www.jusletter-it.eu

Fabian Teichmann / Sonia Boticiu / Bruno S. Sergi

Cybersecurity Trends in 2023

Cybercrime is a serious global problem. Moreover, in light of the COVID-19 pandemic, the cybersecurity landscape has undergone dramatic changes. Cybercriminals have taken advantage of the rise of remote working and cloud adoption and focused their attacks on remote access vulnerabilities. In addition, the war in Ukraine continues to have a profound economic, human and commercial impact on businesses, further exacerbating their situation. As a result, corporate security teams are struggling to keep up with the increasingly sophisticated and frequent attacks that threaten today's cyber landscape. For this reason, this paper aims to review the latest cybersecurity trends and threats that have emerged in light of current events and need to be addressed in 2023. In addition, this paper contributes to the literature by providing companies with practical ways to reduce their exposure to cyber-attacks.

Category of articles: Articles
Region: EU
Rechtsgebiete: Cybersecurity, Cybercrime

Citation: Fabian Teichmann / Sonia Boticiu / Bruno S. Sergi, Cybersecurity Trends in 2023, in: Jusletter IT 20. Dezember 2022

Contents

1. Introduction

[1] Today, technologies underpin almost every facet of the society we live in. For this reason, forensic and cyber security specialists are facing cyber threats on an ever-increasing scale.[1] Indeed, everyday life is facilitated by the development of technological innovations, but these, in addition to the benefits, also make major contributions to crime. Therefore, cybercrime has now become a serious global problem.[2] In addition, since 2020, the COVID-19 pandemic has completely disrupted the cybersecurity threat landscape. The internet has been promoted as a necessity more than ever, especially for school and business activities.[3] However, services and business operations must continue uninterrupted and efficiently. Technologies such as the internet, artificial intelligence, VPN, chatbots, autonomous systems and cloud computing are facilitating the migration of many services and operations online, specifically this digital transformation.[4] Therefore, cybercriminals have taken advantage of the increase in the number of people working remotely and the adoption of the cloud and focused their attacks on remote access vulnerabilities.

[2] In terms of remote working, one example of criminals exploiting cyber security weaknesses has been the series of cyber-attacks on videoconferencing services. Specifically, between February 2020 and May 2020 alone, more than half a million people were affected by breaches in which the personal data of videoconferencing service users was stolen and sold on the dark web.[5] As a result, corporate security teams are struggling to keep up with the increasingly sophisticated and frequent attacks that threaten today's cyber landscape. This has forced organizations to become

[1] Cabaj Krzysztof/Zbigniew Kotulski/Bogdan Ksiopolski/Wojciech Mazurczyk, «Cybersecurity: trends, issues, and challenges», *EURASIP Journal on Information Security* 2018, no. 1 (2018): 1–3.

[2] Sarre Rick/Laurie yiu-chung Lau/Lennon Yc Chang, «Responding to cybercrime: current trends», *Police practice and research* 19, no. 6 (2018): 515–518.

[3] Vladescu Cristiana/Maria-Alexandra Dinisor/Octavian Grigorescu/Dragos Corlatescu/Cristian Sandescu/Mihai Dascalu, «What are the Latest Cybersecurity Trends? A Case Study Grounded in Language Models», in : *2021 23rd International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, pp. 140–146. IEEE, 2021.

[4] Weil Tim/San Murugesan, «IT risk and resilience – Cybersecurity response to COVID-19», *IT professional* 22, no. 3 (2020): 4–10.

[5] Cedric Nabe, Impact of COVID-19 on Cybersecurity, 2022, Available at: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (Accessed 25.10.2022).

security conscious and increase their threat defenses.[6] In addition, some small and medium-sized businesses are taking a Bring Your Own Device (BYOD) approach as opposed to a Corporate Owned Personally Enabled (COPE) approach, which means that company employees can use their personal devices to access company information. This may be one of the reasons for the increase in cyber-attacks, as working from home does not guarantee the same level of cyber security as in an office environment.[7]

[3] However, in addition to the challenges facing companies in the wake of COVID-19, the war in Ukraine continues to have a profound economic, human, and commercial impact on companies, further aggravating their situation. The effects of the invasion are also expected to be felt in various areas of cybersecurity as the conflict drags on.[8] Increasingly sophisticated cyber-attacks that have put the assets and data of governments, corporations and individuals at risk involve machine learning, cryptocurrencies, phishing, artificial intelligence, malware and more.[9] According to Statista Research Department (2022), internet users worldwide experienced approximately 52 million data breaches in the second quarter of 2022, down 56% from the previous quarter.[10] The highest number of data breaches in the period measured was detected in the fourth quarter of 2020, nearly 125 million. By 2025, it is estimated that cybercrime will cost companies around the world an estimated $10.5 trillion annually. Moreover, with an annual growth rate of 15%, cybercrime represents the largest transfer of economic wealth in history.[11]

