DISTRIBUTION STRATEGY GROUP

Cybersecurity in the Age of AI: What's Your Plan?

By Alex Rutkovitz Spigel

In the age of artificial intelligence (AI), distributors need to build walls around their critical customer and business data — and they need to be solid. If you haven't started building, you're at risk.

Since the pandemic, there's been an 81% increase in cyberattacks. It's no wonder cybersecurity is keeping many distributors up at night.

The problem is fast-changing technology and data sprawl make it more complicated and harder to protect businesses. There's an explosive number of connected and mobile devices and increased usage of the cloud. AI has further complicated the landscape.

External threats are on the rise: 80% of attacks are from external forces. But that still leaves 20% of threats coming from inside the organization — a significant concern.

It's critical that every distributor have a plan and structure in place to ensure cybersecurity.

AI is Abundant in Every Aspect of Our Lives

AI tools are woven into the fabric of our daily lives:

- Voice-enabled virtual assistants Siri and Alexa
- Fraud detection, low-balance alerts, mobile check deposits and security of transactions at financial institutions
- Facial recognition to open your phone
- Amazon product recommendations
- Your Netflix movie queue

At work, generative AI platforms such as ChatGPT craft emails and answer questions on chat. AI-powered Grammarly helps users draft error-free messages. Spam filtering technology uses AI to block malicious emails. AI tools are also helping to personalize the customer experience.

AI reacts to the data we feed it, learning from historical data to improve. Behind the scenes is a series of computer algorithms. Some examples include:

- **Machine learning** enables computers to perform tasks without explicit instructions. Instead of being programmed to perform specific activities, machine learning algorithms learn from data and improve their performance over time.
- **Natural language processing** enables computers to understand, interpret and generate human language in a meaningful and contextually relevant way.
- **Deep learning** enables computers to "learn" by interacting with hierarchical data. Computer scientists try to recreate the biological functions of the human brain by creating layers of data that the computer can interact with.

Unfortunately, hackers use these same tools to wreak havoc. They also try to disrupt AI-based software with cyberattacks that target the training data that the software depends on.

AI attacks pose a huge threat to physical safety, privacy concerns, digital identity and national security, making it crucial for distributors to take measures to protect against them.

State of Cybersecurity

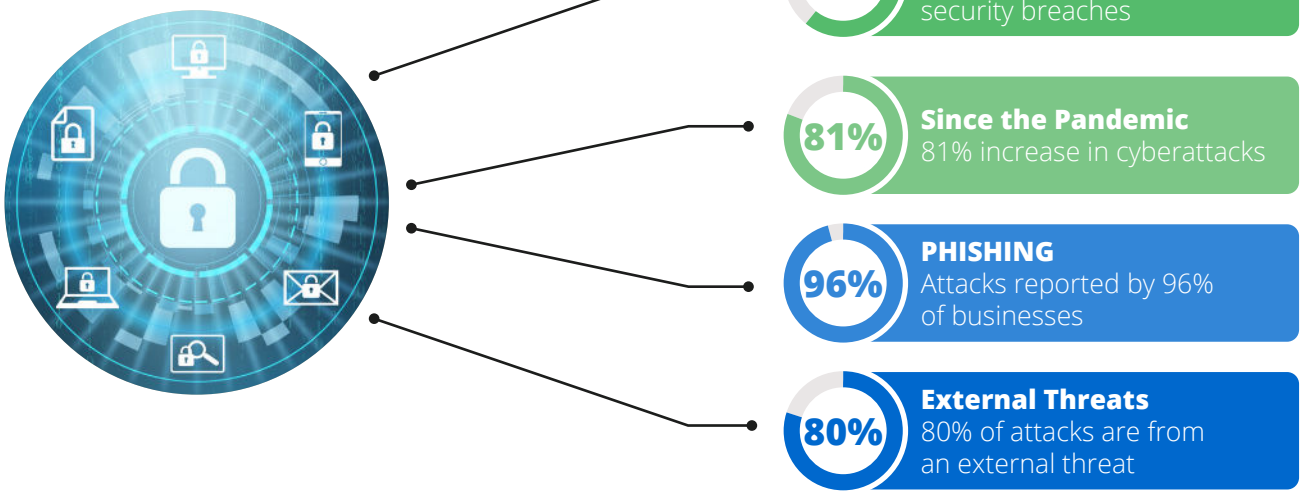
The average cost of a cybersecurity breach in 2023 was $4.45 million. That's a 15% increase over the past three years. The most common breaches include:

