Introduction to Fundamentals of Information Security


COVID-19
CORONA VIRUS

Refers to **new** measures, policies or protocols that have an effect on the attitude and behavior of people in the field of public health after the Covid-19 pandemic.


EPANDEMIC

JAN 2023

ESSENTIAL DIGITAL HEADLINES

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

GLOBAL OVERVIEW

TOTAL POPULATION	UNIQUE MOBILE PHONE USERS	INTERNET USERS	ACTIVE SOCIAL MEDIA USERS
			
8.01 BILLION	**5.44 BILLION**	**5.16 BILLION**	**4.76 BILLION**
URBANISATION	vs. POPULATION	vs. POPULATION	vs. POPULATION
57.2%	**68.0%**	**64.4%**	**59.4%**

SOURCES: UNITED NATIONS; GOVERNMENT BODIES; GSMA INTELLIGENCE; ITU; WORLD BANK; EUROSTAT; CNNIC; APJII; IAMAI & KANTAR; CIA WORLD FACTBOOK; COMPANY ADVERTISING RESOURCES AND EARNINGS REPORTS; OCDH; BETA RESEARCH CENTER; KEPIOS ANALYSIS. **ADVISORY:** SOCIAL MEDIA USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. **COMPARABILITY:** SIGNIFICANT REVISIONS TO SOURCE DATA, INCLUDING COMPREHENSIVE REVISIONS TO POPULATION DATA. FIGURES ARE NOT COMPARABLE WITH PREVIOUS REPORTS. ALL FIGURES USE THE LATEST AVAILABLE DATA, BUT SOME SOURCE DATA MAY NOT HAVE BEEN UPDATED IN THE PAST YEAR. SEE NOTES ON DATA FOR FULL DETAILS.

JAN 2023

ESSENTIAL DIGITAL HEADLINES

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

NOTE: PLEASE READ THE IMPORTANT NOTES ON COMPARING DATA AT THE START OF THIS REPORT BEFORE COMPARING DATA ON THIS CHART WITH PREVIOUS REPORTS

PHILIPPINES

TOTAL POPULATION

116.5 MILLION

URBANISATION

48.2%

KEPIOS

CELLULAR MOBILE CONNECTIONS

168.3 MILLION

vs. POPULATION

144.5%

INTERNET USERS

85.16 MILLION

vs. POPULATION

73.1%

KEPIOS

ACTIVE SOCIAL MEDIA USERS

84.45 MILLION

vs. POPULATION

72.5%

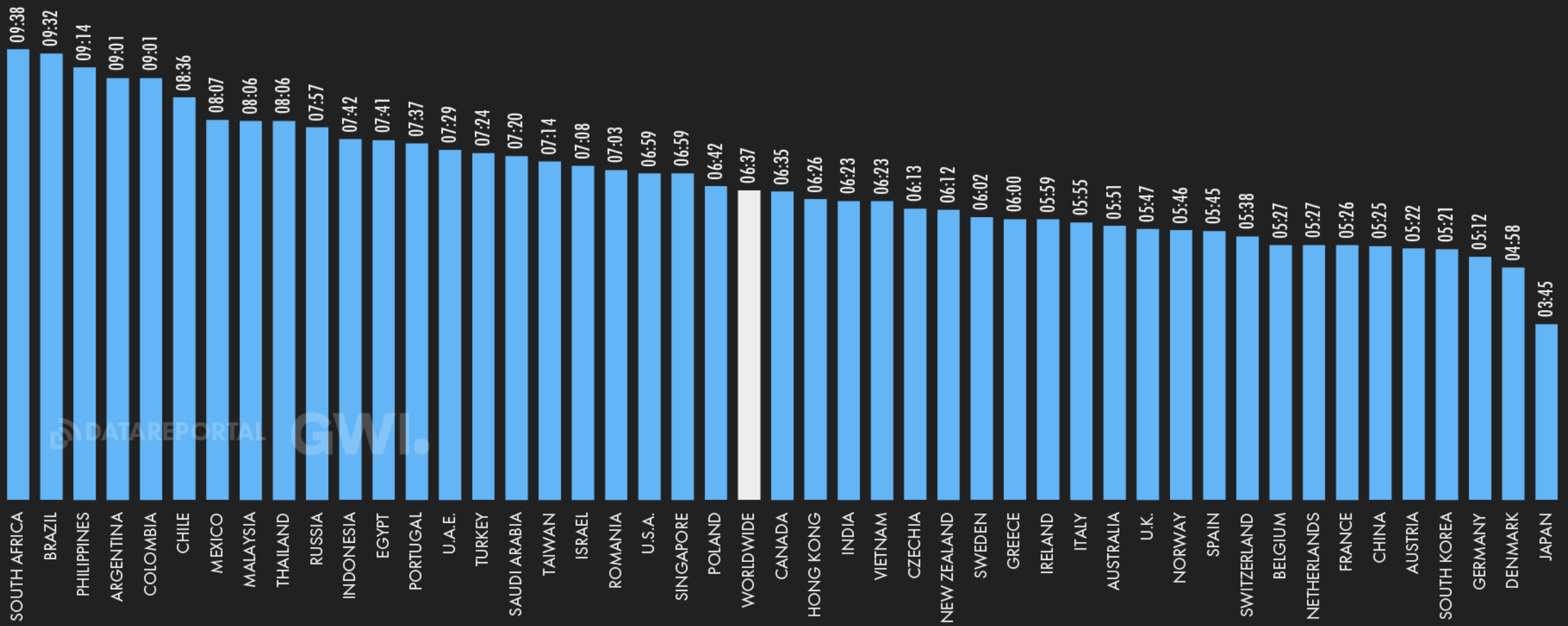
SOURCES: UNITED NATIONS; GOVERNMENT BODIES; GSMA INTELLIGENCE; ITU; WORLD BANK; EUROSTAT; CNNIC; APJII; IAMAI & KANTAR; CIA WORLD FACTBOOK; COMPANY ADVERTISING RESOURCES AND EARNINGS REPORTS; OCDH; BETA RESEARCH CENTER; KEPIOS ANALYSIS. **ADVISORY:** SOCIAL MEDIA USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. **COMPARABILITY:** SIGNIFICANT REVISIONS TO SOURCE DATA, INCLUDING COMPREHENSIVE REVISIONS TO POPULATION DATA. FIGURES ARE NOT COMPARABLE WITH PREVIOUS REPORTS. ALL FIGURES USE THE LATEST AVAILABLE DATA, BUT SOME SOURCE DATA MAY NOT HAVE BEEN UPDATED IN THE PAST YEAR. SEE NOTES ON DATA FOR FULL DETAILS.

