Inside this report:
Sponsors
Key themes
Who attended?
Speakers
Agenda
### Key themes

- What are hackers saying about you online?
- Building better faster SOCs
- Coping with a runaway threatscape
- Who’s who? Improving identity analytics
- The devil’s in the details
- Dealing with the alert tsunami

### Who attended?

<table>
<thead>
<tr>
<th>Cyber-security</th>
<th>We have a 15-year track record of producing the events cyber-security professionals take seriously</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management</td>
<td>We attract senior risk officers with responsibility for information risk assessment and mitigation</td>
</tr>
<tr>
<td>Fraud, Audit, Compliance</td>
<td>We provide the go-to events for fraud prevention and compliance owners at the world’s key corporates</td>
</tr>
<tr>
<td>Data Protection &amp; privacy</td>
<td>We are a key venue for decision-makers with budget and purchasing authority</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Speakers</th>
</tr>
</thead>
</table>
| Matt Arnell, Head of Enterprise Architecture  
Arcadia Group |
| Terry Bishop, Technical Director, EMEA  
RiskIQ |
| Simon Brady, Managing Editor  
AKJ Associates |
| Jennifer Craven, Senior Associate  
Pinsent Masons |
| Kevin Fielder, CISO  
Just Eat |
| Alex Hinchliffe, Threat Intelligence Analyst  
Palo Alto Networks |
| Alphus Hinds, CISO  
Standard Bank International |
| Nick Ioannou, CSO  
Ratcliffe Groves Partnership |
| Tudor James, Solution Architect  
Imperva |
| Nicola Millard, Senior Intrusions Specialist  
EA Games |
| Goher Mohammad, Head of Security, Risk and Compliance  
L&Q Group |
| Lluis Mora, CISO  
GVC Holdings |
| Danielle Papadakis, Product Specialist  
Segasec |
| Thomas Pernot, Online Business – Fraud and Billing Manager  
Square Enix |
| Paul Richards, Head of Information Security Governance  
Rank Group |
| Christina Thakor-Rankin, Principal Consultant  
1710 Gaming |
| Ofer Wolf, COO  
Guardicore |
| Simon Wood, VP Cyber Investigations Manager  
Barclays |
<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00</td>
<td>Registration and breakfast networking</td>
</tr>
<tr>
<td>09:00</td>
<td>Chairman's welcome</td>
</tr>
</tbody>
</table>
| 09:10 | IR challenges in the game industry  
Nicola Millard, Senior Intrusions Specialist, EA Games  
- Keeping up with the developers  
- Not forgetting the small guys  
- Our landscape |
| 09:35 | Why regulation is a good thing  
Paul Richards, Head of Information Security Governance, Rank Group  
- Establishing a dialogue  
- The overlooked benefits of regulation  
- What stands to be gained from collaboration with the regulator? |
| 10:00 | Refreshments and networking |
| 10:25 | Effectively responding to a data breach  
Lluis Mora, CISO, GVC Holdings  
- Preparing the team and the organisation for a data breach  
- DOs and DON'Ts during the incident handling  
- Communicating to stakeholders, customers and regulators  
- Wrapping up and learning from the past |
| 10:50 | Stopping bad bots – gamble on your website not with your website  
Tudor James, Solution Architect, Imperva  
- What is a bad bot and who runs this automated traffic?  
- How do bad bots impact online gaming?  
- Strategy to mitigate automated threats (bad bots)  
- Additional risks presented by web and mobile APIs and how to protect them  
- The experience of an existing customer – case study |
| 11:10 | The days of vLANs segmentation are over  
Ofer Wolf, COO, Guardicore  
- Move away from the traditional wall-based protection into a flexible security posture  
- Use micro-segmentation technology that lets the business run much faster, add and change applications, move them around to and between clouds  
- Keep Zero Trust architecture that creates a strong, application aware security stronghold that protects the crown jewels |
| 11:30 | Prevention – best practice insights  
Thomas Pernot, Online Business – Fraud and Billing Manager, Square Enix  
- What type of fraud are we facing?  
- Fraud prevention  
- In-house vs External fraud prevention providers |
| 11:55 | Refreshments and networking |
| 12:15 | WWLD – what would a layer do?  
Jennifer Craven, Senior Associate, Pinsent Masons  
- Practical tips for the gaming sector  
- Prevention & legal considerations  
- Regulation and codes of practice that should be your priority |
| 12:50 | JavaScript injection attacks – the user browser is the new cyber-battlefield  
Terry Bishop, Technical Director, EMEA, RiskIQ  
- JavaScript injection attacks – what are they?  
- A brief history  
- GDPR implications  
- The current landscape – attackers acting with impunity  
- Steps to defend against JavaScript injection attacks |
## Agenda