- **Ransomware** is malicious software that encrypts the victim's data, rendering it inaccessible until the company pays the ransom. Cybercriminals often demand the ransom paid in cryptocurrencies to evade detection.
- **Phishing** attacks are fake emails, texts or phone calls designed to look like the real thing. Hackers use these tools to lure the unsuspecting into revealing personal or organizational data such as login credentials or financial information.
- **Malware** is a broad term for malicious software that causes harm, including system disruption, data theft and financial losses.
- **Wire fraud** is the unauthorized diversion of money or sensitive information to fraudulent accounts.
- **Password attacks** occur when weak credentials or unsuspecting phishing victims allow cybercriminals direct access to systems, networks and sensitive data.

The target isn't just big companies; 41% of small to medium-sized businesses (SMBs) experienced a cyberattack last year.

Each threat brings the risk of reputational damage, lawsuits and lost customers.

State of Cybersecurity



Phishing attack leads to a costly mess

Phishing is one of the most likely breaches to happen to a distributor. In one example, a criminal sent a $230,000 bill to a customer via email that looked exactly like the invoice they are used to receiving. The customer paid the invoice – and the criminal — via wire.

It's hard to know who is at fault in these situations, and it can take weeks to resolve, with lawyers and cybersecurity experts, security forensics and more involved.

AI Attacks

Every tool can be a weapon, depending on how you use it, and AI is no exception. Criminals can use the same AI algorithms that power your Alexa app to fuel their cyberattacks.

AI-fueled cyberattacks that will grow more prevalent include:

- **Deepfakes** that fabricate hyper-realistic audio and video content indistinguishable from genuine recordings. The problem with deepfakes is that while they pose a serious threat, they have legitimate business uses such as in customer support and call-response applications. It's harder to protect against these threats when using them every day in our business.
- **Poisoning** interferes with AI training data to corrupt the model. For example, a hacker could disrupt a self-driving car so it fails to read a stop sign. Or hackers could retrain a cybersecurity tool to miss a backdoor they use to enter a network.
- **Inference** probes the training data model with different inputs to trick the AI system into making incorrect predictions or classifications. This can result in the leakage of sensitive data. For example, adding noise to an image could cause an image recognition system to misclassify objects.
- **Evasion** refers to a tactic where malicious actors manipulate or adapt their behavior to evade detection by AI-powered security systems.
- **Extraction** is a technique to probe the AI to steal the training model data or learn enough about it to recreate it.

A run-of-the-mill customer call turned cyberattack

Imagine your CSR taking a phone call. The caller ID matches a customer's information. On the line is the voice of a person they've spoken with 20 times before who says, "I'm on a job site, and I need this order right away." They place a $100,000 order for a valuable product. The CSR enters the order, and fulfillment ships it to a destination where it's stolen and gone forever.

Risks to Your Business

Distributors interact with both manufacturers and customers. None of these parties want to be the ramp for a data breach. At the same time, you've captured a lot of customer information that could be a juicy reward for a hacker.

Here are some added risks that come with AI:

- **Intellectual property theft:** Distributors often develop proprietary technologies, algorithms and business processes critical to their operations. AI-powered cyberattacks could result in the theft of intellectual property, including trade secrets, patents and proprietary software code.
- **Privacy violations:** Distributors collect and process vast amounts of customer data, including personally identifiable information (PII) and transactional records. AI-powered data analytics and decision-making systems may inadvertently expose individuals' privacy by analyzing sensitive data or unauthorized use of personal information without consent.
- **Software vulnerabilities:** AI-powered software applications and systems deployed by distributors may contain vulnerabilities or weaknesses that attackers could exploit to gain unauthorized access, compromise data integrity or disrupt business operations. AI algorithms or framework vulnerabilities could also lead to security flaws in distributed applications or services.
- **Reputation:** Deepfake technology, which uses AI algorithms to create realistic but fake audio, video or text content, poses a significant cybersecurity risk for distributors. Malicious actors could use deepfakes to impersonate executives, employees

or customers, spreading misinformation or conducting social engineering attacks that damage the distributor's reputation.

