
TRIDENT
SEARCH
THE CYBER SECURITY
INNOVATION FORUM
THE "RED FLAGS" TO LOOK OUT FOR

# THE RED FLAGS IN CYBER SECURITY

In March 2024, Trident Search welcomed expert guests to the Cyber Security Innovation Forum. Having explored several critical external risks in our previous events, we wanted to put the lens on the very real challenges leaders face within their own security architecture. In other words, we looked at the red flags in our industry, how to spot and mitigate them, and crucially, how to avoid them!

## Key themes:

What are the biggest red flags you need to look out for? In this report we'll cover some of the key discussions that came out of the forum, including:

- AI isn't the solution to all our problems and still isn't understood well enough to be used safely
- Upskilling is our best shot at overcoming the workforce gap
- Legacy vs new: we're undermining our own security architecture by jumping on the newest tools too quickly
- UK incident preparedness is worryingly lagging behind our adversaries

# OUR EXPERTS

**Dinis Cruz,** Chief Scientist, **Glasswall**

**Rob Demain,** CEO, **e2e-assure**

**Dominic Aslan,** CEO, **OutBreach**

**Stuart Jubb,** Group Managing Director, **Crossword Cybersecurity Plc**

**Laura Longhi,** Director of Security Consulting Sales, **Adarma Security**

**Vince Mccaughey,** UK Bank Information Security Director, **The Bank of London**

**Ric Longnecker,** Ex-CISO, **Open Systems**

**Andrew Connor,** Director of Product Security and GRC, **PG Forsta**

**Daniel Walker,** Ex-Senior Manager (SVP), CISO Strategy & Architecture, **TSB Bank**

**Alexandra Phillips,** Senior Manager, **Baringa**

**Simon Goldsmith,** Enterprise Security and Platforms Lead, **OVO**

**Alex Powell,** Ex-Chief Information Officer, Financial Services, UK & Ireland, **SS&C Technologies**

**Alan Miller,** Director of Cyber Risk Services, **Alvarez & Marsal**

**Charlee Ryman,** Director, **Trident Search**

**Lottie MacCallum,** Head of Marketing, **Trident Search**

# *PREPARATION* IS BETTER THAN CURE

Many a boy scout will remember the motto **"be prepared,"** and in today's fast-moving cyber security industry there really couldn't be a better maxim to live by. Indeed, the overarching theme from the forum was the need for preparation in the face of accelerating external threats and risks to security architecture. To avoid getting caught up in the red flags affecting our industry, you need to look inwards at your own teams and systems; getting your own house in order before you can effectively combat the external challenges facing the organisation.

Regardless of size or stage, without preparation all companies face similar issues when it comes to **effective management** and ensuring the best use of the **technologies**, **tools** and **partnerships** they have. This is not to belittle the risk of external threats at all. We had a lively discussion led by Alan Millar on the challenge posed by nation state actors and the superiority of cyber-attack methods employed by Russia, China and North Korea.

It is simply critical to get our internal architecture in order so that we are in the best possible position to combat external threats when they arise.

It seems like a basic idea, but the reality is that too few businesses are investing the time and resources into proactive measures. In 2023, UK companies faced **2.39 million instances of cybercrime**, yet only a tiny fraction (**21%**) had a solid incident response plan in place. As an industry we are not doing enough to ensure effective preparedness, and need to focus more time and energy on:

- **Developing fundamental incident response plans**
- **Ensuring oversight and understanding of existing tech stacks and capabilities**
- **Investing in the right in-house skills**

Get these essentials in order and the following themes will fall into place.

# NAVAGATING TECH DEBT

**The red flag:** Without an understanding of security fundamentals we become too reliant on technology and put ourselves in a precarious position against attackers with more advanced and sophisticated skills.

You might have heard the phrase **"tech debt"** (also known as design debt or code debt), bandied around recently. It refers to the implied future costs incurred when choosing an easy but limited solution over a more time-intensive option that might require more work and fewer cut corners.

The issue really comes into its own when it comes to how we react to geopolitical threats. The skillset of our adversaries in security fundamentals is significantly better than in the UK, where we are **too reliant on technology**. In recent years the response of UK businesses to rising threat levels is to rapidly expand their product range as a defence mechanism.

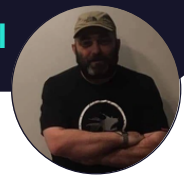
However, investing in new technology without utilising or even understanding what you currently have will cause major problems in the long-term. For one thing, with security budgets stretched to breaking point, this approach is clearly unsustainable. In the latest ISC2 workforce study **47%** of respondents stated they had experienced cutbacks including budget cuts, layoffs and hiring and promotion freezes, meaning there simply won't be the required budget allocation.

Secondly, what happens if the tech fails? Or if your attackers find their way in past your firewalls?

