CYE

When it Comes to Cybersecurity, There's No Time For Games.

The gaming industry:
A giant playground for cybercrime

Over the past decade, online gaming has exploded, with more and more people choosing it as one of their primary ways to unwind and escape. In fact, online gaming generated $159.3 billion in revenue in 2020, a 9.3 percent year-over-year growth, and is expected to surpass $200 billion in revenue by 2023.

The world's 2.7 billion gamers will spend $159.3 billion on games in 2020; the market will surpass $200 billion by 2023

Newzoo

Today, there is unprecedented excitement and competition in the world of online gaming. Younger generations are typically avid and, at times, fanatic players.

Like other industries upon which hackers have set their sights, the online gaming industry is rife with data, which has rightfully been coined "the oil of the 21st century."

COVID-19: less work, more games (and more threats)

While most businesses suffered tremendously as a result of COVID-19, the gaming industry actually propelled forward, with people being confined to their homes and seeking distractions.

In fact, the gaming industry has been a prime cybercrime target since the beginning of the pandemic, with gaming and IT platforms **experiencing a 39% increase in attacks since early 2020.**

It has become clear that only gaming companies with strong cybersecurity postures will be able to thrive in spite of - and after - the pandemic.

Gaming by the Numbers

2.2 billion active mobile gamers globally

40% of smartphone use is due to gaming

62% of people install a game on their phone within a week of owning it

78% of gamers are Android users

58% of the games played are puzzle games

21% of Android and 25% of iOS apps downloaded are games

Data: the oil of the 21st century

With the constant influx of data, global hackers are exploiting the gaming industry to collect social security numbers, credit card information and passwords, which they then sell on the dark web and hold for ransom. In fact, according to IBM, 90% of all data has been created in the last two years.

Gaming app monetization offers users the ability to pay for in-app purchases, subscriptions, advertising and sponsorships. The gamers demographics is known for spending money on in-game commodities, from cosmetic enhancements to gambling. This has ensured the rapid and continuous profitability of the mobile gaming industry, making it one of the most lucrative targets for hackers to turn a quick profit.

How do cyber attacks really happen?

The majority of hacking attacks are not all that sophisticated. They are viral and take advantage of naive players who are all too eager to get free games and seize the opportunity to win big.

In fact, the eagerness of both parties is at fault. On the one hand, companies launch apps as soon as possible (often with glaring vulnerabilities) to please their fans and create new streams of revenue. While on the other hand, eager fans wait endlessly and oftentimes spend countless hours scouring the internet for new games, as they get scammed and hacked across the web.

This makes both young gamers and older gamers (though less so) very prone to phishing attacks and clicking on malicious links that download malware or ask for login credentials.

However, the methods of attacks vary in size and complexity. For example,
SQL injections enable hackers to use online forms to inject SQL codes into databases lying behind forms, gaining access to billions of accounts, without having to obtain credentials.

90% of all data has been created in the last two years

Additionally, local file inclusions enable hackers to use web applications in order to gain access to private files stored on a company's server. Cyber criminals target web-based and mobile-based games with both SQL injections and local file inclusions, enabling them to capture user names, account information and passwords.

Drive-by downloads

Drive-by downloads infect even the most savvy gamer, as they can be executed without a single click or download, leaving malicious code on the user's computer. Victims get infected even if they never stop to click, adding even more complexity to an already perplexing cyber gaming landscape. This is often the first stage in a string of damaging malware attacks that can compromise a user's computer.

These attacks leverage vulnerabilities in a gamer's operating system, apps, browser, and plugins, often due to unsuccessful updates.

Game cheats: a gateway to hacking

Just as professional athletes seek ways of gaining a competitive advantage, gamers do the same by using cheats - arguably one of the best tactics for spreading malware on the Internet.

Creating cheats lead to more intense cyber criminal activity, such as selling stolen account credentials of online gaming accounts, hijacking in-game items and gaining access to services, like VPNs. While it may not be a definite path to more serious cyber crime, it certainly holds the possibility.

> " Offenders begin to participate in gaming cheat websites and 'modding' forums and progress to criminal hacking forums without considering consequences. "
>
> The National Crime Agency

Real world attacks

In 2019, Zynga's popular online game, Words With Friends, was hacked, resulting in the information of more than 218 million users being stolen. The information included names, email addresses, login IDs, hashed and salted passwords and phone numbers.

