CTVG

CONVENIENCE TECHNOLOGY
VISION GROUP

CTVG MEMBERS

VISION GROUP NETWORK CO-FOUNDERS

Cybersecurity: Evolving Trends and Pitfalls

Includes Previous Tech Topics Updates

CTVG VISION REPORT NO. 9
JANUARY 2025

FACILITATOR

Ed Collupy
Collupy System Solutions LLC.

FEATURED SPEAKERS

Daniel Martin
Principal Security Consultant, Field CISO, Verinext

Todd McClelland
Partner, Sterlington

VISION GROUP NETWORK sharing today to shape tomorrow

We are Convenience Technology Vision Group (CTVG), a group of invited leaders of the convenience industry who have volunteered our time to help our fellow retailers, solution providers and product suppliers. The only reason we gather is to discuss, debate and share our experiences and ideas. Each of us is offering our personal opinions. We are not looking for "group think" — we are promoting problem solving and looking to the future. We make our conversations available to everyone in the industry through CTVG Vision Reports. These reports will help you better understand current challenges, solutions, and opportunities while giving you access to different opinions and perspectives, regardless of the size of your business.

Convenience Technology Vision Group is part of the Vision Group Network, whose mission is to gather the best minds in the industry, put them in a virtual room, and let the ideas and opinions develop

This **CTVG Vision Report** is comprised of three parts:

CTVG Views provides a summary of the conversation with additional resources for extra context including and "Valuable Resources" for more in-depth education.

In The Room With CTVG provides you with the meeting transcript, tagged for easy reference, so that you can be "in the room" with us, rather than only having access to selected quotes and paraphrasing.

The full presentation "Cybersecurity: Trends and Pitfalls" is included and linked throughout the transcript for easy navigation.

We highly recommend that you read all three components.

CTVG
CONVENIENCE TECHNOLOGY
VISION GROUP

The main topics in this CTVG Vision Report:

CTVG thanks our **Ally Supporters**

Rovertown

For retailers looking to connect with their consumers in an always-on world, Rovertown's app platform provides the flexibility needed to deliver personalized, meaningful experiences. Unlike our competitors, Rovertown integrates with any technology vendor and goes the extra step to ensure our clients' success through best-in-class implementation and support.

Rovertown was originally founded in 2009 with the goal of helping cost-conscious college students across the United States to access the best discounts for local food and services. By eliminating the need to swipe an ID for discounts, the experience was brought to students' mobile devices in real-time with custom, localized deals.

Rovertown's business has since grown and evolved, but the humble beginnings taught the team the power of personalized experiences delivered through high-quality, branded apps. The Rovertown app platform now powers the mobile experiences of many leading regional convenience retailers.

Ally

CONTACT:
Jeffry Harrison
Co-Founder & President
jeffry@rovertown.com
rovertown.com

ALLY SUPPORTER SPOTLIGHT
The Rovertown team recently hosted several webinars on best practices in mobile app management including push notification tactics, coupon strategies, and more. Watch the recordings on-demand and stay up to date with additional news and insights at Rovertown's Insights webpage.

Abierto

With over 15 years of experience in the convenience store industry, Abierto understands the challenges retailers face in engaging consumers with on-premise messaging. Leveraging cutting-edge technology and dedicated in-house software development and design teams, we create custom, innovative, and integrated digital consumer engagement and messaging solutions tailored for multi-site convenience store retailers.

Headquartered in York, Maine, Abierto powers displays for leading industry retailers nationwide. Our advanced cloud-based platform, OPEN., is a robust yet user-friendly tool that automates digital content distribution and remote device management tasks across store networks. OPEN. also provides detailed content distribution analytics, enabling retailers to optimize their in-store messaging.

In 2020, we introduced OPEN.LED, a groundbreaking line of transparent, adhesive window displays designed to increase in-store traffic by dynamically engaging consumers in the forecourt and parking areas of convenience stores and travel plazas. Today, these displays sport stunning high resolution and brightness for an "impossible to ignore" messaging experience.

Abierto's team of seasoned designers, engineers, developers, and implementation experts work together to help clients execute their vision with precision and creativity. Execute your Vision with Abierto!

CONTACT:
Rick Sales
President
rick@ab-net.us
ab-net.us

ALLY SUPPORTER SPOTLIGHT
Rick Sales, Abierto's president, recently joined Philip Santini from Rutter's on the NACS Convenience Matters podcast where they discussed Rutter's on-premise digital transformation. You can check out the episode here.

CTVG thanks our **Ally Supporters**

You may know us as Gilbarco Veeder-Root, but it's time to get to know Invenco by GVR. In 2023, Gilbarco's well-established Retail Solutions division merged with Invenco, a global frontrunner in the payments and convenience store sectors. Our combined expertise is set to revolutionize the convenience retail space, offering cutting-edge, flexible technology solutions designed to boost efficiency and enhance customer engagement.

Invenco by GVR has a global footprint with industry-leading point-of-sale systems, payment solutions, site automations, workflows, and cloud services. These solutions will be integrated into the ground-breaking iNFX retail operating system to enable digital agility and rapidly deploy new capabilities to our customers. Invenco by GVR Solutions can be found in nearly 165,000 connected devices across 50,000 convenience stores in more than 50 countries. We are redefining convenience, together.

CONTACT:
Larry Bowden
Director, Retail Solutions Sales
larry.bowden@invenco.com
invenco.com

GK Software breaks down the barriers to unified commerce with its open CLOUD4RETAIL platform and a broad portfolio based on it, like OmniPOS for point of sale, self-checkout, mobile POS, GK Drive for forecourt control, mobile customer engagement and a full range of store/back-office solutions. The company is a recognized leader in omnichannel retail, offering a single, global software platform for all retail formats and touchpoints. Ten of the Top 50 retailers worldwide rely on GK, and GK is the fastest growing global POS provider in new installations over the last three years.

CONTACT:
Robert Green
Sales Director
rgreen@gk-software.com

Bill Miller
Vice President, Head of Sales - GK Americas
bmiller@gk-software.com
gk-software.com

CTVG VIEWS

A CONVENIENCE TECHNOLOGY VISION GROUP DISCUSSION

At the winter quarterly virtual meeting, CTVG members tackled the issue of cybersecurity. First hearing a presentation on the trends and pitfalls in the field, the group later discussed concerns, challenges and solutions. A look back at previous CTVG topics also allowed members to share updates.

CTVG
CONVENIENCE TECHNOLOGY VISION GROUP

A Deep Look Into Cybersecurity Trends & Pitfalls

CTVG Facilitator **Ed Collupy**, principal at Collupy System Solutions LLC, set the stage for the December 6, 2024 quarterly meeting on cybersecurity, stressing the critical concern for retail and IT leaders. He cited impressive efforts that businesses invest in combating threats, from ransomware and phishing to third-party vulnerabilities, and expressed appreciation for those IT leaders tackling these challenges. Consumers, he noted, are highly aware of their data and privacy vulnerabilities with villains attacking communications companies, foodservice providers, retail chains and so many other sectors, regularly putting their livelihoods at risk.

Collupy shared startling statistics on the issue: "91% of industries saw ransomware as one of the three most prevalent threats. 50% of social engineering attempts involved pre-texting to pressure victims into divulging sensitive information. 83% of breaches originated from external factors with 95% of those being financially motivated."[1]

Guest speakers **Daniel Martin**, field chief information security officer (CISO) at Verinext, and **Todd McClelland**, a partner at the law firm Sterlington, presented tactics accompanied with ample real-world examples. From the get-go, situational awareness is the key to cybersecurity, data privacy, and AI challenges.

The first section of the two-part presentation outlined key cybersecurity trends. First, Martin stressed the importance of training employees to act as a gateway to internal challenges, both intentional and negligent. He emphasized human risk management stating that "a human firewall is one of your greatest weaknesses. They're the ones that are going to click on something. They're going to click a link. They're going to answer the phone and share a password."

Using the blanket term "insider threat," both stressed preventing phishing scams as well as being cognizant of people inside the organization – employees, contractors, consultants – who wish to do harm whether through information and data theft, means that people are the key to cyber safety and the biggest challenge. AI compounds that threat by employees unintentionally giving away sensitive information in the benign effort to simplify or automate tasks.

1. RH-ISAC. (2024) RETAIL & HOSPITALITY INDUSTRY INSIGHTS 2024 Verizon Data Breach Investigation Report Analysis.

Additionally, AI has further complicated traditional human security measures by allowing foreign hackers to use tools like ChatGPT to create more sophisticated phishing attacks that replicate emails, now eliminating misspellings and weird translations.

Because of this, AI governance is extremely important. Having strong policies in place to decide what is appropriate to share with AI, defining what is sensitive company information and what could generate bias is worth considering, as well. Another trend noted in terms of automation: the big security risk of copyright and code infringement. As processes are automated using code – open source or not – that code might be then combined into different code, causing copyright infringement and other legal implications.

Trends in merger and acquisition activity (M&A) will have an effect on system priorities within merging companies. With M&A activity anticipated to increase, McClelland expects that will complicate the melding of systems between merged companies, creating new headaches in security. Private equity acquirers may dismantle systems after getting the proprietary info they wanted and consolidation could whittle down the number of vendor solutions involved, leaving all the eggs in one basket, so to say.

Additional Resources

Convenience Leaders Vision Group (CLVG) recently discussed cybersecurity at their October quarterly meeting. Download the report, ***CLVG Expecting the Unexpected: Foreseeing Potential Disruptions*** to hear their thoughts.

> “An event that happens can actually close your business down if you’re not properly insured. If the impacts of this singular event can happen, it’s not just a couple days to get online, it can literally shut your business down depending on what you have to do for disclosures and the fees you have to pay that you’re not really insured to do so or you don’t have enough financial capital behind it.
>
> ***Daniel Martin,*** *Chief Information Security Officer, Verinext*

McClelland expanded on these points, emphasizing the increasing complexity of cybersecurity insurance, urging companies to ensure that their insurance policies align with their risk profiles to avoid potential claims denials.

In the second half of the presentation, the speakers examined cybersecurity pitfalls. Supply chain resilience is one to watch, with the presenters highlighting breaches such as those at Colonial Pipeline, Kronos, Solar Winds and CrowdStrike.

From a legal standpoint, McClelland explained that hackers have figured out that targeting the bigger vendors allow them to get the “most bang for their buck.” Therefore, IT pros can’t be focused on just first-, second- and third-party data, but also fourth-party, and beyond since everything is so intertwined.

Another pitfall is AI deep fakes creating an access concern leading to PCI phishing and skimming attacks. The third concern is that data vulnerability necessitates strong governance. McClelland articulated: “It’s a simple matter of knowing what you’ve got, what data do you have and where is it?” The fourth challenge is cyber insurance which is now much more complicated to obtain. With constantly evolving policies and needs from insurance companies, they advised it is in everyone’s best interest to have an attorney specializing in cyber issues to review internal policies and liability risks.

Retailer Cybersecurity Points of View

After the presentation, members were invited to ask questions and provide their own experiences and approaches.

Human Risk Management and Training

A persistent topic was the role of human risk management in cybersecurity with most members having or wanting stronger policies.

Several members emphasized the necessity for stringent training policies, with **Bill Ridge**, VP of technology at Eastern Petroleum Corporation, **Erin Graziosi**, president of Robinson Oil Co. and **Sharif Jamal**, director of real estate and brand development at Chestnut Petroleum Distributors (CPD) Energy Co., among those noting the success of tools like KnowBe4 in transforming employees into vigilant assets.

Abierto President **Rick Sales** shared his company's hardline approach: a policy of "100% paranoia," where employees are trained to avoid clicking on any unsolicited links. This strict protocol, he said, had proven essential in avoiding sophisticated business email compromise attacks that target trusted company relationships in the past.

Similarly, Director of Business Development at The Convenience Group, LLC **Donnie Rhoads** described his company's "scorched earth" policy of extreme caution saying, "If you have a question or a suspicion, just don't risk it," which is frequently reiterated to company employees.

Martin, however, added some nuance to caution against fostering complete distrust, which could hinder legitimate business opportunities coming in via email or contact forms, and instead recommended decision trees to guide employees and the importance of integrating 'internal' email banners that flag potential financial risks or unfamiliar senders. Also, he suggests robust training on handling sensitive, versus public, information. McClelland highlighted the need for "defense in depth," suggesting immediate oral verification for requests of employee financial account changes.

He also reiterated the inevitability of cyberattacks and advised organizations to establish relationships with local FBI offices for quick responses to financial fraud. He emphasized the critical 72-hour window for recovering stolen funds and the importance of having an incident response plan ready.

Jeff Carpenter, director of education and training at Cliff's Local Market and **Jason Collins**, director of IT at Englefield Oil Company pointed out the challenges of high employee turnover in the industry, underscoring the need for ongoing education. Collins reinforced the necessity of consistent and frequent training, recounting incidents where external companies' compromised systems led to phishing emails targeting his organization, underscoring the importance of cross-verification.

Vendor and Third Party Risks

Throughout the conversation, participants agreed on the importance of proactive measures, including leveraging technology, conducting thorough assessments of vendors, and maintaining strong partnerships with regulatory and law enforcement agencies.

United Dairy Farmers Chief Information Officer **Chris Egan** admitted while his company incorporates basic security checks when selecting vendors, this discussion highlighted additional questions they should ask to improve their processes.

Abhi Patel, Director of Information Technology at Nouria Energy, raised concerns about assessing vendors, especially with the involvement of fourth and fifth-party providers like Amazon Web Services (AWS), which might have their own vulnerabilities. He questioned how businesses can navigate these risks effectively and ensure a comprehensive security posture across their entire supply chain. Addressing third-party vulnerabilities, McClelland urged companies to conduct thorough vendor assessments, obtaining attestations of compliance, and documenting security practices. Martin added that questionnaires and data aggregation tools can provide insights into vendors' dependencies, helping companies identify potential risks within their supply chains

Larry Bowden, director of sales, retail solutions at Invenco by GVR and guest of Invenco by GVR's CTVG member **Paul Kern**, reflected on the challenges of balancing retail customer satisfaction with stringent security measures. He underscored the critical role of people, processes, and technology in mitigating risks and noted how requiring double or triple checks for sensitive operations sometimes faces pushback but is essential for reducing vulnerabilities.

> "We see business email-compromised attacks all the time. And then the question is, what's the next line of defense? And one thing, if you haven't done it already, this should be the first thing you do, is your CFO, your controllers, whoever has got access to your bank accounts, they should know that if anyone ever asks them to change an account number, that they should be orally verified on the phone with whoever just made the request. But then you get down to deepfakes, which someone impersonates that voice. But that's the kind of thing, is to have defense in depth. Yes, you can't have 100%, but to have that next layer of defense.
>
> ***Todd McClelland**, Partner, Sterlington*

Industry-Specific Challenges and Solutions

Rhoads raised concerns about the vulnerabilities in fuel pump systems and hardware systems, unique to the convenience and fuel retail industry. Martin acknowledged the difficulty of addressing these disparate components but suggested solutions such as incorporating cameras for fraud detection and improving hardware security with new technologies like Bluetooth to track usage.

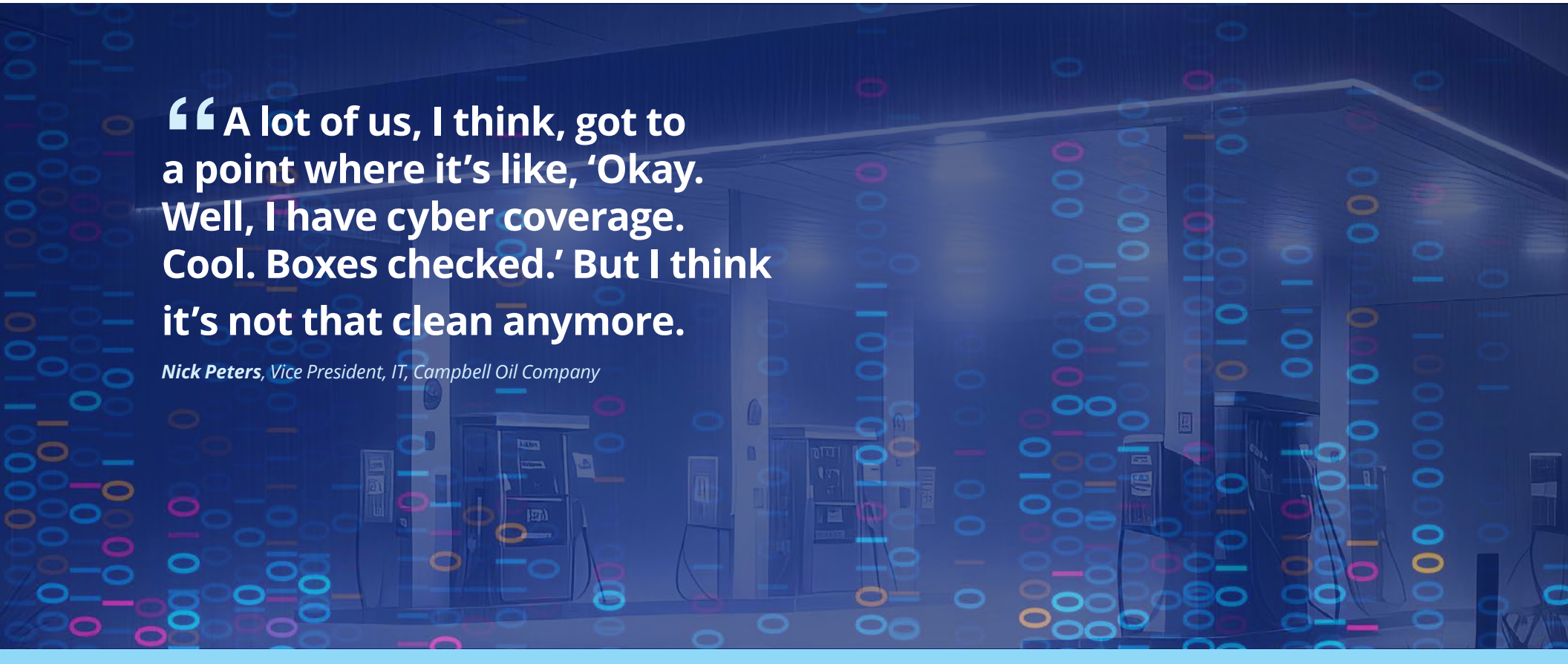
Tyler Grubbs, executive director of digital & store technology at RaceTrac, Inc. shared how his company tackles challenges like these by leveraging real-time data streaming from point-of-sale systems, fuel pumps, and in-ground tanks to detect irregular transactions, such as prolonged pump sessions with minimal fuel dispensed. His team also works closely with law enforcement, the U.S. Secret Service, and regulatory agencies, leveraging video footage and transaction data to aid in fuel theft prevention. Through targeted efforts like these, RaceTrac realized a 99% reduction in fuel theft.

