Hacktales

CYBERSECURITY FOUNDATION PROGRAM

Authors:
Chikodili Udeh & Olajide Adebayo

Contents

Hacktales

01
History of Cybersecurity

- The Evolution: 1960 - 2030
- Cybersecurity Trends

02
Cybersecurity Fundamentals

- CIA Triad
- Pillars of Cybersecurity

03
Cybersecurity Domains

- Defense-in depth
- Knowledge Areas

The History of Cybersecurity

Objectives

Hacktales

01

Understand the evolution of information security over the last five decades.

02

Learn about the major breaches since the inception of technology.

03

Analyze the future of digital security over the next decade.

Hacktales

The Evolution

1960 - 1980

Before 1960	The first computer was created.
1960 - 1970	Physical and password security measures were established. ARPANET was formed.
1970 - 1980	The first-ever virus was born.

Hacktales

The Evolution

1980 - 2010

1980 - 1990

ARPANET became widely available as the world wide web (www).

1990 - 2010

The rise of firewalls, antivirus, and legal fines.

Hacktales

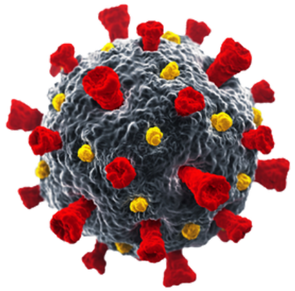
The Evolution

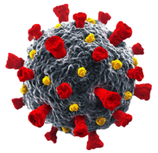
2010 - 2019

2010 - 2013 TARGET Adobe

2014 - 2016 ebay yahoo!

