ISMG INFORMATION SECURITY MEDIA GROUP

FORTRA

Prohibiting AI Use Increases Enterprise Data Risk

Fortra's Tony Kelly on Securing AI Adoption With Governance, Data Protection

ISMG

FORTRA

Tony Kelly

Regional Sales Director, Fortra

Tony Kelly is a cybersecurity leader with more than 20 years of experience driving technical sales and strategic initiatives. At Fortra, he leads GTM for Secure Service Edge (SSE) solutions, collaborating with C-level executives to safeguard critical assets in cloud environments.

Tony's expertise spans DSPM, CSPM, SSPM, and AI-driven automation, and his unique blend of deep technical knowledge and strategic business acumen enables him to bridge the gap between complex security requirements and business objectives.

Previously, Tony held key roles at Netskope and Cisco Systems, earning industry-respected certifications including CISSP and CCIE. He is recognized for his ability to translate complex security concepts into clear business value.

Attempts to block generative artificial intelligence use has often pushed employees toward unauthorized public tools, increasing the risk of exposing sensitive enterprise data. Tony Kelly, regional sales director at Fortra, said organizations need to accept AI adoption as inevitable and focus instead on securing its use through visibility, governance and data protection.

Kelly argued that traditional data protection strategies often fail because many enterprises either have not fully deployed data loss prevention technologies or operate them only in monitoring mode. Modern data protection, he said, could secure AI workflows without disrupting business operations.

"It's not a surprise that 80% of that data going to AI is not protected. But the reality is it can be and we can make it simple," Kelly said. "DSPM is an amazing way to detect a much broader set of critical data, in an automated way. You still need the 'P' part of DLP to protect the data, but DSPM plus DLP is a perfect combination."

In this video interview with ISMG, Kelly also discussed:

- Balancing AI access controls with business productivity and limited IT resources;
- Selecting enterprise-grade AI platforms with stronger security and resilience;
- How Fortra's platform balances AI adoption with security guardrails.

Kelly is a cybersecurity leader with more than 20 years of experience driving technical sales initiatives. He leads Fortra's go-to-market strategy for secure service edge solutions, collaborating with C-level executives to safeguard critical assets in cloud environments. Previously, he held leadership roles at Netskope, Cisco Systems and Sirius Computer Solutions.

Why AI Bans Backfire

TOM FIELD: When you think about shadow AI and employees pasting proprietary content into public tools, where do you see organizations most exposed right now?

TONY KELLY: The organizations that are most exposed are the ones that are trying to keep their users from using AI. Users will always find a way to meet their needs one way or another; there's a lot of shadow AI usage. The challenge with shadow AI is oftentimes it's the personal or public version of AI, where any data you put in it can be used to train their LLMs and it's now their data. That's where the biggest risk is: trying to avoid the consumption of AI. Your users are going to find a way.

Closing the Unprotected AI Gap

FIELD: I've seen reports that up to 80% of AI data goes unprotected. What is stopping security teams from closing that gap, and where do you recommend they start?

KELLY: Data protection has been more of an allow-or-deny approach for a lot of enterprises. They haven't employed a lot of data loss prevention, or DLP, tools, and there's good reason: they're challenging to work with. They can throw a lot of false positives that then upset users and disrupt business needs. A lot of times, folks have not done a good job deploying data protection, and if they have, they put it in alert mode only, not a deny or protect mode. It's not a surprise that 80% of that data going to AI is not protected. But the reality is it can be and we can make it simple.

> **"The organizations that are most exposed are the ones that are trying to keep their users from using AI."**
>
> – Tony Kelly

Why DSPM and DLP Belong Together

FIELD: How does integrating data security posture management and data loss prevention change the way you can actually protect data and AI workflows?

KELLY: DLP was designed to prevent the loss of risky data - financial records, HIPAA records, intellectual property, software, source code. It was all about protecting that data and preventing it from being exposed to the wrong users, the wrong devices and the wrong locations. In order to do that, it always had to detect that critical content, but those detections were pretty static - a lot of Regex identifiers and keywords. It required a lot of compute, and it still led to a lot of false positives. The other thing is DLP tools were designed to find the data you already knew about - financial records, source code, you name it. It was designed to find the data you knew to look for, and that got us so far. But the reality is, there's a lot of critical data, maybe mergers and acquisitions-related data.

In every enterprise, there's a lot of critical data above and beyond things like the credit card data that PCI required you to be compliant with. With DSPM and using AI to scan for any and all concerning data - above and beyond Regex identifiers and dictionaries - now they're using a lot of context and large language models to surface data that was hard to recognize in the past. DSPM is an amazing way to detect a much broader set of critical data, in an automated way. You still need the "P" part of DLP to protect the data, but DSPM plus DLP is a perfect combination.

Access Controls and IT's Constraints

FIELD: IBM research suggests that 97% of organizations with breached AI models lacked any access controls. Is this an awareness problem, a priority problem or something else entirely?

KELLY: My career began in IT, and IT has always been underfunded, understaffed and undertrained. IT is such a great enabler of the business, but at the end of the day, it's about your business - and there's always a cost with IT. The more security tools you want to bring to bear, that's raising your cost and can also disrupt the flow of the business. When in doubt, folks try to be as accommodating to the business as possible, and that just leaves a lot of exposures like what you just described.

"IT has always been underfunded, understaffed and undertrained. IT is such a great enabler of the business, but at the end of the day, it's about your business - and there's always a cost with IT."