With unique challenges inside the store, **Ant Raimato**, store technology engineering lead at Wawa Inc, discussed partnering with internal security teams to implement best practices that ensure both secure operations and a comfortable, trustworthy environment for customers and store associates. He highlighted the shared goal of maintaining customer trust and providing a safe, positive shopping experience.

Toot'n Totum's Vice President of IT **Rance Wells** expressed concerns about the slow industry-wide adoption of advanced security technologies such as tokenization, point-to-point encryption, and anonymization. He shared examples, including challenges with pin pad transactions and the ongoing risks of social engineering scams targeting store associates. Wells noted the turbulence in early digital payment systems before Apple Pay's standardization and pointed to the potential of AI to drive security innovation.

Safe or Sorry: Open Source Code

Nick Peters, vice president, IT, Campbell Oil Company raised a question about the risks of using publicly available code that isn't explicitly labeled as open source. McClelland noted that while the practical risk of being flagged for using such code is low, it becomes more significant during mergers and acquisitions. Companies can use tools to analyze the origins of custom software, potentially uncovering problematic code linked to open-source licenses. Though the risk is negligible, but not zero, it is situational and more likely to arise during due diligence processes. McClelland explained that while open-source licensing has become more defined, using unvetted public code remains risky. Such code could carry unknown licensing restrictions, similar to picking up an open soda bottle off the street "It could be good Coke or who knows what's in that bottle, you picked it off the street. And that's kind of the same with public software."



Small Operator Fire Hose

Roy Austin, director of information technology at Graham Enterprise, Inc. and President of HJB Convenience Corp **Raymond Huff**, raised the challenges of managing cybersecurity for small operators compared to larger organizations. Austin noted that transitioning from large corporations to a smaller business revealed to him the difficulty of managing security with limited resources. Small teams face a "fire hose" of responsibilities, often lacking comprehensive tools like cybersecurity insurance or edicated monitoring systems.

Huff echoed similar challenges, highlighting the reliance on external vendors to address issues such as penetration testing and data security. He also noted that hosting a loyalty program with sensitive customer data, despite not handling credit card information, adds complexity, too. He emphasized the importance of aligning with regulations like GDPR (The European Union's General Data Protection Regulation law) for customer data and continuously navigating evolving risks, from phishing scams.

For smaller companies, understanding what data they have and where it is stored is crucial, says McClelland. From a compliance perspective, businesses should create accurate privacy policies that outline what data they collect, how it is used, who it is shared with, and how long it is retained. Many breaches occur because organizations unknowingly retain data they no longer need and can significantly reduce legal risks and enhance their overall security posture.

Final Reflection

The meeting underscored the importance of proactive cybersecurity measures, from thorough employee training to vendor assessments to real-time monitoring. Members emphasized that while the threats are ever-evolving, the shared knowledge and practices within the group help them stay ahead of potential risks. Maintaining relationships with vendors, insurance providers, and law enforcement is also important to create a robust defense against cybersecurity threats.

New Vision Groups

In closing, **Myra Kressner**, president of Kressner Strategy Group and Vision Group Network co-founder, highlighted newly-created Vision Groups and Vision Reports, including the Conexxus Vision Group (CxVG), Electric Vehicles Vision Group (evVG), Convenience Foodservice Vision Group (CFVG), and Global Convenience Vision Group (GCVG), all aiming to uncover, understand and implement innovation for all retailers across the industry.

Review

LIGHTNING ROUND

In the quick Lightning Round discussion, CTVG members reflected on new developments and thoughts since previous meetings. With so many topics to consider from 2024 meetings, AI was the main area of advancement mentioned.

Jeffry Harrison, co-founder and president of Rovertown shared that his company has been testing advanced ChatGPT models to improve customer relationship management systems and streamlining one-to-one offerings. He emphasized the need to validate emerging technologies before full deployment, a sentiment echoed by others in the conversation.

Jason Collins responded that he was happy to hear industry vendors testing these AI applications, affirming a previous sentiment from retailers that they would rely mostly on vendor AI use than creating their own. A little later in the conversation, he bluntly said that "It's going to be overwhelming," referring to all the AI content and the data risks they pose. **Jeff Carpenter** also fears the prevalence and relaxed comfort level people have with AI and hopes for standards to offer a level of protection. While acknowledging the potential benefits, he stressed the importance of security standards to protect customer data and maintain organizational integrity.

Rick Sales added his perspective on AI, personally starting to use a tool called Read Notetaker to help him stay organized. From the Abierto perspective, they're testing using AI to create dynamic QR code content for on-premises advertising and create interactive dashboards that allow clients to query data intelligently. Sales also dug back into a previous meeting on Retail Media Networks (June 2024), discussing the progress his company has made with programmatic APIs for retail media networks, enabling seamless content distribution and proof-of-play tracking.

Finally, **Steve Morris**, president of Retail Management Inc., shared how his company, RMI, has operationalized AI in foodservice, focusing on customer-facing applications like managing roller grills. This technology enhances safety, labor efficiency, and stock management, highlighting AI's tangible impact on operations.

NOTABLE AND QUOTABLE

"And with the high turnover we have in this industry, that it's really just to focus on the people, people, people is what we do here.

Jason Collins, *Director of IT, Englefield Oil Company*

"In particular, evaluating the sites and being site specific, most of what we saw was where there wasn't as good lighting or where on the outside is where 99% of our fraud was occurring, fuel theft was occurring, is on those outside lanes furthest away from the store, furthest away from just enabling two or four lanes that are on that side, that stopped most of it. It's organized crime that's doing this. So as soon as word gets out, this store, this area, this brand is really cracking down and the dozens of arrests that we've now been able to help law enforcement do, word's gotten out that they're likely haven't stopped stealing fuel, but they're not coming to our lot anymore.

Tyler Grubbs, *Executive Director of Digital & Store Technology, RaceTrac, Inc.*

"Everyone on this call, it's the same goal. Our customer trusts us, our customer likes coming to our stores. Our customer knows that this is a safe place for us. So we are very focused on that from a technology standpoint all around to our business partners.

Anthony Raimato, *Store Technology Engineering Lead, Wawa Inc*

"I don't care how small you are, you should have a relationship with the FBI, someone preferably local...So, reach out to them, get the relationship and have someone on speed dial because it's going to happen.

Todd McClelland, *Partner, Sterlington*

"One of the things that I've been really interested in, I think you nailed a really good point when you were talking about cyber coverage and being concerned about having coverage is one thing, but are you actually insured for the things that you are potentially risked for? Because I think that's becoming a big deal.

Nick Peters, *Vice President, IT, Campbell Oil Company*

"One trend that's clear to me, and according to many studies, is that the retail industry is experiencing more breaches than any other business sector.

Ed Collupy, *Principal, Collupy System Solutions LLC*

VALUABLE RESOURCES

The quantity of materials on this topic would make for an insurmountable pile. To help you navigate through the masses, here are resources worthy of making your "must-read" list.

Ed Collupy, CTVG Facilitator

During our meeting we covered a lot of ground on the broad topic of cybersecurity. As I said, we could have taken any one of the trends and pitfalls and dove deeper in our time together just on any one of them. This made me stop and think about one word from the presentation that Daniel and Todd gave to us that stuck with me: "resilience." They tied it to the supply chain, but as I've reflected on this tough business and technology challenge in front of all of us, I believe that resiliency must be more far reaching. Do you agree that there really needs to be a focus on calling together leaders across your companies to ensure that there are solid plans in place to sustain the business when, what sounds like, some level of an inevitable threat will surface in most retail businesses these days?

Here's some advice from Harvard Business Review on balancing cybersecurity prevention and resiliency I've read since our meeting that fosters my point of view: *When Cyberattacks Are Inevitable, Focus on Cyber Resilience.*

Jeffry Harrison, Rovertown President and Co-Founder

CTVG members might be interested in this C*ybercrime Index* that was published earlier this year by researchers at Oxford University, identifying and ranking key global hotspots.

Cybersecurity has been a major priority for us at Rovertown, as it should be for any mobile app provider. For example, we see that intrusion attempts often come from certain regions, so we've blocked IPs from high-risk areas like China and Russia. We've also strengthened our two-factor authentication system so that only non-virtual, U.S.-based phone numbers can be used. To guard against man-in-the-middle attacks, we've added more encryption measures and integrated certificate pinning. We even use honeypots to detect and ban potential intruders. Finally, because attackers sometimes rely on costly telecom scams (such as using Somali numbers), we block those as well. All of these measures, and more, help us create a safer mobile app experience.

Myra Kressner, Vision Group Network Co-Founder

According to the Dec 13, 2024 article, *Microsoft Confirms Password Deletion For 1 Billion Users—Attacks Up 200%* in Forbes magazine, "The password era is ending...bad actors know it, which is why they're desperately accelerating password-related attacks while they still can."

Microsoft is encouraging passkeys instead of passwords. "Passkeys not only offer an improved user experience by letting you sign in faster with your face, fingerprint, or PIN, but they also aren't susceptible to the same kinds of attacks as passwords. Plus, passkeys eliminate forgotten passwords and one-time codes."

What are you doing about password security?

Rick Sales, Abierto President

The National Institute of Standards and Technology (NIST) provides a dedicated *cybersecurity page* with valuable resources and insights on cybersecurity and information security. I hope you find this resource useful!

Ed Collupy
CTVG Advisor/Facilitator and Principal, Collupy System Solutions LLC

CTVG
CONVENIENCE TECHNOLOGY
VISION GROUP

MEMBERS

VISION GROUP NETWORK CO-FOUNDERS

Myra Kressner
President, Kressner Strategy Group

Eva Strasburger
President, StrasGlobal; CEO, Compliance Safe

Roy Strasburger
CEO, StrasGlobal; President, Compliance Safe

Roy Austin
Director, Information Technology, Graham Enterprise, Inc.

Sanjit Bajimaya
IT Director, Loop Neighborhood

Jeffrey Carpenter
Director of Education and Training, Cliff's Local Market

Jason Collins
Director of IT, Englefield Oil Company

Christopher Egan
Chief Information Officer, United Dairy Farmers

Steve Evans
Chief Technology Officer, Haffner's/Energy North Group

Janeth Falcon
Vice President North America Technology, Circle K

Erin Graziosi
President, Robinson Oil Corp

Tyler Grubb
Executive Director of Digital & Store Technology, RaceTrac, Inc

Jeffry Harrison
Co-Founder & President, Rovertown

Raymond Huff
President, HJB Convenience Corp

Sharif Jamal
Dir. of Real Estate & Brand Development, Chestnut Petroleum Distributors (CPD) Energy Corp.

Paul Kern
Product Leader, Invenco by GVR

Bill Miller
Vice President, Head of Sales, GK Americas

Steve Morris
President, Retail Management Inc.

Abhi Patel
Director Information Technology, Nouria Energy

Nick Peters
Vice President, IT, Campbell Oil Company

Anthony Raimato
Store Technology Engineering Lead, Wawa Inc

Donnie Rhoads
Director of Business Development, The Convenience Group, LLC

Bill Ridge
VP of Technology, Eastern Petroleum Corporation

Rick Sales
President, Abierto

Emily Sheetz
Executive Vice President of Strategy and IT, Sheetz

Scott Smith
Senior Director of IT, Parker's

Cheryl Szczesniak
Executive Vice President of Human Resources, The Spinx Company

Thomas Valeri
SVP, IT, Majors Management

Rance Wells
Vice President of IT, Toot'n Totum

IN THE ROOM WITH CTVG:

Cybersecurity: Evolving Trends and Pitfalls

Convenience Technology Vision Group (CTVG) invites you to join us **In The Room** to experience our meeting on December 6, 2024. We are providing you with the entire conversation so that you can be "in the room" with us, rather than simply reading polished sound bites.

CTVG
CONVENIENCE TECHNOLOGY
VISION GROUP

Agenda

Topic Reference Key

CTVG's mission is to increase the institutional knowledge of the retail industry by sharing ideas and perspectives. For your convenience, we have placed topic indicators throughout the dialogue. Below is a key to the list of topics.

- Foodservice
- Leadership
  - Strategy
- Logistics
  - Supply Chain
- Workforce
  - Training
  - Internal Communication
- Marketing
  - Data Analysis
- Operations
  - Risk Management
  - Facilities
- Fuels
- Legislation
- Technology
  - AI
  - Barcodes
  - Camera Vision
  - Pump Technology
  - POS
  - Digital Advertising
  - Technology Infrastructure

CTVG
CONVENIENCE TECHNOLOGY
VISION GROUP

Ed Collupy

Welcome, Introductions, Meeting Rules

Welcome everyone. Thank you for joining us for our latest Convenience Technology Vision Group meeting. Ed Collupy here and we're going to tackle a persistent challenge I hear retail business leaders and IT professionals talking about, really when the question's asked them, what weighs on your mind the most across the business?

And I often hear data security, payments compliance security, physical and digital security. All in, it's cybersecurity. My reaction when I hear about the investments in time, money, and skilled people is both awe and thanks. Awe in the number of tools, policies and plans that companies like yours are deploying to combat bad actors and protect assets. And thanks that there are new IT leaders taking hold of the evolving threats, and it's not me.

We're fortunate to have two cybersecurity advocates and folks active in the cybersecurity world with us this afternoon. We'll meet Daniel and Todd shortly and hear from them about their thoughts on the trends and pitfalls of cybersecurity. Most importantly, we'll get to hear from you, our members. Your insights that you share with each other and across the industry to our Vision Reports are invaluable.

This screenshot [Publication and Antitrust Statement shown on screen] serves all of us as a reminder of the antitrust statement and publication acknowledgement that CTVG members, and our guests have signed. Our discussion is being recorded. Please keep in mind to use your camera and keep it on as much as possible. And remember to mute your audio unless you're speaking so we're not disturbed by anything else going on around you.

Your willingness to share and participate in candid and versed discussions is appreciated and important. Should you want to make an off-the-record comment, just let us know that what you're going to say or you have said is off the record.

As 2024 winds up, some of our members, including Roy Strasburger, one of our Vision Group leaders, are unable to make it with us today. They have sent along hellos and they'll miss being part of today's conversations. I also want to take a minute to introduce a new face and a new name to the Vision Group Network, Karin Thrift. Karin Thrift is going to be a customer-facing administrative assistant to the Vision Group team. It's a name that you'll see and you'll hear throughout many of the invitations and much of the correspondence that you'll be receiving will be coming from Karin. So just watch for that name or add Karin to your okay list of emails to be receiving. So welcome Karin, and thanks for all you've done in helping us get today's meeting off the ground.

I'm excited also to welcome a number of new CTVG members today. Tyler Grubbs, who's the executive director of digital and store technology at RaceTrac. Ant Raimato is the store technology engineering team lead at Wawa. Thomas Valeri, I don't know if Thomas has joined us yet, but he's the senior VP of IT for Majors Management, and Majors was a CTVG member when we originally started our CTVG group two years back. Sharif Jamal is director of real estate and brand development at Chestnut Petroleum Distributors, who I mentioned would be joining us at our last meeting. And it's also good to have Roy Austin back with us as he recently joined Graham Enterprise. So if each of you could just take a minute or so to introduce yourself and your company, that would be great. Roy, would you get us started?

Roy Austin

Hey everybody, I'm glad to be back. I missed one meeting switching over from Parkland to Graham Enterprise, but I'm starting my fourth week here and it's quite the drop going from a gigantic enterprise to a smaller branch.

Ed Collupy

Very good. Tyler?

Tyler Grubbs

Tyler Grubbs here. I'm the executive director of digital and store technology here at RaceTrac. So, if you're not familiar with the brand, we're a convenience store chain out of Atlanta. We've got about 830 locations across the RaceTrac and RaceWay banners and then fuel supply agreements under the Gulf umbrella at about a thousand locations across the U.S. Our responsibility is centered around anything in-store technology as well as any of the digital, web, and mobile assets, I think loyalty programs, websites, and any of that digital presence. So excited to be here. Appreciate you guys having me.

Ed Collupy

Thanks, Tyler. Sharif.