[4] Both the cyber threat landscape and cyber security are evolving rapidly, and this has been particularly true in recent years. For this reason, this article aims to review the latest cybersecurity trends and threats that have emerged in light of current events and that need to be addressed in 2023. In addition, practical ways to reduce companies' exposure to cyber-attacks are offered. This paper is structured as follows: Section 2 looks at cyber security trends and threats for the year 2023. Section 3 provides practical ways for companies to reduce their exposure to cyber-attacks. The last section contains concluding remarks.

2. Cybersecurity trends and threats for 2023

[5] In recent years, cyber security and the cyber threat landscape have changed rapidly. Especially as the COVID-19 pandemic has brought major changes to business operations and corporate IT

[6] Alawida Moatsum/Abiodun Esther Omolara/Oludare Isaac Abiodun/Murad Al-Rajab, «A deeper look into cybersecurity issues in the wake of Covid-19: a survey», *Journal of King Saud University-Computer and Information Sciences* (2022).

[7] See Nabe (note 5).

[8] Aaron Clarke, Hacking the Invasion: The Cyber Implications of Russia's Invasion of Ukraine, 2022. Available at: http://thirdway.imgix.net/pdfs/hacking-the-invasion-the-cyber-implications-of-russias-invasion-of-ukraine.pdf (Accessed 26.10.2022).

[9] Michelle Moore, 7 Top Trends in Cybersecurity for 2022, 2022. Available at: https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022 (Accessed 28.10.2022).

[10] Statista, Number of data records exposed worldwide from 1st quarter 2020 to 2nd quarter 2022, 2022. Available at: https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/ (Accessed 26.10.2022).

[11] Embroker, 2022 Must-Know Cyber Attack Statistics and Trends, 2022. Available at: https://www.embroker.com/blog/cyber-attack-statistics/ (Accessed 26.06.2022).

architectures.[12] Cybercriminals have taken advantage of these changes and targeted their attacks on remote access vulnerabilities as well as other solutions adopted as part of the new security reality.[13] For this reason, companies are struggling to keep up with increasingly sophisticated attacks and the parallel shift in security trends. Therefore, security leaders who better understand new trends will automatically be better prepared to deal with new risks. For this reason, this section aims to highlight the main cyber threats and trends for 2023.

2.1. Ransomware

[6] Today, ransomware is considered to be one of the biggest cybersecurity threats to businesses of all sizes.[14] Ransomware attacks work by infecting the network and locking up data until the hacker is paid a ransom. Ransoms are usually paid in Bitcoin.[15] In 2021, according to the 2022 Cyber Threat Report, ransomware attacks increased by 105%.[16] These cyber-attacks can be extremely damaging to companies. This is because, in addition to the financial losses suffered, there are also losses of data and productivity. In 2021, 37% of organizations and businesses were affected by ransomware, and the cost of recovering from a ransomware attack incurred by companies averages up to $1.85 million.[17] In recent years, ransomware has changed significantly. While classic attacks still occur, most attacks against businesses now involve dual extortion techniques. Specifically, the victim's data is encrypted and stolen with the intention of making it public if the victim does not pay the ransom. Another emerging trend is extortionware. This involves cybercriminals stealing data without actually encrypting the victim's files.[18]

2.2. Risks with IoT

[7] The Internet of Things (IoT) refers to connecting devices such as laptops and tablets, cars, kitchen appliances, webcams, smart watches, routers, heart monitors and more to the internet.[19] According to Statista, the number of IoT-connected devices is expected to reach 75 billion by

[12] Buil-Gil David/Fernando Miró-Llinares/Asier Moneva/Steven Kemp/Nacho Díaz-Castaño, «Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK», *European Societies* 23, no. sup1 (2021): S47–S59.

[13] Vu Anh V/Jack Hughes/Ildiko Pete/Ben Collier/Yi Ting Chua/Ilia Shumailov/Alice Hutchings, «Turning up the dial: the evolution of a cybercrime market through set-up, stable, and covid-19 eras», in: *Proceedings of the ACM Internet Measurement Conference*, pp. 551–566, 2020.

