The AI Edge

Expert Insights on the Future of Business Resilience

AlertMedia

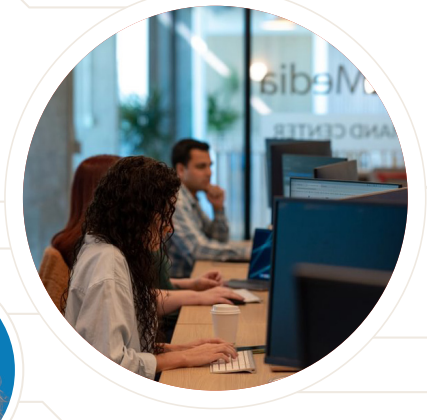


Table of Contents

Building a **Strategic Approach to AI**

As the most significant technological advancement of our time, artificial intelligence is undoubtedly transformative. More than just a tool, AI is a force capable of reshaping industries and societies. The choices we make today about integrating AI and teaching it to adapt will determine how it transforms our future.

To guide you through these choices, we've assembled a panel of leading experts in safety, security, and business continuity.

In the following pages, these industry authorities comprehensively explore AI's role in business resilience. They provide real-world examples and practical advice, sharing a structured framework to harness AI strategically and responsibly.

This framework will help you thoughtfully integrate AI solutions by **focusing on three key areas**:

1

Tactical utility

Identifying safety, security, and business continuity challenges where AI can provide practical solutions

2

Risk & mitigation

Evaluating how AI reshapes risk profiles and informs ongoing assessments

3

Human involvement

Establishing the right interplay between AI and human expertise across operations

Navigating this dynamic landscape can feel like stepping onto a high-speed virtual moving walkway, but you don't have to do it alone. At AlertMedia, we believe in the power of shared knowledge and community support. With contributions from the diverse roundtable of expert voices we've assembled here, you can confidently tackle these challenges and effectively integrate AI into your operational strategies.

"We believe that AI can be beneficial for our functions when humans are involved.

The more people with shared goals who can come together to promote responsible AI adoption for business continuity, risk, security, and employee safety, the more grounded human involvement we have to usher these powerful ecosystems into the future."

Sara Pratley
Senior Vice President of Global Threat Intelligence, AlertMedia

Meet **the Experts**

Join the Conversation Now
Share your insights and experience on LinkedIn with

#TheAIEdge

Dean Baratta | *Group Regional Security Manager, Microsoft*

Dean Baratta is a senior-level intelligence analyst with nearly 40 years of experience working across the military, government, and private sectors. He has created and managed intelligence teams in high-tempo and high-visibility environments such as GitHub, the U.S. Army, and the New Jersey Office of Homeland Security.

Shane Mathew, MPH, CBCP, CHSP | *Principal and Founder, Stone Risk Consulting*

Shane Mathew is a business continuity and crisis management expert with decades of experience providing organizational resilience and risk management services for companies such as Zoom Video Communications, Netflix, Gulfstream, Uline, and Nationwide Insurance.

Dr. Maaz Amjad | *Assistant Professor, Texas Tech University*

Dr. Maaz Amjad is an assistant professor at Texas Tech University and holds a Ph.D. in Computer Science with a focus on machine learning (ML) and natural language processing (NLP). He specializes in AI for social good, addressing misinformation and public health issues.

Sara Pratley | *Senior Vice President of Global Intelligence, AlertMedia*

Sara Pratley leads a team of experienced global intelligence analysts and experts who monitor worldwide threats in support of businesses and employees around the globe. Formerly VP of National News at CNN, she led the network's coverage of major events. Sara holds degrees in Sociology and Broadcast Journalism from Syracuse University.

Karna McGarry | *Vice President of Managed Services, Red5 Security*

Karna McGarry is a security intelligence leader with 20 years of experience in the private sector and the U.S. Intelligence Community. She specializes in managing strategic and tactical analytical teams, corporate intelligence processes, and threat management workflows.

Joseph Heinzen | *Chief Resilience Officer, WorldSafe*

Joseph Heinzen is the driving force behind WorldSafe, a global leader in Safety as a Service (SaaS), offering resilience assessments, safety planning, training, and technology reviews. With over 20 years of experience, Joe specializes in transformative strategies that build the strongest safety cultures within organizations.

Ryan Mayfield | *Advisor, WorldSafe*

Ryan Mayfield is a safety communications expert advising WorldSafe and the Koshka Foundation. He co-authored a pioneering study on tiplines/helplines and has experience with threat assessment, political risk modeling, and national security. A Stanford University graduate, he also worked with BMNT Partners and studied rebel groups with a research team working alongside U.S. Army Special Forces.

Tactical Utility

How to turn AI hype into real-world results

The excitement about AI's potential often outpaces practical implementation. We've seen examples of companies eager to embrace AI that have faced significant issues—like biased AI recruiting tools that discriminate against women[1] and AI-powered diagnostic tools that give unsafe cancer treatment recommendations.[2] These problems highlight the risks of rushing into AI adoption without adequate planning, testing, and understanding.

While business leaders are optimistic about AI's potential—95% of senior leaders say their organizations are investing in AI[3]—these investments must align with organizational needs. Without strategic alignment, there's a risk of adopting technologies that don't address core issues, leading to unnecessary risks and complex mitigation efforts.

Start with the problem, not the technology

Align AI solutions to your specific challenges to ensure impactful results

Aligning AI investments with your specific challenges also ensures you're using AI effectively to enhance human capabilities rather than trying to replace them. For example, AlertMedia's Global Intelligence Team uses generative AI (GenAI) to streamline repetitive tasks, such as organizing global, constantly evolving sources. "We also use an internal AI system to sift through mountains of sources to identify business continuity and employee safety issues daily," explains Ben Schneider, Vice President of Product at AlertMedia. "Once we've narrowed in on every relevant source, on every open platform, across every global location—we still have to contend with an overwhelming amount of signals to isolate what matters. By pairing AI with human vetting, we've significantly shrunk an excessive timeline." This time savings allows the team to focus on high-stakes analysis and decision-making.

