The Symbiotic Threat of Human Error, Intended Action and Cybernetic Security System

Dragoș Cosmin Lucian PREDA,
DBA ORBIS Coneco; Former Minister State Secretary for Telecommunications, Romania
dcl@dragospreda.ro

Monica-Mihaela FRANGULEA,
Ph.D. St. Arch., "Ion Mincu" University of Architecture and Urbanism , Bucharest, Romania; CEO Juxta Foundation
monica_frangulea@yahoo.com

Abstract

Human error plays a significant role in cyber security breaches. In fact, according to a study by IBM, human error is responsible for 95% of all cybersecurity breaches. This can include unintentional actions or even lack of action by employees that cause, spread, or allow a security breach to occur. While software can sometimes be responsible for cybersecurity, human error still remains the leading cause of cybersecurity breaches. Intended actions, such as deliberate actions taken by individuals or groups to compromise security, are another type of cybernetic security threat. These actions can include hacking, insider threats, information sabotage and cyber espionage. This symbiotic threat between human error and cybernetic security highlights the crucial need to understand the relationship between the two in order to develop stronger cybersecurity behaviors and reduce cyber risk. Training and technology can help reduce the likelihood of human error by increasing awareness and knowledge of cyber security best practices. Additionally, cybersecurity awareness training is predicted to be worth $10 billion by 2027, further emphasizing the importance of addressing human factors in cyber security. By understanding the different types of cybersecurity threats, organizations can better prepare and protect themselves against potential breaches. We will present a real case example of human deliberate act - cybernetic attack of compromising an important architectural project designing process that took place in Athens in 2003, the repercussions of this act and what could be done today in order to avoid a similar situation.

Keywords: cybersecurity, cybernetic attack, cyber management, information sabotage, data security.

1. Introduction

In 2005 a famous architectural office in Athens (Greece), was working hard at the final phase of a massive 5000 seats Spots Palace for the Municipality of the Island of Rhodes. Two weeks before the final presentation the team of architects encountered a difficult situation. Overnight, the entire project has been manually removed from the computer systems of the office. Next morning seven computers and a password-protected server did not have any trace of the dozens of blueprints, CAD detailed drawings, site analysis a.s.o.

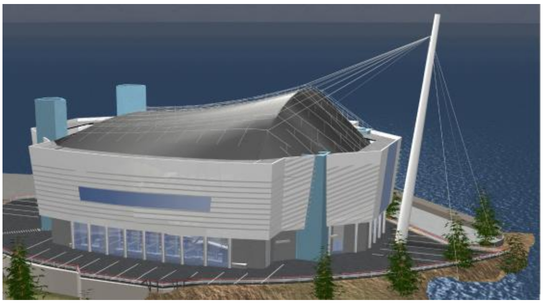

Fig. 1. Palace des Sports project for Rhodes, Greece
Source: Monica Frangulea, main architect of G. Andriotakis D.P.L.G. Comp.

At a closer look and deeper investigation, the evidences showed that one member of the architectural team have deliberately done this from unknown reasons and ran away from the city. The team of architects had to do a tremendous amount of work in order to remake the entire project, starting from a set of recovered older drawings that was previously sent to a structural engineering office. At that point we have understood that even if all architectural work was done digitally, the main threat remained in the real world, before the digital world menaces of remotely hacking, stealing copying or deleting hard work from the computers.

As a Romanian architect working abroad, Monica Frangulea, the head architect of the company, realised that the context of cyber security is much wider that she understood before and the solutions for data and digital work safety are not as simple as professionals in her line of work believed.