[14] Roberto Musotto/David S. Wall, «More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime», *Trends in Organized Crime* (2020): 1–19.

[15] Savita Mohurle/Manisha Patil, «A brief study of wannacry threat: Ransomware attack 2017», *International Journal of Advanced Research in Computer Science* 8, no. 5 (2017): 1938–1940.

[16] SonicWall, 2022 SonicWall Cyber Threat Report, 2022. Available at: https://www.sonicwall.com/2022-cyber-threat-report/ (Accessed 25.10.2022).

[17] Sophos, The State of Ransomware 2021, 2021. Available at: https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469 (Accessed 20.10.2022).

[18] Alexander Culafi, Ransomware in 2022: Evolving threats, slow progress, 2022. Available at: https://www.techtarget.com/searchsecurity/news/252522369/Ransomware-Evolving-threats-slow-progress (Accessed 27.10.2022).

[19] Sita Rani/Aman Kataria/Vishal Sharma/Smarajit Ghosh/Vinod Karar/Kyungroul Lee/Chang Choi, «Threats and corrective measures for IoT security with observance of cybercrime: A survey», *Wireless Communications and Mobile Computing* 2021 (2021).

2025. This, would represent a nearly three-fold increase over the installed base of IoT in 2019.[20] Hackers can access the network through IoT devices and extract data from the cloud to use against users for ransom. Many experts believe that due to the rapid adoption of IoT technologies in enterprises, IoT could become one of the biggest cybersecurity threats in the future.[21]

2.3. Cloud Vulnerabilities

[8] The use of cloud storage has skyrocketed in recent years. As more and more organizations choose to store their sensitive data in the cloud, cyber attackers are keen to find a way to exploit it. Even if cloud applications like Microsoft or Google are well-equipped with security systems, it is the user side that acts as a significant source of erroneous errors, phishing attacks and malicious software.[22] Companies need a comprehensive strategy for effective defense, in addition to the use of cloud security solutions, to combat the role of cloud vulnerabilities in cyber-attacks.[23]

2.4. Attack surface expansion

[9] As a result of significant changes in the use of digital systems, including accelerated use of the public cloud, new hybrid activities, as well as more tightly interconnected supply chains, etc., a dramatic increase in the attack surface has emerged.[24] All these changes have created new and challenging attack surfaces. They also introduce gaps in coverage for log data collection, data protection, preventive controls, business continuity plans, and monitoring and incident response capabilities. All of these lead to an increase in exploitable blind spots.[25]

2.5. DDoS attacks

[10] In 2022 there was a dramatic increase in distributed denial-of-service (DDoS) attacks.[26] According to the 2022 H1 Global Threat Analysis Report published by Radware, cyber attacks have also increased dramatically as a result of the Russian invasion of Ukraine. The first six months of 2022 saw a 203% increase in DDoS attacks compared to the first six months of 2021. Patriotic hacktivism also increased in the first half of 2022. Both pro-Ukrainian and pro-Russian cyber

[20] Statista, Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025, 2022. Available at: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (Accessed 27.10.2022).

[21] Krishna Kagita Mohan/Navod Thilakarathne/Thippa Reddy Gadekallu/Praveen Kumar Reddy Maddikunta/Saurabh Singh, «A Review on Cyber Crimes on the Internet of Things», *arXiv e-prints* (2020): arXiv-2009.

[22] Nikita Duggal, Top 10 Cybersecurity Trends to Watch Out For in 2022, 2022. Available at: https://www.simplilearn.com/top-cybersecurity-trends-article (Accessed 27.10.2022).

[23] Gayatri S. Pandi/Saurabh Shah/K. H. Wandra, «Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation», *Procedia Computer Science* 167 (2020): 163–173.

[24] Susan Moore, 7 Top Trends in Cybersecurity for 2022, 2022. Available at: https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022 (Accessed 28.10.2022).

[25] Pete Shoard, Top Trends in Cybersecurity 2022. Attack Surface Expansion, 2022. Available at: https://www.gartner.com/doc/reprints?id=1-29OTFFPI&ct=220411&st=sb (Accessed 28.10.2022).

