BASIC CYBER DEFENCE EDUCATION FOR EVERYONE

Alexandru TĂBUȘCĂ[87]

Silvia-Maria TĂBUȘCĂ[88]

Abstract:
Basic cyber defence has become a mandatory requirement nowadays, for almost everyone. Gone are the days when only computer science nerds and IT specialists where required to know and take care of the security aspects of electronic devices. Especially after the savage war unleashed by the Russian aggressors onto Ukraine, the whole world realized how important is the safety of our online environment. Only after both the Kremlin led aggressors and the civilized world attacked and counter-attacked within the online battlefield, especially and mostly based on different DDoS attack flavors, most people understood how important cyber defence is today. In an era where virtually everything is run/managed/supervised or at least aided by computers linked to the mother-network, the Internet, we rely on the technology being present, available, and working in all aspects of our lives.

Keywords: you must use between 4 and 8 keywords

JEL Classification: I2, L86, K24

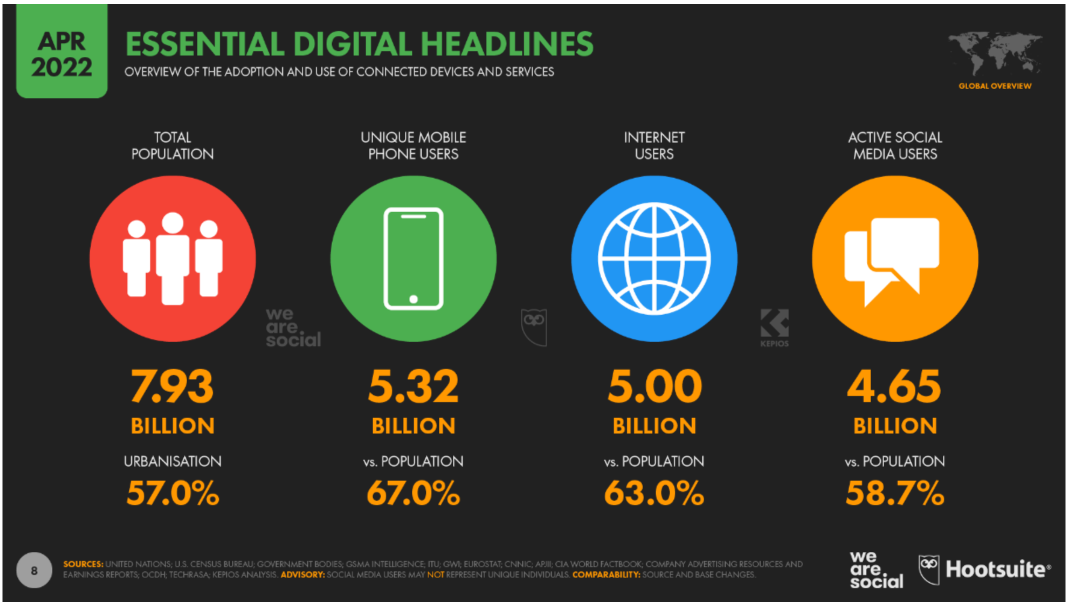
1. Introduction

Basic cyber defence has become a mandatory requirement nowadays, for almost everyone. Gone are the days when only computer science nerds and IT specialists where required to know and take care of the security aspects of electronic devices. Especially after the savage war unleashed by the Russian aggressor hoards onto Ukraine, the whole world realized how important is the safety of our online environment. Only after both the Kremlin led aggressors and the civilized world attacked and counter-attacked within the online battlefield, especially and mostly based on different DDoS attack flavors, most people understood how important cyber defence is today. In an era where virtually everything is run/managed/supervised or at least aided by computers linked to the mother-network, the Internet, we rely on the technology being present, available, and working in all aspects of our lives.

[87] PhD Associate Professor, Romanian-American University, Bucharest, tabusca.alexandru@profesor.rau.ro

[88] PhD Lecturer, Director of the Center for Human Rights and Migration – Romanian-American University, Bucharest, silvia.tabusca@profesor.rau.ro

In 2022, the most up-to-date research show that around 5 billion people are using the all-knowing Internet in order to help them take care of different things. This number means that approximately 62% of the Earth population connects to the internet to work, learn, look for information or conduct business. Moreover, more than 70% of the people that are not yet connected to the internet are in fact restricted from it due to infrastructure problems and the underdevelopment of their living areas – they are mostly located in Africa and Asia (South and East Asia generally).



