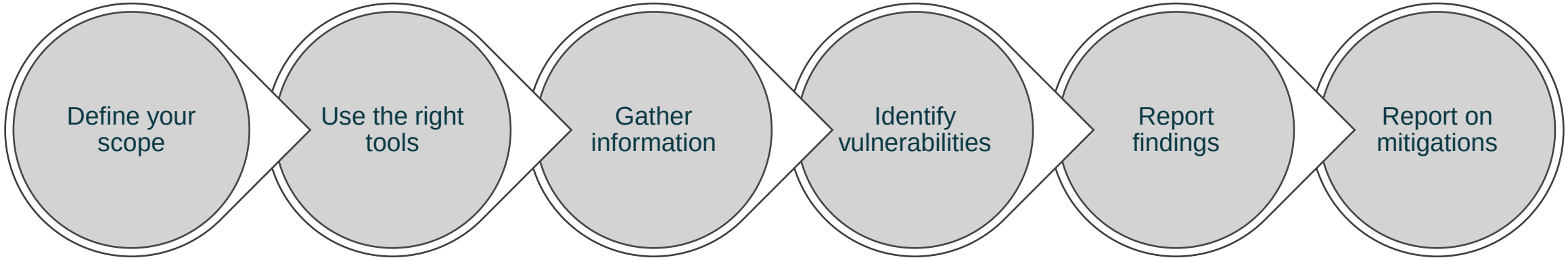
digital square

Security assessment

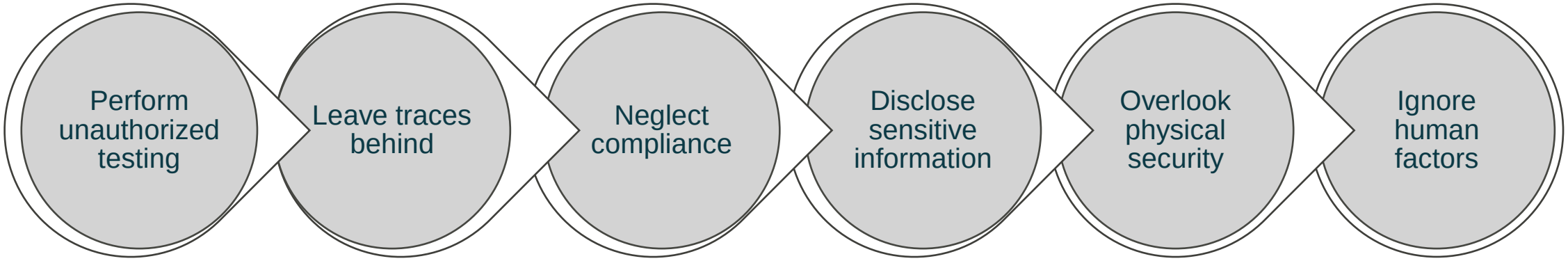
Security assessment is the process of evaluating the security posture of a system, network, or application to identify potential vulnerabilities and threats:

- Identify assets
- Threat modeling
- Vulnerability assessment
- Penetration testing
- Risk assessment

