PROFILES IN *Confidence*

BRADLEY SCHAUFENBUEL

VP and CISO
Paychex

Headquarters: Rochester, NY

Employees: 19,000+

Annual Revenue: $5.57 Billion

Bradley Schaufenbuel has served as Vice President and Chief Information Security Officer at Paychex for over six years, where he leads the company's global cybersecurity strategy. With a career rooted in financial services and strong security leadership, Bradley brings a pragmatic approach to protecting the business.

At Paychex, Bradley operates at the intersection of innovation and risk, helping the organization adopt new technologies such as artificial intelligence while maintaining strong governance and resilience. His leadership reflects a broader shift in the role of the modern CISO, one that requires balancing speed and business enablement in an environment defined by constant change.

MANAGING RISK IN A CONSTANTLY CHANGING ENVIRONMENT

For Bradley, uncertainty is not new, even as the pace of change accelerates. "The pace of change in the cybersecurity field is accelerating, but we have not changed the way we manage uncertainty," he explains. At Paychex, this discipline is embedded into daily operations. "We hold a daily standup in our Cyber Fusion Center where we review economic and geopolitical events and their potential impact on the cybersecurity landscape."

When risk levels shift, the response is immediate and deliberate. "If the risk posed by these changes is material, we then take proactive steps to mitigate those risks," he says. Recent geopolitical events have required rapid adjustments. "The Iran conflict is the latest example of that. We immediately raised our cyber threat level, which meant putting more eyes on glass in our security operations center, focusing threat hunts on techniques used by Iranian APT groups, and accelerating the SLA for remediation of critical vulnerabilities."

BALANCING COST, RISK, AND INNOVATION

"Security budgets are tightening," he says. "There is the expectation that the adoption of AI will drive productivity improvements that will lower costs."

At the same time, expectations continue to rise. "CISOs are also being asked to defend their organization against an accelerating volume of attacks that are AI-driven as well as to govern and secure their organizations' adoption of AI," he explains. This dual pressure is forcing leaders to rethink how they allocate resources. "You end up consolidating existing tools to free up capital to adopt tools that address new threats. It is a delicate balancing act."

AI AS THREATS AND ADVANTAGES

Bradley views AI as a defining force for the future of cybersecurity. "AI is proving to be transformational to both attackers and defenders," he says, "Attackers are already leveraging AI to automate their attacks and improve the sophistication of those attacks."

AI is changing the nature of identity-based attacks. "AI is also being leveraged to generate deepfakes that are driving up the success rate of phishing and social engineering techniques and defeating authentication systems."

At the same time, defenders are using AI to improve their own capabilities. "Defenders are leveraging AI to detect and respond to cyber-attacks faster and to automate the work of defenders," Bradley explains. At Paychex, these use cases are already operational. "We are using AI agents to automate alert triage, alert data enrichment, and investigative processes in our security operations center, which has allowed us to significantly reduce our meantime to respond to cyber-attacks."

Looking ahead, he sees an ongoing race between attackers and defenders. “It will continue to be a cat-and-mouse game between attackers and defenders, with each racing to adopt leading edge technology to advance their respective aims.”

ENABLING AI WHILE GOVERNING IT RESPONSIBLY

As AI adoption accelerates, the business is moving quickly and looking to security for guidance. “The question the business is asking me and most of my peers right now is ‘How can we adopt AI quickly, but also safely and responsibly?’” Bradley says.

The stakes are high. “Most businesses see its adoption as essential to their survival,” he explains. “Non-adoption or slow adoption of AI is seen as an existential threat.” This urgency changes the role of the CISO. “CISOs do not really have the option of saying no to AI or following a slow and methodical process to get to yes.”

Instead, the focus is on enabling adoption with strong guardrails. “They need to have a clear strategy for governing and securing AI, and the timeline for the execution of that strategy must be short.”

At Paychex, that strategy is formalized through a cross-functional governance model. “We assembled an AI Governance Council that includes all lines of defense,” Bradley explains. “That body generated an AI ethics policy that sets forth broad principles for the responsible adoption and development of AI.”

Governance extends beyond policy into execution. “The AI Governance Council reviews and approves every AI use case,” he says. The organization is also implementing technical controls to support that oversight. “We are also evaluating or putting into place tools to govern and secure AI applications, like LLM and MCP gateways that enforce guardrails around the actions of AI agents, automated AI red teaming tools, and dedicated instances of AI applications to avoid data leakage.”

SCALING SECURITY THROUGH AI AND AUTOMATION

AI is also helping Bradley address one of the most persistent challenges in cybersecurity: scale. “We have already developed AI agents for alert triage, alert data enrichment, and investigative tasks that have allowed us to shift tier one SOC analysts to higher value security work,” he says.

The team is continuing to expand these capabilities. “We are in the process of designing or developing AI agents to perform vulnerability triage work, identity and access management tasks, and penetration testing and red teaming.”

These investments are not about reducing headcount, but about enabling growth without adding friction. “These investments in AI are designed to allow us to keep up with a growing volume of work without expanding the size of our team.”

CONTINUOUS MONITORING AND CONTROL OF AI SYSTEMS

Once AI systems are deployed, maintaining visibility and control is critical. “We are building most of our AI agents, generative AI applications, and machine learning applications on platforms that generate detailed operational telemetry,” Bradley explains.

That data feeds directly into existing security operations. “That telemetry is being ingested into our security event and information management system, which is monitored around the clock for anomalous activity by our cyber fusion center.”

He also emphasizes the importance of identifying unsanctioned usage. “We have systems in place for discovering all AI models, MCP servers, AI agents, and AI applications, and alerting us to any unsanctioned AI in our environment.”

Advanced protections are also being implemented to address emerging attack vectors. “We have put in place technology that detects prompt injections, model poisoning, and other real time attacks on AI applications and blocks malicious behavior.”

ALIGNING SECURITY WITH BUSINESS OUTCOMES

Bradley anchors his program in widely recognized frameworks to ensure consistency and credibility. “We align our overall cybersecurity program with the NIST Cybersecurity Framework as well as the ISO 27001 standard,” he says.

This structured approach also supports executive communication. “This allows us to communicate to the executive team that we have adopted industry best practices, and we are either doing that well, or there is room for improvement.”

Beyond AI, his priorities reflect a broader business alignment. “Some areas of focus for us over the next 18 months are improving the cyber resilience of our organization, enabling the business to monetize its data assets while preserving the privacy and security of individual employees and customers, and creating a new source of revenue for the company.”

ADAPTING TO WHAT COMES NEXT

For Bradley, the defining challenge ahead is not any single technology, but the pace of change itself. “What will matter most in cybersecurity over the next 12 to 18 months is the ability of cybersecurity teams to innovate quickly and rapidly adapt to a technological environment and a threat landscape that are changing at an ever-increasing pace,” he says.

His perspective is grounded in a simple but powerful principle. “As Charles Darwin said, it is not the strongest that survive, but those that best adapt to change,” he notes. “You are either going to embrace change or become a victim of change.”