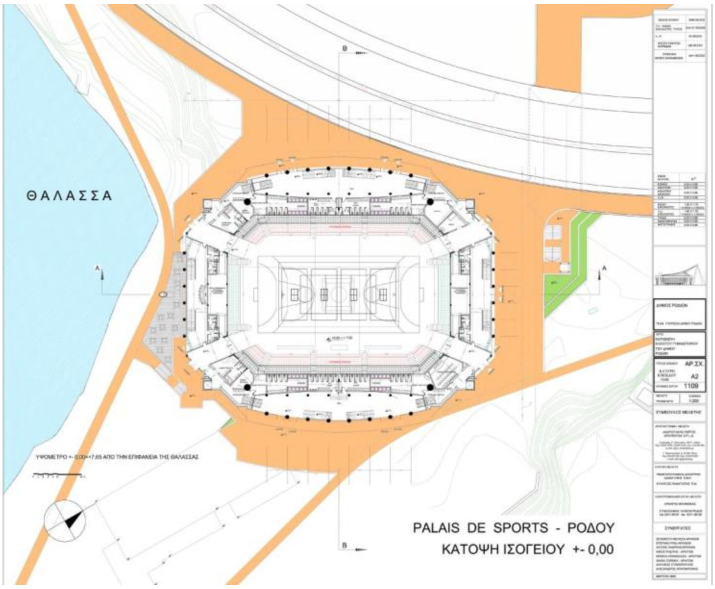

Fig. 2. Palace des Sports project for Rhodes, main floor plan, Greece
Source: Monica Frangulea, main architect of G. Andriotakis D.P.L.G. Comp.

2. Romanian cyber security in the international context

In 2020, under mandate as Minister State Secretary for Telecommunications, part of the governmental committee in charged with the successful mission as of 10th of December 2020 to determine our country hosting the European Cyber Center of Excellence, I stated publicly that "a restart was given in terms of cyber security, and Romania is at the starting line with an extraordinary potential" [1]. It was a teamwork and a national objective.

"In 2020 there was a restart. Romania is at that starting line (in terms of cyber security) and has an extraordinary potential. We have brilliant people. Helsinki Smart City was made by the people from RoboHub. We have examples how we, as Romanians, already implement these things at the international level. So, we have the human resource. We are also in discussions with the academic environment precisely to feed this human resource that we will need to implement and to absorb the reconstruction funds (PNRR and PODD) and not only that. So, we have all the resources, we just need to move from the area of debates to the more pragmatic and applied area and implement them. Only if we join all our forces, cross-party, will we manage to absorb these funds" [2].

I always stated that infrastructure security can include permanent assets such as real estate, but conceptually it is most used to refer to technology assets.

As CEO RADIOCOM I also prospectively focused the future activity of the new EU cyber security center that will be located in Bucharest on the concept of "zero trust".

The development of the European Cyber Security Center in and for Romania it's not just about the two billion dedicated to this Center, but it is about an exponential research-development-innovation and entrepreneurial dynamic thus naturally determined in this regional market – Romania being the regional pillar for everything IT&C means … and here we talk about more than 20 billion EURs. We have all the justifications for accessing all the funds, and I am also referring to the dynamics in the private sector that must integrate with these developments. In this advance you can only work in a very congruent way to absorb these funds and indeed to justify all these successes that Romania has achieved in recent years.

Regarding my insightful debates with companies such as Palo Alto I was always a promoter of the "zero trust", of total mistrust, of permanent verification. I know that these things often scare, but these are the developments at the international level and going beyond the moment of implementation or including this moment, the Cyber Center of the European Union must use in its development the concept of zero trust, a concept that is currently imperative and of great relevance in this dynamic [3].

Organizations are pursuing zero-trust network principles to help address the security requirements driven by digital transformation. We are no longer experiencing digitization. Currently, all entities, both public and private, must have a digital transformation strategy and a CIO/CTO. We cannot do without these elements nowadays, including for attracting brains in our countries. Back in 2020 I already started a series of talks with Prince University in Belfast, the main European academic pillar in cyber security area of expertise and training. All these steps must be correlated and put into this dynamic.

