Future Roles in Digital Security – 2023 and Beyond

What historical trend data tells us about future roles and tasks in digital security

By Yuri Bobbert & Vincent van Dijk

Looking at cyberdata collected in recent times reveals intriguing insights that may affect our future view on digital security education as a prime defense mechanism for dealing with future threats. In this article, we first observe the cumulative change in cyber threat actors followed by summarizing our analysis of more than 20 years of cyberdata, based on the VERIS Community Database[1] in order to distill key trends by extrapolating trends toward the future. When examining these findings, we then used our own expertise and observations to suggest future roles that might dominate the field of cybersecurity.

Introduction

Over the last 21 years, "misuse" and "human error" have been seen as the most significant root cause of data breaches. From 2000 to 2021, we observe 4,457 out of 10,363 "human errors" as the root cause. According to research report Ponemon "*Data breach costs rose from US$3.86 million to US$4.24 million, the highest average total cost in the history* [1]" We also know that *287 is the average number of days taken to identify and contain a data breach. The longer it took to identify and contain, the more costly the breach.*

In Figure 1 we observe that the cybersecurity industry is now better at identifying actors. Second, there is a significant rise in organized crime (5% to 38%), and lastly, the danger of mistakes by developers is increasing (from 0% ten years ago to 11% today). The actors have become increasingly sophisticated, and the impact is more catastrophic than 20 years ago.

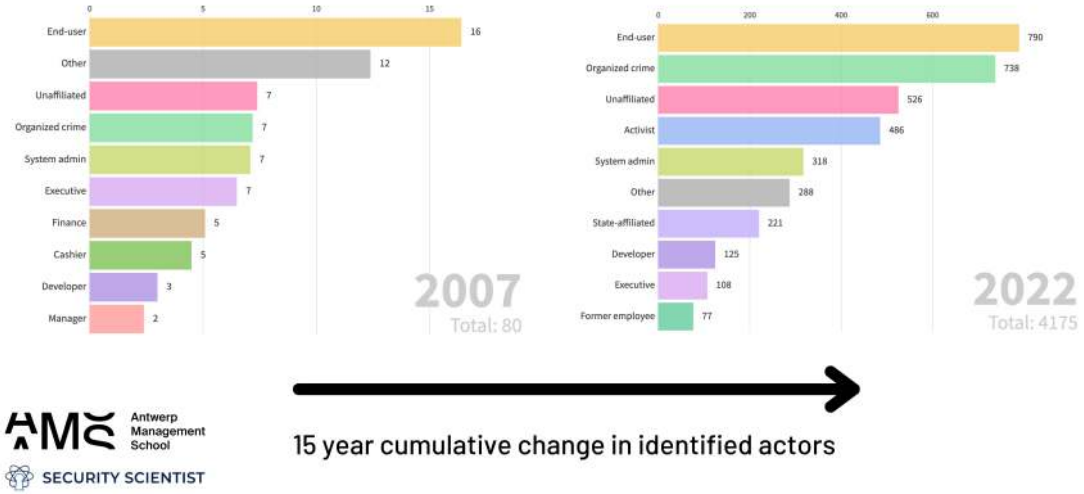

Figure 1 A 15-year cumulative change in identified actors in Cyber security incidents

How can we manage these continuously evolving threats of bad actors manipulating our data and human errors? In our current and future world of machines, robots, and algorithm-based decision-making. Technological and political trends will continue to influence our profession. This new world will call for new capabilities and expertise. Thus, jobs will require new skillsets to take into account, that address the future challenges we see ahead. The role of CEO and CFO will change due to tech dominance in business, and the position of the (chief) security officers and risk and security leaders will change. Zukin et al. (2018) state *"A broader skillset,*

[1] We used the open-source dataset VERIS Community Database - the largest open-source dataset on data breaches. Python programming language was used to format the data. Tableau to create static visualizations and Flourish to create animated visualizations (https://github.com/vz-risk/VCDB).

including communication, change management, and leadership, is required to respond quickly and collaboratively to evolving cyber threats."[2]

Also, the SEC recognizes this as a profession that must be directed top-down from the board[3]. The CSO role is embryonic compared to that of the CFO and not completely clear about expectations, let alone all the positions that work below the CSO required to address the issues mentioned in our introduction.

