Summary:
Why is everyone in the corporate world encountering so many cybersecurity issues? Have organizations already lost in the cybersecurity race? The answer is no, there are some key concepts every organization would benefit from implementing in order to achieve a better level of cybersecurity.

Why is it that…

…so many organizations, and it seems that almost every company connected to the Internet, encounter significant cybersecurity issues in their environment? There are daily news about numerous companies being a victim of a cybersecurity heist and it leads us to believe that those who have not yet been in the news, is not because of their effective cybersecurity controls, but rather because an attack has simply not yet taken place in such organizations. What has changed in the last few years? Has the number of vulnerabilities in their IT environment significantly increased? Is it true that more organizations are connecting their business processes end to end to the Internet to achieve real automation? Is it just the media, which has a better understanding of cybersecurity matters and is able to unveil companies' vulnerabilities and their exposures within no time after occurrence of an attack around the entire globe? Is there a new normal in the business environment resulting from a combination of several factors?

Many security experts and corporate executives are convinced that no technical setup or solution is truly secure these days and it is only a matter of time until an attacker uncovers a vulnerability in their setup. In response to these concerns, the cybersecurity advisory industry offers and performs comprehensive services how to respond to a breach if it were to happen. This is actually nothing new; the concept of Computer Emergency Response Teams (CERT) or incident responders exists in the business environment for quite some time. Any organization involved in doing business over the Internet should have a CERT in place in some sort or fashion. The size, setup and level of sophistication of such a CERT is very much dependent on several factors including the type of business and industry the organization is active in, its size and the kind of B2B and B2C interfaces such organization has in place.

The thesis is, that it is still possible to set up and operate a secure IT environment in today's corporate world and define an approach how to cope with the overwhelming number of different options an organization has to evaluate in regards to establishing an appropriate and effective cybersecurity protection.

Performing a thorough threat analysis is key in order to gain an initial insight and understanding of the various potential actors, components and threats in the cyber environment of the organization. Such an analysis not only helps to understand the external factors but more importantly it helps to assess and understand the organization's own internal environment. It is a fact that the deeper the knowledge and understanding of the organization's own environment, the better and more effective they will be in securing and protecting it. As of today, it is very likely that a large number of organizations omits completely or is only partially performing such a threat analysis. The majority of organizations tends to narrowly focus on the threat landscape and as incidents occur, try to fix them and close uncovered loopholes, instead of choosing a more comprehensive approach. As an illustration, one can draw a comparison with mathematics with complex numbers, which takes the imaginary component of a complex number into consideration and hence makes a step to the side in order to look at the number line from a different standpoint. The perception from that standpoint is certainly different compared to the one if standing on the number line itself. To come back to the cybersecurity environment, such an approach

should be taken while performing a threat analysis, take a step back or to the side in order to get a more holistic view on the different parts, including the attack vector, the implemented defense in-depth architecture and the process organization.

The first step in this comprehensive analysis is the definition and development of so-called threat scenarios. These threat scenarios are the foundation in the development of a risk-based approach for the definition and implementation of an effective internal control system as well as of any additional controls to secure the environment. Accordingly, it is of crucial importance to invest in the process of defining these threat scenarios and gaining full understanding of the own environment. This process helps to determine the potential threat exposure of the analyzed business processes, IT assets and physical assets. The following parameters allow for the definition and description of any possible threat scenario:

- Threat agent
  A person or a group of persons who conduct(s) an attack is a threat agent. This threat agent can be inside an organization or outside or a combination of both. This definition includes that behind every machine or device is a person. It is irrelevant whether a person is acting consciously or unconsciously as a threat agent.
- Method
  The threat agent will use a method to conduct an attack. The most common methods include information system based action, human interaction, or physical access.
- Access point
  The method needs to have an access point, where it launches the attack against the target. The access points often is the weakest point or link in a system.
- Target
  The target is the objective of the attack. The threat agent aims for the target with a particular method.
- Threat exposure
  Every successful attack leads to an exposure for the organization. The impact of the threat measures the exposure, which is often directly or indirectly associated with a financial loss.
- Motivation
  The motivation of a threat agent to engage in an attack defines the severity of the criminal conduct as well as the extent of the impact. The motivation also determines implicitly the probability and the frequency of a threat.

