
# 5th Annual e-Crime Securing Online Gaming

17th October, 2019, London

## The stakes are getting higher

How online gaming and gambling companies can stay ahead of the hackers

http://akjassociates.com/event/gaming

AKJ Associates

SECURING
ONLINE GAMING

SECURING
ONLINE GAMING

# Gaming 2019: Time for a new approach?

Introduction

Online businesses with high-volume, low value transaction models are extremely sensitive to website disruption. While this applies to many e-Commerce models now, from retail to fast food to taxis, the online gaming and gambling sectors are particularly vulnerable because of their combination of large financial flows and small staff and infrastructure.

DDoS attacks can cost hundreds of thousands of pounds an hour in lost revenues; redirects to fake websites can do the same; identity theft can expose sites to fraud and other liabilities; credit card payments mean PCI DSS compliance headaches; and GDPR data privacy is a significant potential operational risk exposure to firms with so many users.

These firms also face challenges unique to the sector:

Gamblers are risk takers. Gamers frequently develop hacks as cheats to make games easier. Users like these pose their own unusual threats to security, through carelessness or malice, adding to the already significant problems the sector faces.

For example, games spawn communities into which cybercriminals can easily insert themselves to gain access to privileged information. The personalities of gaming customers may make this a bigger problem in this sector than others.

Gamers themselves are getting wiser. A recent survey found that three-quarters of gamers worry about the security of gaming in the future and the average gamer has experienced five cyberattacks. Worryingly, fifty-five percent of them reuse passwords across accounts for online services.

**The 5th Securing Online Gaming will cover these and other key subjects for its audience of professionals tasked with safeguarding digital assets and sensitive data. There will be real-life case studies, strategic talks and technical break-out sessions from security teams behind some of the world's most admired brands, who know, just like you, that security is now more important to business than ever.**

Where market-leading solution providers know they will find buyers

SECURING
ONLINE GAMING

# We deliver a focused selling opportunity

Specific, actionable and relevant information for time-constrained industry professionals

**Securing Online Gaming 2019**

The perfect platform for solution providers to deliver tailored advice to the right audience

## Focus

### Target growth

Each event represents a targeted opportunity to address the needs of a specific community whose need for your solutions and services is growing.

## Leads

### Boost sales

Sponsors can tailor messages to the needs of an audience that shares similar concerns and challenges, looking for solutions now.

## Choice

### Meet commercial aims

We work with sponsors to ensure they meet their commercial aims. We offer a number of sponsorship options, each providing specific benefits.

## Value

### Showcase solutions

Our events provide sponsors with a unique platform to showcase solutions, as well as provide advice on how best to solve delegates' key challenges.

SECURING
ONLINE GAMING

# End-users and security professionals need your help ...

Demonstrate your solutions

## 1 To find solutions that fit their needs

With so many providers, so little concrete information and so few metrics, choosing the right solutions is a real challenge. So how can security professionals choose from the provider ecosystem? **This is your opportunity to showcase yours.**

## 2 To deal with data overload

The biggest threat to most organisations is simply the volume of alerts and threat data. This routinely exceeds the capacity of even large firms' human triage teams. Can automation really help? What about AI and SOAR? **Can your products help?**

## 3 To comply with new regulations

Cyber-security is going mandatory. Voluntary commercial codes are not enough. Regulators want companies to demonstrate true cyber-security as well as basic compliance. **How can you help CISOs with this?**

## 4 To better utilise threat intelligence

Cybersecurity spending should be tailored to the threats and vulnerabilities specific to a particular organization. Smarter threat intelligence allows CISOs to map the threatscape to their specific vulnerabilities and invest appropriately. **Can you help?**

## 5 To spot problems faster

Speed of detection and remediation is the biggest single driver of risk (and loss) reduction in cybersecurity. So how can CISOs improve the speed of their security processes. **What solutions are available and affordable?**

## 6 To outsource what they cannot do in-house

Many organisations cannot afford in-house SOCs or security teams big enough to counter cyber threats effectively. So what can they outsource and does outsourcing really solve the underlying risk problem? **What can you offer?**

SECURING
ONLINE GAMING

# They are looking for solutions around ...

Demonstrate your expertise

**Threat intelligence**

## What are hackers saying about you online?

Understanding your vulnerabilities and how they relate to the latest threats is a critical component of good cybersecurity. For gaming companies though, like banks, a peculiar problem is having to defend against hundreds of mimic websites continually being created to trick unwary customers out of their data and money. So how can companies keep up with what the bad guys are doing?

**Identity analytics**

## Who's doing what to whom?

The adoption of identity analytics for identity governance and administration as well as authentication can reduce organizational risk and administrative efforts, while improving user experience. Products without analytics capabilities will over time increase administrative overhead and risk undiscovered security problems. What should CISOs look out for?

