

“Really useful event. I could not improve it, to be honest. Tricky to pitch content to include security specialists and general CTO/CIO but it was done really successfully.”
~ CTO, Hubio



R3: Resilience, Response & Recovery Summit 2016
Your roadmap to a robust incident response plan

📍 Etc Venues St Paul's, London
📅 27 September 2016

The poster features a man in a white shirt and tie sitting on a folding chair in a desolate, open landscape, wearing a gas mask and working on a laptop. The background is a cloudy sky.

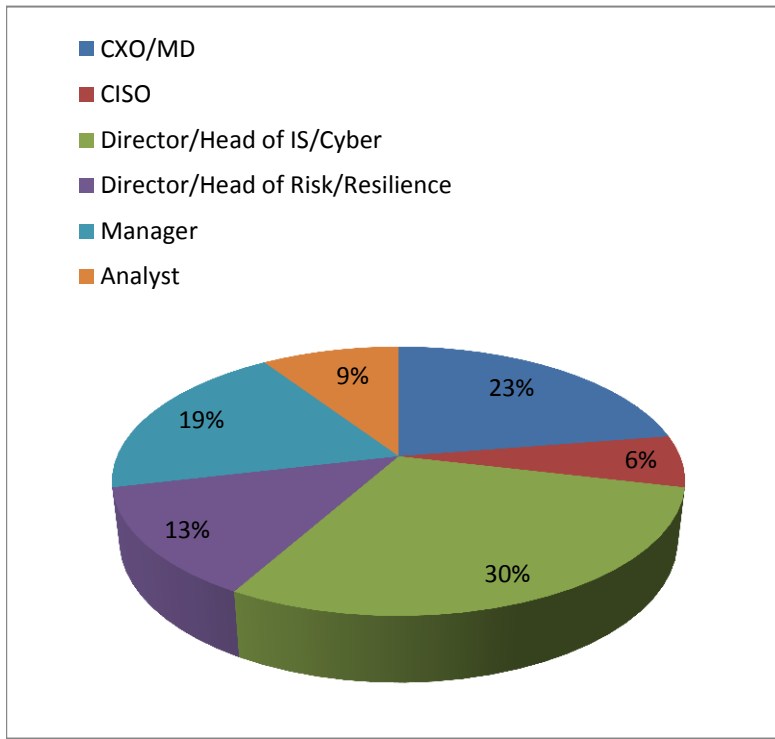
www.r3summit.co.uk

SPONSORED BY:

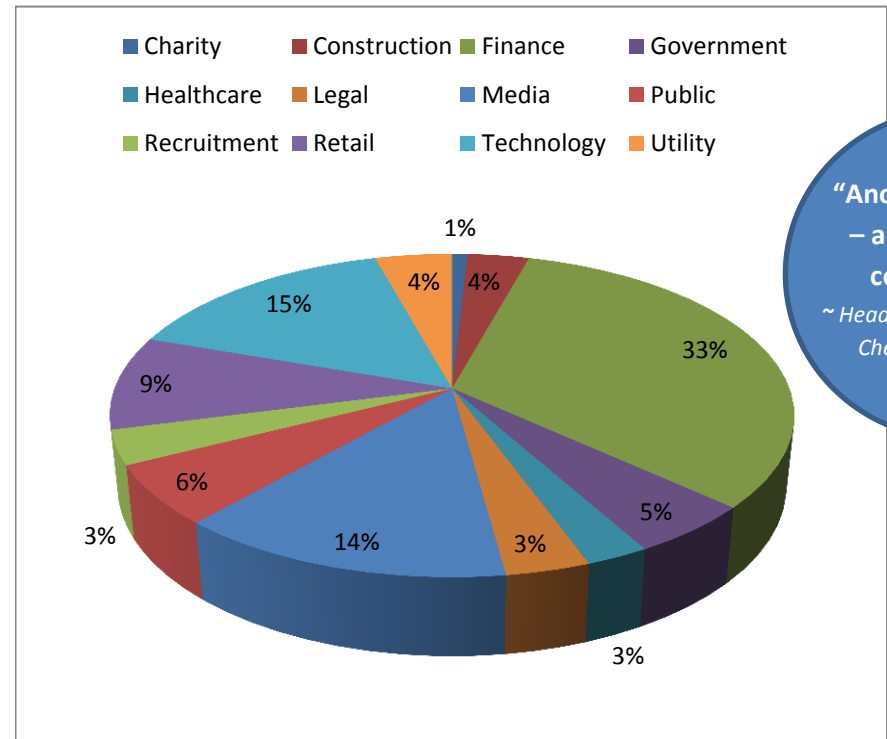


AUDIENCE

By seniority:



By sector:



