**SASIG Daily Webinars 16Nov 20Nov**

#### Monday 16 November, 11am-12noon (GMT)

**Driving real behaviour change: How to build a security awareness program that works**

https://www.thesasig.com/calendar/event/preventing-phishing-attacks-with-security-awareness-training/

**Tuesday 17 November, 11am-12noon (GMT)**

**A global reset: Cybersecurity predictions 2021**

https://www.thesasig.com/calendar/event/20-11-17-incident/

#### Wednesday 18 November, 2 – 3pm (GMT)

**Taking care of ourselves – Strategies to identify and manage professional stress**

https://www.thesasig.com/calendar/event/20-11-18-cisotable/

**Thursday 19 November, 3 – 4:30pm (GMT)**

**SASIG Academy: Getting cyber healthy with the doctor - Cyber risks and cybercrimes**

**for SASIG members only**

https://www.thesasig.com/calendar/event/sasig-academy-getting-cyber-healthy-with-the-doctor-cyber-risks-and-cybercrimes-2/

**Friday 20 November, 11am-12noon (GMT)**

**How to build a SOC when you have limited resources**

https://www.thesasig.com/calendar/event/how-to-build-a-soc-when-you-have-limited-resources/

**SASIG Daily Webinars 16Nov 20Nov**

#### Monday 16 November, 11am-12noon (GMT)

**Driving real behaviour change: How to build a security awareness program that works**

When it comes to modern cybersecurity – ultimately your users are your last line of defence. So you need to arm them with both knowledge and practice to mould dynamic, alert guardians of both your organisation and your data. The key to your success is engaging, entertaining – and crucially – topical security awareness training. So where to start, or how to renew your program? Are you one of the 80% of organisations who allocate two hours or less per year for security awareness, how useful do you judge this small amount of user training to effect behaviour change? Join us as we review valuable strategies on how to create and sustain an impactful cybersecurity awareness education program. Plus we delve deep into the following questions:

* **How do I ensure my users embrace the training? Who are the key influencers internally?
• What is the minimum – and maximum – levels of training shown to have been successful?
• How do I motivate and reward my last line defenders?
• What reporting and measures are the most pertinent to the IT team and alternatively to the C-suite?**

**Tuesday 17 November, 11am-12noon (GMT)**

**A global reset: Cybersecurity predictions 2021**

The year 2020 has been an unprecedented time of change and has shaped up in a way that nobody could have expected. This year’s activities continue to alter the future course of cybersecurity, making it even more critical to ensure that we better prepare ourselves for what’s to come. We are delighted that threat intelligence expert Dr Jamie Collier joins us to share upcoming cyber trends and challenges in 2021. During the webinar, he will touch on various topics discussed in our report, A Global Reset: Predictions for the Future Cyber Security, including:

* **How remote work will evolve and affect organisations operationally**
* **Insights into how threat actors will leverage the pandemic in their attacks**
* **The growing need for intelligence-led security validation**
* **The future state of cloud security**
* **Nation-state activity and changing TTPs**
* **How ransomware has pivoted from business risk to a national security risk**

#### Wednesday 18 November, 2 – 3pm (GMT)

**Taking care of ourselves – Strategies to identify and manage professional stress**

Throughout lockdown, many of us have focussed on supporting our teams and colleagues whilst also maintaining secure behaviours and enabling business to function. However, we have less obviously focussed on ourselves and our own mental health and resilience. So how far should personal responsibility as a leader extend? In this fully interactive roundtable, we will acknowledge the mounting personal pressure on ourselves as we all inevitably assume responsibility for the safety and security of all those around us – business, teams, home, family, etc. We will examine these pressures through the personal experiences of our panellists and discuss the ways they’ve found to maintain their own, business, team and family resilience.

**Thursday 19 November, 3 – 4:30pm (GMT)**

**SASIG Academy: Getting cyber healthy with the doctor - Cyber risks and cybercrimes**

**for SASIG members only**

This second session continues the “Getting Cyber Healthy with the Doctor” training series with a focus on cyber risks, and what constitutes a cybercrime – including venues and prosecution history examples. We explore the profiles of the perpetrators of various cyber crimes, examining cases that have been indicted by law enforcement authorities, and case examples (with technical notes) from personal experience that demonstrate the means, motives, and opportunities exploited by the cybercriminals. The Doctor, Shane Shook, is a recognised information technology and security authority. He has advised and led teams in risk and incident management at multiple Global Fortune 100 companies. With more than 30 years’ experience in the field of cyber forensics spanning a multitude of industries – including banking and financial services, healthcare, and retail – Shane has a deep understanding of today’s most pressing cybersecurity and business technology issues.

**Friday 20 November, 11am-12noon (GMT)**

**How to build a SOC when you have limited resources**

Some organisations have a 24/ 7 security operations centre (SOC) with teams of dedicated analysts carefully monitoring for threats around the clock, every day of the year. Unfortunately, most organisations cannot afford this, what with the costs of having well-trained analysts onsite at all times outweighing the benefits.Join us as Andrew explains how to create an effective SOC by combining three components – people, processes, and technology – to build an efficient security operation.

In this webinar, you’ll learn:

* **What makes a SOC effective, including best practises for success**
* **Cost comparisons of various SOC staffing models**
* **Steps for building a SOC with limited resources**
* **How a NextGen SIEM solution is the ideal technology for building a SOC**