I have developed an approach for defining threat scenarios that applies the methodology of a morphological analysis, which is a method for evaluating a variety of solutions to a non-quantifiable and multidimensional problem. The sector of Industrial design uses this technique in the process of identifying potential options and eventually choosing an appropriate design or solution. In the context of cybersecurity and developing threat scenarios, it has two important applications. The first one is, by applying this technique to the particular control environment under analysis, it generates a very good understanding of the environment. The outcome of such morphological analysis is a comprehensive list of the specific components of the environment, even if it is only on an abstract level, creating sort of an inventory. The second one is that it connects said inventory with threats and shows the majority of variations or so-called threat scenarios.

A full set of parameters, which is a combination of one specific value assigned to each parameter, defines the threat scenario. Each parameter has an infinite number of options or values. Based on the aforementioned parameters the following graph shows an example of a morphological box:

Parameters	Values					
Threat agent	Organized crime	IT employee	Employee Scenario 1:	State actor	Former employee	Supplier or contractor
Method	Abuse of confidence	Malicious coding	Social engineering	Brute force	Hacking	
Access point	Client PC	Internet	Application	Employee	Web server	Mobile device
Target	Application server	Cash	Financial systems	Data	Host	
Threat exposure	Disclosure of information	Unauthorized system access	Information theft	Information modification	Fraud	
Motivation	Financial gain	Disgruntlement	Politics	Fun	Damage	

Graph 1: Morphological box to identify threat scenarios

The number of significant threat scenarios depends on how large and complex the organization is: the larger and more complex the organization, the greater is the number of relevant scenarios. When applying a risk-based approach, the analysis should be limited to the relevant threat scenarios in the corresponding control environment. Over time, an organization can increase the number of scenarios to achieve a more comprehensive analysis.

Description of Scenario 1: The threat agent is an internal employee abusing of the trust relationship he has with his supervisor. This scenario is in the context of a supervisor having delegated accounting tasks to one of his trusted staff members without performing any effective supervision. This accounting staff member has access to accounting and finance systems of the organization in order to be able to execute his function. Such employee then uses his access to the accounting and finance systems to misappropriate money to fund his expensive lifestyle.

This Scenario 1 is fairly simplistic and generic but allows illustrating the application of the threat scenario analysis. In the context of cybersecurity, the threat scenarios defined for the control environment need to be more specific and must consider the process architecture as well as the setup of a particular part of an organization. Identifying and analyzing the weaknesses of systems in the control environment is very important in the process of defining relevant threat scenarios that expose the organization's vulnerabilities. Threat scenarios facilitate the derivation and definition of adequate and effective internal controls. This process clearly supports the importance of knowing and understanding the organization's systems and particularly its weaknesses in the first place in order for an organization to implement effective internal controls subsequently.

For elaborating the threat scenario, it is also useful to profile carefully the perpetrator and try to mimic the threat agent in order to understand the way of thinking of such potential perpetrator. This in turn clearly helps to identify the weaknesses and potential access points in an environment, which need to be protected with adequate controls. In this simplistic example, an obvious and effective control activity such as the implementation of a “four eyes principle” with the manager actually supervising the accounting activities of his employee would limit the threat outlined. There is a large number of possible controls available for any organization that they can tailor and implement in line with their needs and processes.

This scenario technique allows breaking down the complexity of any cybersecurity matter to a comprehensive and graphical analysis. Its use also supports the communication with senior management, which do not necessarily have the in-depth knowledge of the analyzed area of the organization as well as its processes and IT solutions.