Sharif Jamal

Hi everybody. Nice to meet you all. I'm with Chestnut Petroleum Distributors. Also we run a company known as Chestnut Market. We're about 76 company operating stores and a little over 200 stores that are in our dealer network.

Ed Collupy

Excellent. Thanks, Sharif. Ant, whose formal name is Anthony. But he goes by Ant.

Ant Raimato

Ant Raimato. I work at Wawa in the store technology department. We're very similar to what everyone around here does, securing, deploying and supporting our store infrastructure from point of sale, fueling, order management, and things inside the store, outside the store, like loyalty and mobile applications.

Ed Collupy

Very good. I think that's everybody. Hopefully Thomas either joins us later or certainly on our next meeting. But thanks and welcome to all of you. We're real fortunate to have your voice added to the group and I'm confident you'll make a difference with the insights you'll share with us. For all of us as we get under way, let's remember to use the raise hand icon

as often as possible for conversation and I'll work to call on you in order. And of course, no need for raising your hand if you're in a back-and-forth discussion with somebody. Just keep that flow going. And if you're called or need to step away, you can either write a short note in chat or just leave and return when you're able to.

Roy Austin

I did notice the raise your hand icon. I forgot to say that Graham Enterprise is based in Vernon Hills, Illinois, 37 stores.

Lightning Round

Ed Collupy

So during our September meeting, we heard from Liz Sertl and Gena Morgan from GS1. They provided us with an overview of what's to come with the transition from the 50-year-old UPC barcode to the 2D barcode that can be the link to a wealth of new information. And then Cornell professor Randy Allen shared the results of her study into how and how well retailers are putting AI to real use.

In our latest Vision Report, "Technology ABC, & D's: AI, Barcodes, Convenience, and Data," we highlighted some key points including the transition planning from the UPC, possibilities for foodservice with 2D barcodes, challenges smaller retailers have with AI, and the need to partner with vendors. In 2024, this past year, we tackled even more topics during CTVG meetings looking at retail media networks and even made some predictions for what's ahead in retail technology.

So during this Lightning Round, I'd like to hear from you on any of the takeaways from any of those meetings. Have you pursued with your solution providers their readiness for Sunrise 2027 as a number of you said would be important? What AI tool is making a difference at your company? CTVG led the way this year with our retail media network discussion, so perhaps some of you have attended subsequent education sessions and conferences that have been held. So I'd be curious to hear what you may have learned there. And then, how close were Tim Tang's predictions on c-stores [from March 22, 2023 meeting]? He said that c-stores would become community hubs and that leveraging and analyzing mountains of data to understand customer behavior and optimizing operations would be key to the future. Would someone want to get us started? Jeffry, go ahead.

Jeffry Harrison

Yes, I was actually just in a conversation with Colin Dornish last night about this. So Colin Dornish formerly worked at Coen in Pennsylvania and now he is helping NACS with this initiative. So NACS is taking the 8112 initiative pretty seriously

with a combination of Thrivr and a lot of things they're working on. So we're in conversations with them and Gray Taylor from Conexxus about how to kind of roll this out in an efficient way so it's not just a grocery model. So we've been pretty deep in those conversations.

AI

As far as the AI front's concerned, I don't know if anyone saw recently, but **ChatGPT just launched the o1** (OpenAI o1 - new series of reasoning models) and it's pricing it roughly around $200 a month. So that is more of a **complex learning module**. We've been testing that already and beating the crap out of it. So it's been actually pretty interesting writing some new diagrams for some of our data flows. In case, for the new folks that don't know, Rovertown is an app company, so we are more of a platform like a Wix, WordPress, Squarespace for regional chains and we've been doing a lot of testing with that and trying to fix what everyone's working on right now, in our opinion, which is creating a CRM to better communicate and do one-to-one offerings with their customers. We've been testing AutoChatGPT stuff against the new model with that and it's been pretty interesting to see the results.

Ed Collupy Jason, I think you were one of the folks that mentioned it would be important to partner up with vendors relative to Sunrise 2027. Just wondering if you've had any conversations with your providers on that front?

Jason Collins No, nothing yet. I have not heard from any of the providers either. They haven't really mentioned too much at this point. And then what Jeffry said about the AI, a provider like his, like Rovertown, looking at AI is always good for us to hear, that they're evaluating that stuff and I would want to hear that from other vendors too.

Jeffry Harrison We're still working on it, so you haven't really heard from us yet. We're still trying to make sure it works.

Jason Collins It's good that your company is looking at it.

Jeffry Harrison Yes, we're doing a preview.

Jason Collins You're looking at it. That's good.

Ed Collupy Go ahead, Rick.

Rick Sales Yes, happy Friday, everybody. So I started using an **AI note taker** like OtterPilot – this one's called Read Notetaker. I had a meeting with a venture capitalist the other day and he was using it to record our conversation and then he sent me a transcript afterward, and I found it actually quite good. So I tried using it in a planning meeting today. I haven't had a chance to review the results, but these things get better every day.

AI

Editor's Note: Otter.ai and Read Notetaker are both note-taking tools that can help capture and organize information from meetings, lectures, and other conversations:

- *Otter.ai - Uses AI to transcribe speech into text and take notes in real time.*
- *Read Notetaker - Allows meeting attendees to collaborate on creating a meeting report.*

Barcodes

Just a couple of comments. I'm a fan of QR codes. We have integrated them in our solution. We believe that there's a real **future in on-premise advertising using the QR code.** And we have some new projects in that front because you can store a lot of data in these QR codes, and using AI we can generate them quite dynamically and have them have a lot of information. So we're very excited about that.

The other thing that I would point out, I'm like Jeffry. We are working on things, making sure that they actually really work, and there's a lot of really cool tools out there which come with great promises that you have to validate. But one place that I'm particularly interested in is our dashboard. And we work real hard to provide widgets and interactive UI/UX experience (User Interface/User Experience). And I came across a project where you could use a large language model to allow a user to talk to the dashboard and ask questions of the data. And I thought that was quite intriguing and we are pursuing that. Obviously, we provide a dashboard of standard questions on our data that customers are looking for, but the ability to allow the customer to ask an intelligent question of the data is quite intriguing to me.

Digital Advertising

And then finally, I would add on retail media networks. Abierto just released our programmatic **API (Application Programming Interface) for retail media network**, so our digital signage platform can receive a distribution request from another platform via API where a piece of content could come with attributes and we would automatically distribute it. And similarly, a request for proof of play data could be programmatically presented. So we are working with clients that have their own retail media networks and other retail media network providers to have them understand how they can host-to-host talk to us, deliver an ad that has been contracted, but also request the proof of play data. Still lots of work to do, but pretty exciting on all these three fronts. So thank you.

Editor's Note: API: a set of rules or protocols that allows different software applications to communicate with each other, enabling them to exchange data and functionalities by acting as a bridge between them

Ed Collupy

Has anyone attacked the prediction that Tim [Tang] made around data, that data is going to be important and employed any new tools or new strategies around data? Or think Tim was completely wet? Go ahead, Jeff.

Jeff Carpenter

AI

Jeff Carpenter here, Cliff's Local Market. We have 22 stores upstate New York. From my perspective, I see a lot of **additional AI being utilized**, particularly with our vendors, and considering us being a smaller chain and many of our vendors being much larger or having larger breadth or geography, we're seeing the infusion of that. But for us, we're in a place of updating our handbooks the first of the year. In looking at the security piece of that infusion, we look at payment card industry standards. We have a general outline of expectations and certifications and whatnot, and clearly there's not a whole lot out there on the AI end.

And as a smaller retailer looking at these opportunities, we have to constantly remind ourselves of what it is that we may be involving ourselves in. And as consumers learn more about AI, you see the new iPhone platform coming out with additional fusion of AI. There seems to be an **additional comfort level** being surrounded by the use of that AI. But again, that heightens my concern of what are the standards or future standards that should be in place to protect not only our customers but us as an organization as well.

Ed Collupy

Well Jeff, I think you've helped us with the segue unless anyone has any additional comment at this point for our Lightning Round. But with that, thank you for the comments that were made. Oh, Jason, go ahead. I'll let you add on.

Jason Collins

AI

Just one last thing on AI. It's **going to be overwhelming**. There's going to be so many different companies out there doing little things with AI that I feel it's going to become overwhelming of choosing the right ones and trying to figure out how it fits. And then the security side of it too. The bad actors start using some of these AI features to get into our business. That would be something we have to watch for.

Ed Collupy

Got it. Steve Morris

Steve Morris

Foodservice

Yes, since we last chatted, RMI, our company that operates stores for other folks, we've taken that **AI into the foodservice side** of things with a company called UpDog AI, which is helping us manage our roller grills. So from a foodservice standpoint, safety and security is certainly one, and employee and labor is one that we've been watching very closely as that has gone. But really taking this to **operationalize our foodservice programs**, specifically on the roller grill with some really, really good technology that confirms both the stocking and the replenishment and the sales of, and really using that AI technology from an operational foodservice standpoint out on the sales floor instead of back of house, which is where we've seen some other stuff in our other businesses. But this is certainly **customer facing**. So we're excited to roll that out and to see what that brings us here, starting here in a couple of weeks.

The Presentation

Ed Collupy

Thanks Steve. And that'll be an important part of our discussion, the whole technology side of foodservice as we look ahead into 2025. I'll talk about that a little bit later on. But thank you again everybody, but let's continue moving along.

I think the point about security that a couple of you made fits along with what our guest speakers are going to discuss relative to cybersecurity this afternoon. Let me introduce Daniel Martin. He's a field CISO at Verinext, and Verinext is a managed service provider of business technology. And alongside him is Todd McClelland, who is a partner at the law firm, Sterlington.

So, whether it's a ransomware attack or a data breach, through social engineering or phishing, an insider threat or third-party exposure, from malware or insecure IoT devices, the bottom line is, the need for cybersecurity is ever present. Daniel and Todd are going to review the trends they're seeing in their work on cybersecurity.

Data Anaylsis

One trend that's clear to me, and according to many studies, is that the retail industry is experiencing more breaches than any other business sector. A report from the Retail and Hospitality Information Sharing and Analysis Center identified **these following trends**. 91% of industries saw ransomware as one of the three most prevalent threats. 50% of social engineering attempts involved pre-texting to pressure victims into divulging sensitive information. 83% of breaches originated from external factors with 95% of those being financially motivated. And vulnerability exploitation, especially among third parties and third-party suppliers, increased drastically compared to the prior year.

The last finding has run really true to retailers who use supply chain management software provider Blue Yonder's cloud services – that came up just in the last week or so. Foodservice giant Starbucks, on the heels of the resulting outage of their scheduling and shift tracking system, said it would be paying their associates the prior week pay and then working to adjust once they're back online.

Another retailer in the news recently was Ahold Delhaize, who operates the Food Lion, Hannaford, and Stop and Shop grocery stores in the United States. The impact hit home to me. My wife and neighbors were chatting for days about empty produce bins and other shelves at local Stop and Shop stores. But what was interesting to me about this cyber incident was that each of Ahold's brands seems to have reported and, publicly at least, different areas of the outages. Food Lion on the pharmacy side, Hannaford on the loyalty side, and after being offline for 12 days hadn't informed customers

the details regarding the issue. And then Stop and Shop, their out-of-stock conditions, led them to issuing a $10 coupon to their rewards customers.

I found it really interesting that there would be this type of disparate reporting of the effects from the attack across brands of the same company and wonder if communications are a potential pitfall area retailers face.

Consumers question how cyber security incidents impact them, as someone just mentioned. And I wonder if their business of choice can be trusted. Just look at T-Mobile. They're picking up the pieces from various reporting disputing allegations that Chinese state-sponsored hackers breached their systems and stole sensitive customer data, saying their defenses have worked throughout their network and stopped the attack from advancing. The reports go on and on. Even across the convenience mobility industry we all work in, as Daniel and Todd know so well from their work with clients in this space. Let's have them take us through the presentation and points of view they have and then they'll join us for a discussion and Q&A. So please take notes, and they're happy to go back to a slide later if needed. So Daniel, you want to get us started?

Daniel Martin

Thanks a lot and I will encourage everyone to use chat as Todd and I are going to go through this deck pretty quickly to open it up to more collaborative conversation afterwards. Write down your messages, your questions in chat. That'll allow us to go back and make sure we touch them and we don't forget them either.

So like Ed mentioned, I'm glad to be here. I am with a company called Verinext. We're a value-added reseller, kind of like your SHIs or CDWs (IT Solutions Providers) of the world. We also have managed services that Ed touched on a little bit. I am their field CISO, which is a Chief Information Security Officer for those that might not be familiar with that term. And basically what that means is after 30 years roughly of IT security, I build programs around security and making sure that we're compliant in those natures with our customers. Todd, I'll let you do a quick introduction to yourself as well.

Todd McClelland

Thanks, Dan. My name is Todd McClelland. I'm a partner at Sterlington, as Ed shared previously. I'm also based in Atlanta, Georgia. I've been doing this for more than 20 years. My background is a bit technical. I started as a mechanical engineer. I used to program industrial control systems for, if you're down here in Atlanta, you may remember the old Ford Hapeville facility or certainly where they make the Mustangs up in Dearborn, Michigan. I've been both places and spent a lot of time around the country before I went to law school doing this kind of stuff.

Back then, security was a lock and key and a control panel, and it probably still is on the factory room floor. But what I've

been doing for the last 20 years is advising companies on just basic technology matters, but with a particular focus on both data privacy and cybersecurity, specifically cybersecurity breaches. And of course, with AI coming about, that's just changing everything and we're obviously expanding to that and looking forward to discussing that more today.

Daniel Martin

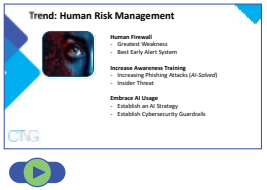
One of the things I'll say is if you don't have Todd's contact information, his is probably going to be more valuable than me because when you go through a data breach, if you do not have an attorney to advise you what to say and what not to say and put it under that client attorney privilege, some things can be open to disclosure in your mail and things like that. And Todd can talk about that for hours after if you need to.

But today, let's talk a little bit. Todd and I are going through the cyber trends and pitfalls today. So there's a couple of different areas. We're going to hit trends first, then transition into some of the pitfalls. So we're seeing four main things, and again, there's a lot of things that happen, but one of the four core things that we see, human risk management, AI governance, and we've talked about AI a little bit today, and automation. And AI and automation go hand in hand, but at the same time, AI is like a new term that we're throwing around every single day in our vocabulary. Automation's been around for decades and we're still trying to use it just like we're trying to figure out AI. How are we using automation to help us with a lot of the different problems we have with staffing and resources and just kind of being more efficient in our operational endeavors?

And then of course mergers and acquisitions and all those types of opportunities for new business development. You're going to see some of the pitfalls in that where you might be relying on a third party, and then that turns into a different type of company when they go through a merger/acquisition. Todd, anything to add here?

Todd McClelland

No, although I do want to circle back to something Ed said, and you said again, Dan, about communications. I like to think of clients just in terms of how important communications are and the impact on brands that breaches have. A friend of mine was talking about the Target breach years ago, and their saying is, "Expect more, pay less." In the wake of that data breach, someone suggested their new motto ought to be, "Expect more, pay cash." And so these breaches certainly have an impact on branding and reputation, and that can't be overstated and that's probably a good conversation for another time.



Daniel Martin

I couldn't agree more, Todd, because we'll have a slide later about brands. You've got to think about it. Cyber insurance, another topic we'll talk about in just a few minutes. An event that happens can actually close your business down if you're not properly insured. If the impacts of this singular event can happen, it's not just a couple days to get online, it can literally shut your business down depending on what you have to do for disclosures and the fees you have to pay that you're not

really insured to do so or you don't have enough financial capital behind it. So it's something, again, it's part of our pitfall, which we'll touch on later, but it's something definitely to keep your eye on to make sure that you have a plan to execute against.

Workforce

Training

So one of the first trends is **human risk management**. We want to focus on this because a lot of the aspects we're seeing today, we used to call it the human firewall. Human firewall is, one, your greatest weakness. They're the ones that are going to click on something. They're going to click a link. They're going to answer the phone and share a password. They're going to pretty much break your security, but at the same time, if you **train them well**, they can be your best alert system that says, "Hey, wait a second. This doesn't seem right."

Me winning a million dollars today if I click on this is just not right. It is too good to be true. And so embracing that human element and saying, "Okay, well, how can I make sure my employees that I have here, that they're actually going to be the greatest protection?" We're seeing a lot of trends to that and that builds into **awareness training programs** that they have today that even embrace a lot more of the short snippets, almost look like a TikTok or a Facebook Reel. Real quick, it adapts that learning curve of what they're used to today. And even in some of that repetitive action. We want to see a trend against insider threat. It's a term that we don't use all the time, but it's one of those that we're starting to see tick up as well.

Insider threat as individuals go from one company to another. And when I mentioned about AI here, the one aspect I want to think about is we always used to be able to identify phishing emails and attacks because most of the other countries that are attacking the United States, English is not their first language. And so they've always had typos here and there, or not using the right pronunciation or verbiage of something.