JAN 2023

DAILY TIME SPENT USING THE INTERNET

AVERAGE AMOUNT OF TIME (IN HOURS AND MINUTES) THAT INTERNET USERS AGED 16 TO 64 SPEND USING THE INTERNET EACH DAY ON ANY DEVICE

GLOBAL OVERVIEW



SOURCE: GWI (Q3 2022). FIGURES REPRESENT THE FINDINGS OF A BROAD GLOBAL SURVEY OF INTERNET USERS AGED 16 TO 64. SEE GWI.COM FOR FULL DETAILS.

we are social

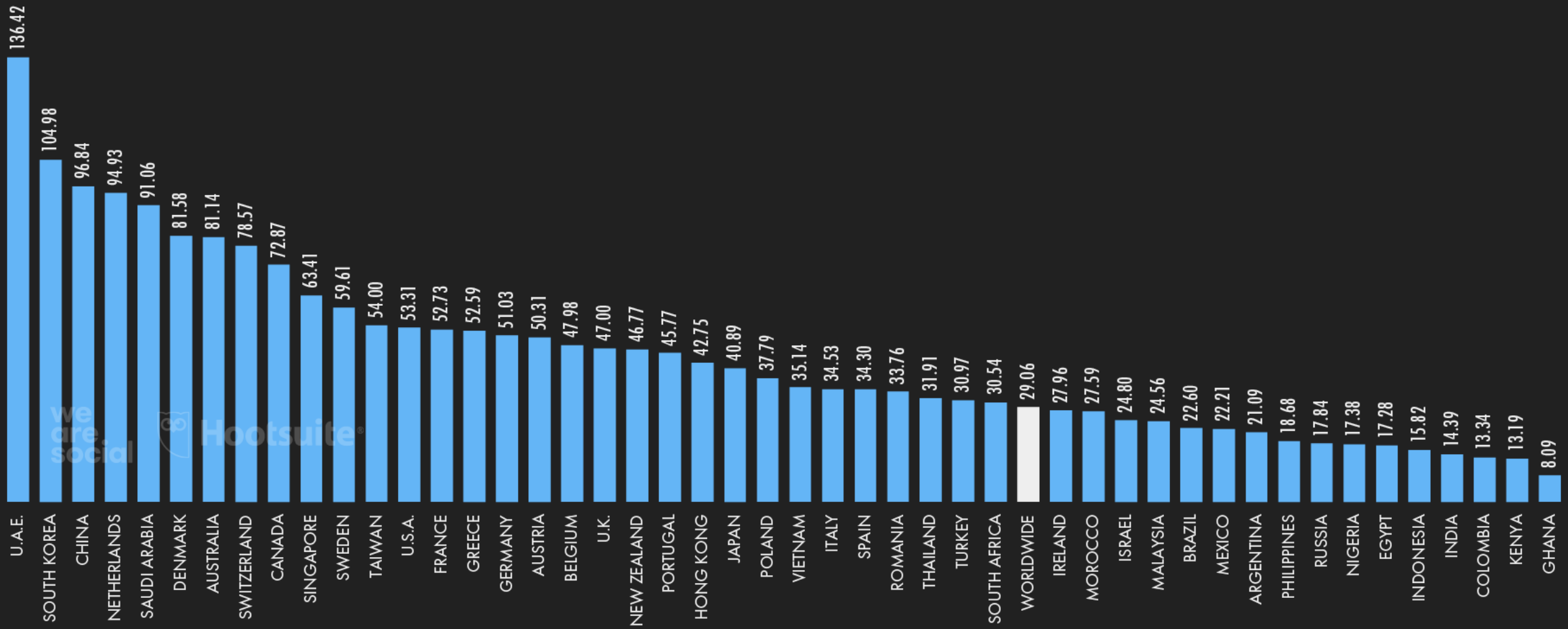
Meltwater

JAN 2022

MOBILE INTERNET CONNECTION SPEEDS

MEDIAN DOWNLOAD SPEEDS FOR MOBILE INTERNET CONNECTIONS (IN MBPS)

GLOBAL OVERVIEW



SOURCE: OOKLA. **NOTE:** FIGURES REPRESENT MEDIAN DOWNLOAD SPEEDS (IN MEGABITS PER SECOND) IN NOVEMBER 2021. **COMPARABILITY:** VERSIONS OF THIS CHART THAT FEATURED IN PREVIOUS REPORTS IN THIS SERIES USED MEAN VALUES (RATHER THAN MEDIAN VALUES), SO VALUES SHOWN HERE ARE NOT COMPARABLE WITH THOSE SHOWN IN PREVIOUS REPORTS.

Internet Evolution

LAN connectivity

Application-specific
More online content

Application/data
hosted in the “cloud”

Different ways to handle security as the Internet evolves

(APNIC)

Imperva

https://www.imperva.com/resources/resource-library/reports/2021-cyberthreat-defense-report/

CYBEREDGE GROUP

2020 Cyberthreat Defense Report

SURVEY DEMOGRAPHICS

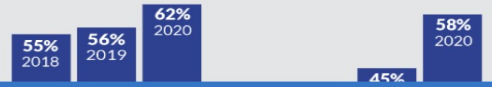
1,200 Qualified IT security decision makers & practitioners

19 Industries represented

17 Countries represented around the world

ARE PAID RANSOMS FUELING RANSOMWARE?

Ransomware attacks are at a record high, and so are the percentage of victimized organizations that paid associated ransoms.



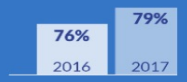
SECURITY'S BIGGEST OBSTACLES

These obstacles inhibit IT from defending cyberthreats:

- 1 TIE — Lack of skilled personnel
- 1 TIE — Low security awareness among employees
- 3 — Too much data to analyze
- 4 — Poor / insufficient automation of threat detection

RECORD-SETTIN

For the first time in the hi organizations experience (and more than a third su



SUSCEPTIBLE NA

The percentage of respor last year varied by nation

ACCESS OF EVIL

Cyberthreats causing the greatest concern include:

HELP WANTED

The percentage of organizations experiencing a shortfall of skilled IT security personnel keeps rising.

JISITIONS

gies targeted for

- Network behavior analysis (NBA)
- Deception technology / distributed honeypots

JISITIONS

gies targeted for

- 2 — Deception technology
- 4 — Application control (whitelist/blacklist)

RESEARCH SPONSORS

PLATINUM: (ISC)², Gigamon, imperva, Menlo Security

GOLD: CARBONITE, COLORTOKENS, netskope, opentext, perimeterx, WEBROOT

SILVER: ANITIAN, CybelAngel, Cymulate, DivvyCloud, expel, sysdig, ZEROFOX

Two years later… still the same!

What does means for us?

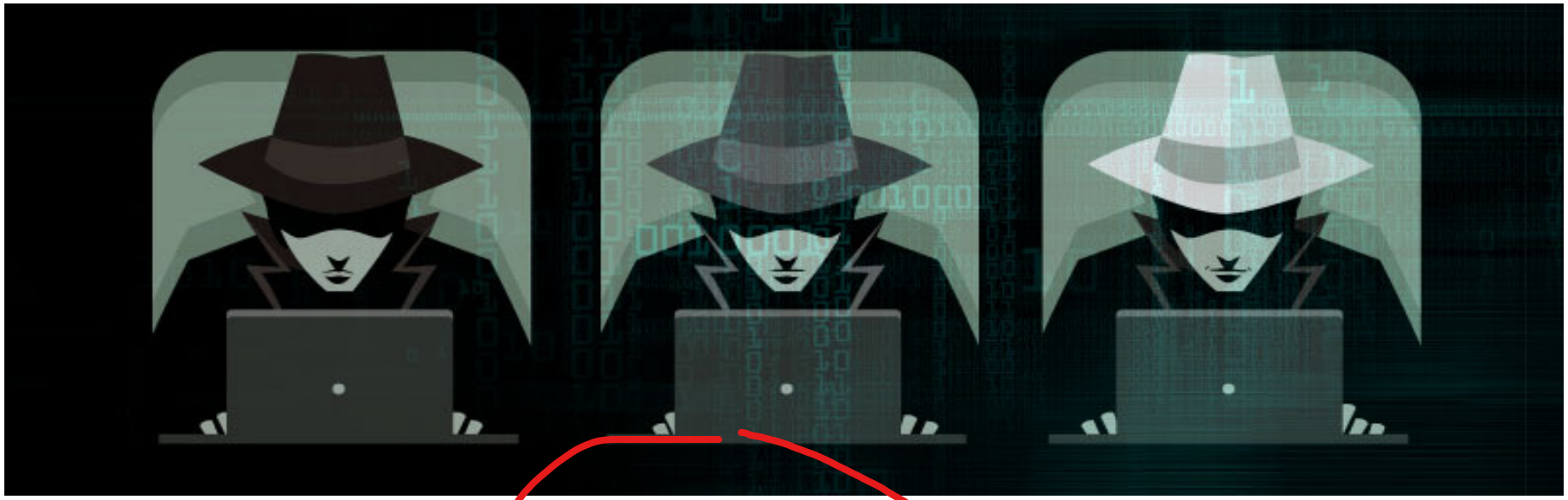
Motivation

- There are important ways you can protect yourself and your organization.