Earlier that year, the same Zynga hacking group (Gnosticplayers) compromised more than 26 million online user accounts on 6 websites and placed the stolen records for sale on Dream Market, the dark-web market of choice for stolen data.

One month prior, the same hacking group published three rounds of stolen accounts for sale on the same marketplace.

In the first wave, the group posted details of over 600 million online accounts hacked from sixteen websites; in the second wave, it posted over 127 million from eight sites; and in the third, posted ninety-two million from eight websites.

Security readiness in highly targeted gaming companies

Protect what matters most

The user base is often the most important asset in gaming and, as a result, gaming companies need a comprehensive assessment that they can use to identify all the routes leading up to -- and blocking -- their most critical assets.

In order to do this, companies need to adopt a hacker's mindset in order to reveal possible attack routes, starting from external reconnaissance and leading to critical assets, thereby enabling enterprises to improve their cybersecurity postures and correct their vulnerabilities.

Words with Friends: data stolen from over 218,000,000 users

Mitigation steps should be prioritized according to business risks, rather than security risks. Instead of relying on an endless list of vulnerabilities, security teams need solutions that provide actionable mitigation plans across the attack surface.

Too many moving parts call for continuous security

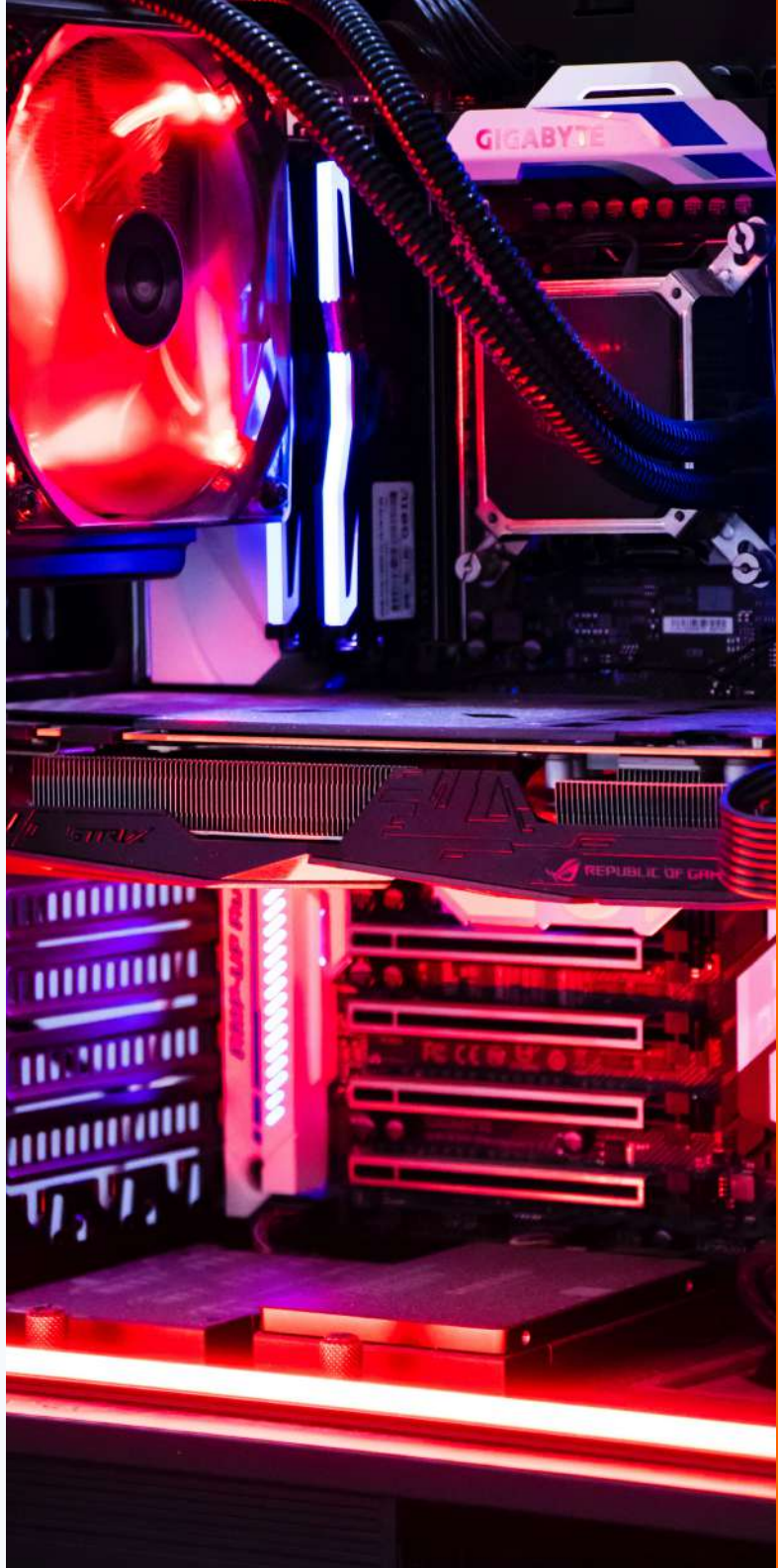
In the gaming world, there are a multitude of users, systems, integrations, payments, and other varieties of moving parts. To ensure the cybersecurity program works as planned, organizations need to test the implementation of these components, which requires continuous security validation.