APR 2022

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
7.93 BILLION	5.32 BILLION	5.00 BILLION	4.65 BILLION
URBANISATION 57.0%	vs. POPULATION 67.0%	vs. POPULATION 63.0%	vs. POPULATION 58.7%

8

SOURCES: UNITED NATIONS; U.S. CENSUS BUREAU; GOVERNMENT BODIES; GSMA INTELLIGENCE; ITU; GWI; EUROSTAT; CNNIC; APJII; CIA WORLD FACTBOOK; COMPANY ADVERTISING RESOURCES AND EARNINGS REPORTS; OCDH; TECHRASA; KEPIOS ANALYSIS. ADVISORY: SOCIAL MEDIA USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. COMPARABILITY: SOURCE AND BASE CHANGES.

Figure 1. Internet usage in 2022[89]

A quick view to the above infographic in Figure 1 shows that most of the world population, approximately 57% lives in urban areas. As these areas are more prone to modernization, and as the latest 5-years trends show that more and more people move to the urban areas (or their areas become urbanized), the normal trend of internet users will for sure remain on the increasing side. During the last years, due to the COVID-19 pandemic, there were a couple of reverse trends in punctual areas, including a movement of population from urban towards rural areas, all over the United States of America [1] and Europe [2]. Nevertheless, that trend was heavily countered by the explosion of the online activities, with practically everything from education to health services, from meetings to accounting, from exams to shopping, from banking to networking, moving to the online stage. This fact brought a huge increase in the number of Internet users, especially constant users of online services.

Even though the Internet has long become a standard utility in our lives, especially within the European and North American areas, but also in (most of) Asia and the other continents, the right to use the internet, as a regulated right, is something of a new. Only in 2010 there

[89] Source: https://datareportal.com/global-digital-overview

was the first official law that [3] enforced, in Finland, the internet connection as a right similar to having access to water, electricity or education services.

2. Current context

Of course, the reliance on Internet, online, usage has brough by a huge temptation for a lot of actors to try and interfere with malevolent intent. From wannabe hackers to plain dumb spammers, from economic schemes to cyberterrorists and even state actors. From current research, different cybercrimes were successful at an ever-increasing rate during the last 7 years – with a different degree of importance and loss-level. In 2014 specialists calculated that more than 61% of entities with an online presence have been compromised by one type of cyber-attack (at least, with any type of such an attack). Besides a temporary setback in percentages, in 2018, the trend is unfortunately on a constant upwards direction.

