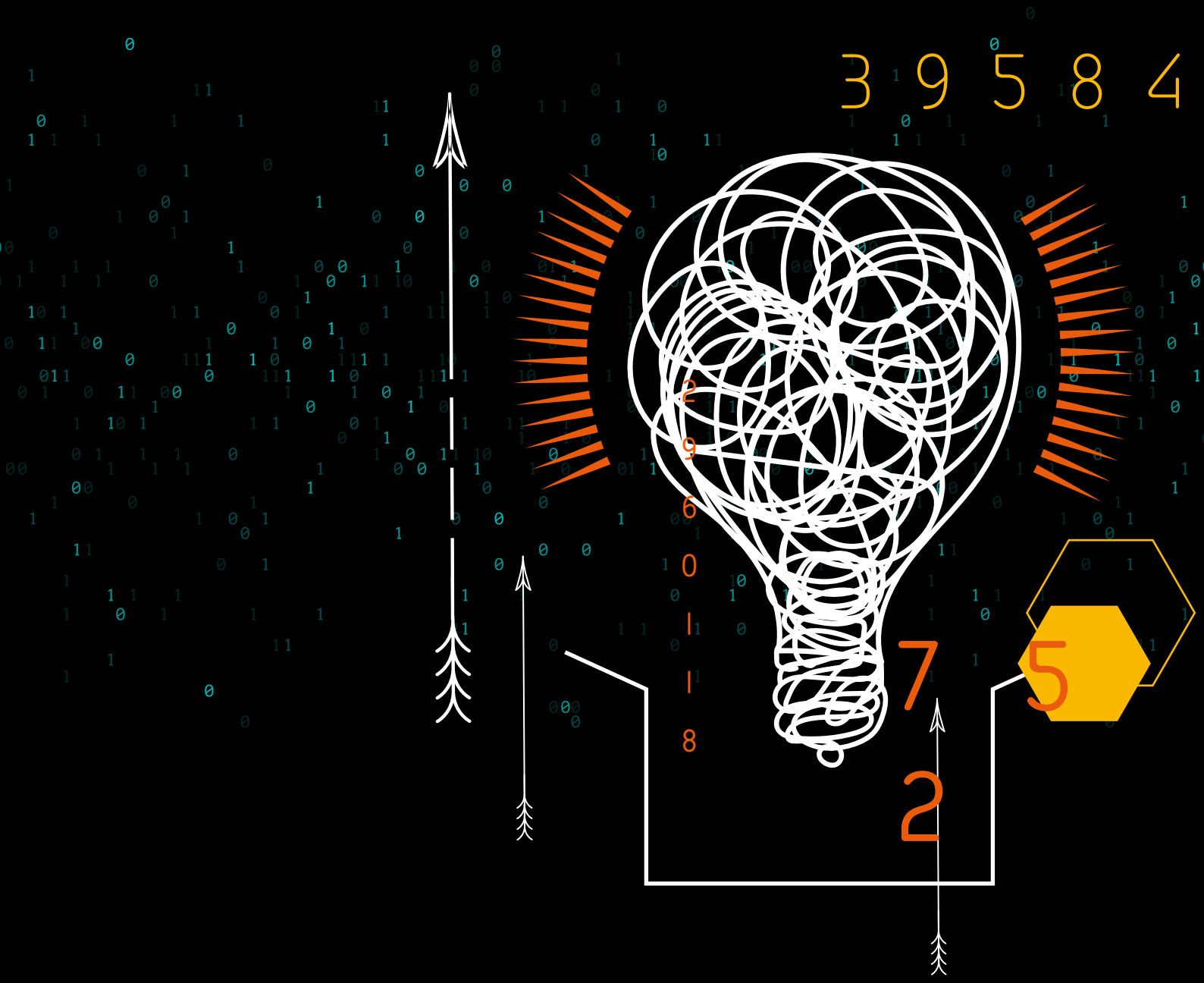
BAE SYSTEMS



Cybersecurity skills crisis

INSURANCE INSIGHTS
FROM BAE SYSTEMS

Five ways we can crack the cybersecurity skills crunch

At a time when cybersecurity professionals are needed more than ever, there's a global shortage of four million workers (according to the (ISC)² Cybersecurity Workforce Study, 2019). And the gap has grown by 100% in the past year. This ultimately puts businesses, the economy and society in jeopardy.

In this latest instalment in our Insurance Insights series, hear from experts across the industry on why business, government and academia must work together to address the skills crisis.

A spotlight on cybersecurity in financial services

The question of how to tackle the cybersecurity skills shortage isn't a simple one. So, unfortunately it follows that there isn't one simple answer. The discussions that we have had with experts across industry have seen a wide range of perspectives and viewpoints covered – suggesting that solving this challenge will require a multi-faceted, collaborative effort.

Cybersecurity is particularly crucial to the financial services sector. A decade ago, we were looking at small-scale opportunistic crimes. Nowadays, attackers build advanced capabilities to target core banking systems and are more aggressive in disrupting their victims' ability to respond.

The infamous 2016 Bangladesh Bank heist hinged on the attackers' knowledge of cybersecurity protocols. More recently, in 2018 $15 million was stolen from five institutions linked to Banco de Mexico's electronic payments system. A month later, Banco de Chile lost $10 million through international payment transfer scams. Since then, there have been further attacks in India, Pakistan, Chile and Malta. Attempts are being made on banks around the world on a weekly basis.

Cybersecurity is already a boardroom issue. And cyber hygiene and protection against endemic attacks will only become more important as financial services organisations fall into the crosshairs of an increasingly sophisticated criminal economy.

