IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation

In Conversation with Luke Dash

Carol Baker

As ISMS.online's latest 'State of Information Security' research reveals that deepfakes are now ranking as the second most common information security incident for UK businesses in the past year, trailing only behind malware infections, we talk to Luke Dash, Chief Executive Officer at ISMS.online about the startling trend of deepfake attacks hitting the business sector and what can be done about it.

*As CEO of ISMS.online (https://www.isms.online), **Luke Dash** enables companies to achieve their information security and compliance goals.*

With decades of experience driving sales, revenue, and operational growth for organizations like Lead Forensics, The Indigo Group, Ascential, and IQPC, Luke provides the strategic guidance businesses need to protect their data. His leadership optimizes efficiency, ensures security best practices, and maximizes ROI across departments.

Luke has a proven talent for implementing solutions that allow enterprises to thrive in today's data-driven landscape.

Tell our readers a little bit about yourself and what attracted you to ISMS.online

I have been involved with SaaS businesses for over 15 years. After joining ISMS.online as Chief Revenue Officer in 2021, I was made Chief Executive two years ago when its founder, Mark Darby, the CEO of Alliantist, the organization behind ISMS.online decided to step back.

Since its inception in 2005, ISMS.online has been at the forefront of the SaaS compliance industry, providing a cutting-edge cloud platform that revolutionizes how organizations approach their information security management. ISMS.online is changing the way businesses across the globe handle data privacy and information security compliance.

As Chief Executive of ISMS.online, my role is to accelerate commercial growth. Over the past three years, we have had unprecedented success, and ISMS has grown by 500% and continues to grow. Quite recently, we were acquired by a new equity partner, ECI, and that has been a real game-changer for the business, allowing us to scale at pace and enhance customer value without compromising our core principle of user-first innovation.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

One of the things about being a Chief Executive is that it is a role in which you constantly learn. I'm a big believer that a company is only as good as its people, so you must take them on the journey with you. Technology is the enabler, but people are the heart of a business, and giving them all the skills they need to help them excel is essential. When your people excel, so does your business.

How do you see the current cybersecurity landscape?

Information security management is an extremely fast-moving sector, so at times, it can be difficult to look too far ahead as changes are happening all the time. For instance, last year, when we surveyed participants for our 'State of the Information Security' report, no one reported the threat of deepfake. This year, when we ran the same survey, 32% of respondents in the UK said their business has experienced a deepfake security incident in the last 12 months. In particular, attackers are using AI-powered voice and video-cloning technology to trick recipients into making corporate fund transfers – similar to the CEO email scam, but this time using voice and video instead of just the text of an email.

There are also use cases where deepfake has been used for information and credential theft, leading to reputation damage with attackers bypassing facial and voice recognition authentication. A couple of years ago, businesses were concerned about malware and phishing emails; now, in addition to these, they tell us that they worry about becoming victims of deepfakes.

To stay current, cybersecurity firms need a good relationship with auditing bodies which can support businesses undergoing their certification processes. It is vital to understand the cybersecurity market, know what's coming up next, and know how the cybersecurity firm can stay one step ahead of the attackers. It's a highly competitive marketplace that faces constant challenges. The number of certifications handed out in the last 12 months has risen almost 100% compared to the previous year, showing that more businesses are finally taking information security more seriously.

ISMS.online is run slightly differently from some of the more venture capitalist-backed businesses that go in for really, really high growth at any cost. We are more sustainable in our approach: less focused on just pure profit – instead looking at making sure the business can build and grow reliably over time. We have a highly skilled people, and we create an environment where skills can be updated, creating a nurturing environment where people feel valued. Not only do we see our staff perform at their best, but we also give them the tools and training that will allow them to excel.

We say to businesses, don't just be super passionate about technology, even though it is a great enabler, but invest in your people because they are your biggest asset and most significant risk.

The newest version of attack that criminals will put together is never too far away, so every business needs to be agile and invest in its people, processes, and tools. People are the most critical part of the journey, even with technology!


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

How are criminals using AI-powered technology to breach cybersecurity?

One of the exciting findings from this year's report was that despite AI being a considerable part of the problem, businesses are also adopting AI and machine learning (ML) technologies to thwart threats. Although 72% of respondents agree that AI and ML will help their companies to improve data security programmes, adoption remains in its early stages, with just over a quarter of firms (27%) saying that over the past 12 months, they have put initiatives in place.

So, AI has both a good side and a bad side. It's important not to brand AI and paint it with a brush of negativity the way criminals are using it because it is also going to be an incredible enabler for businesses to embrace and use to protect themselves. AI is no longer just around the corner; it has arrived and is here to stay.

Deepfake is normally associated with social media platforms, so why the jump into the business sector?

