CY – 824

Cyber Security – Fundamentals with tools and techniques for defense

Cyber Security – Foundation Module

Part 1

What is Cyberspace?

A global domain within the information environment consisting of the interdependent network of information system infrastructures including the

internet,

telecommunications network,

computer systems and

embedded processor & controllers

SCADA/DCS etc.

What is Cyber Security?

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks.

Also known as Information Technology (IT) security (InfoSec)

Cyber security measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization

Cyber Defence

The ability to protect or defend the use of cyberspace from cyber attacks.

It involves protecting everything that can be accessible through cyberspace and **everyone** who is vulnerable …

From: Mail Delivery System <Keusink@keusink.net>
Date: Friday, 27 October 2023 at 2:18 AM
To: Mohan Ram Chandrasekar <mrc@fisstacademy.com>
Subject: Your storage is Full

This is a mandatory service communication

Storage is Full

Your storage space is completely full on **Thursday October 2023**
You must immediately free some space in order to send and receive messages.

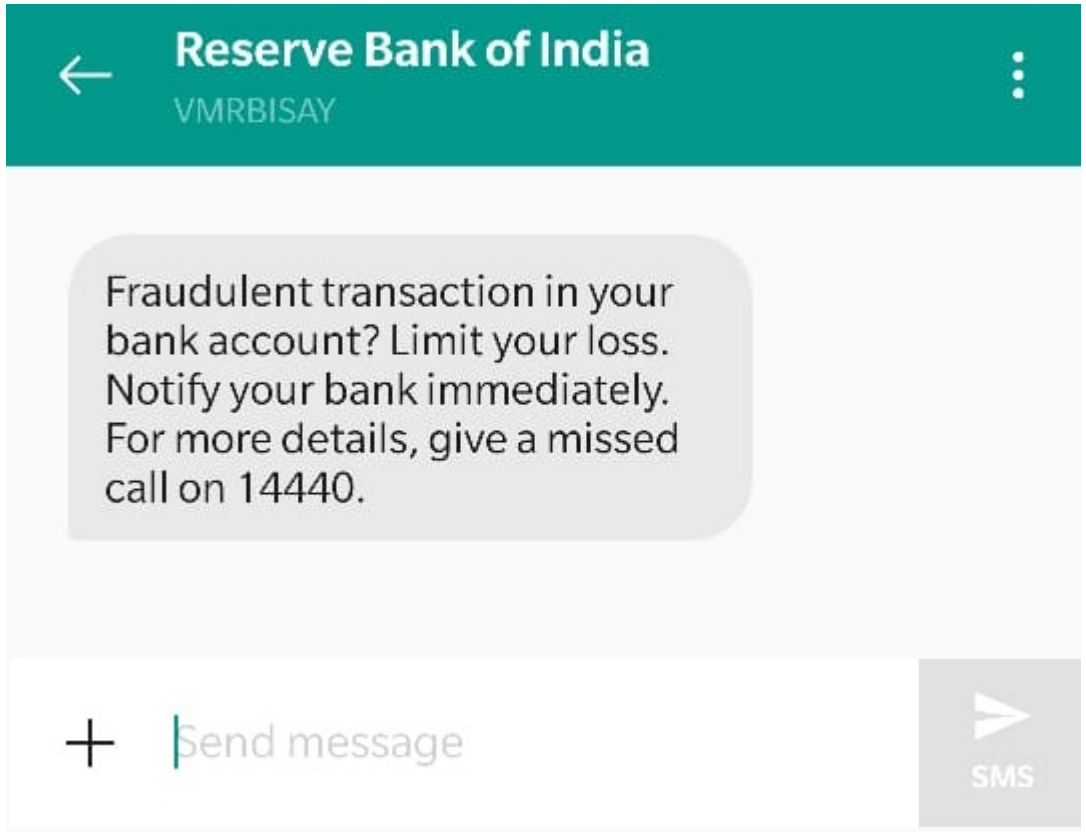
Free Up Space

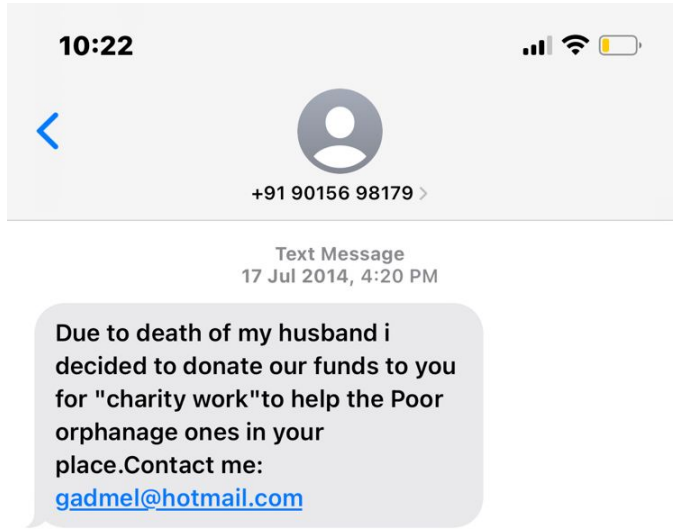
Attention: Action is required on **26/Oct/2023**

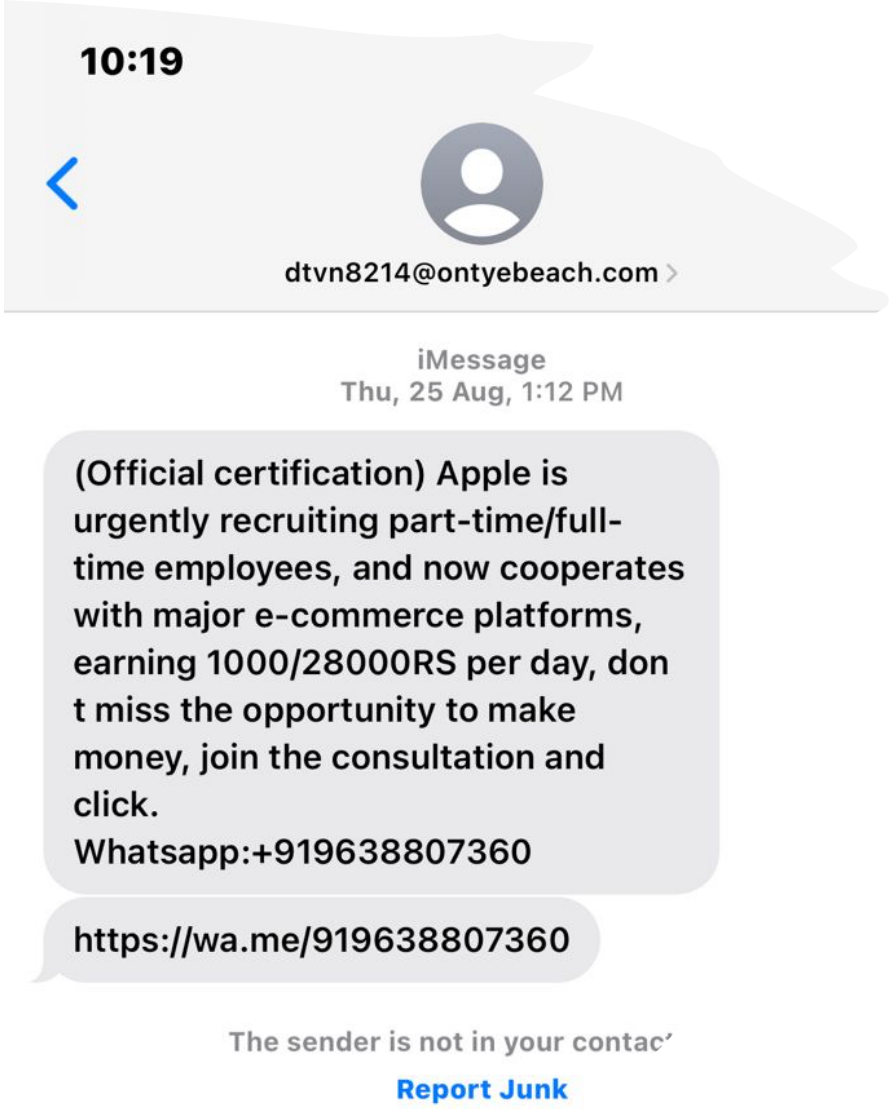
Account Information

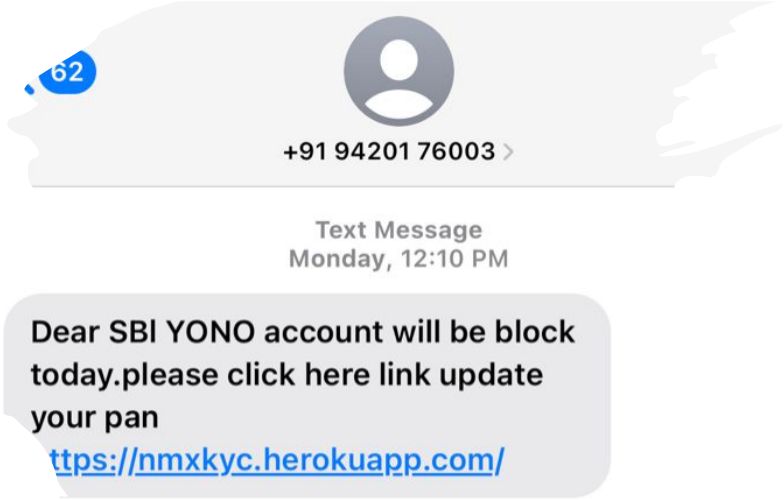
Email:	mrc@fisstacademy.com
Domain:	Fisstacademy
Storage Capacity:	0.1% of 100%

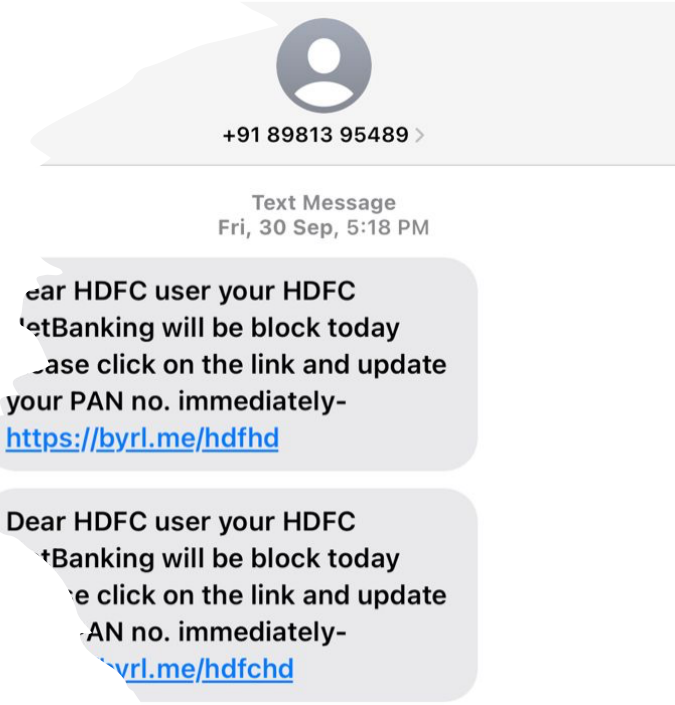
What is Wrong Here?



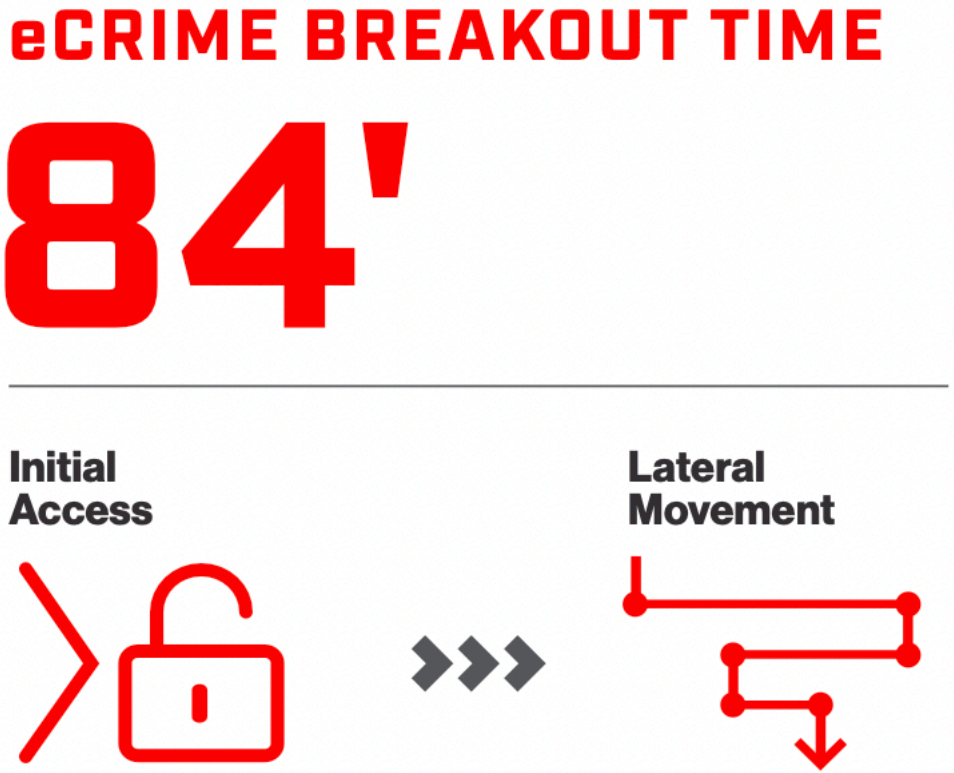








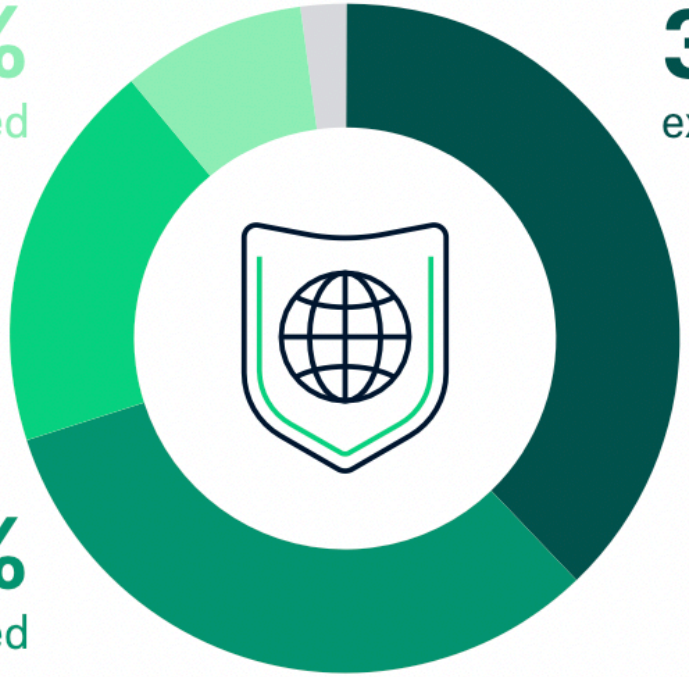
SMS



The average breakout time for interactive eCrime intrusion activity declined from 98 minutes in 2021 to 84 minutes in 2022.