AI

AI solved that. All these hackers now are **asking AI to generate an email** from a US-based manufacturing organization as an office receptionist. And here is my email and include this link for phishing in there. And it's making it look very difficult to solve those problems. We want to embrace AI. We're going to talk about some strategies and governance around there, but also establishing guardrails. We're going to talk about coming up with use cases, but don't just dive in. And a lot of our customers, and I want Todd's input here as well, the customers that I consult with are looking at it as in AI, we need to come up with use cases first and we're creating pretty much a "you must ask before you get to use" policy in the organization and they're having a steering committee basically make a determination yay or nay if you're able to access those AI models because they just don't know how to really do that today with corporate data. Todd, what's your input?

Workforce

Todd McClelland

Well, let me add a few things. I love everything you just said there and I think you're absolutely right. We'll expand more on that kind of...I call it steer, but don't stop when it comes to AI. You're not going to stop it. You got to steer it, right? But kind of zooming back out on the **insider threat**, a couple thoughts. One, just consistent with what you're seeing. The trend certainly is more insider and we're seeing both it on the negligent insider, the person who clicks the phishing email with the prevalence of AI using it for sophisticated social engineering. That's on the rise. I'm also seeing a rise in intentional insiders, insiders looking to steal data, company secrets, whatever it may be. I had one involving a government contractor recently, employee decided it was going to go set up a competing shop across the road and stole a whole bunch of company data that includes some government data with it.

So we're certainly seeing a rise of that. Also, **insiders are more than just your employees**. When most of us talk about insiders, we're thinking our employees, of course we would, but our consultants, our contractors, anyone we give that kind of internal access to, they're an insider and we need to **treat them just the same we would as our employees** or at least hold them to the same expectations. A big issue with lingering insiders, we fire that person but we don't cut off their credentials. Still seeing that as a big attack factor, seeing lots of breaches where some employee, often disgruntled, comes back into our systems and wants to do some bad stuff to us. And so that's still a huge trend we're seeing. Employee theft I mentioned and kind of what you were going to towards there at the end is **employee use of AI.**

AI

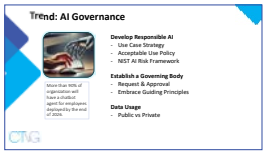
If it's out there, employees are going to use it. If they can see a way to work on some marketing and cut their work time to a fraction, they're going to go use an AI and have some AI generate an image for them. Or if they can write a letter, they're going to put all of that sensitive data into ChatGPT to write that beautiful letter. Now ChatGPT has your sensitive data. Here's another completely different angle when it comes to this kind of an insider thing, and that is the threat of whistleblowers. Everyone's familiar with, most probably are, the Joe Sullivan conviction.

Editor's Note: Joe Sullivan, the former Chief Security Officer (CSO) at Uber, was convicted of obstruction of justice and failing to report a felony in connection with a 2016 data breach

Workforce

What's going on with Tim Brown over at SolarWinds. Last year, 2024, maybe 2023 were the years where we started to see CISOs and other security and IT professionals start to become direct targets of government investigations, third-party lawsuits. And this is something where a lot of people are concerned. You yourselves might be concerned, but you may have employees who are concerned. So that insider threat is someone who's the **employee on the inside**. Maybe they see an incident that doesn't get fully disclosed. Maybe they see something that's not being shared with shareholders or

investors. They perceive something's wrong, right or wrong. That's another insider threat we have to think about. We need to have a program or an approach to deal with our employees or ourselves as whistleblowers. So just another thing to throw out there.

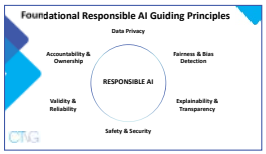


Daniel Martin

Another trend – **AI governance**. A lot of this is diving into that AI where what are we going to do? Come up with a use case strategy. Acceptable use policies are really a good way of driving that because you usually talk about that to your employees as well. Some of the acceptable uses, just putting lines in there that says you are not to use AI to augment your work performance unless it's authorized by your manager. Something like that. And the main thing about the AI that makes it difficult is making decisions on the company's behalf and what the legal impacts are to that. So we recommend thinking about **establishing a governing body** of inbound requests and how that's working. Create some principles, which I have a slide for in a minute.

Leadership

And then really understanding that when you start talking about the data that AI gets to read into and use, is that a public AI like ChatGPT or is it a private one, like a private Copilot that accesses your data specifically? So how are you going to use it and what data you're going to give can change exactly how you're going to govern that in a business.



And if you take the approach of just responsible AI, think about these aspects like being fair and biased decisions that AI can make, that can come into where you're starting to feed it, making decisions. Steve was mentioning about using UpDog and then making sure that that visual AI awareness making decisions, is it good, is it bad? Well, when you do that with resumes and things like that and making decisions because some keywords like I live at 420 African Boulevard. Oh, now I'm a black person that smokes marijuana. And that's a bias put into your AI. You have to validate certain things like that when you start diving into AI. Todd, anything you want to add real quick?

Legislation

Todd McClelland

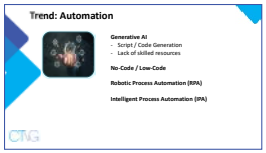
I'm going to be quick on this one, but the first overall message is this is a trend. It's not going away. You got to get in front of it just to state the obvious, but more specifically, regulators like to regulate. You'll never see anything a regulator doesn't want to put a law in front of. And this is no different. **We've got laws coming** all over the place. And if you go back to that chart real quick, they're hitting every facet of this chart. We don't show as civil rights, but that's a huge one. And bias, there's a study that showed that a lot of companies in the marketing side like to do look-alike audiences. This is our customer base. We want to have more names we can market to who look like this. Well, guess what? If those people all live in a white affluent community, what do you think the output is going to be?

Legislation

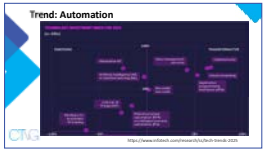
More white affluent people. So garbage in, garbage out, some would say. So we've got to be very mindful. **There's laws here.** They're coming about quickly. They're coming out from places like Colorado and Utah. We've got NLRB, we've got privacy laws and being transparent about what our algorithms do. I love these laws with transparency and what the algorithms do because no one knows. I mean, all this data goes in and we train it. And if you're going to have someone explain how it made a decision, no one knows. So regulators are creating these laws that I don't know how we're going to comply with them, but they're coming rapidly and that's going to be the biggest challenge and they affect nearly everything you've got here. Privacy, transparency, automated decision making, consumer rights, employee rights, intellectual property. I'll get back to that one later, but it is just the message you hear is be mindful that there's **laws covering nearly every facet of using AI.**

Daniel Martin And legislation too. So we've got that coming out from White House and other places.

Todd McClelland There's more and more. Exactly, Daniel.



Daniel Martin Another trend is automation. We used to do it in a lot of the different types of manufacturing, you're doing robotic processing, intelligent processing. With resource allocations and being equipped to be able to execute, no code applications are coming out where again, using AI to generate Python scripts in various word functions and capabilities in there. It's changing the way we're going to be able to execute by just using our language. Again, and it's helping us. And we're getting into a lot more automation space to how do we make sure we keep our performance high. We do not need a data scientist to be able to be more effective and efficient. Todd?



Todd McClelland Real quick, we got to be very mindful of the **employment implications of using automation**. There was a big strike that was threatening the ports on the East Coast and one of the things that people were threatening to strike over, they may have even struck for a few days, was the use of automation in port facilities. And so that's not relevant to this group of course, but it is to the extent that we're starting to use automation in our stores, in our food processing, in our supply chains. This is going to be something that people are going to start to see. Jobs are going to continue to drop because of automation. So we need to be very thoughtful about the labor and employment implications.

Workforce

On the code deployment, where does this training come from? Well, it comes from GitHub and other big source code repositories. What's in those repositories? A lot of third party copyrighted code, a lot of open source code. I think we're going to see, and we're already starting to see it, a lot of people saying, well, hold on a second, my intellectual property is now getting coded into your code and you're infringing my code, patents, copyrights, trade, secret rights, whatever

it might be. So just one thing to be mindful of here is if we are using any kind of AI for code development, there's a very real risk that we could be infringing someone's intellectual property with whatever comes out. Just something to keep in mind.

Editor's Note: GitHub: a web-based platform that allows developers to store, share, and manage code

Daniel Martin Great points. And I just leave this chart up here as you talk about what's being invested in next year. A lot of the topics we've been talking about are the trends in here. So again, just something to be aware of about where the investments that people are making today in their organization. And if you're not on board, you're already behind.

Todd McClelland I like that.

Technology

Daniel Martin And lastly, mergers and acquisitions. We're seeing this a lot in how we handle technology. And again, as a value-added reseller in **evaluating technology**, we're seeing a lot of consolidation of the tool sets. We're seeing that consolidation dive into platforms. So now it's not just a single product and now I have 27 IT technology products that handle security. I'm going to be able to consolidate those through those acquisitions into a single platform, a single point of glass so to speak, where we're pulling together best of breed as well as enterprise legacy products that are still very robust and mature. And we're bringing all those together to really make it easier where you can kind of get all the visibility, all the data comes from one place and you kind of have, again, limited staff working for you now. Those people have access to be able to make better decisions because again, some of that consolidation.

And with private equity, we ask are they doing well? Some private equities like to flip companies, some will pull it together and literally just dismantle an entire product, but they want the backend data, the user information, the proprietary information, the code to build some onto other applications or functions and services that they have. So sometimes it's better together. And then companies that were public have gone private. And without private you don't have as many compliance needs as you have. The disclosure of breaches do not have to happen in the same way. Todd, what do you see from that legal standpoint here with mergers and acquisitions?

Technology Infastructure

Todd McClelland Three points. One, the last two years have been pretty slow in M&A. I think with the new administration, everyone's projecting that next year might be a strong year in M&A. For all of you, that means more acquisitions or divestitures, which means you've got companies that you're suddenly responsible for if you're responsible for security. But it means more work, frankly, and it means more risk because now we **suddenly own that company's infrastructure**.

We're responsible for their data, whatever their data may be. So that's the thing on just the overall M&A. I think you're right on private equity. Private equity is hard to read. I've seen some companies get bought by private equity companies, they're stripped down, service goes down, quality goes down because they're trying to really reduce cost in order to flip it for a profit. On the other hand, I've seen some companies improve because they use that the first company as the platform through which to aggregate a bunch of other companies, and that one company becomes a much bigger company, more resource, and it becomes better.

So it's kind of hard to read what happens when a vendor of ours goes through or a partner goes through private equity, but it something we always want to kind of just look at. On the consolidation, I think I agree with you, Daniel. That was my thought that we're seeing a lot of acquisitions. We saw Mandiant get bought by Google. We saw Splunk get acquired by Cisco. So we're seeing a lot of acquisitions. And there again, what happens? With fewer companies out there because everyone's getting bought, we run the risk of being siloed down a particular vendor. Do we go all in with Palo Alto? Are we going to be an IBM shop? What are we going to do?

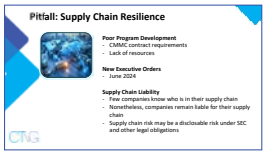
Microsoft, I mean, a lot of people are going over to Microsoft Defender. It's a good EDR (Endpoint Detection and Response) solution, but they're going away from the Falcon or Sentinel One or whatever and going to Defender because they're getting a cheaper price as a part of their overall enterprise procurement. So those are just things to be thinking about.

Daniel Martin

AI

And that drives us now from the trend setting to some of the pitfalls. And we also threw in four options here that we saw as pitfalls in supply chain management. Todd already briefly touched on this a little bit with what's going on in third and fourth chain, and we'll talk a little bit about that.

Deep fakes. This is again, AI taking it to the **next level of faking and espionage** and fraud and the whole thing other areas like that. And where there was AI, we want data governance, just the data governance and lack of data governance because we're private companies under a new kind of private equity, maybe we don't have the same aspects of governance that we should really be prioritizing and it's biting us in the rear. And then cyber insurance and making sure that you're doing what you need to do to ultimately retain cyber insurance because it's getting harder and harder to actually keep each year.



Supply Chain

Legislation

Risk Management

Every year, there's a lot of breaches and there's a lot of costs to those. So pitfall number one is **supply chain resilience**. This comes back to Colonial Pipeline. Ed mentioned three others. Colonial was local to us on the eastern seaboard, both Todd and I. For those that really rely on our supply chain stores, Kronos had a breach that created an outage for all the time clocks and things like that. This happens because you're not doing any governance on your parties and fourth parties and you kind of don't realize are they doing their part? Are you doing your part as custodians of data or delivering services? So poor programs, CMMC (Cybersecurity Maturity Model Certification) really gets back into the Department of Defense. There's new requirements that if you want to actually scrub toilets at an Air Force base as a service, you have to comply with government regulations now.

So it's not just like, 'oh, well I don't touch data.' No, if you are on property, if it's access, it goes a lot of different ways now and the government's setting a lot more standards. You've got **executive orders** coming out with how we handle AI. What we're doing with this, we all are going to have to **level up our game**, especially our supply chain game because we've relied on people managing our computers, managing our access control, managing everything for us to do a better job, so we don't have to do it. It's not our forte and we don't really have those trained people. And so then it turns around when there's a breach, we just do finger pointing. Todd, how are you seeing it on the legal side?

Todd McClelland

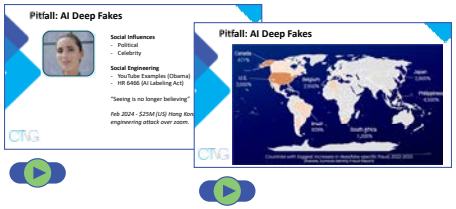
Hackers are efficiency minded. They're going to go after a company where they can get the most bang for their buck. And what they've seem to have found is if they go after SolarWinds or CrowdStrike or any of these other vendors, by hitting one company, they get multiple companies. And so that's why they're kind of the big flavor of the day is because hackers have realized this, although I think they've known for a while. So that's the pitfall. But a couple thoughts about that. Number one, you're ultimately **liable for your vendors**. And so the peril here is your vendor has a breach and you're the one who's holding the bag which partly becomes a contract issue. How are the **liability limitations** drafted and who indemnifies who and who's ultimately responsible for that? But the chances are it's probably you, which also becomes an insurance angle we will come back to later.

But then we also have our fourth parties whom I'm really concerned with, which is who are the vendors of our vendors or their vendors? I mean, it goes on endlessly, but that's the risk here is just really getting our arms around that. So what do you do about it? I think it's a matter of, first of all, knowing who your vendors are. We're still dealing with a lot of shadow IT out there that no one knows about and knowing what data our shadow it is getting. So it's a matter of figuring out who our vendors are and what data they've got. Are they worthy of being our vendors, doing **risk assessments**, having kind

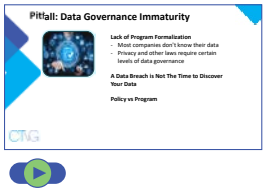
of an overall vendor risk management program. These aren't projects. I say these are programs. That's something we need to be continuously in front of, but that's the risk. If they have a breach, it's on us. We're the ones who are holding the bag and there's compliance issues that go along with that, including AI. So that's the overall risk that I see, Daniel.

Daniel Martin

And it's the contracts, making sure you get those things in the contracts appropriately before you bring them on, not relying your business on them and then being like, oh, can we change this?



AI



Leadership

Deep fakes, if you haven't heard about deep fakes happening, it's **influencing decisions**. It's influencing what we do, how we do. Seeing is no longer believing and what you think can't happen, I mean, it's happening today. And if you Google Obama deep fakes, you're going to see examples that you can't believe are really happening. So again, government's getting it, they're seeing it, but if you don't take any type of consideration, you're just in the mindset that it doesn't happen to you. It's going to. The U.S. is 3000% up on deep fake fraud. It might not happen to you, but it's the same aspect that 'I don't need to worry about PCI (Payment Card Industry) phishing and skimming machines at my stores.' Surprise, you probably do now. And this is just one of those things, if you're not thinking about it can really bite you in the butt.

And then another pitfall is the **governance**. Immaturity. It's not something I need, is it a single piece of paper in a checkbox versus what Todd had mentioned, a program to manage something. It's constantly being evaluated and assessed on a normal basis. So things like that. If you don't have something in place today and formalizing what you're looking at, those are the things that really can get a company [in trouble] because you're not **doing your due diligence**. If you can ask, are you doing your due diligence to protect your customer's data that you are in possession of? And you can say, yes, great. How are you doing that? And just make sure you have an understanding of that. Seek advice on how to build those if you need to. But it's just not going to happen to me. It's just not going to be good enough for corporate companies that get impacted with these threats that are happening to all of us. And we've talked about them.

Todd McClelland

When deciding on that, Daniel, yes, there's a big compliance angle on that. A lot of people have varying degrees in their **governance program**. I've seen these big elaborate programs. For smaller companies, it's a simple matter of knowing what you've got, what data do you have and where is it? And the reason you need that from a compliance perspective, is you may have to put out a privacy policy where you're supposed to disclose what you collect, what you use it for, who you share it with, how you retain it. And if you don't even know what you got, how can you possibly get an accurate privacy policy? And then on the cybersecurity side, how do you protect it if you don't know what you got and where it is? And so it's just a fundamental blocking and tackling matter and just knowing where your data is, what you've got, so you know

what you got to protect. And once again, if you don't, I can't tell you. Most breaches I do, it's a matter of we're sitting there doing forensics and finding what data they've got that they didn't even know they still had. So it can greatly reduce your legal risk if you know where your data is.

Daniel Martin

I completely agree. And when you think about, especially from credit card, because most people here have some type of credit card data, if they even store some of that or use it in transactional, each record of data is about $35 to $55 that if it's breached, that is how much it costs every single record of your company to pay. And you better have the right coverage in your insurance policy to cover that or else again, it can bankrupt your company.

