Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215976

Cybersecurity in Games

Cezary BELLA
Warsaw University of Technology
ORCID: 0000-0003-4355-1921
E-mail: cezary.bella@pw.edu.pl

Abstract

The gaming industry has become one of the fastest growing and most exciting parts of the digital world, mixing entertainment, social interaction, and real economies. However, this quick development also made gaming a major and popular target for cybercriminals. Modern games depend on cloud infrastructure, cross-platform systems, and virtual markets, which significantly increase their exposure to cybersecurity risks.

This article examines the key cybersecurity challenges that affect both players and game developers. It discusses threats like account theft, phishing, malware hidden in game modifications, ransomware, and large-scale data breaches. Several well-known cases demonstrate how social engineering, poor access management, and weaknesses in supply chain can compromise even biggest studios.

For players, the incidents often lead to privacy violation, loss of personal data, or fraud including virtual goods. For developers, the risk includes stolen source code, server attacks, and not meeting international data protection requirements.

As new technologies like artificial intelligence, blockchain, and metaverse become more common in gaming, security must be treated as an essential part of the design, operations and business strategy, rather than a secondary technical detail. Increasing resilience, promoting awareness, and respecting privacy principles are crucial to ensure a safe and sustainable future for digital gaming.

Keywords

gaming industry, game development, cybersecurity

Introduction

The gaming industry has been highly evolving for the past couple of years. Becoming one of the world's most valuable entertainment industries, worth over $200 billion annually[1], with more than 3 billion active players, serving social interactions and online economies worldwide.

Modern video games are no longer simple, standalone pieces of software - they have evolved into complex, online-driven ecosystems[2]. This high level of

[1] ZipDo Education, Global gaming industry statistics: Reports 2025. https://zipdo.co/global-gaming-industry-statistics/. [access: 25.10.2025].

[2] E. Goh, O. Al-Tabbaa, Z. Khan, Unravelling the complexity of the Video Game Industry: An integrative framework and future research directions, Telematics and Informatics Reports 2023, https://doi.org/10.1016/j.teler.2023.100100.

interconnection and sophistication has turned the gaming industry into an attractive target for cybercriminals, scammers, and hacktivists, who use various types of cyberattacks against both game developers and players. The main reasons include the massive user base, which often holds valuable personal and financial data, as well as the always-online nature of most games, which greatly expands the potential attack surface.

In addition, virtual assets now carry real-world monetary value and are strongly tied to players' emotions. Because of the significant financial and emotional investment in these digital worlds, players often react impulsively when they feel their assets are at risk - a behaviour that attackers frequently exploit.

In this article, we discuss potential vulnerabilities within the industry, recent data breaches, risks for both players and game developers, as well as simple prevention mechanisms and future of gaming in terms of cybersecurity.

Cybersecurity Threats for Developers

There are many layers on which game development studios might become affected by cybersecurity issues. In this chapter we are going to discuss some of potential risks that developers may face.

One of the common attacks are Distributed Denial of Service (DDoS) attacks targeting game servers to disrupt gameplay for players or extort companies. Very often e-sport events and new online games launches are target with DDoS attacks[3]. There are several mitigation strategies that companies may use, and these are using load balancing solutions, Content Delivery Networks (CDNs) or advanced anti-DDoS services, but none of it guarantee full protection against cyberattacks.

Another example may be privacy invasion of player's data. Meaning gaming studios that collect vast ranges of data - behaviour analytics, voice chat, geolocations, different types of events - may go under attack and leak not only their production data and documentation, but also gamers private information stored on their databases. This challenge is further being complicated by new data protection policies, like General Data Protection Regulation (GDPR)[4] or California Consumer Privacy Act (CCPA)[5], imposing strict obligations on data protection. Failure to secure players data can lead to major fines and significant damage to a company's reputation.

We already mentioned production data and documentation leaks. Hackers, while targeting gaming studios, often aim to affect (leak, steal, encrypt) games source code and assets. In next chapter we are going to discuss several such incidents from past couple of years.

Another threat for developers is cheat development that often uses reverse engineering in order to analyse game binaries to create cheats and exploits.

[3] Security Magazine, 49% of DDoS attacks targeted gaming organizations. Security Magazine. https://www.securitymagazine.com/articles/100943-49-of-ddos-attacks-targeted-gaming-organizations [access: 29.10.2025].