2023 GLOBAL THREAT REPORT, Crowdstrike

How concerned are you about a potential attack on your company?



9 %
not concerned

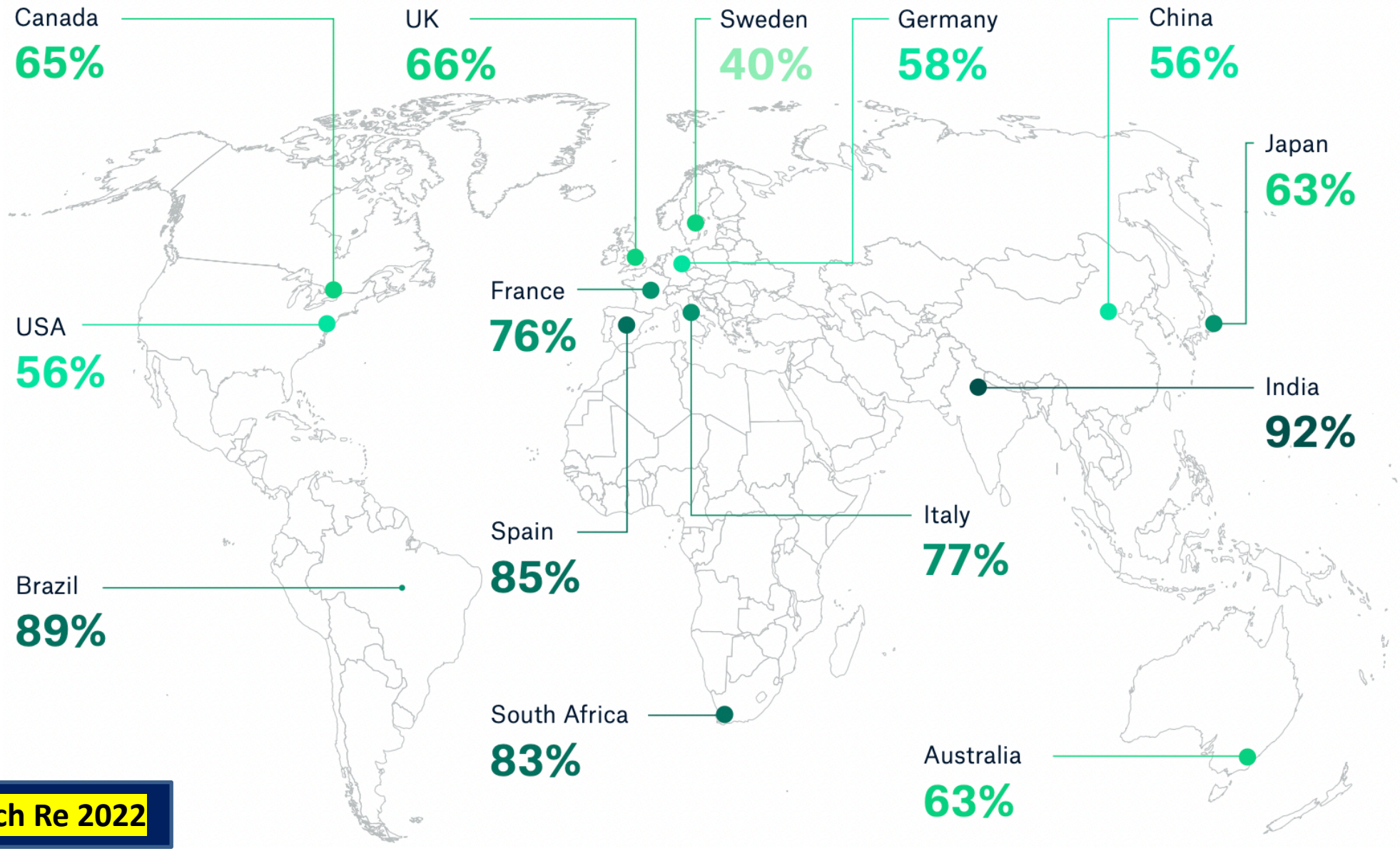
19 %
somewhat concerned

32 %
concerned

38 %
extremely concerned

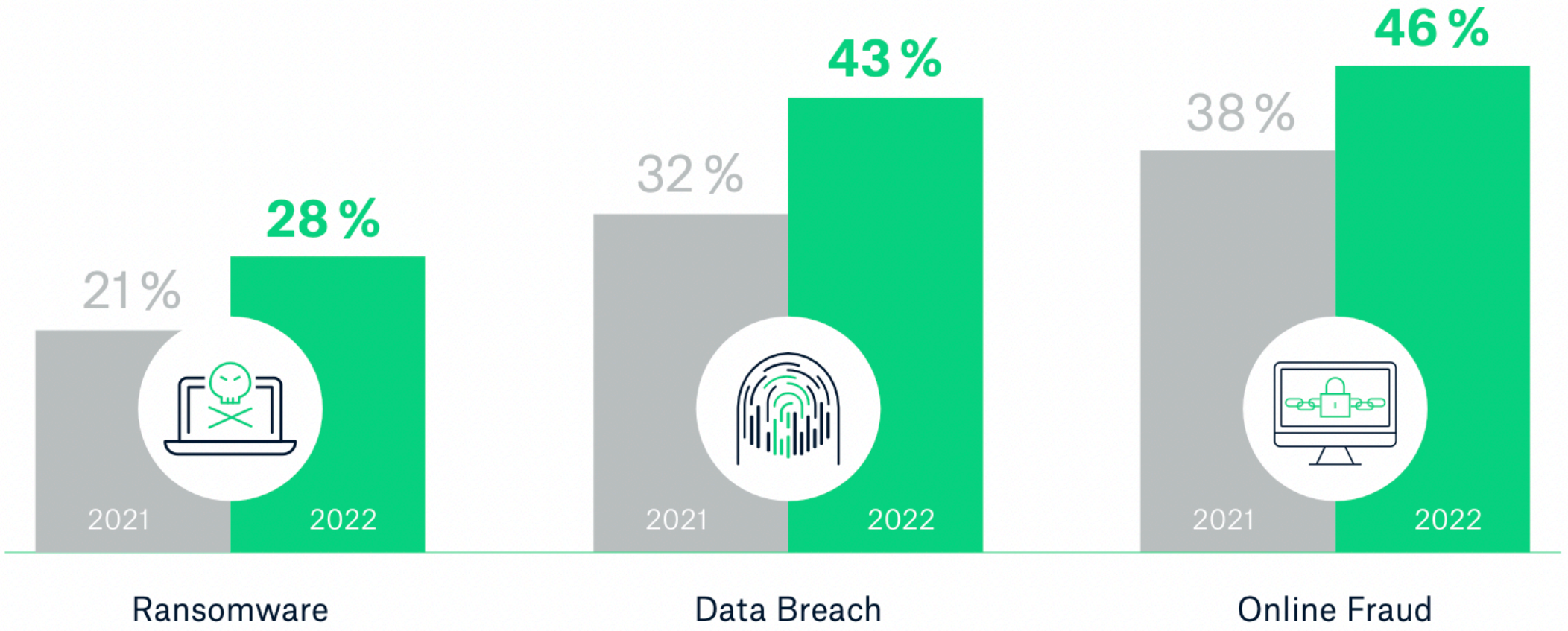
The number of C-level participants who are „extremely concerned“ has increased from 30 to 38%.

How concerned are you about a potential attack on your company?



Source : Munich Re 2022

Which of the following have you ever been affected by?



Major increase in attacks on India

The pandemic has surely come as a curse for Indian cybersecurity as there is a surge in cyberattacks in the country.

Throwing light on these attacks, National Cyber Security Coordinator Lt Gen (retd) Rajesh Pant said in a Cyber Security Seminar -

> “In such unprecedented times, the two Cs the challenge of Corona and challenge of cyber are known. Actually, at the perch which I sit, there are 3 Cs. The third ‘C’ of course is on our northern border, which is another challenge that we are facing. In such an environment, cyberattacks have gone up multi-fold. **There are four lakh malwares, we find everyday and 375 cyberattacks take place (daily).**”

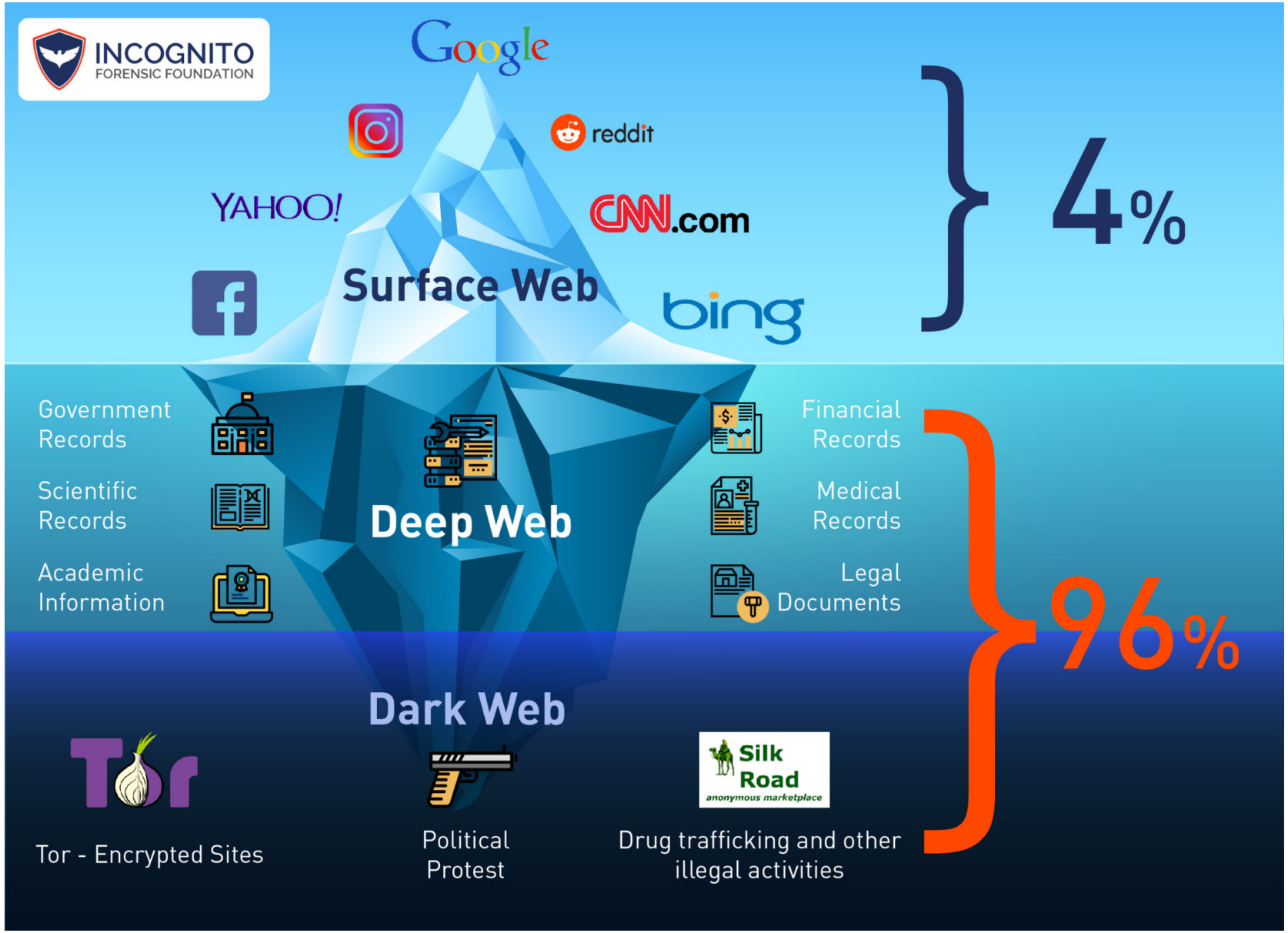
Major increase in attacks on India

The pandemic has surely come as a curse for Indian cybersecurity as there is a surge in cyberattacks in the country.

Throwing light on these attacks, National Cyber Security Coordinator Lt Gen (retd) Rajesh Pant said in a Cyber Security Seminar.

> People should be very careful about hoax calls and click-baits whose sole intention is to dig information from an internet user, he suggested.
>
> "This disease of just clicking on the link, this is another reason where the malware drops in mobile and computers" he said, asking everybody to study the recent cases of frauds at City Union Bank, where a person entered the core banking system through a click, and also the ones at Bangladesh Bank and Cosmos Bank.