Furthermore, infrastructure security includes not only protection against a traditional cyber-attack but also protection against natural disasters and human errors. Returning to this part of the infrastructure, which is imperative: if we want to experience this digital transformation, we must talk about connectivity and a common European calendar of connectivity, and here reference was also made to the transposition of 5G. This is to be able to have the same opportunities. In history, when we recovered from the crisis, we recovered through investments in infrastructure: previously in railways, roads, and classic ones, currently the dynamics is on digital ones, including data infrastructure. Infrastructure security can include permanent assets such as real estate but is most used to refer to technological assets: computers, network systems, cloud resources, both hardware and software. The actual concept of infrastructure security includes not only protection against a traditional cyber-attack but also the protection against natural disasters, again an extremely important thing that I highlighted also at the level of such entities as the National Radiotelecommunications Society, the company I used to manage and built in some historical achievements and restored it from a 18 million deficit back in 2019 to a 122 million in accounts by the end of 2021 and a 25 million profit at a 246 million turn over with a 15% raise on salaries for 1251 employees. It is imperative to create these future-proof systems, which have been active for almost 10 years at the international level [4].

The goal is to enhance security measures and minimize downtime and associated wear and tear for both customers and the potential loss of a brand reputation, to reduce compliance costs faced by companies and of course the state. Fundamentally infrastructure security describes a highway of thinking about the protection of the entire technological perimeter of the organization. Several tactical plans must be made how do we protect the data on employees' laptops, how do we educate them, the training of the end user, each individual citizen is a major topic in this new cyber security thinking. For example, in a company, a common way of looking at security includes securing the following 4 levels: firstly, the physical level, the infrastructure has need for physical protection, we are talking about backup generators, security cameras and the like, also fail-over plans that locate the backup equipment, after that is the network level. At its core, network security protects data as it is transported within the network, this includes traffic encryption, whether local or cloud, proper firewall management, the use of authentication and authorization systems, and then the application/ apps level: this includes protecting data against attacks such as SQL injections, as well as hardening other applications against unauthorized use of malicious exploits. At the same time, data protection at the lowest level, regardless of where and how it is stored.

I also launched back in 2020 a challenge at the company level to find a solution to cover all white areas in the country with satellite communications, including the 5,000 schools that are not served by the telecommunications network… for all these developments human capabilities are at the core.

3. Managing human failures, Zero Trust and McCumber cube

As I already stated, regarding the implementation of the *zero-trust concept* the architecture of the implementation of the EU Cyber Center, must be solid, based on the Cybersecurity Cube (also called the McCumber cube), a tool for managing network protection, domains and the Internet, which systematizes the domain approach on three dimensions.

The first dimension of the Cybersecurity Cube includes the three principles of information security. This concern: information states, characteristics of critical information and security measures [5]. Information states include transmission, storage and processing. Characteristics of critical information include confidentiality, integrity, and availability. Security measures include technology, policies and practices, as well as people/user education, training and awareness.

The second dimension identifies the three states of the information or data.

The third dimension of the Cube identifies the expertise required to provide protection.

These are often called the three categories of cybersecurity safeguards.

3.1. Principles of Security – The CIA Triad

The first dimension of the cyber security cube identifies the objectives of protecting cyber space. The objectives identified in the first dimension are the fundamental principles. These three principles are confidentiality, integrity, and availability, commonly referred to as the CIA triad (confidentiality, integrity, and availability).

Privacy prevents disclosure of information to unauthorized persons, resources, or processes. Integrity refers to the accuracy, consistency, and reliability of data. Availability ensures that information is accessible to authorized users when needed.

These principles are used to ensure focus and prioritization of actions when protecting networked systems.

3.2. Protect states: Transit, Rest, Storage, In Process

Cyberspace is an area that contains a considerable amount of important data (big data), which is why cybersecurity experts must focus on protecting data.

The second dimension of the Cybersecurity Cube focuses on the issue of protecting data in cyberspace in each of its possible states: Data in transit, Data at rest or stored, Data in process.

Protecting cyberspace requires cybersecurity professionals to consider data protection in all three states.