- **Fake information:** AI-powered bots, chatbots and automated systems can generate and disseminate fake information or malicious content across digital channels, including social media, websites and online forums. Fake news, phishing scams and disinformation campaigns could undermine trust in the distributor's brand, products or services, leading to financial losses or reputational damage.

Do Fence Me In: Building Layers Around AI

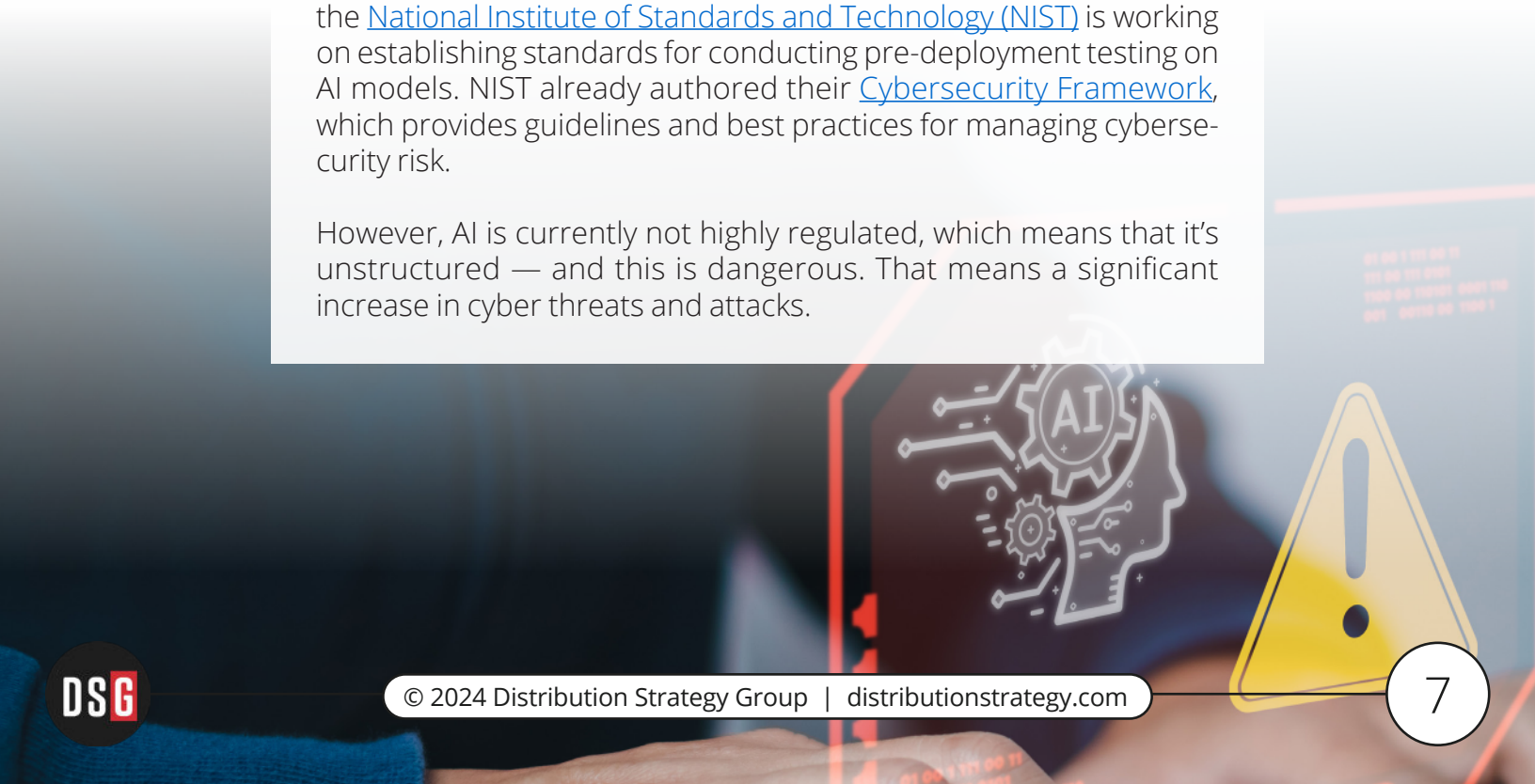
The biggest vulnerability for any business will always be your people. Distributors need to define how employees should use AI. They need clear, repeatable standardized AI usage rules, constant training, evaluation and testing.