Layers of Web



Recent Breaches - 1

2022 card data

On October 12, 2022, cybersecurity researchers from AI-driven Singapore-headquartered CloudSEK discovered a threat actor advertising a database of 1.2 million cards for free on a Russian-speaking Dark Web cybercrime forum.

This followed another incident of 7.9 million cardholder data advertised on the BidenCash website. This included data belonging to customers of the State Bank of India (SBI).

Recent Breaches - 2

Dominos India — May 2021

On May 22, 2021, Dominos India, a subsidiary of Jubilant FoodWorks, experienced a cyberattack resulting in the leakage of data from 180 million orders. The breach exposed order details, email addresses, phone numbers, and credit card details.

Recent Breaches - 3

Air India — May 2021

In May 2021, Air India fell victim to a cyberattack that compromised the personal details of approximately 4.5 million customers worldwide.

The breach exposed personal data registered between August 26, 2011, and February 3, 2021, including names, dates of birth, contact information, passport information, ticket details, Star Alliance and Air India frequent flyer data, as well as credit card data

Recent Breaches - 4

Recently, grocery delivery platform Bigbasket faced a data breach from the hacking group “Shinyhunters” where over 2 Cr users’ data was compromised in the attack.

Recent Breaches - 5

On October 16, US-based cybersecurity firm Cyble reported a data breach on PM Modi's website narendramodi.in, believed to have impacted 5 lakh users which shows the poor cybersecurity infrastructure in the country.

Recent Breaches - 6

Haldiram's also witnessed a ransomware attack on its servers by unidentified hackers who have allegedly stolen crucial data and demanded a ransom of $7,50,000.

Several Indian platforms in the past have seen data breaches. Earlier in May, it was reported that data of 4.75 crore Truecaller Indian users was found to be up for sale on the dark web.

> The development which was denied by the Swedish mobile application platform Truecaller India, was a result from its data leak.

CERT – IN Report

Indian Computer Emergency Response Team (CERT-In) has further informed it has detected and prevented 2,83,581, 4,32,057, 3,24,620 malicious scams during the years 2020, 2021 and 2022 respectively”

https://threatmap.checkpoint.com

Cyber Threats Landscape

bmc

Types of Cybersecurity

THE CYBER THREAT LANDSCAPE

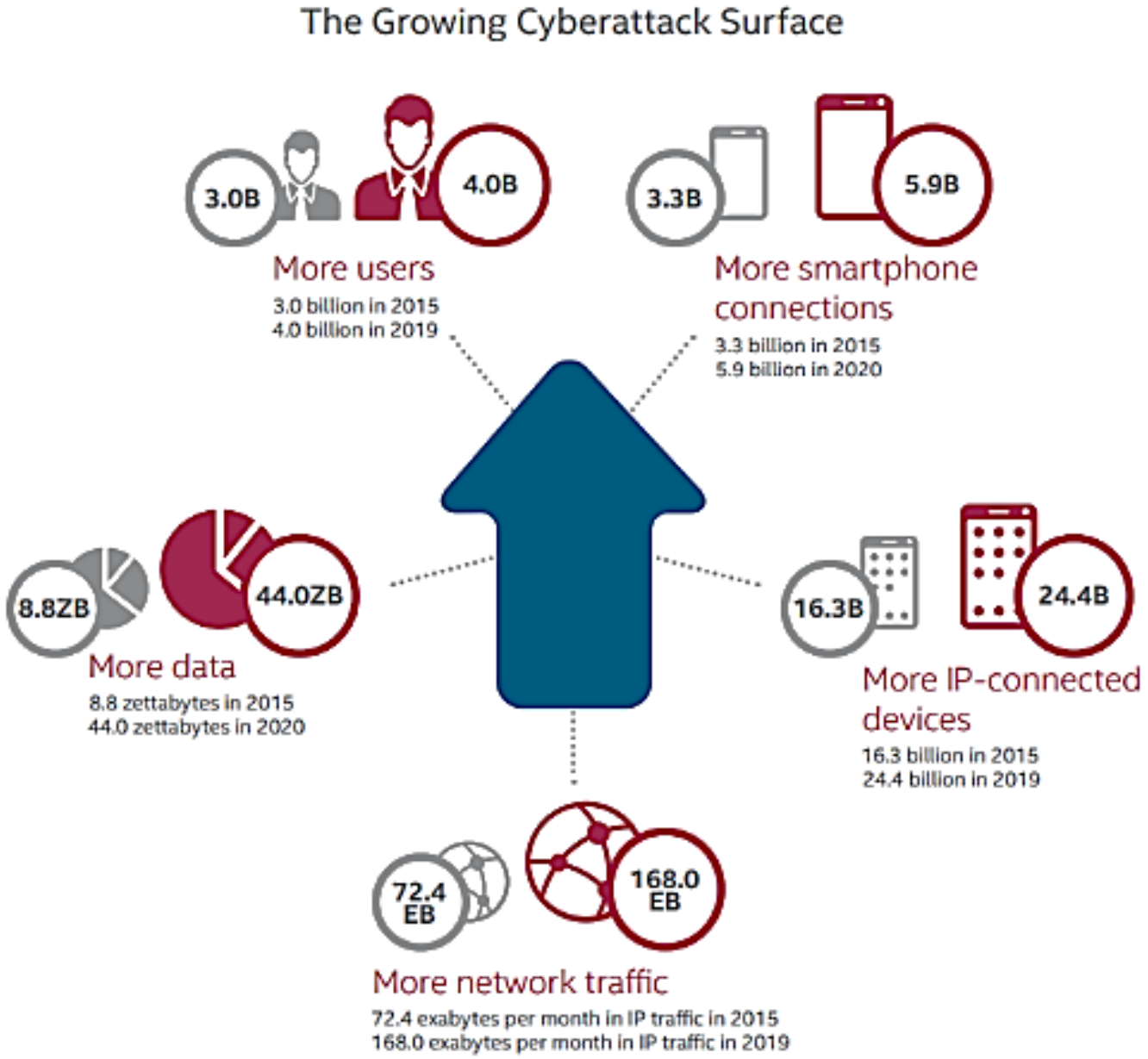


Image Source: [04/08/2018] https://rapidscale.net/cyber-threat-landscape/


AIRBNB
GUESTS BOOK
747 STAYS
AMAZON
SHOPPERS SPEND
$455K
X
USERS SEND
360K
TWEETS
6.3M
SEARCHES
HAPPEN ON
GOOGLE
WHATSAPP
USERS SEND
41.6M
MESSAGES
LINKEDIN
USERS SUBMIT
6,060
RESUMES
VIEWERS WATCH
43 YEARS
OF STREAMING
CONTENT
3,720
USERS DOWNLOAD
INSTAGRAM
THREADS
CYBER-
CRIMINALS
LAUNCH 30 DDOS ATTACKS
EVERY MINUTE
01:00
OF THE DAY
PRESENTED BY
CHATGPT
USERS SEND
6,944 PROMPTS
INSTAGRAM
USERS SEND
694K REELS VIA DM

THE CYBER THREAT LANDSCAPE

Digital transformation is demanding change at an unprecedented pace

Image Source: [04/08/2018] https://blogs.cisco.com/enterprise/enterprise-network-security-is-it-in-your-dna

THE CYBER THREAT LANDSCAPE

Security is an iterative process – continuously ask and answer four basic questions:

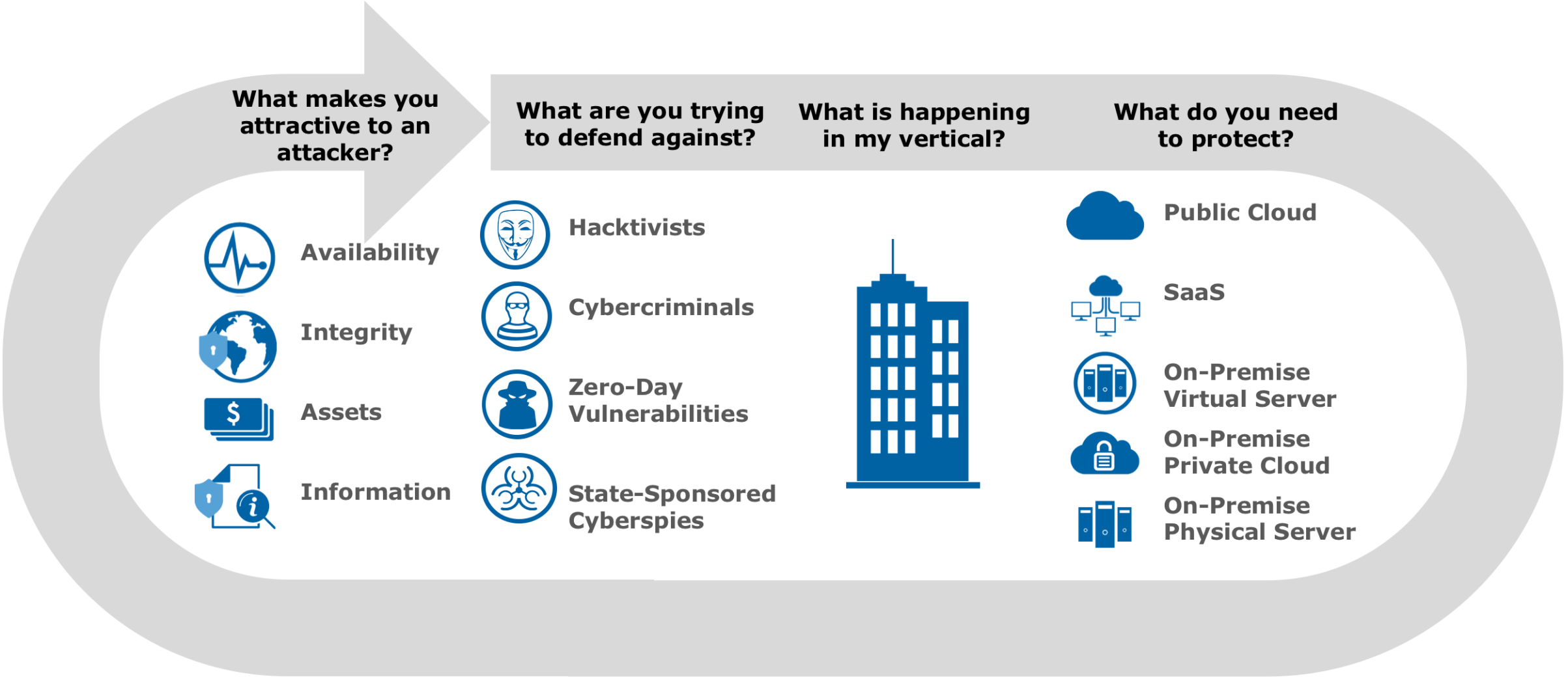


Image Source: [04/08/2018] Framework for Resilient Cybersecurity - White Paper, VeriSign, 2016

Top Threats


1
TREND
Malware
2
TREND
WWW
Web-based attacks
3
TREND
Phishing
4
TREND
Web application attacks
5
TREND
Spam
6
TREND
DDoS
7
TREND
Identity theft
8
TREND
Data breach
9
TREND
Insider threat
10
TREND
Botnets
11
TREND
Physical manipulation, damage, theft and loss
12
TREND
Information leakage
13
TREND
Ransomware
14
TREND
Cyberespionage
15
TREND
Cryptojacking

Need for Cyber Security Training
Alarming trends

#1 | Cybercrimes are becoming more sophisticated

#2 | Cyber Crime to cost $6 trillion in 2021 (double from 2015)

#3 | 300 billion passwords worldwide by 2020

#4 | Personal data sells for as little as $0.20

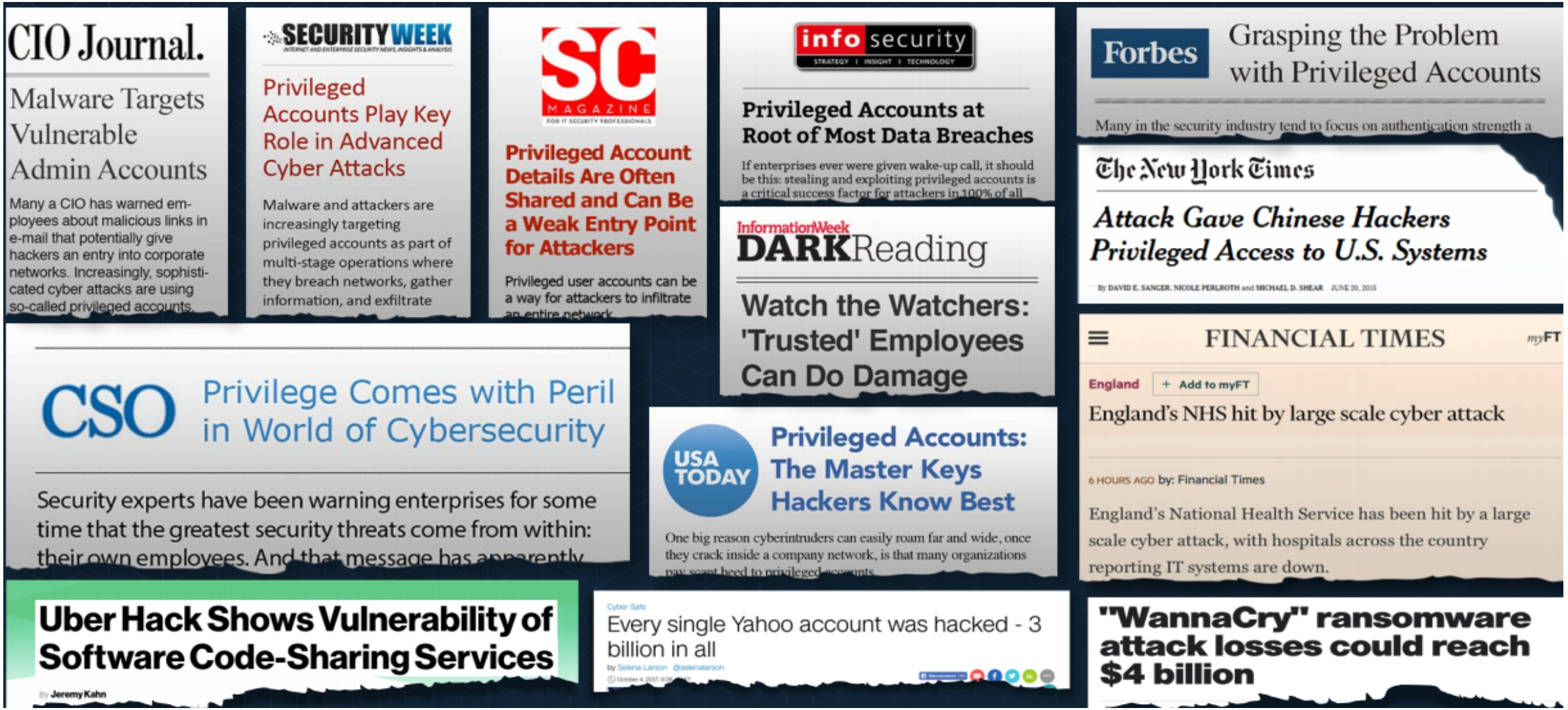
#5 | Companies take over 6 months to notice / detect a data breach.

