Game on: the need for Cybersecurity in gaming

The gaming industry has evolved in leaps and bounds from the time of arcade games to the mega multiplayer games such as Fortnite, FIFA 17, Call of Duty, GT Sport, Metal Gear Solid, and PUBG. From video games to online gaming, gaming platforms have evolved a lot to offer browser and app-based games on Windows, macOS, Android, iOS, various gaming consoles such as Xbox, PlayStation etc., and casinos. The industry has grown tremendously and there is serious money involved. In fact, gaming industry revenues are predicted to touch 180.1 Bn by 2021[i]. Gaming has created such a craze that media giants such as Netflix consider Fortnite to be a bigger competitor than HBO[ii]! A valid concern with billions of people across demographics engaged in gaming globally.

It is no surprise that such a lucrative industry has caught the eye of cyber criminals. Predictably, the gaming industry has been plagued by cyberattacks with hackers carrying out 12 billion attacks in just 17 months[iii] according to an Akamai report!

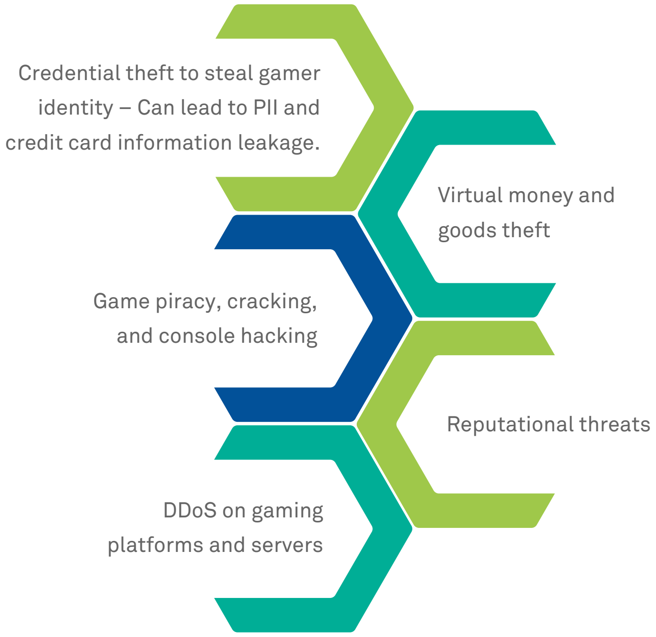
"The online gaming community will be an emerging hacker surface, with cybercriminals posing as gamers and gaining access to the computers and personal data of trusting players."
---- 2019 Experian Data breach industry forecast

The stakes are high

The gaming industry is sitting on a hotbed of coveted data – vast amounts of instances of personally identifiable information (PII) and credit card information of gamers worldwide. It's the responsibility of the industry to protect this information and ensure that their platforms are a safe environment for gamers.

As evidenced from other industries such as banking and retail, the impact of a customer data breach can be far-reaching. Other than making gamers vulnerable via disclosure of sensitive personal data, gaming companies themselves are at risk of financial and reputational damage. Regulations around privacy and personal data protection are also becoming increasingly stringent to protect gaming companies, gamers, financial institutions and taxpayers. For instance, the gaming industry is required to comply with the global Payment Card Industry Data Security Standard (PCI DSS) that requires that gamers' credit card details are kept secure. The GDPR (General Data Protection Regulation) gives supervisory authorities the power to fine non-compliant organizations €20 million or 4% of global annual turnover, whichever is greater. Various local regulations also require that gaming transactions can be audited.

Top Cyber Threats in Gaming


Credential theft to steal gamer identity – Can lead to PII and credit card information leakage.
Virtual money and goods theft
Game piracy, cracking, and console hacking
Reputational threats
DDoS on gaming platforms and servers

However, the most significant impact of a breach is on customer trust. Gamers often spend a lot of time and money to build their online identity, making it a valuable asset that must be protected. Even if a game does not pay out real money, virtual assets in multi-player online games can often be sold for hard cash. Heavy users and high rollers increasingly expect gaming companies to protect their identities and therefore their assets. A breach of this trust can cause irreparable damage to customer loyalty.