Important Trends

Based on our research we have identified the following significant trends impacting the capabilities required from the workforce, and we use these to distill – in the next section – some important job profiles:

- A top-down approach to cybersecurity [2]
- The risk of spreadsheet-based security assurance [3]
- An increase in technology adoption requires "craftmanship" [4]
- Security spending is under scrutiny [4] [5]
- Sophistication and dynamics of cyber actors and attacks[5] [6]
- Lacking awareness campaigns [6]
- State-sponsored spionage [6] [7] [8] [9] [10]
- Mis-configurations and human errors [7]
- Machine learning and artificial intelligence [4]
- Distributed – fragile – hybrid environments [11] [12] [13]
- Cybersecurity alarm fatigue[8]
- New ways of working (DevOps, Agile, Scrum) [12]
- Continuous software development [3]
- Regulatory and assurance (integrated reporting) pressure [14]
- Outsourcing of security tasks[9] [10]
- Ethics in cybersecurity [11] [10]

---

[2] L. Zuzkin, J. Lopez, E. Weiss Kaya en A. Smallwood (2018), "Cybersecurity readiness trough workforce development," in *Navigating the Digital Age*, Tim Dempsey, 2015, pp. 307-311

[3] https://www.forbes.com/sites/bobzukis/2022/04/18/the-sec-is-about-to-force-cisos-into-americas-boardrooms/
[4] Is Digital Security a market for lemons? (https://12ways.net/blogs/digital-security-in-2025-when-the-novelty-wears-off-and-budget-pressure-remains)
[5] https://12ways.net/blogs/never-trust-and-always-verify-the-increasing-number-of-cyber-threats-risks/
[6] Why Security Awareness Campaigns aren't enough for secure behavior (https://12ways.net/blogs/why-security-awareness-campaigns-arent-enough-for-secure-behavior)
[7] What the hack happened? A CISO perspective on the Cosmos DB vulnerability, https://12ways.net/blogs/what-the-hack-happened-a-ciso-perspective-on-the-cosmos-db-vulnerability/
[8] Four angels to avoid the risk of Cyber Security Fatigue. https://12ways.net/category/blogs/
[9] The IKEA effect on Cybersecurity investment decisions https://12ways.net/blogs/the-ikea-effect-on-cybersecurity-investment-decisions/
[10] Wakefield Research and Deloitte Report on *The future of cyber survey 2019*, polled 500 C-level executives who oversee cybersecurity at companies with at least $500 million in annual revenue including 100 CISOs, 100 CSOs, 100 CTOs, 100 CIOs, and 100 CROs
[11] *The ethics & economics of cyber risk* (https://12ways.net/blogs/the-ethics-economics-of-cyber-risk)

- War on talent
- Difficulties with handling data according to regulatory requirements [15]
- Virtual identities.

Our objective is not to be exhaustive but to give you some significant trends based on our experience and external research reports and articles. These trends will demand other capabilities and, therefore, roles in the cyber domain such as: **Cyberdata Analyst**, **Cyber Attack Agent, Cyber Calamity Forecaster, Machine Risk Officer, Virtual Identity Defender, Data trash engineer, Cloud orchestration architect, Security vaccinator, Cyber talent magnet, and AI auditor.** We briefly explain each function in the section below to give you an idea about what those roles mean. In the end, we blend this into our vision of the part of the CISO and the future – workforce – curriculum.

Due to the rapidly changing threat landscape and the morphing actors, it is hard to keep up with this knowledge and translate it into actions. These actions seem to work. We also identified that the cybersecurity in the healthcare industry was substantially improved, resulting in the percentage of medical data compromised decreasing from 44% in 2010 to 14% in 2021 (Figure 2) based upon 100% deviation between the several data types (might be so that amount of data increased). Financial data has also become less exposed. The reason for that is that regulated companies expend more efforts on cybersecurity and framework implementations that are designed to prevent financial data from being exposed. On the other hand, we note that regulatory requirements and associated frameworks are not a 'silver bullet' and that personal data breaches have increased (from 20% in 2011 to 43% in 2021) despite mandatory data protection laws (e.g. GDPR, CCPA[12]) in place since early 2018. The main reason for this is the lack of knowledge and skills [to implement technical measures], confirmed by research at Antwerp Management School in 2020 [15]. All of these trends make us wonder what our future priorities should be: should we put technology *or* education first?