**Behavioural analysis**

## Better ways to spot the bad guys

One promising development in the search for more efficient ways to detect malicious activity is behaviour-based analysis tools to complement signature-based detection solutions. So how do these tools actually work? Are they scalable? And how much do they cost?

**PCI DSS**

## The devil is in the details

As one anonymous CISO told AKJ recently, the single biggest reason for PCI DSS compliance failure was a lack of senior management commitment to compliance. But as Verizon has stated, those who lose card data tend not to be compliant with PCI DSS, and under GDPR, cardholders now have access to class action lawsuits on broader 'non-material damage' grounds. So what's the best way to ensure compliance?

SECURING
ONLINE GAMING

# Why do so many blue-chip vendors work with us? Real buyers ...

Where the real decision-makers allocate budgets

100%

**The most influential solution buyers**

You will be surrounded by the key budget-holding cybersecurity and digitalisation professionals at online gaming and gambling companies.

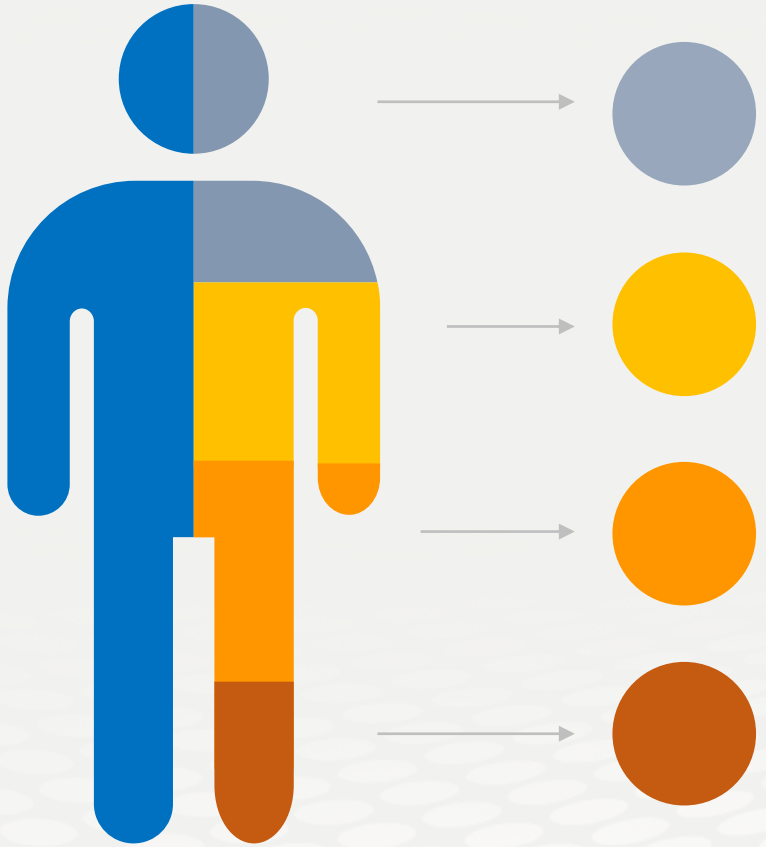
AKJ Associates has been building relationships with security and data privacy professionals since 1999 and our cybersecurity and payment security community is the largest of its kind globally.

We know the senior executives who drive strategy from the top, we know the enterprise architects who often control the largest budgets, we know the IT Security Leads and Engineers and we know the security and data specialists.

All of these job titles attend Securing Online Gaming in 2019.

We understand that every vendor needs to sell more. That is the bottom line.

Getting in front of the right people at the right time always increases the lead generation and always increases profitable sales activity



### Cybersecurity specialists

We have been producing the events these professionals take seriously for more than 15 years

### Digital transformation

We attract senior executives tasked with digital transformation and the associated need for new security solutions

### Fraud, Audit, Compliance, Risk

We provide the go-to events for fraud prevention, digital risk managers and compliance owners at the world's key corporates

### Data Protection & privacy

We are a key venue for decision-makers with budget and purchasing authority in privacy and GDPR

http://akjassociates.com/event/gaming

Our testimonials speak for themselves: we have many more

SECURING
ONLINE GAMING

# What our sponsors say about us

proofpoint.

eCrime remains a critical event for security pros. Year after year, AKJ manage to stay on top of market trends and satisfy attendees' demand for topical expertise; we are delighted to be part of the eCrime series.

cigital

My team and I were impressed with the volume and caliber of the audience e-Crime Congress attracts. This event gave us the opportunity to expand our networks and learn more about our customers.

COFENSE

We found the event very productive, it was good to meet potential customers and gives a chance for decision makers to meet us and understand what we do and how we can help them with their security.

**Ninety five percent of our exhibitors and sponsors work with us on a number of occasions each year.**

**Our sponsor renewal rate is unrivalled in the marketplace.**

**This is because our sponsors generate real business at our events every year.**