3.3. Safeguards through skills, discipline, policies, procedures, and education

The third dimension of the Cybersecurity Cube defines the skills and discipline that a cybersecurity professional can access to protect cyberspace.

Cybersecurity professionals use several different skills and disciplines when protecting data in cyberspace, taking care to always stay on the "right side" of the law.

The Cybersecurity Cube identifies the three types of skills and disciplines used to provide protection.

The first capability includes the technologies, devices, and products available to protect information systems and protect against cybercriminals. Cybersecurity professionals have a reputation for mastering the technology tools at their disposal.

However, McCumber reminds that technological tools are not enough to defeat cybercriminals. Cybersecurity professionals must also build a strong defense by establishing policies, procedures, and guidelines that allow cyberspace users to stay safe and adhere to best practices.

Finally, cyberspace users must strive to continuously update themselves on cyberspace threats and establish a culture of education and awareness.

The location of the EU Cyber Center in Romania places us in a position as a regional and European leader in the field of cyber security, but also as a pole of technological expertise in cyber security at the European and international level.

This will contribute to the promotion of Romania at the European and international level as a strong digital country, with a competitive economy, with exceptional prospects for increased investments, in the direct or related fields of cyber security.

4. Human Errors and Critical Infrastructure

Everyone can make errors no matter how well trained and motivated they are. However, in the workplace, the consequences of such human failure can be severe. Analysis of accidents and incidents shows that human failure contributes to almost all accidents and exposures to substances hazardous to health. Many major accidents eg Texas City, Piper Alpha, Chernobyl, were initiated by human failure. To avoid accidents and ill-health, companies need to manage human failure as robustly as the technical and engineering measures they use for that purpose.

The challenge is to develop error tolerant systems and to prevent errors from initiating; to manage human error proactively it should be addressed as part of the risk assessment process, where: significant potential human errors are identified, such as poor design, distraction, time pressure, workload, competence, morale, noise levels and communication systems – performance influencing factors (PIFs).

Control measures are devised and implemented, preferably by redesign of the task or equipment. I recently came up with and idea of using neuronal redesign games at the level of human resources management.

This Key Topic is also very relevant when trying to learn lessons following an incident or near miss. This also involves identifying the human errors that led to the accident and those factors that made such errors more likely.

4.1. Types of human failure

It is important to be aware that human failure is not random; understanding why errors occur and the different factors which make them worse will help you develop more effective controls. There are two main types of human failure: errors and violations.
A human error is an action or decision which was not intended. A violation is a deliberate deviation from a rule or procedure.

5. Study case – Critical Infrastructure and Industrial High Pressure Equipment

Knowing what needs to be done to achieve excellence in pressure equipment integrity (PEI) is one thing, but knowing how to organize everything to be successful in the field is quite another, namely how to organize all stages of PEI work to achieve overall success, to ensure that everything that needs to be done is done using Management Systems (MS) and Work Processes (WP).

Without an effective organizational strategy for EIP, many of the essential elements of EIP can become derisive as there may not be a management system in place to ensure that each element is properly planned, scheduled and completed at precise intervals by an entity responsible.

However, with an effective MS PEI, each site should be able to maintain pressure equipment integrity (i.e. no containment breaches) and achieve pressure equipment reliability (i.e. have pressure equipment available to operate as planned default / as well as business), both defining excellence in PEI.

5.1. What is excellence in PEI?

It is simply doing what needs to be done, doing it right, doing it when it needs to be done, to create, implement and sustain the PEI program to avoid containment violations. Having effective management systems (MS) for all PEI issues that need to be managed is the foundation of a successful PEI program.

5.2. What is a management system (MS)?

It is simply a compendium of all the necessary information describing what needs to be done, why it needs to be done, how it needs to be done, and how often or when. Some operating sites then combine MS PEI with PEI work process (WP) maps and descriptions to show who is involved and how the work is being done.

