

A vertical illustration of a human skeleton is positioned on the left side of the slide, extending from the top to the bottom.

Disclaimer

This Presentation is solely for the use at ZDFU public lecture organised by MoICT and Courier Services in the Cyber Security Awareness Month of November 2023. No part of it may be circulated, quoted, or reproduced for distribution outside the Ministry of ICT without prior written approval from Ministry of ICT and Courier Services. This material was used by Dr W Rukanda of MorniPac Digital Forensics during an oral presentation; it is not a complete record of the discussion.

A vertical illustration of a human skeleton on the left side of the slide.

Technology **O**wes **E**cology **a**n **A**pology

If you exchange information internationally, you must strengthen **Data Protection**

Maslow Hierachy of Needs



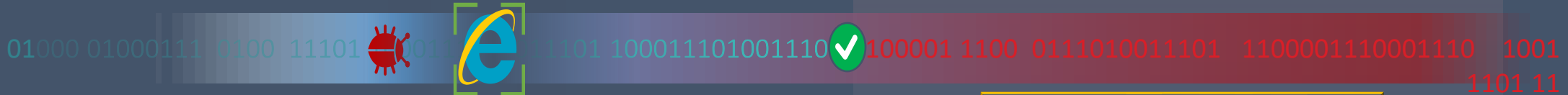
Vo WiFi



The Problem with Legacy Firewalls and IPS

Focus on the Apps...

...but miss the threat



Basic IPS Signature not matched

Legacy FWs can reduce attack surface area but advanced malware, APT, Polymorphic attacks often evades security controls.



Sometimes the chains that prevent us from being free are more mental than physical



**USER
THREATS**



**APPLICATION
THREATS**



**INFRASTRUCTURE
THREATS**



Table of Contents / Agenda

1

Nuggets

2

Quick Look and Zimbabwe

3

Cyber Crime / Cyber Security

4

Case Studies

5

Conclusion



**USER
THREATS**



**APPLICATION
THREATS**



**INFRASTRUCTURE
THREATS**





Disruptive Technologies

1

Digital Darwinism

Implies that organizations which cannot adapt to the new demands placed on them for surviving in the information age are doomed to extinction

2


Disruptive technology

A new way of doing things that initially does not meet the needs of existing customers

3

Sustaining technology

Produces an improved product customers are eager to buy

A vertical illustration of a human skeleton on the left side of the slide.


“Cyber crime is not an **anonymous victimless crime** as some believe. There should be real-world consequences to people’s actions in cyber space and the international activity on this nature of criminality,”

Some Nuggets

- OMG Cable
- Samsung Reset 500 times – falls off password
- OSINT – Open Source Intelligence (How do we access App, Gmail & etc)
- Dark Web (Visanet Transfer Issues)
- Checkpoint, ZONE H
- Bluetooth in Cars
- Tracking
- Platforms Aggregation (Middleware and BI Issues)
- AI, GenAI, Machine Learning, Cybercology and Metaverse
- Quantum Computing – Quantbits , megabytes
- POTRAZ – Incidence response center - Elon Musk - device
- ACT DPA – committees – Business – Funding
- RSA – SITA – ZITA.....



Cyber Crime

A vertical illustration of a human skeleton is positioned on the left side of the slide, extending from the top to the bottom.

Cyber-crime is typically understood to consist of accessing a computer without the owner's permission, exceeding the scope of one's approval to access a computer system, modifying or destroying computer data or using computer time and resources without proper authorization.

Cyber Security Policy

- A **poor cybersecurity policy can disrupt business continuity** making a cyber-attack more likely as defensive measures aren't in place. It can also make attacks worse as policies necessary for recovery aren't established and ultimately impact revenue and productivity, all of which affect the bottom line




Some Observations

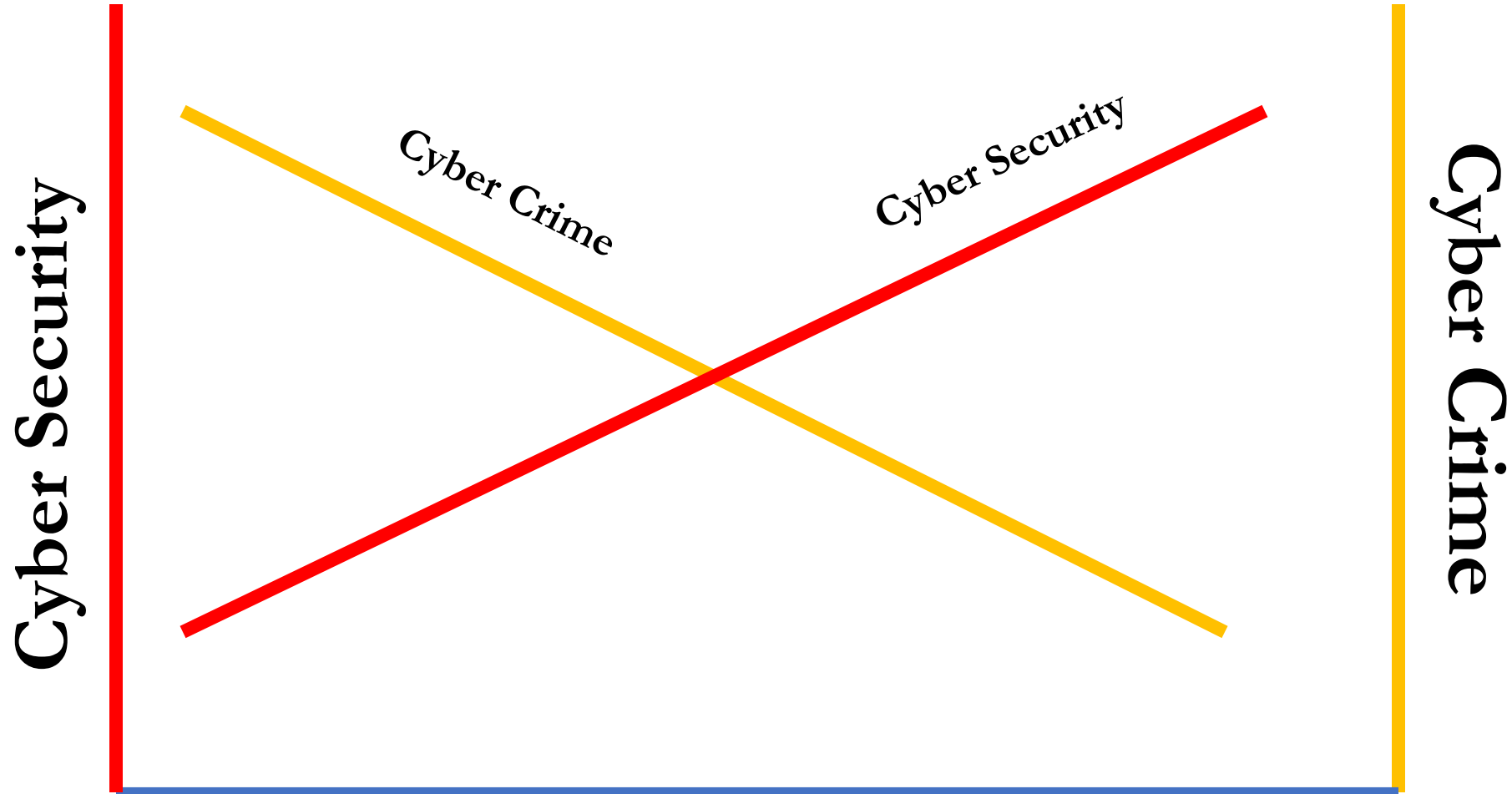
- ICT is one of the biggest issues
- ICT has become inherent in doing business
- Technology owing ecology an Apology
- ICT has significant ecosystem and crop yield impacts across the globe
- The evidence of ICT impact is unequivocal
 - Industry and Commerce
 - Government
 - Education
 - Community
 - various observations
- These are inter-related and constitute a major development , harnessing growth and / or sustainable development issue



Cybersecurity

- 
- A vertical illustration of a human skeleton is positioned on the left side of the slide, extending from the top to the bottom.
- **Cybersecurity** - has been of great importance in industry and commerce
 -
 - **Richness and Reachness** – Information Ubiquity
 - **Everyone** – e.g. seems to be going cashless, using digital money (**data privacy**)
 - **Banks and enterprise cybersecurity.** (to target, regulatory consequences – issues of VAPT & Cyber Exposure Assessment)