[26] Alexander Gutnikov/Oleg Kupreev/Yaroslav Shmelev, DDoS attacks in Q2 2022, 2022. Available at: https://securelist.com/ddos-attacks-in-q2-2022/107025/ (Accessed 27.10.2022).

legions aimed to disrupt and create chaos through information theft and leakage, defamation, and denial-of-service attacks.[27]

2.6. Social Engineering

[11] Social engineering attacks involve compromising a person to get them to unknowingly disclose confidential information and bypass security protections. Criminals use cunning and deception to lure employees into falling for the bait. These attacks usually take the form of phishing, by sending emails with malicious links, and scareware, by scaring users with false alarms to get them to buy infected software.[28] Such attacks are on the rise, which is why it is essential that individuals and organizations are aware of their relevance and develop strategies to combat their effectiveness.

2.7. Evolution of multi-factor authentication

[12] The multifactor authentication market was valued in 2020 at $10 billion and is expected to exceed $28 billion by 2026.[29] Multi-factor authentication refers to an electronic authentication method that allows users to access an application or website after submitting two or more types of proof of identity to an authentication system. Although this method is considered to be highly secure, Microsoft claims that the SMS and voice authentication method poses increased security risks. SMS authentication methods are vulnerable to automated man-in-the-middle attacks. However, experts still recommend using SMS authentication if there are no other security options.[30]

3. Discussions and recommendations

[13] Many businesses have not been adequately prepared to meet the challenges of remote working and the rise of sophisticated cyber-attacks. In terms of working from home, it is recommended that employees are provided with a license for anti-virus and malware software for use on personal computers. While this is not necessarily a fail-safe protection, it does help eliminate many low-level attacks.[31] In addition, businesses need to develop well-organized cyber security risk management plans and train employees on the prevalence and detection of cyber-attacks. Staff

[27] Radware, 2022 H1 Global Threat Analysis Report, 2022. Available at: https://www.radware.com/pleaseregister.aspx/?returnurl=18bf850e-6320-44a7-85e3-65f9ef072dc8 (Accessed 27.10.2022).

[28] Jack Koziol/Rob Watts/Cassie Bottorff, Most Common Cyber Security Threats In 2022, 2022. Available at: https://www.forbes.com/advisor/business/common-cyber-security-threats/ (Accessed 28.10.2022).

[29] BusinessWire, $28.34 Billion Multi-factor Authentication Market – Global Growth, Trends, and Forecasts 2021–2026 – ResearchAndMarkets.com, 2021. Available at: https://www.businesswire.com/news/home/20210311005630/en/28.34-Billion-Multi-factor-Authentication-Market—Global-Growth-Trends-and-Forecasts-2021–2026—ResearchAndMarkets.com (Accessed 28.10.2021).

[30] Josh Howarth, 8 Huge Cybersecurity Trends (2022), 2022. Available at: https://explodingtopics.com/blog/cybersecurity-trends (Accessed 28.10.2022).

[31] See Nabe (note 5).

should always be up to date with cloud storage best practices and always be vigilant when receiving emails, checking the authenticity of the sender's address first.[32]

[14] Although ransomware is one of the biggest cyber threats to businesses today, there are still many ways for companies to protect themselves against ransomware infection. It is necessary that all applications, operating systems, and software are regularly updated. Automatic updates are even more effective, as the latest security patches are updated automatically.[33] Another method of protection is to limit users to only accessing the data they need to work. A well-developed incident response plan is also necessary so that during a ransomware event, the company's IT security team knows what steps to take.[34] In addition, social engineering comes in many variations, making it difficult to prepare the organization for what may happen to it. For this reason, a strong cybersecurity awareness training program is necessary to prevent a social engineering attack.[35]

[15] One way to reduce the vulnerability of IoT devices is through network segmentation techniques, which allow specific components to be isolated from others to improve security. Network segmentation can help prevent malicious people or attackers from connecting or prevent compromised devices from infecting other parts of the network.[36] Another way to reduce vulnerability to attacks is to require full authentication of all devices. It is recommended to use the most secure authentication available on the device and never use factory default passwords.[37]

[16] The first step that should be taken if multiple users can access a company's cloud storage is to introduce authorization levels. For example, all employees of a certain rank should be given a single password that allows them access to the information they need. Of course, if a company wants to be even more vigilant, it can give each employee a special password and unique identifier. In addition to strong passwords to make company accounts impossible to break into, two-step authentication can also be implemented. This means that, as an extra precaution, users will also receive a time code on their email addresses or phones.[38] However, while multi-factor authentication is considered by many to be very secure, SMS authentication methods can be vulnerable to man-in-the-middle attacks. The biggest risk is posed by online banking, due to the inefficiency of multi-factor authentication methods, almost always performed via SMS verification. Cybersecurity experts recommend hardware security keys for verification whenever possible to reduce the risk of unauthorized access to accounts.[39]

[32] Wu He/Zuopeng Zhangz, «Enterprise cybersecurity training and awareness programs: Recommendations for success», *Journal of Organizational Computing and Electronic Commerce* 29, no. 4 (2019): 249–257.