Our adversaries in Russia, China and North Korea don't need the same level of investment in technology as they have gone the other way in nailing security fundamentals and an understanding of the cyber landscape. To keep ahead of the curve and prevent greater risks, we need to **focus on security basics** and **shore up our own systems and processes**. This involves understanding security tools better, investing in training and education in cyber basics and building trust with our partners along the supply chain to ensure we're effectively managing our assets and security stance.

*"Russian infrastructure inside the Moscow ring-road is world-leading. Unlike the West, our adversaries have invested time and state funding into understanding cyber fundamentals rather than relying on technology to meet this need. Now in the global arena they are using this to great effect to disrupt society for their advantage."*

**Alan Miller, Alvarez & Marsal**



## SOLUTIONS - HOW TO WORK SMARTER, NOT HARDER:

**Training and education:** Ultimately, we've got to start with the basics - keeping our operating systems patched and data storage in top shape to strengthen our defences and minimize potential risks. Our teams need the fundamental knowledge to achieve this without relying on technology so that they are prepared in the event of a breach or system outage. Invest in training to upskill and develop essential knowledge in both the security team and wider business.

**Enhanced disaster preparedness:** Dinis Cruz advocated for running P3 scenarios as P1's so that when crises occur your team are better prepared and aware of the processes they need to follow. In a disaster, every second counts, so proactively streamlining your response times could make all the difference.

**Invest strategically:** Before purchasing new tools, pause and consider whether they will solve business challenges at the fundamental level or whether the need could be met by better utilisation of existing tools and training on enhanced security measures instead.

**Establish trust with partners:** Enhance your partnerships with vendors or MSSPs by prioritizing the establishment of trust and transparency rather than just looking at them as simply transactional. You never know when their input will help you identify pain point in your architecture or ways to improve your offering.

# LEGACY APPLICATIONS

**The red flag:** Investing in new tools without understanding your core technology and systems wastes time and resources, as well as exposing new vulnerabilities to attackers.

With the volume, velocity and variety of data organisations have to process and analyse increasing daily, legacy hardware and software cannot keep up with the evolving threat landscape. Yet these systems play a fundamental role in data security and IT architecture, meaning a failure to patch them will risk the **accidental exposure of vulnerabilities**. Expanding on-premise infrastructure to address new risks adds both capital expenses and operating costs into already stretched security budgets, but failing to scale to meet demand could inhibit revenue growth and put you at a competitive disadvantage.

Conversely, we've seen a real increase in larger companies in the end-user space jumping onto the newest, shiniest product or tool rather than taking care of their existing security arsenal. This has certainly come to the fore with the rise of **AI technologies** and products designed to "fight AI with AI".

Investing in unnecessary tools can be a huge waste of resources, and when teams are distracted by the newest models they fail to maintain or patch their existing product selection.  In large organisations it is estimated that only around 25% of the security arsenal is being utilised fully. Before investing we need to **analyse our existing capabilities** and understand if there are any areas you could capitalise on within your current systems and tools instead.

*"Within the industry there are still many core legacy applications, operating systems and databases which are required to support business need. Yet each one is a potential attack surface, meaning we must be mindful and proactive with patching. It can be difficult to secure Board or leadership approval for adequate maintenance or replacement of systems that seem outdated, which is where leveraging new tech such as AI to model the potential risks they pose can help."*

**Alex Powell, Security Leader**

## SOLUTIONS - HOW TO BALANCE BUSINESS NEEDS:

**Use AI for architecture monitoring:** Employ AI to stress test your environment before considering new investment. Simulating attack scenarios can help to show where your existing security tools are being underused, or where there are deficiencies in the security architecture that could be fixed through product expansion or skills training.

**Streamline your product selection:** Instead of jumping on the newest tech, focus on managing your existing assets and prioritize upgrading outdated legacy systems to align with cloud compatibility. By streamlining your product selection based on identified pain points and needs, you can optimize costs, usage and resource allocation.

**Align with the actual risk level:** Build your future roadmap by first mapping out your estate and identifying areas of need or under-utilisation before going out to market for new products. This enables leaders to align organisational investments with the risk register and be more proactive in their selection.

# RESOURCING

**The red flag:** Unless you create the time to upskill existing teams and new hires, you'll be unable to maximise employee ROI and will fall behind larger competitors, leaving yourself vulnerable.

The risks of poor resourcing in cybersecurity are multifaceted and potentially severe. Simon Goldsmith points out that the issue isn't merely "a lack of security personnel but rather a scarcity of individuals actively engaged in security tasks". This lack of knowledge and training outside of security teams not only burdens cyber professionals but also **increases the risk of critical gaps in defence**. The solution lies in upskilling your existing personnel to improve the in-house skills base.

Yet the cost to business owners of training or investing in diversity initiatives is inhibitive, especially to SMEs. Thus, the experts all recognised the need to improve the visibility of free resources and transparent information on **certifications and qualifications** so that professionals have access to tools and guidance without being put off by costly barriers.