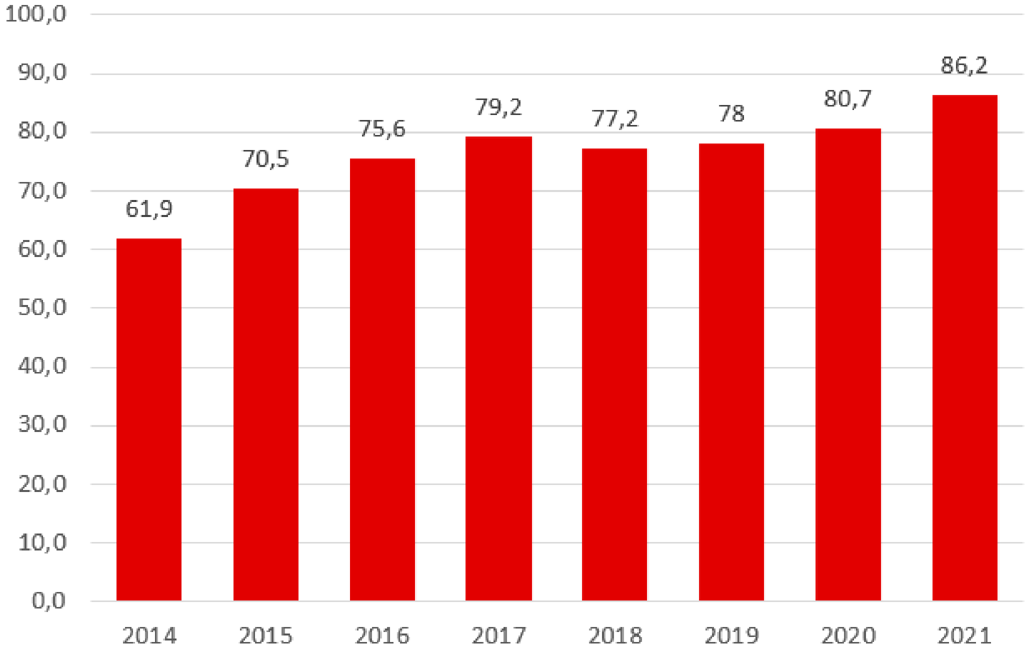


Figure 2. Entities that were targeted by at least one successful cyber-attack (percentages)[90]

These grim statistics require a coordinated and fast response from the entire society. Within the entities mentioned above (companies, government organizations, NGOs, education institutions, etc.) we count no less than approximately 75% of all registered entities in the European Union and United States of America. This huge number of entities employ a huge

[90] Source: https://securityboulevard.com/2021/11/choose-the-right-vapt-services-provider/

number of people but, unfortunately, only a very small percentage of them are IT specialists, out of which an even smaller number are active in the field of cyber security.

In order to tackle the ever-increasing numbers of cyber security specialists need by the business environment the educational systems have brough to the market new educational programs defined in this field. Alas, there is an impossibility to radically increase the number of available cyber-defence specialists in short time. First of all, the graduation of such programs take time, and second, the graduation of such programs is a much difficult task than other study programs. It is not possible to become a cyber-security specialist without a very strong technical background and special skills. The cyber-security area is a very specialized, niche, area within the computer science field, requiring even more specialized and complex skills and capacities for becoming a successful professional. The only short-term response that cand save the day is to increase the basic knowledge of most undergraduate or even high school students in the field of cyber-security. Most of the successful attacks are based on human weakness, either at direct level (week passwords, shared secret credentials, etc.) or indirect (social engineering, fishing, etc.). If we could, even with basic information, increase the level of awareness related to cyber-security for a huge number of employees, this would make a real difference.

3. Cyber-security basics for the masses

As we already mentioned earlier, there simply are not enough highly skilled cyber-security professionals available on the labour market. But, even if there were enough persons with these skills available for hire, the ugly truth is that we would not be able to stop all attacks within the online environment. There simply are too many possible threats, they always evolve and are permanently looking for opportunities to breach the IT defence.

We can mention here: pre-existent exploits related to programming errors/backdoors inside our IT software/hardware assets, internal attacks carried out by our employees that abuse their right/privileges to access different resources, mistakes of our employees that can by mistake transmit material they are not supposed to, different and numerous ways for all-kind of malevolent actors to breach our cyber-security defenses. One very dedicated attacker (either individually or within a group) will eventually be able to penetrate almost all kinds of defenses but the most updated and secured one (usually found only at governmental/military/intelligence levels).

Nevertheless, the facts mentioned above must not mean that we have to surrender! Even though we cannot stop 100% of the cyber-attack we can limit the penetration exposure of our entity and prevent the vast majority of attacks by just knowing and enforcing several basic key-elements of cybersecurity and paying attention to keep a permanent cyber-security relevant posture. The concept of cyber-security posture represents an all-around level of awareness and active measures in the field of cyber-security. Our entity has a strong cyber-security posture if we have covered all the required elements that must be put in place to help mitigate the impact of cyber-attacks on our entity.

Most specialists in the field agree to the following list of elements (eight) as mandatory for a powerful cyber-security posture at entity level:

- Asset management and inventory identification
- Management of risks
- Access rights management
- Management of threats
- Security controls
- Disaster recovery and business continuity
- Management of security incidents
- Cybersecurity education, training, and awareness

These elements, even though they might sound very technical, can be satisfactorily covered with educational training at basic level, even for employees without specific IT technical background.