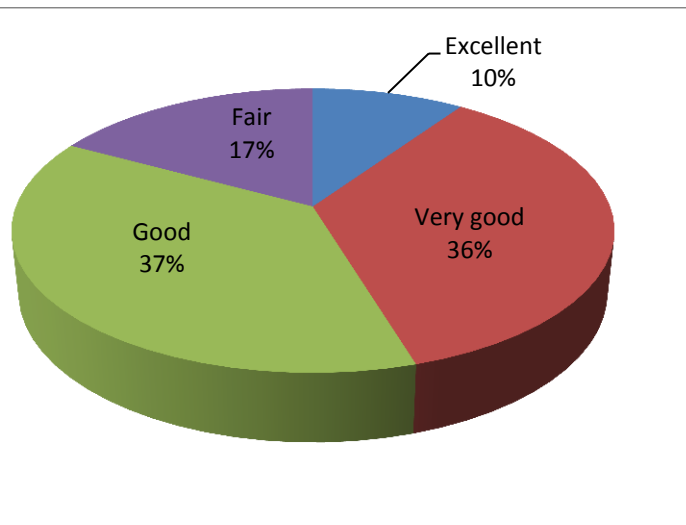
“Another good event – a lot of engaging conversations”
 ~ Head of Threat Prevention, Check Point Software Technologies

Companies included:

Artemis, AT&T, Birmingham City Council, Bloomsbury, Cheque & Credit Clearing Company, Covea Insurance, Cyber Rescue, DB Schenker, Department of Business Energy & Industrial Strategy, Department for Business, DVLA, First Actuarial, GE Capital, Harrods, Horizon Discovery, Information Security Forum, Intralinks, Islington Council, JD Sports Fashion, Kroll Associates, LaFosse, Legal & General, Lloyds Banking Group, London Internet Exchange, London Stock Exchange Group, Maersk, McCann World Group, Mencap, Menzies Distribution, Mi-Pay, Moneycorp, NBC Universal, Newton Investment Management, NS&I, Office for National Statistics, Pearson, Robert Walters, SABMiller, Seadrill, Sky PLC, Smart Focus, Sony Interactive Entertainment Europe, Southern Water, Spire Healthcare, SportPursuit.com, Sun Life Financial of Canada, Think Money Group, Thomson Reuters, UBS Wealth Management, Vanguard Asset Management, Vitality, Vodafone Group, Wesleyan Assurance Society, Which?, Workspace, Zenith Vehicle Contracts, ZMARTA Group

HOW DID THE AUDIENCE RATE OUR 2016 SPEAKERS?

“This event was so brilliant and professional – I learned new tips and found it really inspiring and helpful. Thank you!”
~ Privacy & Information Solicitor, Birmingham City Council



TOPICS REQUESTED FOR 2017:

- Use of analytic tools to detect internal threats
- Updates of UK legislation in comparison with European legislation
- Key challenges in the implementation of GDPR
- Breach response in the Cloud
- Updates on trends in cyber threat vectors

• 2016 speakers included:

- Director of Security, **Payments UK**
- Chief Risk Officer, **British Business Bank**
- Managing Director, **Information Security Forum**
- Senior Red Team Specialist & Ethical Hacker, **ASOS**
- Detective Inspector, Organised Crime Command, **Metropolitan Police Service**
- Group CISO, **OCS Group**
- Head of Cyber Intel & Investigations, **LinkedIn**
- Board Member, **Cyber Rescue Alliance**
- Head of Information Security & Payments, **Capita**
- Head of Business Resilience, **Modern Times Group**
- Head of UK Information Security, **AXA**
- Founcer & Chairman, **ClubCISO**
- Former CISO, **NFU Mutual**
- Partner, **Osborne Clarke**

If you are interested in addressing these topics, or want to propose another subject, contact:

Alice Macklin, Event Producer,
a.macklin@business-reporter.co.uk

CONTACT US

For speakers and topics:

Alice Macklin, Event Producer

a.macklin@business-reporter.co.uk

0208 349 6494

For media partnerships:

Ivan Ujvari, Marketing Manager

i.ujvari@business-reporter.co.uk

0208 349 6493

For sponsorship opportunities:

Marc Morrow, Sales Director

m.morrow@business-reporter.co.uk

0208 349 6453

www.r3summit.co.uk

1. Create **one centralised reporting process for employees** to report incidents, and undertake regular testing on the most common types of attack that your company suffers (e.g. phishing).
2. The 2nd most important part of incident management is the **lessons learned, to prevent a repeat**. But the average investigation period is 31 days – too long to suspend business operations. Have recovery plans in place ahead of time.
3. Cyber risk insurance policies may not cover losses caused by rogue employees, business partners, contractors, social media, or a failure to comply with a business' own security or privacy processes. Be careful of the contract fine print, and **never lie to the insurer** about your processes or resources.
4. In order to **reduce ICO fines in the event of a breach**, firms must have cyber governance and planning, situational awareness and intelligence mechanisms, ways of assessing their cyber resilience and plans for cyber responses.
5. In your response plan, **factor in when to involve law enforcement**. The most useful evidence is often obtained during the first few hours after an incident.
6. A threat is capability, intent and opportunity. A risk is vulnerability, impact and probability. **Cyber security is in the threat management business**, not the risk management business.

We look forward to seeing you at

The European Information Security Summit on 21-22 February 2017!

“Many great talks
from expert
speakers”

~ Head of Information
Security, Catalyst
Housing