Risk Management

And finally, the last pitfall we have is cyber insurance. It's harder to get today, the constant increase in controls. You used to be able to answer five questions to **get cyber insurance**. It's up to 300 something now at different times and different brokers are dividing it instead of just one or two. It's now 25 brokers depending on what your policy cut terms are. So service accounts, these are those administrative accounts, the privileged accounts, the 'god accounts' of your systems and applications. Know who they are, know where they are. Everything needs to have multi-factor authentication enabled on it today. If not, you're almost going to get declined in this. Todd, last thoughts on this?

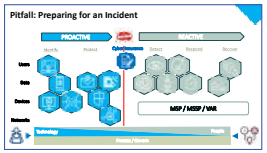
Editor's Note: In IT a "god account" refers to a user account with unrestricted access to a system, essentially giving the user complete control over all functions and data

Strategy

Todd McClelland

Well, first of all, and this is not self-serving, is get **legal counsel to advise you** on your cyber liability policy. This is not what I do. So this is not a self-serving statement. This is me looking out for you guys, but get an attorney who knows how to do this, who knows about cyber liability policy. Have them review. Your policy needs to actually squarely align with whatever your risk profile is. Is it cardholder data? Is it employee data? What's your risk and is it covered? These policies are evolving. A lot of the new risks are being expressly excluded from the policies. So you need to make sure that what you're being insured for is what you're at risk for.

And like I said, get a lawyer to advise you. Don't rely on your broker, I just wouldn't. I've seen it go wrong before and I'd advise you. And that questionnaire, Daniel, you're exactly right with that. They are long. They can and will be used against you. What you put in there, you have to be very careful about. If you don't do something and you say you do and you later have an incident and that's in any way a trivial incident, it'll be used against you to deny your claim. And so you've got to be very careful with that. I'd have a lawyer look at that as well, an insurance lawyer. That's not what I do. So this is not self-serving. So those are my two quick little bits of input on that.



Strategy

Daniel Martin

Great adds. And finally, I just want to throw this slide up. It's a visual that I use when we talk about when something happens, like when you actually have a ransomware breach and so forth. To the left of this line with cyber insurance to cover, having that helps cover a lot of your coverages. But the main thing is you **do a lot of things in your technology stack and your people** and these icons represent different programs like email security and Microsoft Defender for endpoint for EDR (Endpoint Detection Response). That's what it represents. They're all things, and if you look at the bottom, it's all technology you've invested in to protect you from these events from happening.

But when they do, I want you to know that all the action you do to detect, respond, and recover requires people. And if you do not have the people, your partnerships, your vendors, things like that in place today, if something does happen, it's going to take days if not weeks to months to recover sometimes because you don't have the right people in place for that. So on that, Ed, I'm just going to pass it over to you for some questions and answers.

The Discussion

Ed Collupy

Well, thank you very much, Daniel and Todd, for all that you shared with our CTVG members this afternoon. That ever prevalent and ever evolving threat and the diligence needed in this one aspect of technology to avoid the pitfalls is really immense. Keeping an eye on the trends and working towards avoiding the pitfalls isn't easy. It's more than a full-time job, one that each of our member companies really takes on using different approaches given the diversity of our member companies and then perhaps they even have some first-hand experiences with the incidences, whether they're small or large, a threat or an actual incident that they've had themselves.

I'll be sure to share the deck with our members ahead of the Vision Report just so that you have it. I think having this particular presentation ahead would be a timely thing for you to have. And right now, it would be really great to hear from our retail members about your own experiences and approaches. For example, Daniel and Todd, point to the human element threat. And I think, Jeffry, your question goes to one that I had kind of teed up as well. So Jeffry Harrison and Jeff Carpenter, I'm sure this is probably on your mind too given your bailiwick at your company, but the question for you guys is, would you recommend **training staff members** to be 100% skeptical for inbound emails, text messages, phone calls, et cetera, from unknown parties. Jeffry says, "I would be curious to know the recommended balance of this approach." So thoughts on that one?

Training

Daniel Martin

I'll take the first pass on that from my perspective. So one is we always look at everything as people, process and technologies. It's like the triangle kind of perspective. If you can incorporate technology into it, such as smart banners for incoming email that says, hey, they're asking something about finances today, or you've never talked to this person before, **using technology to help** you validate the integrity of this email coming in or this text message. The second piece of that is the people side. And that is training them, and I **wouldn't say 100% skeptical** because if 100% gets to loss of business, you're going to lose opportunity where someone was just kind of referenced or whatever, and they're on the phone trying to get you to help them as the new customer, new supplier or whatever it is.

Training

But it's the catches on that. What are they asking? How fast are they needing you to do something? Is there a loss there for you? Sharing information like your boss's number, something that's public, can be a very safe approach to say, this is public information. It's easy to share. Private information, people who are in your payroll, HR, things like that. Maybe more caution in your training to teach them not to share that information to others outside because that's internal information, more confidential and that can help them in their decision tree. What should I do next? What should I say?

Todd McClelland

We see business email-compromised attacks all the time, and I agree with everything Daniel just said. And then the question is, what's the next line of defense? And one thing, if you haven't done it already, this should be the first thing you do, is your CFO, your controllers, whoever has got access to your bank accounts, they should know that if anyone ever asks them to change an account number, that they should be orally verified on the phone with whoever just made the request. But then you get down to deepfakes, which someone impersonates that voice. But that's the kind of thing, is to **have defense in depth**. Yes, you can't have 100%, but to have that next layer of defense.

Strategy

And have things like banners, like if it's an external email, flag it as an external email. That way if someone's trying to spoof an internal email gets flagged and caught and it's shown to be an external email address. "Why is Todd showing up as an external email? That can't be right. Oh, it's a spoof." So those are the kinds of things we're looking at.

Ed Collupy

Nick Peters asked a question in the chat and I'll come back to the other folks that have your hands up. I see them. But Nick, your question was around code and if code is publicly available but not explicitly defined "open source," what are some implications of using that code? Perhaps that's a Todd question.

Todd McClelland

Yeah, so does anyone remember SCO? S-C-O?

Ed Collupy

Yeah.

Todd McClelland

Technology

A long time ago, SCO was a company that purported to own the copyrights in UNIX. Some code supposedly got into Linux. So SCO sued IBM for copyright infringement. They also sued AutoZone and GM who are purported to be end users of it. But that's kind of what **started open source as a big issue** and when we had things like the GPL and the LGPL and Apache and all these other open source licenses. So what these licenses do, say if you incorporate GPL code, any distribution of that software has to also be under the same license, the GPL or what they call copyleft licenses.

Editor's Note: GPL (GNU General Public License) and LGPL (GNU Lesser General Public License) are free software licenses that govern how open source software can be copied, modified, an redistributed. Learn more at: https://www.mend.io/wp-content/uploads/2024/07/2024-complete-guide-for-open-source-licenses.pdf

And so the risk here is you go out, you use publicly available software, you don't know where it came from. It's kind of like picking up an open bottle of Coke on the street. It could be good Coke or who knows what's in that bottle, you picked it off the street. And that's kind of the same with publicly available software. You don't know if it came from SCO, you don't know if it came from some open source repository, what license terms. So you've got to use it at your own risk frankly.

Now that being said, what's the real risk in doing it? I mean if I'm being pragmatic about it, what's the risk someone gets access to your source code and then does some kind of like a Black Duck (a software composition analysis tool that scans code to identify open-source security vulnerabilities and other risks) scan, see where the source code came from? Never going to happen. But then that takes us to mergers and acquisitions where we routinely see companies, when they buy a company, if you've got custom code, they're going to run a Black Duck scan and see where the software came from. And if it's flagged as belonging to some opensource product, that might be something you've got to deal with.

But I would say that frankly the risk is probably low. But I wouldn't say it's no risk. If you're an M&A, it could very well get caught then through some kind of a scan, but that's the risk.

Ed Collupy

Nick, that take care of your question? Thumbs up. That's good. Let's see, Rick Sales, you were next.

Rick Sales

Training

Thank you, Ed. So just a couple of comments here I want to make. To Jeffry's question about being 100% paranoid and training your people, our policy is to **be 100% paranoid and to train** our people. I just feel hackers are getting so much better. I've had my people firewall come to see me and says, "This is not you, right?" Where the hackers know the relationships between the people in my company from LinkedIn and other sources and they're writing to my controller telling them that I've approved a contract asking for a payment. But my controller is looking at that and going, "I don't know about this contract and this doesn't sound like Rick."

So we've seen a lot of those attacks. I find them to be troubling because somehow, they understand the relationships between us. It's not just people trying to poach me. There's a company that was purchased by PDI a couple of years ago that had a policy on security that we believe in. And pardon my French, but their tagline is, "Don't click on shit." And that's our policy.

Strategy

And you know what? I mean you don't know what's going to happen when you click on something. You don't know what's executable you're going to launch. You are not even guaranteed that you're going to where it says you're going. So **our policy is you don't click on anything**. People are people so we remind people quarterly of this because people forget, people get tired and things of that nature. So just want to make that point.

Training

I also want to make the point that as we grow, we always felt that the goal is to be able to compete with enterprise level clients. So enterprise level clients have key security requirements that we try to be proactive because we believe in security, but they require a manual. All of them require a manual. I used to think this was a burden, but in fact I think **the manual is one of our most powerful tools**. And the manual covers three things and somebody made a similar comment earlier, our systems, our procedures and our people. And everybody has to read the manual and they need to understand what systems we have and what they do, what are procedures for verifying that, checking for penetrations, for verifying that our policy's up-to-date, what is our procedure? If there's a breach, what are we going to do?

So an ISRs (Information Security Requirements) manual, if you don't have one, you should look online and try to write one because it will allow you to communicate with the rest of your team about these things that they need to know about, what your systems are and what they do, what your procedures and what they're engaged in and what your people can and cannot do, who needs to have multi-factor authentication. It's a great way to organize what is a very big topic.

Editor's Note: ISRs: protects data through technical and organizational measures that meet international standards and quality guidelines.

Technology

And finally, I would add that as we evolve with this, we're an AWS (Amazon Web Services/AWS Cloud Security) customer and we've relied **heavily on a lot of the tools** that they offer and the services that they offer to protect our cloud space and to be able to deal with. There's a lot in there as well as in other places where you might be in a cloud environment.

So this is a real thing. If you're running any kind of host, this matters to you if you're entering into an agreement with a client, they want to know and you want to know what you're doing to protect them and to protect yourself.

Training

And the manual might seem like a minor thing, but I got to tell you, it's a great point to talk with your people. It's a great point to talk with your customers and it's a great document to define for your company what you're all supposed to be doing.

Ed Collupy Jeff Carpenter, I'd be curious to hear your thoughts. I think your bailiwick at your company is around training and development and those types of things. How do Rick's comments hit you around training and stuff?

Jeff Carpenter I mean that's key. I mean, when you think about the number of people that you have under your umbrella, I mean there's so many opportunities for those types of malicious penetrations from a numerous variety of opportunities. So unfortunately, the malicious individuals are always going to be one step ahead, so to speak, so there's no shortage of time or investment in those areas.

Ed Collupy Very good. Donnie, you went next up.

Donnie Rhoads Yes, two things I guess. First of all, I agree with what Rick mentioned about his policy on Jeffry's question. We are **100% skeptical** as well. It just seems like these people never rest and they're getting smarter and smarter at ways to try to find weak points in our people and in our systems.

Strategy

We're a smaller company, so what we tell our employees is, "If you have a question or any kind of suspicion, **call me.** Literally, you have my cell phone number and I will tell you what you need to do." And usually it's ignore or forward it to me and ignore, that kind of thing. We're getting hit with spam calls and that's the one that they spend the most time, I think, worrying about consciously, is because when you have another human on the other line saying, "Oh hey, I'm from corporate and I need to get access to this and that," that's worrisome. But then that makes me think when we keep adding more and more digital solutions and more and more stuff happens over a computer or on a tablet, that just increases the risk and decreases potentially their sensitivity over time to just, "Oops, I accidentally clicked that attachment and now it's running that code or it's executing an operation." I don't think that there's enough... there can never be enough visibility for that problem for us.

So that's a constant thing. It's brought up in pretty much every single meeting we have and our policies kind of scorched earth. If you have a question or a suspicion, just don't risk it.

Fuels

I wanted to pose sort of a question or a prompt both to our guests and to everybody else in the call. Most of us in this call, or a lot of us, **we sell fuel**, and so we have fuel pumps. That whole **architecture of that system is really unique**.

It's unique to our industry. In my opinion, that **creates weak points** in our hardware and access points that most industries and other cyber security professionals don't have to reckon with. So do we have any thoughts on best practices or guidance on how to avoid attacks or other things related to our fuel ecosystem and our hardware?

Ed Collupy So Daniel, I know that you have worked with a wholesale distributor of fuel and petroleum products. Did this challenge come up that Donnie's talking about?

Daniel Martin I think it always comes up, yes, because it's a couple things that safety and fraud always comes up into those conversations. Some of those aspects can be solved with some of the technology today, and that is just having **cameras and video cameras** that are more aware of crowdsourcing or violent attacks. They can identify guns in use and license plates and you've got Flock Safety (Public Safety Operating System) that does those and calls the police when there's warrants. Things like that help make safety more applicable in your environment.

Camera Vision

When you're talking now about more of like, "Well, how do I reduce fraud both from theft or credit card kind of fraud?", now you start diving a little bit more into the hardware. And that's very unique for every single distributor. It gets back into OT. We talk about **operational technology** and what that looks like and how do you secure it. **A lot of it is very slow to change** because when you want to, say, think about how to incorporate something, a new initiative aspect, even adding Bluetooth to be able to determine usage on pumps and things like that or access to who accessed it last and it's getting more identity connected to access, those have been challenging. We don't have really a best of practice because I'm not specialized in that area. I definitely can do some more research and look for you in those areas, but that's really...It usually gets into this cost versus reward final decision. When you start talking about using things that's usually more expensive than the way you're doing it now, and a lot of the customers just opt to do what they've been doing, maybe add another layer of physical processes to it. And that's how they've adapted to it so far, the rest of the crew.

Technology

Ed Collupy Thanks. Tyler, your hand went up when Donnie asked the question. Did you have something? I was thinking maybe you had something to add to his specific question.

Tyler Grubbs I could share some of the things that we've done. That was a really big problem for us on the RaceTrac side in 2013, early 2013, and 2020 too. And so we took a bunch of actions related to that in kind of a myriad of different ways. So I can share some of those things with you briefly here. And then if you're interested in talking more, happy to connect you with our team or the requisite folks.

POS

But a couple of things that we did. So we are actively **live-streaming data out of the point of sale**, actively live-streaming data out of the pumps themselves. We're a Gilbarco shop, so Insight360, remote management, and streaming inventory data out of the in-ground tanks themselves, marrying those three things up to say, "What is the point of sale thing happened? What does the pump thing happened? What actually left the tank?" And so relatively in real time, you can get a sense for something looks like it's going wrong. That transaction's 20 minutes long but only pumped one gallon. That's a little suspicious. We should maybe take an action, right?

Strategy

So some of those things that directly alert you intraday, in the moment, where you've got the **camera footage** and then again the ability to grab that footage to be able to then tie a face to a pump to a transaction where that's occurring is what law enforcement really needs. And so we've kind of **built an ecosystem and a people process** to make that happen **in partnerships with local law enforcement**, Secret Service, Department of Agriculture, all the requisite folks.

Pump Technology

And then on top of that, there's some physical components you can add as well. So we're a Gilbarco shop, they've got a **security stack** that you can do **inside of the pump itself**. And then there's a few other of the pump techs that have created some their own unique solutions that, think about when you pop open the bottom part of that pump, actually trips the breaker to the power to that unit. If I'm a tech, no big deal because I'm going to go back into the store, I'm going to flip the breaker once I'm done with the work that I need to get done. It's authorized use, they're there, they're under a work order, much better. And so you're in the event that that happens, you're at least stopping someone on that first instance. And one of the things that we saw too is again, cost versus reward.

Facilities

To put that out at 19,000 fueling locations across our ecosystem's pretty expensive, hot pockets in specific areas. And in particular evaluating the sites and being site specific, most of what we saw was where there wasn't as **good lighting** or where on the outside is where 99% of our fraud was occurring, fuel theft was occurring, is on those **outside lanes** furthest away from the store, furthest away from just enabling two or four lanes that are on that side, that stopped most of it.

It's organized crime that's doing this. So as soon as word gets out, this store, this area, this brand is really cracking down and the dozens of arrests that we've now been able to help law enforcement do, word's gotten out that they're likely haven't stopped stealing fuel, but they're not coming to our lot anymore.

And so some of those things are just a few of the number of things that we're doing to try to get really creative in that space. It was a very, very big problem for us. Again, focused on theft and diesel more than anything, less folks doing it after 87 [octane]. But that was a major problem for us that we put in a tiger team and had 15 folks working the problem

for six months and **saw an immediate 99% reduction in fuel thefts** almost overnight after turning in some of these things. So it was pretty successful with a financial impact, direct financial impact.

Ed Collupy Thank you so much, Tyler, for sharing those specifics with us. It's great sharing among the group to have those specifics. Bill Ridge, you had a question a few minutes ago, or a comment.

