ISSN 2704-6419

Europe's Cyber Resilience

Julia Wurm

International Institute for Global Analyses

Vision & Global Trends. International Institute for Global Analyses
Piazza dei Navigatori 22, 00147 – Rome (Italy)
Analytical Dossier – N. 31/2020 – November 2020

First Edition: November 2020

Analytical Dossier 31/2020 - ISSN 2704-6419

www.vision-gt.eu
info@vision-gt.eu

 ISSN 2704-6419

Europe's Cyber Resilience

A False Sense of Security in the Private Sector as a Warning Sign and Means to Assess the Effectiveness of Cyber Security Awareness Measures

Julia Wurm

Vision & Global Trends - International Institute for Global Analyses

In today's world, no organization or enterprise is completely safe from cyber-attacks or their possible consequences. In fact, one may even argue that the effects of Cyber Security incidents on our increasingly interconnected world have the potential to negatively affect every single individual on this planet. As a result, and aided by a progressively complex landscape of regulatory and legal requirements in this field and beyond, raising awareness of Cyber Security threats and, by extension, building Cyber Resilience, have developed from a traditionally rather technical matter into an increasingly important strategic topic for businesses, on the one hand, and into a critical diplomatic challenge for States, on the other hand.

The EU Network and Information Security Directive was the first piece of EU-wide Cyber Security legislation and aims to enhance Cyber Security across the EU. The national supervision of critical sectors, such as energy, transport, water, health, and critical digital service providers, including online market places, as well as the enhancement of national Cyber Security capabilities and facilitation of cross-border collaboration, are the key topics covered by the NIS Directive.1 Moreover, the NIS Directive is part of the EU Cyber Security Strategy, which states "achieving Cyber Resilience" as one of its five priorities.2 However, the fact that the NIS Directive was only adopted in 2016, with a deadline for national transposition by EU member States as recent as May 9, 2018, illustrates that Cyber Security and Cyber Resilience are relatively new topics in international collaborative efforts surrounding security and stability in Europe. One may argue that this recency inherently implies a certain lack of preparation for Cyber Security incidents; thus, vulnerability.

"The technology of today serves not only a Weberian predictability imperative – to further rationalise society. It makes society less safe and its individuals less free" – recently stated my former professor Anis H. Bajrektarevic discussing the EU cyber-related legislation.3 Hence, a preparation, in other words – strategic investment in preventative measures and resources, is considered an essential aspect of Cyber Security as well as critical to Cyber Resilience. While Cyber Security is primarily concerned with the protection of information technology and systems,4 Cyber Resilience aims to ensure the effective continuation of an

[1] ENISA. *NIS Directive*. n.d. https://www.enisa.europa.eu/topics/nis-directive (accessed June 25, 2020).
[2] European Commission. *EU Cybersecurity plan to protect open internet and online freedom and opportunity*. February 7, 2013. https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94 (accessed June 25, 2020).
[3] Bajrektarevic, Anis. *Twinning Europe and Asia in Cyberspace: the EU GDPR Legislation and its Transformative Power*. January 2019. Diplomat Magazine (Hague-Brussels)
[4] RSI Security. *What is cyber resilience and why is it important?* August 14, 2019. https://blog.rsisecurity.com/what-is-cyber-resilience-and-why-is-it-important/ (accessed June 25, 2020).

organizations operations and to prevent demobilization of business- or organization-critical functions in the event of security incidents.5 To be more specific, it is "the ability to prepare for, respond to and recover from cyber attacks" and other security incidents, such as data breaches, that is commonly referred to as Cyber Resilience.6

In this context, it has been argued that the creation of a resilience-conscious culture is a key element of successful Cyber Resilience strategies.7 Creating such a cyber resilient culture involves raising awareness of Cyber Security threats, such as phishing and malware, and communicating ways to minimize risks stemming from them to people outside of Cyber Security functions.8 The main goal here is to facilitate a cyber resilient mindset through awareness-building measures, leading to the question: If promoting awareness of Cyber Security threats ultimately enhances Cyber Resilience, how can we, first of all, assess the status quo of Europe's Cyber Resilience and subsequently, monitor the progress and effectiveness of such awareness building measures, in order to better understand, compare and ultimately enhance the Cyber Resilience of individual States and Europe in its entirety?