We are so used to seeing social media flooded with deepfakes, and it isn't easy to differentiate what's real from what's not. If you think of deepfakes, you automatically think of a video of a celebrity or famous person that sounds and looks right. Still, it can be much more rudimentary and basic in business. For example, an audio message either on its own or accompanied by a video clip that sounds and looks like the company's CFO saying, "I'm stuck here at the airport; I need you to make a transfer to this account." This is the type of thing that is catching businesses out. And it's more common than you think. Over 30% (32%) of respondents in the UK say they had experienced this type of deepfake incident. In the US, it was 35%, and in Australia it was 24%.

Using this type of deepfake in business is just the start. Criminals are constantly evolving the ways they try to penetrate enterprises. When they first introduce a new approach, they have a high success rate – for example, when phishing was new, there was a very high success rate. But as businesses started to adapt, evolve, and get smarter, the success rate dropped significantly from those early days.

Now, when we think of AI and deepfake as the latest iteration of criminals, they have taken something that was built for good and turned it into something that can be quite damaging. But businesses are wising up. Even in a challenging economic climate, firms are making much more significant investments in protecting their businesses from information security attacks because the cost of not doing something far outweighs the cost of doing it. In fact, our report highlighted that more than 51% of businesses expected their information security spending to increase by at least 25%, and 22% expected it to grow by more than 25% in the next year to tackle the challenges that businesses now face.

What are the risks of deepfakes surrounding vendors?

The phrase 'you are only as strong as your weakest link' is critical. A business can do a lot to protect itself from attack, starting with its people, processes, and the tools it uses, but as soon as it looks at its supply chain, the weakness can be seen. Our report found that almost 80% of UK businesses were impacted by an information


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

security management breach relating to a third party or supply chain partner. This was a 25% rise compared to a year ago, and it's a threat that continues to grow.

The burden of responsibility for a business is not just to look at itself but also to look at who they are doing business with and ensure all partners have the proper security in place. The Gold Standard remains ISO 27001, the global information security standard. From the volume of companies embracing information security, certification is being taken more seriously, with many organizations now making it a prerequisite. There are now very few large-scale enterprise businesses that will work with anyone who doesn't have some form of information security management certification in place. In the UK, there is no chance of working with anyone in the public sector without the correct certification.

What about the need for training and upskilling your workforce?

Although we are a software business promoting the value of an information security management platform that enables you to manage your processes, we are huge advocates of staff training and ongoing training in the business. Many of us remember working in organizations where there would be a meeting around information security once a year, where people would be encouraged to send any issues to a particular email address. After sitting through a training section often lasting half an hour once a year, you would return to your day job – with very little probably embedded in you. The responsibility is on businesses to ensure they accelerate the value in training and learning and keep it ongoing throughout the business, not just cover it once a year in passing. After all, there are plenty of creative, fun ways to educate people about cybersecurity, and these must be part of an ongoing process within the business. Whatever your role in an organization, it is essential to keep learning.

Looking at the key regions in the report – the UK, USA, and Australia – is there a reason why Europe doesn't feature?

The UK, USA and Australia are areas where ISMS.online has had unprecedented success, with almost 40% of our business being driven by UK demand and 20% both in the USA and Australia. These regions are particularly focused on ISO 27001 as the supply chain requirements within those countries are particularly stringent. Until recently, ISO 27001 was not a requirement across Europe, but we now see demand for ISO 27001 in France, Germany, and Spain. As such, we will look to incorporate Europe in future editions of the State of Information Security report.

Looking at the data for the various regions of the report, one thing that stands out is how many more businesses in the UK suffered from vendor-connected incidents. In the report, 37% of the USA talked about third-party and supply chain management being the issue, whereas in the UK, the figure was 79% – almost double.

Our research also shows that 41% of UK respondents cited partner data (41%) as the most compromised in the past 12 months. More businesses need to be vigilant about the risk posed by their third-party vendors and suppliers, especially considering the new, sophisticated attack methods.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Enhancing training and awareness is crucial across the supply chain and internally to counteract these increasingly advanced attacks. Nearly half of the respondents (47%) acknowledged this by placing greater emphasis on employee education and awareness initiatives. In addition, almost two-fifths (38%) say financial allocations for securing supply chain and third-party vendor connections are set to increase by up to 25% in the coming year – particularly as the research found that 79% of businesses have been impacted due to an information security incident caused by a third-party vendor or supply chain partner.

Are there any other closing thoughts you would like to get over to our readers?

More businesses are taking a serious view of cybersecurity, which is happening across the board, from the largest organizations down to the smallest SMEs. Every company must have a good blend of people, processes and technology. When discussing the dangers of advanced technology, it is also essential to talk about the benefits of technology and how it enables businesses to do fantastic things, so take a balanced view. In today's uncertain world, one thing we can all be certain of is that cyberattacks will continue to evolve – so businesses will need to evolve faster!