- But first
  “It is vital to understand the major methods cyber criminals use to accomplish attacks! “


TO BEAT A HACKER YOU NEED
TO THINK LIKE A HACKER

Types of Hackers and what they do



Black-hat hacker is an individual who attempts to gain unauthorized entry into a system or network to exploit them for malicious reasons.

Grey hat exploit networks and computer systems in the way that black hats do, but do so without any malicious intent, disclosing all loopholes and vulnerabilities to law enforcement agencies or intelligence agencies.

White-hat hacker, on the other hand, are deemed to be the good guys, working with organizations to strengthen the security of a system

Attack Motivation

- Nation States want **SECRETS**
- Organized criminals want **MONEY**
- Protesters or activists want **ATTENTION**
- Hackers and researchers want **KNOWLEDGE**

http://cartoonsmix.com/cartoons/national-security-agency-cartoon.html

Source: NANOG60 keynote presentation by Jeff Moss, Feb 2014

Attack Motivation

- Criminal
  - Criminal who use critical infrastructure as a tools to commit crime
  - Their motivation is money
- War Fighting/Espionage/Terrorist
  - What most people think of when talking about threats to critical infrastructure
- Patriotic/Principle
  - Large groups of people motivated by cause - be it national pride or a passion aka Anonymous

Attack Motivation

- Script kiddies:
  - little real ability, but can cause damage if you're careless
- Money makers:
  - Hack into machines, turn them into spam engines, etc.
- Government intelligence agencies, AKA Nation State Adversaries

Joy Hacks

- For fun
  - with little skill using known exploits
- Minimal damage
  - especially unpatched machines
- Random targets
  - anyone they can hit
- Most hackers start this way
  - learning curve

Opportunistic Hacks

- Skilled (often very skilled) - also don't care whom they hit
  - Know many different vulnerabilities and techniques
- Profiting is the goal - bank account thefts, botnets, ransomwares….
  - WannaCry? Petya?
- Most phishers, virus writers, etc.

Targeted Attack

- Have a specific target!
- Research the target and tailor attacks
  - physical reconnaissance
- At worst, an insider (behind all your defenses)
  - Not-so happy employee ☹
- Watch for tools like “spear-phishing”
- May use 0-days

Advanced Persistent Threats (APT)

- Highly skilled (well funded) - specific targets – Mostly 0-days
- Sometimes (not always) working for a nation-state
- An attack in which an unauthorized user gains access to a system or network and remains there for an extended period of time without being detected.

- Note: many lesser attacks blamed on APTs

Attack Vector

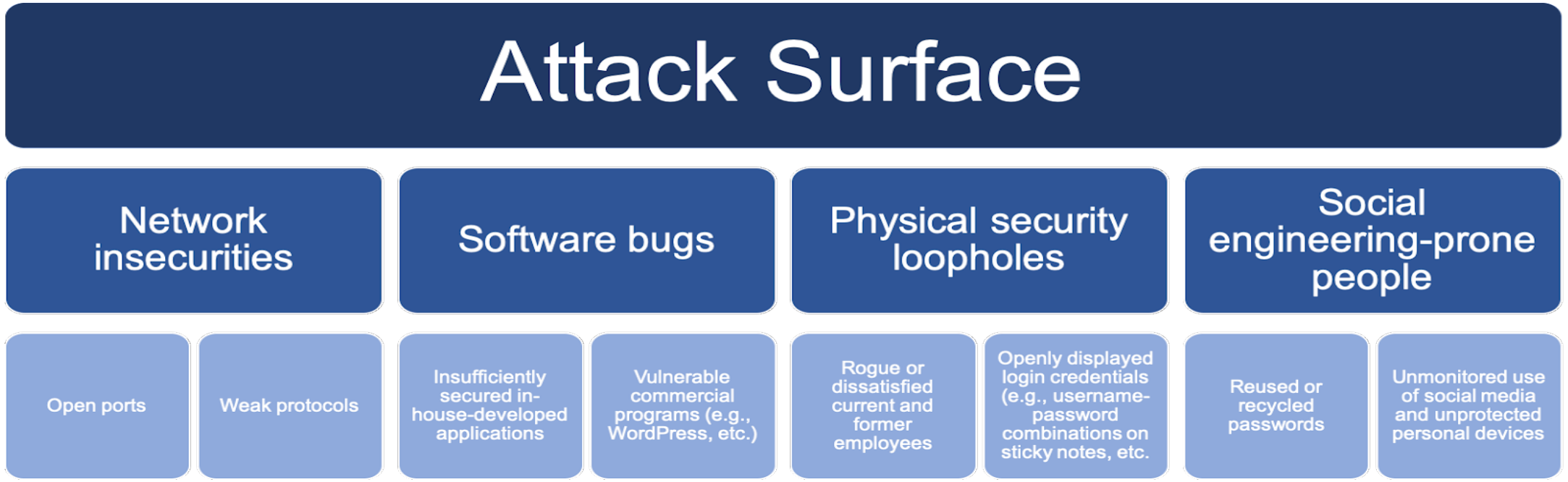
VS

Attack Surface

Attack Surface

What is an Attack Surface?

represented by all of the points on your network where an adversary can attempt to gain entry to your information systems.



Attack Vectors

What is an Attack Vector?

Attack vectors are the methods that adversaries use to breach or infiltrate your network.

Major Attack Vectors

1. Social Engineering: Phishing
2. Remote Access
3. Insider Threats
4. Brute-Force Attacks
5. Ransomware
6. Denial of Service
7. Access through Intermediaries

Social Engineering: Phishing

- Manipulating people into performing actions or divulging confidential information

Phone Call: This is John, the System Admin. What is your password?

In Person: What ethnicity are you? Your mother's maiden name?

BDO

Inbox

BU BDO Unibank

Terms And Conditions : OTP Confirmation!

SCAM!

Dear Valued Client,

Greetings from **BDO Online Banking**

Please be advised that we are requiring everyone to update their mobile number as part of our new online system.

Please immediately do so or the transactions you have made will not be processed.

You can verify your account at https://online.bdo.com.ph/

This link will lead to a FAKE BDO LOGIN site. Do not click!

These communication channels are available to you 24 hours a day, 7 days a week.

Thank you for banking online with us!