This essay will argue that "a false sense of security" in the private sector is a warning sign regarding the Cyber Resilience of States, hence, a warning sign regarding the status quo of Europe's Cyber Resilience. Moreover, it will argue that "a false sense of security" can serve as a valuable indicator for the effectiveness of, and increased need for Cyber Security awareness measures. This will be accomplished through the following approach:

Firstly, the essential need for and feasibility of active preparation for seemingly unlikely crisis situations, will be emphasized. To illustrate this point, the controversy surrounding the classification of the COVID-19 pandemic as "black swan event" will be discussed. Secondly, the discussion of several recent Cyber Security related incidents and their implications, will highlight that businesses and governments worldwide must, more than ever, and especially due to the C-19 related acceleration of digitalization, improve their Cyber Resilience. The main goal here will be to draw attention to the worldwide existing deficiencies regarding Cyber Resilience and, based on this, illustrate the need for and value of finding new ways to assess Cyber Resilience, but also key aspects of Cyber Resilience.

[5] De Groot, Juliana. *What is Cyber Resilience.* February 4, 2019. https://digitalguardian.com/blog/what-cyber-resilience (accessed June 25, 2020).
[6] IT Governance Ltd. *What is cyber resilience?* n.d. https://www.itgovernance.co.uk/cyber-resilience (accessed June 25, 2020).
[7] Hughes, Mark. *Beyond awareness: Create a cyber resilient culture.* September 2019. https://thrive.dxc.technology/2019/09/10/beyond-awareness-create-a-cyber-resilient-culture/ (accessed June 6, 2020).
[8] Hughes. *Beyond awareness: Create a cyber resilient culture.* September 2019.

Thirdly, current insights from the recently published study "Cyber Security in Austria"9 will be discussed and contrasted with the respective risk assessment from The Global Risks Report 201910 to illustrate apparent discrepancies in security related self-perception in the private sector versus the reality of the risk situation. It is important to note here that "a false sense of security" means feeling safe in an unsafe environment. Therefore, such discrepancies represent "a false sense of security". As a final step, possible implications and limitations of the presented ideas will be discussed.

A black swan event is an unpredictable, highly improbable and rare event that has serious and potentially catastrophic consequences. One main characteristic of black swan events is the widespread insistence that their occurrence was obvious in hindsight; thus, should have been foreseen.11 In the recent past, this concept, which the Lebanese-American philosopher, professor and former Wall Street trader, Nassim Nicholas Taleb, developed and already described in 2007, has, in connection with the C-19 pandemic, again become a topic of conversation - not least because of social media, such as Twitter (#blackswan). While there seems to be general disagreement as to whether the ongoing C-19 pandemic constitutes a "real" black swan event, Taleb himself stated in an interview that the eventual outbreak of a global pandemic with all its consequences was, in fact, a predictable "white swan" event, arguing that companies, corporations and especially governments, had no excuse, not to be prepared.12

Regardless of swan color, however, in connection with the aforementioned ability to prepare for cyber-attacks, it can be argued that a particularly relevant consequence of the C-19 pandemic, in terms of Cyber Security and subsequently, security in Europe, has been the acceleration of digitalization throughout the world, affecting the public and private sector, as well as the private sphere of people's homes. Exit restrictions and other social-distancing measures imposed by governments worldwide, in an effort to curb the spread of the virus, have caused the global demand for remote working technologies to skyrocket within a remarkably short period of time. For example, the video conferencing solution provider Zoom experienced, within just a few weeks, a surge from around 10 million daily active users at the end of December 2019, to over 200 million daily

[9] KPMG. *Cyber Security in Österreich.* Study, Vienna: KPMG Security Services GmbH, 2020.
[10] World Economic Forum. *Risks of Doing Business 2019.* 2019. https://reports.weforum.org/global-risks-report-2020/survey-results/global-risks-of-highest-concern-for-doing-business-2020/ (accessed June 25, 2020).
[11] Chappelow, Jim. *Black Swan.* March 11, 2020. https://www.investopedia.com/terms/b/blackswan.asp (accessed June 25, 2020).
[12] Taleb, Nassim Nicholas, interview by Bloomberg TV. *Taleb Says "White Swan" Coronavirus Was Preventable* (March 31, 2020).