A truly optimal approach to cyber defense is one that takes a holistic approach, focusing on the real risks to business continuity and optimizing the cybersecurity investment.

By conducting hands-on organizational cybersecurity and risk assessments, businesses can proactively prevent attacks using an actionable, business-savvy mitigation plan.

Have a crisis recovery program

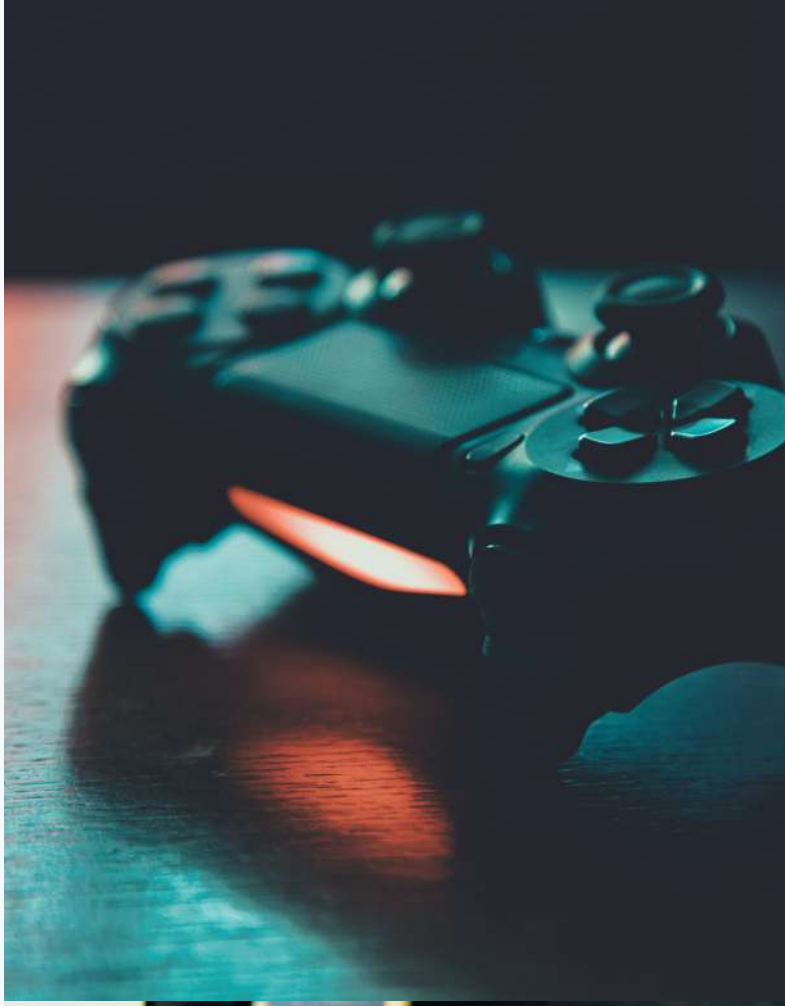
Even when the best-known security measures are implemented to perfection, breaches may still occur. In these cases, time is critical in retrieving business continuity with minimal disruption. Companies must have trusted cybersecurity advisors on their side, ready at a moment's notice. Furthermore, it is crucial to conduct a thorough investigation after the attack in order to learn from past mistakes and prevent such attacks from occurring in the future.