The BDO Online Banking Team

Important: Please save this message for future reference

BDO Unibank is supervised by the Bangko Sentral ng Pilipinas with contact number (02) 8708-7087 and email address consumeraffairs@bsp.gov.ph

Be smarter than a scammer.
#BDOAntiScam

Remote Access

- How
  - Through open ports or the exploitation of web code, hackers are able to gain unauthorized access to a server.
  - Via SQL injection, malware download…

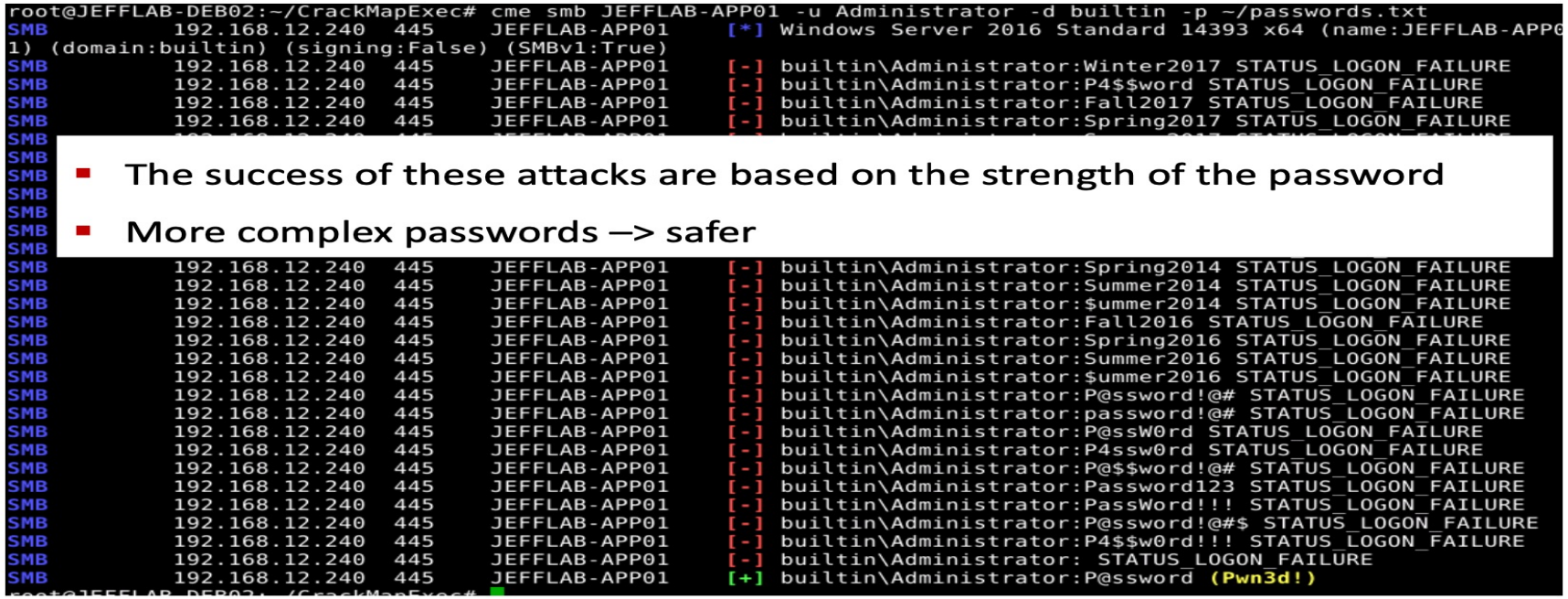
- Poorly configured devices are also easily accessible using default username/passwords known to each device
  - Identifying which particular device is easy via shodan.io

Insider Threats

- How:
  - Criminals are aided by the conscious assistance of an organization's employee(s)
- In some cases, weak security of an employee's devices is leveraged to launch further attacks from within the network
- Includes any kind of unauthorized or malicious use of organizational resources
  - Although most of the attacks are facilitated by external actors, insiders (with or without privileged access) are playing a key role in data breaches

Brute force Attacks

A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered.

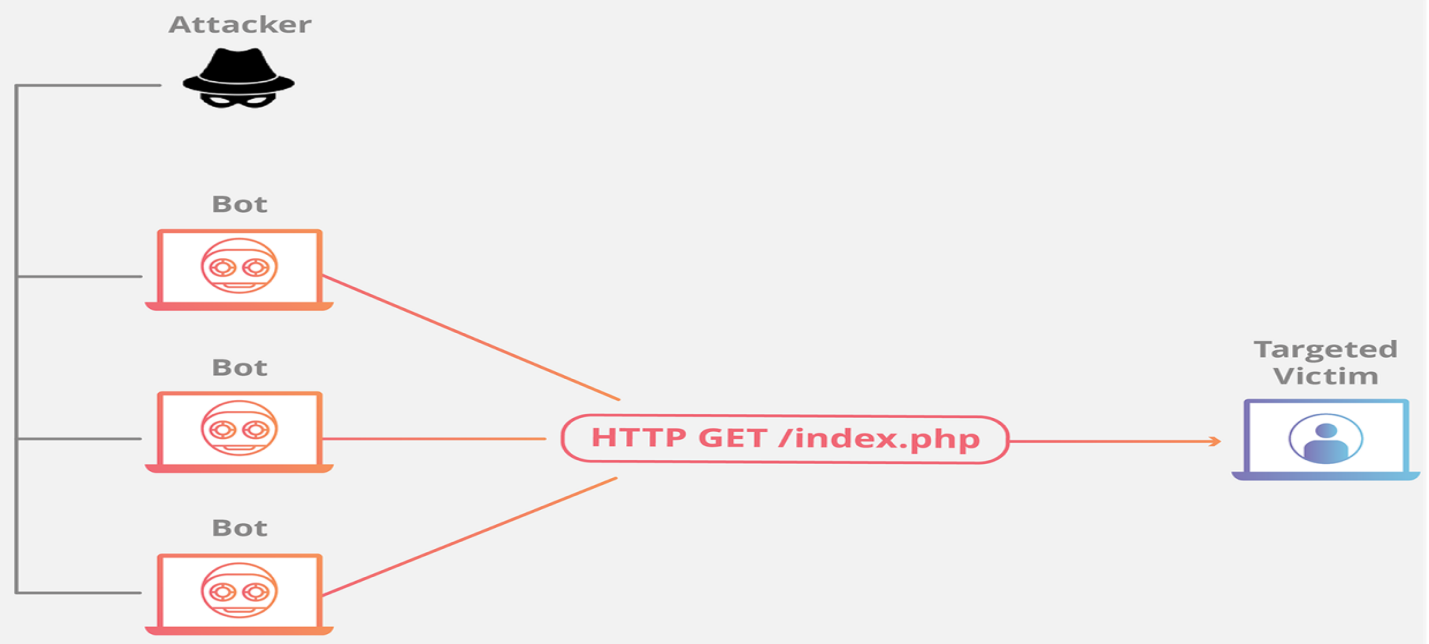


Ransomware

- Restricting access to a computer until a ransom is paid
- If no payment is received, the data is deleted or leaked
- Organizations have to chose between paying
  or
  losing critical data forever

Denial of Service

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.



Access through Intermediaries

- Doesn't require physical access to target machine(s)
- Leverages on Autorun feature of removable devices
  - And infects other removable devices soon-after
- Remember Stuxnet ?