active users in March 2020.13 It was not long before data privacy and data security related problems with Zoom became apparent: "Zoom bombing" or video hijacking, which refers to the unwanted and disruptive intrusion of a person into a Zoom video meeting, a lack of end-to-end encryption and, in this regard, misleading information advertised on part of the provider, along with various IT security related vulnerabilities that allowed hackers, among other things, unauthorized remote access to end user's Mac computers - including webcam and microphone access, Zoom's deployment of in-app surveillance features, as well as questionable handling and alleged trade with the obtained user data were, already by April 2020, seen as a considerable cause for concern, leading security experts to describe Zoom as "a privacy disaster", and "fundamentally corrupt". Moreover, Arvind Narayanan, associate computer science professor at Princeton University, was quoted as saying: "Zoom is malware".14 The most memorable piece of news concerning Zoom was, however, arguably about the British prime minister Boris Johnson accidentally posting sensitive information, including the Zoom meeting ID and the login names of several participants, when sharing a screenshot of his first-ever digital cabinet meeting via Twitter.15

The example of Zoom illustrates how companies, organizations, governments and private individuals benefit to an unprecedented extent from the advantages of digitalization, especially in the context of the ongoing C-19 pandemic, but also beyond such global crisis situations, while at the same time being faced with the considerable challenges and security risks brought about by the new technologies of what is known as the Fourth Industrial Revolution. This Fourth Industrial Revolution, being "characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres", is changing the ways we live, work and interact,16 resulting in significant risks to the privacy of natural persons, as well as to security and stability in general.

Several recently occurring or publicly emerging Cyber Security incidents underpin the scope of these risks: A cyber-attack on the British airline EasyJet, in the course of which personal data including email addresses and travel plans of 9

---

[13] Fuscaldo, Donna. *Zoom's Daily Active Users Surged to 200 Million in March... and That's Part of the Problem.* April 2, 2020. https://www.nasdaq.com/articles/zooms-daily-active-users-surged-to-200-million-in-march...-and-thats-part-of-the-problem
(accessed June 25, 2020).
[14] Paul, Kari. *'Zoom is malware': why experts worry about the video conferencing platform.* April 2, 2020. https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing
(accessed June 25, 2020).
[15] futurezone. *Netzpolitik: Boris Johnson postet aus Versehen sensible Infos.* April 1, 2020. https://futurezone.at/netzpolitik/corona-boris-johnson-postet-aus-versehen-sensible-infos/400800110
(accessed June 25, 2020).
[16] Schwab, Klaus. *The Fourth Industrial Revolution: what it means, how to respond.* January 14, 2016. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/
(accessed June 25, 2020).

million EasyJet customers and additionally, credit card details of over 2,000 customers, were stolen, became known in May 2020.17 This once again demonstrates that companies of all kinds can at all times become targets and victims of cyber-attacks. Costly penalties for violations of the General Data Protection Regulation (EU) 2016/679 (GDPR), as well as claims for damages and lawsuits by those affected and, last but not least, the loss of reputation often caused by such security incidents, pose significant challenges for companies under any circumstances. These challenges can, however, easily become existence-threatening, especially in view of the C-19 induced crisis situation, in which particularly the aviation industry currently finds itself in, as recently highlighted, when Austrian Airlines received EUR 450 million in financial aid from the Austrian government.18

On the one hand, the EasyJet security incident illustrates that Cyber Resilience has, in recent years, developed from a formerly predominantly technical matter into a business-critical strategic topic and, in today's world, competitive advantage for companies, whereas on the other hand, the case of Austrian Airlines requiring millions of Euros of state aid to continue their operations, illustrates how crisis situations faced by private companies can and do affect States.

As a matter of fact, we live in a time where the vulnerability of critical infrastructure is a real concern among security specialists19 and States, as illustrated by the following example: A joint memo, sent out in May 2020 by German intelligence and security agencies, warned German operators of critical infrastructure against hacker attacks. The memo included a description of the hackers ’approach as well as information indicating long-standing compromises in corporate networks of companies operating in the energy, water and telecommunications sector,20 in other words, critical sectors covered by the EU Network and Information Security Directive 2016/1148 (NIS).

