

How to deal with the wave of cyberattacks: Revisiting the Essence of Cyber Security

Paper serving as a basis for presentation to the academic conference of
BAASANA August 2021

**Dr. Frank Owarish, CEO, International Institute for Strategic Research
and Training (NYS registered think tank), New York City, USA**

&

**Dr. Donald Hsu, Professor Dominican College, Doctoral Faculty
University of Phoenix, President Chinese American Scholars
Association, New York City, USA**

Introduction

Cyberattack 101

A **cyberattack** is any offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. An attacker is a person or process that attempts to access data, functions, or other restricted areas of the system without authorization, potentially with malicious intent.^[1] Depending on the context, cyberattacks can be part of cyberwarfare or cyberterrorism. A cyberattack can be employed by sovereign states, individuals, groups, society, or organizations, and it may originate from an anonymous source. A product that facilitates a cyberattack is sometimes called a cyberweapon.

(source: Wikipedia)

Cyber attacks

There has been a wave of cyberattacks recently.
The pandemic is a factor, with increasing use of computer systems
Most of these systems do not have sophisticated security systems
and are thus vulnerable

Cyberattacks, ransomware

We have made strides in computer technology yet we keep hearing of cyberattacks. Is this a technical or political issue or both?

The Colonial Pipeline showed the agony that can happen. In a statement June 07, 2021 Pipeline CEO Joseph Blount said he was grateful for the FBI's efforts and said holding hackers accountable and disrupting their activities "is the best way to deter and defend against future attacks of this nature. "The private sector also has an equally important role to play and we must continue to take cyber threats seriously and invest accordingly to harden our defenses," he added.

Thought

Is not that reasoning faulty?
Being reactive compared with proactive
Is not prevention better than cure?

Review of the basics: computer security, cyber security, IT security

The protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. The field is becoming increasingly significant due to the increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.^[3]

(Source: Wikipedia)

The 4 Fundamentals to IT Security are:

Data Confidentiality. One of the biggest roles of IT security is protecting sensitive information, especially concerning the data that needs to be kept confidential. ...

Data Integrity. ...

Data Authenticity. ...

Data Availability.

www.pacetechnical.com

More cyberattacks

Thousands of companies affected worldwide

<https://www.msn.com/en-us/news/us/hacking-attack-likely-hit-thousands-of-new-targets/ar-AALIU9d?ocid=msedgdhp&pc=U531>

Survey finds

Massive gaps in awareness of cyberattacks

<https://www.zdnet.com/article/survey-finds-massive-gap-in-awareness-of-cyberattacks/>

Ransomware

Hackers may be in over their heads

<https://www.msn.com/en-us/news/world/ransomware-hackers-may-be-in-over-their-heads-they-may-not-even-get-paid/ar-AALQZ5S?ocid=msedgdhp&pc=U531>

Cyberattacks on email system

<https://www.tessian.com/blog/email-attack-types/>

How to protect against cyberattacks

Many companies are using systems which are old and under protected

The question is why don't we invest in the necessary security mechanism considering that the protective technologies are available?

Universities can help at relatively low costs (training, system design); government agencies as well

High level strategy and action

As cyberattacks surge, President Biden is seeking to mount a better defense

<https://www.npr.org/2021/06/04/1003262750/as-cyber-attacks-surge-biden-seeks-to-mount-a-better-defense>

International agreement

In June 2021, Russia, US and other countries reached an agreement on cyber hacking

https://www.washingtonpost.com/national-security/russia-us-un-cyber-norms/2021/06/12/9b608cd4-866b-11eb-bfdf-4d36dab83a6d_story.html

Protection mechanisms

Obviously, Microsoft (exchange servers worldwide) and Kaseya (technical support to businesses worldwide) did not do enough to protect their clients

New threats

With the pandemic, more workers do their work from home; more online purchases and so vulnerabilities are everywhere; even education from home facing challenges (children at risks sex predators)

Protection through several layers of security

Almost like an onion, for example, for gift card transaction, Macy's asks for and correlate several sets of information including the bank or credit or debit card company to verify; at times, canceling the order and asks the one making the order to call a special phone number when there is a verification process and the order goes through

Bunch of tools

Encryption, firewalls: bunch of tools with necessary investment of resources

https://www.google.com/search?q=encryption&rlz=1C1APWK_enUS915US915&oq=encryption&aqs=chrome..69i57j0j0i433j0j0i433j0l5.14278j0j15&sourceid=chrome&ie=UTF-8

Conclusion 1

UK Comprehensive approach
National Cyber Security Centre

<https://www.ncsc.gov.uk/>

Conclusion 2

All the tools are available, but costs and skill of implementation depends on organizations: companies have to develop and maintain adequate security systems with clear policies to employees and clients; offsite back up

and individuals have to be properly informed and vigilant.

Above all. regular review of the adequacy of security systems with upgrade as needed

Conclusion 3

<https://www.sentinelone.com/>