Any company investing in or using AI products needs to invest in cybersecurity measures to counter potential attacks. They should also understand common hacker techniques and be on the lookout for them.

Finally, any technology that doesn't have rules will end up with malicious behavior, whether intentional or unintentional. That's where a real structure and a plan really come into play.

When AI is involved, cybersecurity is built in layers. There is no one solution. Federal agencies are trying to help us with this; for example, the National Institute of Standards and Technology (NIST) is working on establishing standards for conducting pre-deployment testing on AI models. NIST already authored their Cybersecurity Framework, which provides guidelines and best practices for managing cybersecurity risk.

However, AI is currently not highly regulated, which means that it's unstructured — and this is dangerous. That means a significant increase in cyber threats and attacks.



How to Build a Culture of Compliance & Security

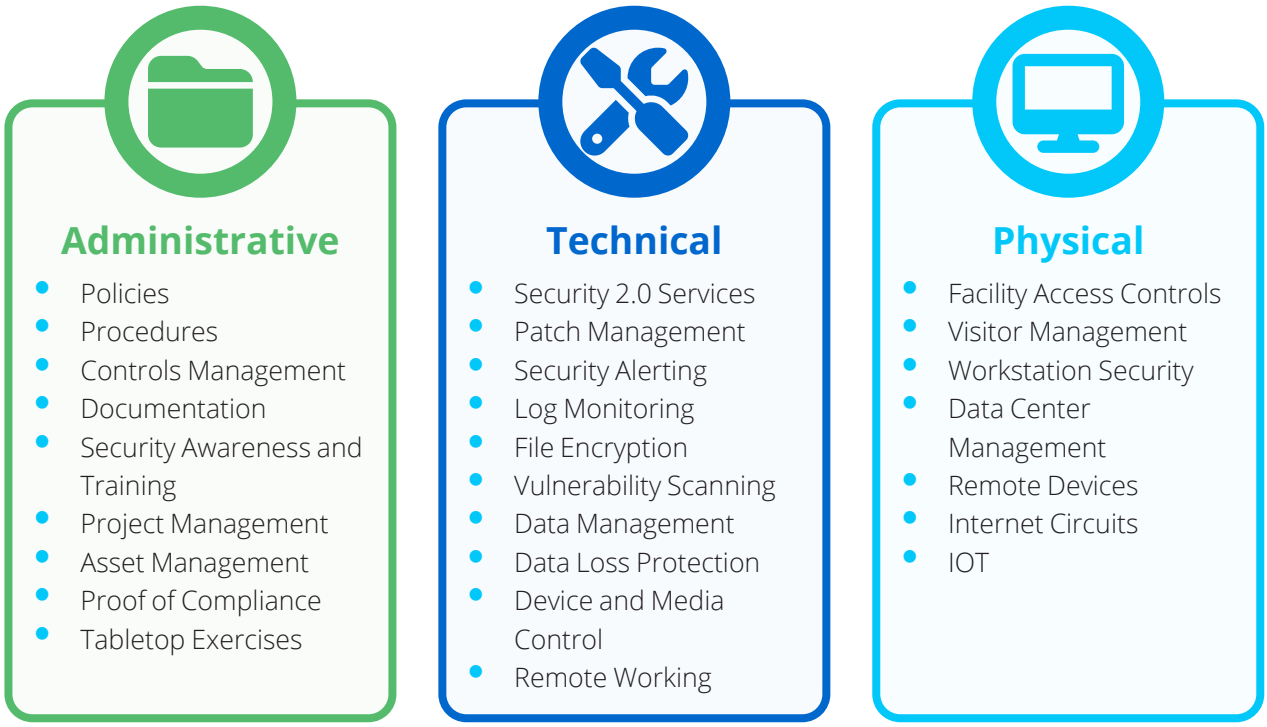
It's imperative for distributors to build a culture of compliance and security. This approach weaves the people, technology, compliance and workflow into their existing cybersecurity strategy and practices. But you can't build a foundation for AI on the 25th floor; you must build the layers up underneath your usage of these tools.