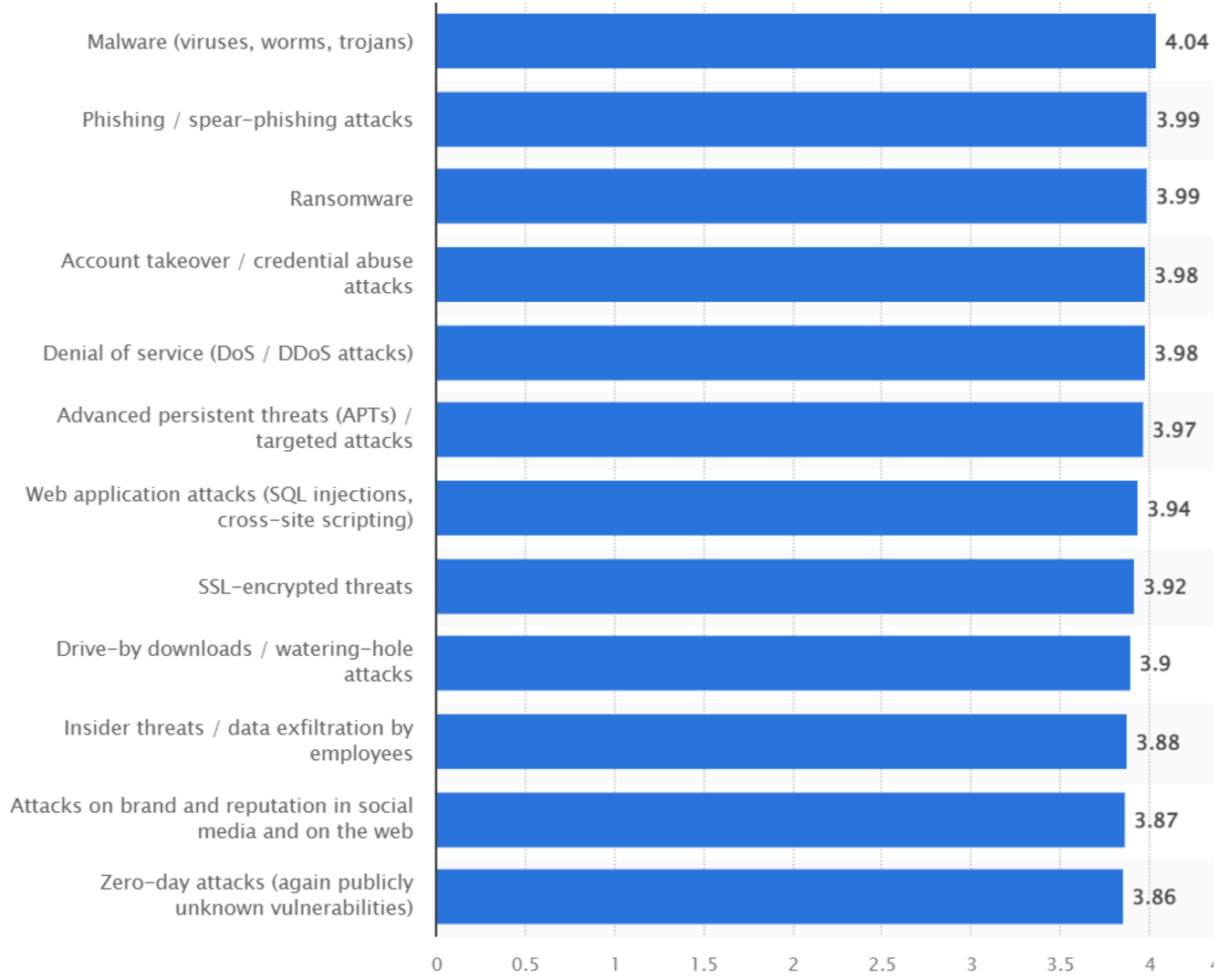
2017 - 2019 First American





The Evolution

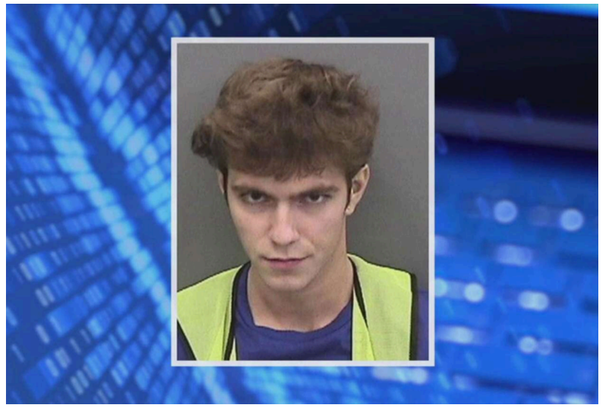
2020 - 2021



Source: Statista

Case Study: Twitter (X)

Hacktales



HACKED

Joe Biden @JoeBiden · 2m

I am giving back to the community.

All Bitcoin sent to the address below will be sent back doubled! If you send $1,000, I will send back $2,000. Only doing this for 30 minutes.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Enjoy!

Twitter Support @TwitterSupport · 43m

We are aware of a security incident impacting accounts on Twitter. We are investigating and taking steps to fix it. We will update everyone shortly.

2.5K 15K 26.2K

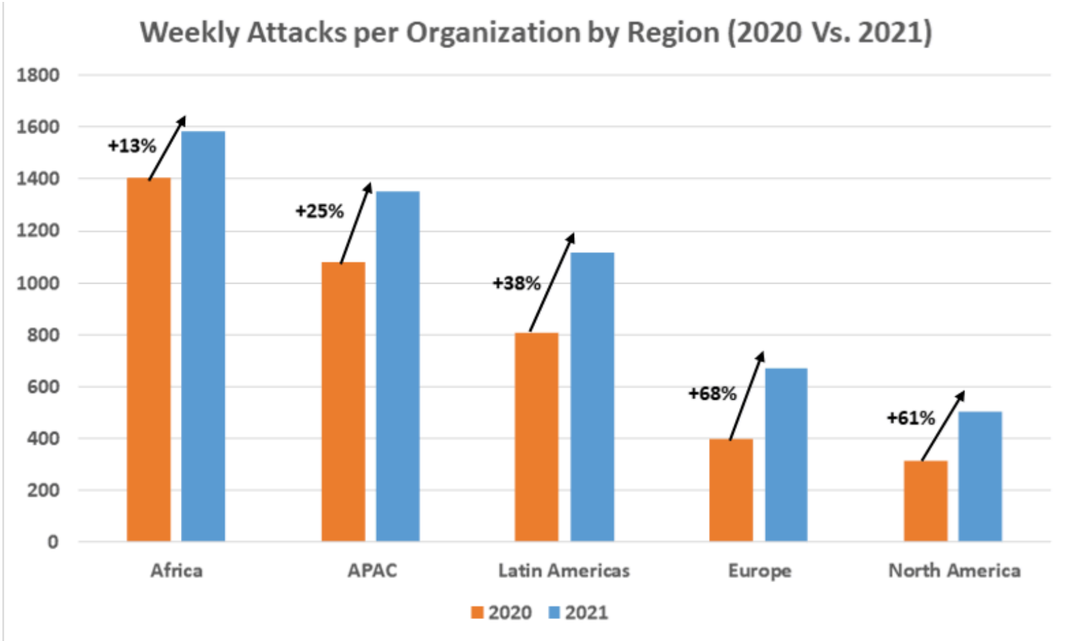
Twitter Support @TwitterSupport · 9m

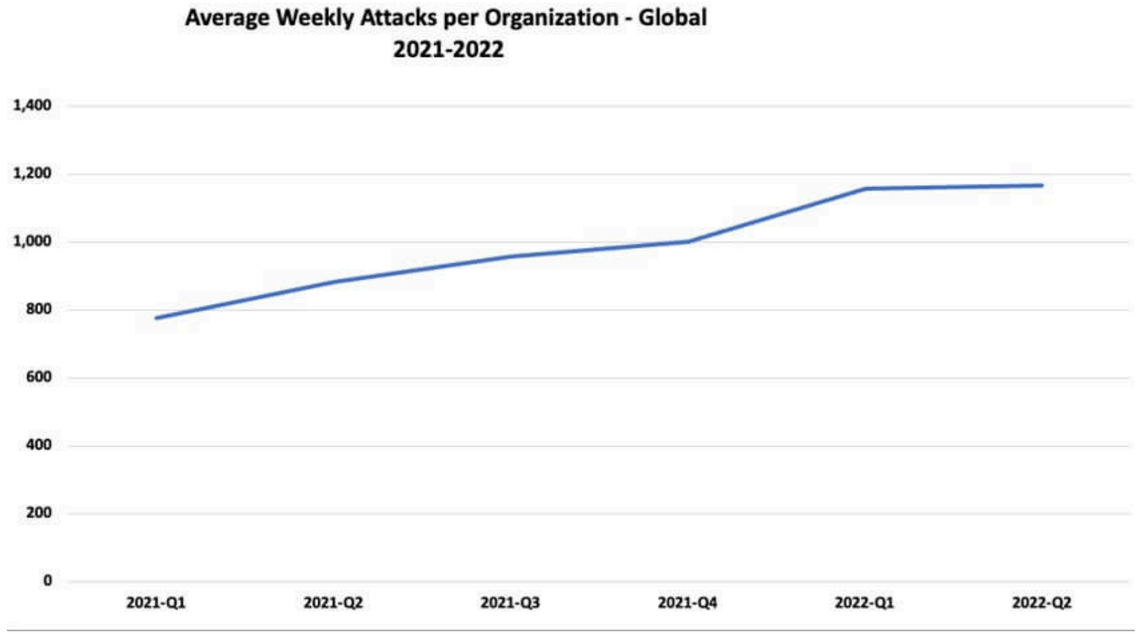
You may be unable to Tweet or reset your password while we review and address this incident.