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 [access: 28.10.2025].

[5] California Consumer Privacy Act of 2018, California Civil Code §§ 1798.100–1798.199. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article= [access: 28.10.2025].

Using such software may break game for other players and affect in-game markets.

Attackers may not only target gaming studios themselves, but may aim at third-party software that developers use and integrate into their games. Exploiting Software Development Kits (SDKs), various plugins, modifications, or even Continuous Integration / Continuous Delivery (CI/CD) tooling may be sufficient to gain significant access to the ecosystem or critical data (both payers' and developers'). Games using insecure Application Programming Interfaces (APIs) or cloud services for matchmaking or in general online gaming, leaderboards, or in-game purchases may also be targeted.

While talking about different types of threats, we can not forget about human weaknesses. People can be bribed, phished, coerced into leaking data or even just talk about certain things without knowledge about their secrecy. We are talking about employees, but also outsource companies, media or third-party contributors.

Peaking into the future we might also see some potential risks rising on the horizon. Increasing interest in artificial intelligence opens up huge danger in AI-generated phishing campaigns, deepfake videos of famous people or even auto-aim bots becoming more and more sophisticated and second to impossible to detect.

The rising interest in cross-platform gaming - where players on different devices such as personal computers, consoles and mobile devices can interact within the same online environment - has significantly expanded the potential attack surface for cybercriminals. Each platform operates on distinct architectures, operating systems, and security models, which introduces additional layers of complexity for developers trying to maintain consistent protection across all endpoints. Attackers can exploit inconsistencies in authentication systems and vulnerabilities within APIs, or weak integration layers between platforms to gain unauthorized access to player accounts or even servers.

Another example might be augmented reality that is slowly rising throughout years, but we can clearly see more movement in recent years. More companies are investing money in creating better and more reliable headsets. These devices can collect lots of crucial data about the user, we are talking biometrics, like facial geometries and iris scans, motion and even behavioural data. Often geolocation data and scanned surroundings are also stored by the manufacturer[6]. If these data become intercepted it might be misused by hackers.

In the next chapter, some examples of how cybersecurity became a real issue for several studios are depicted.

Case study: Threats for Gaming Companies

During recent years, the gaming industry has reported several major data breaches aimed at big international gaming companies. In this chapter we will discuss some of these incidents, providing analysis of what has happened, when possible - not every studio shared results of their investigation.

In 2022 Rockstar Games felt victim to social engineering cyberattack, in result of which their new upcoming game Grand Theft Auto VI source code and

[6] K. Reyes, VR Data Ranking: What Your Headset Company Knows About You. https://vpnmentor.com/blog/research/vr-data-collection-research/ [access: 28.10.2025].

assets leaked into the internet[7]. Moreover, over 90 videos of in-development gameplay, developer documentation and internal tooling have been stolen. From the statement that Rockstar Games released after the incident, we know that the attacker used social engineering to trick one of their employees into providing them credentials or granting remote access via Slack. Besides the reputation damage and loss of secrecy around their flagship title, Rockstar also suffered loss of trust from their investors group, having to reassure them that the timeline for the project has not been affected by this incident.

Another example that involves a big studio would be the CD Projekt RED, studio known for The Witcher series and Cyberpunk 2077 games[8]. In 2021 shortly after the release of Cyberpunk 2077 studio suffered from a ransomware attack, resulting in source code of The Witcher 3 and Cyberpunk 2077 being released to the public[9]. Additionally, studio's servers got encrypted and lots of employees data has been stolen. The attackers infiltrated CD Projekt's network, most probably through compromised credentials or a phishing campaign. They were able to deploy ransomware software that both encrypted and exfiltrated data. CD Projekt was requested to pay the ransom, which they did not, resulting in stolen source code being later auctioned on dark web markets.

Also in 2021 Electronic Arts, studio behind multiple well-known titles, like FIFA, The Sims or Battlefield series, suffered from source code theft[10]. Event resulting in approximately 780 GBs of internal data being stolen, that included source code and development tools for FIFA games and Frostbite engine. Attackers impersonated a technical support agent in order to trick an employee via Slack, trying to steal session tokens. After succeeding this operation they gained access to internal servers. Player's data has not been affected, but intruders tried to sell stolen source code online using dark web markets.