We also need to adjust the way we are looking at diverse hiring. Unless you've got the environment and infrastructure set up to invest in diversity initatives, apprentice schemes and the like, you'll never be able to access new talent pools.

For start ups and smaller businesses, it's important to change the approach instead - perhaps providing a longer runway for unexperienced hires or promoting accessible training resources alongside the business induction for employees to upskill whilst performing their role.

## SOLUTIONS - HOW TO IMPROVE DE&I:

**Invest in upskilling: :** Laura Longhi emphasized the important of ongoing investment in training and retention to ensure the longevity of talent within the organisation. This requires sustained efforts and resources to support professional growth and career advancement but will ultimately help to leverage greater ROI from employees.

**Prioritize skills over job descriptions:** According to Dinis Cruz, we should shift the focus from rigid job descriptions to identifying candidates with the right skillsets, including adaptability and a willingness to learn. Then the focus should be on creating a supportive environment for DE&I and learning once inside the organisation.

**Revamp hiring processes:** Rob Demain highlighted the inefficiencies in current hiring processes, including AI-generated applications and misaligned job descriptions. To address this, you should reevaluate your recruitment strategies, leveraging technology responsibly to streamline candidate selection.

# ARTIFICIAL INTELLIGENCE (AI)

**The red flag:** Before jumping on the AI bandwagon, pause and reflect on whether tools are right for your business. Too many companies are descending on new tech without the required understanding and capabilities in AI security.

There's no doubt that AI tools have wide ranging uses, including threat monitoring, automating workflows, streamlining processes and understanding organisations and systems to a much greater extent. Indeed, there was a strong feeling amongst our experts that AI can be used to help us **spot and address red flags in security systems** and is an incredibly useful element of their work for that reason.

Yet in many ways, the tech itself is a red flag for many organisations. Too many security leaders see AI tools as a quick win to meet security needs, **disregarding their existing tools** in the process. With the availability of generative AI tools on the open market, we also run the risk of **sensitive data being exposed** in open-source environments, something that has already been witnessed in financial markets.

As an industry, we need to slow down and try to understand AI before we implement it. **Guard rails will be essential** as the technology evolves to prevent unchecked issues playing havoc with our systems. Indeed, as Dinis Cruz says, "anyone who works with AI is in for a shock" as the technology is moving so quickly, meaning we have no predictive measures for how AI technological developments are going to play out.

We need to stop thinking about AI as an end-all solution to our problems. Too few businesses understand the capabilities of AI tech to be able to do this anyway, and without better knowledge we risk unintentionally exposing weaknesses in security systems. Instead, consider how to **leverage AI to address the other red flags** covered in this report, using AI tools alongside your security architecture to manage issues with upskilling, systems monitoring and hiring.

## SOLUTIONS - HOW TO USE AI MORE EFFECTIVELY:

**Using AI to streamline systems:** Simon Goldsmith proposed implementing AI to automate tasks and streamline processes like email nurture funnels. He referenced a system he'd seen which utilized paired AI systems for outputs like these, which check each other and reduce the need for human oversight. This automation frees up staff resources, allowing them to focus on more ROI-generating tasks.

**Addressing bias in AI models:** Every AI system will be built with a bias unless you build it yourself. As Daniel Walker suggested, only by maintaining your own systems will you have the guarantee of clean, internally generated data which can be used to predict trends, identify issues, and develop actionable insights. Although setting up customized AI models requires significant effort initially, it yields long-term benefits in streamlining processes and mapping strategies.

**Developing organisational insights:** An underrated use of AI is to enable an organisation to stress test existing systems in a safe and securely monitored environment. In this way it is helping us to rapidly assess architectural vulnerabilities and find sweet spots where we can implement data hygiene and system management before an attack takes place.

**Tailoring security messages:** By using AI to translate messages for various audiences with differing levels of security knowledge, organisations can simplify communication processes. Automation saves your team time and prevents resource wastage with software taking on the manual process of translating messages for different audiences.

*"AI presents such an exciting opportunity for our industry. For the first time we have the technological capabilities to truly understand all the workings of a business; using gen AI to delve into the root causes of the challenges facing it and harnessing data analysis and modelling to establish the best means of overcoming issues without costly investments in custom technology and consulting services."*

**Dinis Cruz, Glasswall**

TRIDENT SEARCH

Securing an organisation starts with the CISO and his or her team, but it involves everyone within the business and all stakeholders who come into contact. The aim of this session was to explore the biggest threats to security posture, but through a discussion that encompassed topics as wide-ranging as nation state actors, diversity and inclusion and the technological future, we uncovered the key actions you can take to mitigate the risks from these challenges before you hit crisis point.

**For more information on this event, or to register your interest for future forums, contact:**

**Charlee-Ben Ryman**
Director of Recruitment
E: charlee.ryman@tridentsearch.co.uk