The answer to a secure and trustworthy system lies in a strong cybersecurity approach.

Protecting the turf with Cybersecurity controls

Recent checks have discovered several vulnerabilities in large gaming platforms that leave user data vulnerable. According to the ThreatMetrix Gaming and Gambling Cybercrime Report, approximately 5% of new accounts created on online gaming sites are connected to a fraudster[iv]. And hackers are coming up with new strategies! In a creative hack of a popular game, young players were being taught to hack others' accounts to collect rare and valuable skins[v] – a breach that has led to a class-action lawsuit against the gaming company[vi].

In a world where cybercriminals are getting bolder (think a billion data records released on the dark web by a hacker[vii]), it's imperative that gaming companies invest in and make use of the right security controls. The industry should adopt cybersecurity in the entire lifecycle of game development and deployment along with the platforms on which these are used.

High-level guidelines to achieve better security assurance:

- Enable multi factor authentication to protect against identity theft
- Comply with PCI DSS and institute safe online payments to protect financial information
- Ensure confidentiality of databases to protect sensitive information from being disclosed to unauthorized parties
- Put a stop to back date frauds
- Ensure protection against DoS and DDoS attacks that disrupt gamer experience by breaking connectivity
- Ensure that security is embedded in the entire lifecycle of game development, release campaigns, marketing etc.
- Protect against in-game phishing that usually happens via the messaging feature within the games

Wipro has been working with several gaming clients to build and strengthen cybersecurity. With our vast experience in various verticals that have higher risk potential and our best-in-class security offerings, we can partner to provide higher cybersecurity assurance to gaming companies. Our Cybersecurity and Risk Services (CRS) practice helps customers define their cybersecurity strategy and needs, incorporating best-recommended practices across the people, process, and technology platforms.

A safe space

At the end of the day, people indulge in gaming for entertainment. If it becomes a threat to their financial and reputational well-being, they will shy away from it and seek other safer modes of entertainment. To prevent such a scenario, the gaming industry needs to bake cybersecurity into the software, hardware, and networks, with stronger authentications and other security controls to make it tougher for attackers to take over. Finally, a large number of gamers are young players with limited understanding of security practices. It's a moral responsibility of the industry to provide them with a trusted community to play in.

What is your experience with security in the gaming industry? How do you see industry players adopting cybersecurity practices?

About the authors

Harshwardhan Kamdi
Practice Partner in Cybersecurity
& Risk Services (CRS)

Harshwardhan is Practice Partner in the Cybersecurity & Risk Services (CRS) team and leads the CRS focus on the TECH Business Unit of Wipro. He is a cybersecurity professional with over 16 years of experience. He has played various roles across multiple domains of cybersecurity, spanning consulting, delivery, system integration, advisor and practice development by strategizing, leading, and implementing cybersecurity initiatives in organizations across the globe. He has worked and managed projects relating to Secure SDLC, threat modelling, secure coding, and penetration testing, and has advised on security best practices for global clients in technology, banking and financial services and manufacturing sector. He is an active participant and speaker in many forums and conferences on cybersecurity and is a qualified Offensive Security Certified Professional (OSCP). He can be reached at **Harshwardhan.kamdi@wipro.com**

References

[i] https://venturebeat.com/2018/04/30/newzoo-global-games-expected-to-hit-180-1-billion-in-revenues-2021/

[ii] https://techcrunch.com/2019/01/18/netflix-thinks-fortnite-is-a-bigger-threat-than-hbo/

[iii] https://venturebeat.com/2019/06/12/akamai-hackers-have-carried-out-12-billion-attacks-against-gaming-web-sites-in-17-months/

[iv] https://chargebacks911.com/online-gaming-fraud/

[v] https://www.greenmangaming.com/newsroom/2018/12/21/pressure-grows-on-epic-to-address-fortnite-account-hacking/

[vi] https://www.greenmangaming.com/newsroom/2019/08/13/fortnite-data-breach-lands-epic-games-with-class-action/

[vii] https://www.cybersecurity-review.com/news-april-2019/a-hacker-has-dumped-nearly-one-billion-user-records-over-the-past-two-months/

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035, India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**