1 Billion Bots involved in 210 Million Fraud Attempts in Q1 2021

More than 210 million attempted fraud attacks occurred during Q1, 2021, representing a 62% increase from 2020. Record volume of 1 billion BOT attacks of which, 100 million of those attacks came from mobile device users.

~ThreatMatrix, Q1 2021 CyberCrime Report

Need for Cyber Security Professionals
Alarming trends



Data Breach
Alarming trends

Yahoo Data Breach
Date: October 2017
Impact: 3 billion accounts

1.Adobe
2.Adult Friend Finder
3.Canva
4.Dubsmash
5.eBay
6.Equifax
7.Heartland Payment Systems
8.LinkedIn
9.Marriott International
10.My Fitness Pal
11.MySpace
12.NetEase
13.Sina Weibo
14.Yahoo
15.Zynga

First American Financial Corporation Data Breach
Date: May 2019
Impact: 885 million users

Marriott International Data Breach
Date: September 2018
Impact: 500 million guest records

Facebook Data Breach
Date: September 2019
Impact: 400 million users

FriendFinder Networks Data Breach
Date: October 2016
Impact: 400 million accounts

Bangladesh Central Bank Heist – 81 Million Dollars

(850 million dollars escaped due to Spelling mistake by Hacker)

Case Study

Bank Hacks

Bank hacks have traditionally focused on stealing the login credentials of bank account holders---either individuals or small businesses.

Billions have been stolen successfully in this way & continues to increase every year (with Sophistication – AI/ML used !)

Bangladesh Heist

But the hacks in this case targeted the banks themselves and focused on subverting their SWIFT accounts, the international money transfer system that banks use to move billions of dollars daily between themselves.

What is SWIFT?

SWIFT stands for the Society for Worldwide Interbank Financial Telecommunication and is a consortium that operates a trusted and closed computer network for communication between member banks around the world.

The consortium, which dates back to the 1970s, is based in Belgium and is overseen by the National Bank of Belgium and a committee composed of representatives from the US Federal Reserve, the Bank of England, the European Central Bank, the Bank of Japan and other major banks.

The SWIFT platform has some 11,000 users and processes about 25 million communications a day, most of them money transfer transactions.

What Happened?

On February 4, 2016, unknown hackers used SWIFT credentials of Bangladesh Central Bank employees to send more than three dozen fraudulent money transfer requests to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.

The hackers managed to get $81 million sent to Rizal Commercial Banking Corporation in the Philippines via four different transfer requests and an additional $20 million sent to Pan Asia Banking in a single request.

But the Bangladesh Bank managed to halt $850 million in other transactions.

Discovery of Heist

The hackers might have stolen much more if not for a typo in one of the money transfer requests that caught the eye of the Federal Reserve Bank in New York. The hackers apparently had indicated that at least one of the transfers should go to the Shalika Foundation, but they misspelled “foundation” as “fandation.”

A printer "error" helped Bangladesh Bank discover the heist. The bank's SWIFT system is configured to automatically print out a record each time a money transfer request goes through. The printer works 24 hours so that when workers arrive each morning, they check the tray for transfers that got confirmed overnight.

But on the morning of Friday February 5, the director of the bank found the printer tray empty. When bank workers tried to print the reports manually, they couldn't. The software on the terminal that connects to the SWIFT network indicated that a critical system file was missing or had been altered.

How this could have happened ?

According to SWIFT, the hackers have obtained valid credentials the banks use to conduct money transfers over SWIFT and then used those credentials to initiate money transactions as if they were legitimate bank employees.

How they got the credentials is unclear.

News reports have indicated that insiders might have cooperated and provided the credentials to the hackers.

Other reports indicate that lax computer security practices at Bangladesh Bank were to blame: the bank reportedly didn't have firewalls installed on its networks, raising the possibility that hackers may have breached the network and found the credentials stored on the system.

How Did the Hackers Cover Their Tracks?

They installed malware on the bank's network to prevent workers from discovering the fraudulent transactions quickly. In the case of Bangladesh Bank, the malware subverted the software used to automatically print SWIFT transactions. The hackers installed it on the bank's system some time in January, not long before they initiated the heist money transfers on February 4.

In the case of the bank in Vietnam, the custom malware targeted a PDF reader the bank used to record SWIFT money transfers. The malware apparently manipulated the PDF reports to remove any trace of the fraudulent transactions from them, according to SWIFT and the *New York Times*.

Is your sensitive data secure?

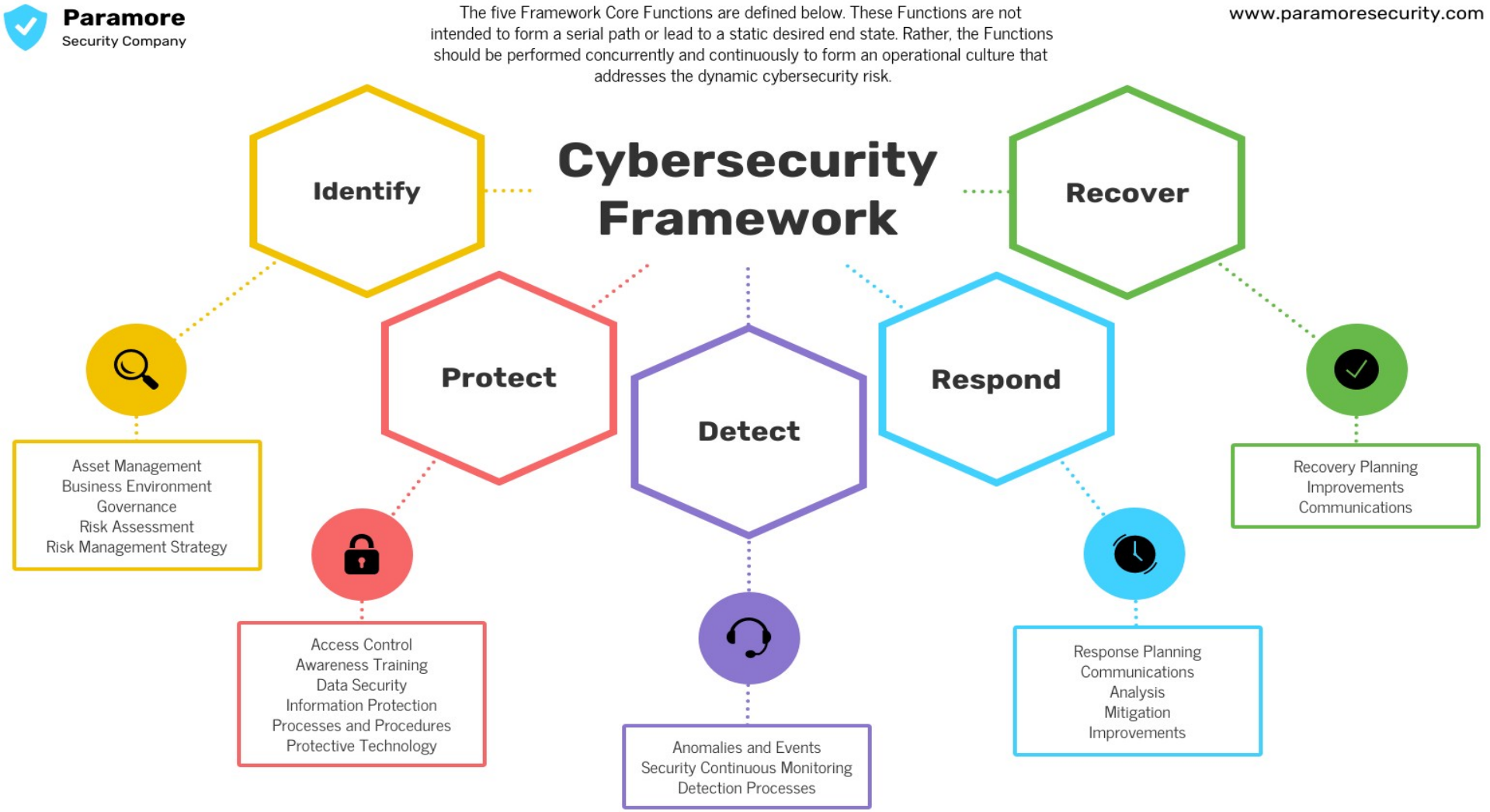
It’s no exaggeration: any company can fall victim to cyber crime.

Reports of cyber attacks come from government organizations, educational and healthcare institutions, banks, law firms, non-profits, and many other organizations.

Hackers, insider threats, ransomware, and other dangers are out there.

Smart businesses are investing more in cybersecurity to eliminate risks and keep their sensitive data safe, and this has already brought the first results.

Cyber Security Framework



36 billion

Records were exposed in first half of 2022

95%

Cyber risks are caused by human errors

$270.4 billion

As per Gartner - worldwide information security market by 2024

The Current State of Cyber Attacks

1 in 5 business have suffered a data breach or cyber attack, **double the number in 2015**.

52% of business consider it inevitable that they will become a cyber victim.

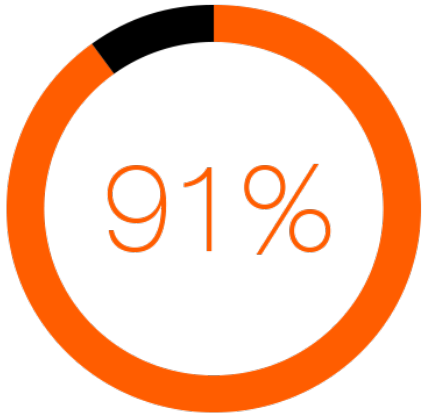
Only **36%** of business are concerned about someone deceiving their employees into transferring funds, despite a **2,370% increase** in losses from such scams in two years.

95% of businesses rely on their computer systems functioning properly for their business to operate.

Yet some are unprepared…

23% are not familiar with their cyber insurance options

How Are Businesses Handling Cyber Threats?



People that are confident their company have implemented best practices to avoid/mitigate a cyber event. Yet most have not taken some basic steps.

55% have not completed a cyber risk assessment for their business

62% have not written a business continuity plan

63% have not assessed the cyber security of vendors with access to their data

50% of business do not purchase cyber insurance

75% say that it is difficult to keep up with the evolving cyber landscape, information and developments

Shortfall of trained Cyber Security resources is the reason for increasing attacks

India Market is Booming – NASSCOM report

India’s cybersecurity market is projected to grow to $35 billion by 2025, according to Nasscom.