492 3.9K 4.5K

The Evolution (2021 - 2022)

Hacktales





Source: Checkpoint

Hacktales

The Evolution

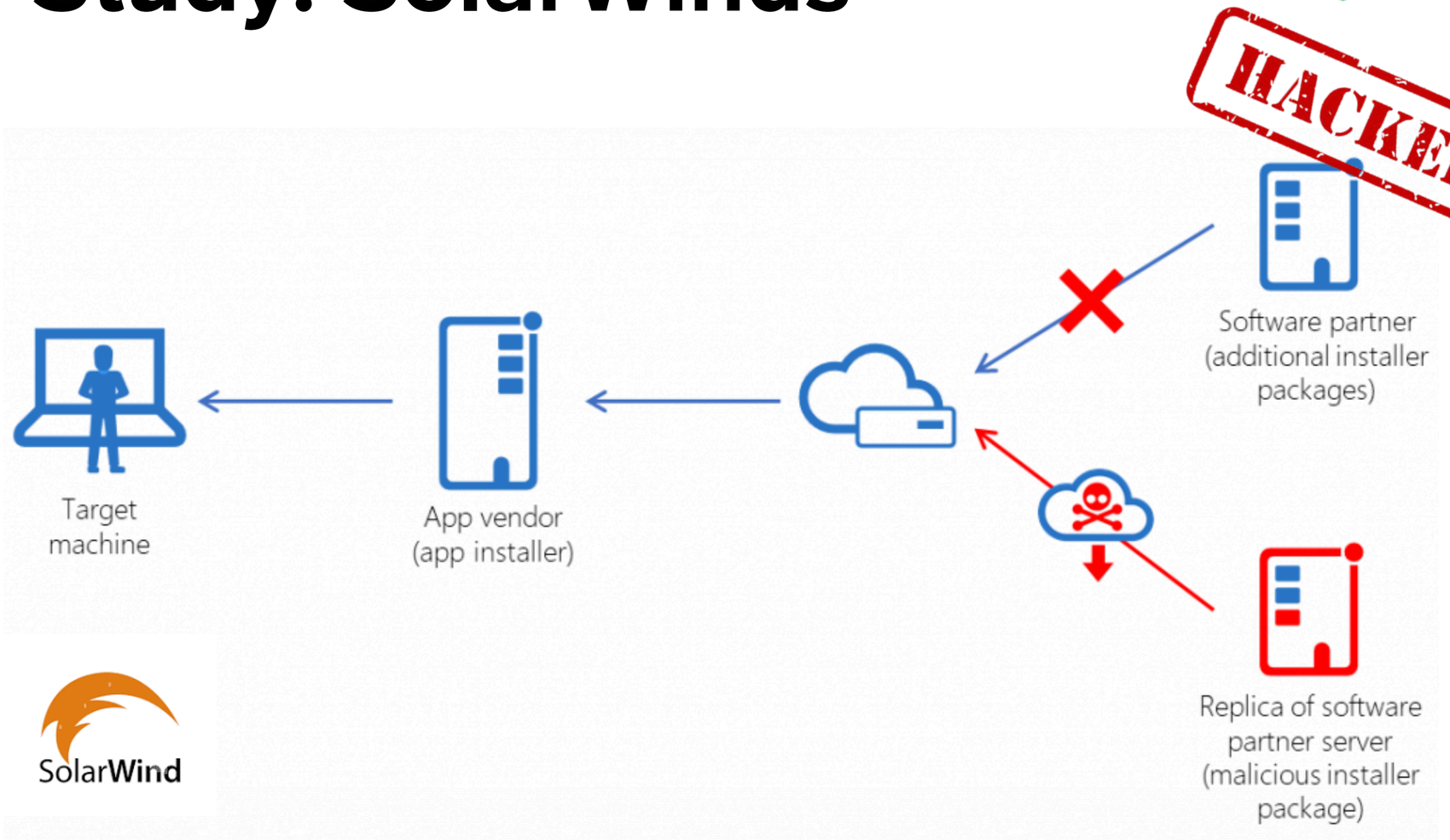
2023 - Present

Region	Weekly Average of attacks per org	YoY Change
Africa	*2164*	*+23%*
APAC	*2046*	*+22%*
North America	*1011*	*+18%*
Latin Americas	*1745*	*+9%*
Europe	*1013*	*+5%*