Graph - two sides of the same coin

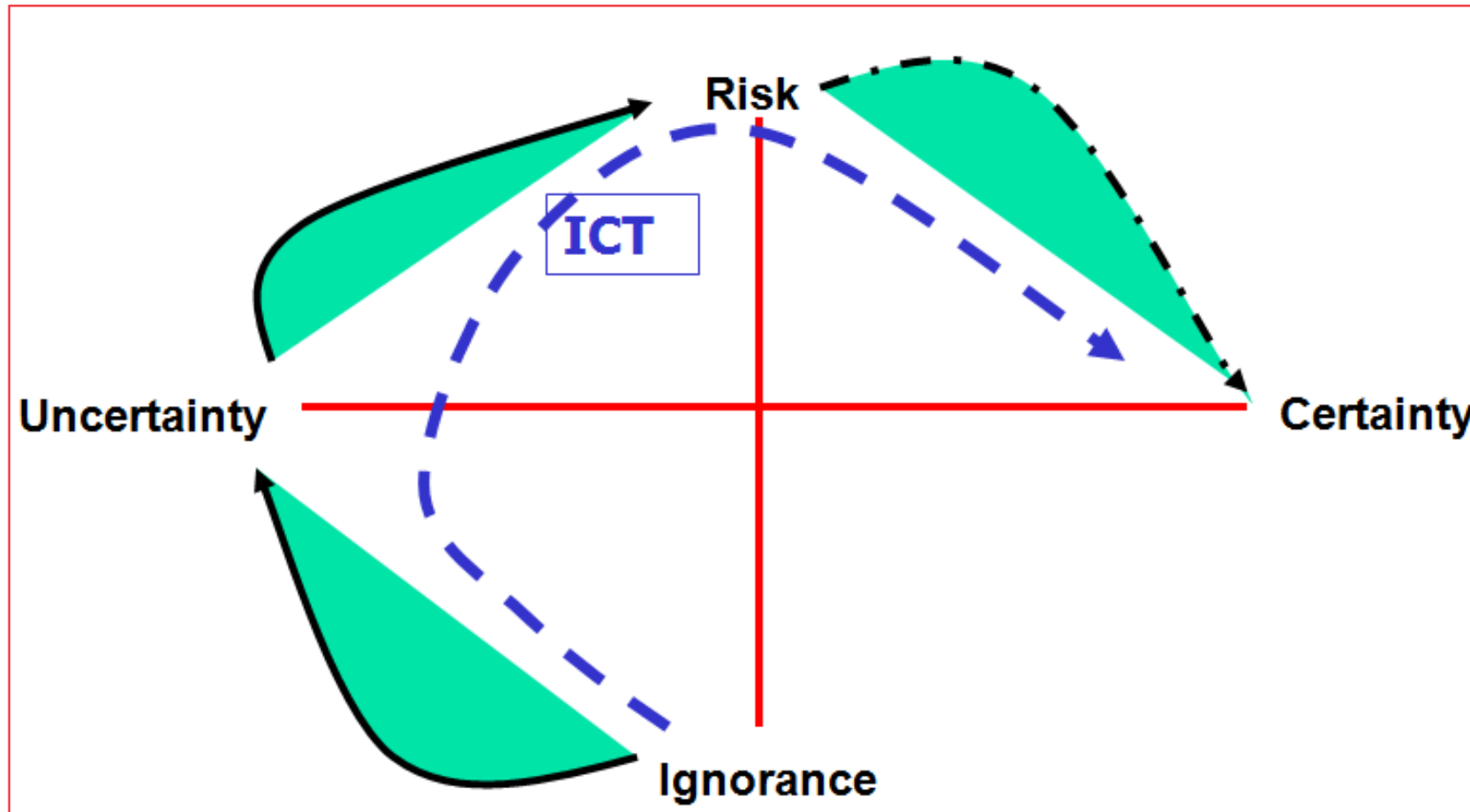


Decrease in broken software =
Increase in good software




Why Technology ?

ICT enhances the Quality and Timeliness of Decision Making



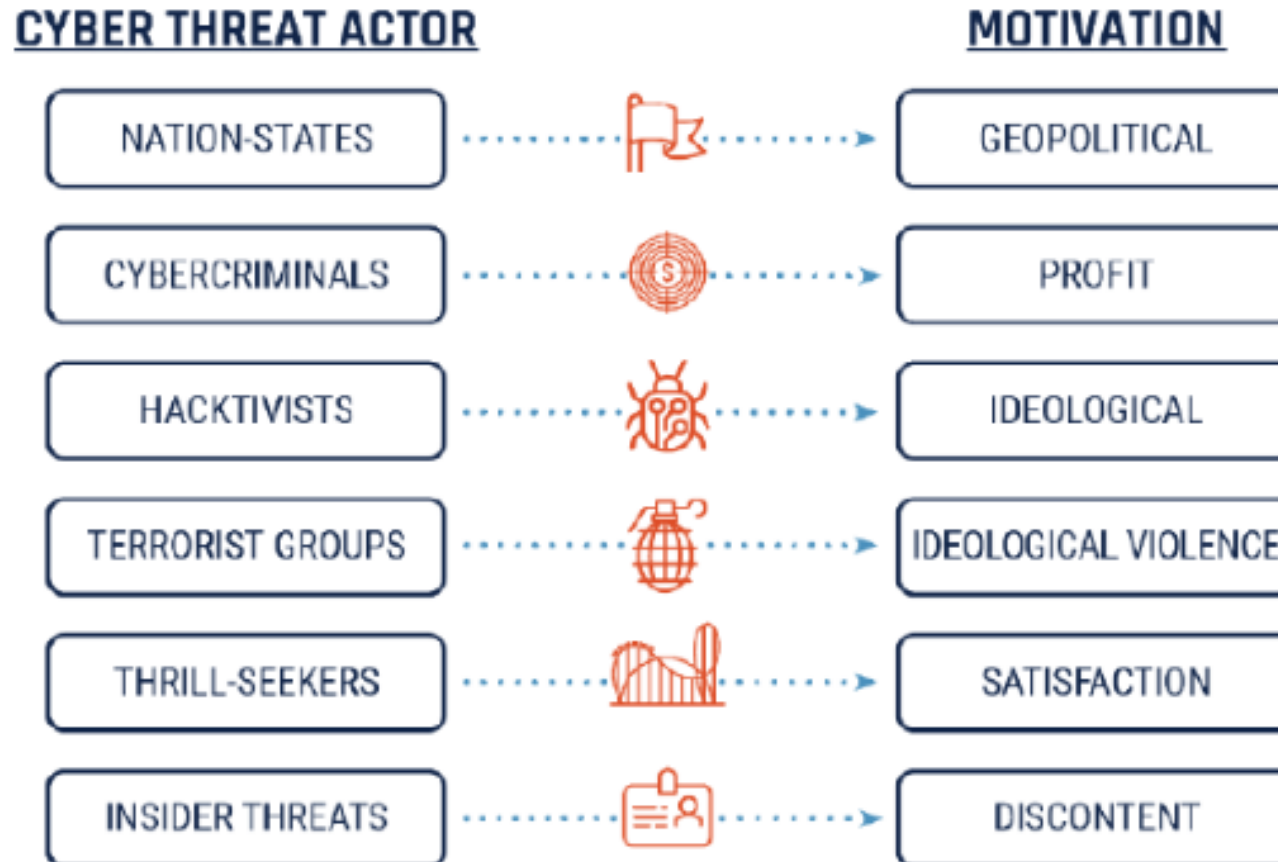
Cyber **C**rime and **B**usiness **D**isruption

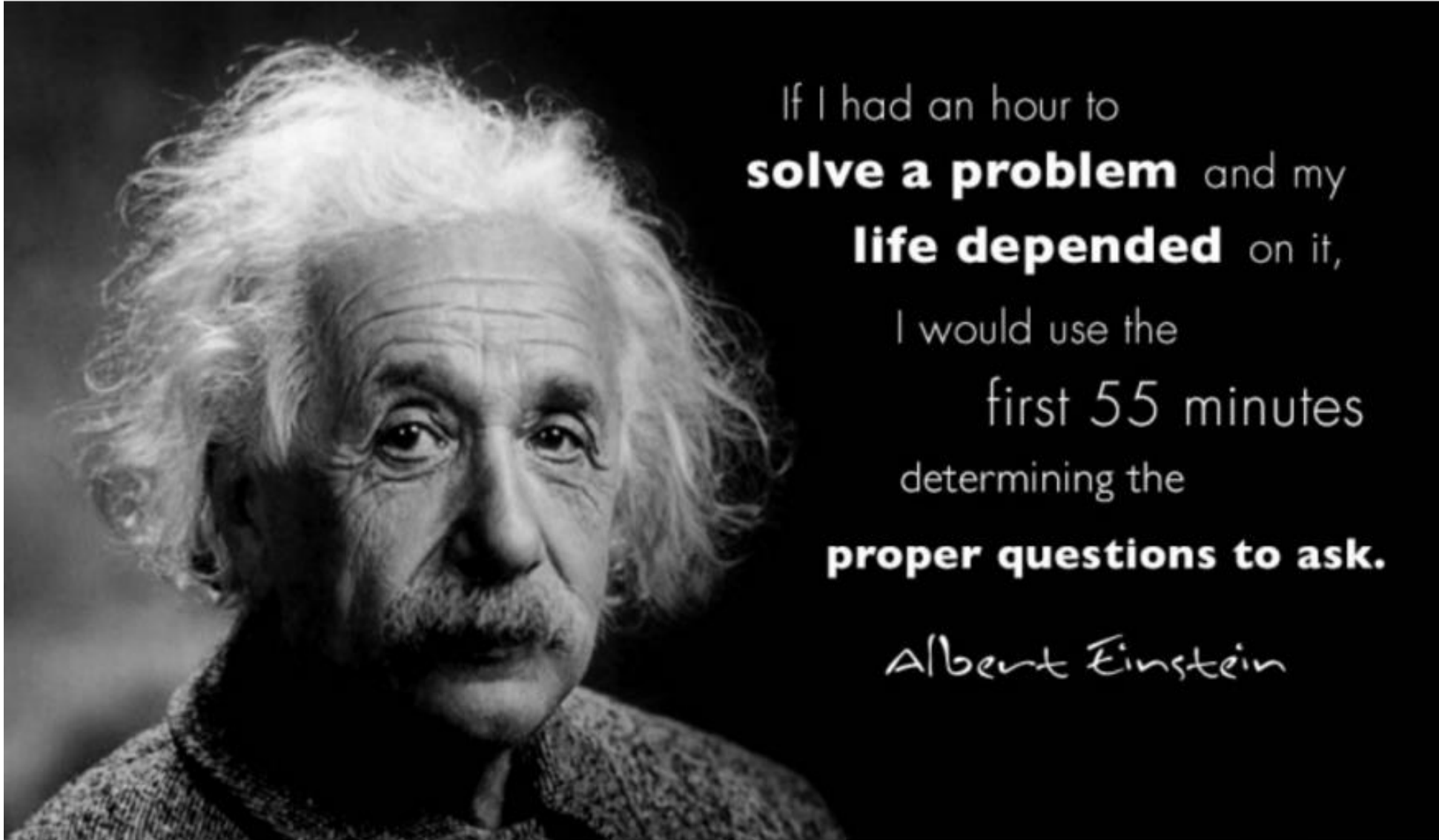
A vertical illustration of a human skeleton is positioned on the left side of the slide.

