In brief | Cyber security in gaming

Protecting what matters most

Online gaming poses an array of risks to the industry—but it also represents the next step in gaming's evolution. With heightened concern over the security of internet based information, how can gaming businesses provide immersive gaming experiences for the player while protecting their own assets and reputation? And how can government, regulators and gaming businesses create information security and governance processes that give confidence that no one is undermining the system?

Gaming businesses and regulators need to take lessons from other industries with high security risks—like finance and banking. To provide a safe gaming environment, you need a strategy that goes beyond what services to offer and how to offer them – one that considers the technologies, processes and governance structures that will ensure players and operators are well protected from online threats.

Connecting the player

The next generation of players are tech-savvy and able to merge in-person and virtual activities more readily than ever before. To be successful in the future, gaming organizations need to understand the lifecycle of their players—who they are, how and when they want to interact, and what security risks they fear when they interact online (e.g. providing financial or credit card information). Gaming business can use this knowledge to create alignment across multiple platforms and to underpin the technology architecture needed to provide a safe and secure gaming environment that enhances player connectivity while reducing risks.

Understanding the risks

As technology continues to evolve and gaming offerings move online, the risks associated with cyber-security will only grow. New innovations, pairing of existing and newer systems, and increasing collaboration across businesses only adds to the complexity of the risk landscape.

To be cyber-secure, gaming businesses need to be on top of emerging technologies and their associated risks. One-off solutions aren't enough. Technologies used in the front and back offices need to be aligned to provide a secure and seamless player experience, in person and virtually. Gaming industry participants can look to other industries, such as banking, to see how risks are identified and managed in an online environment considered constantly under attack.

pwc

In brief | Cyber security in gaming

Protecting what matters most

Protecting data

To protect data, gaming businesses need to understand what the data is, where it's stored, who might want it and how it could be accessed. Putting up a wall around confidential information is no longer a simple or completely secure solution—especially as the gaming industry collaborates more to align offerings with a player-centric model.

Organizations need to look at cyber-security as more than a way to manage regulatory compliance. Instead they should consider implementing a risk-based approach to compliance—one that considers and manages risks across people, processes, distribution and data. This risk-based approach can help an organization integrate risk management activities across functional and service lines and form the basis for providing appropriate training for all employees.

Creating a secure gaming industry

Every gaming business has a role to play in fostering a secure gaming industry—whether offerings are provided in-person or virtually. Governments, regulators and public and private operators need to work together to find solutions that enhance the security and integrity of the industry as a whole so that everyone can benefit.

Collaboration is key for regulators as they work to develop an online strategy that:

- Supports industry growth
- Enhances confidence that governance requirements are being addressed
- Ensures operators have the right people, processes and technologies to reduce risks

When it comes to protecting what's most important, gaming businesses should create a security strategy that aligns activities across all aspects of their organization—people, processes, and technology. A risk-based approach can bring cyber-security issues to front of mind while recognizing that the risk landscape will continue to evolve.

The stages of cyber resilience

Creating an effective cyber resilience structure has three phases:

Envision the right cyber-security strategy that captures the complexity of a multi-platform gaming environment so that you can confidently grow your business and the gaming industry as a whole.

Transform organizational processes and technologies so you can create a seamless, yet safe environment for your players.

Protect what's important to your business by understanding, managing and responding to risks before incidents occur. A single breach can have a significant impact on the reputation of a company and its growth for years.

To start a conversation contact:

Salim Hasham
Partner, Cyber Resilience and Information Security Leader
s.hasham@ca.pwc.com
416 365 8860

Arryn Blumberg
Director, National Gaming Practice
arryn.blumberg@ca.pwc.com
416 687 8014