### 13:10 Cybersecurity: No big deal. The unimportance of cybersecurity and what that means for today’s information security leader

**Simon Brady**, Managing Editor, AKJ Associates  
- Do we have the cybersecurity we deserve? If cybersecurity does not pose an existential threat, then how can we expect businesses to take it seriously? Is the ‘band-aid’ approach good enough?  
- Cyber-risk is not like other risk. How the operational risk leaders view cyber-risk and how it compares to other forms of operational risk

### 13:20 Lunch and networking

### 14:30 Blind spots

**Christina Thakor-Rankin**, Principal Consultant, 1710 Gaming  
- Thinking like a criminal – understanding how criminals use gambling as a sandbox  
- Gambling industry – from first responder to rinse-r  
- The age of tech – from going back and going beyond  
- Fraudsters Ltd v Sector Ltd – how cross-sector collaboration could be the best form of defence

### 14:50 Cyber-threat landscape for the gaming industry – insights from Unit 42

**Alex Hinchliffe**, Threat Intelligence Analyst, Palo Alto Networks  
- Introductions and public-private partnerships  
- Threat landscape targeting the gaming industry  
- Credentials phishing, theft and abuse  
- Conclusions and take-aways

### 15:10 Phishing 3.0: Stakes are high for gamers and the online gaming industry

**Danielle Papadakis**, Product Specialist, Segasec  
- The new reality of phishing attacks, and why protecting your users means protecting your brand  
- The modern hacker, a sophisticated storyteller  
- Demo – a phishing attack in the online gaming industry  
- Proactive solutions that incorporate best-of-breed detection, non-brand defence, take-down, and deception  
- Measures and counter-measures that effectively reduce the number of attacks on your clients and your brand

### 15:30 EXECUTIVE PANEL DISCUSSION Co-op mode: Cross-sector insights for online gaming

**Simon Wood**, VP Cyber Investigations Manager, Barclays  
**Nick Ioannou**, CSO, Ratcliffe Groves Partnership  
**Matt Arnall**, Head of Enterprise Architecture, Arcadia Group  
**Goher Mohammad**, Head of Security, Risk and Compliance, L&Q Group

### 16:05 Networking and refreshments

### 16:30 Grass-roots security from the ground up

**Kevin Fielder**, CISO, Just Eat  
- How to build a cohesive cybersecurity strategy from the ground up  
- Why are senior management, stakeholders and investors now paying attention to cybersecurity as a real business risk? What is at stake?  
- How to create a business efficient cyber-risk framework  
- Creating scalable cyber-infrastructure for an agile environment. How to manage digital evolution  
- Case study: building grass roots security at Just Eat

### 16:50 Security and innovation – hand in hand or hand to throat?

**Matt Arnall**, Head of Enterprise Architecture, Arcadia Group  
- How perceptions of security have changed, how engineering has changed  
- The dangers of high-volume agile. Is agile innovation and security an unsustainable relationship?  
- Solutions and key takeaways: how it’s possible to have both – with examples from logistics, retail, hospitality and fashion

### 17:10 Keeping cyber simple. Are we over-complicating cybersecurity? And how can we simplify the problems, so we can get the right solutions?

**Alphus Hinds**, CISO, Standard Bank International  
- The challenges of managing security at an international remit. What are the siloes, and cross-jurisdictional issues and risks that you need to take into account.  
- The over-complexity of cybersecurity. Are we making cybersecurity more complicated than it needs to be? Is this affecting the communication of cybersecurity as a business risk to the board? And what can be done?  
- The move to the Cloud. What do information security leaders need to take into account when it comes to accountability for Cloud security and dealing with CSPs  
- The evolving digitalisation of the financial services and how FinTech and open source platforms are changing the landscape of security. Are APIs the industry’s worst nightmare?

### 17:30 Conference close