[33] Kyle Chin, How to Prevent Ransomware Attacks: Top 10 Best Practices in 2022, 2022. Available at: https://www.upguard.com/blog/best-practices-to-prevent-ransomware-attacks (Accessed 28.10.2022).

[34] Chen Po-Hao/Robert Bodak/Namita S. Gandhi, «Ransomware recovery and imaging operations: lessons learned and planning considerations», *Journal of Digital Imaging* 34, no. 3 (2021): 731–740.

[35] See Koziol/Watts/Bottorff (note 28).

[36] John Allen, 7 Mitigation Strategies to Address IoT Security Risk, 2021, Available at: https://www.codemotion.com/magazine/backend/iot/7-mitigation-strategies-to-address-iot-security-risk/ (Accessed 31.10.2022).

[37] Tal Guest, Top IoT Security Risks and Vulnerabilities and How to Mitigate Them, 2022. Available at: https://www.beyondtrust.com/blog/entry/top-iot-security-vulnerabilities. (Accessed 31.10.2022).

[38] MJ Shoer, How to mitigate cloud security threats, 2021. Available at: https://www.industrialcybersecuritypulse.com/iiot-cloud/how-to-mitigate-cloud-security-threats/ (Accessed 31.10.2022).

[39] See Howarth (note 30).

4. Conclusion

[17] The COVID-19 pandemic has shown us that preparedness is key to limiting the risks of cyber-attacks. The ability to react in a timely manner to unforeseen events goes a long way towards reducing the impact of a cyber-attack.[40] Since the onset of the pandemic, cyber-attacks have increased exponentially, resulting in financial and reputational losses for many businesses. In addition to the challenges companies are already facing as a result of the pandemic, the trade implications of the conflict in Ukraine will be felt far beyond the region's borders. Therefore, the geopolitical repercussions of the conflict between Russia and Ukraine are now a critical time for businesses to assess their exposure to cyber-attacks. In addition, the effects of the invasion are expected to be felt as the conflict drags on in various areas of cyber security. Given the existing threat environment, it's only a matter of time before an organization suffers a cyber-attack. Nevertheless, there are ways to reduce the likelihood and impact of a cyber-attack, but it takes action and focused planning. For this reason, this paper aims to review the latest cybersecurity trends and threats that need to be addressed in 2023. In addition, this study aims not only to help the reader become familiar with the changes in cybercrime and highlight new tactics used by cybercriminals, but also to provide measures to protect against them. These measures offer companies practical ways to reduce their exposure to a cyber-attack. They can be used to guide future research and improve current understanding of how organizations can better equip themselves to respond appropriately to cyber threats.

Fabian M. Teichmann is an attorney-at-law and public notary in Switzerland. After earning an undergraduate degree in Economics and Finance (Bocconi University, Italy), he earned graduate degrees in Management (Harvard University, USA), Accounting and Finance, and Law (University of St. Gallen, Switzerland). He also holds a PhD in Law (University of Zurich, Switzerland), a Doctorate in Economics and Social Sciences (Kassel University, Germany), and an LL.M. (King's College, England). Teichmann teaches courses on compliance, corruption, money laundering, and terrorism financing at various universities. He is the author of several books and over 100 scholarly articles.

Sonia R. Boticiu is a research associate at Teichmann International (Schweiz) AG. She is is currently enrolled in an Executive Master of Laws (LL.M.) program in Banking and Financial Market Law at the University of Liechtenstein. She completed her Bachelors and Masters degree in Law at the University of Craiova, Romania. Boticiu has co-authored publications in diverse fields such as money laundering, compliance, corruption terrorist financing and ransomware.

Bruno S. Sergi teaches on emerging markets and the political economies of Russia and China at Harvard University; he is an Associate of the Davis Center for Russian and Eurasian Studies; and he is Scientific Director of the Lab for Entrepreneurship and Development at Harvard. He also teaches international economics at the University of Messina, is the Series Editor of *Cambridge Elements in the Economics of Emerging Markets*, Co-Series Editor of the Emerald Publishing book series *Harvard Lab for Entrepreneurship and Development*, an Associate Editor of *The American Economist*, and Co-Founder and Scientific Director of the International Center for Emerging Markets Research at RUDN University in Moscow.

[40] See Nabe (note 5).