Compliance is the best possible driver of a security-focused culture. A company without a compliance framework is like a road without traffic lights. There are no lanes and no rules; it's a free-for-all.

Security is different from compliance. Security is being safe from threats.

Compliance follows a set of rules or requests from local, state or federal entities to keep data safe. For example, all 50 states have personal identifiable information laws. Eight states have privacy laws with California being the strictest. There are new AI regulations being added every day.

A compliance or best practices framework creates structures with policies, procedures and rules to protect the organization and your clients, your customer data and your sensitive data.



Compliance can be broken into three components: administrative, technical and physical.

Administrative is the human element of cybersecurity. The reality is that most cyberattacks begin with the people in your organization. Failing to change passwords or using the same password across systems, clicking on a phishing email or even leaving a laptop in a car to be stolen — these security risks cost companies billions every year. That's why creating a culture of cybersecurity must encompass user awareness training, testing and a process for password management for all the digital devices they use for work. In the case of cybersecurity, keeping the risks top of mind is an ongoing initiative. Vigilance is safety.

Technical cyber controls include firewalls, patch management and secure backups, antivirus software or advanced endpoint protection. Adding a compliance or cybersecurity best practices framework elevates your capabilities to next-level security. This could include adding endpoint detection and response (EDR) software, a cybersecurity solution designed to detect and respond to advanced threats and malicious activities on endpoints, such as desktops, laptops, servers and mobile devices. EDR solutions continuously monitor endpoint activities, collect telemetry data and analyze behavioral patterns to

identify suspicious behavior indicative of a security breach or compromise. Again, this is a good tool for the AI era, but it's also almost a necessity in a work-from-anywhere employee environment.

The physical side of cybersecurity includes facility access controls and visitor management policies in your distribution centers. But this also includes your internet circuits, remote devices and the Internet of Things (IoT) — all your physical assets.

To ensure full compliance, distributors must:

- Develop robust security control, tools and resources
- Establish strong policies, procedures and recordkeeping systems to verify compliance measures
- Implement comprehensive and accurate reporting for auditing, logging, scans, etc.
- Provide ongoing security awareness training for all personnel
- Conduct risk assessments on a routine basis
- Perform appropriate vendor management

How Can You Start Building Your Fence?

Start with a cybersecurity risk assessment. A risk assessment identifies, analyzes and evaluates potential cybersecurity risks and vulnerabilities within an organization's IT infrastructure and systems. It could include:

1. **Network Discovery:** Identifies all devices, systems and resources connected to the organization's network. You're basically creating an inventory of network assets to understand the organization's attack surface and identify potential entry points for cyber threats.
2. **Applications Discovery:** Identifies and catalogs all internal and external software applications and services running on the organization's network, including third-party software. The goal is to assess each application's security posture, identify vulnerabilities and ensure that they are properly configured and patched.
3. **Data Flow Analysis:** Maps the flow of sensitive data throughout the organization's network and systems, including data sources, repositories, transmission pathways and processing activities. The goal is to understand how sensitive data is accessed, transmitted, stored and processed within the organization's environment and assess the effectiveness of existing data protection controls.