How to conduct security assessment



What to avoid during a security assessment

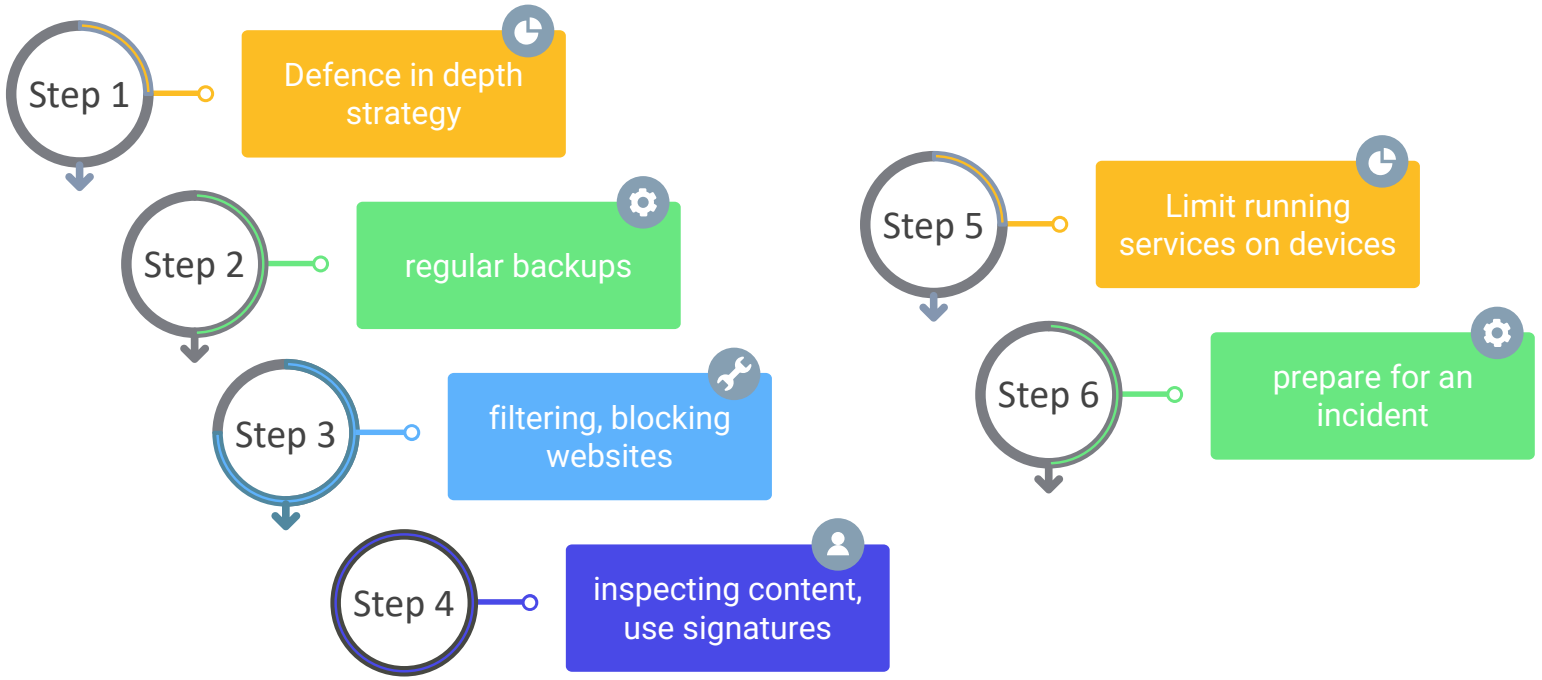


Incident Response Planning: Focused Preparation
Gabe Smit, Timothy Smit, 2021

Malware prevention

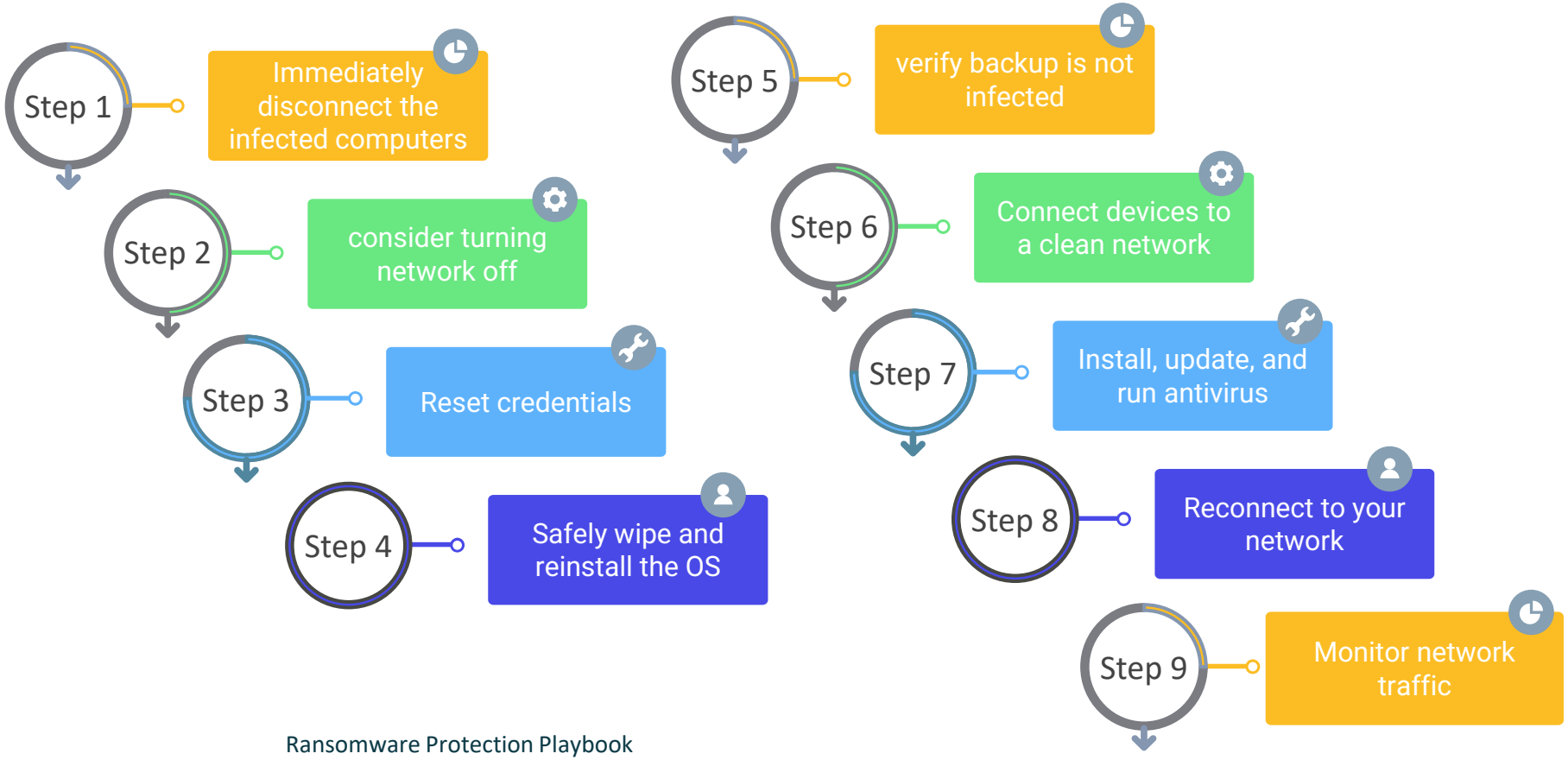
Malware is malicious software that is designed to damage or disrupt computer systems, steal data, or gain unauthorized access.