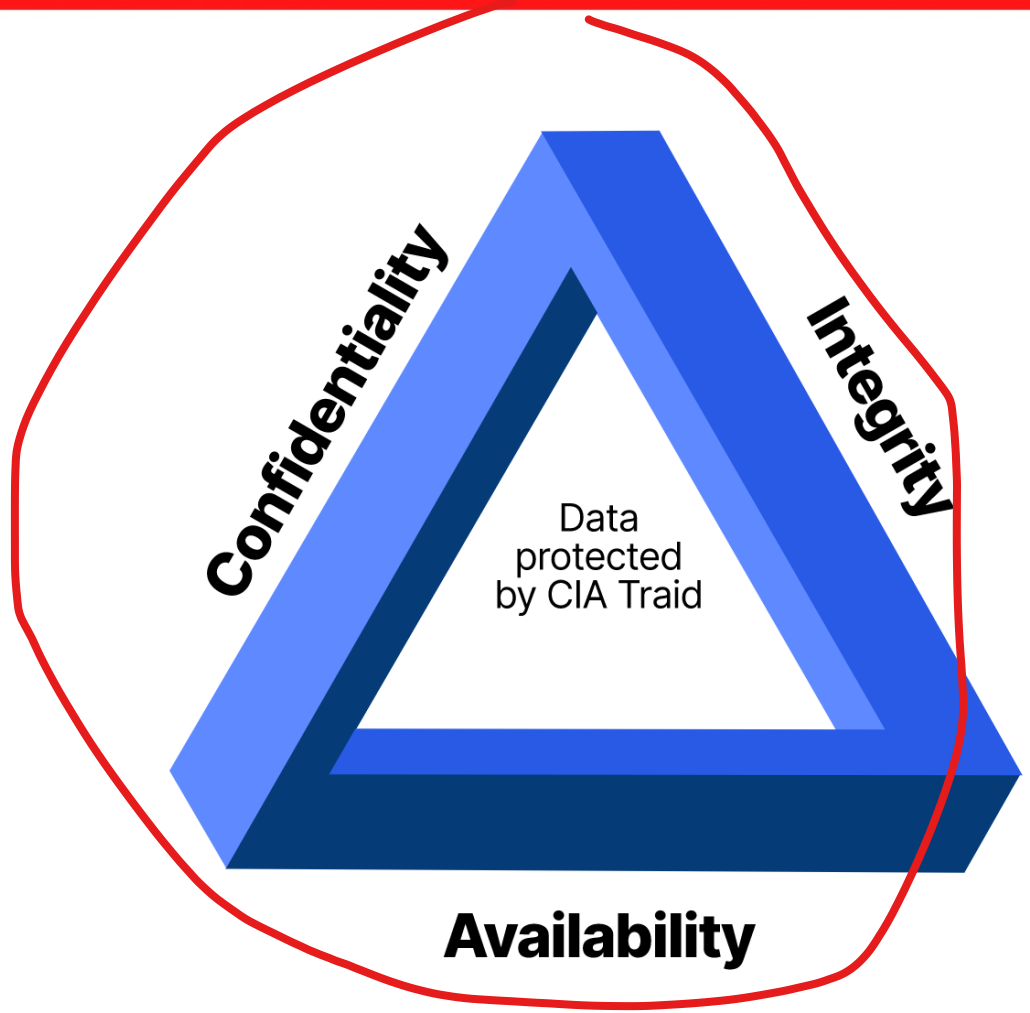
- .... is a malicious computer worm, first uncovered in 2010, thought to have been in development since at least 2005 !
- jointly built American/Israeli cyberweapon
- typically introduced to the target environment via an infected USB flash drive

Send your question

Is there any Differences?

CIA TRIAD

- The CIA triad is a common, respected model that forms the basis for the development of security systems and policies.



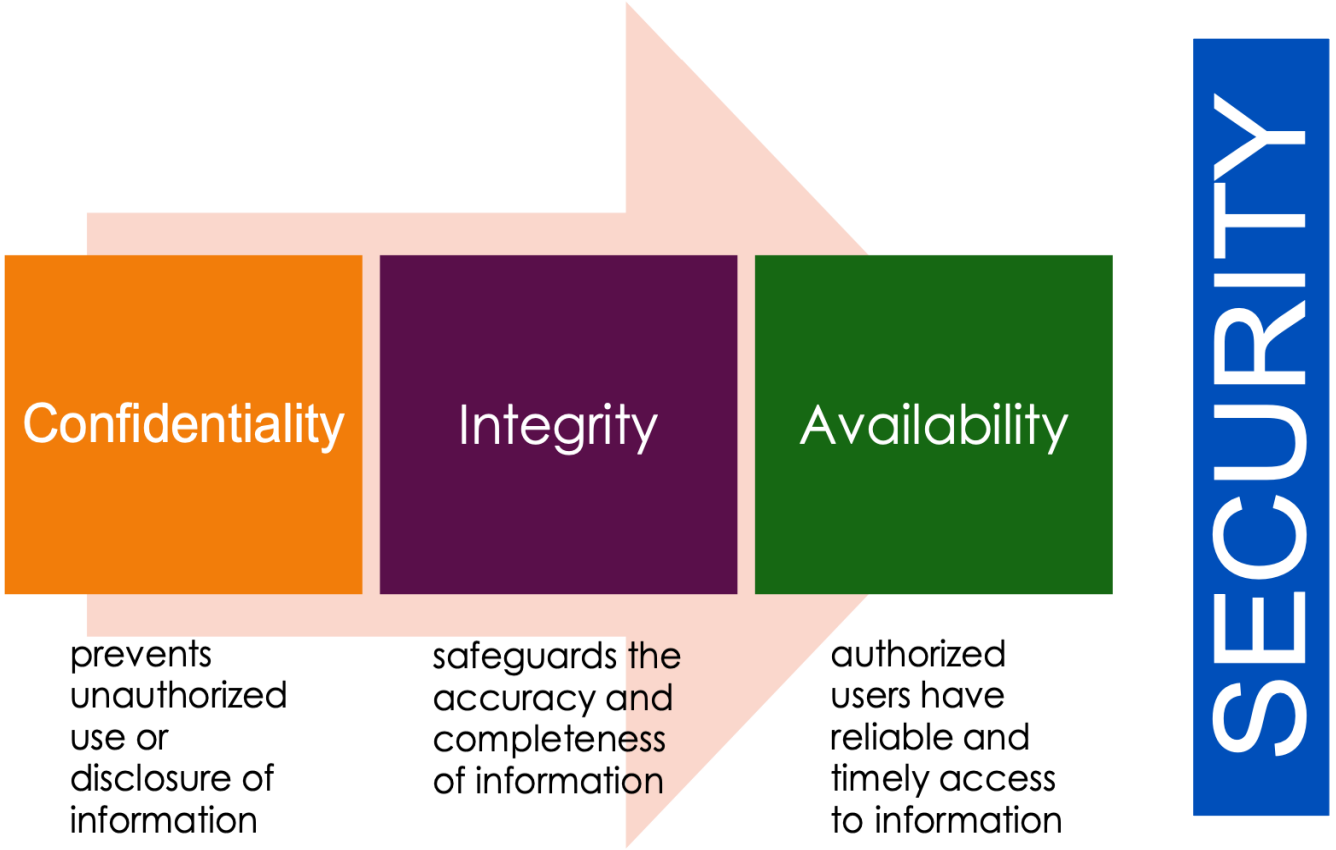
CIA TRIAD

Information Security (InfoSec)

- Information Security (InfoSec) is preservation of confidentiality, integrity and availability of information.