In addition to actual financial damages, companies often face indirect costs from cyberattacks, such as the possibility of a major interruption to operations that can result in lost revenue. Cybercriminals can use any number of ways to handcuff a company's normal activities, whether by infecting computer

Cyber Threat Actors

Cyber threat actors
(Courtesy of the Canadian Centre for Cyber Security [CCCS, n.d.])





6 **W**ays **C**yber **C**rime **I**mpacts **B**usinesses

- i. Increased Costs
- ii. Operational Disruption
- iii. Altered Business Practice
- iv. Reputational Damage
- v. Lost Revenue
- vi. Stolen intellectual Property



• THE END

• OF

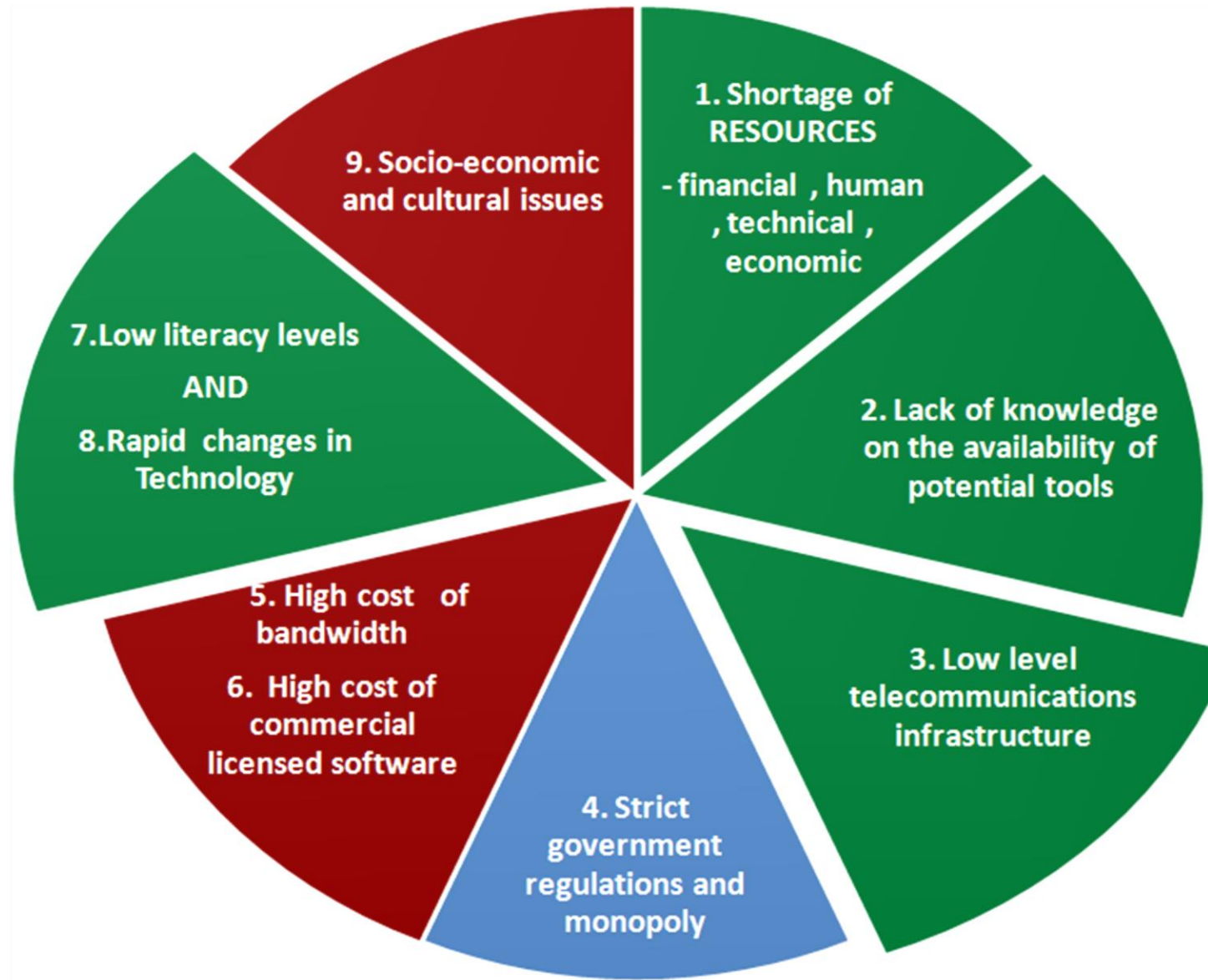
• NUGGETS



Brief Look at Zimbabwe



Factors Affecting ICT – Development in Zimbabwe



WHERE ZIM SHOULD BE

- Road Map
- Policy
- Skills Development
- Re-Skilling
- Implementation
- Security Improvement
- Stability
- Image and Perception
- ICT Opportunities & Openness
- ICT into Government
 - Education
 - All ministries
 - Performance indicators
 - FDI
 - Globalisation

ZIMBABWE POTENTIAL

- Available Tools
- Benefits
- Employment
- ICT Research
- Competitive Intelligence
- Economic Growth
- Global Village
- ERP & Automation
- Banking
- Communication
- Production
- Government Policy
 - Barriers
 - Bandwidth
 - Duty & Fees
- Internet
- Social Networks Effect

WHERE ZIMBABWE IS

- Banks & Banking Sector
- Telecoms
- Commerce
- Manufacture
- Mining
- Agriculture
- Communication & Contact
- Government
 - Education
 - Health
 - Transport
 - Security
 - Defence
 - Police



Some Cyber Crimes Common Modus Operandi

- Fraud (Card cloning micro chip abuse).
- Fraud alternatively Cyber crime (Hacking of bank accounts).
- Fraud OTP.
- Cyber crime with hacking and unlawful sim card replacement.
- Cyber crime with hacking of whatsApp accounts
- Cyber crime with hacking of Facebook accounts
- Cyber Crime with hacking of Websites
- Fraud and cyber enabled Pyramid or investment scams
- Fraud BEC



Cyber related cases investigated by CID CCD N/Region for period **1/01/23** to **7/11/23**

- ❑ Fraud (Card cloning) : **51**
- ❑ Fraud alternatively Cyber crime (Hacking of bank accounts): **05**
- ❑ Fraud OTP :**01**
- ❑ Cyber crime with hacking and unlawful sim card replacement:**06**
- ❑ Cyber crime with hacking of whatsApp accounts: **07**
- ❑ Cyber crime with hacking of Facebook accounts:**02**
- ❑ Cyber Crime with hacking of Websites: **02**
- ❑ Fraud and cyber enabled Pyramid or investment scams: **766+**
- ❑ Cyber bullying:**08**
- ❑ Fraud BEC :**03 TOTAL CASES: 848+**



Growth challenges in Zimbabwe

- Poverty alleviation
 - Almost half of the African population is living on less than \$1.25 dollar per day as at 2008 . For Zimbabwe its \$0.50 per day.
- Energy transition
 - Only about 31% of the population in Sub-Sahara Africa has access to electricity with about 14% electrification rate in the rural areas
- Economic growth and employment
 - The economic growth experienced in the last decade has failed to generate significant employment
- Infrastructure, urbanization and industrial development
- Political Challenges
 - Parties, Democracy, Political Risks
- FDI & World Bank Issues
 - Funding, Currency Issues, BOP Deficit, X-M position

Zimbabwe needs to grow in order to meet these challenges

Photo: Arthur Gilroy (online: SouthAfrica.to)



ICT SECURITY IDEAL STRUCTURE

BOARD COMMITTEE



BANK CEO

CHIEF INFORMATION
SECURITY OFFICER

ICT EXECUTIVE
&
DIGITAL STRATEGY

Information Security Assets

Security Operations & PM

Access Control

Application
Security

Operations &
Network
Security

BCP Planning
& Incident
Handling

Risk and
Compliance

Source Mapping

Protect, Shield, Defend, and Prevent Departments, Subfunctions, and Activities

Monitor, Hunt, and Detect Departments, Subfunctions, and Activities

Respond, Recover, and Sustain Departments, Subfunctions, and Activities

Govern, Manage, Comply, Educate, and Manage Risk Departments, Subfunctions, and Example Activities

