

THE LATEST BYTE



ONE STEP SECURE IT | VOL 2 | 2025

AI in Business

The **Double-Edged**
Sword of Technology

AI in Business: The Double-Edged Sword of Technology



Artificial intelligence (AI) has become a driving force in the modern business world, reshaping industries and redefining what's possible. As businesses adopt AI-powered tools to enhance threat detection, automate processes, and improve compliance monitoring, they also face the growing threat of cyber criminals leveraging AI for malicious purposes. When it comes to security, AI is both a powerful ally and a potential vulnerability.

This issue of *The Latest Byte* explores the dynamic relationship between AI and business operations. From the ethical considerations of AI adoption to actionable steps for protecting businesses against AI-fueled cyber threats, we provide insights that business leaders need to make informed decisions.

AI is more than a tool; it's a strategic asset—if wielded wisely. Join us as we explore its transformative potential and provide practical guidance for using AI to strengthen and protect your business.

About One Step Secure IT

We are an outsourced IT company with over three decades protecting our customer's data from breaches to alleviate the dread of cyber attacks, costly downtime, and loss of customer trust.

Our expertise includes Cybersecurity, Managed/Co-Managed IT, Information Security, and Compliance Services. We understand that as business operations evolve, so do the security threats. Our expert team collaborates closely with you to create a customized IT strategy, identify vulnerabilities, and strengthen your IT infrastructure.

Our corporate headquarters are in Phoenix, AZ, and we proudly serve businesses nationwide. To learn more about how One Step Secure IT can enhance your technology, visit our website at www.onestepsecureit.com.

NOW STREAMING

S3 EP 01: **HACKERS IN THE DRIVER'S SEAT**

➔ **Cybersecurity Challenges
Auto Dealerships Can't
Afford to Ignore**



The automotive industry has become a prime target for cyber criminals. Scott Kreisberg and Kevin McAdam uncover why hackers are targeting dealerships and the steps to lower the chances of cyber incidents. Learn how to optimize the operations that bring in revenue.

COMING UP NEXT

S3 EP 02: UNDERSTANDING THE LEGAL AFTERMATH OF A CYBER STRIKE

➔ **Featuring Attorney
Andrew Garbarino**



Scott Kreisberg and legal expert Andrew Garbarino explore the legal consequences of cyber breaches and what companies must do to minimize exposure and avoid costly legal battles—because ransomware is just the beginning. **APRIL 24, 2025**

S3 EP 03: RETAIL'S CYBER WAKE-UP CALL

➔ **Lessons from One of the
Largest Retail Breaches
in History**



In October 2024, a massive breach exposed 57 million customer records from major retailers like Hot Topic and Torrid. Experts Scott Kreisberg and Tim Derrickson break down the vulnerabilities behind the breach and share key strategies for protecting customer data, ensuring compliance, and maintaining trust. **MAY 22, 2025**



One Step Beyond Cyber Podcast: Season 3

The Best Season Yet—Don't Miss a Beat

Cyber threats are escalating, and businesses can no longer afford to sit on the sidelines. Season 3 of the *One Step Beyond Cyber* Podcast dives headfirst into the world of cybersecurity, business resilience, and technology innovation. This is not just a conversation—it's your front-row seat to expert insights, game-changing strategies, and invaluable revelations in cybersecurity, technology, and business leadership. Join CEO and host Scott Kreisberg as he unpacks critical topics with leading experts. Trust us, you'll want to hit play.

**Start Your Season 3 Journey
Here: Don't Miss the Premiere!**

www.youtube.com/@onestepsecureit/podcasts



How **AI** will help businesses improve operations over the next few years.

Artificial Intelligence (AI) is more than just a buzzword— it's a transformative force that's reshaping how organizations operate and compete. As the CEO of a Managed Service Provider (MSP), I've seen firsthand how AI-driven solutions can elevate efficiency, strengthen security, and spark innovation across virtually every sector. Over the next few years, these technologies will become even more ingrained in our daily workflows, providing tangible benefits that go far beyond mere automation.