It is in light of security incidents like these, that the results of and contradictions arising from this year's "Cyber Security isn Austria" study (KPMG,

---

[17] Hauser, Christine. *EasyJet Says Cyberattack Stole Data of 9 Million Customers.* May 19, 2020. https://www.nytimes.com/2020/05/19/business/easyjet-hacked.html
(accessed June 25, 2020).
[18] Hodoschek, Andrea. *Wirtschaft: AUA-Rettungspaket steht: 450 Millionen Euro Staatshilfe.* June 8, 2020. https://kurier.at/wirtschaft/aua-rettungspaket-steht-450-millionen-euro-staatshilfe/400934555
(accessed June 25, 2020).
[19] Allianz. *Cyber-attacks on critical infrastructure.* n.d. https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html
(accessed June 25, 2020).
[20] Tanriverdi, Hakan. *Kritische Infrastruktur: Behörden warnen vor Hackerangriffen.* May 27, 2020. https://www.br.de/nachrichten/deutschland-welt/kritische-infrastruktur-behoerden-warnen-vor-hackerangriffen,S0CJ1JP
(accessed June 25, 2020).

2020),21 may be perceived as especially worrying: According to the study, 27% of 652 companies surveyed place great trust in their Cyber Security measures, while 58% "rather" trust their Cyber Security measures. At the same time, 57% of participating companies became victims of cyber-attacks in the past 12 months, of which 74% where phishing attacks.22 It is important to note here, that, when it comes to the prevention of phishing attacks, security experts consider regularly training employees on security awareness, essential.23 In the context of such Cyber Security awareness measures, it seems especially interesting that the study highlighted the significance of employees in the detection of cyber-attacks, as opposed to merely focusing on employees as a potential weakness: 79% of companies stated that they had become aware of a cyber-attack through their own employees, while internal security systems ranked second (72%) as a means of detection. Awareness building measures must, therefore, remain a high priority for companies.24

Furthermore, the study established that one third of companies believe it would take them 1 to 4 weeks to safely remove attackers from their systems, while a fourth of companies even believe it would merely take them between 2 and 6 days. These findings are in direct contradiction with the considerably longer and demonstrably increasing average "dwell time" (100 to 170 days) of attackers in corporate networks.25 Regarding Cyber Resilience, it is worth noting here, that although 69% of companies surveyed invest in awareness and security monitoring to protect themselves against cyber-attacks, only 25% prepare for possible damage through cyber insurance coverage.26 Also, the study found that 82% of companies would like to see established a government agency dedicated exclusively to Cyber Security issues and 77% would like to be supported more by the State, while at the same time, 57% state that they do not trust the authorities when it comes to Cyber Security. Additionally, it was found that the primary expectation (64% of companies) companies have toward the State is the provision of information and EU-wide support as well as exchange between experts from the State and private sector, in order to learn from each other.27 Considering the companies ' expectations regarding the exchange of information between experts, it seems particularly striking that about 90% declined to comment on the effects that past Cyber Security incidents had in terms of damage caused to their reputation. Based

[21] KPMG. *Cyber Security in Österreich.* 2020.
[22] KPMG. *Cyber Security in Österreich.* 2020: 6.
[23] Lord, Nate. *Phishing Attack Prevention: How to Identify & Avoid Phishing Scams in 2019.* July 12, 2019. https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams (accessed June 25, 2020).
[24] KPMG. *Cyber Security in Österreich.* 2020: 13.
[25] KPMG. *Cyber Security in Österreich.* 2020: 4.
[26] KPMG. *Cyber Security in Österreich.* 2020: 6.
[27] KPMG. *Cyber Security in Österreich.* 2020: 23.

on this finding, it was concluded that a trustful exchange of information must be encouraged and observed, that changes to the existing legal framework would help facilitate open communication on cybercrime.28

All in all, it was concluded that Austrian companies mistrust others, but do not protect themselves sufficiently, that they demand cooperation, however, shy away from open communication and that they feel more secure than they are.29 In other words, "a false sense of security" in the Austrian private sector, emerged as a key finding.