Bill Ridge Mine was not really a question. I just wanted to comment really quickly on the human factor, which is something that we were really concerned about, not just us, our people were too. We're a smaller retailer. Most of our people are not young, they're not tech-oriented. So we **decided to go with a company called KnowBe4** (https://www.knowbe4.com/). And we've had really good results with it. Our people were really scared at the beginning of all this, but after getting testing on this and mail sent their way that they shouldn't click on and they were worried about it, but they ended up being really good at it. We got really good feedback from them. There's also a big education piece to all of it. It's not just testing. So they've gone through all this.

Workforce

I think you had one on one of your slides that **they've become your assets, and they really have**. I mean the people really have changed from being something that we were really worried about, to are now educated and are making good decisions and pointing things out. So it's really helped us a lot. That's all really I have. That's really helped us a lot.

Ed Collupy Excellent. Thanks.

Daniel Martin Bill, that's putting a program in place right there. That's all it is.

Bill Ridge It's been great.

Ed Collupy Very good. Erin, I know one thing rang when Bill mentioned the employee profile that they've got at his company, and I know you've talked about being kind of a low-tech company in some of our discussions earlier. How are you looking at this and what Bill said using a tool like KnowBe4 or something? Have you considered that or using tools to educate people?

Erin Graziosi We've used that for years. So same. We talk a lot about different examples, especially from industry friends that we know. And when they get hit with something, we bring it up and share it. But yes, we use that same system. And so every month if you get an email because you clicked on something wrong, it's just a learning opportunity. But it's made people really question things.

Internal Communications

And I forget who said it earlier, but same thing. We've said, **"If you have a question, just get on the phone or walk to the office** and you can confirm real easily if it's true or not." So we just try to be very transparent about it all and try to keep very **open lines of communication** and encourage people checking in, like, ask the three questions. It's okay, no one's going to be offended. You're not kind of breaking any protocol. We'd rather have you ask. And so that's kind our method with that.

Ed Collupy Excellent. Thank you, Erin. Nick, you were next with questions or comments.

Nick Peters This question's actually for Todd. One of the things that I've been really interested in, I think you nailed a really good point when you were talking about **cyber coverage** and being concerned about having coverage is one thing, but are you actually **insured for the things that you are potentially risked for**? Because I think that's becoming a big deal, to your credit, that you called out earlier.

Risk Management

A lot of us, I think, got to a point where it's like, "Okay. Well, I have cyber coverage. Cool. Boxes checked." But I think it's not that clean anymore.

Todd McClelland Right.

Nick Peters And I wanted to get your perspective and opinion on like, I'm just going to throw up a specific use case, let's say a perpetrator gets into the network, convinces the AP department to make a change to account information and then wire fraud occurs. I'm curious, to your point, at what point from your perspective is it less about cyber coverage and more it cuts over to general liability. And I just wanted to get your thoughts on that a little bit to see what your perspective was.

Todd McClelland Nick, you're stretching the bounds of my knowledge there. This is where we start getting into insurance land, which when I took that class in law school, I found I would never do.

It's a great question. Is it under CGL (Commercial General Insurance), D&O (Director and Officer Coverage), E&O (Errors and Omissions Insurance)? Where does it exactly fit? It's a bit of a hot potato where the insurance companies, they want it to fall somewhere, which is not for the policy they've written. And so I don't know. It's a very common use case and it all depends upon how that policy is drafted and what are the exclusions, right?

For all of you guys, I would ask, are you guys covered under your D&O, director and officer coverage. With that risk, I was mentioning that **whistleblower risk**. That's the more common question I'm getting these days, "Am I covered?" Well, are you an officer of the company. And being a CISO is not being an officer necessarily. So these are all great questions you

Risk Management

asked Nick. I'm afraid I don't know the exact [answer]. It's going to really depend upon what your policy says. But that's exactly, to your point, that's what you ask your insurance lawyer about. And if anybody needs a referral, I'm glad to give you one. But those are the kinds of questions. Think about your risk. If you're doing your TRAs (Targeted Risk Analysis) right now for your PCI compliance, these are all things to be running those TRAs by your policy. But anyways, that's how I would handle that.

Ed Collupy Very good. Thanks. Jeff Carpenter put a note in the chat just saying that he's using the same product (KnowBe4) as Bill and Erin as well. So they do a nice job, he says, "I struggle to think of another industry where the exposure is as great relative to the high turnover, low wage employee environment."

And Jason, your hand's up. I didn't forget you, but maybe now you have two comments to make, which is great.

Training

Internal Communications

Jason Collins No, it's more of we do the **100% thing here, training**. It's all people when it comes to cybersecurity in our world. I really focus on making sure they put out **constant communication** about what the latest threats are and then make sure they're not clicking on links. And if they really have a question about somebody sending them something, to call that person, to get that confirmation, that they meant to send it or know they actually got hacked on the other company. So we've seen that a number of times too, where emails go out from a different company that come into here where the other company got hacked. So one phone call, we got confirmation, then we can go in and block that and find that. So we find that to be very effective. And with the high turnover we have in this industry, that it's really just to focus on the people, people, people is what we do here.

Ed Collupy Go ahead, Todd.

Todd McClelland Well, since we're kind of talking about this business email compromise and what happens when our accounts get hacked, just one thing I wanted to share. This is really important. If you have one of those kinds of attacks, someone's stolen money out of your bank accounts, someone told the employee in AP, as Nick was describing, to send funds here, or someone hacks the CFO and tells them, "Our new wire address is this," you've got about 72 hours from the time that your funds leave your account to get the money back. And time is of the essence. The FBI has a unit that specializes in this.

Strategy

I don't care how small you are, you should **have a relationship with the FBI**, someone preferably local. And know who to call in case you have any kind of financial fraud. Because if you move quick, you might be able to get the money back. So it's really important to have that in place. You're going to get hacked. It is just a matter of when, not if. I hate to be kind of

pessimistic there, but the best defense is just to anticipate it, be able to go have that incident response plan ready, have a phone number at a relationship you've got at the FBI. They will talk to you. They love to.

I spoke on the panel at NACS with the guy from the FBI. He's from their local Las Vegas office, and he'll tell you, "You want that relationship? We'd love to have a relationship." That's what they're trying to do is get their field agents to have direct relationships with local companies. So reach out to them, get the relationship and have someone on speed dial because it's going to happen. And if you move quick, you can get your money back.

Ed Collupy Thanks, Todd. One of the comments that was made during the presentation in terms of a threat was around M&A. And I think the guys focused in on M&A on the supplier side and solution providers side of how those have come together, as well as some considerations for the growth of M&A activity in the convenience industry. So that hit me, Abhi, because Nouria has announced an acquisition that's forthcoming. Know you can't share a lot, but how are you thinking about things like cybersecurity as you look to bring on another large group of stores?

Abhi Patel We are working on it, Ed. I can only talk a little bit about that, but yes, that's the biggest challenge that in this particular scenario, how are we going to bring or how are we going to extend the security measures, the practice, the policies during this, within transition and after the transition. So that's a new challenge for us. It's part of our growth and we're working on it.

Ed Collupy Excellent. Very good.

Abhi Patel I have a question.

Ed Collupy Go for it, please. Yes.

Abhi Patel So Todd mentioned about the fourth party and fifth party. So we all deal within our industry with a vendor, a solution provider, API, and now AI. And the assessment of the vendor, it's very difficult because everybody's using, as Rick mentioned, AWS. Well, Rick may have a solution, but then he relies on AWS. How do you come across a better program for vendor assessment, any vendor assessment you put together you always find a challenge in the next one. And not every vendor, most of them, unless they're big, has the full insight. And this is just a general question, I'm sure everybody is in that same boat.

Ed Collupy Todd, do you want to take that?

Todd McClelland

Sure. That's a great question. And when you're a smaller company, you have no leverage over these. You're not going to get AWS to change their terms, conditions, or their security approach. I mean, we've got to be realistic, right? We're not going to do that. Or even if you're in petro, Gilbarco, VeriFone, we're not going to get them to change their security practices. So how do we do it? I call it **creating a defensible position**. Let's find out what we can, let's get copies of their ROCs (Report on Compliance). Well, they're not going to give out their ROCs, but at least their AOCs (Attestation of Compliance), their attestations of compliance for PCI (Payment Card Industry Data Security Standard) . Let's get their security literature and documentation. And let's document that we've at least done some type of due diligence on these vendors. And if we have any kind of RFP (Request for Proposal), that should be a part of the RFP process when we're going out and getting them. But it's a matter of going out and getting whatever public information they have first.

Strategy

And then let's push them. Let's see **what information we can get from our vendors**, whether it's annually, every other year. You guys have limited resources. We want to be pragmatic about this of course, but let's figure out who our key vendors are. Where are we most at risk with our particular vendors? And let's see if we can't do some kind of assessment. Are they going to come in and let us do **pen testing**? Probably not. But let's see what information we can get from them so at least we can create that defensible position that we did as much due diligence as is reasonable under the circumstances.

Editor's Note: Pen testing or penetration testing is like hiring a friendly hacker to find and fix security weaknesses in your computer systems before real attackers do.

So what are we trying to guard against? We're trying to guard against, at least in my world, I'm guarding against some kind of a federal trade commissioner or a state AG investigation, and I'm trying to guard against some kind of a third-party lawsuit if we have a breach.

Now, when you have a data breach these days, there's going to be a lawsuit. It's almost guaranteed. And so we want to create that kind of, "We had reasonable security." That's what we're trying to create there. And if we can show we've done the due diligence, we hired vendors, AWS, who would've thought AWS would've done something wrong? They're the big vendor. They do it better than anybody. Or at least that's the story.

I hope I'm answering your question, but it is a matter of just trying to show that you're doing the best. Now, smaller vendors, maybe we can get a bit more from them. In which case, is it a questionnaire? Do we want to see if they have any kind of like an ISO (Internal Organization for Standardization) certification? What kind of documentation they can evidence to

us that shows someone has done some kind of an independent assessment of that vendor? So that's how I might think about it.

Abhi Patel Thank you.

Daniel Martin I'll add a little bit to that as well. Questionnaires usually include the first aspect of, "I want to ask you some questions on do you use in your services." And adding a question or an appendix to it that says, just like the insurance companies are going to ask you for your service accounts, I'd like to ask my service providers, who are your providers? Who do you rely on as well? You just trust that the answer is accurate as they've been giving it to you.

Data Analysis

But the other aspect is there's organizations out there that actually buy and **aggregate data sets**. So everyone comes from a public IP, so my domain is going to have a lot of traffic inbound and outbound based on certain IPs of digital footprint. There are companies that are actually tracking digital footprints and aligning that to say, I'm seeing this type of software access to Microsoft Office 365 or Splunk or these various companies. And they can make estimations that they use GitHub, that they use Adobe, that they use these things because of aggregated data sets.

And so some of that's happening today as well to identify those downstream aspects. But questionnaires are probably the easiest, but there are customers that do vendor risk management and they're looking specifically at third and forth through **data aggregation** and buying different data sets from different service providers or different data sets. Then they can tell you who's using specific software, who relies on specific architectures, ISPs, things like that because of just what they can find during that analytics side.

Ed Collupy Abhi, were you going to add something on after Daniel's comments?

Abhi Patel No, I think it's a useful insight. We have a program, we have the RFP process and all, but it's always challenging. It's time is of the essence, always business wants something. You are waiting for the third party. Third party has a fourth party. So that's always a challenge.

Daniel Martin And the biggest example we have right now is CrowdStrike. Like Todd mentioned a little bit when CrowdStrike had an operational impact, how many people now use CrowdStrike? If everyone in your entire vendor supply stream used CrowdStrike, even if you didn't, you are getting impacted. And so some of those things are really where, as an example today, you have something that you can lean on that says maybe we need more due diligence because I need to ask some questions like do you use Azure? Do you use Office 365? Are you a Google shop? And hit the big players where you can kind of now make analogies that says everybody in my supply chain uses the single piece of software, maybe I need

one person who doesn't use that. And that's just a little bit more resilience. But again, is the effort worth it? You have to determine that in your business.

Ed Collupy

Very good. Rick, I see your hand up, I'll come to you in a second. But Larry Bowden, I wanted to touch base with you just relative to this concept of third party because you often would be viewed as a third party here. How do you work against this whole cybersecurity in helping protect your customer base?

Larry Bowden

Oh my goodness. There's a lot of smarter people than I am, within Gilbarco and Invenco by GVR, that could speak to that Ed. And I listened to all this and as a solution's provider and a hardware provider, as consumer, all this stuff is really, really scary. I know that we have got a **dedicated focus group** around payment security primarily. And somebody mentioned earlier, what can a large vendor like Gilbarco provide? Articles of compliance? We definitely will provide those. One of the things that resonated with me is the triangle of people, process and technologies and how that all goes together. I know even within our own company sometimes the vulnerability is the people part, we try to take as much of that out of the equation and make it a requirement to double or triple check something. And we sometimes get caught out for it negatively. Like, this is too hard for me to get this information, or you should give me more access into that database. So sometimes it's hard to balance the commercial implications of we want to please our customers, but also we want to keep our customers safe and minimize the liability for our own company. So it's a balancing act and I don't think I really answered your question, but those are the things that are going through my mind as I reflect on the last hour and a half of listening to you folks.

Strategy

Ed Collupy

Thank you very much. Chris Egan, I'm going to put you on the spot. You've been working through a number of transitions to new systems and to Abhi's point of how do you put questions to vendors. Did you do anything in particular on data security in your search for vendors?

Chris Egan

We asked that, but there's certainly some questions that were brought up today that I'm kicking myself, oh, I should ask that one. But I can't say it was our prime factor. We're looking to make sure do they check some of the basic boxes and that was not our leading factor in our selections.

Ed Collupy

Very good. And just one more point I'll make relative to this third party and x-party kind of information. It was interesting today, mid-morning I got the email from PDI. First it said a security reminder, so I thought it was going to be something about PDI security and something there, but it was really PDI who for Daniel and Todd, you may or may not know, but

Todd McClelland PDI is one of the huge solution providers to the convenience industry.

Ed Collupy Know them well.
So their particular email today talked about the Salt Typhoon cyber attack that impacted major telecommunications companies. So here's a third party telling us about x-parties that we may or may not be using that have a potential threat. So I just found it interesting how this whole communications flow is moving.

[Comment removed at request of member]

Ed Collupy

Roy Austin, I'm curious to know, you've been at Graham now for four weeks. What's your first impression? Or what's it like walking into a new environment and having this challenge in front of you? What have you discovered?

Roy Austin

Well, like I said, this is a new small environment to me coming from Parkland and EG before that. With those companies, we had large groups of people that were monitoring all the stuff we're talking about today. And now we're down to a small group of people where we're questioning if we even have a lot of the stuff in place, like cyber security insurance and who's monitoring all of spam filters and all the fun stuff that comes with all this stuff. So it's a fire hose when you come into a small business versus having huge teams. But we're definitely looking for ways to be more secure and do everything we can to lock everything down here.

Ed Collupy

Very good. Yes, and I was thinking about you and Ray Huff when the comment was made about 15 people on a fire team that Tyler had. And Ray, how do you as a small operator deal with this problem of cyber security?

Raymond Huff

It's very similar to how everyone else is. We use outside vendors. The penetration piece is a big deal because we host a lot of data here, but we don't host credit card data. So it's not a PCI piece of it, but we do host our own loyalty program. That has phone numbers. And from the phone numbers you can really figure out who that person is.

Strategy

So on the cyber security side, **we adopted the GDPR (General Data Protection Regulation) stuff pretty quickly**, mainly because we were in so many different states all over the place. We just like, "okay, you want to be forgotten, boom, you're forgotten." Then they call us and say where are their rewards? They're like, "Hey, you said to delete everything and we did." But it is problematic for us, especially as we have new employees.

Some of you guys will remember this. The old thing that we used to deal with is people calling and getting our people to buy receipt tape. That was the extent of how much we could get hacked. That's no longer the case. I mean it's big money, it's deposits, it's all kinds of issues that we have to work through.

The comment about the insurance is a real big deal. We spend now, even when we do the renewal, we're spending three hours just going through on the insurance to make sure we have all the proper coverage for what we actually do have in house i.e. we run our own loyalty program, and they see that as some level of a risk. So we deal with it by using outside experts to help us through it.

Ed Collupy

Very good. Sharif and Ant, you're the new guys to CTVG. I want to give you a chance to chime in here. Thoughts? Ant want to go first since you hit it big in the alphabet?

Ant Raimato

Strategy

We bake a lot of the security technology pieces in. Of course a lot of good comments. The only thing I didn't hear explicitly was **pin pad**, right? All the different attack vectors, both for payments from a corporate perspective, but inside our stores it's a challenge. So we **partner a lot with our internal teams** from security. And we **trust their guidance** on a lot of best practices on how to deploy out to our stores. How to make it easy for our store associates to just look at the technology around them and really feel comfortable that we're providing a good experience for the customer at the end of the day, right?

Everyone on this call, it's the same goal. Our customer trusts us, our customer likes coming to our stores. Our customer knows that this is a safe place for us. So we are very focused on that from a technology standpoint all around to our business partners.

Ed Collupy

Thanks Ant. Sharif, here you are.

Sharif Jamal

Training

We use the KnowBe4 system as well, and its been going great for in-house training. Just getting everybody prepared and just **keeping everybody knowledgeable** about all these emails and preventing them from getting hacked and then retraining everyone. We're doing a lot more training in the field as well. We are doing a lot of online training for our day-to-day operations which includes some more cybersecurity through RTO (Ready Training Online). Generally we have an in-house IT department that actually has been extremely busy. We're just switching over to PDI, so a lot of new things are being implemented within our company. We brought in Dave Gauthier and he does a fantastic job and keeping everyone on their toes keeps us monitoring and really, we're hoping safe forever but who knows, with all the AI that's going on.