Source: Checkpoint

Case Study: SolarWinds

Hacktales



The Evolution

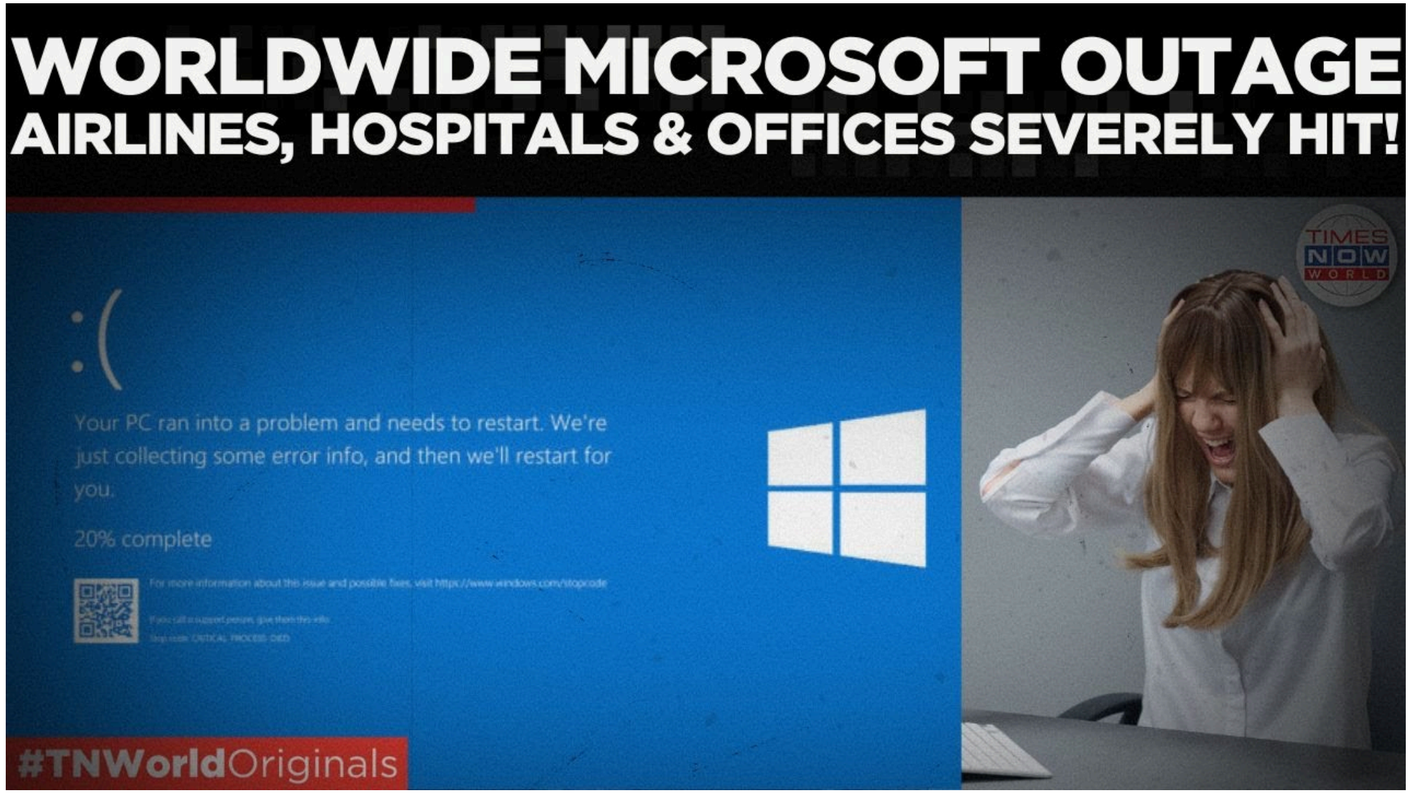
2024 - 2030

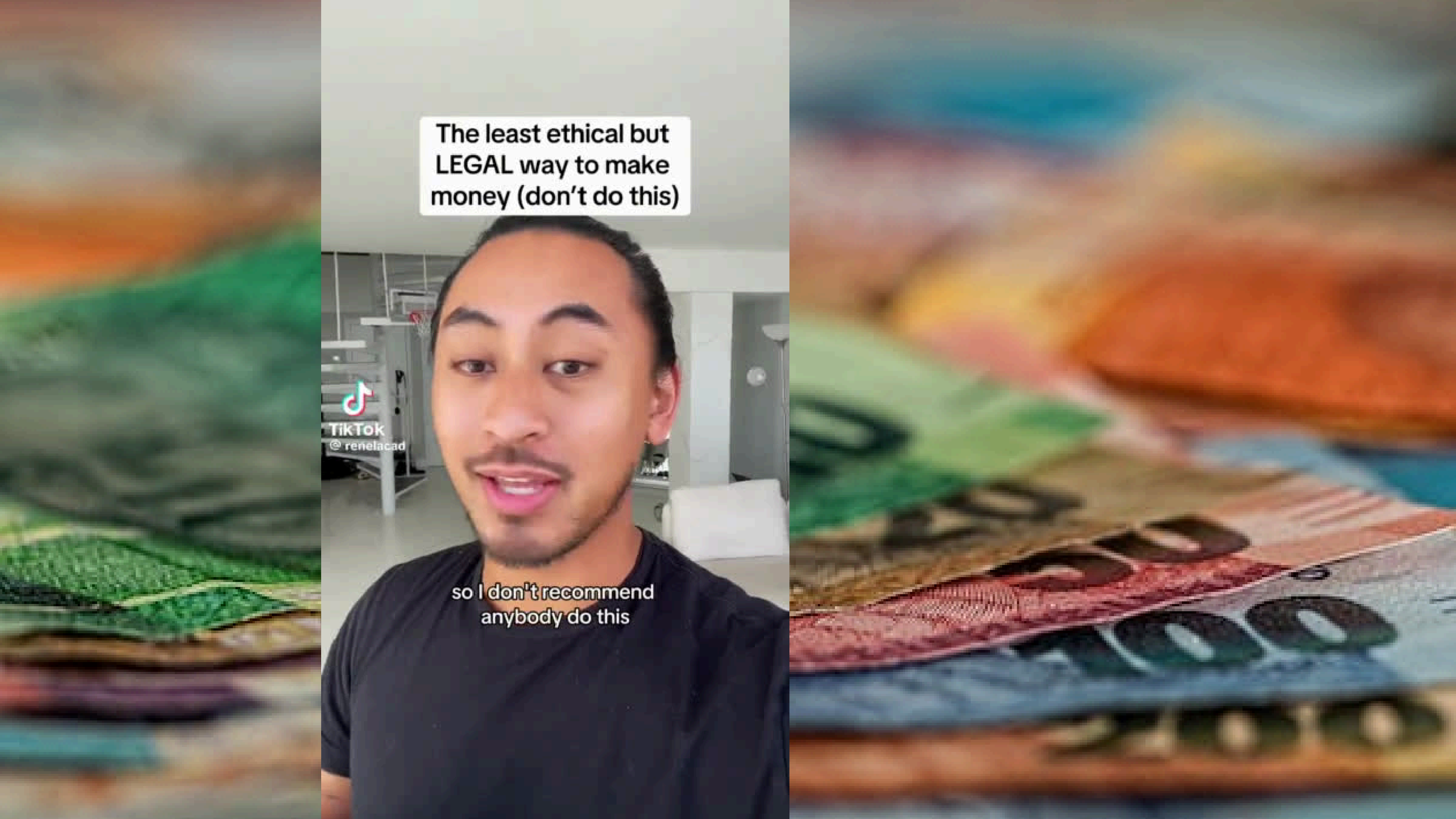
Source: ENISA

Case Study: CrowdStrike

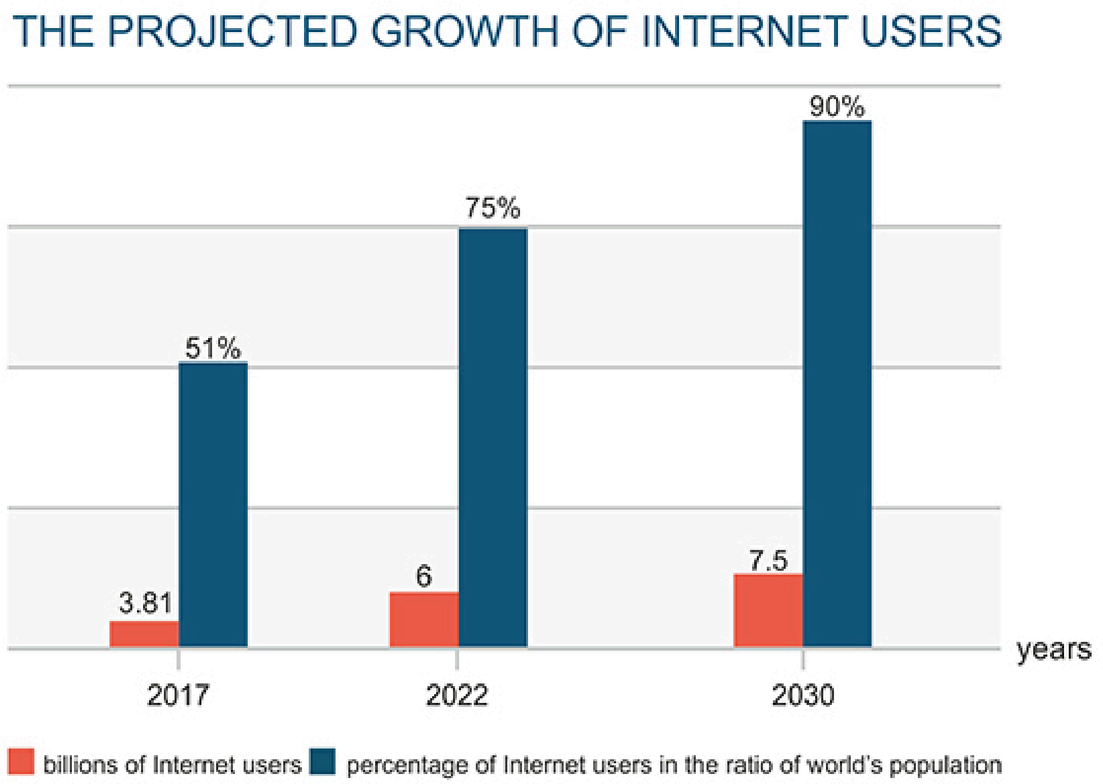
Hacktales

CROWDSTRIKE




The least ethical but LEGAL way to make money (don't do this)
TikTok
@ renelacad
so I don't recommend anybody do this

Hacktales



Module 1: Introduction to Cybersecurity
Cybersecurity Foundation Program

Date:
April 26th 2025

Cybersecurity trends: Looking over the horizon

Hacktales

$101.5

billion in projected spending on service providers' by **2025**

15%

annual increase of costs related to cybercrime, will reach **$10.5 trillion** a year 2025

85%

of small and midsize enterprises intend to increase IT security spending until **2023**

3.5

million cybersecurity positions now open worldwide

+21%

forecast of compund annual growth for direct cyber insurance premiums until **2025**

* Service providers include consultants harware support implementations and outsourcing
* Source Center for Strength and International Studies IBM; identity Theft Resource Center; Kaspersky Lab; National Cyber Security Center; press PurpleSec data survey; Statista; McKinsey Market Map

Hacktales

Got Questions?