Malware prevention and actions to take



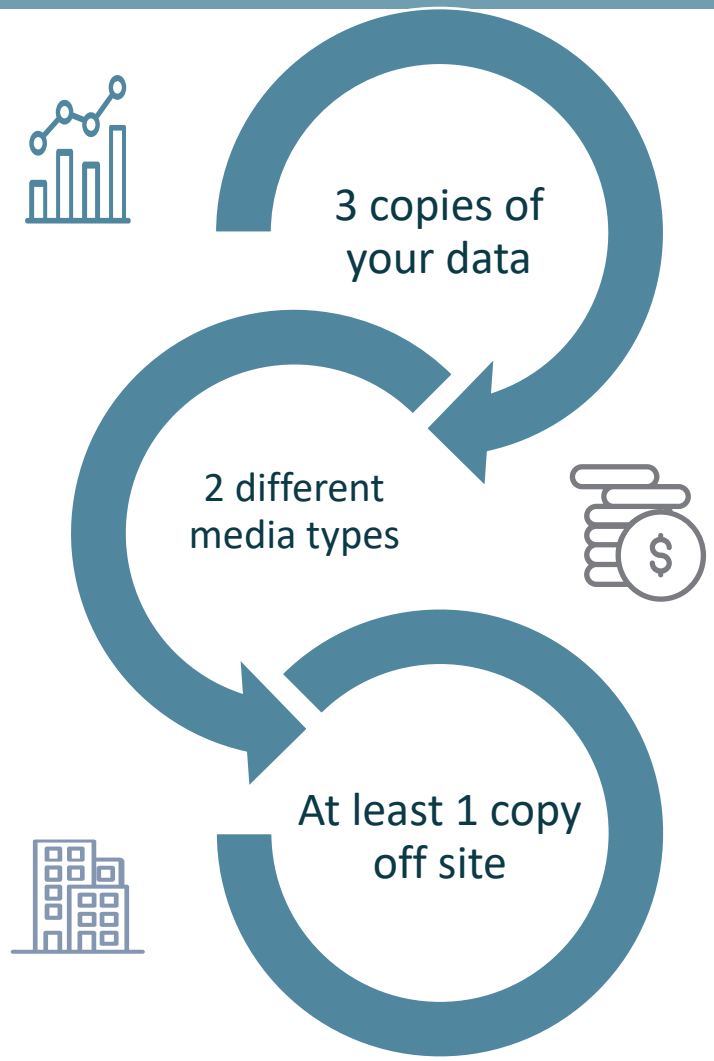
Ransomware Protection Playbook
Roger A. Grimes, 2021

Steps to take if your organization is already infected with malware



Ransomware Protection Playbook
Roger A. Grimes, 2021

3-2-1 backup strategy



Mastering Veeam Backup & Replication: Secure backup with Veeam 11 for defending your data and accelerating your data protection strategy
Chris Childerhose, 2022

Q&A

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.