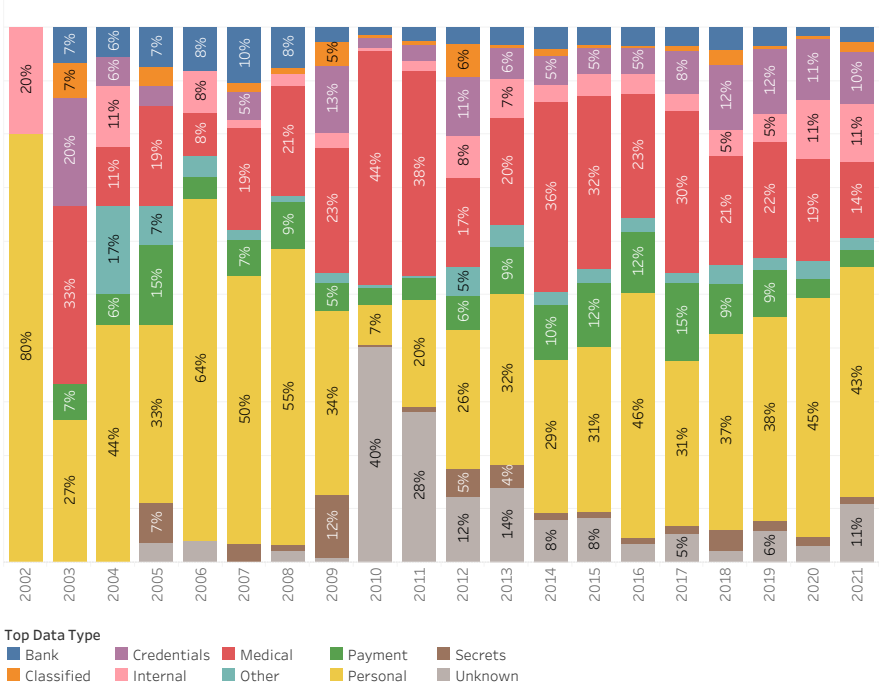

Figure 2 Top 10 data types compromised in the last 20 years.

The **Cyber Calamity Forecaster** reveals overlooked possibilities and exposes unexamined assumptions about the cyber world. The ideal candidate will provide analytical, advisory, and technical expertise and analysis related to global cyber activities by assessing the current and predicted cyber environments and geopolitical

[12] California Consumer Privacy Act

developments. It issues cyber products, alert bulletins, and forecasts. But this calamity forecaster requires that three significant new capabilities are combined into one role.

In current network security, vigilance in relation to new threats and attack vectors is becoming increasingly critical. Rapid detection, risk assessment, and preventive or mitigating measures are gaining prominence.

Issues when dealing with threats at – a larger – scale

To face this problem, cyberthreat agents or Security Operations Centers (SOCs) rely on a vast body of reports of newly detected (or suspected) threat avenues that are reported in public sources: newsfeeds, mailing lists, Twitter streams, forums, etc. Many non-public sources are also offered: like paid vendor threat bulletins and announcements in closed channels. This forms a growing challenge, which is a specific instance of the 'firehose' data problem. A lot of data is available. Beforehand, its veracity is never beyond doubt. Moreover, it is not guaranteed to be structured so that automated or emi-automated processing is easily enabled. And, with many data sources potentially shedding light (potentially from different perspectives) on issues that share underlying coherence, discovering the relationship between reports from various sources is a critical enterprise. Also of note is that data sources are linguistic, with a wide range of potential source languages. Many are in English (of varying quality), but far from all, and one should never exclude the possibility that a highly relevant and urgent report could be published in Russian, Korean, Chinese, German, French (etc.) first.

