CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

In Conversation

In Conversation with Chris Newton-Smith

Carol Baker

Recent IO research shows that 60% of UK and US cybersecurity leaders find third-party and supply chain security risks "innumerable and unmanageable". We speak with Chris Newton-Smith, CEO, IO, about what businesses should do now to build resilience, especially as attacks on smaller suppliers persist. With many organizations unprepared for future supply chain disruptions, we ask what impact will the public face?

Chris Newton-Smith
Chief Executive Officer
IO
https://www.isms.online/

Chris brings decades of expertise in scaling businesses, driving global market expansion, and leading innovation, positioning him to accelerate IO's impressive growth trajectory.

Most recently, Chris was the Chief Operating Officer (COO) at Boku helping to build a regulated, non-card Local Payment Method (LPM) network for the world's largest digital merchants including Amazon, Meta, and Netflix, accelerating Boku's revenue and EBITDA growth to more than 30% annually, and doubling the valuation of the company to >$650 million.

Prior to that, Chris was part of the senior leadership team at Redknee, growing the business from a start-up to a publicly listed company, from $5 million to $250 million in revenue and from 10 to 1,600 employees across the mature and emerging markets through organic growth and M&A.

Chris has led companies and teams through significant transformations, including strategic acquisitions and carve-outs, expanding into new regions, and winning and delivering software solutions to global companies including Marriott, Four Seasons, Telefonica O2, and Vodafone.

Tell our readers a little about yourself.

My background is in B2B technology and software. I'm originally from Canada, but I've been based in Europe for a number of years now. I joined IO as the CEO earlier this year, and before that I had a chance to work in a couple of different companies. Most recently, I was the Chief Operating Officer at a global payments business called Boku, which is based in London, but operates in the local payments market around the world.


CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

Talk about some of the key findings from IO's The State of Information Security report.

Together with Censuswide, IO surveyed more than 3,000 cybersecurity and information security leaders across the UK and the US.

A couple of things really stood out in the report. First, respondents flagged that the attack surface that they're seeing keeps expanding. Over 40% (41%) say they were struggling with third-party risk, 39% said that they were having challenges securing some of the emerging technologies, and 37% flagged an issue with cloud security. Secondly, respondents also cited the people (or human side). When it came to cybersecurity, the skills gap continues to be a concern for 42% of respondents.

Whilst these are well known issues that remain a concern in the industry, our research revealed the rise of a newer risk – 'shadow AI'. Our survey revealed that shadow AI was prominent in 37% of organizations with respondents reporting that employees were using of genAI tools without approval. That is quite a high percentage and explains why 95% of respondents then went on to say that their organizations are thinking about investing in AI governance to try and get ahead.

Some of the threats which we have seen for a number of years continue to be there, but new ones are coming onto the radar based around AI, and supply chain is also jumping up in importance as well.

What is the best advice / best practice for organizations when it comes to managing third-party risk and performing due diligence on new third parties, and the importance of continuously monitoring existing supply chain partners if companies are to accurately assess their security posture and track changes in their risk profiles?

Defining the security challenges around third-party risk really shone out from the report. Over 60% (61%) of respondents said that they had been impacted by a third-party-caused incident in the past 12 months.

But also, I think if you just look the press coverage on security breaches which have taken place in the past few months, a lot of them have been traced back to third-party-caused incidents.

For many organizations, third-party relationships are part of doing business. As such, they become part of your organization's attack surface. Therefore, it is important to think of them as an extension of your own security perimeter. This means that when you put in place governance and best practices for your organization, you need to be extending those out to your suppliers and third parties as well.

But this is not something that you can do as a one-off checkbox. You've got to be continually reassessing risk and potential risks based on how your vendors and third parties are themselves managing said risks. Our customers use regulatory frameworks such as ISO 27001 as a way of aligning their standards with their


CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.
The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

suppliers to ensure that they are meeting their minimum requirements for security as well. If you looked at some of the results in the report, 34% of the respondents said that they require ISO 27001 for information security from their suppliers.

When it comes to addressing third party risk around AI governance, 28% of respondents say they are going to mandate the newer standard, ISO 42001 certification, from their suppliers.

How can companies enforce the principle of 'least privilege' to ensure that vendors and supply chain partners only have access to the data and systems absolutely necessary for their function?

This is something that always sounds simple in concept, but is hard for companies to execute. It means that an organization needs to restrict access rights for their suppliers quite closely based on job function, or make them time-bounded. ISO 27001 certainly reinforces least privilege enforcement as a strategy to improve cybersecurity.

Ultimately, its about setting out those least privilege requirements, segregating third-party suppliers into specific environments, creating zero trust zones within those boundaries. In doing so, it is important that you make sure your suppliers extend that out to their own third parties as well. Effectively putting in place those types of controls within your environment, but also requiring your vendors to apply the same controls to their subcontractors as well.

Please talk about the financial impact on companies.

Our research found that 71% of organizations reported that they had been fined for non-compliance in the past 12 months, and with a third of those, the fines had exceeded more than £250,000.

In addition to direct penalties such as fines, the report also flagged that 42% of organizations had experienced some sort of customer loss due to compliance or security issues, with a further 38% citing reputational damage as a top consequence of having challenges with their cybersecurity.

Regulatory risk is also a top concern. In the light of NIS2 and DORA especially in the EU, we see the potential impact of non-compliance or a breach in regulated industries growing. Failure to comply with requirements or a cyber breach presents a fundamental business risk if they were to lose their license to operate. Not only is there some quite significant potential financial impact on companies issued with fines, but it also filters downstream and others further down the line feel the consequences of those fines as well. But many firms don't realize this.

