JS|HELD

PERSPECTIVES

Top Ten Strategic Advantages of a vCISO with AI Expertise for Developing Business and Protecting AI Applications

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

Copyright © 2025 J.S. Held LLC, All rights reserved.

INTRODUCTION

In today's fast-paced digital landscape, Artificial Intelligence (AI) is reshaping industries, unlocking new efficiencies, and enabling transformative business models. Companies leveraging AI to create applications or enhance their business practices are at the forefront of this technological revolution. However, as businesses innovate and integrate AI into their operations, they face unique cybersecurity, privacy, and ethical challenges that require specialized expertise. This is where a virtual Chief Information Security Officer (vCISO) with experience in cybersecurity, risk management, compliance frameworks, AI development, and governance becomes invaluable.

As businesses race to develop AI-driven solutions or embed AI into their processes, the risks associated with cybersecurity grow exponentially. From protecting proprietary AI algorithms to securing the vast amounts of data AI systems require, businesses need a tailored cybersecurity strategy that understands both the complexities of AI and the nuances of modern security threats.

In this article, we'll explore the distinct advantages of having a vCISO with AI expertise on your team and how it can position your company for success, all while maintaining robust cybersecurity protections.

1. SAFEGUARDING PROPRIETARY AI TECHNOLOGY

AI is a highly valuable asset for companies - whether it's a proprietary algorithm, a machine or language learning model, generative AI, or an AI-driven product. The development of AI applications involves the creation of intellectual property that is critical to a business's competitive advantage. If this proprietary technology is compromised, it could lead to catastrophic consequences, including loss of business, intellectual property theft, and legal exposure.

A vCISO with expertise in AI risk management understands the unique threats to AI technologies and how to mitigate them. With deep knowledge of machine learning models and neural networks, a vCISO can design security systems that protect sensitive AI systems from hacking, reverse engineering, or misuse. This ensures your organization can innovate freely without fearing the theft or exploitation of its most valuable technologies.

2. MITIGATING AI-SPECIFIC SECURITY THREATS

Unlike traditional cybersecurity threats, AI applications often present new and evolving risks. These include adversarial attacks, where malicious actors manipulate data to confuse AI models. Another threat is data poisoning, which is an attack or inadvertent issue where corrupted, misleading, or biased data is introduced into a system, compromising the integrity of machine learning models or analytics. For example, a bad actor injects misleading data into a training set (e.g., spam attackers feeding fake "ham" emails to an anti-spam filter, making it misclassify actual spam). Another case might be inadvertent poisoning where poor data collection or faulty labeling leads to biased or inaccurate models (e.g., a facial recognition system trained on a non-diverse dataset, causing biased predictions).

Both cases can degrade model performance, introduce security risks, or lead to incorrect decision-making.

One such example of mitigating AI-specific security threats is Microsoft's efforts to combat adversarial attacks on its AI models. In 2020, Microsoft partnered with MITRE to develop the Adversarial ML Threat Matrix, a framework that helps organizations identify and mitigate security vulnerabilities in AI systems. One notable case involved Microsoft enhancing its Azure AI services to detect and defend against adversarial attacks, where attackers manipulated input data to deceive AI models.

For businesses developing AI solutions, these risks are compounded by the complexity of the AI systems themselves.

Copyright © 2025 J.S. Held LLC, All rights reserved.

A vCISO with experience in AI can assess these unique threats and implement targeted strategies to mitigate them. This expert can ensure the AI models – and the underlying infrastructure – are effective against these sophisticated attacks by leveraging AI-driven security systems, conducting rigorous vulnerability assessments, and establishing real-time threat detection measures. With a proactive AI-centric security approach, your business can safeguard its AI investments from the ground up.

3. ENSURING DATA PRIVACY AND COMPLIANCE IN AI PROJECTS

AI systems often require vast amounts of data to function, and this data may include sensitive information such as personal identifiers, proprietary business data, and intellectual property. This creates significant concerns regarding data privacy and regulatory compliance, particularly as new data protection regulations—such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA) in the US—are continuously evolving.

A vCISO with AI experience can ensure that your business not only follows compliance regulations but also understands how AI systems handle data privacy at every stage. Whether it's ensuring data encryption during AI model training or implementing secure data storage protocols, the right vCISO will ensure your AI practices comply with all applicable laws while protecting your customers' and employees' data. This is crucial for building trust and avoiding costly fines for non-compliance.

4. SECURING THE AI SUPPLY CHAIN

For businesses developing or utilizing AI applications, the AI supply chain can be complex. From third-party data providers to external AI model developers, each link in the chain presents a potential vulnerability. As businesses increasingly depend on AI as a service (AIaaS) or integrate third-party AI models into their products, managing these external risks becomes critical.

Efforts like Microsoft's AI supply chain security efforts serve as an example of the importance of identifying supply chain risks. Microsoft has emphasized the need for securing machine learning pipelines by implementing techniques like model provenance tracking, robust validation mechanisms, and supply chain risk assessments. Their AI Red Team actively tests AI models for vulnerabilities, ensuring that third-party AI components integrated into Microsoft products meet stringent security standards.