Given the data stream's size ('firehose'), the scalability problem arises; a high level of automation is called for. With this problem in mind, we define three related capabilities:

1. Assessing Data Source Quality
2. Intelligent Correlation, Relevance, and Risk Determination
3. Automating Data Source Handling Process Flow and directing that to target audiences in a presentable and actionable format.

Based on the threat data, the calamity forecaster can carry out trend analysis on sectors (finance, retail, manufacturing), countries, platforms (Microsoft, Oracle, etc.), environments (Industrial plants), etc. This role is becoming more and more critical since the majority of the people do not see the trees in the wood anymore and need somebody to translate calamity information into possible decisions.

New Roles in Digital Security

Unlike the role of a security analyst, the **Cyberdata Analyst** is not concerned with operational cybersecurity issues. Instead, the Cyberdata Analyst examines on a tactical and strategic level how to predict upcoming threats based on the organization's data. These predictions serve as a compass for correctly prioritizing cybersecurity efforts.

The role of the **Machine Risk Officer** will be essential in developing new trust mechanisms and imagining new risk-benefit approaches for working with intelligent machines. The employee in this position will define roles and responsibilities between humans and machines and set the rules for how human counterparts should handle machine-based wrongdoing.

The role of the **Cyber Diplomat** will be essential for managing stakeholders and regulators and finding collaboration and allies with other public and private companies and governments. The reason why wars are won is by having the right allies – and enough – allies. Going to war without them is a receipt for failure, as history teaches us (ref. Napoleon and Hitler).

The employee in this position will form solid alliances and influence the external world about the entity's opinion.

As a **Cyber Attack Agent/SEAL**, you'll form part of a new Special Operations division within the SOC, tasked with developing, undertaking, and leading the cyber deterrent program. As a key member of this team, you will assist in developing and, in wartime (e.g. currently in Ukraine), delivering strategic cyber offenses against

adversaries' infrastructure and public and private sector systems. To be considered for this critical role, you must display an excellent track record of cyber hacking, "gray-hat-focused" software development, or distributed denial of service attack experience. Cyber attack agents/seals will need to operate as an effective and highly nimble team, collaborating closely with each other and the National Cybersecurity Centers (NCSC) cybersecurity teams.

In the role of **Data Trash Engineer,** you'll apply analytical rigor and statistical methods to data trash to guide decision-making, product development, and strategic initiatives. This will be done by creating a "data trash nutrition labeling" system that will rate the quality of waste datasets and manage the "data-growth-data-trash" ratio. This role is needed to avoid 'obese' data collection by organizations and to adhere to GDPR regulatory requirements such as data retention schemes.

The **Cyber Philosopher** will keep the discussion about the balance between humanity and machines alive to prevent "Judgment Day" from happening.

The **AI Auditor** will form an independent opinion about the integrity of the AI. This auditor will be a member of a governmental institute that audits without asking and without any financial incentives. As we will see below, the Auditor can not be part of a commercial organization.

The **Security User Experience (SUX)** Designer is an expert in building security within products and services and not giving them an unfriendly experience. This is caused by the way security has been designed as an integral part of the product or service, resulting in a perfect balance between ease of use and a secure and safe experience. In a world where it is unknown who can be trusted, trust will become essential for business strategy.

The role of Permanent Education

For these future roles, you need educated talent. Many learning and certification programs that have already been developed are a complete forest of trees for many HR professionals or recruiters. For the HR professional, it is becoming more and more complex to distinguish talent from amateurs. You simply cannot judge on certification alone; one needs to look deeper into intrinsic motivations and personal capabilities. This seems obvious, but in Information security, it is not easy for an HR professional to see how good someone is in a particular domain.