Cyber Security

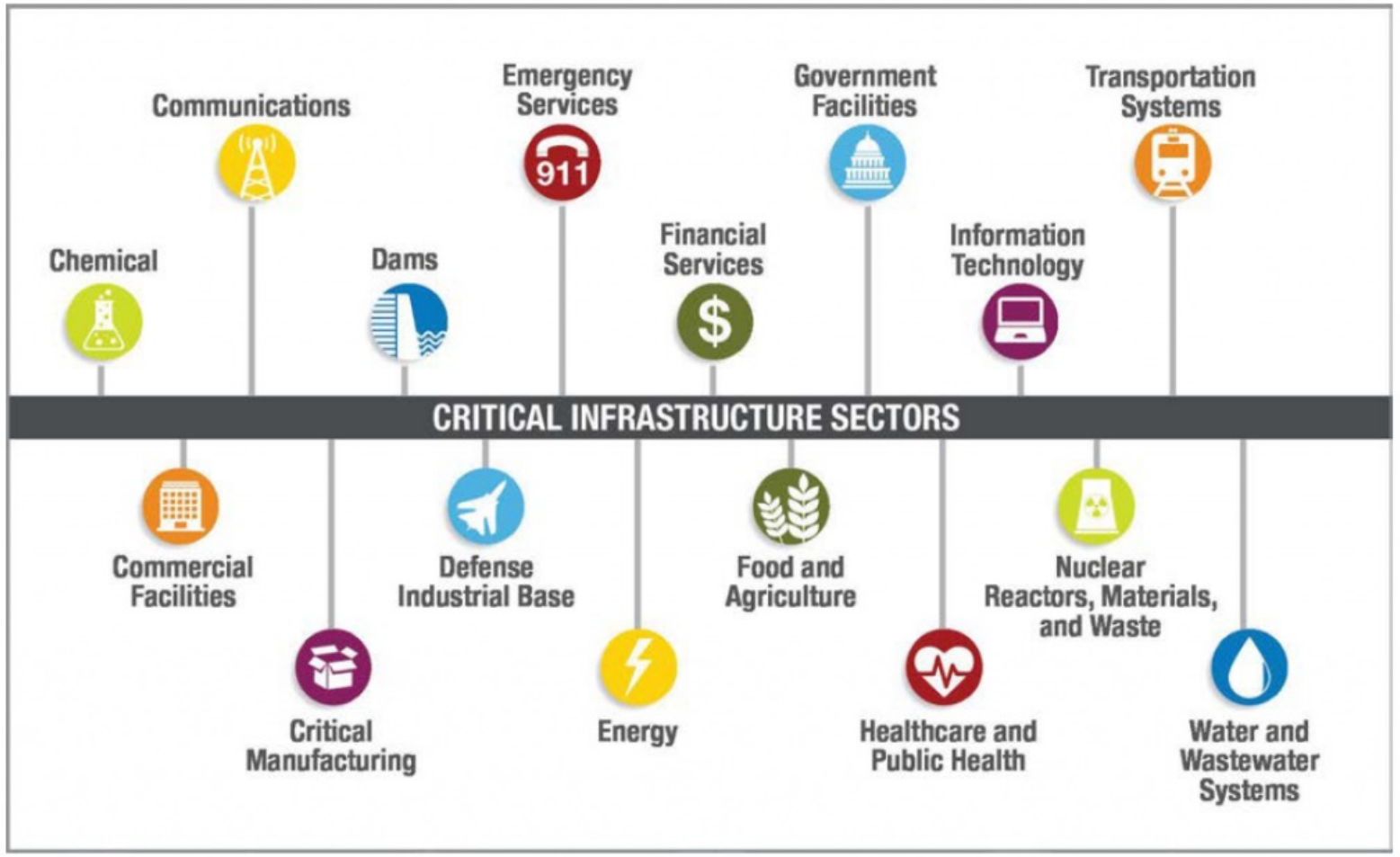
- Defined as the "preservation of confidentiality, integrity and availability of information in the Cyberspace."



CIA objectives

To achieve the CIA objectives organizations must protect two aspects or their IT environment: *application security* and *data security*.

Critical Infrastructure



Critical Infrastructure is the body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public's health and/or safety.

The United States recognizes 16 distinct sectors of critical infrastructure, which are systems that are considered crucial to national economic security and national public health.

Critical Infrastructure

Information technology is the fundamental sector on which all others depend.

Recent Major Cyber Incidents involving Critical Infrastructure

Critical Infrastructure

“Mr Blount also told Senators the decision to pay a $4.4m (£3.1m) ransom to hackers in Bitcoin was the "hardest decision" in his career.

Economy | Global Car Industry

US fuel pipeline hackers 'didn't mean to create problems'

By Mary-Ann Russon
Business reporter, BBC News

10 May

COLONIAL PIPELINE

A cyber-criminal gang that took a major US fuel pipeline offline over the weekend has acknowledged the incident in a public statement.

"Our goal is to make money and not creating problems for society," DarkSide wrote on its website.

https://www.bbc.com/news/business-57050690

THE
NATIONAL LAW REVIEW

June 9, 2021
Volume XI, Number 160

Another Attack on Critical Infrastructure – New York's Subway Hacked

Tuesday, June 8, 2021

In April, New York's subway authority was hacked by a group of cybercriminals with suspected Chinese government connections. The authority is responsible for operating all of New York's train and bus systems and the attack exposed vulnerabilities in the services used by millions every day.

Fortunately, the authority operates a multi-layered security system which reportedly prevented the attack from spreading to other related systems. It's been reported that the attack didn't compromise any personal information of customers or employees and didn't involve any ransom or demands.

It's still not clear why the authority was targeted, but reports in the New York Times have suggested two theories: (1) that the motivation for the attack could have been related to China's rail car production industry and

ARTICLE BY

Cameron Abbott
Rob Pulham

K&L Gates
Cyberwatch: Australia

K&L GATES

Administrative & Regulatory
Communications, Media & Internet
Consumer Protection
Corporate & Business Organizations
Global
New York

TRENDING LEGAL ANALYSIS

Cal/OSHA Approves Revised Emergency Temporary Standards
By Sheppard, Mullin, Richter & Hampton LLP

Wisconsin Supreme Court Limits Tort Claims Related to Conduct Following Worker's Compensation Injury
By Ogletree, Deakins, Nash, Smoak & Stewart, P.C.

Global Employment Law Update - Part 4: Isreal to Malaysia
By McDermott Will & Emery

Cal/OSHA Approves Minor Modifications to COVID-19 Prevention Emergency Temporary Standards (ETS)
By Mintz

In the News #ran #diversity #weeklywrap #silicon #remoteworkforce #deepdive #kubernetes #electionsecurity

Articles / News

SolarWinds Supply Chain Attack Led to FireEye, U.S. Government Breaches

Jessica Lyons Hardcastle | Managing Editor
December 14, 2020 11:26 PM

Share this article:

Supply Chain Attack is a type of cyber attack targeting and attacking insecure elements of the software supply chain.

- A vulnerability within the Solarwinds Orion monitoring products.
- Sunburst and Supernova malware