CISO Function to Source Mapping

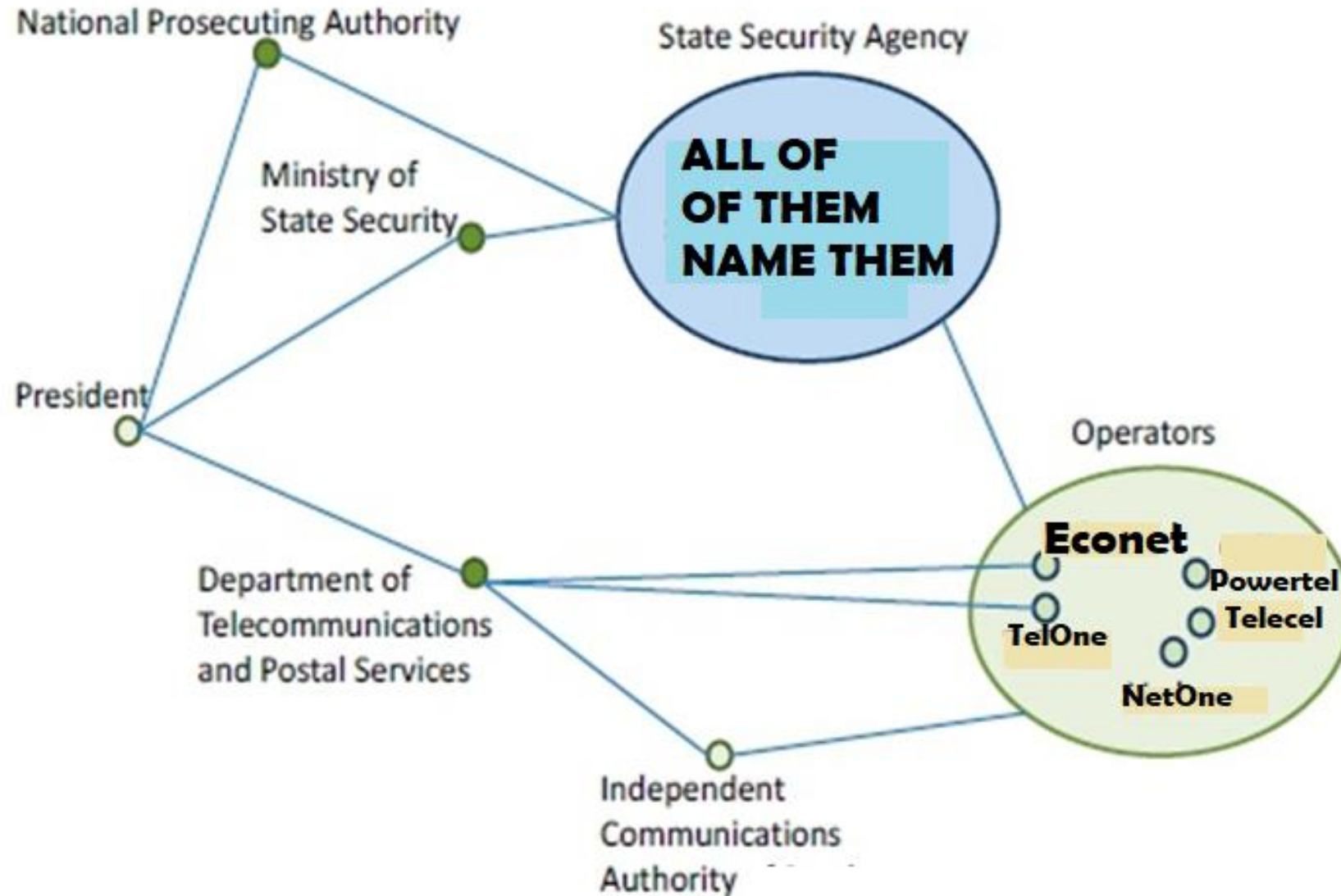


DISRUPTING NATIONAL SECURITY

All countries continue to encounter threats; the priority extends beyond organizational borders to include embracing innovative concerns, for instance, cyber-attacks, cyber-crimes, and additional internet-centered crimes (Oberheiden, 2021). Governmental authorities strive to shield and defend their perspective societies from disruptions owing to cataclysms or disasters. National security becomes the foreground of concern when one or more of a country's vital interests become predisposed to danger (Nobles, 2019). National Security Strategy examines the threats, appraises how to avert them, and what to do when a misfortune befalls. Particular to this is the disruption of national security. Any threat defies a country's

Example of a working Surveillance System

Surveillance System at WORK



Issues for you to SOLVE



- Ignorance of technology vulnerability
- Chaos and confusion – Mob mentality
- Hunger for more technology
 - From Google Glasses to Smart Glasses
 - Wrist tool
 - Automobile computers...etc
 - The more we have, the more we rely on it, the more vulnerable we become!
- **We want to trust the technology but cannot**
 - CANNOT trust any site, access or person
 - We act on emotion not thought
 - We cannot see the danger
 - Anti Virus protection is about 35% effective unless updated daily and then only 75%
- We are arrogant about what we want to do
- No or little compliance by businesses (COSO, SOX, GDPR)
 - Target...et. al.
- We seem not to learn from the past
- IPv6 – the future or not?
- Cyber Security Software (VAPT, SIEM, VAS, PAM)



Management Implications of Cybercrime

1. **Financial Losses:** Cybercrime can result in significant financial losses to organizations, such as theft of funds, loss of revenue, and damage to equipment or systems. Management must ensure robust cybersecurity measures to prevent cyber-attacks and minimize their impact on the organization's finances.
2. **Reputation Damage:** Cybercrime can damage an organization's reputation, decreasing customer trust and loyalty. Management must ensure effective communication strategies to manage the fallout from a cyber-attack and restore customer confidence.
3. **Legal and Regulatory Compliance:** Cybercrime can result in legal and regulatory violations, leading to fines, penalties, and legal liability. Management must comply with applicable laws and regulations, such as data protection and privacy laws, to avoid legal and regulatory consequences.
4. **Business Continuity:** Cybercrime can disrupt an organization's operations, leading to business downtime, decreased productivity, and loss of revenue. Management must have robust business continuity and disaster recovery plans to minimize the impact of cyber-attacks and ensure that the organization can quickly resume normal operations.
5. **Employee Morale:** Cybercrime can also affect employee morale, leading to increased stress, anxiety, and fear among employees. Management must provide a supportive work environment and ensure that employees are adequately trained on cybersecurity best practices to minimize the risk of cyber-attacks and mitigate their impact.

Overall, cybercrime poses a significant risk to organizations, and management must take proactive steps to mitigate these risks and protect their organization's assets, reputation, and employees.



Top business industries suffering cybercrime

Top Business Industries Suffering from Cybercrime (Ekran System, 2022; Manship, 2018)	
2022	2018
Public administration.	Business
Healthcare & pharmaceuticals	Healthcare/Medical
Finance & Insurance	Banking/Credit/Financial
Education & Research	Government/Military
Retail	Education
	Energy/Utilities

Which Cyber Security Certification Is Best?

1. (ISACA: CISM - Certified Information Security Manager.
2. EC-Council: CEH - Certified Ethical Hacker.
3. ISACA: CRISC - Certified in Risk and Information Systems Control.
4. ISACA: CISA - Certified Information Systems Auditor.
ISACA: CGEIT - Certified in the Governance of Enterprise IT.
- 5.(ISC)2: CCSP - Certified Cloud Security Professional
- 6.ISACA: CISA - Certified Information Systems Auditor
- 7.(ISC)2: CISSP-ISSMP - Information Systems Security Management Professional
- 8.(ISC)2: CISSP-ISSAP - Information Systems Security Architecture Professional
- 9.ISACA: CGEIT - Certified in the Governance of Enterprise IT
10. EC-Council: CHFI - Computer Hacking Forensic Investigator
11. CDFE – Certified Digital Forensic Expert
12. CCST - Certified Cyber Security Technician

Aug 28, 2021

4th Industrial Revolution

What is Happening?



The Way We Do Business



The Way We Calculate Metrics



The Way we Analyze Statistics



The Way we Meet Targets Changes

The Way we Work



Different Ideas Are Being Brought Together



The Way We Meet Our Goals



The Way We Travel Changes



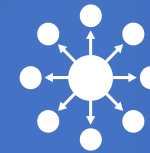
The Way We Communicate



The Way Our Hour Time Works



What We Do In The Hour



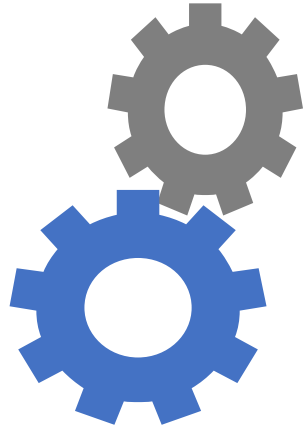
Different Technologies are Coming Together.