Currently, more than 30,000 cybersecurity jobs are available in the country, said HR experts. Job portal Indeed reported a jump of 150% in cybersecurity jobs within one year

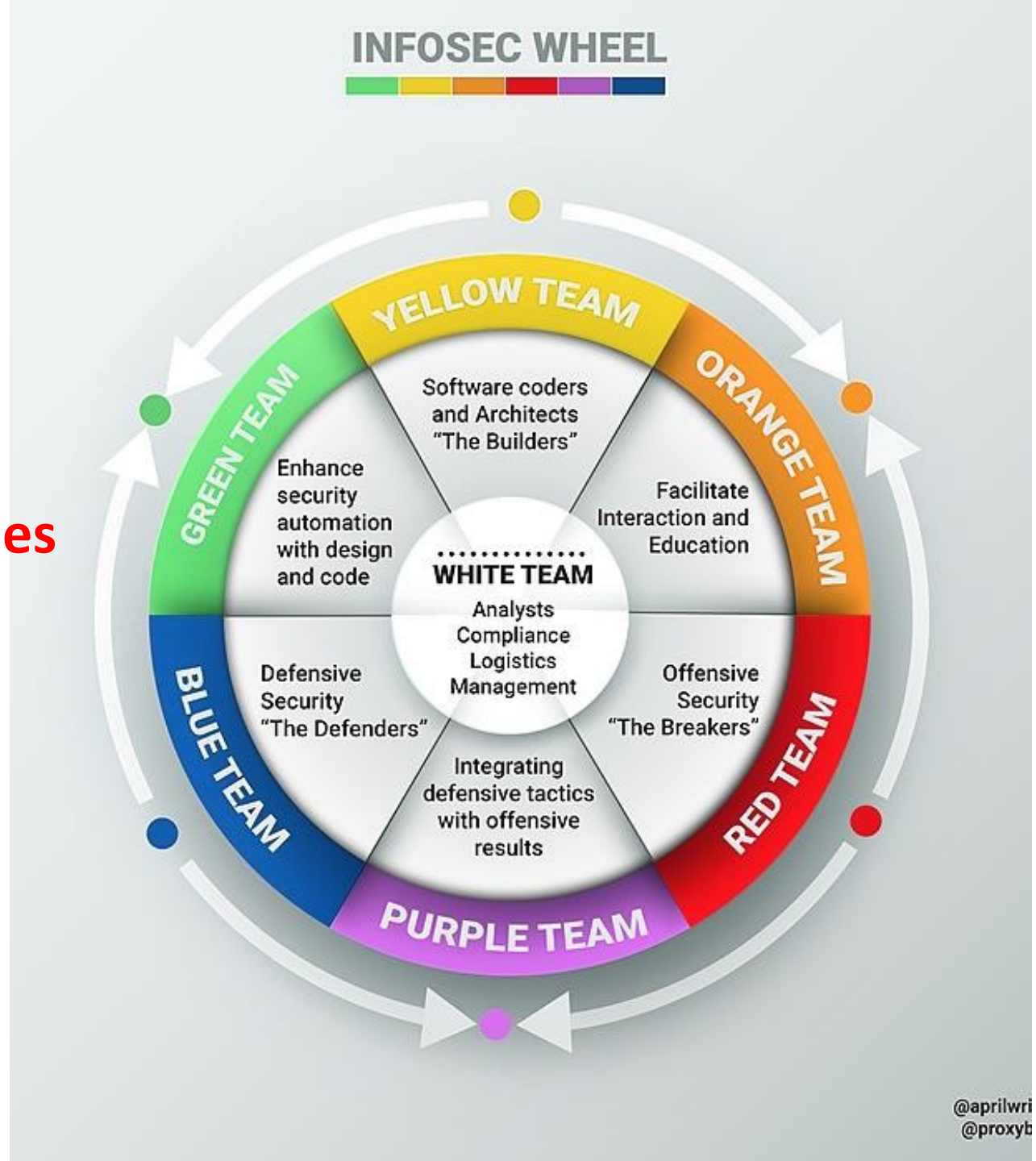
https://economictimes.indiatimes.com/industry/tech/cybersecurity-first-responders-in-demand/articleshow/67496994.cms?from=mdr

Global in-house centres (GICs) and IT consulting companies are hiring CFRs with around two years of experience at an average salary of about Rs 15 lakh a year, according to industry executives. They said professionals with two-three years of experience draw up to Rs 20 lakh while those with five-eight years of experience are offered Rs 35-40 lakh.

Pioneering Excellence in Education, Research & Innovation

Predict Detect Protect FISST

Job Roles – 70+ titles



YELLOW TEAM

- Software Builders
- Application Developers
- Software Engineers
- System Architects

ORANGE TEAM

- Inspire coders and architects to be more security conscious
- Benefit from current exposure to evolving security threats
- Offensive critical thinking included in builder's intrinsic thought pattern
- Decrease in overall security bug count over time

RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

PURPLE TEAM

- Facilitate improvements in detection and defence
- Sharpened the skills of Blue and Red team members
- Effective for spot-checking systems in larger organizations

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

YELLOW TEAM

- Software Builders
- Application Developers
- Software Engineers
- System Architects

GREEN TEAM

- Improved logging capability, working to standardise and prioritise important events
- Better data for digital forensics and incident response cases
- Safer Change Management including integrity monitoring
- Full coverage monitoring including improved Anti-Virus and End Point Protection on systems

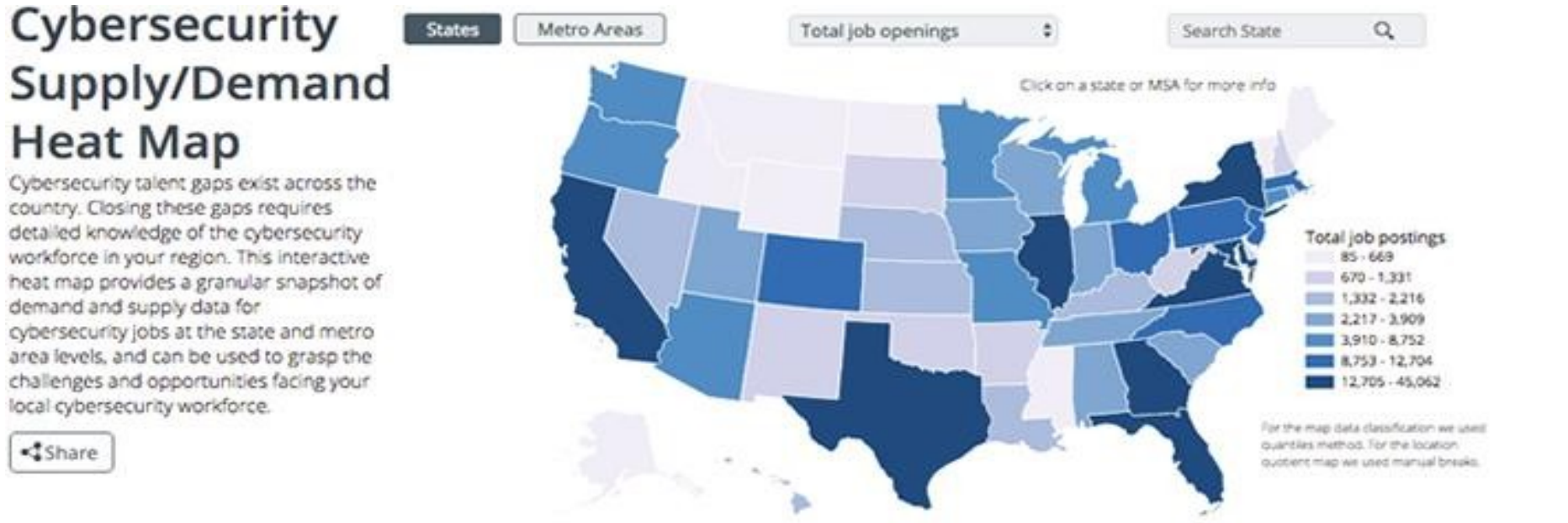
BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

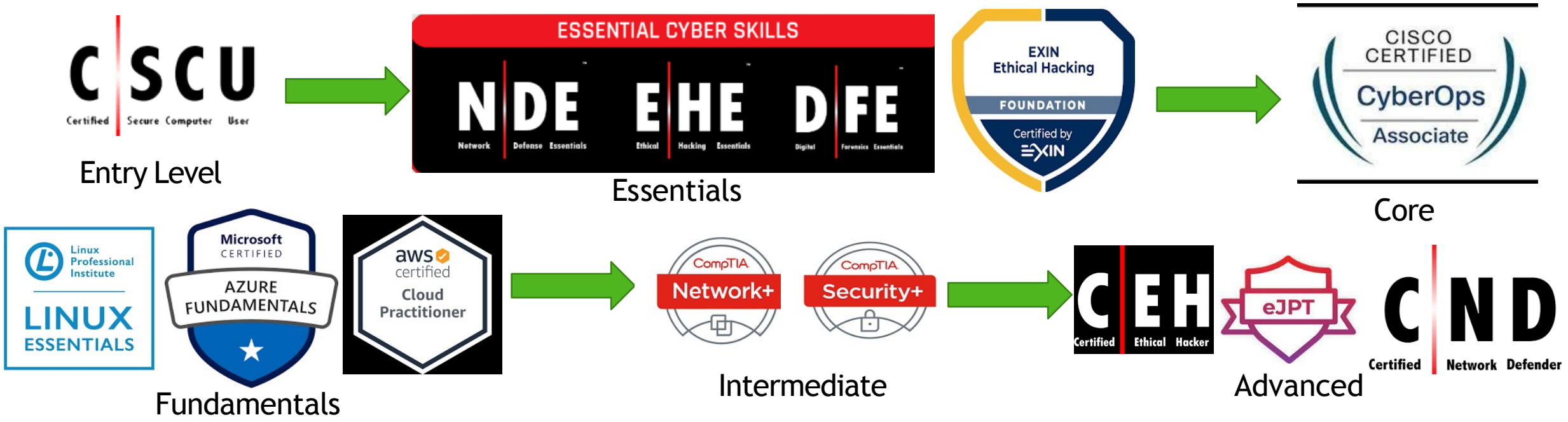
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt00e09df814b51cf8/60a3f1af11dac1533c75d229/Coolest_Careers_in_Cybersecurity.pdf

Cyber Security Jobs Demand

- This is the only map of Requirements in the United States!
- But it already shows how much information security professionals are needed.



International Certifications



Relatively expensive and limited recognition / validity

Possible Training & Certifications

IIT Madras has been pioneering Cyber Security Training

Trained over 1000+ students and professionals with 80% placement record (only Placement Assistance)

Certified Cyber Warriors (CCW) v3.0

- 120 hours of specialized training with 70% hands-on with over 90 practical tools
- Practice “Live” attacks and defense using Cyber Range (1200 incidents loaded)
- Best mix of Academic Faculty and Industry Experts

Certified Cyber Engineer (CCE) – Computer & Network Security

(aligned to NASSCOM QP 0917)

- 40 hour – Hybrid mode of training with over 25 tools
- Cyber Range access for few practical exercises including Firewall misconfigurations

New tracks under approval by IIT M as CCE

- Cloud Security & DevSecOps
- Secured Coding and Software Engineering

How do YOU take advantage of this HUGE Demand

- In addition to receiving basic training and following a certification journey, like the one suggested on the previous slide.

- Practicing in labs is essential, especially so that his skills continue to grow and you can face challenges, such as certification exams and future job interviews when the time comes.

- In addition to making good professional decisions. If possible, connect to mentors, who can help and provide professional training as well.

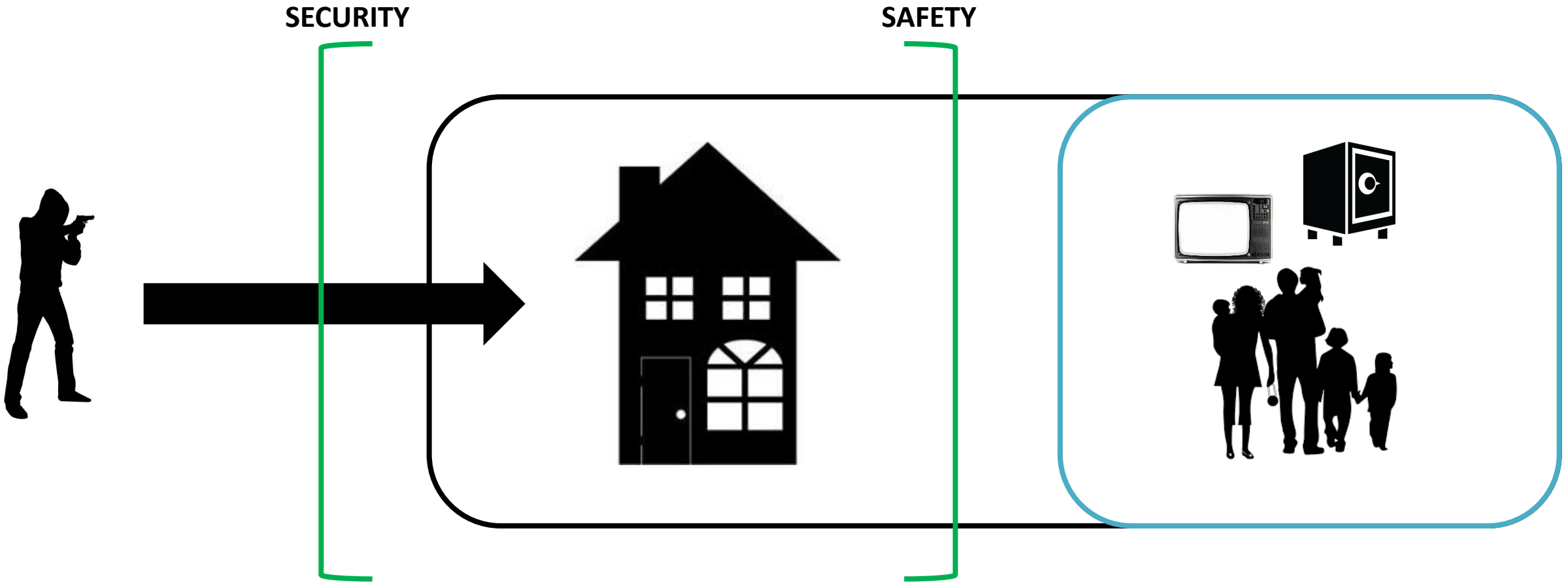
What does security & safety mean?

What does security imply?

What is Safety ?

Any difference ???

What is Security and Safety?



Measures taken for Protection against attacks

Measure taken by oneself to Ensure something Doesn't cause harm

Layers of Security

- Physical security
- Personal security
- Operations security
- Communications security
- Computer security
- Network security
- Information security

Source: [27/12/2016] https://www.pinterest.com/homecontrols/home-security/

Vulnerabilities, Threats & Controls

What is a vulnerability?

What is a threat?

What is a control?

Vulnerabilities, Threats & Controls

Vulnerability = a weakness in a system

Allows a threat to cause harm

Threat = a potential negative harmful occurrence

Earthquake, worm, virus, hackers.

Control/Safeguard = a protective measure

Reduce risk to protect an asset.

CIA ??

The CIA Triad

Source: [04/01/2019] http://keywordsuggest.org/gallery/151304.html

Attacker Needs

What are 3 things must an attacker have?

An Attacker Must Have:

Method: skills, knowledge, tools.

Capability to conduct an attack

Opportunity: time and access to accomplish attack

Motive: a reason to want to attack

Software Vulnerabilities

Define some different types.

There are many to chose from….

Software Vulnerabilities

Logic Bomb: employee modification.