One of AI's most prominent advantages lies in **streamlining day-to-day operations**. Companies will increasingly rely on AI to automate repetitive tasks, including data entry, scheduling, and basic customer support, so that employees can focus on higher-value activities. This strategic reallocation of manpower not only reduces costs but also empowers teams to devote their time to creative problem-solving and building lasting customer relationships. In this manner, AI won't replace human experience but rather enhance it, creating an environment where employees can do their best work without being bogged down by administrative burdens.



Beyond process automation, AI is revolutionizing **data analytics and decision-making**. Advanced algorithms can rapidly process massive amounts of information, identifying patterns that humans may struggle to detect. This capacity for deep insight allows businesses to anticipate market trends, address potential bottlenecks, and respond to customer needs more accurately. For instance, AI-enabled analytics can help retailers optimize inventory management, ensuring the right products are in stock at the right time. Meanwhile, service-based organizations can leverage predictive analytics to tailor offerings that align with shifting consumer preferences. As AI models become more sophisticated, the quality of these insights will continue to improve, driving smarter decisions at every level of the organization.

Another critical area benefiting from AI is **cybersecurity**. In an era of relentless cyber threats, from phishing attempts to complex ransomware attacks, companies need robust, proactive defense mechanisms. AI-powered security tools can analyze network traffic and user behavior in real-time, spotting anomalies that might indicate a breach or malicious activity. By detecting these threats early, organizations can neutralize issues before they escalate into full-blown crises—ultimately saving time, money, and reputation. This AI-driven vigilance will become increasingly vital as cyber threats evolve and become more difficult to detect through manual methods alone.

Moreover, the rise of **generative AI** is opening new frontiers in areas like content creation

and design. Tools that can quickly produce draft marketing copy, generate personalized emails, or even design basic graphics will become standard across industries. While the creative touch of a human remains indispensable, generative AI can drastically reduce turnaround times and allow teams to iterate more rapidly on their ideas.

From my perspective as an MSP leader, the key to successfully adopting AI is pairing the right technology with expert guidance. Businesses that collaborate with experienced MSPs can ensure their AI integrations align with strategic objectives, comply with regulatory requirements, and maintain robust security protocols. MSPs can also assist in training staff to use AI tools effectively, maximizing the return on investment.

In summary, AI holds immense promise for businesses of all sizes. As the technology matures, it will continue to streamline operations, safeguard digital assets, and provide powerful insights to drive growth. Those who embrace AI thoughtfully—leveraging both technological and human intelligence—will be best positioned to stay agile, innovative, and competitive in the years to come.

AUTHOR

**Scott
Kreisberg**

One Step Secure IT
Founder and CEO



AI in CYBER

Artificial Intelligence (AI) is transforming cybersecurity, revolutionizing threat detection, decision-making, and security frameworks. As organizations adopt AI-driven technologies, they also expose themselves to new security challenges. From automated threat detection to AI-powered cyber attacks, AI plays a dual role—both as a defender and a potential threat. While AI enhances cybersecurity, it also creates new vulnerabilities that cyber criminals exploit.

AI has proven highly effective in automating threat detection, mitigating cyber risks, and strengthening businesses' overall security posture. However, the same technology is being weaponized by attackers to create sophisticated attack vectors and exploit system weaknesses. Cybersecurity professionals must constantly balance AI's advantages and risks—protection versus exploitation, automation versus manipulation, and security versus vulnerability.

AI as a Cybersecurity Enabler

AI-powered security tools enhance protection by detecting real-time threats. Machine learning models analyze vast amounts of data, identifying patterns that indicate malicious activity. Security Information and Event Management (SIEM) systems now incorporate AI to improve anomaly detection, accelerating response times and mitigating damage before threats escalate. By auto-

ating routine monitoring tasks, AI allows security teams to focus on strategic defense measures rather than manual threat analysis.

AI is also revolutionizing identity verification and access control. AI-driven authentication methods, such as biometric recognition and behavioral analytics, improve accuracy in identity management. Adaptive authentication systems dynamically assess risk, granting or restricting access based on real-time user behavior. AI strengthens the Zero Trust security model by continuously monitoring user activity, detecting anomalies, and adjusting security policies in real-time to prevent unauthorized movement within networks.