– Tony Kelly

Innovation Without Compromise

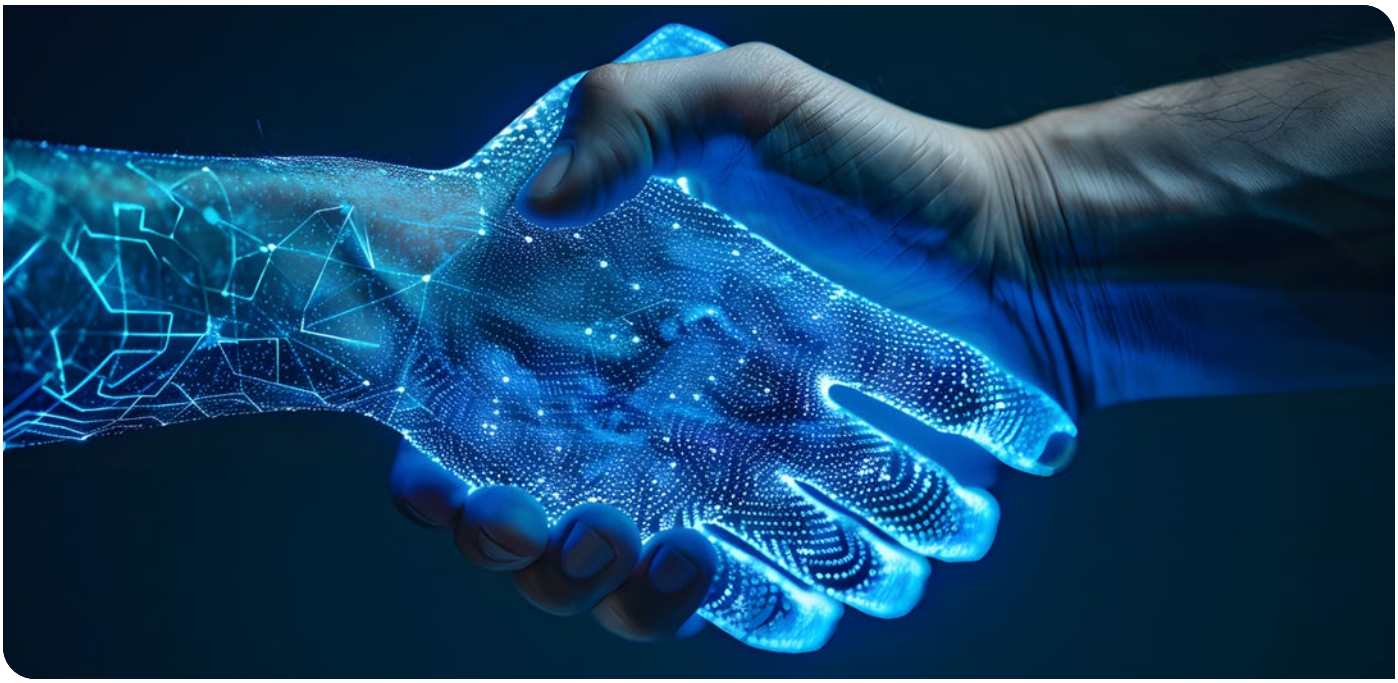
FIELD: Security leaders are under a lot of pressure today to enable AI adoption without increasing risk. What does innovation without compromise actually look like in practice?

KELLY: At Fortra, we don't look at ourselves as the team of "no." Often the security team is here to say, you can't do this, you can't go there, or you can't have access to this data or that data. Instead, we want to enable your business, but enable you to do it in a safe, user-friendly manner. We've got protections that we layer in the guide that helps a user safely adopt generative AI: the right data with the right gen AI. It's a layered approach that we recommend for our customers, kind of like putting the guardrails up on the bowling alley to keep that bowling ball going down the lane that you want. That's the approach, and it's working well.

The Fortra Approach

FIELD: How is Fortra helping customers approach AI and data security differently?

KELLY: It starts with discovery. There's a lot of shadow AI out there - both internal to the enterprise environment, but especially external, with the use of SaaS environments, gen AI and cloud apps. It's easy: If you've got access to the internet, there's a wealth of systems you can use, which is good and risky. What we do is we guide the user community, through our platform, to correctly use AI. If you go to a gen AI site that's not in the authorized category, you'll be redirected to a list of gen AI sites that are authorized. Instead of it just being a killed connection, "no" - we give them choices on the gen AI solutions that are authorized by the company.



Choosing Enterprise-Grade Gen AI

FIELD: What questions do our viewers need to be asking about their AI deployments today?

KELLY: The first thing is every gen AI site is different. Some are designed to help software developers, some to help writers - they're all a little bit different. Make sure you're identifying the right AI site for whatever your needs are. The other thing is some are enterprise grade; in other words, they've got disaster recovery, business continuity and data centers. They provide encryption for any data that you've allowed to go into that AI site. They have strong authentication mechanisms. Enterprise-grade gen AI sites are the way to go. And the big five that I keep hearing across my customer base are clearly Microsoft's Copilot, Google's Gemini, Claude AI - which is huge - ChatGPT and Perplexity. Those are the five that continue to come up. Certainly there's Grok; there's Meta AI. But Meta may be more suited to consumers, given the Facebook heritage, than to enterprise. Definitely get a business-grade service that has the ability to give greater protections and has the business continuity that you need.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 · sales@ismg.io

BANK INFO SECURITY · CAREERS INFO SECURITY · HEALTHCARE INFO SECURITY · GOV INFO SECURITY · infoRisk TODAY

CU Just for Credit Unions INFO SECURITY · Data Breach TODAY · AIToday.io · OT.today · PaymentSecurity.io · FraudToday.io · DeviceSecurity.io

CIO.inc · CyberEd.io · CyberEdBoard · CXO ADVISOR · CYBER THEORY · Xtra mile LIFECYCLE MARKETING · ATHENA

QC MEDIA · SUMMIT · custom events · roundtables · NULLCON · hardwear.io · iSMG Studio

iSMG

902 Carnegie Center · Princeton, NJ · 08540 · www.ismg.io