Trojan Horse: Overtly does one thing and another covertly.

Virus: malware which requires a carrier

Trapdoor: secret entry points.

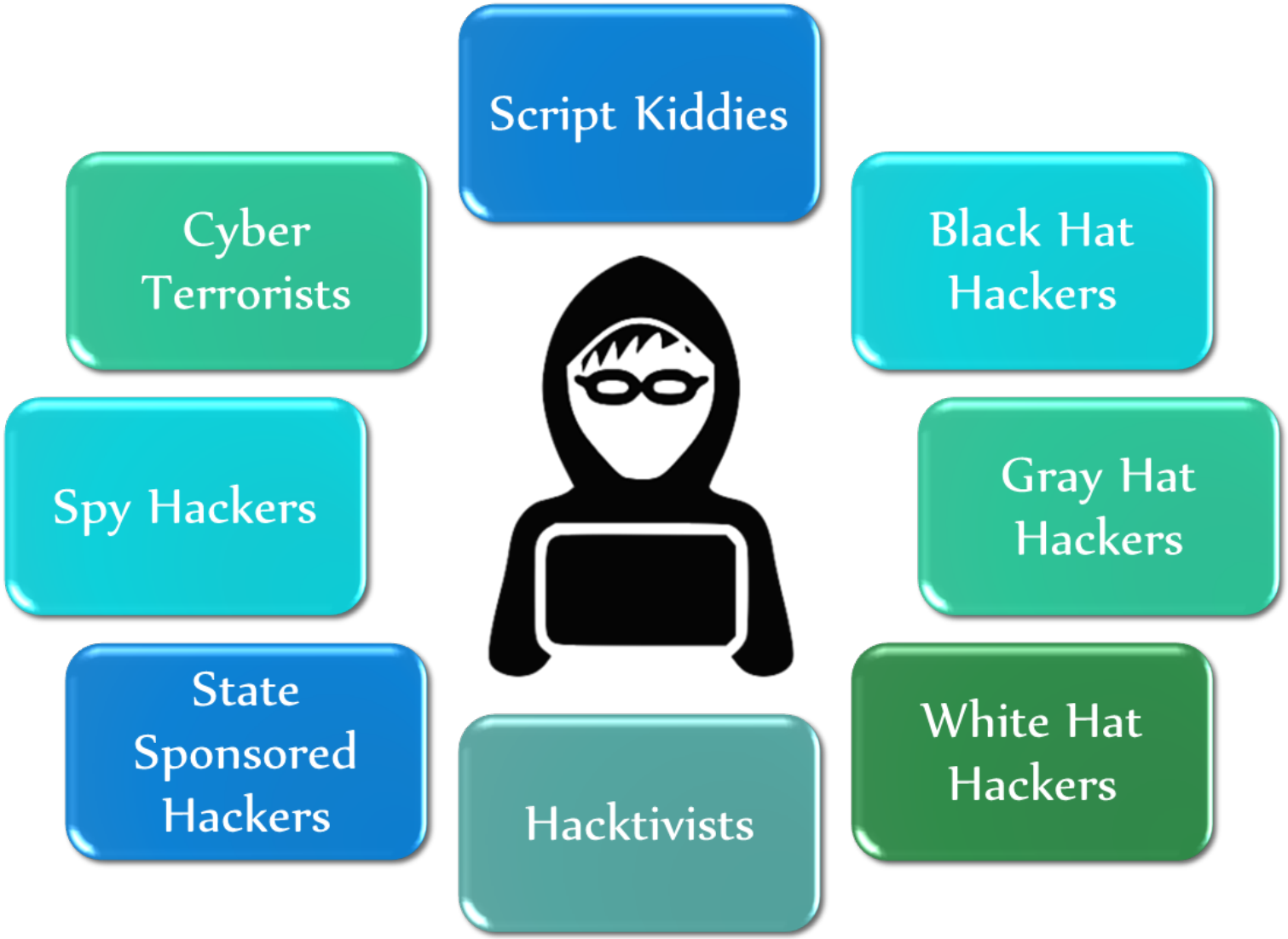
Information Leak: makes information accessible to unauthorized people.

Worm: malware that self-propagates.

Criminals

Define different types of computer criminals / intruders and their motive or motives?

Types of Intruders



Motives

Financial gain: make money.

Competitive advantage: steal information.

Curiosity: test skills.

Political: achieve a political goal.

Cause Harm/damage: reputation or financial

Vendetta/Disgruntled: fired employees.

Threats

Interception: gained access to an asset.

Wireless network, hacked system, etc.

Impacts confidentiality.

Interruption

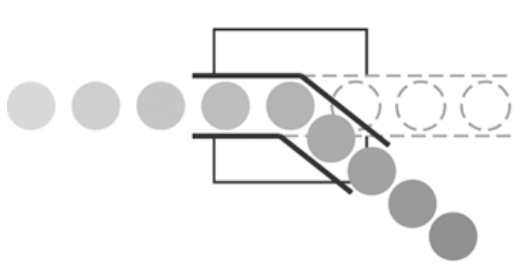
Unavailability, reduced availability.

Modification

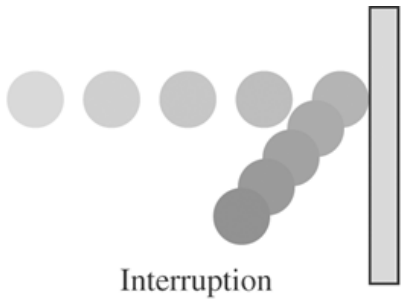
Tamper with data, impacts integrity.

Fabrication

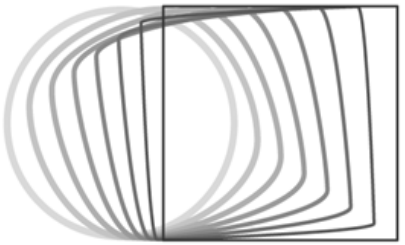
Spurious transactions, impacts integrity.



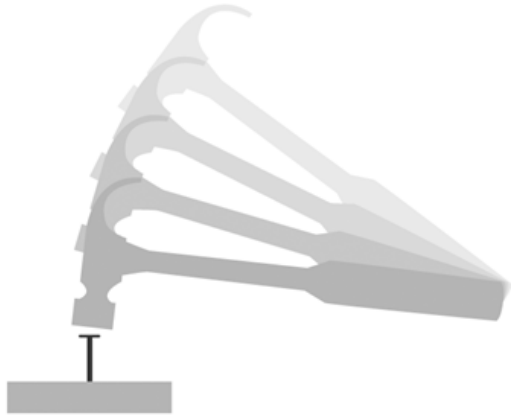
Interception



Interruption



Modification



Fabrication

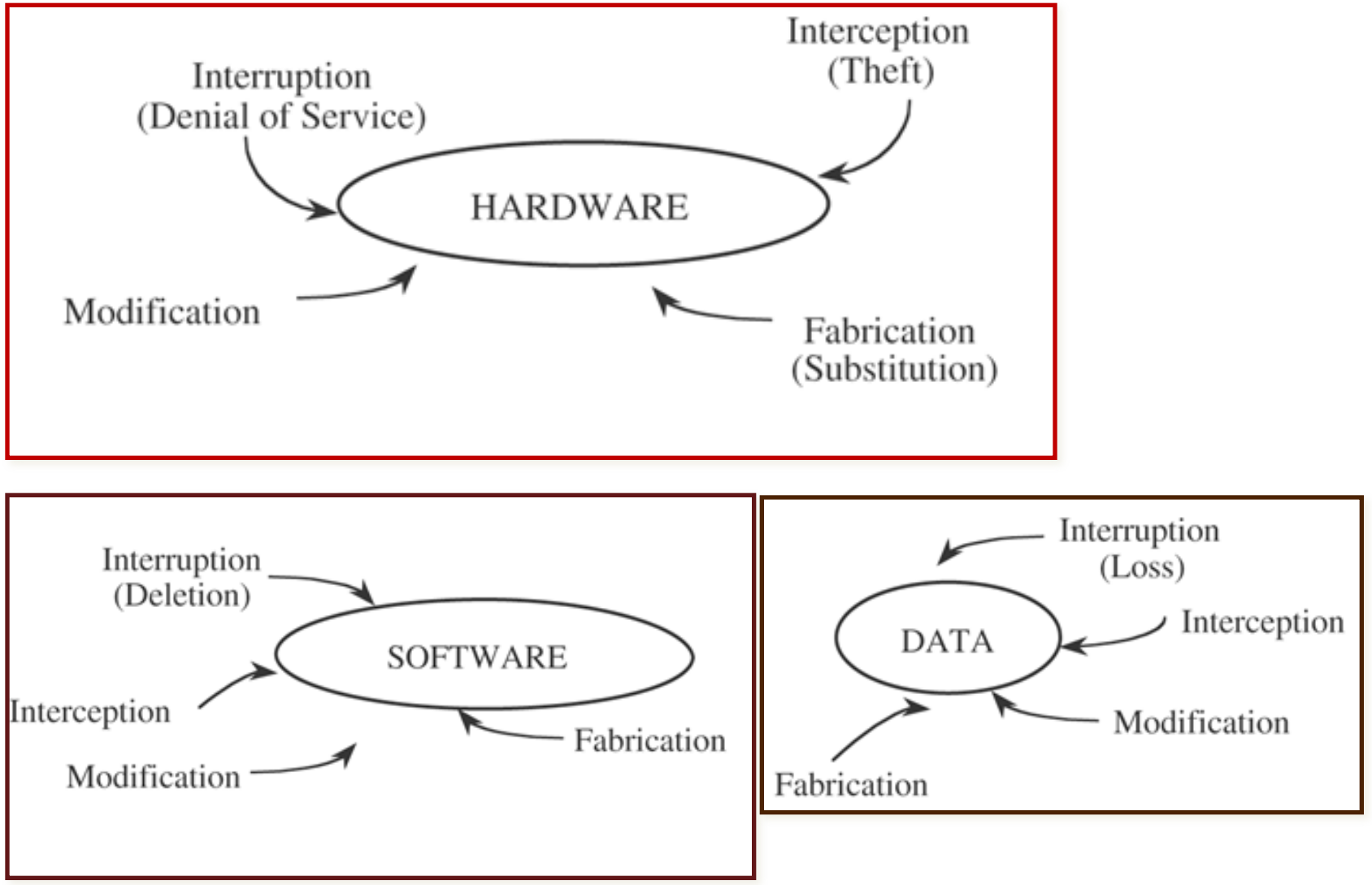


Figure - Vulnerabilities of Computing Systems.

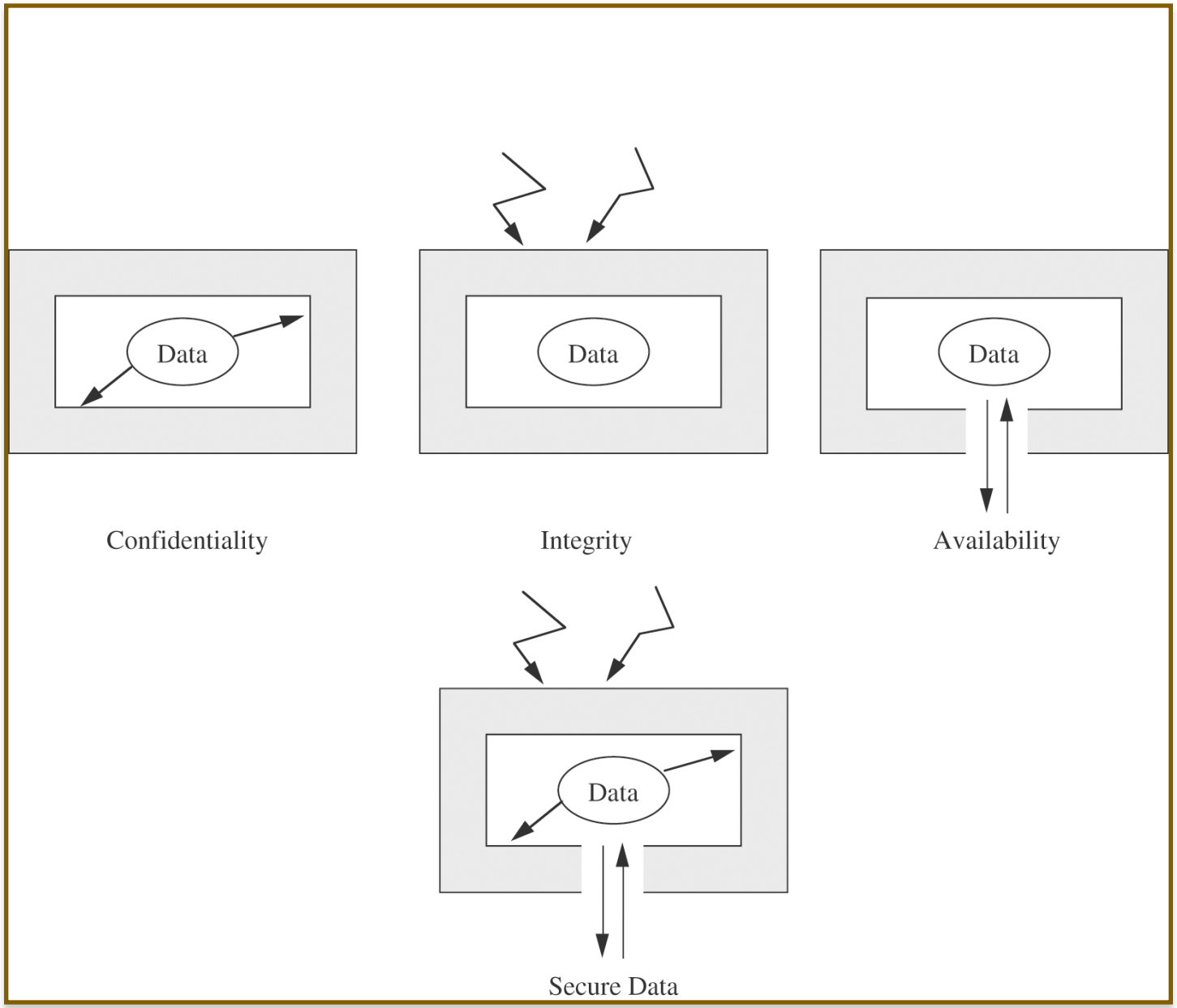


Figure - Security of Data.