Past, Present

- Cyber security is a young and immature field
- The attackers are more innovative than defenders
- Defenders are mired in FUD (**fear, uncertainty & doubt**) & fairy tales
- Attack back is illegal or classified

Future

- Cyber security will become a scientific discipline
- Cyber security will be application and technology centric
- Cyber security will never be “solved” but will be “managed”
- Attack back will be an integral part of cyber security



• THE END

• OF

• NUGGETS



Why Cybercrime

- Passion of youngsters
- Desire of Making quick money
- Confidential information is online
- Negligence
- Loopholes in Systems
- Inaccessibility of criminals
- Lack of evidence



CyberCrime?



CYBERCRIME-AS-A-SERVICE (CAAS)

Akyazi et al. (2021) emphasized that as cybercrime becomes business as usual, it is essential to understand the cyber-attack value chain and its demand. CaaS would not exist without customers demanding malicious cyber services (Akyazi et al., 2021). The supply and demand for CaaS are critical and highlight the evolving cybercrime landscape (Akyazi et al., 2021) and the structuring by malicious actors to provide illegitimate services. The ascendancy of cloud computing enables illicit parties to flatten the support hierarchy and capitalize on the positive aspects of cloud computing.

Due to the internet, cybercrime continues to change and grow and has transformed into a highly beneficial, profitable, and systematized business under CaaS (Akyazi et al., 2021). When utilizing the *as-a-service business* model, cybercriminals provide their skills, services, and hacking tools to everyone prepared with payment, whether the total price or a divided revenue (Balito-Centeno, 2021). Names of CaaS include CAPTCHA solvers, Phone/SMS verification, E-whoring, Proxies, and Remote Desktop Protocol (RDP).

CaaS, operating on the dark web, expresses a prepared organizational model wherein cybercriminals, malware developers, and other bad actors offer payment cybercrime services to consumers (Akyazi et al., 2021). CaaS allows for the easy launching of cyberattacks or contribution to some level of cybercrime by interested parties. Do customers need technical knowledge? No, customers do not need to gain specialized technical knowledge, including coding skills. Because CaaS providers offer the underpinnings compulsory to swiftly launch a fruitful cyberattack with minimal effort. This cybercrime network provides expert help, for instance, code development for malware and exploit kits created to influence a particular susceptibility.



Types of Cybercrime

As technology advances, cybercrime evolves when malicious actors capitalize on the digital sphere by pursuing nefarious activities. Below is a list of cybercrimes (Batra et al., 2020; Deora & Chudasama, 2021)


1. Phishing
2. Identity theft
3. Hacking systems and websites
4. Child pornography
5. Cyber grooming
6. Copyright violations
7. Selling illegal items
8. Soliciting/producing child pornography
9. Financial theft
10. Cyberstalking
11. Business email compromise

According to Morgan (2020), cybercrime includes:

Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm



Who Commits Financial Crime

- 
- A vertical illustration of a human skeleton is positioned on the left side of the slide, extending from the top to the bottom.
- There are essentially **seven groups of people who commit** the various types of financial crime:
 - i. Organized criminals, including terrorist groups, are increasingly perpetrating large-scale frauds to fund their operations.
 - ii. Business leaders or senior executives manipulate or misreport financial data in order to misrepresent a company's true financial position.
 - iii. Employees from the most senior to the most junior steal company funds and other assets.
 - iv. From outside the company, fraud can be perpetrated by a customer, supplier, and contractor or by a person with no connection to the organization.
 - v. Corrupt heads of state may use their position and powers to loot the coffers of their (often impoverished) countries
 - vi. Increasingly, the external fraudster is colluding with an employee to achieve bigger and better results more easily.
 - vii. Finally, the successful individual criminal, serial or opportunist fraudsters in possession of their proceeds are a further group of people who have committed financial crime

What are the main types of Financial Crime?

- Financial crime is commonly considered as covering the following offences:
- Fraud
- Electronic Crime
- Money Laundering
- Terrorist Financing
- Bribery And Corruption
- Market Abuse And Insider Dealing
- Information Security




Types and Modes of Cyber Attack

Types of Hacker Attack


- Cyber Fraud
- Cyber Spying
- Cyber Heist
- Cyber Stalking
- Cyber Bullying
- Cyber Assault
- Cyber Warfare
- Cyber Extortion



Types of Hacker Attack

- 
- Crisis
 - Computer Crimes
 - Hacker Attacks
 - **Modes of Computer Security**
 - Password Security
 - Network Security
 - Web Security
 - Distributed Systems Security
 - Database Security
 - **Active Attacks**
 - Denial of Service
 - Breaking into a site
 - Intelligence Gathering
 - Resource Usage
 - Deception
 - **Passive Attacks**
 - Sniffing
 - Passwords
 - Network Traffic
 - Sensitive Information
 - Information Gathering

CYBER CRIMES PERCENTAGE



➤ Financial fraud.	11%
➤ Sabotage of data	17%
➤ Information theft	20%
➤ System penetration from outside	25%
➤ Denial of service	27%
➤ Unauthorized access by insiders	71%
➤ Employee abuse of internet privileges	79%
➤ Viruses	85%

The Cost of a Breach (and Other Cyber Events)

Direct Costs

- Discovery/Data forensics.
- Notification costs.
- Identity monitoring costs.
- Real-time crisis management costs.
- Additional security measures, remediation.
- Lawsuits.
- Regulatory fines.

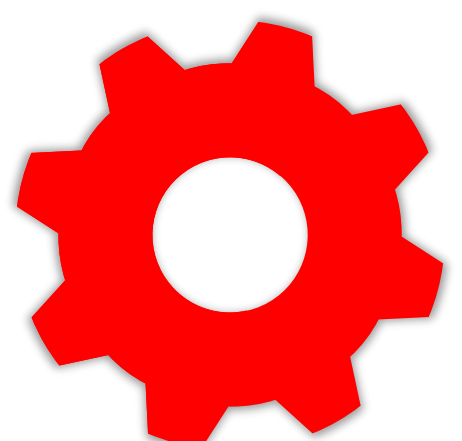
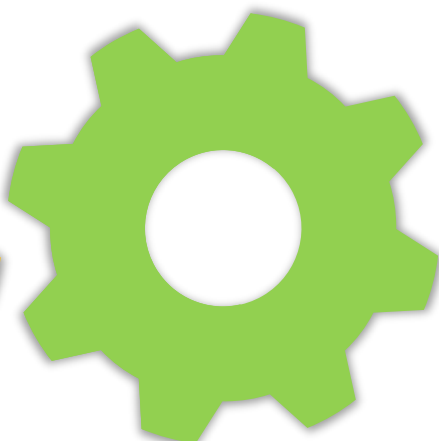
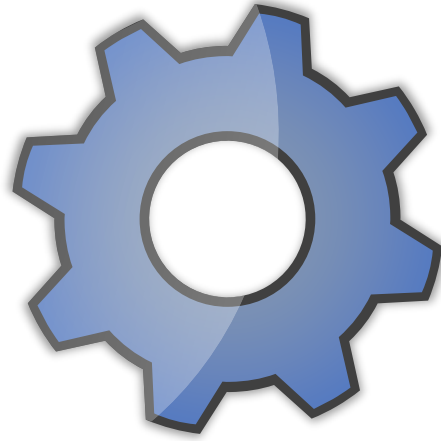
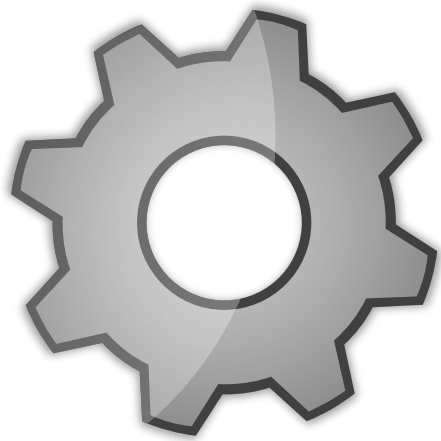
Indirect Costs

- Loss of customer confidence.
- Executive management distraction from core business objectives.
- Loss of employee productivity.
- Lost sales.
- Higher customer acquisition costs.
- Lower stock price.
- Loss to reputation/brand.

Similar Costs for other Cyber Events = Reputational Risk



Modes of Computer Security



Password
Security

Network
Security

Web Security

Distributed
Systems
Security

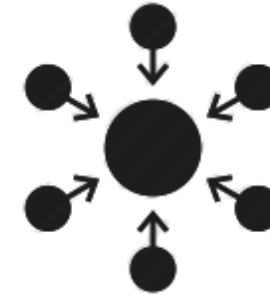
Database
Security



4th Industrial Revolution

What's happening?