3.1. Asset management and inventory identification

Probably the most important aspect, and for sure the steppingstone, of a powerful cyber-security awareness posture is to be able to know exactly what assets you do have inside your entity and connected to your network(s). Being able to correctly identify all electronic devices and software applications that interact within your network(s) is crucial for keeping a tight security and close entrance doors for malicious users from the beginning. Usually, the device identification will bring about an inventory list comprising some/all the electronics on the following list (and not only, we list only most common-found devices):

- Smartphones
- Laptops
- Tablets
- Desktop PCs
- Workstation PCs
- Servers
- Multifunctional Printer/Scanner/Fax
- Routers / switches

Form the point of view of software platform identification, we need to know what is the platform used by each and every device. Most commonly found software platforms today are Windows, Linux/Unix, Apple. Being able to know and register which platform is running on which identified device is very important for the management of our IT assets both on short and long term, because it will help us know what devices would be (possibly) in need for a software security-related patch or what devices were/can be compromised and in case of a missing existing patch they should be isolated as soon as possible.

Besides having identified all devices and their corresponding software platforms on our network(s), other critical issue for asset management is managing the changes to our inventory of devices, their platforms, and their configuration settings. The change/update management is quite a continuous and ongoing process. This brings the need for a very careful approach in order to avoid creating by ourselves security vulnerabilities if we do not exactly record every change as to permanently reflect the current up-to-date situation.

3.2. Management of risks

The issue of managing the risk involved in the cyber-defense area is very much related to the previous topic of asset management and identification. In reality, some of the risks can derive directly from the previous step. For example, unsecured routers or old-version software platforms can be identified and labeled as risks even during the first step related to asset id. One of the most relevant components of the management of risks is the implementation of a risk assessment. The target of the risk assessment process is to map the possible risks and register their potential impact on our entity (in case the risk materializes successfully). The process might imply vulnerabilities scan only, but it would be better to conduct a more thorough approach and analyze the control environment also.

The process of assessing the risks should, of course, be implemented after the asset identification process is completed. This procedure will make sure that we already know all the devices and their details, and as a consequence we do not skip analyzing any of them during the risk assessment phase. This phase records all identified risks and sorts them with a different level of priority, based on the level of threat and easiness of mitigation. Usually, more relevant threats which are also easier to patch should be solved with priority over other lower threats that might be more difficult and could take a lot more time to solve.

A standard risk assessment process would take into account the following

- Mapping of the entity systems (processes, applications, functionalities)
- Identify possible threats
- Calculate each determined risk’s impact
- Analyzing of the control environment
- Determining the likelihood of happening
- Rate the found risks

3.3. Access rights management

There is one crucial sentence for this phase - who has been granted access and to what data? Besides that, there are several other questions that need to be answered here - by what means do users get their access? Do users actually need access to all the information they are entitled to access right now?

The management of access rights/credentials require answers to all these questions… and more, for each authorized and registered user within our systems. The process of managing access rights is actually a sum of different sub-processes:

- Data classification
- Access control
- Lowest privilege

All information within our network and devices should be classified and organized into different categories. This process would greatly help find users who actually need access to it. Different entities can put in place different classifications, based on the kind of information they manipulate and the classes of users that should be allowed to interact with these data.

The access control tackles the specific protocols and software tools used within our entity in order to implement different restrictions. Among this software/hardware tools we can mention:

- NAC – network access control
- Wireless access – implementation of different policies for WAN connections
- Wired access – policies related to devices that are cable-connected to our network
- Physical access – relates to physical security, such as guards, locks, fireproofing, etc.

The lower privilege concept relies on each user's role for granting the minimum necessary of information required for them to be able to fulfill their activities. Application of this concept is very important for minimizing the entity's exposure in case a user set of credentials is compromised. The successful attacker will be able to compromise only the data/information that the compromised user was actually allowed to access.

3.4. Management of threats

This concept tackles with another relevant question – do you know the potential weak spots within your network infrastructure, and do you know how can a malevolent entity exploit them? The management of the possible threats represents a process that involves the identification and assessment of different possible threats to our entity, from the point of view of cyber-security. Usually, it involves three sub-processes:

- Penetration tests
- Management of vulnerabilities
- Management of the patching procedures

The penetration testing sub-process actually consists of a set of tests created and deployed in order to expose possible exploits in our network – they simulate a malicious intrusion process. For some years now, it is a fairly standard procedure by many entities looking to find exploits within their protocols and software applications. It is also often deployed as a verification step, after the patching of a previously found and solved issue, to check if the vulnerabilities/exploits have actually been solved.