Below we've gathered together the five key themes from recent industry discussions. They're a starting point – building blocks to begin solving this challenge. But the discussion doesn't end here. So, when you've explored the topics below, add your perspective to the dialogue by getting in touch with us or heading to The Intelligence Network's website.

#1: Driving diversity

Cybersecurity needs to become a welcoming and fulfilling career for everyone. It's not just the number of cybersecurity professionals globally that needs to be addressed – greater diversity is needed within the profession too.

According to the (ISC)² Women in Cybersecurity Report, only 24% of the overall workforce is female, and pay inequality is a major issue.

> Sian John MBE, Chief Security Adviser at Microsoft, has highlighted:
>
> "Even though they may have the answer to a particular problem, many girls end up taking a backseat compared to boys, because of the way they have been socialised."

People from different cultural and social backgrounds need to be engaged too – both ethnic minorities and older people who are changing careers. The greater the diversity in a workforce, the greater the innovation and problem-solving capabilities we will have.

Cybersecurity is a fantastic career for life. You're doing your bit to protect nations, businesses and society. And you can make very good money whilst doing so.

> Jonathan Luff, Co-founder of CyLon, an accelerator programme for cybersecurity start-ups says:
>
> "We have seen an astonishing range of entrepreneurs coming through our programmes, seeking cyber opportunities from a variety of backgrounds."

#2: Transferrable vs. technical skills

Following on from diversity, industry discussions have also focused on transferrable capabilities. Many professionals may have previously dismissed a career in cybersecurity due to its apparent "tech-centricity". Historically, there's been an overemphasis on technical skills.

But cybersecurity is actually a dynamic discipline requiring a broad range of capabilities.

With a better understanding of the breadth and variety of roles in cybersecurity, potential candidates could better comprehend the value their transferrable skillsets could offer.

The industry needs curious people with great communication and problem-solving skills, and a thirst for knowledge. The emphasis should be on recruiting people with a learn-it-all attitude, not a know-it-all one. This opens up a far greater pool of candidates.

#3: The effect of emerging tech

With artificial intelligence and machine learning automating rudimentary basic tasks, cybersecurity becomes less about managing technology and increasingly about managing business impact.

To that end, companies can train their existing staff in areas where there are skills deficits. For example, organisations are up-skilling data analysts to become data scientists.

In fact, emerging platforms and tools are able to assess the impact of automation on a workforce and suggest where individuals can be retrained or reallocated (to areas such as cyber security) to deliver maximum value for the business.

#4: Willing forces

Everyone within an organisation must be willing to take responsibility and play their part in defending against cyber security threats. It shouldn't just be an IT issue. The general workforce – all the way up to board level – must step up and commit to becoming cyber-savvy.

That doesn't just mean one-off training or empty platitudes in personal development plans. It demands a real commitment – and an ongoing investment of time and energy – to stay on top of the latest trends and evolutions in cybersecurity.

> Thomas Clayton, Senior Underwriter for Cyber-Liability, Zurich Insurance has referenced this:
>
> "The security risk from humans is just as high as the risk posed by technology. Instead of simply phoning IT if they've clicked on something they shouldn't have, people need to learn how to behave with responsibility and security."

#5: Excelling in education

Steps are being made to fill the education gap around cybersecurity. The government has funded a £20-million cybersecurity skills programme for 14–18-year-olds.

> Meanwhile, on Tuesday 21 April 2020, The National Cyber Security Centre (NCSC), launched the cross-governmental 'Cyber Aware' campaign, which offers actionable advice for people to boost skills in protecting passwords, accounts and devices.

However, our universities still have a lot of work to do. Many experts agree that universities need to work more closely with businesses to ensure that graduates are learning the relevant and specific skills needed to step straight into employment, without requiring costly training top-ups.

> Producing graduates who are up to speed and can stay on top of sector changes is a real challenge, as Max Vetter, Chief Cyber Officer, Immersive Labs has highlighted.
>
> "Because the threats change at such a rapid pace, degrees in cyber can very quickly become outdated."

Playing our part

Here at BAE Systems, we're doing our bit to help improve cyber education. We invest £90 million in STEM in the UK (which includes digital and cyber skills). We're also training almost 3,000 apprentices, while our schools roadshow programme goes to 450 schools across the country.

In fact, such is our commitment to improving cybersecurity skills – not only in a professional context but also in a personal one – it forms a core area for an industry initiative that we're leading. The Intelligence Network – launched in 2018 by BAE Systems with the aim of safeguarding society in the digital age – lists educating digital citizens and the next generation as one of its key challenges. We'll be revealing more about our progress on this mission soon.

£90 million	3000	450
STEM investment	Apprentices	Schools

Explore our range of resources and further reading

In the meantime, we've collected some further reading about cybersecurity (and developing the next generation of cybersecurity specialists) below. Explore the materials and share them with your networks.

- Check out: our cybersecurity expertise and current projects in the financial services sector
- Review: The Intelligence Network's Vision for Tackling Cyber Fraud
- Join: The Intelligence Network's LinkedIn group

About James Hatch

Director of Cyber Services at BAE Systems Applied Intelligence

James Hatch is Director of Cyber Services at BAE Systems Applied Intelligence. He leads a diverse cyber security business covering cyber intelligence, security advisory and technical services, managed security services and government security programme.

As well as his cyber security portfolio work, James has direct experience of information security management in financial services and central government. James has spent five years building the company's UK-based cyber security consultancy business, running large scale security transformation programmes and managing the response to high profile security incidents for clients. He was previously head of information security for a UK-based internet bank.

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK
E: learn@baesystems.com | W: baesystems.com/insuranceinsights
linkedin.com/company/baesystemsai
twitter.com/baesystems_ai