Different technologies are **coming together**
(convergence)



This is bringing different areas together



This affects social & economic sectors

The way we work, buy
and sell things



The way we travel



The way we live



10 corporate cyber security risks to prepare for



1. Failure to cover cyber security basics
2. Not understanding what generates corporate cyber security risks
3. Lack of a cyber-security policy
4. Confusing compliance with cyber security
5. The human factor – the weakest link
6. Bring your own device policy (BYOD) and the cloud
7. Funding, talent and resources constraints
8. No information security training
9. Lack of a recovery plan
10. Constantly evolving risks
11. Aging infrastructure
12. Corporate inflexibility
13. Lack of accountability
14. Difficulty in integrating data sources
15. Holding on to a reactive mindset
16. Disconnect between spending and implementation










Internet of Everything Internet of Things

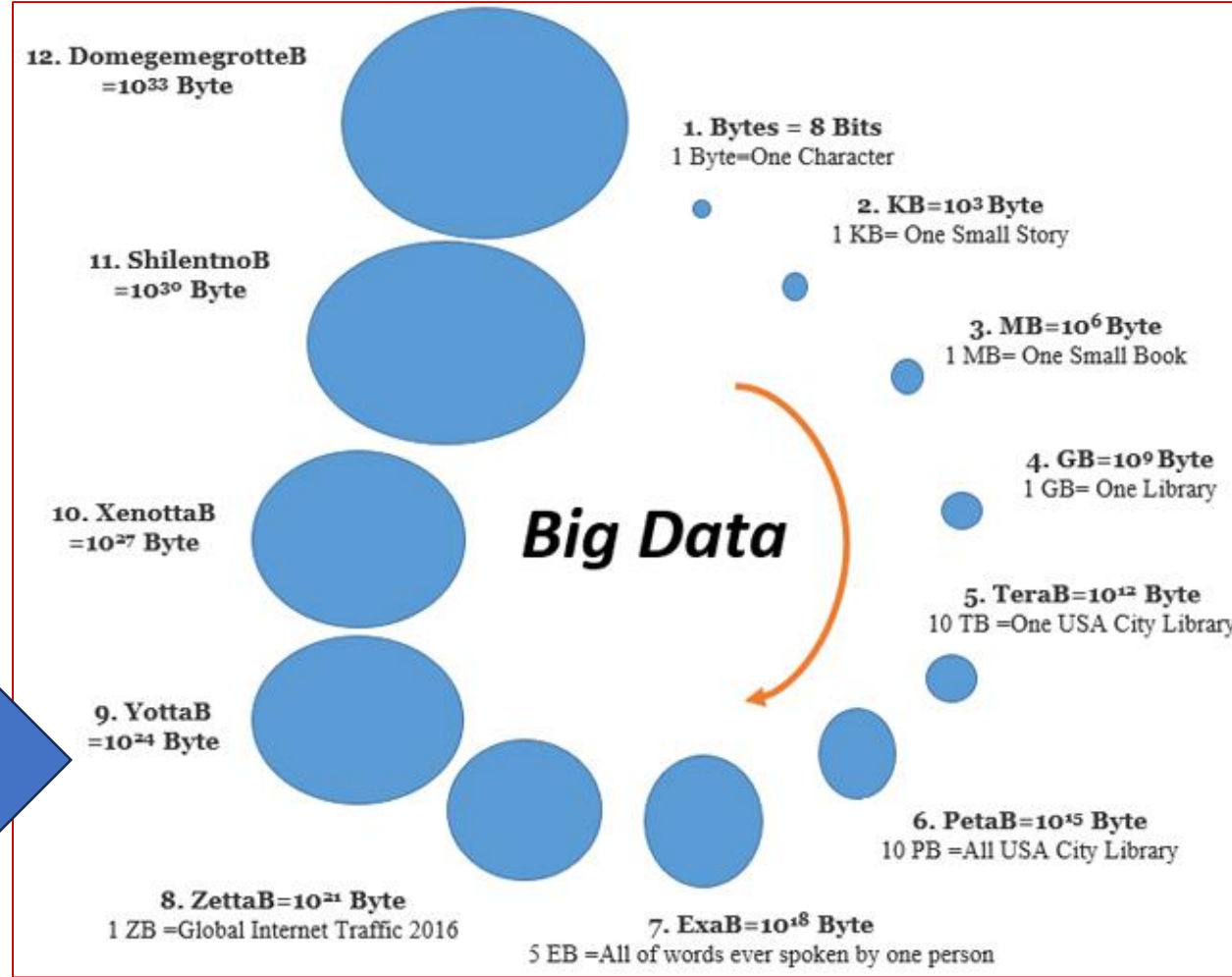
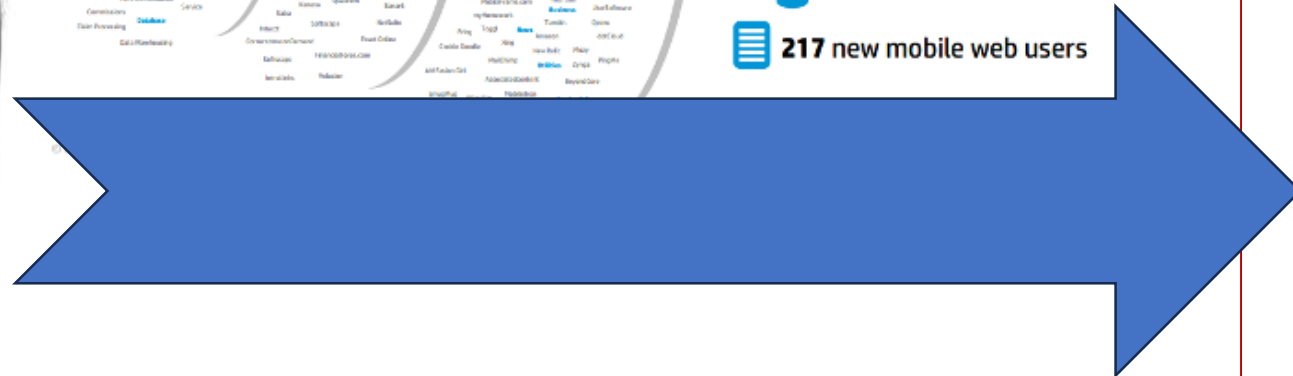
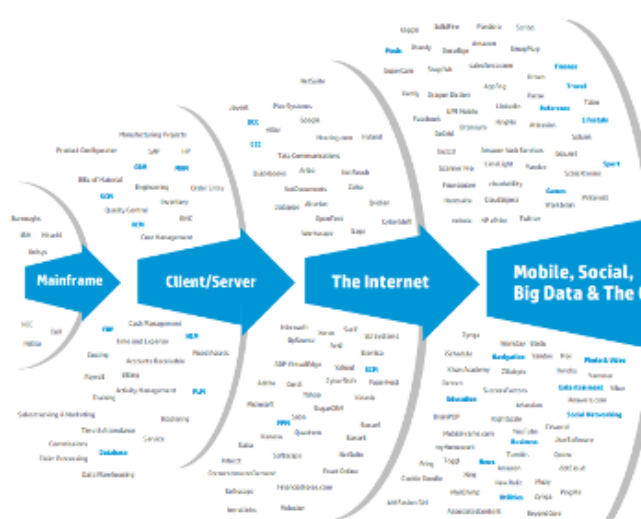
Every 'Thing' is Connected





Every 60 seconds

-  **98,000+** tweets
-  **695,000** status updates
-  **11 million** instant messages
-  **698,445** Google searches
-  **168 million+** emails sent
-  **1,820TB** of data created
-  **217** new mobile web users



How Big Data is Revolutionising the World



Cybercrime-as-a-service: The Naughty Nine

Access-as-a-service

Gaining access to compromised accounts and systems in bulk through RDP and VPN credentials, web shells, and exploitable vulnerabilities

Malware-as-a-service

Facilitating the distribution of malware within specific regions or sectors with watering-hole attacks, crossover with access-as-a-service listings, and other vulnerabilities

Phishing-as-a-service

How threat actors are offering end-to-end services for cloned sites, hosting, emails to bypass spam filters, and other phishing campaigns

OPSEC-as-a-service

Bundled services provided by threat actors designed to hide Cobalt Strike infections to minimize the risk of detection

Crypting-as-a-service

Common on many forums, crypting as a service involves the use of encrypted malware to bypass detection for a one-time purchase or subscription

Scamming-as-a-service

Designed as classified ads, scamming kits and services help threat actors pose as support specialists for cryptocurrency scams

Vishing-as-a-service

How threat actors offer to rent voice systems to receive calls where victims opt out and speak to a bot, rather than a human

Spamming-as-a-service

Infrastructure designed to build or manage bulk spamming services through a variety of mechanisms, including SMS and email

Scanning-as-a-service

Offering access at discount prices for legitimate commercial tools such as Metasploit and Burp Suite to find and exploit vulnerabilities



Cyber Crime and Business Disruption

- the most important ways cybercrime can hamper businesses today.
- **KEY TAKEAWAYS**
- About 6% of companies report having to pay a ransom to regain control of critical IT systems.
- Businesses that come under cyberattack also incur higher costs from operational disruption and altered business practices.
- The biggest losses come from reputational damage. Companies that have lost control of their customers' data have paid millions to settle claims



BUSINESS **D**ISRUPTION



Increased Costs

- **1. Increased Costs**
- Companies that want to protect themselves from online thieves have to pull out their wallets to do so. Firms may incur any number of outlays, including:
 - Cybersecurity technology and expertise
 - Notifying affected parties of a breach
 - Insurance premiums
 - Public relations support
- **Ransomware**, which can prevent workers from accessing IT systems unless the company pays off a hacker, can also create a major financial burden. According to Hiscox, 6% of companies paid a ransom in 2019, creating \$381 million in losses.¹
- In addition, businesses may have to hire lawyers and other experts to remain compliant with cybersecurity regulations. And if they're the victim of an attack, they may have to shell out even more for attorney fees and damages as a result of civil cases against the company.