The following real-world applications illustrate AI's tactical utility in various fields:

Bridging skills gaps

86% of chief information security officers (CISOs) believe GenAI will help bridge security skills gaps and address talent shortages.[4] This sentiment reflects AI's potential to enhance existing security measures and alleviate the pressures of a shortage of skilled professionals.

Enhancing accuracy

American researchers have trained generative adversarial networks—advanced machine-learning algorithms—to spot discrepancies between sensor data and manual surveillance in nuclear power plants to improve anomaly detection and reduce human error.[5]

Improving public services

In the public service sector, state chief information officers (CIOs) are also exploring AI's potential, investigating how it can enhance human-centered design and better serve constituents.[6]

In the following Q&A, our experts offer practical advice on applying AI to address specific challenges. They'll guide you in identifying suitable problems for AI to tackle, optimize AI usage to enhance human capabilities, and use predictive analysis to drive efficiency. Their insights will help you ensure your AI investments are not just technology-driven but also aligned with your strategic objectives to deliver real, tangible value.

Aligning AI With Your Business Strategy

What should teams focus on when considering AI integration?

Ryan Mayfield

AI is not just one thing—it's a collection of many different tools. But some of the hype around AI can be overwhelming, making safety professionals think it's either a magic bullet or just more noise. Safety professionals need to get specific about what AI tools are essential to them and what problems they are trying to solve. **You need to lead with a problem to avoid bloatware.** For example, AI won't fix a leaking pipe during a crisis, but it can ensure the right person is in the right place at the right time. By focusing on how AI can augment our capabilities and improve efficiency, we can leverage its strengths effectively.

Karna McGarry

Efficiency is AI's premier selling point, but we need to dig deeper. Efficiency alone isn't a satisfying answer. Security practitioners should start by asking, "What specific challenges do we want AI to address?"

Answering that question involves identifying pain points, existing gaps, and areas where additional support is needed. From there, we can better understand how to integrate AI to provide the most value and support for security operations.

What are the most significant benefits AI can offer?

Joe Heinzen

AI's real value lies in its ability to augment and complement human capabilities in three specific ways: clarification, classification, and escalation. AI helps by clarifying complex data and providing actionable insights, classifying large volumes of information to accelerate threat identification, and automating the escalation of critical issues to ensure they are addressed promptly. By handling repetitive or data-intensive tasks, AI allows security professionals to focus on more strategic aspects of their work.

Shane Mathew

From a practical standpoint, **AI and language learning models (LLMs) act as force multipliers,** especially for small teams juggling numerous tasks. On a broader scale, companies can now feed large amounts of data into AI systems—not just the process data used by business continuity professionals—which has huge implications for supply chain optimization and overall efficiency. For example, trucking companies can use AI to monitor their fleets and predict when maintenance is needed. This means fewer equipment failures and smoother operations, which are major benefits for business continuity professionals.

How should teams get started with adopting AI?

Karna McGarry

When starting with AI, it's best to focus on areas where the tasks are straightforward and involve established patterns and rules. For instance, AI can be very effective in physical security tasks, such as analyzing camera feeds or supply chain metrics. However, AI should complement, not replace, analysts' expertise. AI tools should enhance your team's capabilities rather than take over their critical thinking. While AI can handle routine tasks, the value of human skills—like analysis and communication—is still essential. **Integrating AI means balancing its benefits with the continued development and use of your team's expertise.**

Shane Mathew

For teams looking to dip a toe into the AI waters, using LLMs to design tabletop exercises or create safety presentations is an easy, low-cost way to start. My advice for anyone new to AI is to learn how these models are developed, how to interact with them effectively, and how to distinguish between good and bad AI models. **By experimenting with AI in simple ways, you'll build familiarity and be better prepared when your company decides to invest more in AI.**

What are some practical ways teams can use AI?

Shane Mathew

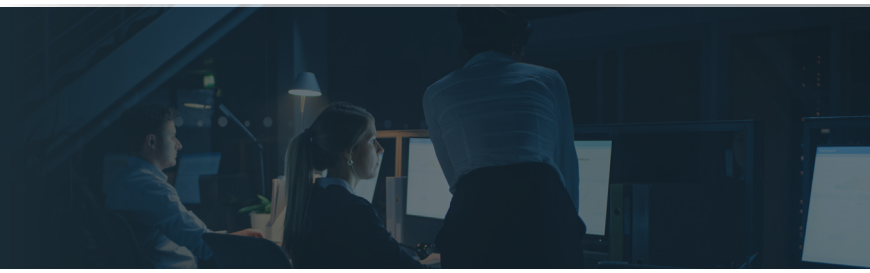
AI can change how business continuity teams operate by reducing the number, frequency, and size of incidents. Instead of being bogged down by routine problems like server outages, **AI can help us predict and prevent many of these smaller events, freeing up our time to focus on the bigger, unpredictable challenges**—like natural disasters—that really need our attention.

Joe Heinzen

AI can be used for predictive analysis, particularly in understanding the origins and seasonality of threats. Not all threats are black swan events like active shooter situations. Some, like mental health crises, follow seasonal patterns. **AI can help forecast these patterns, allowing teams to prepare for cascading effects and mitigate risks.** This not only helps in managing workloads and staffing but also addresses the critical issue of security specialist burnout.

"There's a lot we can do with AI, but we need to ask ourselves, 'What should we do?'"

— Joe Heinzen



WORKSHEET

Taking a Problem-Centric Approach to AI

This worksheet guides you in pinpointing the specific challenges and gaps in your operations so you can assess where AI might provide targeted solutions. This is just the start of a needs assessment to help focus your AI strategy. Continue to evaluate the problems that need solving to ensure that any integration is not simply about adopting new technology but also enhancing your team's ability to protect and secure.