TIME TO REBOOT
12:45 - 1:00PM

Cybersecurity Fundamentals

Objectives

Hacktales

01

Get to know the principles that drive cybersecurity in today's world.

02

Understand the impact of cybersecurity on business strategy and delivery.

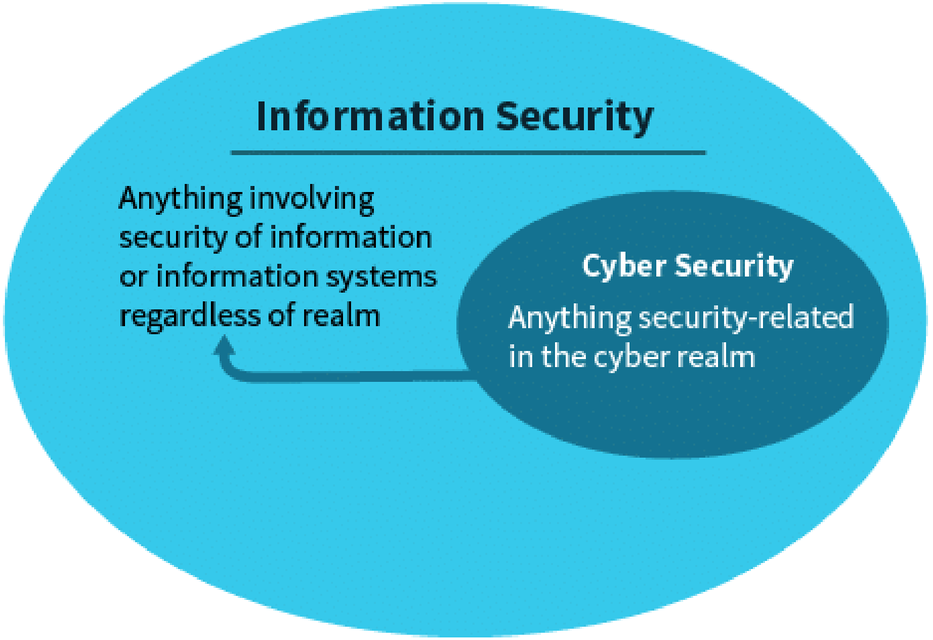
03

Gain insight into the core pillars of cybersecurity.

Information vs. Cyber Security

Hacktales

The practice of protecting sensitive information from unauthorized activities including access, modification, recording, and any disruption or destruction.



CIA Triad

Hacktales

There are three main principles that drive information security...

CIA Triad vs. CIAAN

Hacktales

AUTHENTICATION

Recognizing a user's identity and providing access based on it.

NON-REPUDIATION

Prevents a person or entity from denying having performed a particular action related to data for proof of obligation, intent, or commitment; or for proof of ownership.

Hacktales

It’s a common misconception that cybersecurity is all about technology (hardware and software).

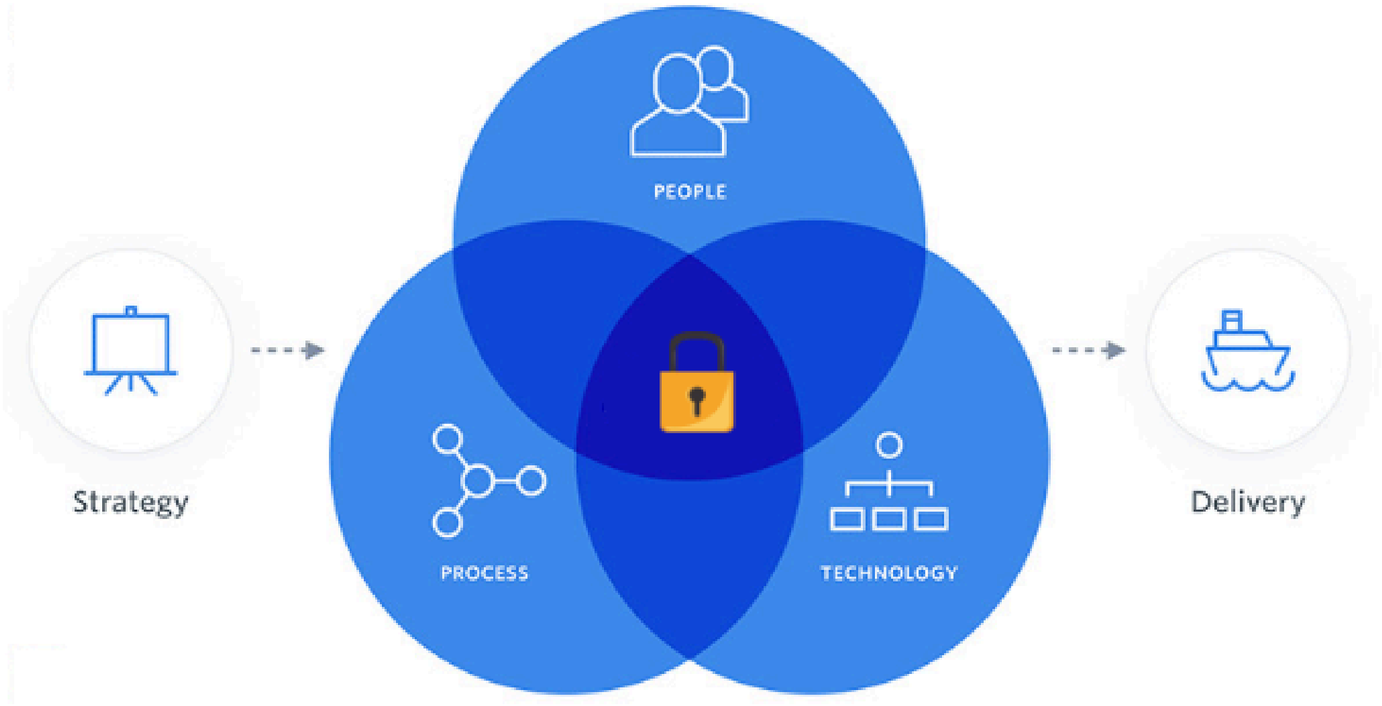
Technology is obviously a massive part of cybersecurity, but it is not enough to protect against modern cyber threats.