The management of vulnerabilities relates somehow to another previous phase – the management of risks. This sub-process implies the use of vulnerabilities scanners and assessing the identified vulnerabilities (if any are found), in order to classify them and prioritize their mitigation.

Last, but not least, the sub-process representing the management of patching procedures is a continuous one. It is used to keep track of the solutions/patched applied for solving identified vulnerabilities. This sub-process supports the quality control as to not insert new vulnerabilities when patching old ones. The tasks here can be quite complex and complicated if we take into account the interactivity that must be flawless between lots of different software and hardware elements – one solution might bring another vulnerability or induce a system instability within another component.

3.5. Security controls

This step actually comprises a lot of different types of controls that are deployed within out entity in order to restrict the access to different categories of data. There can be physical controls (guards, secure locks, keys, etc.), administrative controls (IDs, badges, office restrictions, etc.), or technical controls (passwords, eCards, biometrics, etc.).

The physical controls, from the cyber-security point of view, are related mostly to different means that we deploy in order to protect our entity's physical assets from unauthorized access.

The administrative controls are usually comprising the development and enforcing of cyber-security policies and procedures inside our entity's working environment. The most visible result is usually the employees-related policy that guides the personnel as to how/when/where to access data/information withing our network infrastructure.

The technical security controls comprise a very large number of possible specific cyber-security measures deployed in order to ensure the protection of our data/information. Among these we can mention:

- Perimeter security
- MFA – multi-factor authentication for electronic credentials
- Network segmentation – in VPNs, IP classes, VLANs, etc.
- Endpoint security – software applications on each individual device
- Content filters – for blocking access to different electronic contents

3.6. Disaster recovery and business continuity

These concepts that make up the current phase are critical and can be very complex, and very expensive also. The disaster recovery concept, as well as the business continuity one, encompasses in reality a lot of different complementary systems and different contingency plans especially designed in order to keep our entity's IT infrastructure in top-shape, up-and-running condition, even during crises that could prevent normal access to our data/information/systems.

Even though the term disaster recovery might bring about the idea of natural disasters (such as floods, earthquakes, fire, etc.), in our cyber-security specific environment it means more that. It also covers power failures, DDoS attacks, Internet service interruptions, hardware equipment failures/blocks, software applications erratic behavior etc. In fact, the disaster recovery plan must cover all possible scenarios for loss of access to our data/information, loss that can have a negative impact on our entity's capacity to fulfill its mission/role.

A good disaster recovery and business continuity plan is deployed to create fail-safe points in order to prevent any one possible failure point from severely impacting our data/information. Usually, a must for such a plan comprises the existence of regular backups on remote equipment, live-copies of the software environment, redundant equipment etc. A good disaster recovery and business continuity plan can make the difference between surviving an IT catastrophe or going out of business. A good such plan can help an entity transform a potentially-catastrophic event into only a nuisance, while a bad (or missing) such plan can direct an entity straight out of business.

3.7. Management of security incidents

The management of security incidents represent the set of policies and procedures deployed by our entity in case of the need to answer to a specific cyber-security scenario. All incident management plans can have different individualized steps, depending on the type of incident, the type of entity and the amount/set of resources that the entity can employ in response to the security incident. Nevertheless, a standard plan for managing the security incidents should take into account the following aspects:

- Preparation – it covers the steps we take for preparing our entity to face security incidents
- Identification – it usually makes use of intrusion detection systems that should be used to supervise, log, and later analyze and document security incidents.
- Containment – in case of a specific, materialized attack, it covers the steps taken to mitigate and limit the exposure of our assets to the attacker
- Eradication – it covers the process of removing the detected threat from our entity's systems
- Recovery – it covers the solutions deployed to restore the normal service of attacked/exposed assets
- Lessons learned – it must cover the data analysis of the cyber-security incident, in order to better understand the threat, improve future response and address the vulnerability definitively

3.8. Cybersecurity education, training, and awareness

As is the case with all documentation and research phases, just the creation of an excellent set of policies and procedures that must be followed by the entity's employees will actually help too much in reality. The personnel must be aware of all these policies and procedures, they must understand why they should apply them, they should understand as best as possible specific details, they should be part of regular exercises and specific training programs in order to be able to uphold a powerful cybersecurity prone mindset. In order to achieve this, we should put together and create a synergetic response between cybersecurity education, training, and awareness.