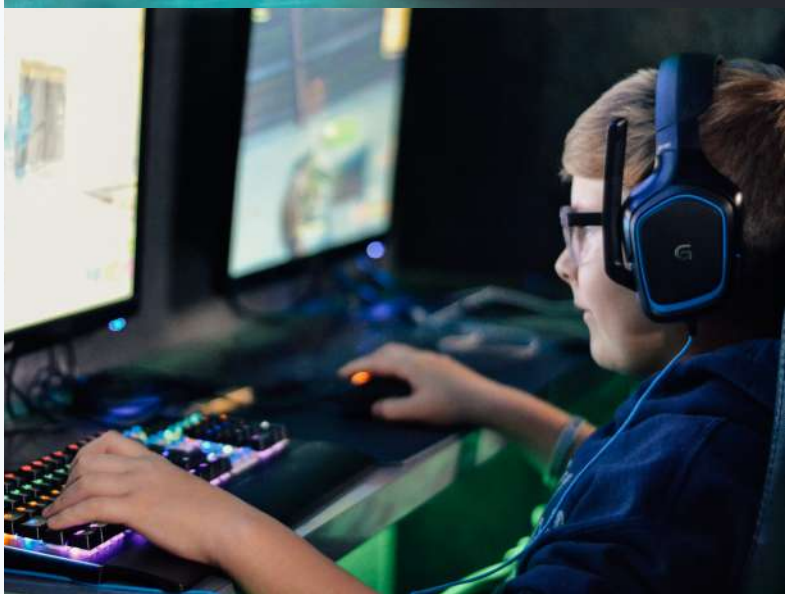


Conclusion and Recommendations

The online gaming industry has become acutely aware of the threats posed by cyber attacks and, as a result, have implemented high security budgets, robust fraud detection, strong IT infrastructures and substantial financial tracking systems. However, despite their significant allocation of resources, their budgets are often not being allocated properly. For example, most online gaming companies are very secure when it comes to their main gates, where users need to input credit card information, but the problem lies when a hacker tries to attack the company from the inside, as their internal infrustructures are often poorly protected. As a result, while their budgets may be high, their overall cyber resilience is quite low.

We have seen time and time again that organizations are not allocating their resources properly, understanding their own threat landscapes or assessing their cybersecurity postures in a holistic way that takes into account all organizational assets.





CYE is the only cybersecurity company that:

- Provides a comprehensive, end to end cybersecurity solution that includes assessment, risk evaluation, risk correlation and mitigation optimization based on the external threat landscape.

- Unlike other cybersecurity providers, we offer a holistic, multi-layered cybersecurity approach, understanding that every organizational asset is within scope and part of the game. Limiting scope limits understanding and does not provide organizations with the ability to see the overall picture or the holistic view of their cybersecurity vulnerabilities.

  As we have seen time and time again, attackers exploit the weakest links in the chain in order to infiltrate an organization. As a result, we leave no stone unturned and assess all aspects of the organization, including OT, IT, IoT, the cloud and so on.

- Unlike other cybersecurity providers, we do not provide our customers with an endless list of vulnerabilities. Rather, we prioritize our customers' most critical business assets in order to provide them with the most practical, efficient and cost-effective solutions for their businesses.

- We understand that when conducting security assessments, there is no "one-size fits all." Rather, we look at each and every organization in a personalized and tailor-made way, providing our customers with a specific and dedicated platform that is based on their priorities, critical business assets and so on. What is critical for organization A, may be of little or no significance to organization B, and vice versa.

As CISOs of online gaming companies continue to understand the severity of their vulnerabilities by not abiding by basic cyber hygiene, we believe it is essential to take a fact-based and mathematical approach that constantly challenges assumptions. We believe that taking a "back to basics" approach, which focuses on returning organizations to their security foundations, is the most effective way of securing their most critical assets.

About CYE

CYE brings a fact-based approach to organizational cyber defense, managing real business risks and optimizing the cybersecurity investment. CYE serves as a trusted advisor to medium-sized and Fortune 500 companies in multiple industries around the world.

Trusted by

World Economic Forum, Zurich, Francisco Partners, EQT, ALSO, softwareONE, UBS, freepik, Schindler, Investec