Identify core challenges	What are the primary challenges we're currently facing?	Which of these challenges has the most significant impact on our operations?
Evaluate inefficiencies	Where are our current processes slow or inefficient?	What tasks consume the most time and resources?
Assess vulnerabilities	What are our most significant vulnerabilities?	Where do we see the most significant risk for errors or oversights?
Examine training and skill gaps	Are there gaps in our team's training that we could fill with AI?	Which skills are we lacking that could enhance our efforts?
Identify untapped opportunities	Are there areas in our operations where AI could create new opportunities?	What processes or tasks could be automated to free up human resources for higher-level work?
Evaluate adoption and governance needs	What are our security, privacy, and data protection requirements for integrating AI into our operations?	What resource limitations or constraints should we anticipate when adopting AI?

Risk & Mitigation

Approaching AI implementation with eyes wide open

Just as you wouldn't implement a significant business initiative without assessing potential pitfalls, AI deployment demands a strategic approach to risk management. Neglecting to address these risks can jeopardize operational integrity and security. With a structured approach to identifying and managing risks, you can harness AI effectively while maintaining high security and operational excellence standards.

So, what risks should you be mindful of when implementing AI?

Technical risks

Issues related to data quality, system reliability, and scalability issues have been linked to several high-profile AI failures.[7] For instance, shortcomings in AI incident reporting have exposed gaps in regulatory safety, demonstrating the need for rigorous technical oversight.[8]

Operational risks

Challenges related to integration, user adoption and over-reliance on AI all highlight the importance of managing operational risks. A recent survey found that 70% of CISOs are concerned that GenAI could give cyberattackers an edge, emphasizing the need for robust operational strategies.[9]

Ethical and legal risks

Managing risks related to bias, discrimination, and privacy is crucial when implementing AI. While 98% of CEOs agree AI could benefit their organizations, trust issues remain prevalent.[10] This uncertainty reflects broader concerns about AI's ethical and legal implications, including the need for transparency and accountability.

Strategic and competitive risks

When your AI strategy does not align with business strategy—a problem reported by 70% of executives[11]—it can undermine business performance and competitive positioning. Ensuring that AI initiatives are closely integrated with your overall strategy is essential.

Reputational risks

Failures or adverse outcomes associated with AI can damage your organization's reputation. Since public scrutiny of AI technologies is a growing issue—90% of all criticisms toward AI have taken place since 2018[12]—it's essential to have a strategy to manage and mitigate these risks proactively.

Security risks

Concerns arise when employees unintentionally upload sensitive data to AI platforms, risking data leakage. Since 31% of employees acknowledge having entered sensitive information into AI tools,[13] implementing robust cybersecurity measures is vital to prevent unauthorized access and misuse of AI.

Social and cultural risks

AI can impact employees and organizational culture. From resistance to change to fear of job displacement by AI—a concern felt by 60% of workers[14]—these issues can hinder the successful adoption of AI technologies.

Financial risks

The costs of implementing AI and the uncertainty around its ROI are vital concerns. Although 32% of executives acknowledge that measuring the business impact of AI is a challenge,[15] it's critical to carefully manage costs and assess ROI to ensure AI investments deliver sustained value.

With our experts' insights, you'll gain a deeper understanding of the considerations and risks to address before implementing AI. In the Q&A that follows, they explore how to balance AI and human expertise, manage AI's role in high-pressure scenarios, and ensure AI deployments enhance rather than replace critical skills. Their advice will help you navigate AI deployment risks, aligning your investments with strategic goals while maintaining operational integrity and security.

EXPERT INSIGHTS

Balancing **AI Risks and Rewards**

What makes you the most anxious about advancing AI technologies?

Dr. Maaz Amjad

AI is providing many new opportunities but also introducing new problems we need to consider. **Bad actors are equally empowered by AI technology and can use those infrastructures to create new business threats.** AI can be a force multiplier—for both good and bad—so we need to understand these risks and how to mitigate them.

Karna McGarry

My main concern is the push for efficiency and quickness for that sake. It's especially risky when looking at threat monitoring, particularly social media. For instance, if an AI tool flags an online post as threatening, it might not grasp the context, syntax, or even the latest use of emojis or slang. Without understanding these nuances, the AI could mistakenly escalate a situation, wrongly identifying someone or a group as a potential threat when there's no real danger. **These errors can lead to unnecessary alerts and false alarms, which can cause more harm than good.**

What are the risks and limitations of relying on AI during high-pressure situations?

Shane Mathew

We have to consider a few things when using AI in pressure-sensitive situations. The first is data quality—**AI systems can provide you with results that are only as good as the data they're founded on.** For example, some of the older models of ChatGPT were based on data up until just 2021. Then it became 2023, but still, it's not real-time. So that's one intrinsic challenge with these models—that they often don't have the latest and most relevant data available for them to make decisions.

AI can't be programmed to handle every ethical nuance. You can't program ethics for every situation into a computer at this point. As much as we might say AI can reason, that reasoning is based on the inputs it was given. All of that said, expecting AI to deliver real-time decision-making accuracy is risky. While its potential is immense, you can't circumvent human oversight and scrutiny.

"AI can be a force multiplier —for both good and bad—so we need to understand these risks and how to mitigate them."

—Dr. Maaz Amjad

What are the most significant weaknesses of AI tools for safety and security?

Dean Baratta

One of AI's most significant weaknesses is its tendency to hallucinate or make things up. That's a massive concern, especially when putting together something as critical as an event or executive protection plan where fabricated data could lead to disastrous outcomes. Beyond that, AI can stifle creativity and insight if not integrated thoughtfully. **LLMs are excellent at processing and analyzing the data they've absorbed but fail to generate new, innovative ideas.**

For instance, I recall a time back in 2010 when my team was trying to estimate the number of gang members in New Jersey. We struggled with the available data until I randomly stumbled upon a public access channel discussing how researchers estimate deer populations. Their method sparked an entirely new approach for us—something that would never have occurred if we were relying solely on an AI model. LLMs can't escape the boundaries of what they know. They don't make those creative leaps that human minds do, so it's crucial to ensure human insight remains a core part of our processes.