Data Breaches

- Equifax, one of the [top three credit bureaus](#), learned this the hard way after a 2017 data breach that compromised the personal data of 147 million customers. As a result of subsequent litigation, the company agreed to pay up to \$425 million to assist affected individuals. [2U.S. Federal Trade Commission. "Equifax Data Breach Settlement."](#)



6 Ways Cyber Crime Impacts Businesses

• 2. Operational Disruption

- In addition to actual financial damages, companies often face indirect costs from cyberattacks, such as the possibility of a major interruption to operations that can result in lost revenue.
- Cybercriminals can use any number of ways to handcuff a company's normal activities, whether by infecting computer systems with malware that erases high-value information, or installing malicious code on a server that blocks access to your website.
- Disrupting business as usual is the favored tool of so-called "[hacktivists](#)," who have been known to breach the computer systems of government agencies or multinational corporations in the name of calling out a perceived wrong or increasing transparency.
- In 2010, for example, hackers sympathetic to WikiLeaks retaliated against credit card giants [Mastercard](#) and [Visa](#) by conducting attacks that temporarily crashed their websites.³
-



6 Ways Cyber Crime Impacts Businesses

- **3. Altered Business Practices**
- Cybercrime can impact businesses in more than just financial ways. Companies have to rethink how they collect and store information to ensure that sensitive information isn't vulnerable. Many companies have stopped storing customers' financial and personal information, such as credit card numbers, [Social Security numbers](#), and birth dates.
- Some companies have shut down their online stores out of concern they cannot adequately protect against cyberattacks. Customers are also more interested in knowing how the businesses they deal with handle security issues, and they are more likely to patronize businesses that are up front and vocal about the protections they have installed.



6 Ways Cyber Crime Impacts Businesses

• 4. Reputational Damage

- Although tough to fully quantify, companies that fall victim to larger cyberattacks may find their [brand equity](#) significantly tarnished. Customers, and even suppliers, may feel less secure leaving their sensitive information in the hands of a company whose IT infrastructure was broken at least once before.
- Retail giant Target ([TGT](#)) saw its reputation take a hit after a 2013 data breach involving the credit card information of more than 40 million customers, a security failure that cost it \$18.5 million to settle.
- JPMorgan Chase & Co. ([JPM](#)) endured a similar black eye in 2014, when criminals compromised the data of its banking customers. Hackers gained access to the names, addresses, phone numbers, and email addresses of 76 million household accounts and seven million small business accounts.
- In addition to reduced institutional trust, research suggests that publicly traded companies are likely to see a short-term drop in market value. Security researchers Comparitech studied 40 data breaches at 34 companies listed on the [New York Stock Exchange](#). It found that the share prices of compromised companies fell an average of 3.5% following an attack, and underperformed the Nasdaq by 3.5%.⁶[Comparitech. "How Data Breaches Affect Stock Market Share Prices."](#)

•



6 Ways Cyber Crime Impacts Businesses

- **5. Lost Revenue**
- One of the worst outcomes of a cyberattack is a sudden drop in revenue, as cautious customers move elsewhere to [protect themselves against cybercrime](#). Companies can also lose money to hackers who try to extort their victims.
- Case in point: **Sony Pictures came under attack in 2014** as it prepared to release “The Interview,” a comedy which depicted an assassination attempt on North Korean leader Kim Jong Un. Hackers pilfered sensitive information, including embarrassing e-mails and performance evaluations from its staff.
- North Korea is widely believed to be behind the attack, although it denied the allegations. As a result, Sony Pictures pulled the film from most theaters in favor of an online release, a move that cost it \$30 million, according to the National Association of Theater Owners.



6 Ways Cyber Crime Impacts Businesses

- **6. Stolen Intellectual Property**
- A company's product designs, technologies, and go-to-market strategies are often among its most valuable assets. Intangible assets accounted for 87% of the value of S&P 500 companies in 2015, according to intellectual property advisory Ocean Tomo.
- Much of this intellectual property is [stored in the cloud](#), where it's vulnerable to cyberattacks. Nearly 30% of U.S. companies report having their intellectual property stolen by a Chinese counterpart within the past 10 years. [8CNBC. "CNBC Global CFO Council Survey, Q1 2019."](#)

-



POS Vulnerability

Tap-to-Pay (NFC)

BYOD Infection

**Security on
mobile devices**

Beacon Tracking

**Reasons
Why Cyber Attacks
Hit Retailers**

**Antiquated
Systems**

Hacked QR Codes

Multi-channel

Hacker Customer

Cyber attack case studies on Law firms

2017



2015



2016

APPLEBY

2014

Booz
Allen



CRAVATH

WEIL
GOTSHAL

Wiley
Rein
LLP



CASE STUDIES OF CYBER ATTACKS ON RETAIL INDUSTRY

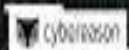


CASE STUDIES ON TELECOMS COMPANIES

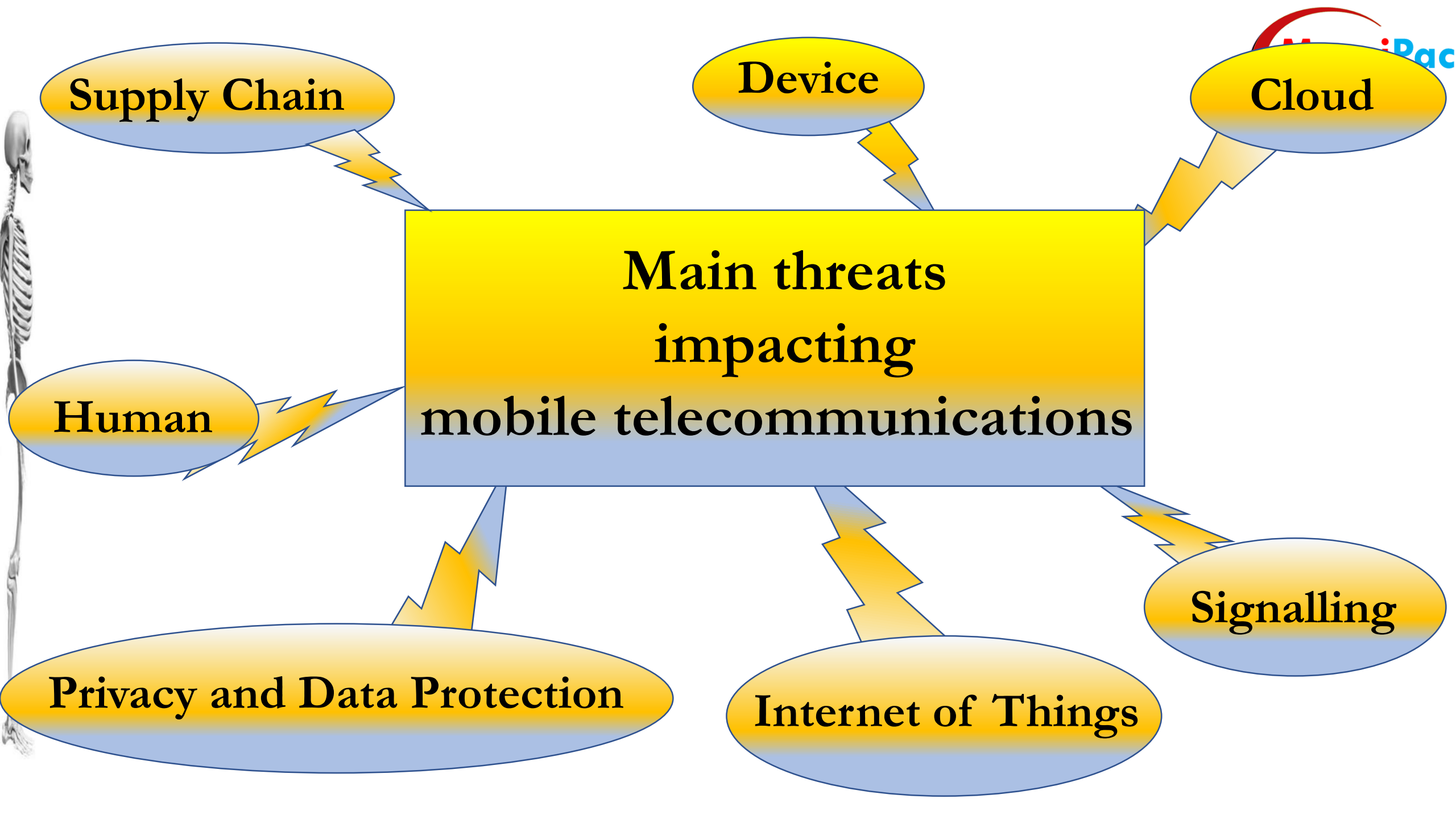


Encrypted email, based in Switzerland.