Ed Collupy

Rance Wells

There you go. Thank you, Sharif. Any last comments from anybody? Well with that Rance, my friend in Amarillo. Go for it, Rance.

Through all of these talks, I've been at this a long time now. It doesn't feel like it, but gosh, it goes quick. Tokenization. It just seems like us as an industry, we should be further along to where we're not having to throw all these regulations at it. So that we're doing a better job as an industry to where we're not having to have all the PCI regulations. Point-to-point encryption, tokenization, anonymization, all of these things in place so that a 20-store retailer or a 500-store retailer doesn't have to go through all of these hoops. I'm never hopeful in this industry anymore about that stuff. It's so slow to come to market, but those are things I'm always hopeful for.

There was this latest Verifone situation where tap-to-pay didn't work because people were able to do some store and forward stuff and take advantage of not paying for transactions. That was a turn-on-a-dime thing our organization had to do to get that up and running. It's wild that that can even happen. When Apple came to market with their wallet and did Apple Pay, I think a lot of people on this call remember the turbulence before that. Everyone had their own wallet and their own ideas, but then Apple came to market with that and it kind of standardized payments. I was hoping that tokenization that happens on that would trickle over to the rest of the world. It still hasn't, but Apple, and we were speaking about AI as well. This new release of Apple and Google and everyone else has their own flavor of AI inside there.

Strategy

It seems like the winds have changed too. **We've got to innovate with AI at the forefront.** And security, it's still there for what it is. "Card not present" transactions have gone up tremendously over the years. And again, to what Ray was talking about, we run into people calling the store and being very convincing with their social engineering and wanting someone to empty out the safe and go to a Bitcoin ATM in another town to go deposit.

This stuff happens. It's bananas that it can still happen, but we're always blocking and tackling even on that stuff in today's world. So that's really all I have to add to these conversations. It was really good. The presentations were great.

Thank you.

Closing Thoughts

Ed Collupy

Rance, thank you for wrapping us up. I really appreciate it. And I really appreciate Daniel and Todd for being with us. When we were preparing, we said that each one of the threats and each one of the pitfalls could have a conversation really of its own. So we wrapped up eight things and all the things that our members brought to the table this afternoon. Your willingness to share, your insights is really impressive. As I said at the very beginning, I'm thankful that there's folks like you out there doing this work and that I get to do work like this now. So, thank you.

So for our next meeting, we're going to talk about foodservice technology. And some of this was spurred on by Steve Morris and the work he's doing with UpDog. So Steve, I'll be in touch to make sure we extend the conversation. We might want to think about how we get to show it during our call.

But anyhow, you'll be receiving invites for next year's quarterly meetings early next week from Karin Thrift. Including the first meeting of 2025 planned for Friday, March 7th. So please be sure to reach out to me, send along any feedback from today or ideas you have for any other topics for our 2025 meetings.

I'll be at the RetailROI Super Saturday event and the NRF big show event, both in New York City in mid-January. If you're attending, let us know. And I'll look forward to seeing you certainly in March, but maybe at some events ahead of time. And with that I am going to turn it over to Myra who has some news to discuss regarding the kickoff of the Conexxus Vision Group that just started this past month, along with some other groups that are getting ready to kick off in the Vision Group Network.

Myra Kressner

Well thank you and thank everyone. And I know folks are going to be leaving, but absolutely want to thank our Ally Supporters Rovertown, GK, Invenco and Abierto. So we appreciate your participation and your commitment to CTVG. Also, good that Jason, you're coming to NRF. Would anyone else please let Ed and me know as well if you're going to be coming to NRF, either you personally or someone else from your company because we're looking to possibly do some VGN activity. So if you could let us know, that would be great.

Regarding the Conexxus Vision Group – Raymond , we have the pleasure of you not only being on CTVG but also the Conexxus Vision Group and we've got Donnie's dad, Don, is a member of CxVG as well as Dae Kim with Loop, and several others as well. Ray, do you want to just mention what you thought about the Conexxus Vision Group? Just even in relation to the couple of years that you've been on CTVG?

Raymond Huff The Conexxus Vision Group was extremely interesting and I realized I need to go back to school. There are a lot of people there that are a lot smarter than I am. And I think that when those reports come out, they are going to be really sought after in the industry. Just like this one. This one's great. This one I think will be very well read also. So, look for a lot of good things come out of that group.

Myra Kressner Yes, the Conexxus Vision Group. There was some question, what's the difference between that and CTVG? It really is actually looking at innovation. Not necessarily has to be technology innovation, but how does the convenience industry really engage with the practicalities of the innovation that is in other industries? And to be able to engage with that throughout the organization, particularly bringing in the C-suite into this conversation that everyone seemed to feel that that was very important as well. So thanks Ray.

We did have our first Electric Vehicles Vision Group, or evVG, a few weeks ago. And that was really interesting. We brought in the entire ecosystem of the EV world. And in fact Nouria is a member of the EV Vision Group as well. So you'll be reading more about that in the Vision Report. We have our first Global Convenience Vision Group meeting virtually on January 15th. And our Convenience Foodservice Vision Group is starting on January 23rd. And then of course we have our Convenience Leaders Vision Group that has been doing some really great things.

So if there's anyone that wants to participate in those groups, we're very open to your thinking about that. We welcome additional participation. And I know we've run over time and I don't want to do that. So thank you for everyone being on the call today, being part of Convenience Technology Vision Group. This was a great meeting. Thank you, Todd and Daniel, and everyone. Have a great weekend and happy holidays. Be well and safe and we'll see you next year.

CTVG

CONVENIENCE TECHNOLOGY
VISION GROUP

VISION GROUP NETWORK

BACK TO DISCUSSION

Cybersecurity: Trends & Pitfalls

Daniel Martin, Field CISO – Verinext

daniel.martin@verinext.com

www.verinext.com

Todd McClelland, Partner – Sterlington

todd.mcclelland@sterlingtonlaw.com

www.sterlingtonlaw.com

CTVG

BACK TO DISCUSSION

CTVG Views | In The Room with CTVG | Presentation

Daniel MARTIN, Principal Security Consultant, Field CISO

verinext

A Force Multiplier in Mitigating Security Risk Across Organizations

- Keynote and guest speaker for industry trends and cybersecurity alignment
- Balances people, processes, and technology to form defense-in-depth security strategies
- Eliminates threat vectors through evangelizing and awareness training
- Ensures regulatory compliance integrates best practices with automation technology
- Practitioner with 10 years CISO experience in healthcare and finance

HIS WORK

Daniel works to protect company assets by developing a security life cycle that's integrated with the fabric of the business. He uses human-centric risk mitigation strategies to deliver business driven outcomes

HIS EXPERIENCE

HIS CERTS

Industry recognized as a thought leader and mentor to the next generation

- CISSP
- CISM
- CRISC
- CDPSE

Former:

- *QSA*
- *C|EH*

LinkedIn: https://www.linkedin.com/in/atlciso/

BACK TO DISCUSSION

Todd McClelland, Partner, Sterlington, PLLC

Todd McClelland is a lawyer with 20+ years of experience advising clients on complex legal issues related to cybersecurity breaches and compliance, data privacy compliance, AI and technology transactions.

Todd's practice includes advising companies in all industries on global cybersecurity incidents, designing cyber governance and risk management programs, advising on global data privacy compliance issues, and supporting companies with data licensing and large-scale systems integration projects. He is also an experienced litigator in patent, cyber, privacy and tech litigation.

Todd has been recognized, among others, by The Legal 500 US and The Best Lawyers in America. He has also been named "Lawyer of the Year" in IT Outsourcing Law. Todd obtained his J.D. from FSU, and his bachelor's degree in Mechanical Engineering from Georgia Tech. Before law school, Todd programed and designed industrial control systems (e.g., PLCs, HMI systems) for companies such as Coca-Cola and The Ford Motor Company.

BACK TO DISCUSSION

CTVG Views | In The Room with CTVG | Presentation

2025 Cybersecurity Trends

Human Risk Management

Automation

AI Governance

Mergers & Acquisitions

CTVG

BACK TO DISCUSSION

Trend: Human Risk Management

Human Firewall
- Greatest Weakness
- Best Early Alert System

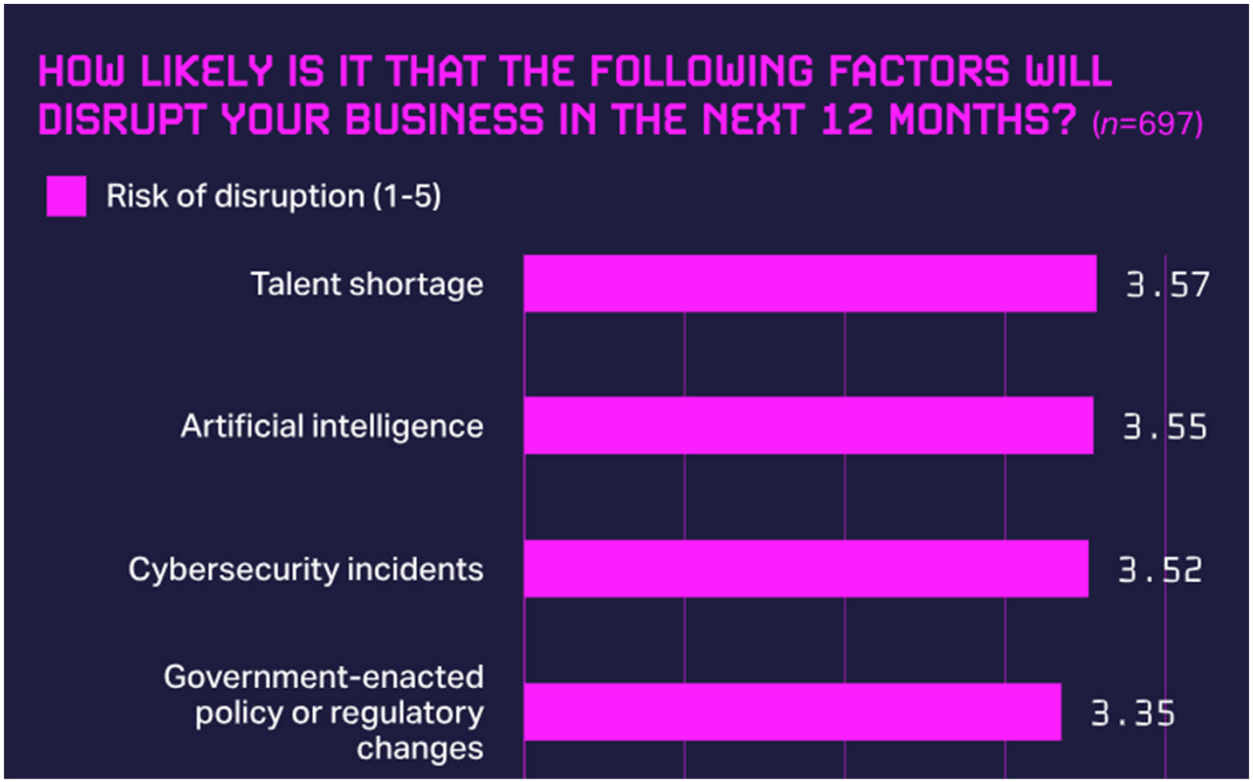
Increase Awareness Training
- Increasing Phishing Attacks (*AI-Solved*)
- Insider Threat

Embrace AI Usage
- Establish an AI Strategy
- Establish Cybersecurity Guardrails

CTVG

BACK TO DISCUSSION

Trend: Human Risk Management



https://www.infotech.com/research/ss/tech-trends-2025

BACK TO DISCUSSION

Trend: AI Governance

More than 90% of organization will have a chatbot agent for employees deployed by the end of 2026.

Develop Responsible AI
- Use Case Strategy
- Acceptable Use Policy
- NIST AI Risk Framework

Establish a Governing Body
- Request & Approval
- Embrace Guiding Principles

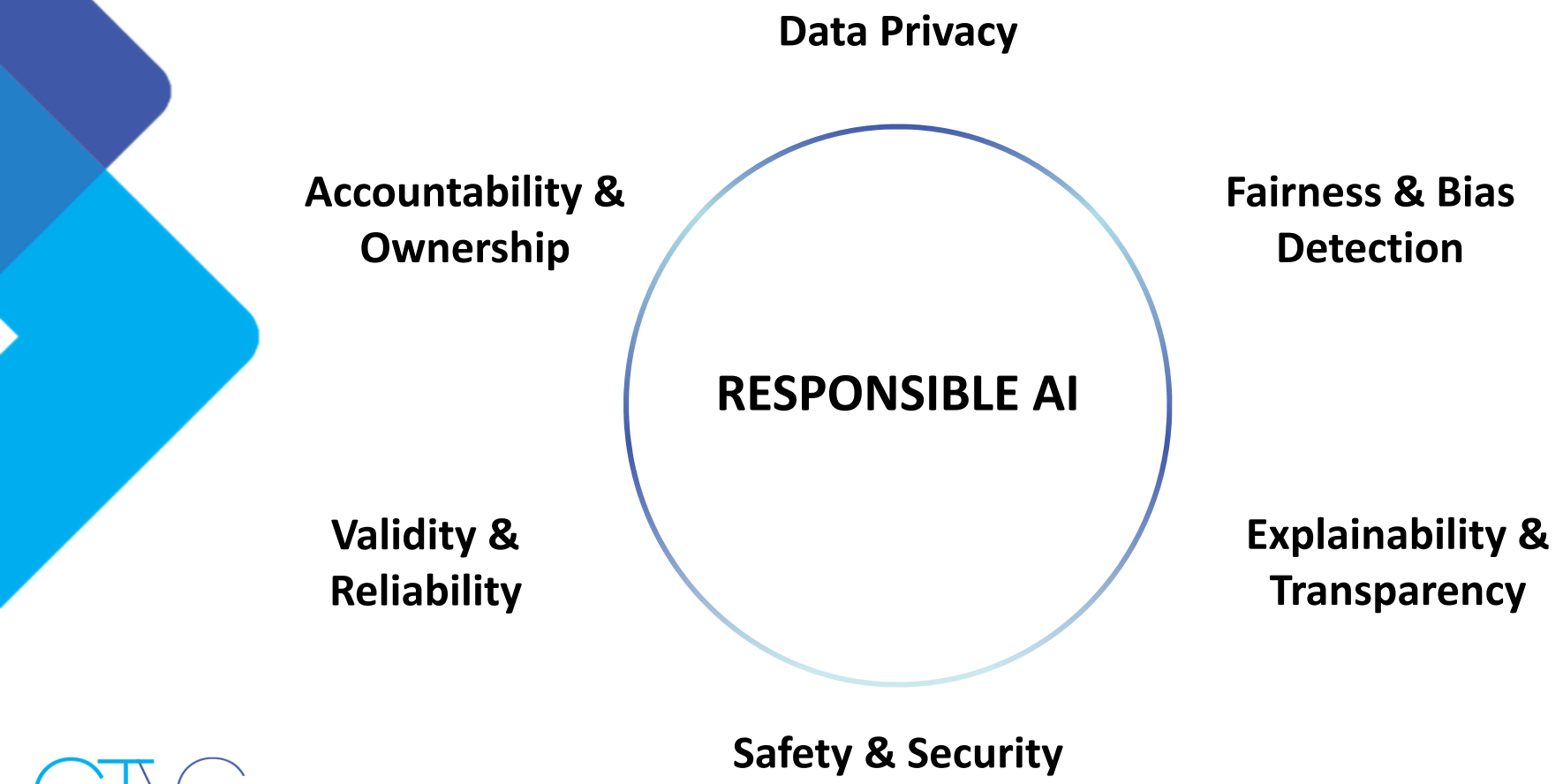
Data Usage
- Public vs Private

CTVG

BACK TO DISCUSSION

CTVG Views | In The Room with CTVG | Presentation

Foundational Responsible AI Guiding Principles



BACK TO DISCUSSION

Trend: Automation

Generative AI
- Script / Code Generation
- Lack of skilled resources

No-Code / Low-Code

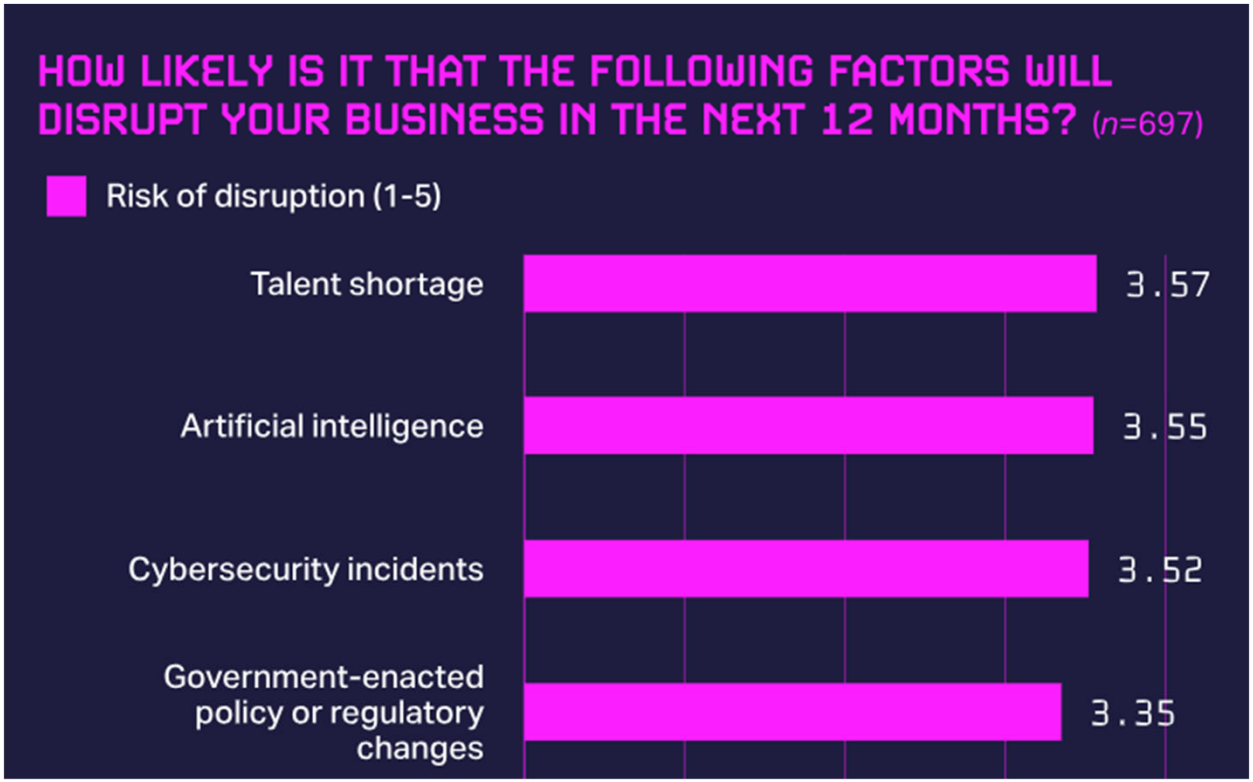
Robotic Process Automation (RPA)