A vCISO with AI expertise can assess the risks posed by your AI supply chain and work with vendors to ensure all third-party AI solutions are secure. By auditing AI providers for compliance, evaluating their security protocols, and continuously monitoring for potential vulnerabilities, the vCISO can ensure that the entire AI ecosystem is fortified against cyber threats.

5. BUILDING A RESILIENT AI INFRASTRUCTURE

AI systems depend on high-performing, resilient infrastructure. Whether hosted on-premises, in the cloud, or in hybrid environments, the infrastructure must be designed to support the unique needs of AI applications—processing large datasets and executing complex models without performance lags or downtimes. In addition to infrastructure resilience, one must take into consideration strong governance to ensure security, compliance, ethical use, and operational stability. Organizations must implement robust data governance practices to maintain data integrity, prevent bias, and comply with privacy regulations such as GDPR and CCPA. Security measures, including access controls, encryption, and continuous monitoring, are essential to protect AI models from adversarial attacks like data poisoning and model inversion. Compliance with industry standards such as NIST AI RMF and ISO 42001, along with alignment to emerging regulations like the EU AI Act, ensures responsible AI deployment. Regular testing for bias, model drift, and fairness is crucial, as is human oversight in critical decision-making.

Copyright © 2025 J.S. Held LLC, All rights reserved.

A vCISO experienced in AI will not only focus on securing the AI applications themselves but will also evaluate and strengthen the underlying infrastructure. From ensuring that the AI systems are hosted on secure cloud platforms with robust security features to implementing failover mechanisms that ensure uptime during potential attacks, the vCISO ensures your AI infrastructure is as resilient as it is innovative.

6. AI-DRIVEN THREAT DETECTION AND RESPONSE

One of the most prominent benefits of employing a vCISO with AI experience is the ability to leverage advanced AI algorithms to detect and respond to cyber threats in real-time. Traditional security systems often rely on predetermined rules or patterns, making them vulnerable to sophisticated and previously unseen threats. AI, on the other hand, utilizes machine learning and behavioral analytics to identify unusual patterns in network traffic or user behavior, even before an attack occurs.

A vCISO skilled in AI can incorporate customized tools and systems that learn from each interaction, continually improving threat detection capabilities. This proactive approach significantly reduces the time between detecting a breach and mitigating its impact, which is critical when it comes to avoiding costly data losses or reputational damage.

7. PROACTIVE THREAT INTELLIGENCE AND INCIDENT RESPONSE FOR AI ENVIRONMENTS

The evolving nature of AI and its applications means that the security landscape is in constant flux. A vCISO with experience in AI and cybersecurity is well-versed in monitoring emerging AI-specific threats and can provide proactive threat intelligence.

By utilizing AI-driven security tools themselves, these vCISOs can detect anomalies in real-time, respond to AI-related incidents swiftly, and implement post-incident analysis to continually improve the organization's security posture. Whether it's identifying an attack on a machine learning model or addressing vulnerabilities in AI-powered business applications, the vCISO ensures rapid, effective responses.

8. ALIGNING AI INNOVATION WITH ROBUST SECURITY STRATEGIES

In organizations developing AI applications, there is often a tension between innovation and security. Businesses must innovate rapidly to stay ahead of the competition, but they also need to ensure that their AI solutions are secure from the outset.

One real-world case is Google's work on TensorFlow Privacy, an open-source tool that implements differential privacy to ensure AI models can learn from data without exposing sensitive information. This is particularly crucial for applications like Google's Smart Compose feature in Gmail, where AI suggestions are trained on user data while maintaining privacy. Additionally, Google uses Federated Learning, which allows AI models to be trained across multiple devices without centralizing sensitive data, reducing the risk of data breaches.

A vCISO with AI expertise bridges this gap, helping to align security strategies with business objectives. They can integrate security measures into every stage of the AI development lifecycle—ensuring that AI projects are not only innovative but also secure, compliant, and resilient. With the right vCISO in place, companies can innovate with confidence, knowing their AI systems are protected at every stage.

Copyright © 2025 J.S. Held LLC, All rights reserved.

9. ENSURING THE PROTECTION OF INTELLECTUAL PROPERTY IN AI PROJECTS

In the rapidly changing landscape of artificial intelligence, protecting intellectual property (IP) is a critical challenge, as AI projects often involve proprietary algorithms, sensitive training data, and innovative models that give organizations a competitive edge. The vCISO plays a vital role in safeguarding these assets by implementing robust security frameworks, access controls, and data governance policies to prevent unauthorized access, theft, or compromise. This proactive approach not only mitigates external threats like cyber espionage and insider risks but also fortifies an organization's ability to defend its AI-powered intellectual property in a constantly shifting threat landscape.

Beyond technical security, a vCISO helps organizations navigate legal, regulatory, and contractual obligations tied to AI development. With many AI projects relying on third-party data sources, cloud-based processing, and open-source components, ensuring compliance with licensing agreements, data privacy laws, and ethical AI standards is crucial to avoid legal exposure. A vCISO provides strategic risk management insights that help organizations implement secure AI supply chains, enforce non-disclosure agreements, and establish cybersecurity-driven IP protection measures—ensuring that proprietary AI models remain exclusive and defensible. By bridging the gap between security, legal, and business strategy, a vCISO enables AI-driven organizations to innovate with confidence, knowing their intellectual property is well-guarded against emerging threats.