If you look at some of our survey results around investment, compliance and security, 96% of organizations report that they are now prioritizing, achieving or maintaining certifications such as ISO 27001. First, for risk mitigation and trying to make sure in an audit that their systems are in place to prevent some of these


CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

issues from happening. Secondly, if these firms themselves are delivering their services into other organizations, often it's now becoming a mandated requirement. So, in a sense, it becomes a commercial or revenue enabler. If you don't have these compliance or certifications audited and in place, you may not be able to win business and generate new revenue.

As companies double down on their digital transformations, what can we expect to see when it comes to attacks on surfaces, and how can this be mitigated?

One of the challenges of digital transformation is that it often introduces new suppliers and new types of technology. A lot of digital transformation is now cloud based or based on a cloud infrastructure, so in a way, digital transformation projects are actually expanding the attack surface for organizations.

In our survey, 39% of companies cite that emerging technologies were a risk, with 37% of respondents identifying cloud security as a top concern.

As a company goes through its digital transformation, it brings in new systems and tools into the organization. This creates a tech sprawl, and 35% of respondents flagged the sprawl of disconnected systems as being major security challenge. Add the challenges facing businesses around AI, the security issues around digital transformation become bigger.

Please talk about the digital resilience challenge facing organizations, and how can businesses strengthen their resilience to shadow AI, data poisoning and malicious use?

Another big theme in the report was the new threats which are emerging from AI around data poisoning and deep fake scams.

As a company starts out on its digital transformation journey, the solution isn't to slow down transformation or innovation, but organizations should focus on how to integrate security into it from the beginning.

If you look at best practice in the space, a lot of it is adopting security by design or resilience by default principles into the project itself so that you are embedding security and governance controls successfully from the start. What both ISO 27001 and ISO 42001 are asking of organizations is to adopt these principles early into projects, making sure they are a key part of the design, so that there can be continuous improvement.

When it comes to people risk, how is employee burnout is impacting on the corporate cybersecurity chain?

Employee burnout is becoming, or is already, a security risk. In our research, 32% of organizations cited staff fatigue and burnout as a major challenge to maintaining cybersecurity.


CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

When people are stretched thin or when they're fatigued, they could be slow to respond. They could miss signals and make errors which are then potentially exploited by adversaries who are looking to attack organizations with phishing and social engineering. It's a compounding problem, because we also had 42% respondents saying that their organizations were directly impacted by the shortage of cybersecurity skills, so the organization is faced with the double whammy of people feeling fatigued and burned out, but also not being able to bring the right people into the organization because they are unable to find those skills they need in the market.

First, to deal with this, organizations are investing in tools and software which provide more automation and more management so that current employees can be made more effective and efficient.

Secondly, is training and upskilling. If an organization is unable to find those skills in the market, how can it better develop its own staff to take on new capabilities?

As an example, at IO , we have been training our own staff on ISO 42001, in the same way we did for ISO 27001 previously.

So, for me, it's a combination of training and developing the staff in place; and then secondly, looking at where you can use tools and automation, and potentially AI, to relieve some of the pressure on the humans as well.

Do you feel that supply chain risk now poses a greater risk than people risk?

Supply chain risk and people risk is very closely connected. Whilst, one is not greater than the other, the more people challenges you have, supply chain risks become amplified.

A tired or understaffed security team is less likely to spot a supplier breach or a misconfiguration in your supplier infrastructure that could cause a supplier issue to take place.

Our report reveals that supply chain incidents were becoming a more sizable problem. Over 60% of respondents say that they had been impacted by a vendor or a supply chain incident.

Ultimately the solution, or how to address it, is kind of the same and relies on putting in place better skilled, and a more automated security organization, and then deploying that and asking your suppliers to have similar standards and approach in their own organizations as well.

As companies shift cybersecurity away from the previously seen IT-focused function and cost centre, and how can this shift be used as an enabler to driving sustainable business growth?

When you look at cybersecurity compliance, the trend is moving away from being entirely a cost centre to something that is part of the business. We see this every


CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

day with our customers. One of the reasons our customers use our software is to manage their risk and governance. They are not doing it solely for the benefit of the IT organization, but are doing it because their C-level executives and their boards are asking them for that kind of visibility in terms of what's happening with cybersecurity and compliance. For example, what the progress is, the issues arising, and what does continuous improvement look like?

As C-level executives undertake these bigger transformation projects around AI, introducing new capabilities into the business, people are now starting to ask for compliance and resilience by design – they are a fundament part of those projects. It is no longer just about launching new tech into the business as quickly as possible, but doing it in a structured way. High-profile cybersecurity issues and even some of the fairly high-profile AI issues have put compliance and resilience on the boardroom agenda as well.

Any closing thoughts?

Organizations now need to consider the challenges around shadow AI and AI governance. How to ensure good AI governance, whether you're just using AI tools within your organization or starting to build them yourselves, is an important topic. Having solid AI governance within the business is just critically important and will be a key measurement of the success of the rollout of AI in the future. As such we see the newer standard from ISO 42001 as providing a really great framework that can be used across the globe to address these different requirements.

Additionally, I think it's important for organizations to proactively address AI governance as it will give greater confidence in the use of AI within the business and ensure that AI is being adopted and used in a safe, secure and ethical way. For organizations everywhere, thinking about AI governance, getting informed about it, finding out more about what some of the best practices are, and the challenges and solutions, would be a really important next step for a lot of organizations.