What ethical issues arise when deploying AI in scenarios directly impacting people's health and safety?

Dr. Maaz Amjad

In critical situations, such as a mass casualty event with limited resources, AI's role in deciding who gets treated first is complex and time-sensitive. If an AI model that was developed on specific data points—say, tailored to a particular demographic—fails to account for other groups, it might not work effectively.

For example, there was a case where a computer vision model designed for a white population was later applied to a Black population, leading to a wrongful extended detention because the police officers lacked proper training on how to interpret the model's outputs. This story highlights that **AI is still a tool, and the real concern lies in who is using it, how they are using it,** and how that information influences decision-making processes.

Are there any risks associated with over-reliance on AI?

Shane Mathew

Over-reliance on AI definitely comes with risks. One of the biggest issues is the potential for basic computational errors. **There's a tendency to think that because it's a computer, it must always be right.** But I've used tools where even simple errors slip through, and if you're not keeping a sharp eye on the output and double-checking it, you could miss those mistakes. Sometimes, it's not even the tool itself but issues like an algorithm error or a processing glitch. Without human oversight, these errors can go unnoticed and cause real problems.

Karna McGarry

The danger with over-relying on AI is falling into a mindset of "good enough." It's similar to how we've rewired our brains by constantly relying on the internet for quick answers—we're not truly absorbing or handling the knowledge. In security, you always need to be anticipating and questioning, and your best analysts are the creative ones. I don't see the value in taking that experience away from them. It's crucial to identify gaps in training and ensure that from a management standpoint, we're emphasizing the importance of how information is written and organized.

While AI tools have their place, they should never replace the human element, especially for newer practitioners who still need to build those foundational skills. The next generation of leaders will have only the skills and experience they've developed, so we need to focus even more on internal training.

"Think of working with AI tools like sculpting a clay statue. The data you feed into the AI is like the clay itself—the raw material. If the clay has impurities or debris, the statue is hard to work with and, ultimately, flawed. Likewise, you can ***mitigate risk by making sure you start with clean, integral data and a solid foundation of human oversight."***

—Shane Mathew

TEMPLATE

Evaluating and Managing AI-Related Risks

As your organization adopts AI solutions, you need a plan to incorporate related risks into assessment, mitigation, and monitoring processes. Use this worksheet to examine a problem and/or solution related to artificial intelligence. Consider your risk tolerance, the degree of oversight that still nets efficiency, and areas where you must have a human in the loop.

Core Challenge:

AI Solution:

Risk Analysis

Risk Type	Description	Likelihood (1–5)	Impact Level (1–5)
Operational			
Financial			
Brand / Reputational			
IT / Technical			
Ethical / Legal			
Strategic / Competitive			
Security			
Social / Cultural			