Risk

What are the different ways a company can deal with risk?

How to deal with Risk

- Accept it: cheaper to leave it unprotected.
- Mitigate it: lowering the risk to an acceptable level e.g. (laptop encryption).
- Transfer it: insurance model.
- Avoid it: sometimes it is better not to do something that creates a great risk.

Risk mitigation

- Prevent it by fixing vulnerability,
- Deter it making it harder,
- Deflect it by making other targets more attractive,
- Detect it as it happens,
- Recover from its effects

Possible Controls

- Encryption: confidentiality, integrity
  - VPN, SSH, Hashes, data at rest, laptops.
- Software: operating system, development.
- Hardware: Firewall, locks, IDS, 2-factor.
- Policies and Procedures: password changes
- Physical: gates, guards, site planning.

Types of Controls

1. Preventive: prevent actions.
2. Detective: notice & alert.
3. Corrective: correcting a damaged system.
4. Recovery: restore functionality after incident.
5. Deterrent: deter users from performing actions.
6. Compensating: compensate for weakness in another control.

Security Principles

- Easiest Penetration: attackers use any means available to attack.
- Adequate Protection: protect computers/data until they lose their value.
- Effectiveness: controls must be used properly to be effective. Efficiency key.
- Weakest Link: People are the weakest link
  - People → Process → Technology

CIA summary

Confidentiality: authorized access

Integrity : accurate unmodified consistent data

Availability: get when needed.

Security implies 'trust'.

Formal Definition: CIA Triad

Confidentiality

Confidentiality is the property, that information is not **accessible** (made available or disclosed) to **unauthorized** individuals, entities, or processes. In ensures sensitive data does not land in wrong hands.

Integrity

Integrity means that data cannot be **modified** in an **unauthorized** or **undetected** manner. It provides assurance over accuracy and completeness over entire data life cycle.

Availability

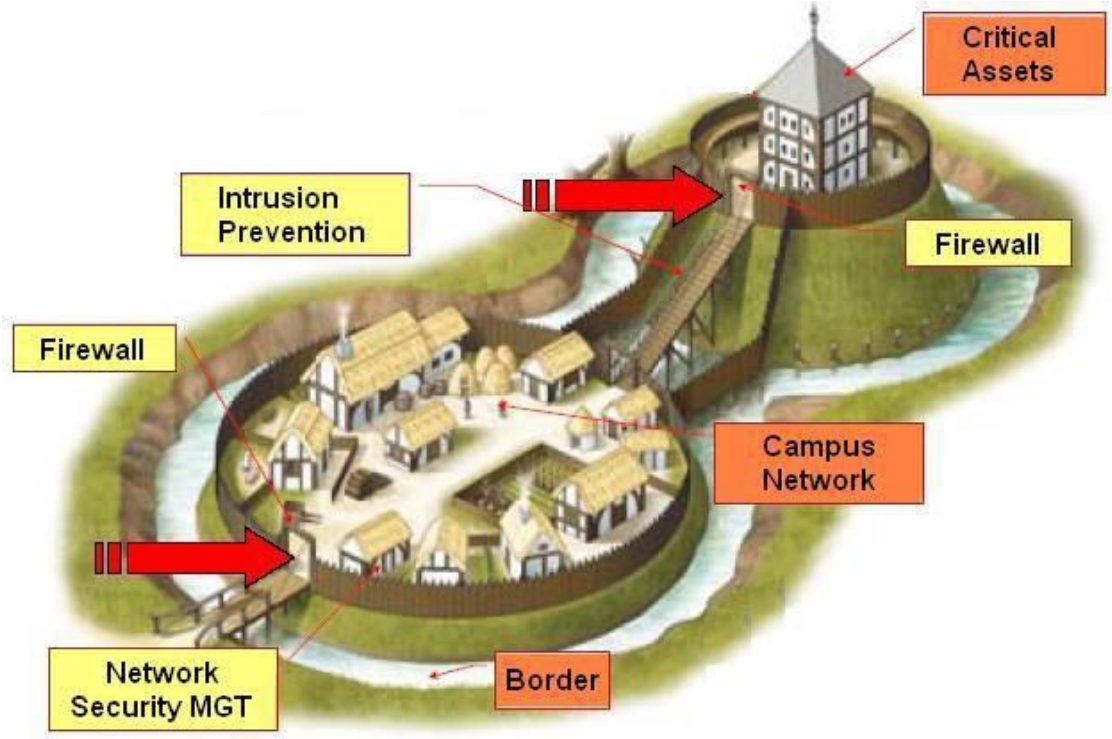
Availability means relevant information is readily accessible to those authorized to view it at all times. It ensures information is available when needed.

Defense in Depth – Classical Military

Information Security draws idea from conventional military doctrine

Defense in depth:

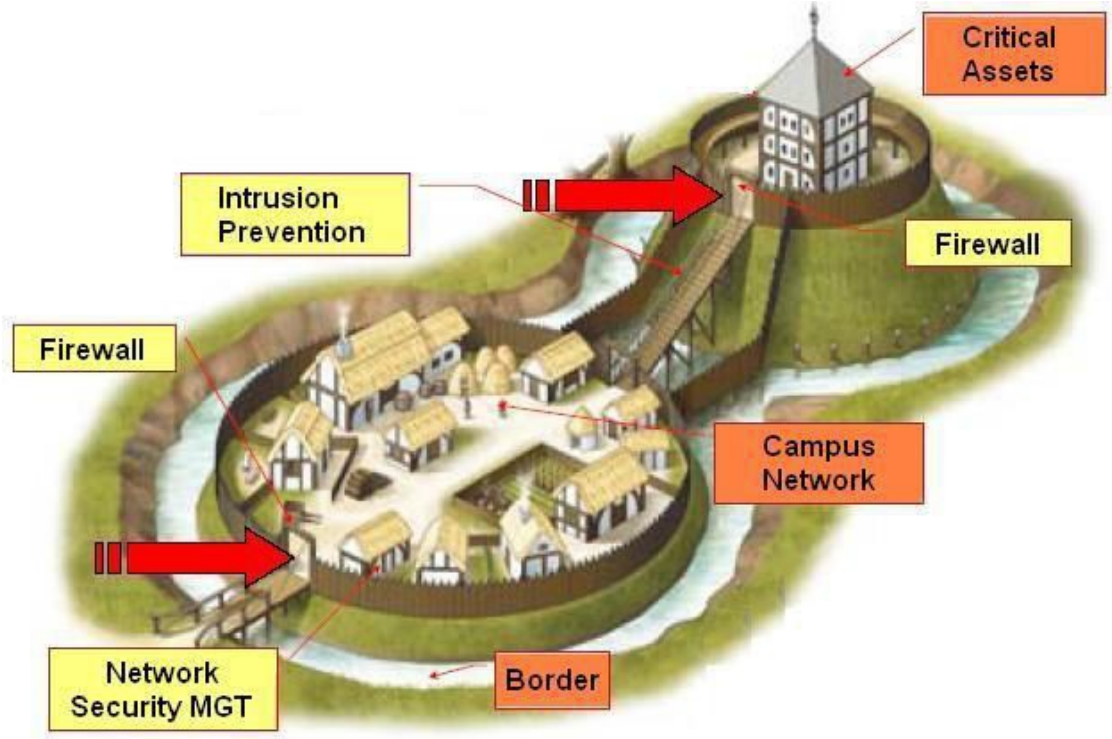
- Moat (with moat monsters)
- Drawbridge (with spikes)
- Protective walls, narrow stairs
- Offensive Security: Archers, Soldiers with boiling oil etc.



Defense in Depth – Information Security

Defense in depth:

- DMZ
- Firewalls + WAF
- Privileged Identity Management
- IDS / IPS
- AV & Anti-malware
- Anti-APT
- Honeypots
- Hardened Systems

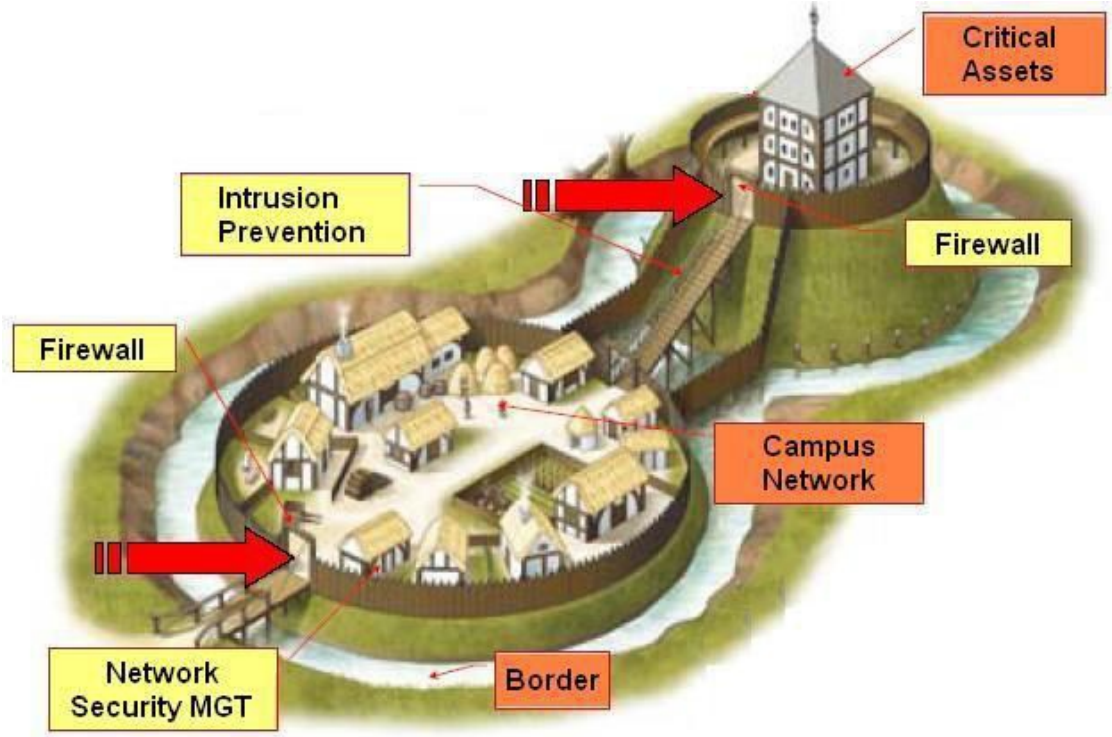


Defense in Depth

Network Security Gateway (MGT)	Network Security Gateway is a combination of two or more security solutions that prevents unsecured traffic from entering an internal network of an organization
Firewall (Network + WAF)	A device that forwards packets between the less secure and more secure parts of the network, applying rules that determine which packets are allowed to pass, and which are not
Intrusion Detection & Prevention Systems (IDS / IPS)	A security function that examines more complex traffic patterns against attack signatures/pattern, and alert administrators about an attack on the network and can prevent (IPS) the initial packet from entering the network
Honeypots	A system designed to look like something that an intruder can hack. Normally built for many purposes, but the overriding purpose is to deceive attackers and learn their tools and methods
Hardened Systems (secured with Anti-virus & Anti-malware)	Network devices and end points in an organization which carries the critical information and generally equipped with host based security solutions

Question – Differences?

What are some of the differences when we compare classical military strategy with cybersecurity differences?



Key differences from classical military:

- Loss of strength gradient (inverse)
- Lack of counter attack / deterrents(?)
- Attribution (close to impossible)

Authentication

First Line of Defense: Authentication

Authentication is a process of
proving
you are who you claim to be.