The cybersecurity education and training usually involve formal and informal approaches, teaching to employees the basic elements of cybersecurity and making them aware of their critical role in ensuring a powerful cyber-protection posture. The trainings should also include practical sessions, with real-life scenarios based on real equipment, hardware and software assets, simulating exactly possible scenarios (like social-engineering attacks, phishing, social-media attacks, unsecured WiFi transmissions intercepts, etc.).

The awareness step usually relates to the entity's continuous activity in order to ensure its employees already know details about different specific cybersecurity issues, e.g., social engineering attacks, phishing, IoT possible vulnerabilities, bring your own device policies and risks, and basic security concepts like recommended best practices for passwords, requirement of multi-factor authentication, etc.

4. Conclusions

All the steps presented above are in fact covering the most important, basic, components of cybersecurity. Nevertheless, there is one more critical aspect that is sometimes overlooked. All these steps must be executed diligently and skillfully, with a good supervision of the execution and the management of implemented controls and answers.

For a cybersecurity to be really effective our entity must also assign the needed resources, both from the perspectives of the financial and personnel support. In case we allocate/spend enough resources, but we do not employ the right personnel for implementation (professionals, authorized to effectively deploy the solution), or we do employ and authorize the right people, but we do not allocate the necessary resources for software/hardware/training, then the allocated resources are misused and will not provide a reliable solution stack.

Another area which might be of tremendous help in mitigating the shortage of cybersecurity professionals on the labour market is the short-term trainings, even within the higher education sector. The students that are already enrolled in a university will, in vast majority, work with different electronic resources, online environments and multiple types of electronic devices. Even if they are not registered to IT study programs, they would be much more prone to obtaining a basic set of cybersecurity skills within a short-term training. The usage of the good-practices they learn will then wide-spread and the added level of security will be a welcome bonus.

In Romania, in 2020, there were funded several cybersecurity-oriented research and development projects, focused on internships with cybersecurity-related content. The Romanian-American University is currently implementing such a project, called "Let's Protect our Future Better! Advanced Cybersecurity"[91]. Within the framework of this project, no less than 23% of the students registered and approved for internship stages were not

[91] practica-cybersecurity.rau.ro

from computer science schools, but from different fields, like law, management, marketing, tourism, or physical education. Each of these categories has been assigned to different internship stages, tailored to their specific fields, but still focused on cybersecurity concepts: cyberlaw for law field students, personal data protection for management and marketing fields students, data regulations for tourism field students. The success rate of the internships for students at the IT-adjacent fields was astonishing, with 100% successful internships completed (after final evaluations and reports). This fact supports the above-mentioned idea of short-term specific-field trainings for higher education students, as a dissemination tool for cybersecurity basics.

References

[1] Rajib Paul, Ahmed A. Arif, Oluwaseun Adeyemi, Subhanwita Ghosh, Dan Han - *Progression of COVID-19 From Urban to Rural Areas in the United States: A Spatiotemporal Analysis of Prevalence Rates*. The Journal of Rural Health. ISSN 0890-765X. doi: 10.1111/jrh.12486. 2021

[2] Aberg, H.E.; Tondelli, S. - *Escape to the Country: A Reaction-Driven Rural Renaissance on a Swedish Island Post COVID-19*. Sustainability, volume 13. ISSN 12345678901. November 2021

[3] Tabusca, Silvia-Maria. *The Internet Access as a Fundamental Right*. Journal of Information Systems and Operations Management, vol. 4, no. 2: p. 206-212, ISSN 1843-4711, December 2010

Bibliography

Moseley, Ralph – *Advanced Cybersecurity Technologies*. Taylor & Francis Ltd., ISBN 9780367562274, 2021

Evans, Lester – *Cybersecurity. An essential guide to computer and cyber security for beginners*. Bravex Publications, ISBN 9781647482749, 2020

https://datareportal.com/global-digital-overview - Digital Around the World, last access: May 23, 2022

https://securityboulevard.com/ - Security Boulevard, last access: May 23, 2022

https://www.itgovernance.co.uk/what-is-cybersecurity - last access: May 17, 2022