Mitigation Controls

Technological	Human	Process

Human Oversight

Key Personnel	Oversight Process

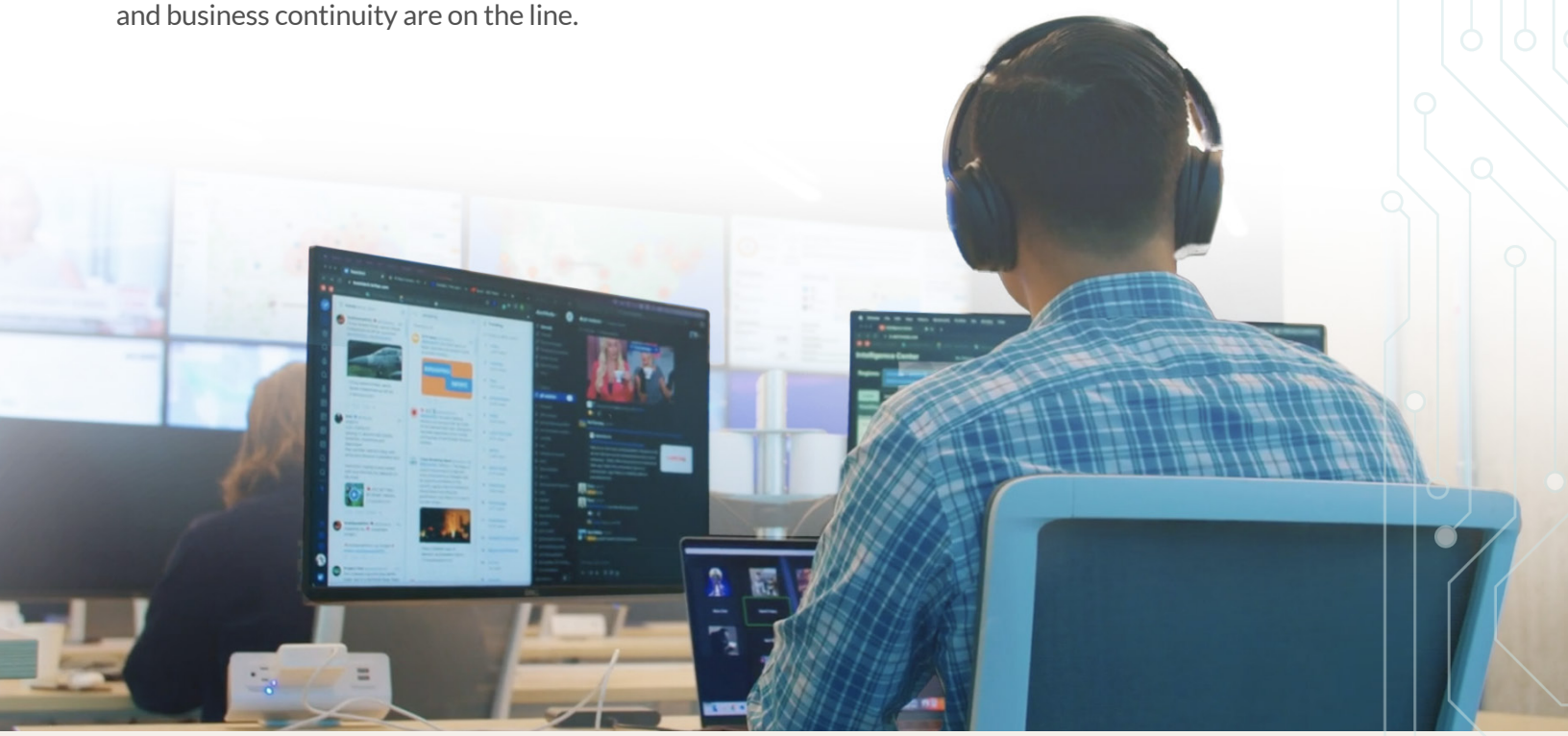
Human Involvement

The critical role of human oversight in AI implementation

Finding the right balance between human and artificial intelligence is essential in protecting employees, facilities, assets, and operations. Adopting new technology is just one small step toward building and maintaining an ecosystem that promotes and enhances human expertise.

Think of AI as a ship's high-tech navigation system. It processes large amounts of data, identifies patterns, and helps spot potential hazards. But it still needs a captain to steer. Humans provide the critical oversight AI lacks. We're responsible for programming, setting and enforcing policies, generating prompts, and quality assurance. When AI suggests a course of action, it's up to us to evaluate and implement it—especially in high-stakes situations.

While AI excels at repetitive tasks and data analysis, it lacks the critical thinking and ethical judgment only humans can drive. Human involvement remains indispensable during critical events when safety, security, and business continuity are on the line.



In the following Q&A, our panel of experts explores the nuanced interplay between human expertise and AI in security operations. Firm in their beliefs that AI should enhance, not replace, human judgment, they highlight the importance of continuing to develop your team's skills alongside AI adoption. You'll learn how to use AI to support less-experienced staff, how it can offer consistency during high-stress situations, and the training security teams should undergo to work alongside AI systems most effectively.

A Blueprint for **Human-AI Collaboration**

How do you navigate the uncertain boundary between human and machine roles?

Dean Baratta

There is still a lot of untapped potential within humans. People coming into the field right now have so much capacity. And one of the things I want to make sure we don't do is push them to the side to put our time and effort into this shiny new thing. **So oddly enough, even though AI is heralded as something that will save time and give us more flexibility, I think we actually have to spend more interpersonal time with our staff**—especially with the new generation coming in. We need to mentor them and make sure they develop that full set of analytical communication and professional skills so that they can be those super-powered security professionals they should be.

How do you balance leaning on AI with developing your people's skills?

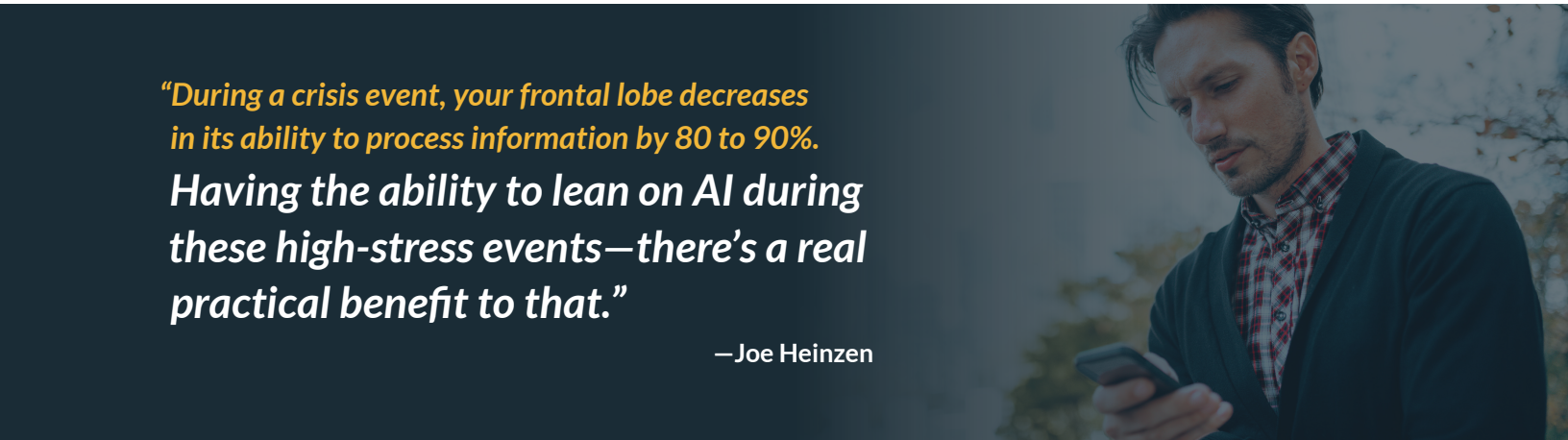
Karna McGarry

Focus on maximizing the potential of your current workforce before turning to AI. Rather than viewing AI as a means to cut costs, start by developing and training the people you already have. Many teams are surprisingly small, and often, inefficiency stems from underutilized personnel who aren't fully trained in core skills like writing and critical thinking. Once your team is well-prepared and aware of their needs, then look for AI tools to complement their work. Instead of jumping straight to new technology, understand your team's challenges and pain points first. AI should be an enhancement, not a replacement, and should be chosen based on how well it meets the actual needs of your team.

"During a crisis event, your frontal lobe decreases in its ability to process information by 80 to 90%.

Having the ability to lean on AI during these high-stress events—there's a real practical benefit to that."

—Joe Heinzen



How can AI be used to augment human capabilities?

Joe Heinzen

AI can play a significant role in what I call "repetitive compliance." **Integrating AI into training exercises helps reinforce consistent behaviors among security personnel.** This consistency of response is essential in crisis events, where multiple studies have shown that our frontal lobe's ability to process information can drop by 80 to 90%. Having AI support during these high-stress events offers a practical benefit—ensuring security teams can rely on structured tools to maintain effective responses.