Mechanisms:
- Something you know (Passwords)
- Something you have (Tokens)
- Something you are (Biometrics)

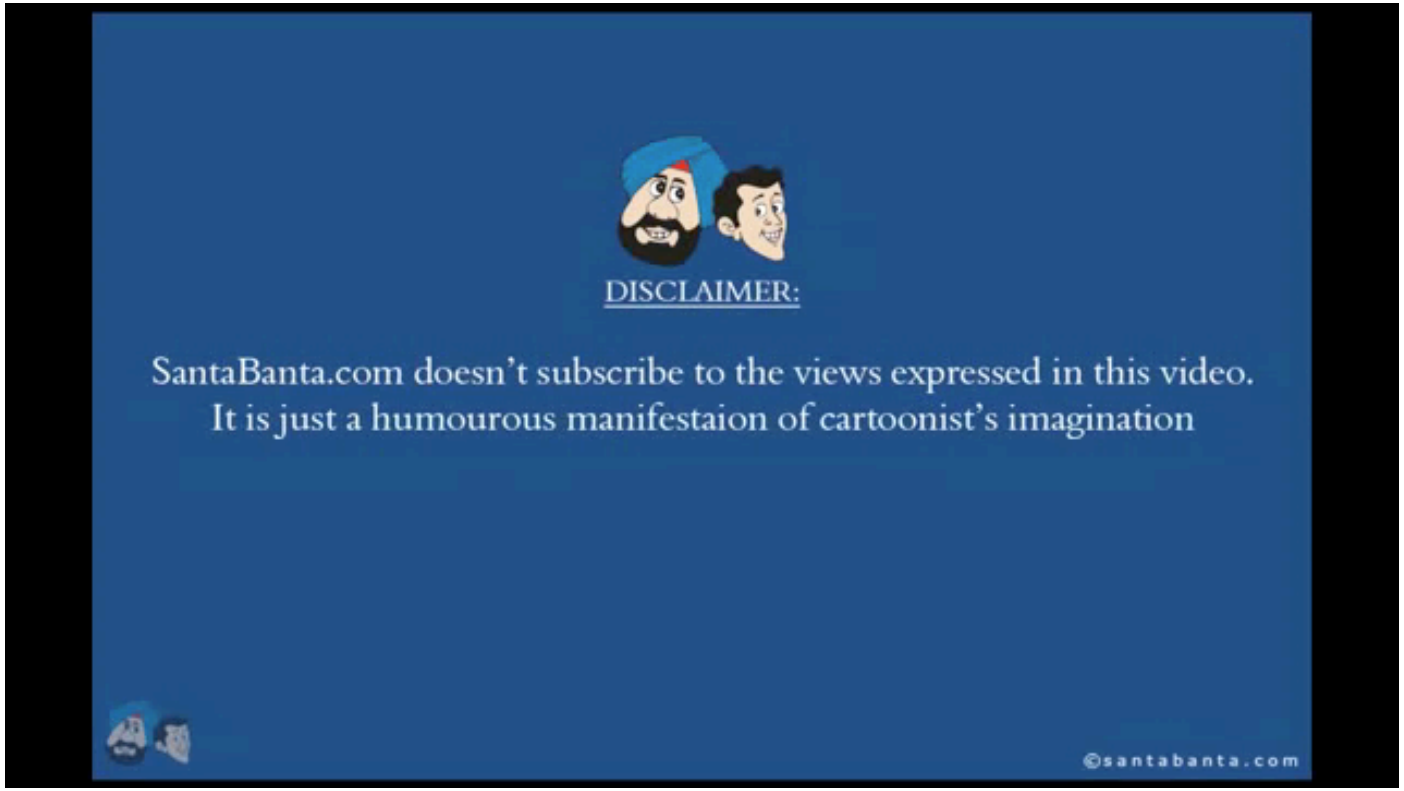
Passwords …
&
Importance

Passwords

Good passwords are the first line of defense against malicious attackers.

What makes a good password?

Authentication & Authorization–Passwords

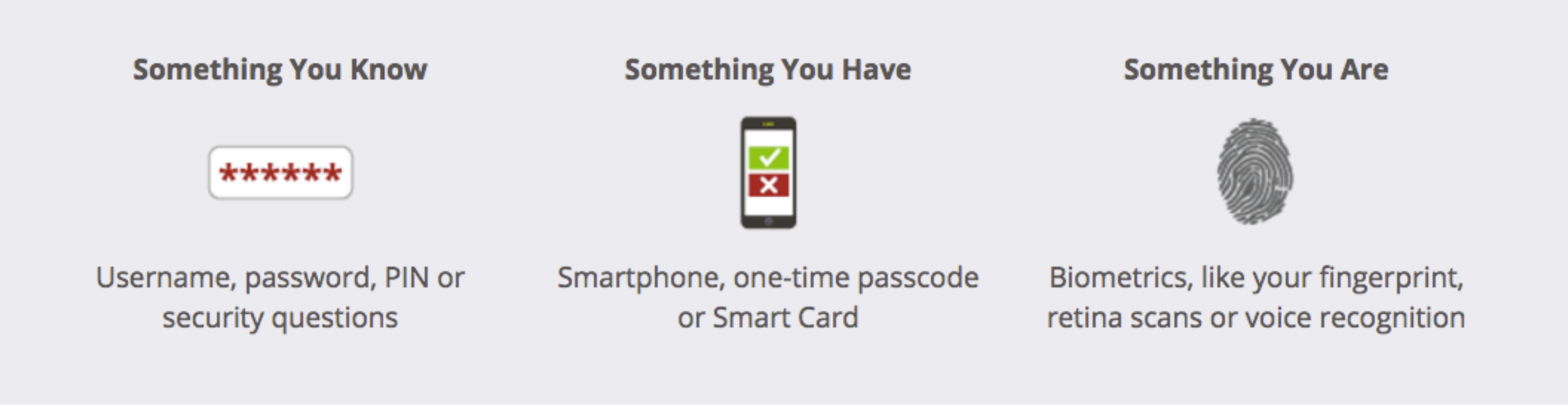


https://www.youtube.com/watch?v=G0wQWa6X0jE

Authentication & Authorization – Passwords

Authentication

Authentication is a process of **proving** you are who you claim to be.



Source: [04/01/2019] https://blog.centrify.com/sfa-mfa-difference/

Authentication & Authorization – Passwords

What are Passwords?

A password consists of a sequence of characters or numbers or both used to verify the identity of a user in order to access various resources in a computing system, which are generally not accessible without a valid password.

Good passwords are the first line of defense against malicious attackers.

Source: [10/01/2018] https://now.avg.com/how-to-make-a-strong-password-in-3-easy-steps/

Authentication & Authorization – Passwords

What makes a Good Password?

It should be at least 10 characters long.

It should not contain user name, real name, institution name.

It should not contain any complete word or dictionary word.

It should contain characters from each of the following categories:

- Uppercase letters (eg. A,B,C,D)
- Lowercase letters (eg. a,b,c,d)
- Special characters (eg. @,!,#,$,*)
- Numbers (eg. 1,2,3,4,5)

Solid Password - suggestion

J&Jw^dh2fapofH2O

Jfd&bh^^&Jcta2

T2l*?Iw?Ur!

You can be innovative in making it complex – yet simple to remember !

Authentication & Authorization – Passwords

Password Security Implications

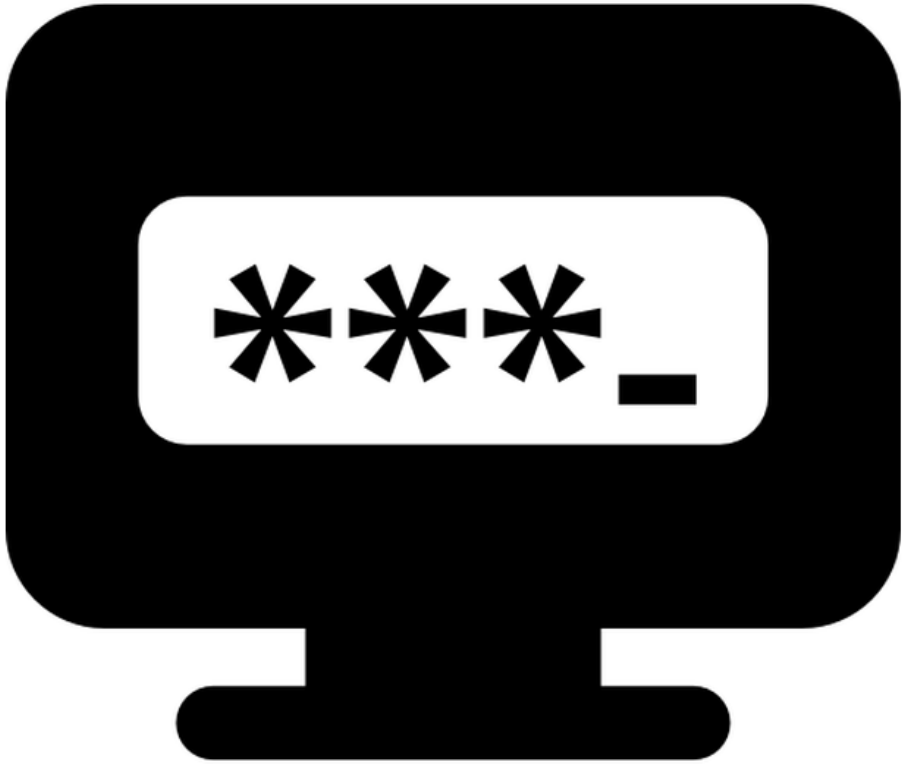
- Personal Information in Passwords
- Use of Default Passwords
- Use of Weak Passwords
- Sharing passwords with stranger
- Falling into the Phishing trap and revealing password details
- Write passwords on pieces of paper
- Repeat passwords across sites

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

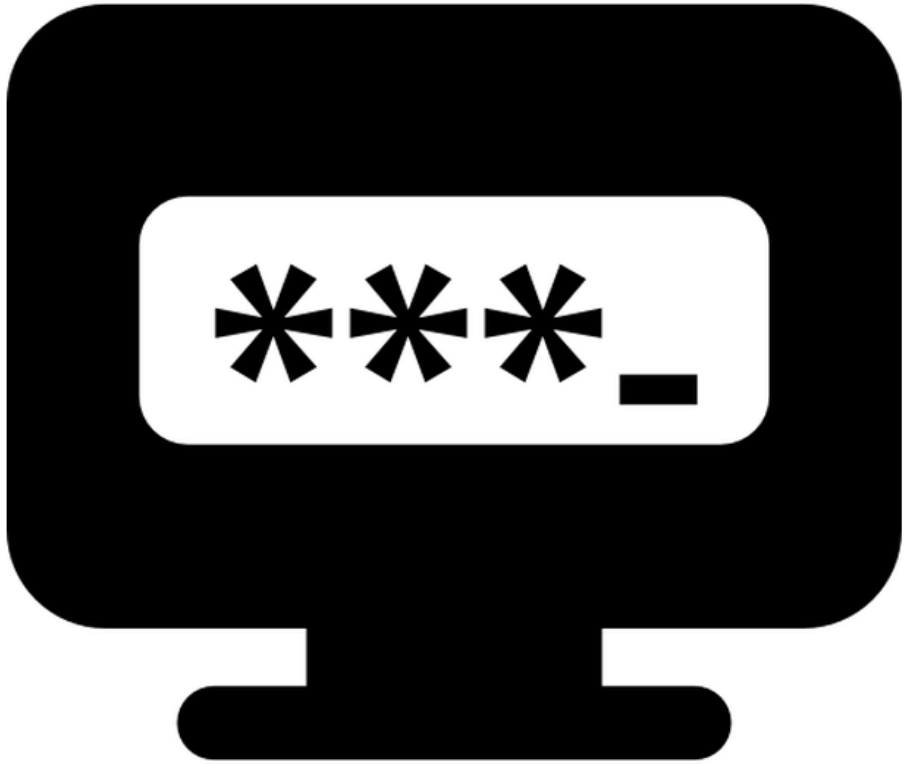
Source : Hive Systems Report - 2020

How passwords work: Creation



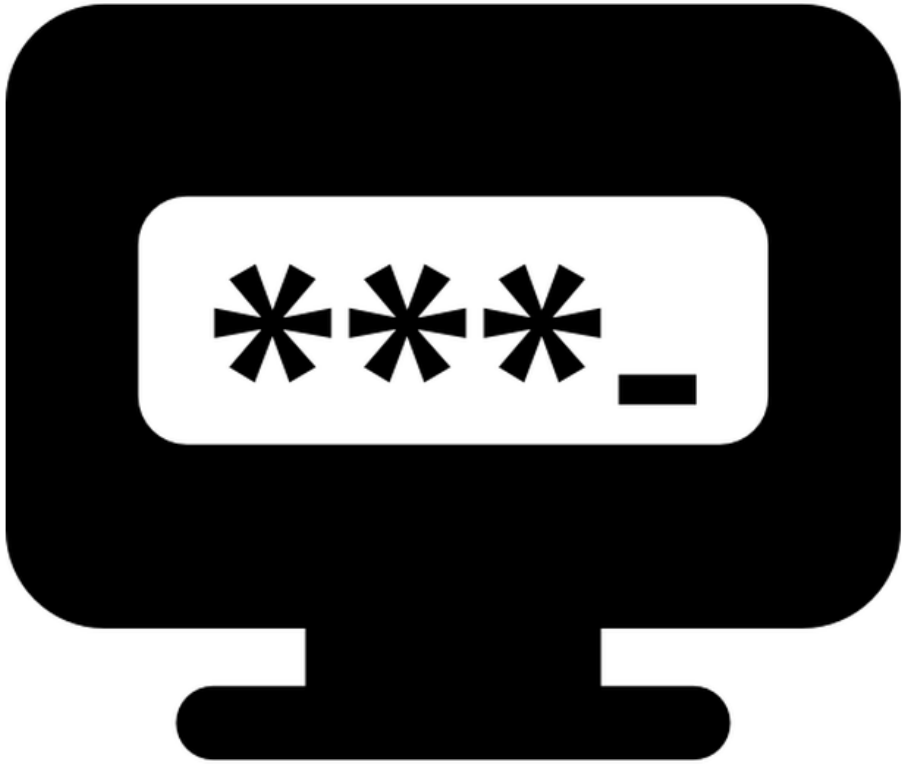
- User enters a password first time (plain text)
- System forces the password to comply with complexity rules
- Ideally password should be transmitted to the system over encrypted channels

How passwords work: Storage



- User entered password is hashed.
- Algorithms used:
  - Linux: MD5, SHA 256, Blowfish etc.
  - Windows: LM, NTLM hashing
  - Recommended: Bcrypt, Scrypt, PBKDF2

How passwords work: Comparison



- User enters a password to authenticate. System takes the password and hashes it
- Compares the hash of what the user entered against the hash stored in the password file
- If they match, allows access. Else declines.

(Watch out for error messages!)

Password Cracking

- Time needed to crack: understanding password strength.
- Mechanisms:
  - Online Brute Forcing
  - Offline Cracking: Via the obtained password hashes (John the ripper)
  - A different approach: using pre-computed hashes (Rainbow tables)
- Prevention: account lockout, captcha, two factor, salting, complex passwords

Authorization

- Authorization is a mechanism of verifying that a particular user is allowed to perform an action that user is attempting
- Does subject S have right R for object O
  - Subject: various users
  - Rights: Read, Write, Execute
  - Objects: Files, programs etc.
- In real world, this is often done as Role Based Access Control (RBAC). Various roles defined, users assigned to those roles, rights granted accordingly