AI as a Cybersecurity Threat

While AI bolsters security, it is also leveraged by cyber criminals to launch more advanced attacks. Hackers use AI to automate phishing campaigns, evade Endpoint Detection and Response (EDR) systems, and develop malware that adapts to security defenses. Social engineering threats, such as deepfake technology, are becoming increasingly sophisticated, making it harder to distinguish legitimate users from attackers. AI-driven cyber threats are evolving rapidly, forcing cybersecurity professionals to use AI not only for defense but also to counteract these emerging risks.

SECURITY

Guardian or Threat?

Written by Tim Derrickson

One Step CISSP, Director of IT & Security Services



Balancing AI's Benefits and Risks

Businesses must carefully balance AI's security advantages against its potential threats. Ensuring transparency in AI-driven security decisions, minimizing bias in threat detection models, and aligning AI implementations with regulatory frameworks such as GDPR and NIST are critical. As AI becomes an integral part of security infrastructure, organizations must prioritize hiring skilled cybersecurity professionals and investing in AI governance. Training security teams in AI threat mitigation strategies will be essential to managing AI-enabled security operations effectively.

A Proactive Approach to AI Security

AI is reshaping cybersecurity in profound ways, presenting both challenges and opportunities. As cyber threats evolve, businesses must harness AI responsibly—ensuring it serves as a security enabler rather than a vulnerability. A proactive approach that integrates AI with human oversight, regulatory compliance, and continuous monitoring will be key to securing the future of AI-driven business environments.



SECURING THE AUTO INDUSTRY: HIGHLIGHTS FROM NADA

2025 NADA SHOW

One Step Secure IT
attended the Auto Industry
event of the year.

LOCATION

New Orleans

WHEN

January 23-26

AUDIENCE

Automotive Dealers

THE SHOW

The NADA Show offered a full program of innovative products, emerging trends and networking opportunities for automotive dealers.

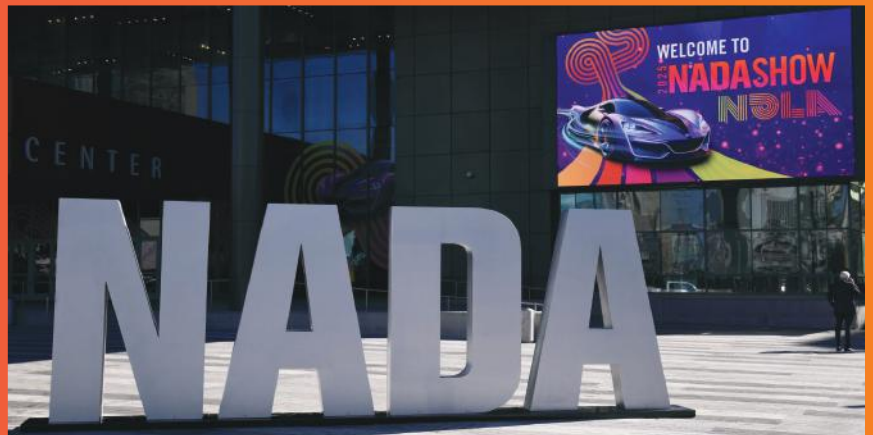
WHO IS NADA

For more than 100 years, the National Automobile Dealers Association (NADA) has been the national voice of franchised new-car dealerships, their employees and their customers.

The One Step Secure IT team had a great time connecting with business leaders at the NADA Show, one of the largest auto industry trade shows in the U.S. This event brings together dealers, manufacturers, and industry professionals to explore the latest in auto technology, dealership operations, and business strategies.

With dealerships handling sensitive customer data, cybersecurity is more critical than ever. We discussed best practices to prevent cyber attacks and downtime, helping businesses safeguard their data and customer trust.

Check out some highlights from NADA!