Lee proposes in the article "Seeking the Purple Squirrel" to opt for an open job description named "Desired Experience": *"Security is a rapidly evolving space, made up of numerous different technologies, and no single person is expected to possess every characteristic in this list. A curious mind, an ability to think about the rules and how to break them, and a willingness to learn are the most important traits we look for. If you have some of the following and are willing to learn more of them, we want to hear from you."*[13]

Despite great progress in the industry, the race for talent, and the search for the Purple Squirrel, data and information inaccuracy remain a considerable challenge for many organizations. Inadequate detection rates and slow response to attacks are evidence of this. The lack of craftsmanship is the leading root cause for these insufficiently configured security tools and the many-point solution. But the stakes are high. An inadequate and seemingly weak response to breaches can negatively impact a company's perceived value and potentially its share price. This information rarely trickles down to operational teams. There is a task here for all security professionals to communicate "fact-based data" upstream and downstream. The Executive Master's program in Cybersecurity at Antwerp Management School focuses on many aspects, such as Cybereconomics and decision-making, Security in distributed environments, API security, Leadership, Data Security, Incident Response, and HR.

---

[13] Lee, M. (2019) ISACA Journal; Stop Looking for the Purple Squirrel: What's Wrong With Today's Cybersecurity Hiring Practice.

About the authors

- Prof. Yuri Bobbert is Academic Director for Antwerp Management School's Executive Master's program in IT and Cybersecurity.
- Vincent van Dijk, MSc is the Founder of Security Scientist and a researcher at Antwerp Management School.

Sources Used

[1] Ponemon, "Cost of Data Breach Study: Global Analysis," Ponemon Institute LLC, United States, 2016.

[2] WhiteHouse, "Executive Order on Improving the Nation's Cybersecurity," https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, Washington, United States, 2021.

[3] Y. O. N. Bobbert, "LockChain technology as one source of truth for Cyber, Information Security and Privacy," in *Computing Conference*, London, 2020.

[4] Y. Bobbert and M. Butterhoff, Leading Digital Security; 12 ways to combat the silent enemy, Utrecht: https://12ways.net/blogs/emerging-roles-in-digital-security/, 2020.

[5] AFCEA, "The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment," *AFCEA CYber Committee,* 2013.

[6] MITRE, "Attack Groups," 2021. [Online]. Available: https://attack.mitre.org/groups/.

[7] AIVD, "AIVD Annual Report 2020," 2022. [Online]. Available: https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2021/06/04/aivd-annual-report-2020/AIVD+Annual+Report+2020.pdf.

[8] AIVD, "Cyberaanvallen door statelijke actoren," Ministerie van Defensie Militaire Inlichtingen- en Veiligheidsdienst, The Hague, 2021.

[9] AIVD, "Publication AIVD and MIVD 'Cyberespionage: are you aware of the risks?' A joint publication by the AIVD and MIVD on the threat of cyberespionage for businesses and agencies.," Ministry of the Interior and Kingdom Relations of the Netherlands General Intelligence and Security Service (AIVD), The Hague, 2017.

[10] BakerMcKenzie, "The rising importance of safeguarding trade secrets," 2017. [Online]. Available: https://www.bakermckenzie.com/-/media/files/insight/publications/2017/trade-secrets.

[11] T. Kumar, What is the impact of distributed agile softWare development on team performance?, Antwerp: Antwerp Management School, 2020.

[12] Y. Bobbert, M. Chtepen, T. Kumar, Y. Vanderbeken and D. Verslegers, Strategic Approaches to Digital Platform Security Assurance, Hershey, PA: IGI Global, 2021.

[13] E. Botjes, "Defining Antifragility and the Application on Organization Design," Antwerop Management School (AMS) - https://zenodo.org/record/3719389/files/Master_Thesis_Antifragile_Edzo_Botjes_202005014_v1.0.pdf?download=1-, Antwerp, 2020.

[14] Y. Bobbert, Improving The Maturity of Business Information Security; On the Design and Engineering of a Business Information Security Artefact, Nijmegen: Radboud University, 2018.

[15] J. Kuijper, "Effective Privacy Governance-management reserach_A view on GDPR ambiguity, non-compliancy risks and effectiveness of ISO 27701:2019 as Privacy Management System," Antwerp Management School, Antwerp, 2020.

[16] J. Pfeffer and R. Sutton, "The Knowing-Doing Gap: How Smart Companies Turn Knowledge into Action," no. Harvard Business School Press, 2001.