This time around, in 2020 Ubisoft was targeted by a ransomware group, claiming that approximately of 580 GBs of Watch Dogs: Legion was stolen[11]. Moreover, development documents and infrastructure details have been

[7] N. Balu, Take-Two confirms GTA VI leak, says game development unaffected, Euronews 2022, https://www.euronews.com/next/2022/09/19/grandtheftauto-cyber-take-two. [access: 21.10.2025].

[8] S. Shah, CD Projekt Red says internal data from ransomware breach is being spread online. Engadget 2021, https://www.engadget.com/cd-projekt-red-data-breach-online-114047285.html. [access: 26.10.2025]; D. Goodin, CD Projekt Red does an about-face, says ransomware crooks are leaking data, “Ars Technica” 2021, https://arstechnica.com/gadgets/2021/06/cd-projekt-red-says-its-data-is-likely-circulating-online-after-ransom-attack/ [access: 26.10.2025]; M. Kraus. Cyberpunk 2077 game developer hit with cyber-attack, CNBC 2021, https://www.cnbc.com/2021/02/09/cyberpunk-2077-game-developer-cd-projekt-red-hit-with-cyber-attack.html. [access: 27.10.2025]; L.H. Newman, Cyberpunk 2077 Maker Was Hit With a Ransomware Attack and Won't Pay Up, Wired, SECURITY 2021, https://www.wired.com/story/cd-projekt-red-ransomware-hack-cyberpunk-2077-source-code/ [access: 27.10.2025]; C. Criddle, Cyberpunk 2077 makers CD Projekt hit by ransomware hack, BBC, “Gaming, cyber security” 2021, https://www.bbc.com/news/technology-55994787 [access: 28.10.2025].

[9] T. McNulty, Cyberpunk 2077, Witcher 3 Source Code & More Stolen Data Appears Online. ScreenRant 2021, https://screenrant.com/cyberpunk-2077-witcher-3-source-code-stolen-data/ [access: 16.10.2025].

[10] B. Fung, Hackers breach Electronic Arts, stealing game source code and tools, “CNN Business” 2021 https://edition.cnn.com/2021/06/10/tech/electronic-arts-hack/index.html [access: 23.10.2025]; B. Ashcraft. Report: Hackers steal FIFA 21 and Frostbite source code from EA, Kotaku 2021, https://kotaku.com/report-hackers-steal-fifa-21-and-frostbite-source-code-1847072725. [access: 25.10.2025].

[11] S. Singh, Watch Dogs: Legion has reportedly been hacked, source code leaked, NME 2020, https://www.nme.com/news/gaming-news/watch-dogs-legion-has-reportedly-been-hacked-source-code-leaked-2808756 [access: 26.10.2025].

exposed. Attackers infiltrated Ubisoft's network and exfiltrated data before deploying ransomware. The setback to Ubisoft's intellectual property was visible. Possibly some engine level vulnerabilities were also exposed, allowing for future attacks.

Another example is Axie Infinity, which represents different genre within gaming industry[12]. They have created a play-to-earn game that suffered massive cryptocurrency theft from blockchain bridge in 2022. Resulting in approximately $620 million USD in Ethereum being stolen, which stands for largest crypto-related gaming hack to date. Attackers compromised private validator keys used to approve transactions on the bridge. They gained access to only five (out of nine) validators, but that was enough to approve fraudulent withdrawals. Company reported severe financial losses for players and developer. The in-game economy has collapsed and the game itself was temporarily unavailable.

In 2023 Riot Games has become a cyberattack target, causing several games and internal tooling source code being stolen[13,14]. It began with massive DDoS attack and was followed by a data breach that resulted in personal data of millions of players being leaked. Since attackers also gained access to internal system, they had to be rebuilt. This example shows how DDoS may disrupt well-known and already established gaming studio functionality.

Another example of DDoS might be the Activision Blizzard case from 2021[15]. The attack has exploited vulnerabilities in company's server infrastructure. Despite the fact that the studio has not disclosed financial losses, the disruption to online availability of their services likely resulted in temporary revenue loss, inquiring additional costs for mitigating future attacks.

Year 2020 was not perfect for Cupcom as well, developer behind titles like Resident Evil series[16]. Hackers stole over 1 TBs of data, including employee information, unreleased game details and personal data of around 400 thousands users.