Date:
April 26th 2025

Pillars of Cybersecurity

Hacktales

1. People
2. Process
3. Technology



Pillar 1: People

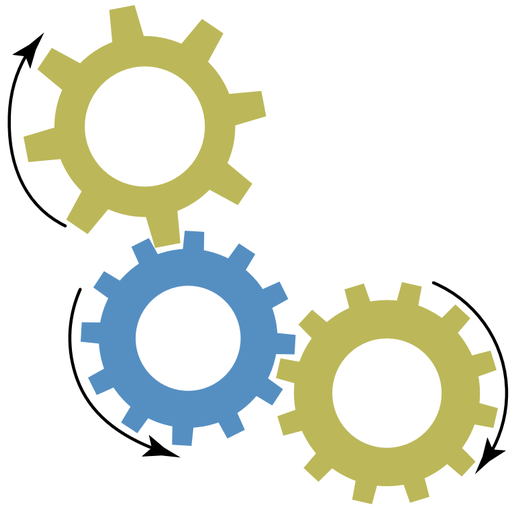
Hacktales

How security aware are employees/users?

At the heart of cybersecurity are the individuals who design, implement, and monitor defenses. These people are also the biggest risk, as human error, lack of awareness, and susceptibility to threats like phishing or social engineering often lead to security breaches. Building a security-conscious mindset and fostering continuous education are essential.

Pillar 11: Process

Hacktales



What policies and procedures govern business processes?

Effective cybersecurity relies on well-defined and consistently applied processes. Processes provide the blueprint for managing threats proactively, ensuring consistency, and maintaining compliance with regulations.

Pillar 111: Technology

Hacktales

What tools are in place to combat threats against systems, applications and data?

Technology serves as the toolkit for enforcing cybersecurity measures. Tools are critical for defending against evolving threats, but they are only as effective as the people managing them and the processes ensuring their proper use.

Hacktales

Got Questions?

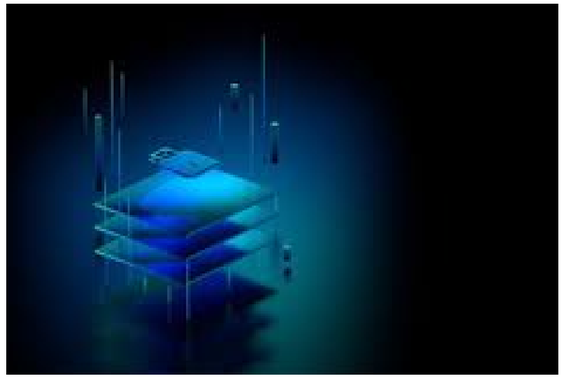
Cybersecurity Domains

Objectives

Hacktales

01

Evaluate the defense-in-depth strategy.



02

Review cybersecurity knowledge areas.

03

Analyze the technical and non-technical domains in cybersecurity.

Defense-in-depth

Hacktales

Defense-in-depth originated in the military era as a defensive strategy aimed to protect lives and properties within the castle.

Defense-in-depth

- **Administrative controls**

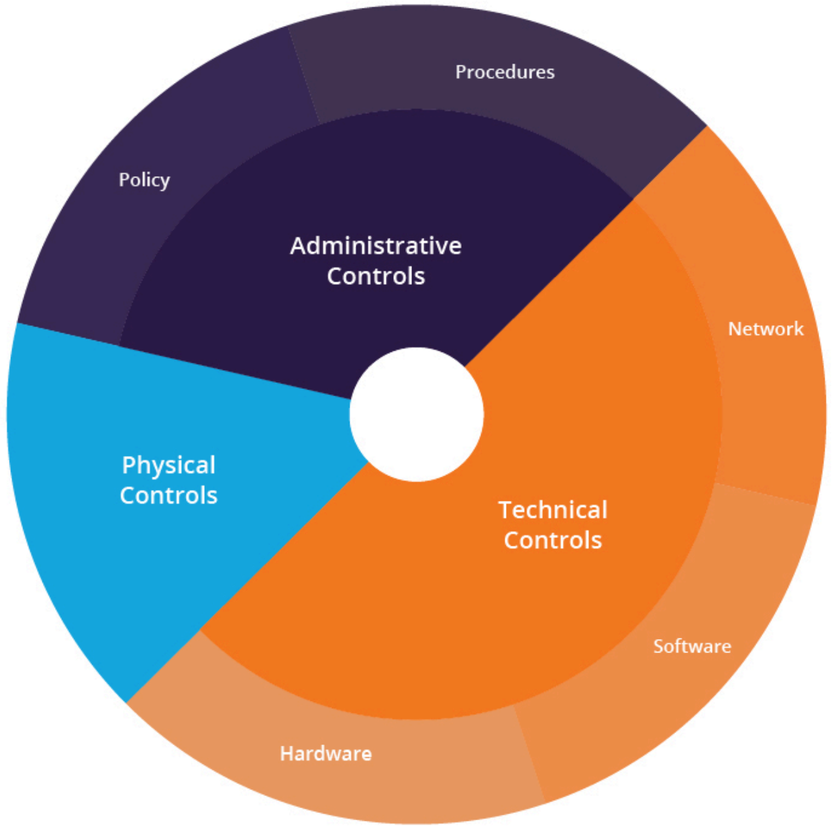
User training and awareness, clean desk policy and principle of least privilege.