Ryan Mayfield

When high turnover affects a security team, the experience levels of personnel can vary widely. A professional with 20 years of experience might instinctively know what questions to ask if they hear gunshots, for example—while somebody new to the job could benefit from AI tools that provide prompts and investigative steps. **Although AI can't fully replace human decision-making, it can guide less-experienced staff and escalate issues to the right experts when needed** to prevent "crying wolf" scenarios. In this way, AI can help lower-level personnel manage incidents more effectively, preventing unnecessary false alarms and ensuring specialists are reserved for genuine emergencies.

What training should security and business continuity professionals undergo to work alongside AI systems effectively?

Shane Mathew

Start by building a solid foundation in data literacy and basic AI principles. Take advantage of the wealth of free online resources, such as courses from Udemy. Understanding the fundamentals of AI and data analysis is crucial. Hands-on practice is also essential. And don't be afraid to make mistakes—that's a vital part of the learning process. **Experiment with AI tools, refine your prompts, and use feedback to improve. The goal is to become comfortable and proficient, like learning to ride a bike.** By focusing on these foundational elements and gaining practical experience, teams can learn how to integrate AI into their workflows better.

Karna McGarry

We have to focus on fundamental analytical skills like vetting and validating sources. Just because AI tools ingest data doesn't guarantee the data is real or accurate. For instance, one thing I ask my analysts is: If you're doing a social media scrub and you have all these comments, how do you know they're actually from a person or multiple people and not from a chatbot that keeps rolling? How are you going to vet and validate that? How are you going to test it?

It's tempting to rely on technology to do that work for us, but it's crucial to verify whether these come from real people or automated sources by cross-checking them with authoritative sources like government press releases or official websites. **Training should focus on developing investigative skills, best practices for validating data, and regularly re-engaging these core skills.**

A Glimpse Into
AI Policy Development at AlertMedia

On some level, everyone in an organization is responsible for mitigating risks associated with AI. As use cases expand, the sooner you establish boundaries and expectations for acceptable use, the better.

Here, our Vice President of Security & Compliance, Matt Ray, describes how we've approached AI policy development at AlertMedia.

Matt Ray
Vice President of Security & Compliance, AlertMedia

Why we took action

Recognizing the clear and significant impact of AI, our leadership team was eager to understand its potential benefits for both our company and our customers. From there, we could clarify our intentions and establish meaningful policies around use cases. Like most organizations, we knew we already had employees using generative AI tools, at the very least, so we needed to establish guardrails as quickly as possible.

How we did it

We started a GenAI taskforce, pulling together leaders from across the company. Policy writing in a bubble makes for policies that don't fit the whole company. So, we sought to understand how different teams—marketing, sales, engineering, etc.—were thinking about and using AI. This way, we could align on the right tools, get licensed, and establish clear, company-wide practical guidelines that make sense for everyone.

What the policy includes

According to our official AlertMedia policy, "The first rule of GenAI is: 'Human in the Loop.' The second rule of GenAI is: 'Human in the Loop!'" In other words, the use of AI is acceptable only when the user is situationally aware and thinking critically. In the policy, we've outlined approved tools, data security reminders, an incident response process, and an evaluation process for potential new tools and use cases.

What's next

We're staying cautious and continuously updating our guardrails to adapt to new security challenges and use cases. Our focus remains on using AI responsibly while safeguarding the trust our customers place in us.

AlertMedia

Setting Up a Human-in-the-Loop System

Ensure that AI enhances rather than compromises safety, security, and business continuity. Following these steps will help you strike the right balance between automation and human oversight so that artificial intelligence is a reliable partner in decision-making and risk management.

1 Define clear objectives

- Conduct assessments to identify where AI can enhance existing systems.
- Set measurable and realistic goals that align with broader organizational priorities.

2 Establish a company policy for AI use

- Outline acceptable AI use, including privacy, transparency, and security standards that meet regulatory requirements.
- Communicate the policy throughout the organization.

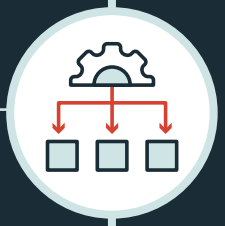
3 Develop ethical and compliance guidelines

- When drafting guidelines, address bias, fairness, and the potential for unintended consequences.
- Implement a compliance monitoring system to ensure ongoing adherence to procedural and ethical standards.

4 Establish accountability and governance

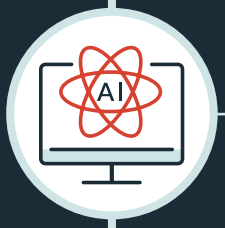
- Define clear roles, responsibilities, and oversight mechanisms to maintain control over AI systems.
- Set up an AI governance committee with IT, security, compliance, and operations representatives.

5 Design the workflow



- Map the interactions between AI systems and human operators, pinpointing where human intervention is critical.
- Create workflows for easy escalation to human operators in case of anomalies or uncertainties.

6 Develop the interface



- Create user-friendly tools that enable employees of varying technical expertise to interact effectively with AI systems.
- Include features for operators to override AI decisions when necessary and provide feedback on AI performance.

7 Implement threat monitoring and alerts

- Set up AI-driven monitoring systems to detect unusual patterns or behaviors.
- Configure alert systems to notify human operators of threats, providing contextual information to support decision-making.

8 Train and empower human operators

- Develop comprehensive training to ensure operators can confidently intervene and make decisions.
- Cover both the technical aspects of the workflow and the critical-thinking skills to assess AI outputs.

9 Plan for continuous improvement

- Establish a feedback loop for reporting issues and opportunities.
- Schedule periodic audits to assess compliance.
- Foster a culture of innovation and collaboration.