Final example would be Zynga, a mobile gaming representative, that in 2019 fall under a similar attack from hackers[17]. The attack affected over 170 million players worldwide. Leaked data included usernames, emails and salted passwords. That was one of the largest breaches in mobile gaming history, that proves that even casual games may face enterprise-level threats.

---

[12] Security Affairs, Attackers stole $625 million worth of cryptocurrency from Axie Infinity. https://securityaffairs.com/129609/cyber-crime/625m-axie-infinity-ronin-hack.html. [access: 23. 10.2025].

[13] Riot Games, DDoS Prevention Guide, https://support-leagueoflegends.riotgames.com/hc/en-us/articles/201751764-DDoS-Prevention-Guide [access: 28.10.2025].

[14] A.R. Heaton, The Riot Games Cyber Attack of 2023: What Happened and How to Protect Yourself, Medium 2023, https://medium.com/@heaton.adam79/the-riot-games-cyber-attack-of-2023-what-happened-and-how-to-protect-yourself-b48c6398c445. [access: 24.10.2025].

[15] D. Antoniuk, Activision Blizzard games crippled by hours-long DDoS attack, The Record 2023, https://therecord.media/activision-blizzard-crippled-by-ddos [access: 27.10.2025].

[16] TechCrunch, Capcom hit by ransomware attack after hackers steal confidential data, https://techcrunch.com/2020/11/16/capcom-resident-evil-game-maker-breach-ransomware/ [access: 25.10.2025].

[17] Security Affairs, Zynga data breach impacts more than 170 million accounts. SecurityAffairs.com., https://securityaffairs.com/95696/data-breach/zynga-data-breach.html. [access: 28.10.2025].

Cybersecurity Threats for Players

Cybersecurity issues are not only a problem for developers. More and more hackers are into stealing personal data from players directly.

First and foremost issue that we should highlight is account theft and credentials stuffing[18]. Attackers often steal credentials directly from players or buy them from leaked data breaches, using them to gain access to gaming accounts on various platforms - both intermediate services that provides games and direct access to accounts on game developers servers. Such behaviour may cause major damage, that allows attackers to steal in-game assets or currencies. Moreover, personal data and payment details may also be affected providing attackers to gain even more from stolen data.

Attackers often use social engineering techniques or phishing using fake websites, communicators scams or different, also in-game communication channels to trick users into revealing their credentials directly or by visiting malicious links. Latest example includes the account with the most trophies begin stolen, despite having multi-factor authentication enabled. Hackers used social engineering techniques to manipulate platform technical support personnel[19]. Additionally, malware or cheat software can often be utilized in the similar manner, players downloading game modifications or cheat engines to enhance their gaming experience often download malicious software like key loggers or cryptocurrencies miners[20]. Software like these are often written in a way that obfuscates antivirus, making it almost impossible to detect by players.

Having said that, we not only talk about stealing personal data and credentials, but also potential system compromises and hijacking computing resources[21,22].

Another growing concern from a cybersecurity perspective is in-game market manipulation, there attackers - often in form of organized groups - exploit virtual economies for unfair or illegal financial gains. Modern games feature complex trading systems, virtual currencies and digital assets that can often be exchanged for real money. This creates an environment that attracts not only ordinary scammers, but also market manipulation mafias who specialize in controlling virtual economies. Such manipulation can take many forms, some use automated bots to buy and resell in-game items creating artificial demand inflating process. Others exploit software vulnerabilities or loophole to duplicate items or generate in-game currency without authorization.

---

[18] Kaspersky, 1 million gaming accounts leaked in 2024, report finds. Technobaboy. https://www.technobaboy.com/2025/08/14/11-million-gaming-accounts-leaked-in-2024-report-finds [access: 21.10.2025].

[19] A. Corsetti, PlayStation Network security slammed after support leaks trophy hunter's account to hacker, https://www.notebookcheck.net/PlayStation-Network-security-slammed-after-support-leaks-trophy-hunter-s-account-to-hacker.1137714.0.html [access: 22.10.2025].

[20] Activision Blizzard, Activision investigates password-stealing malware targeting gamers. TechCrunch, https://techcrunch.com/2024/03/28/activision-says-its-investigating-password-stealing-malware-targeting-game-players/ [access: 22.10.2025].

[21] CyberMagazine, How hackers secretly mine cryptocurrency by infecting pirated games. https://cybermagazine.com/network-security/how-hackers-are-secretly-mining-crypto-infecting-games [access: 25.10.2025].

