The Protectors: Meet the Top Security Experts at Scientific Games

Published August 21, 2024

The most successful companies in the world rely on security experts to protect their business and help their customers operate safely.

At Scientific Games, global cybersecurity is led by Chief Administrative & Compliance Officer Steve Richardson, who came to the company in 2018 after 22 years with the U.S. Federal Bureau of Investigation. In 2022, he was appointed to the National Technology Security Coalition's Board of Directors, joining chief information security officers from a broad cross-section of enterprise companies who share security threat information to help improve national cybersecurity standards.

Steve Richardson
Chief Administrative & Compliance Officer
Former FBI cybersecurity expert

Shadd Hauck
VP, Tech Ops Engineering
Omnichannel-focused tech operations leader

Joe Bennett
VP, Instant Game Production
Game security patent creator

Lottery systems expert Shadd Hauck, VP, Tech Ops Engineering, began his 24-year Scientific Games career at the ground level of day-to-day lottery operations and progressed through every operational role. Today, he has a deep understanding of each individual function of lottery systems technology and knows the impact an integrated enterprise system can make. For the past decade, he's seen slow adoption of iLottery, particularly in the U.S. Now, he's leading with digital as the company's newest omnichannel systems pick up momentum with lotteries internationally.

Joe Bennett, VP, Instant Game Production, is well-known to many in the industry for dedicating his 33-year career at Scientific Games to instant game security – highlighted by developing a number of patented solutions that advanced game security. His depth of knowledge has guided lotteries across the globe through game security matters. All told, Bennett has been involved in every aspect of rigorous security for more than 45,000 games produced by Scientific Games.

But the story actually begins 50+ years ago with the company's founders (an engineer and a mathematician) who developed technology to produce the world's first secure instant game. For the first time, no one would ever know if a lottery ticket was a winner until they scratched. So, Scientific Games' foundation was built upon security.

Since then, the company's security experts have continuously pioneered new technologies and processes to keep its systems and games secure. The tools are refined and, in some instances, replaced with new solutions as new security threats develop. All innovated to ensure Scientific Games' operations and the lotteries it serves can adapt and protect the security of their business.

We checked in with all three security leaders to see what they want World Lottery Association members to know first and foremost.

Cybersecurity update from former FBI Exec Steve Richardson

For the good of the global lottery industry, cybersecurity is the most important thing Scientific Games does on a 24/7 basis to keep our customers, employees and company information safe. In the world of cybersecurity, threats from phishing, ransomware, and other sophisticated techniques – are growing rapidly and exponentially for all companies.

In the past 10 years (2013 to 2023) the number of cybersecurity intrusions rose 613% worldwide. In 2023, the average global data breach cost USD$4.45 million.

With a multi-layered security platform in place, we stay on top of it all by gathering global cybersecurity information and using gold-standard tools for protection. These same tools are used by many U.S. federal government agencies to protect their systems from bad

actors. Our advanced tools and highly trained cybersecurity experts – computer scientists and information security analysts – are the best in the lottery industry.

By continuously fine-tuning our information security tools, we can identify, quarantine, and eliminate anomalies in the data traveling through our internal and external systems providing immediate risk mitigation.

When sharing information back and forth with lotteries, Scientific Games uses advanced data encryption standards (AES 256-bit encryption), the same standard used by federal agencies. This allows for sensitive information to be transmitted in a very secure manner.

But every employee of a lottery must remain vigilant. This means lottery leadership should make sure their workforce is educated about cybersecurity not once, but regularly. Background checks on every employee candidate before hiring are crucial. The duties of lottery employees must be segregated. A multi-factor authentication system must be in place. Admin rights must be given only to those employees who need access for critical duties. Lastly, complex passwords must be used across all systems, including employee computers, laptops, tablets, and mobile devices.

This may seem like basics, but surprisingly many companies don't take these simple steps to help secure their systems and information. Not doing so creates huge vulnerabilities and easy ways in for unauthorized users.

Above all, lotteries must be proactive by putting cybersecurity measures in place, so they don't have to be reactive in the event of a bad actor gaining access.