Intelligent Process Automation (IPA)

CTVG

BACK TO DISCUSSION

Trend: Human Risk Management



https://www.infotech.com/research/ss/tech-trends-2025

BACK TO DISCUSSION

Trend: Mergers & Acquisitions

Technology
- Consolidation
- Platform
- Best of bread
- Brand maturity

Private Equity
- Do they integrate well?
- Better together?
- Public > Private

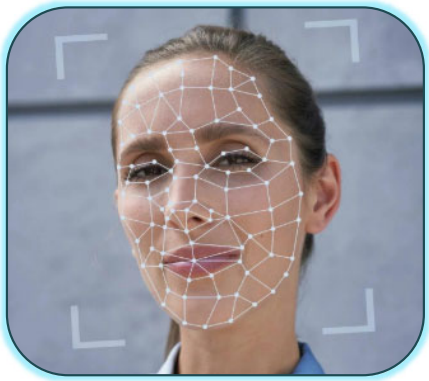
BACK TO DISCUSSION

CTVG Views | In The Room with CTVG | Presentation

2025 Cybersecurity Pitfalls

Supply Chain Management

Data Governance



AI Deep Fakes

Cyber Insurance

CTVG

BACK TO DISCUSSION

Pitfall: Supply Chain Resilience

Poor Program Development
- CMMC contract requirements
- Lack of resources

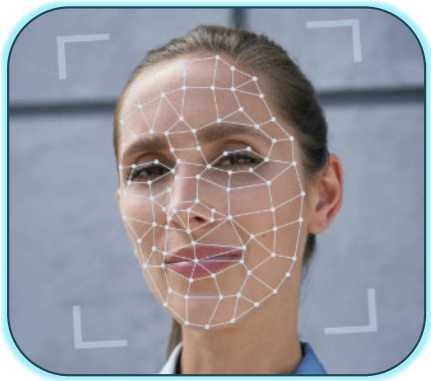
New Executive Orders
- June 2024

Supply Chain Liability
- Few companies know who is in their supply chain
- Nonetheless, companies remain liable for their supply chain
- Supply chain risk may be a disclosable risk under SEC and other legal obligations

BACK TO DISCUSSION

CTVG Views | In The Room with CTVG | Presentation

Pitfall: AI Deep Fakes



Social Influences
- Political
- Celebrity

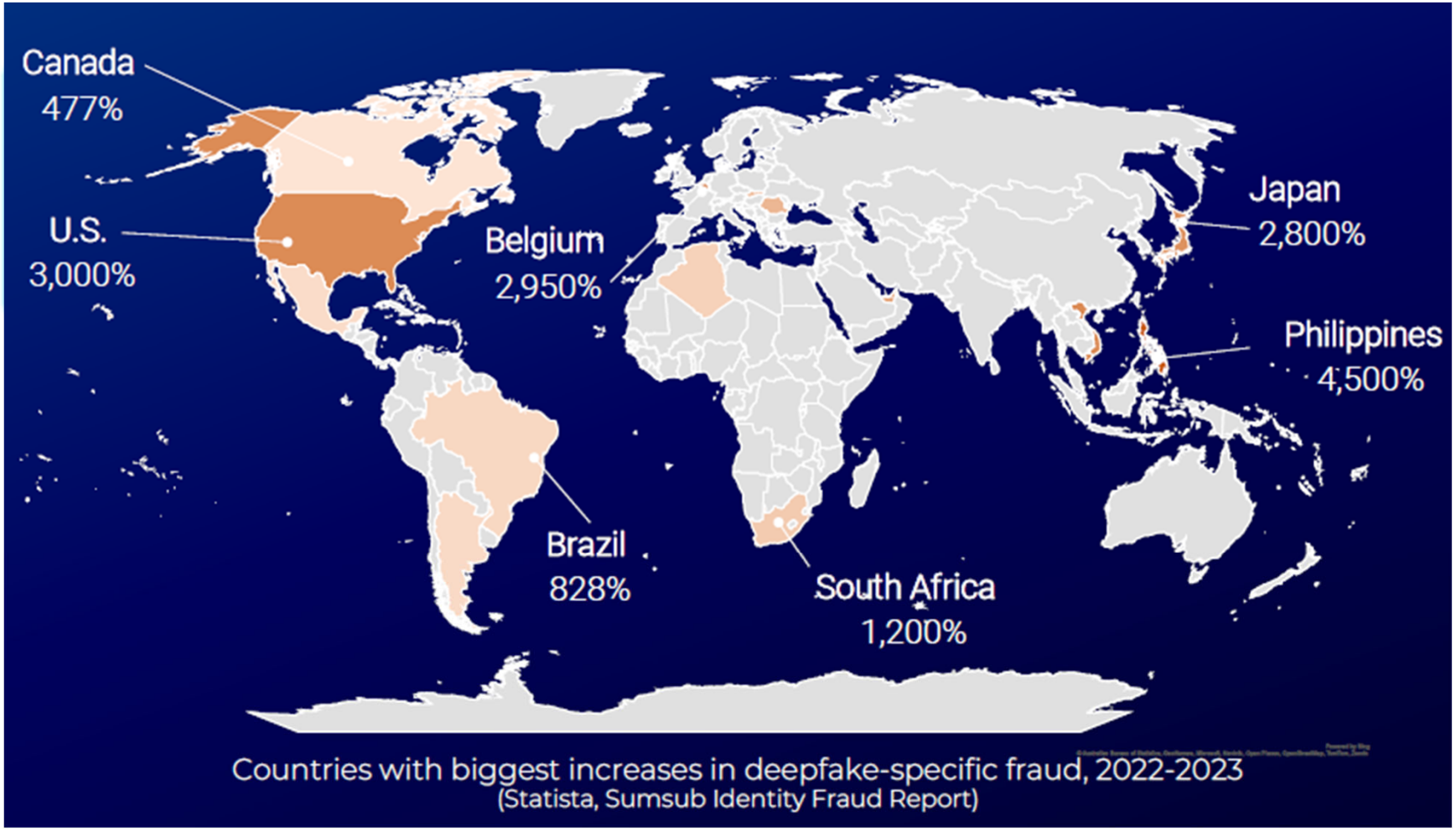
Social Engineering
- YouTube Examples (Obama)
- HR 6466 (AI Labeling Act)

"Seeing is no longer believing"

Feb 2024 - $25M (US) Hong Kong social engineering attack over zoom.

BACK TO DISCUSSION

Pitfall: AI Deep Fakes



BACK TO DISCUSSION

Pitfall: Data Governance Immaturity

Lack of Program Formalization

- Most companies don't know their data
- Privacy and other laws require certain levels of data governance

A Data Breach is Not The Time to Discover Your Data

Policy vs Program

CTVG

BACK TO DISCUSSION

Pitfall: Cyber Insurance

Increasing Identity Controls
- Service accounts
- Multifactor authentication (MFA)

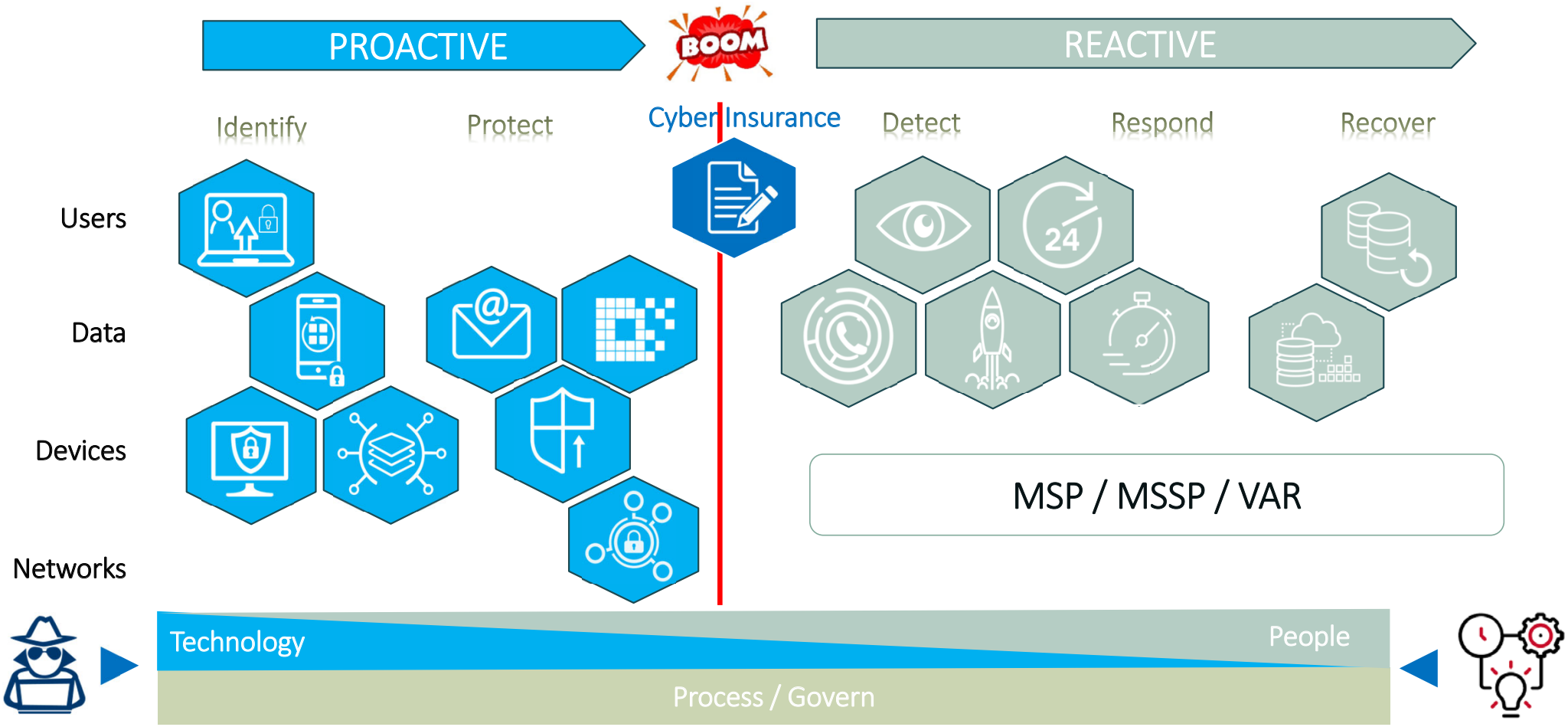
Vendor Management / Supply Chain
- Increased questionnaires
- Added federal regulations

Self-Insured?

Insurance Coverage is Evolving
- Seek counsel from specialized legal counsel to maximize your coverage
- Emerging threats may not be covered

BACK TO DISCUSSION

Pitfall: Preparing for an Incident



BACK TO DISCUSSION

The Convenience Technology Vision Group (CTVG) brings together convenience technology leaders for quarterly virtual meetings. The group addresses trends, challenges and disruptions and solutions in AI, computer vision, alternative payments, robotics, IoT, blockchain, cybersecurity, data analysis, EVs, food tech, frictionless checkout, digital experiences, workforce management and more. The group is committed to sharing its views and perspectives to advance the convenience retailing and mobility industry. CTVG operates under the Vision Group Network, which gathers the collective knowledge and ideas of its members to create a legacy of sharing within the retail community. For more information and to sign up for future Vision Reports, visit our website: **vgnsharing.com/vision-report-library**

CTVG
CONVENIENCE TECHNOLOGY
VISION GROUP

A part of Vision Group Network

For more information about Vision Group Network email us:

Myra Kressner
myra.kressner@vgnsharing.com

Eva Strasburger
eva.strasburger@vgnsharing.com

Roy Strasburger
roy.strasburger@vgnsharing.com

VGN VISION GROUP NETWORK sharing today to shape tomorrow

Want more? Access the growing library of FREE Vision Reports at vgnsharing.com

sharing today to shape tomorrow

CONVENIENCE LEADERS VISION GROUP

CLVG Expecting the Unexpected: Foreseeing Potential Disruptions
November 2024
Challenges facing the convenience retailing industry including emergency preparedness, cybersecurity, preparing for unrest, supply chain disruption and the next pandemic, appetite-suppressive drugs

CLVG Near and Far: Looking at Global Convenience Retailing
August 2024
Trends and innovation in global convenience retailing and mobility

Envisioning Sustainability in Convenience Store Design
May 2024
A Balancing Act for Sustainability vs. ROI, the 80/20 Rule and Customer Opinion, telling the Sustainability Story and Greenwashing

Making the Convenience Industry an Employer of Choice
February 2024
Expanding the persuadable applicant pool; onboarding, engagement, and training; cleaning up industry image; recruitment and retention; strategies; mental health support and kindness campaigns

AI: Predictive Fuel and Dynamic In-Store Pricing
December 2023
Examining AI fuel and product pricing potential.

AI: Dawning of a New Era in Retail Analytics
June 2023
The dawning of a new era in analytics as generative AI evolves, generative AI in simple terms; how AI is quickening the pace of business today; A micro perspective of AI at TXB stores; personalization through AI

The Business Case for EV Charging: Is It for You?
March 2023
The pace of EV adoption; c-store operators' views of the EV-charging customer; three pathways of EV retailing; a micro case study

Currents of Change
January 2023
Changing work schedules and the gig economy; foodservice tipping
in the convenience segment; alternative fuels and the timeframe for electric vehicles

CONVENIENCE TECHNOLOGY VISION GROUP

Retail Media Networks: More Than Meets the Eye
July 2024
Customer experience matters, small operators considerations, resource complexities

Fighting for Tomorrow's Customers
April 2024
What it means to fight for customers, reflecting on winning the "fuel" customer, reliance on 3rd party technology, data analytics, loyalty, and payments

Generative AI and Retailing: Real Results and Real Challenges
January 2024
AI and data integrity, how retailers are currently using AI and what's next for AI in convenience retail?

In Focus: A CTVG Conversation with POS Solution Providers
November 2023
POS decoupling; major oil companies; foodservice as the future; the unique needs of independent operators; integration challenges

To the Point: The Evolving State of POS in Convenience Retail
September 2023
EV Infrastructure and Strategy Updates and POS Systems Challenges and Opportunities.

Unraveling the Road to EV Charging Infrastructure
July 2023
Explosive EV growth; the role of utility companies; government funding programs; operators moving forward

Tech Trailblazing
May 2023
Debating the AI hype, tech as it relates to shift flexibility, and the breaking point on data collection

THE VISION GROUP disruptive solutions

Loosening the Tight Labor Market
February 2024
Journey to Become an Employer of Choice; Expanding the Applicant Pool; Retaining Employees Though; Skill Growth; A Post-COVID Reality

CONEXXUS VISION GROUP PART OF VISION GROUP NETWORK

Envisioning Technology Innovation in the Convenience Store Future
January 2025
Conexxus, IRC and CxVG, data management, AI, employees, electric vehicle charging

ELECTRIC VEHICLES VISION GROUP

Windows for EV Adoption--Opening or Closing?
Late January 2025
The ripple effect of U.S. elections on EV sector growth, The Musk factor, state and local Umbridge, EV tax credits, NEVI and infrastructure investment incentives, balancing public and private investment

VISION GROUP NETWORK

We Value Your Feedback

VISION REPORTS SURVEY
Please take a moment to share your thoughts with us on our Vision Reports.

SUBSCRIBE
Subscribe to receive notifications for all new Vision Reports

LinkedIn

FOLLOW
Follow us on LinkedIn

VISION GROUP NETWORK sharing today to shape tomorrow