Management systems are the inputs to WP maps and descriptions.

There are many ways to organize a successful PEI MS program. Some ways of organizing a PEI MS program can be just as effective as others, as long as all the necessary elements are included, programmed and carried out according to plan. Without effective PEI MS, even if we know what needs to be done, we may be wasting time and other critical resources rather than doing what needs to be done effectively to prevent containment breaches.

5.3. The ten PEI management systems

The literature generally reveals 10 essential MS required for an effective PEI program that can achieve excellence:

- Managerial leadership and support for PEI
- Integrity Operating Windows (IOW)
- Management of change (MOC)
- Damage Management and Control
- Risk assessment and inspection planning
- Life cycle management

- PEI codes and standards
- Site procedures and work processes for (WP) PEI
- PEI record keeping and data management
- Continuous improvement of the PEI

For each of these, we will have several sections where we will record all procedures, standards, guidelines, work processes, best practices, engineering assessments, failure analyses, metrics, etc. that we need to design and operate a successful PEI program.

A robust PEI program means much more than inspection procedures and standards.
PEI is not just the result of a competent inspection program!

An effective multidisciplinary approach with management, operations, engineering, maintenance and inspection is needed to achieve what needs to be done to achieve excellence in PEI. All these MS of the PEI must be strongly integrated to achieve success in the PEI.

Those operating sites that still have each of their functions largely "working in silos" and are not effectively integrated with other MS will not be able to achieve the level of success in PEI that is vital in today's competitive environment, which requires excellence in cost optimization and reliability.

5.4. Managerial leadership and support for PEI

Like all 10 MS, if we do not have all the systems in place for managerial leadership and support for the PEI program, we are unlikely to achieve the level of success expected. So this is a critical component of the PEI's MS...as are the other 9. At its best, when this MS is fully functional, the PEI group aims for strong leadership and support for the PEI's mission and goals, and as such , all eyes are on the actions and decisions of the management that manages the PEI. At worst, where leadership and management support are lacking, the PEI group spends a lot of time managing critical situations, and we all know what usually happens when such situations arise.

This MS, Managerial Leadership and Support for the PEI Program, describes the systems and work processes that are required from operating site and company management to provide the direction and resources necessary to achieve excellence in PEI. These resources include budgeting, staffing, training, certification, upskilling, a shared asset management attitude, knowledge transfer from PEI to others who need and want to know, and pro-active management - doing what we say.

An overview of the 10 MS of the PEI that are necessary to achieve and maintain excellence in the PEI "Compliance" is not the absolute end of a successful business plan. The integrity of the pressure equipment and subsequent reliability of the pressure equipment is part of a good business plan. PEI of excellence is needed to achieve subsequent reliability.

These PEI MS are always improving and expanding to keep pace with changing business conditions and requirements.

But in the end, it all boils down to people and personnel and career management and our nursery and the value of our competitiveness lies in the academic space and the ongoing work with it.

References

[1] The statement can also be found at https://www.bursa.ro/videoconferinta-securitatea-cibernetica-dragos-preda-ceo-radiocom-in-2020-a-fost-dat-un-restart-securitatii-cibernetice-21650541 as of 8th of December 2021

[2] Statement to be found also https://www.agerpres.ro/english/2021/02/18/dragos-preda-eu-cybersecurity-center-must-adopt-zero-trust-security-model--664211 as of 18th of February 2021

[3] See also in https://www.thediplomat.ro/2021/04/06/secretary-of-state-dragos-preda-the-construction-of-ngn-backhaul-infrastructure-requires-more-than-2-billion-euros/ as of 6th of April 2021

[4] Regarding the concept of future proof my article https://www.themarketforideas.com/challenges-and-opportunities-for-the-future-of-competitiveness-a266/ as of 22nd of February 2017

[5] See also https://umbrela-strategica.ro/centrul-cyber-al-ue-cubul-mccumber-si-zero-trust/ as of 15th of January 2021