OPERATION
SOFT CELL



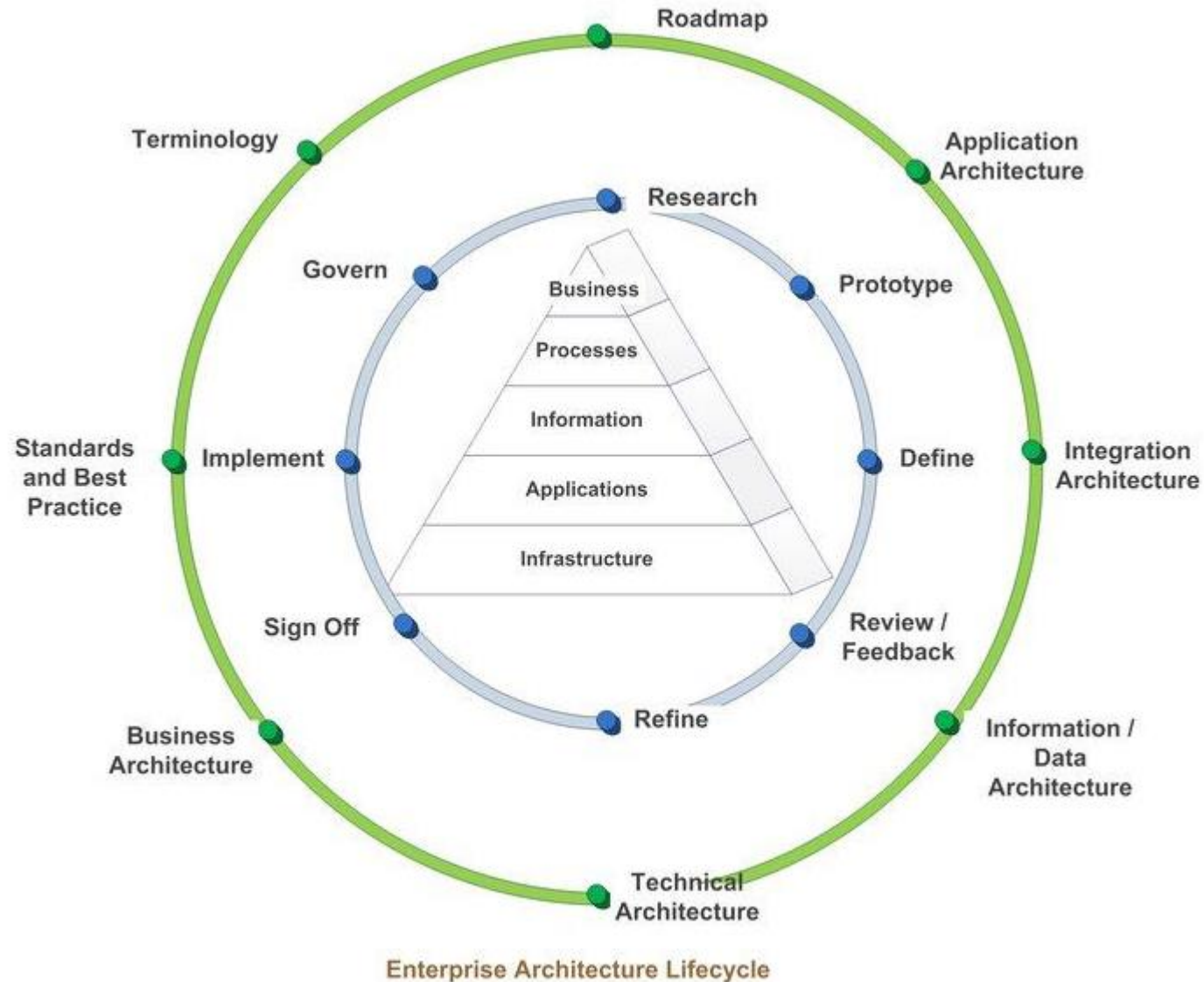
TalkTalk






Threat	ID Verification	Biometrics & Liveness	Anomaly Detection	Simulated Attacks	Backup & DRaaS	Employee Training
Identity Theft	✓	✓	✓			✓
Account Takeover	✓	✓	✓			✓
Synthetic Fraud	✓	✓	✓	✓		✓
Ransomware				✓	✓	✓
Social Engineering	✓	✓		✓		✓

Key Information Security Areas



Some Key ICT Security Challenges

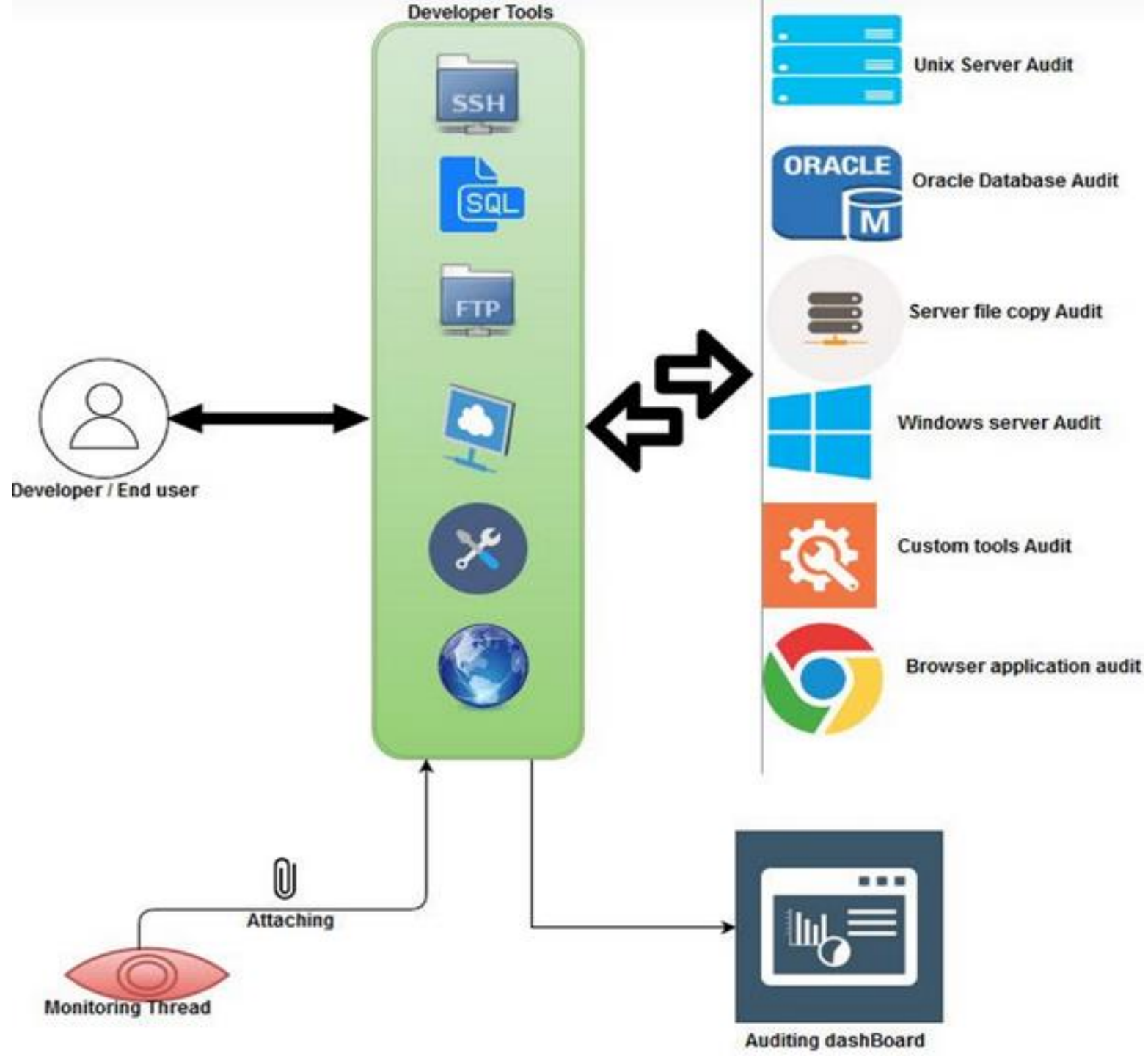
- 
- A vertical illustration of a human skeleton is positioned on the left side of the slide.
- There is no end to end monitoring(eg: OS, Network, Database)
 - No user monitoring of who is doing what Performance degrade -when enabling Audit
 - No control on the data copy and stealing from database/server
 - No alert on suspicious activity
 - No control on user actions VS details given on change/incident systems
 - No automated password rotation
 - No firewall restriction/Any one can login from any server
 - No view on who has access to which server Compliance / Risk control

- Most Policies are Not Signed
- Some Policies, Rules, Standards and Guidelines Still under Development
- No Signed Data Policy
- No comprehensive UAP
- Policies not operationalised (no DR Servers)
- Data not clean
- No Staff Skills Matrix
- No Segregation of Duties





Solution Architecture



Conclusion

A vertical illustration of a human skeleton is positioned on the left side of the slide, extending from the top to the bottom.

CONCLUSION

Cybercrime as a sustained business is a universal concern for governments and companies. Cybercriminals continue to outmaneuver and out-strategize organizations to seize the tactical advantage by capitalizing on crossing jurisdictional boundaries to engage in illicit behavior and activities. The upward trend in cybercrime stems from the lack of a standardized definition and legal disparities across international borders. Organizations rely significantly on emerging technologies to advance business efforts or provide government services; consequently, cybercriminals exploit human and technological vulnerabilities to access sensitive information, intellectual property, financial resources, and critical infrastructure.