[22] Vice, Fortnite cheat program found to contain hidden cryptocurrency miner, https://www.vice.com/en/article/fortnite-cheat-crypto-miner [access: 28.10.2025].

Prevention

As the gaming industry continues to expand, the importance of cybersecurity strategies has never been higher. Both developers and players are responsible for ensuring that games remain safe and trustworthy digital environments. While methods and tools differ the goal remains the same - to build resilience against increasingly sophisticated cyber threats.

From developer's perspective prevention begins at the design stage, while integrating a secure development lifecycle (SDLC) that ensures that potential vulnerabilities are identified and resolved before a game releases. Moreover, regular code audits, penetration testing and threat modelling should be employed to anticipate exploitation attempts. In addition, cybersecurity trainings should become a standard within gaming companies, building the awareness and teaching about emerging threats and social engineering tactics.

Equally important is the players data protection, where strong encryption and secure cloud architecture are key to success. Sensitive player information should be encrypted following up-to-date security standards.

Additionally, for multiplayer titles the development of anti-cheat and anti-bot systems can help identify suspicious behaviours that might indicate automation or market manipulation of any sort.

Beyond technical measures, being prepared and building awareness remain key defensive pillars. Developers should maintain structured incident response plans, enabling quick reaction when breaches occur.

Developers are not the only ones responsible here, players too play an essential role in the fight against cybercrimes. The most effective personal defence still begins with basic digital hygiene - strong and unique passwords, using multi-factor authentication and scepticism toward messages or suspicious links - verifying information on official communication channels is always advised. Since phishing and social engineering remain the most common entry points for attackers, awareness and caution are invaluable tools.

Summary

The cybersecurity in gaming industry is no longer a niche in IT concern, it has become integral business continuity, player trust and brad reputation. A single breach can now lead not only to financial loss but also to long-term damage to a studio's credibility and player loyalty. As games merge with artificial intelligence, blockchain and metaverse technologies the attack surface will continue to expand. Development studios should invest in cyber resilience rather than just prevention. Transparency with players about security practices and data breaches should become a standard. Furthermore, the complexity of modern cyber threats require collaboration across different platforms, companies and government. Shared threat intelligence, standardized security and partnership can help the gaming sector to respond to large-scale attacks more effectively.

Literature

Wijayasekara K., From Pixels to Protection: A Comprehensive Review of Cybersecurity in the Gaming Industry, DOI:10.13140/RG.2.2.22959.14248.

SCB Economic Intelligence Center. (n.d.). Gaming industry. https://uploads4.craft.co/uploads/operating_source/document/1097912/6c293d7bc1b660f7.pdf.

Accenture, Global gaming industry value now exceeds $300 billion, new Accenture report finds. Accenture Newsroom. https://newsroom.accenture.com/news/2021/global-gaming-industry-value-now-exceeds-300-billion-new-accenture-report-finds.

Bridgwater A., The impact of cyberattacks on corporate reputation, “Strategic Direction” 2018, vol. 34, no. 2.

Huang J.H., Li D., Ye C., Cheng Z.H., Zhang Y., Understanding in-game virtual item purchase behavior: A study of gaming motivations, payment preferences, and purchase intentions, “Computers in Human Behavior” 2020, vol. 104.

Eset, 11 massive video game companies recently targeted by cybercriminals. https://www.eset.com/uk/about/newsroom/blog/11-massive-video-game-companies-recently-targeted-by-cybercriminals/.

Szatmáry K.S., Cybersecurity of the Gaming Industry. IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY), Pula Croatia 2024, doi: 10.1109/SISY62279.2024.10737510.

Ibrahim A., Guarding the Future of Gaming: The Imperative of Cybersecurity. 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates 2024, doi: 10.1109/ICCR61006.2024.10532843.

Sharma K., Mukhopadhyay A., Cyber-risk Management Framework for Online Gaming Firms: an Artificial Neural Network Approach, Inf Syst Front 25. https://doi.org/10.1007/s10796-021-10232-7.

Genezi Research, Exploiting virtual economies: A historical analysis. https://research.genezi.io/p/exploiting-virtual-economies-a-historical.

Nardone M., Cybersecurity threats and attacks in the gaming industry: Secure game players’ and developers’ data and systems, “Apress Pocket Guides” 2025, https://doi.org/10.1007/979-8-8688-1492-1.