Framework for AI Success: **Key Strategies and Insights**

Drawing from these discussions with our experts, **we've developed a three-step framework for AI integration** that balances practical and strategic considerations:

1

Start with a problem-centric approach

Clarify organizational needs and target specific challenges with AI solutions

2

Reassess risk and realign strategies

Regularly update your risk profile and mitigation strategies with AI considerations

3

Establish human-in-the-loop systems

Integrate human oversight and AI capabilities to enhance operations

We spoke with Sara Pratley, Vice President of Global Intelligence at AlertMedia, to understand how this framework can be applied in the real world.

Sara Pratley
Senior Vice President of Global Intelligence, AlertMedia

Can you tell us about your Global Intelligence Team and some of its challenges?

Our team is made up of intelligence professionals and experts with diverse experiences spanning both the public and private sectors. Our collective focus is helping the 3,500+ organizations we serve to mitigate risk and improve safety for their employees. Our team operates around the clock, collecting and analyzing threat data 24/7/365.

Given the vast number of sources today and the volume of information flowing from those sources, we need a way to filter out irrelevant data—without compromising our ability to capture the threats that do need our attention. Technological solutions are essential for managing this flood of data while optimizing our analysts' time and expertise.

With a close look at the team's problems, what solution were you able to identify?

The sheer volume of open source intelligence (OSINT) data hampers both speed and scalability. ***We want our analysts focused on strategic, value-added activities, not bogged down by endless data feeds.*** And while many aggregator tools exist, those tools don't give us complete control of the data going in and coming out. We need control of the funnel so we're confident that we're seeing everything, the outputs are valid, and there aren't gaps.

With full command of the data inputs and criteria for flagging threats for analysis, an AI tool like this can save our analysts significant time. It enables them to focus and investigate critical events and threats rapidly and inform our impacted customers. So, we decided to make our own AI-powered platform for intelligence gathering.

How do you balance the risks involved with using artificial intelligence?

Before developing our homegrown solution, we used external AI tools, such as LLMs, to collate and categorize incoming data from thousands of sources. This approach allowed us to complete tasks in hours that would have taken weeks or months and demonstrated that AI could outperform human error rates in certain routine tasks.

Many of the risks of external AI—hallucinations, bias, and confidential data inputs—prompted us to develop an internal solution. The models are only as good as the data that informs them, so we focused on generating high-quality data to yield productive algorithms. Our developers partnered with analysts to understand how they handle data, which helped in training the tool to act on diverse inputs.

The system, now fully functioning, is exclusively trained by our team to minimize external biases. However, risks of hallucinations and biases from OSINT data remain, so a human will always be involved. The system's insular nature also enhances explainability, helping us better understand and trust its decisions and outputs.

The algorithm identifies patterns and summarizes events, but our team members validate the outputs, assess, and analyze the impacts. ***Of course, there's still the risk that the models aren't reporting on everything we need them to at any given time,*** so our analysts continuously monitor a range of threat detection tools to ensure no critical information is overlooked.

What does the human-in-the-loop ecosystem look like at AlertMedia?

The AI-powered system acts like the top of the funnel, vacuuming from sources like RSS, social media, news media, and threat intelligence feeds. It categorizes incoming content—whether related to weather events, acts of violence, transportation disruptions, or something else—and assesses its threat level with a confidence score. This is a measurable way we can keep training the system to get closer to human insights.

Analysts then review and analyze the AI's outputs. The tool has identified high priorities, so the analyst may start with those reports to do a deep dive. They'll ask, "Is this threat real? What is its extent?" and write more detailed and thorough content after applying their analysis. They can also access the algorithm's 0%-confidence list of inputs to ensure they aren't missing any threats.

Not only is there a human in the loop—there is a human in control. The loop involves ongoing model training, with analysts correcting misinterpretations and expanding the AI's understanding of language and context. Maintaining data integrity is our primary concern for the system's progress.

We continually refine the type, amount, and quality of data used for training. We iterate on how we ask questions of the models. We give context about how the tool should answer a question as if it were a global threat analyst.

As we continue to evaluate our own outputs, we also conduct after-action reports to understand where we can find information faster, and this weighs heavily into adding sources and changing criteria for the AI. ***The tool's success relies on continuous human guidance to direct its existence, purpose, and limits.***

How can industry collaboration promote responsible AI adoption for a safer, more resilient world?

As a company, we believe that AI can be beneficial for our functions when humans are involved. The more people with shared goals who can come together to promote responsible AI adoption, the more grounded human involvement we have to usher these powerful ecosystems into the future.

Begin with the three-step framework to align with business needs and problems to solve. Then, reevaluate your risk profile to consider AI's role as a threat and potential mitigation control. Engineer any artificial intelligence to depend on the human's influence even as it helps to maximize the human's capacity.

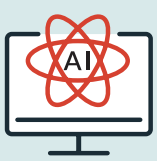
At AlertMedia, we are transparent about our AI practices. We engage with customers and industry peers to align our solutions with their needs and learn from their experiences. Through these discussions, by participating in industry conferences, and by publishing this collection of interviews, we aim to contribute to a landscape that strengthens organizational resilience and promotes thoughtful AI integration.

Embracing AI: A Balanced Perspective

AI has the potential to be a transformative tool for protecting people and business operations. But its impact is not inherently positive or progressive—it can tip the scales in either direction. The effectiveness of AI solutions depends heavily on the humans operating them and teaching them to adapt. Each prompt or data input leaves an impression. By developing a clear plan for balancing innovation with responsible stewardship, our actions and influence are purposeful.

This technology is uncharted territory, and we're all navigating it together. As we chart this course, we must work collectively to ensure AI makes a profound and positive impact on safety, security, and business continuity.

This is not the end but the beginning of an ongoing conversation—one that will evolve alongside technological advancements, driving real and meaningful progress.