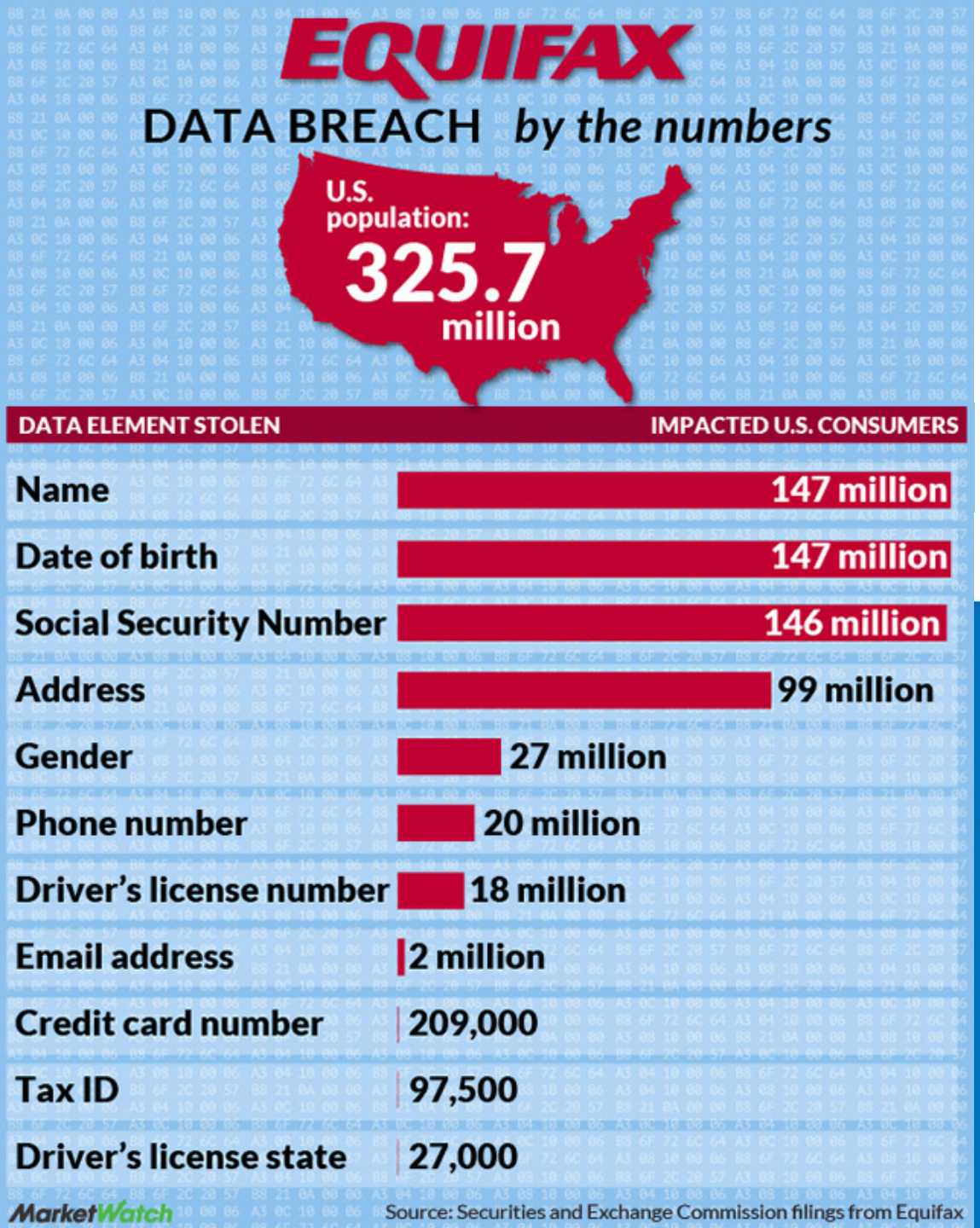
December 2020

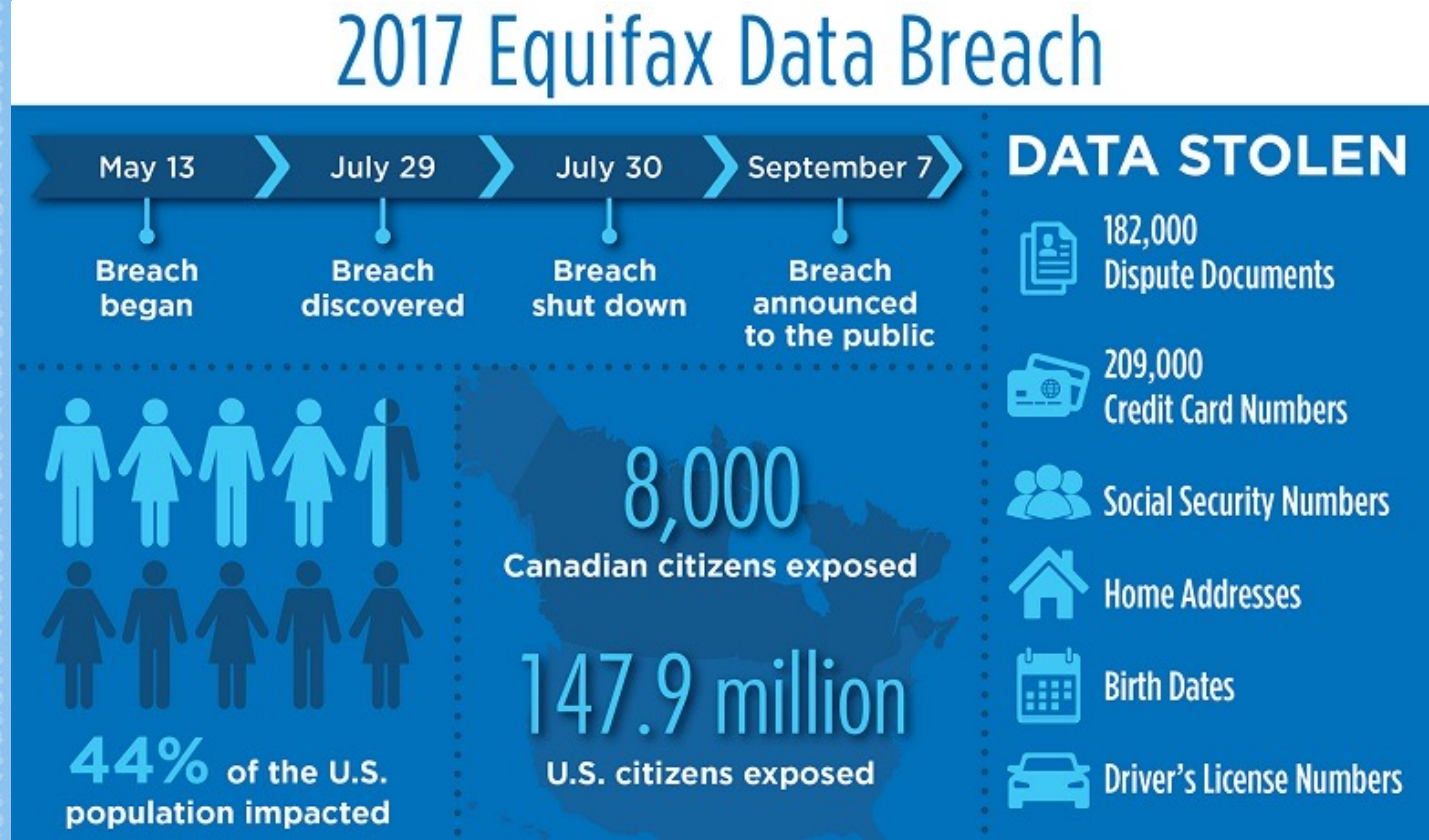
Send your question


amazon
UBER
Microsoft
Google
TESLA
The world's most valuable resource is no longer oil, but data.
The Economist - May 2017
David Parkins

Recent Major Cyber Incidents involving DATA Breach

The Equifax data breach occurred between May and July 2017 at the American credit bureau Equifax. Private records of 147.9 million Americans along with 15.2 million British citizens and about 19,000 Canadian citizens were compromised in the breach, making it one of the largest cybercrimes related to identity theft.