Omnichannel ops pro Shadd Hauck talks security

In the lottery industry, cybersecurity is not only about protecting players' personal and financial data but also ensuring the integrity and fairness of games and drawings. It's imperative for every lottery to establish a comprehensive security framework. This framework should address all aspects of security, from data protection and regulatory compliance to advanced threat detection and incident response. By doing so, the lottery can safeguard its operations and maintain the public's trust.

A comprehensive approach involves regular risk assessments, updated security protocols, and adherence to industry standards like ISO/IEC 27001 and NIST. Protecting players' personal and financial data requires strong encryption, stringent access controls, and compliance with data protection regulations such as the General Data Protection Regulation (GDPR). Continuous system monitoring and a well-defined incident response plan are essential for timely detection and resolution of breaches.

Human error remains a significant risk, so regular training and awareness programs are critical to mitigating phishing and social engineering threats. Additionally, managing third-party vendors to ensure they comply with stringent security standards and conducting regular audits is crucial.

Lotteries must embrace emerging technologies, such as AI for advanced threat detection, and stay updated with regulatory requirements.

With our industry's digital transformation, advanced tools are indispensable. Implementing a Web Application Firewall (WAF) protects against threats like SQL injection and cross-site scripting by filtering HTTP requests. Database Activity Monitoring (DAM) provides real-time oversight of database activities to detect and respond to unauthorized behavior. Ensuring API security through gateways, authentication mechanisms and regular testing prevents data breaches.

Scientific Games also prioritizes Static Application Security Testing (SAST) to identify vulnerabilities early in the development process, and we use encryption and multi-factor authentication to secure transactions and player data. Secure payment processing, ensuring PCI DSS-compliant gateways, protects cardholder data. Regular security audits and our vulnerability management program help us identify and address vulnerabilities.

We emphasize the importance of offensive security practices. Our internal offensive security team conducts regular penetration testing to uncover and remediate potential weaknesses. It's a collaborative effort to ensure our defenses are robust and adaptive to evolving threats.

A proactive and multifaceted approach to cybersecurity, including WAF, DAM, API security, SAST scanning, and a strong emphasis on offensive security practices, is essential for safeguarding lottery operations. As our industry continues to evolve, staying ahead of cyber threats will ensure the integrity and trustworthiness of the entire ecosystem.

Industry vet Joe Bennett explains instant game security

In the player's mind, there has to be trust in the games. Trust that everyone has the chance to win. The core of the instant product security comes from the game data imaged under the scratch-off coatings. There are 15 to 20 layers of Scientific Games security on every ticket we produce. This foundation of security ensures trust in our games.

To begin, we create the game data within Scientific Games' secure production environment. This ensures the data remains encrypted from the point of creation throughout the game's entire imaging process. Our multiple and overlapping custom

systems then ensure that all data is confidential and represents the exact logical specifications of the game.

Moments after tickets are imaged onto paper stock, our systems automatically delete the encrypted game data. Then, a host of custom tools ensure complete security throughout the life of the game. Our patented *SG Keyed Dual Security* system gives lotteries additional control and confidence that the production and management of every ticket is as secure as possible.

Finally, our *SG Real Time Marking* system analyzes the quality metrics of every ticket. Defective tickets are identified by vision systems, sensors and scanners – as well as by experienced press operators – and fed into our *SG Quality Tracking System*.

These systems all work together with high-speed cameras and specialized scanners located on our finishing lines to verify that all tickets meet the game's required physical specifications. Any defective product is removed from the workstream automatically based on data from the *SG Real Time Marking* system.

Combined, these systems form the basis of Scientific Games' continuous security improvement programs and ensure that only secure, high-quality tickets reach the lottery and its retailers – and ultimately, the player.

A tour of any Scientific Games facility or a meeting with Steve Richardson, Shadd Hauck, Joe Bennett or any of the company's security experts leaves no doubt in anyone's mind that security comes first and foremost. It's in Scientific Games' DNA. After all, solving security challenges is where it all began. Five decades later, security is still exactly what 150 government-sponsored lotteries rely upon when doing business with Scientific Games.