It was already established earlier that "a false sense of security" means feeling safe in an unsafe environment. Therefore, it seems only logical to look in more detail at the threat environment, also known as risk environment, in which businesses in today's world operate in. For the sake of coherence and comparability, the following section will, first of all, examine Austria's situation before briefly considering the global risk environment:

The "Risks of Doing Business 2019" report (World Economic Forum) rates cyber-attacks as the most critical business risk in Austria (46.7%) and data fraud or theft as second critical (34.1%).30 Taking into account the previously discussed findings regarding levels of trust companies place in their security measures (27% trust "greatly", 58% "rather" trust)31 and unrealistic company estimates of attacker "dwell time" in corporate networks, "a false sense of security" clearly reemerges. The top Risks of Doing Business 2019 on a global scale are fiscal crises (28.9%), closely followed by cyber-attacks (28.2%) as the second critical risk and unemployment or underemployment (28.2%) as the third critical risk, while data fraud or theft ranks seventh (22.4%),32 firmly establishing technological risks among the most critical risks globally.

Overall, and especially against the background of the global risk environment and increasing interconnectedness of the public and private sector, "a false sense of security", or to be more precise, "a false sense of Cyber Security" in the private sector must, therefore, be considered a significant threat for the security of private companies and, consequently, the security in Europe, a warning sign regarding the status quo of Europe's Cyber Resilience and, one may argue, valuable instrument in assessing the effectiveness of Cyber Security awareness measures.

While the scope and purpose of this essay did not allow for an in-depth analysis of how "a false sense of security" may practically be translated into a

[28] KPMG. *Cyber Security in Österreich.* 2020: 14.
[29] KPMG. *Cyber Security in Österreich.* 2020: 4.
[30] World Economic Forum. *Risks of Doing Business 2019.* 2019.
[31] KPMG. *Cyber Security in Österreich.* 2020: 6.
[32] World Economic Forum. *Risks of Doing Business 2019.* 2019.

quantifiable, clearly defined key performance or risk indicator, it may serve as a starting point in doing so. Also, it may rightfully be argued that any indicator of performance or risk must be evaluated in the context of already established key performance and risk indicators, as well as existing efforts, procedures and best practices in the field, in order to fully assess its value and usefulness. Again, the scope of this essay did not allow for an in-depth analysis in this regard. Nevertheless, it may prove useful as a starting point in doing so. Other limitations and challenges arising from the scope, purpose and choice of approach as well as ideas advanced in this essay, include the risk of bias when generalizing from Austria to Europe and the risk of response bias (demand bias) when utilizing survey questions to identify "a false sense of security" with the same participants.

Nevertheless, despite these limitations, it seems possible to derive the following conclusions from the analysis conducted in this essay: a) the security and stability in Europe depend on the ability of States to continuously improve and maintain their Cyber Resilience, b) Europe's Cyber Resilience is closely tied to the Cyber Resilience of each States 'private sector and, as a result, the actors operating within them, c) improving cooperation and trust between the public and the private sector as well as between States is necessary to improve Europe's Cyber Resilience and, d) an organization with the appropriate authority, financial and professional capacity as well as reach, such as, one may argue, the OSCE, must act as the initiator and governing body of projects aiming to utilize "a false sense of security" to assess Europe's Cyber Resilience and existing security awareness measures.

All in all, one may conclude that in order to ensure and enhance security and stability in Europe in our increasingly interconnected world, especially in the face of rapid technological progress, new technologies and the recent acceleration of digitalization, an urgent need to continuously improve and monitor Europe's Cyber Resilience exists. This will call for more and more cooperation between the public and private sector, as well as between States and will, consequently, likely even heighten the significance of international organizations, such as the OSCE, in initiating, financing, overseeing and supporting Cyber Resilience initiatives in Europe.

ISSN 2704-6419

The Author:

Julia Wurm *is a Vienna-based specialist in cyber security and the EU cyber legislation.*

ISSN 2704-6419

Vision & Global Trends - International Institute for Global Analyses

www.vision-gt.eu info@vision-gt.eu