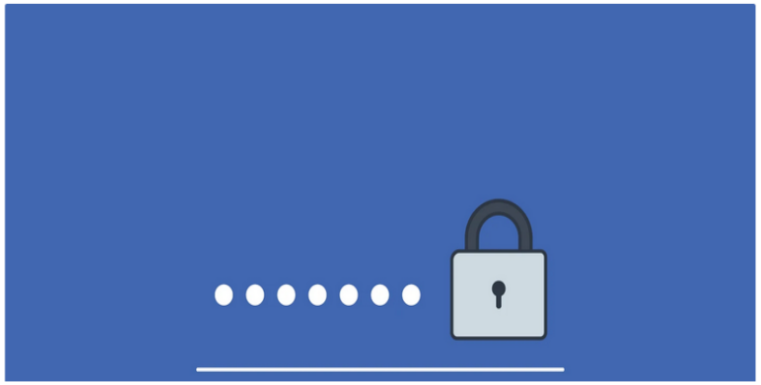
Recent Incidents

- Facebook (March 2019)
  - announced that it was storing user passwords (~600 million) in plain text
    - since 2012!
    - Could be read by FB employees
  - April
    - Oops.. Wasn't just Facebook accounts, but also some Instagram accts ☹

Facebook

Keeping Passwords Secure

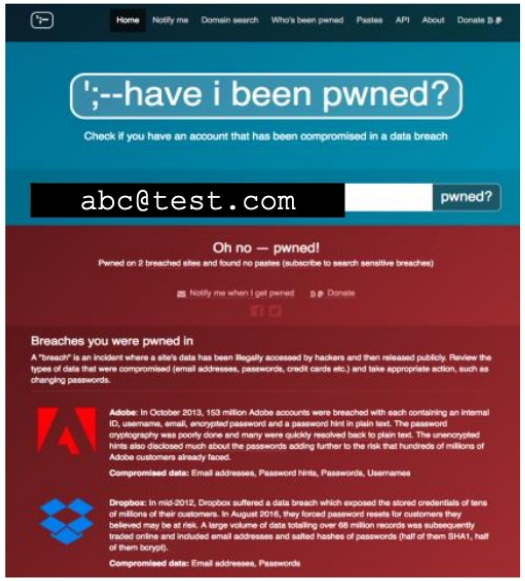
March 21, 2019

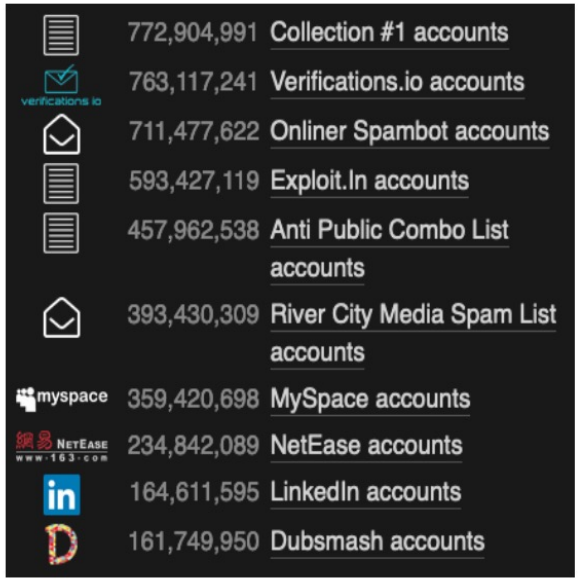


https://about.fb.com/news/2019/03/keeping-passwords-secure/

haveibeenpwned.com

- Have you been compromised?
  - Tracks compromised accounts and released into the wild
    - 364 pwned websites
    - >7 million pwned accounts
    - ~100K pastes





'Data breach' reportedly exposes 345K sensitive SolGen documents

By CNN Philippines Staff

Published May 3, 2021 4:49:42 PM

Updated May 3, 2021 6:01:00 PM

Latest from this section

ASEAN, China agree to exercise self-restraint, avoid disputes in South China Sea

statement on reported breach of 879,699 Filipino accounts

APR 5, 2021 5:46 PM PHT

GELO GONZALES

Statement of NPC on S&R data breach

November 24, 2021 | 9:27 PM GMT+0800 Last Edit: November 24, 2021

The National Privacy Commission (NPC) received an initial breach notification report on November 15, 2021, 4:47 PM, from S&R Membership Shopping in relation to a cyber-attack that may have compromised its members' contact information. The S&R said that it discovered the security incident last November 14, 2021.

The company has then submitted an supplemental breach report today, November 24, 2021, confirming that the subject of the ransomware attack was the S&R membership system affecting twenty-two thousand (22,000) data subjects. According to the said report, the following personal data were compromised:

Philippines Response to Cyber Security Threats

- **R.A. 10175**
  Cybercrime Prevention Act of 2012
- **R.A. 10173**
  Data Privacy Act of 2012

What are the look up references for the cyber crime and data privacy risks that must be mitigated?

R.A. 10175 **Cybercrime Prevention Act of 2012**	An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefore and for other purposes
R.A. 10173 Data Privacy Act of 2012	An act protecting individual personal information in information and communication systems in the government and the private sector, creating for this purpose a National Privacy Commission, and for other purposes.

R.A. 10175
Cybercrime Prevention Act of 2012

1. It is offense against the confidentiality, integrity and availability of computer data and systems.

1.1 Illegal Access.	Access to the whole or any part of a computer system without right
1.2 Illegal Interception	Interception made by technical means without right
1.3 Data Interference.	Intentional or reckless alteration, damaging, deletion of computer data
1.4 System Interference	Intentional alteration or reckless interference with the functioning of a computer or computer network
1.5 Misuse of Devices	Use, production, sale, procurement, importation, distribution, or otherwise making available, without right
1.6 Cyber Squatting	Acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same

2. It is offense related with the use of computer.

2.1 Forgery	Input, alteration, or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic
2.2 Fraud	Unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent
2.3 Identity Theft	Intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right.

3. It is offense related to creation and sharing of content.

3.1 Cybersex	Willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system
3.2 Child Pornography	Unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system
3.3 Libel	Unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system

Data Privacy vs Right to Privacy

Data Privacy Violation

- Privacy violation is illegal or unwanted act that endangers the privacy rights of a person and security of personal data.
- Data privacy violation is penalized act according to R.A. 10173 Chapter VIII. The complaint can be made through the use of NPC Complaint-Assisted Form.

Section 25 Unauthorized processing	Section 30 Concealment of breach
Section 26 Negligence in access	Section 31 Malicious disclosure
Section 27 Improper disposal	Section 32 Unauthorized disclosure
Section 28 Unauthorized purpose	Section 33 Combination of acts
Section 29 Unauthorized access or intentional breach	

Data Privacy Violation

1. Unauthorized processing 3-6 years imprisonment 500K-4M penalty	It is when personal information is processed without the consent of the data subject, or without being authorized using lawful criteria
2. Negligence in access 1-6 years imprisonment 500K-4M penalty	It is when personal information is made accessible due to negligence and without being authorized by any existing law.

Data Privacy Violation

3. Improper disposal 6 mos-3 years imprisonment 100K-1M penalty	It is when personal information is knowingly or negligently disposed, discard, or abandon in an area accessible to the public or has otherwise placed the personal information of an individual in any container for trash collection
4. Unauthorized purpose **1-7 years imprisonment** **500K-2M penalty**	It is when personal information is processed for purposes not authorized by the data subject, or otherwise authorized by any existing laws.

Data Privacy Violation

5. Unauthorized access or intentional breach 1-3 years imprisonment 500K-2M penalty	It is when an individual handling personal information knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information are stored.
6. Concealed breach 1-5 years imprisonment 500K-1M penalty	It is when an individual or entity who has knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f) of the Act, intentionally or by omission conceals the fact of such security breach.

Data Privacy Violation

7. Malicious disclosure 1-65years imprisonment 500K-1M penalty	It is when an individual or entity with malice or in bad faith, discloses unwarranted or false information relative to any personal information or sensitive personal information obtained by him or her
8. Unauthorized disclosure 1-5 years imprisonment 500K-2M penalty	It is when an individual or entity discloses to third party personal information not covered by legitimate purpose, lawful criteria, and without the consent of the data subject.

“Innocent of the law excuses no one.”

Send your question

Email:

manaagas@clsu.edu.ph
marlon.naagas@prime.edu.ph