The Importance of **AI** in Retail & Why Collaboration Matters

Article brought to you by **Retail AI Council**

The retail industry is undergoing a seismic shift, driven by the rapid adoption of artificial intelligence. From hyper-personalized shopping experiences to precision-driven inventory management, AI is no longer an optional tool—it's the foundation of modern retail success. Retailers that embrace AI are unlocking new efficiencies, driving revenue, and elevating customer engagement. However, true success doesn't come from adopting AI in isolation. The key to staying ahead lies in collaboration. By joining forces with the Retail AI Council, retailers gain access to the expertise, insights, and network needed to maximize AI's potential and lead the industry forward.

AI's Role in Retail and Its Impact on Growth

AI is reshaping nearly every aspect of the retail experience. One of its strongest impacts is personalization—retailers can now analyze vast amounts of consumer data to deliver tailored recommendations, customized promotions, and individualized shopping experiences, driving stronger engagement and loyalty.

Chatbots and virtual assistants are already enhancing customer service, providing instant, 24/7 support and guiding customers through product selection and inquiries with-

out human intervention. These AI-driven tools are well-established in e-commerce and are increasingly bridging the gap in physical stores, helping customers get real-time assistance while improving operational efficiency.

AI is also optimizing inventory and supply chain management. AI-powered forecasting models predict demand with high accuracy, ensuring the right products are available at the right time while reducing waste and minimizing costs. Retailers using AI in logistics are seeing leaner operations, better stock management, and improved customer satisfaction.

Looking ahead, AI is set to push retail innovation even further. Customer sentiment analysis will allow retailers to interpret facial expressions and engagement levels in real-time, enabling proactive service and creating more personalized in-store interactions. Digital twin technology is also emerging, allowing retailers to create virtual replicas of stores and supply chains to test layouts, optimize inventory, and improve efficiency before making real-world changes.

By leveraging both proven AI applications and emerging innovations, retailers can move beyond automation into intelligent, adaptive retailing—one that anticipates demand, enhances in-store experiences, and ensures customers feel engaged and valued.

Retail AI Council and the Power of Collaboration

While AI is transforming retail, many retailers struggle with where to start, how to scale, and how to implement AI strategically. For small and mid-sized businesses, resource constraints can make AI adoption feel daunting. Even larger enterprises grapple with navigating new technologies, integrating AI across multiple systems, and ensuring responsible AI use.

That's where Retail AI Council comes in. As the leading voice in AI for retail, we bring together retailers, AI innovators, and industry experts to drive actionable AI adoption, thought leadership, and collaboration. We cut through the noise, providing access to cutting-edge research, best practices, and AI solutions that retailers need to stay competitive.

Through the Retail AI Council's ecosystem, members gain:

- Exclusive access to AI research and industry insights
- Peer-to-peer collaboration with top retail leaders
- Education on AI best practices, ethical considerations, and implementation strategies
- A direct line to the latest AI innovations, tools, and expert guidance

AI is evolving rapidly, and retailers who collaborate with Retail AI Council position themselves at the forefront of that evolution. Our network provides a real-time pulse on the industry, ensuring members are informed, prepared, and proactive in shaping AI's future in retail.

The Competitive Advantage of Collective Intelligence

Retail is evolving at breakneck speed, and AI adoption isn't just a competitive advantage—it's a survival strategy. Retailers that leverage AI in isolation risk falling behind, while those who collaborate, share insights, and co-develop solutions are the ones leading industry transformation.

By working together through the Retail AI Council, retailers don't just keep up with AI trends—they define them. Our members don't wait for innovation to happen; they actively shape the future of AI in retail.

The Bottom Line: AI is Non-Negotiable—Collaboration is the Multiplier

The future of retail is AI-driven, and retailers who act now will set the standard for what's next. But AI transformation isn't a solo endeavor—it requires strategic collaboration. Retail AI Council is the premier authority on AI in retail, helping businesses navigate AI adoption, accelerate innovation, and future-proof their operations.

Joining Retail AI Council isn't just about staying informed—it's about staying ahead. AI will continue to redefine the industry, and the retailers who embrace collaboration, education, and innovation will be the ones leading the way.

Learn more about Retail AI Council and join for free at <https://www.retailaicouncil.com/>.



One Step Secure IT
22520 North 18th Drive
Phoenix, AZ 85027



www.OneStepSecureIT.com | (623) 227-1997

Connect with us @OneStepSecureIT