- **Physical controls**

CCTV surveillance systems, access control, alarm systems and ID scanners.

- **Technical controls**

Antivirus, Two Factor Authentication (2FA) and Encryption.



Defense-in-depth

Hacktales

- **Perimeter (External Network)**

The secure boundary between an internal network and the internet.

- **Network (Internal Network)**

A private collection of computers accessible only by authorized individuals.

- **Hosts (Endpoints)**

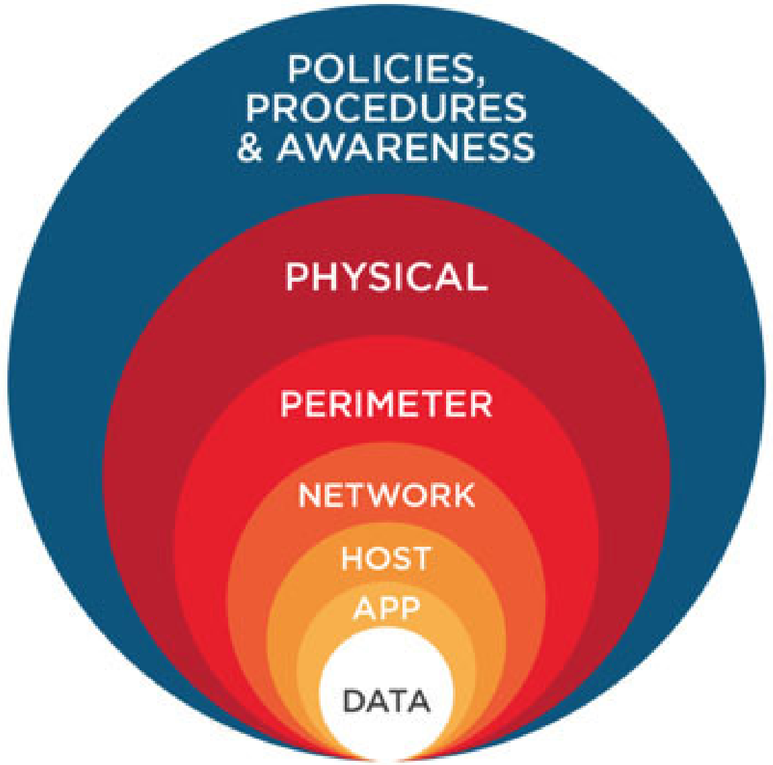
Any device that connects to a computer network.

- **Applications**

A computer software that performs specific functions or tasks.

- **Data**

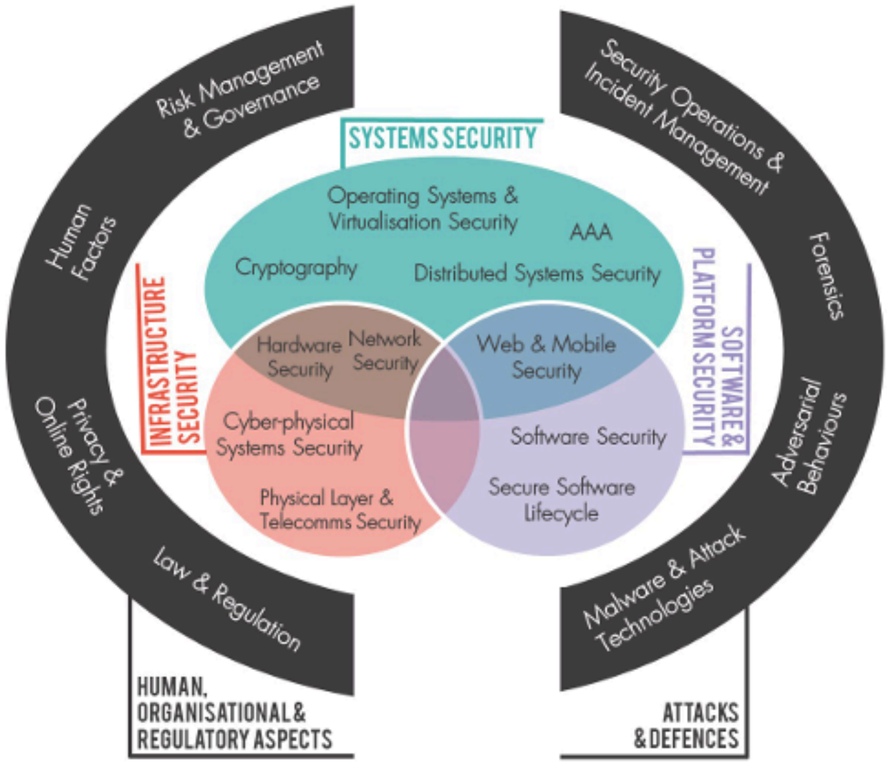
Information processed or stored by a computer.



Career Domains

There are five major knowledge areas within cybersecurity which include:

- Human, Organizational and Regulatory aspects
- Infrastructure Security
- System Security
- Software and Platform Security
- Attacks and Defenses



Source: CYBOK

Hacktales

Got Questions?

© 2025