4. **Vulnerability Scanning:** Uses automation to identify and assess vulnerabilities and weaknesses in the organization's IT infrastructure, systems and applications to identify potential security vulnerabilities that attackers could exploit to gain unauthorized access, compromise data integrity or disrupt business operations.
5. **Policy Gap Analysis:** Evaluates the organization's cybersecurity policies, procedures and controls against industry best practices, regulatory requirements and internal security standards.
6. **Compliance Framework:** Provides a structured set of guidelines and requirements to ensure that the organization's cybersecurity practices comply with relevant laws, regulations and industry standards.

AI should be woven into every component of this effort. Organizations should ask what AI is in place today, how employees are using these tools, what information they are entering and whether the AI systems are in the cloud or on-premises.

Where to Start

- Responsibility Matrix
- Security Awareness Training
- Document Existing Practices
- Incident Response, Business Continuity & Disaster Recovery Planning
- Information Security Policy, Acceptable Use, BYOD & Teleworking

Who owns the budget?

IT should not own the budget for cybersecurity. Compliance is a company-wide responsibility that goes beyond IT budget allocations. Collaboration and integration are critical for effective compliance management. And the ROI is clear: Strategic investment in compliance will yield long-term benefits.

Cybersecurity in the Age of AI

Years ago, we knew a quality assurance professional who always said that a mobile home park caused tornadoes. His point was simple: If you build a mobile home park, a tornado will show up because that happens when you expose yourself to risk. The same is true today when preparing for cybersecurity threats. If you do not prepare and protect your company, you're just inviting the tornado.

A comprehensive approach to cybersecurity in the age of AI must include people, technology, regulatory compliance and the rules and workflows that make you more secure. Building a culture of cybersecurity to mitigate AI risks starts with preventive measures and security controls:

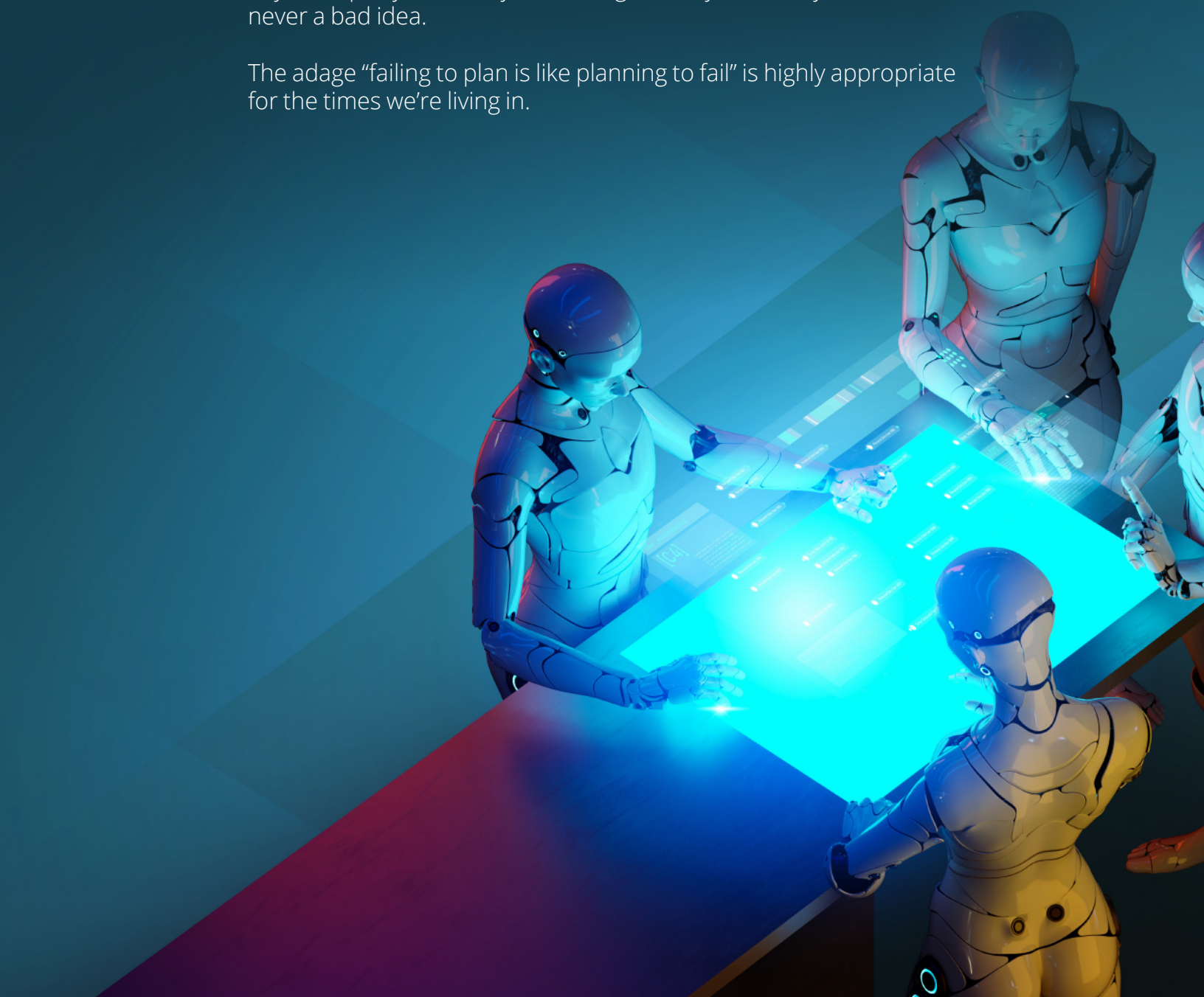
- Conduct regular security assessments and audits to identify and address vulnerabilities in AI-powered systems and applications.
- Implement robust access controls, encryption protocols and data protection mechanisms to safeguard intellectual property and sensitive information.
- Educate employees about cybersecurity best practices, including the risks associated with deepfakes, fake information and social engineering attacks. Then test them on these best practices.
- Monitor digital channels for signs of fraudulent activity, fake content or suspicious behavior using AI-powered threat intelligence platforms or anomaly detection systems.