10. INNOVATIVE AND ADAPTIVE RISK MANAGEMENT STRATEGIES

AI's ability to analyze vast amounts of data at lightning speed is a game-changer for risk management. A vCISO with AI expertise can implement predictive models that forecast potential risks and vulnerabilities based on historical data and emerging trends. These insights are invaluable for creating a proactive, rather than reactive, approach to cybersecurity.

By using AI to continuously assess the risk landscape, a vCISO can offer precise recommendations on how to safeguard your assets, whether it's by patching vulnerabilities, adjusting access controls, or fortifying sensitive data areas. This ensures that your organization's cybersecurity posture remains agile and resilient to new threats.

CONCLUSION – BOLSTERING AI SECURITY WITH VCISO EXPERTISE

As businesses increasingly turn to AI to drive innovation, the need for robust cybersecurity becomes more critical. A vCISO with expertise in AI development and implementation is uniquely equipped to address the complex cybersecurity challenges of AI-driven environments. By employing a vCISO with extensive experience in AI security risks, AI threat detection, and overall risk management, your business can not only protect its valuable assets but also confidently pursue AI innovations without compromising security.

By leveraging AI to automate routine tasks like monitoring, reporting, and initial threat triage, a vCISO can focus on higher-level strategic decisions. This allows businesses to allocate their resources more efficiently, reducing the costs associated with overburdened security teams and mitigating the risk of human error.

However, hiring a full-time CISO is a major financial commitment, often out of reach for many organizations. A vCISO offers a cost-effective alternative, delivering the same level of expertise and oversight—without the overhead of a full-time executive. Additionally, a vCISO can provide access to a team of seasoned professionals who can be strategically deployed as needs arise, ensuring both tactical execution and long-term security leadership. When paired with AI tools,

Copyright © 2025 J.S. Held LLC, All rights reserved.

a vCISO can maximize the return on investment by optimizing resources.

ACKNOWLEDGEMENTS

We would like to thank our colleagues, Kevin Gorsline, Antonio Rega, and Denis Calderone, for providing insight and expertise that greatly assisted this research.

Kevin Gorsline is a Managing Director in J.S. Held's Global Investigations Practice who joined following J.S. Held's acquisition of TBG Security. For several years, Kevin served as the Chief Operating Officer and head of the Risk and Compliance practice at TBG Security, where he was responsible for providing the leadership, management, and vision necessary to ensure that the company had the proper operational controls, administrative and reporting procedures, and people systems in place to effectively grow the organization and to ensure financial strength and operating efficiency. His experience and leadership throughout his career have been focused on developing and delivering information security services and solutions, providing outstanding client service, and driving profitable revenue growth. Kevin brings established proficiency as an IT leader with extensive experience in risk and compliance services, applications development, and implementation projects both in the United States and abroad.

Kevin can be reached at kevin.gorsline@jsheld.com or +1 843 890 8596.

Antonio Rega is a Managing Director who leads the emerging technology and data governance service areas within the Digital Investigations and Discovery group in J.S. Held's Global Investigations Practice. He has more than 20 years of experience providing consulting, advisory, and subject matter expertise in the areas of digital forensics, incident response, data privacy, governance, and discovery on behalf of global corporations and law firms. Based in New York, Antonio regularly assists clients with advice and strategy through all phases of a given client need, including regulatory compliance, responses to government subpoenas, and expert testimony when required.

Antonio can be reached at antonio.rega@jsheld.com or + 1 551 345 8502.

Denis Calderone is a Senior Managing Director who leads Cyber Security Services within the Digital Investigations and Discovery group in J.S. Held's Global Investigations Practice. He joined the company in October 2022 following J.S. Held's acquisition of TBG Security. Denis brings nearly three decades of experience in the information technology field, with more than 20 years dedicated to information security. He holds multiple security certifications, including the CISSP and CISA certifications. His key technical expertise is in network and application penetration testing as well as Vulnerability Assessments, Security Policy, Development, Regulatory and Standards Compliance Testing. Denis also plays a CISO / CSO on-demand role for numerous consulting customers. Previously, he led the technical consulting arm of TBG Security and performed the role of CSO. Prior to TBG Security, Denis worked for Exodus Communications as part of their Northeast Security Practice, and for Lycos as their information security engineer.

Denis can be reached at denis.calderone@jsheld.com or +1 516 621 2900.

Copyright © 2025 J.S. Held LLC, All rights reserved.

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal, or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation, or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.

J.S. Held, its affiliates and subsidiaries are not certified public accounting firm(s) and do not provide audit, attest, or any other public accounting services. J.S. Held is not a law firm and does not provide legal advice. Securities offered through PM Securities, LLC, d/b/a Phoenix IB or Ocean Tomo Investments, a part of J.S. Held, member FINRA/SIPC. All rights reserved.

Copyright © 2025 J.S. Held LLC, All rights reserved.