Coming back to the initially outlined question: “Why is it that…?”, the answer is that a combination of different factors lead to more exposure for any organization. In today’s interconnected world, organizations often operate with a very complex setup, including architecture, processes, organizational structure, to be competitive in providing their services and/or product offerings to their customers. An overwhelming complexity, a lack of properly skilled people to understand and operate in such a complex environment, budgetary constraints failing to maintain an adequate cybersecurity level, are factors to consider. A cybersecurity level of due care is certainly insufficient today. As the threat landscape continuously evolves, organizations need to stay abreast and dedicate resources to establish and maintain an adequate level of cybersecurity. Does this mean an organization needs to spend large sums of money to maintain the required level of security, and in that sense some organizations could not afford to have their required level of security? The answer is definitely no. Having skilled and well-trained security staff and establishing the subject of cyber security as part of an organization’s culture and as such an increased level of awareness, leads to a lower requirement for financial resources.

Does this imply that no organization, which has been a victim of a cybersecurity breach, has the right people employed? Mistakes are human, however, it is a given that the dark side of the cybersecurity equation focus on the low hanging fruits first. Having well informed people helps to protect an organization from being a victim of an easily preventable attack. Organized crime is very active in committing cyber-attacks and it reached a certain level of proficiency in some attacks. At the same time, a huge number of attacks are less sophisticated, such as (spear-) phishing attacks, which are rather easily preventable and count as part of the low hanging fruits. Today probably, eight or nine out of ten successful cyber-attacks still start with a phishing or spear-phishing email. This is certainly surprising given the large media coverage and great efforts of professional organizations to rise cybersecurity awareness over the past two decades. Anyone should be aware and understand the risks associated with clicking on links or opening attachments in emails or even disclosing credentials, particularly if the sender is unknown or if there is no reason to receive such emails or requests. The weakest link in the cybersecurity chain still seems to be the human being and not the machine as the majority would expect.

Besides focusing on the people within an organization who are relevant and responsible to keep up the adequate level of cybersecurity, third party vendors such as suppliers, providers and outsourcing partners are also major contributors to cybersecurity. In order to make sure this group and their provided services or solutions fit within the organization’s risk appetite towards security, a two-step plan can be considered. Firstly, the following question needs to be addressed: Can the particular vendor transparently assure the level of cybersecurity of their service or solution? If the answer to this question is yes then the next step is a comparison of the two levels of cybersecurity of the organization and the vendor, respectively. The goal is to achieve an alignment of these two levels to the top one. On the opposite, if the answer to the

question is no and the vendor is unable to assure or cannot provide appropriate evidence of an adequate level of security together with their services or solutions, then the second step for the organization is to establish an adequate level of security itself. Having services and solutions from vendors that cannot provide an adequate level of security, the organization must implement internal controls to secure applications and thwart specific attacks.

For developing and implementing secure applications, every organization should have secure coding guidelines in place. In addition to functional testing, non-functional testing should also test the program code against these guidelines to ensure compliance. More mature organizations could implement these secure coding guidelines as part of their continuous integration. The goal of these secure coding guidelines is, on the one side, to provide clear instructions to follow when developing software within an organization, and on the other side, to make developers aware of threats to anticipate during the development phase. A mandatory building block for developing new software is performing proper input validation and output encoding. The implementation of input validation prevents a high number of potential application related attacks. If an organization does not write its own secure coding guidelines, it can always request it from their outsourcing provider. If the outsourcer does not have secure coding guidelines or is not following such guidelines, this is a clear red flag and most likely means that this provider is not the right outsourcing partner. Requiring an adequate level of cybersecurity is essential. An organization must have a rigorous vendor risk management, which overseas such requirements and most importantly makes sure that the organization is getting the appropriate level of security for third party software or services.

There are of course many more items to consider in the set up and operation of a secure IT environment. However, if an organization were to conduct a proper risk assessment, in which the threat analysis plays a crucial role, it would definitely be able to implement and maintain a more mature level of cybersecurity.

Roger Auinger (CISSP)