- Collaborate with industry partners, cybersecurity experts and law enforcement agencies to share threat intelligence, best practices and mitigation strategies for addressing AI cybersecurity risks.
- Stay informed about emerging threats, trends and technologies in AI cybersecurity, and continuously update security policies and procedures to adapt to evolving risks and challenges.

Distributors have a lot to gain from preparing for AI's impact on cybersecurity.

Understanding the potential risks and ensuring they're part of your business continuity, disaster recovery and instant response planning is an important goal. This effort should include setting standards for any third-party vendors you're using. Also, cyberliability insurance is never a bad idea.

The adage "failing to plan is like planning to fail" is highly appropriate for the times we're living in.



About the Author

Alex co-founded Choice Cyber Solutions in April 2016 and is the firm's COO. In her current role, Alex's primary focus is partnering with MSPs to deliver top-notch security and compliance services to their clientele. Alex's strong customer service, IT risk assessment and regulatory compliance expertise enable her to bridge the gap between technical requirements and client needs. She is highly skilled in pinpointing vulnerabilities and crafting proactive solutions that meet clients' unique needs.

DISTRIBUTION STRATEGY GROUP

Thought Leadership for Wholesale Change Agents

Distribution Strategy Group helps you compete and win. In an evolving business environment marked by digital transformation, shifting customer preferences and the pivotal role of AI, we are your go-to source for research-backed webinars, whitepapers, blogs and live events that will help you make better decisions.

Our proprietary, specialized, distributor-focused analytics systems provide actionable insights you can use to drive superior outcomes with customers and employees, and versus competitors.

Contact us:

distributionstrategy.com | 303-898-8626 | contact@distributionstrategy.com

Thank you to our sponsors:

epicor.com

How Much Can an ERP Impact Your Bottom Line?

Turns out, a lot.

Market research firm IDC published a new study on distributors using Epicor for Distribution solutions, who reported **45%** more orders dispatched, **21%** higher productivity, and **35%** more inventory turns.

DOWNLOAD THE REPORT

EPICOR.COM/DISTRIBUTION

EPICOR

SOLUTIONS FOR: Automotive | Building Supply | ***Distribution*** | Manufacturing | Retail