Join the Conversation Now

Share your insights and experience on LinkedIn

#TheAIEdge

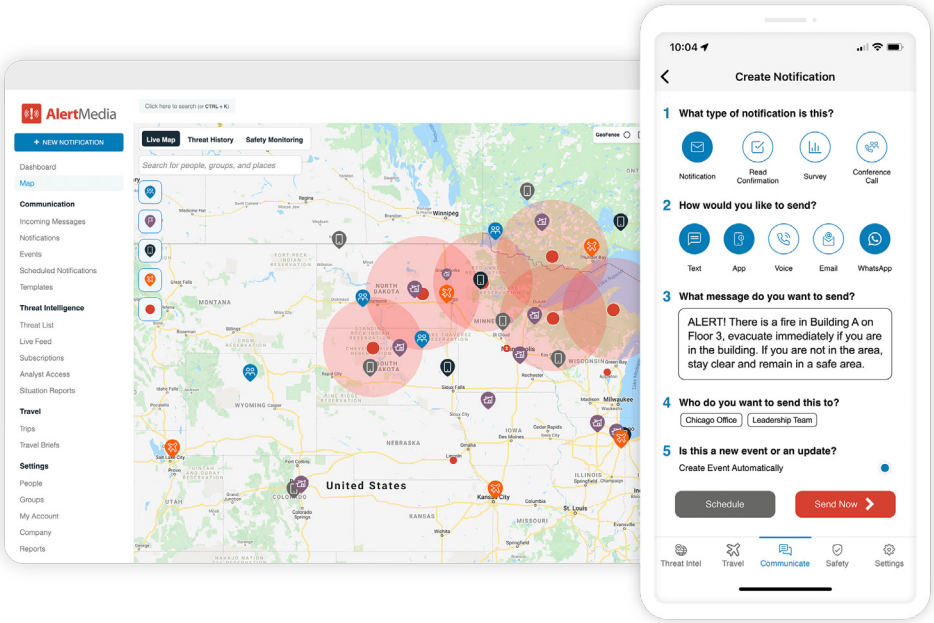
AlertMedia

An Intelligence Solution You Can Trust

AlertMedia is the only solution that integrates analyst-vetted threat intelligence with reliable emergency communication and travel risk management capabilities to help you achieve 24/7 situational awareness.

Our in-house analysts work around the clock to monitor thousands of data sources, filter out the noise, and deliver only the most relevant view of events that may impact your employees and operations.

Schedule a personalized tour to see if AlertMedia is the right solution for your business.



Trusted by thousands of world-class organizations

LEARN HOW YOU CAN IMPROVE ORGANIZATIONAL RESILIENCE WITH ALERTMEDIA

SCHEDULE A DEMO

sales@alertmedia.com // (800) 826-0777 // alertmedia.com

Footnotes

1. Dastin, J. (2018, October 10). Insight - Amazon scraps secret AI recruiting tool that showed bias against women. Reuters. https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/.

2. Chen, Angela. (2018, July 26). IBM's Watson gave unsafe recommendations for treating cancer. The Verge. https://www.theverge.com/2018/7/26/17619382/ibms-watson-cancer-ai-healthcare-science.

3. EY. (2024, July 15). New EY research finds AI investment is surging, with senior leaders seeing more positive ROI as hype continues to become reality [Press release]. https://www.ey.com/en_us/newsroom/2024/07/new-ey-research-finds-ai-investment-is-surging-with-senior-leaders-seeing-more-positive-roi-as-hype-continues-to-become-reality.

4. Splunk. (2023). The CISO Report. https://www.splunk.com/en_us/campaigns/ciso-report.html.

5. Gursel, E., Reddy, B., Khojandi, A., Madadi, M., Baalis Coble, J., Agarwal, V., Yadav, V., Boring, R. (2023, February). Using artificial intelligence to detect human errors in nuclear power plants: A case in operation and maintenance. Nuclear Engineering and Technology. https://www.sciencedirect.com/science/article/pii/S1738573322005137.

6. Knell, N., & Kinkade, L. (2024, July/August). What Does AI Mean for Human-Centered Design? Government Technology. https://www.govtech.com/artificial-intelligence/what-does-ai-mean-for-human-centered-design.

7. Olavsrud, T. (2024, April 17). 10 Famous AI Disasters. CIO. https://www.cio.com/article/190888/5-famous-analytics-and-ai-disasters.html.

8. Leyden, J. (2024, July 1). AI incident reporting shortcomings leave regulatory safety hole. CIO. https://www.cio.com/article/2510708/ai-incident-reporting-shortcomings-leave-regulatory-safety-hole.html.

9. Splunk. (2023). The CISO Report. https://www.splunk.com/en_us/campaigns/ciso-report.html.

10. Workday. (2023, September 14). Workday Global Survey: 98% of CEOs Say Their Organizations Would Benefit from Implementing AI, But Trust Remains a Concern [Press Release]. https://newsroom.workday.com/2023-09-14-Workday-Global-Survey-98-of-CEOs-Say-Their-Organizations-Would-Benefit-from-Implementing-AI,-But-Trust-Remains-a-Concern.

11. Mitchell, Sean. (2024, May 24). Executives trust AI but struggle with strategy alignment says survey. CFOtech UK. https://cfotech.co.uk/story/executives-trust-ai-but-struggle-with-strategy-alignment-says-survey.

12. Holweg, M., Younger, R., Wen, Y. (2022, January 24). The Reputational Risks of AI. California Management Review. https://cmr.berkeley.edu/2022/01/the-reputational-risks-of-ai/.

13. Yu, E. (2024, February 22). Employees input sensitive data into generative AI tools despite the risks. ZDNET. https://www.zdnet.com/article/employees-input-sensitive-data-into-generative-ai-tools-despite-the-risks/.

14. Accenture. (2024, January 16). Accenture Report Finds Perception Gap Between Workers and C-suite Around Work and Generative AI [Press Release]. https://newsroom.accenture.com/news/2024/accenture-report-finds-perception-gap-between-workers-and-c-suite-around-work-and-generative-ai.

15. McCann, D. (2024, May 29). 40% of executives say AI not ready to achieve accurate outcomes: Report. CFO. https://www.cfo.com/news/artificial-intelligence-not-ready-teradata/717261/.