EXPERT OPINION

What Does 2024 Hold for Cybersecurity?

Our annual poll of experts on the trends and developments to watch out for in 2024 in AI, data privacy, cybersecurity, e-discovery and more.

January 09, 2024 at 11:52 AM

Cybersecurity

By Steve Salkin | January 09, 2024 at 11:52 AM

Our annual poll of experts on the trends and developments to watch out for in 2024 in AI, data privacy, cybersecurity, e-discovery and more.

Our thanks to: Richard Robbins, Epiq Managing Director, Applied Artificial Intelligence; Daniel Barber, CEO of DataGrail; Christopher Bray, SVP of Partner and eCommerce Sales, Sectigo; Matthew Rasmussen, Founder & CEO, ModeOne; Stefania Quintaje, Axiom; Bob Rudis, Vice President Data Science, GreyNoise Intelligence; Kelly Griswold, CEO, Onna; Jason Mark Anderman, Head of Legal & Compliance, Certa; Dr. Gina Taranto, Director of Applied Sciences, ProSearch: Brian Meegan, Director of Sales and Marketing, ProSearch; Ryan Costello, Head of Data Privacy, ProSearch; Oscar Chavez-Arrieta, Executive Vice President of Latin America, SonicWall; Oliver Silva, Director of Enterprise Accounts, Casepoint; Amy Hilbert, Executive Vice President, Public Sector, Casepoint; Bobby Cornwell, Vice President Strategic Partner Enablement & Integration, SonicWall; Joe Pirrotta, Director of Review Services, ProSearch: Sarah Hutchins, partner, Parker Poe: Amit Dungarani, Vice President, Partnerships & Strategic Initiatives, Casepoint; Tony Donofrio, CTO, Veritext Legal Solutions; Ajith Samuel, Chief Product Officer, Exterro; Matt McKeever, CISO & Head of Cloud Engineering, LexisNexis Legal & Professional; Emili Budell-Rhodes, Director, Engineering Culture, LexisNexis.

So let’s just start with the obvious: AI. Where do you think AI will take us in 2024? How will lawyers and support staff use AI in 2024 that we’re not using it for now?

Generative AI can be life-changing, whether helping to review the intricacies of contracts and legal documents or creating product descriptions for millions of retail SKUs, or anything else we can dream up. There are limitless use cases. We’ve identified a couple interesting ways technologists are using AI in a legal setting. For example, Consumer Reports recently launched Permission Slip, a mobile app that helps people take back control of the personal data companies have on them. To scale Permission Slip, the team used large language models to read through thousands of privacy policies, answer questions about the privacy policy, and pull out the source text — all of which was fed into the app, advising the consumer how to control their data within a new app. Another unique application of AI in the legal setting is descrybe.ai. Descrybe.ai makes complex legal information more accessible to professionals and laypeople alike. It’s an easy way to search for, and understand, case law. — *Daniel Barber, CEO of DataGrail*

I expect the coming year will be marked by the start of a transition from evaluation and limited experimentation to more active use, first with an emphasis on administrative and process-focused tasks as opposed to client work product. Technology will be increasingly infused into traditional workflows and applications. In other words, rather than being faced with a proliferation of new tools, many of our tools will become more capable or at least easier to use. As technology evolves, each of us will be on a journey to figure out how to engage with it to make us more effective in our work. Those who invest the time and energy to learn how to use them effectively and responsibly will be rewarded. — *Richard Robbins, Epiq Managing Director, Applied Artificial Intelligence*

The shift to more a deliberate, outcome-focused use of AI will create interesting dilemmas around the notion of appropriate use. It's very different to use AI capabilities to enhance existing work patterns according to standards that are widely accepted, compared to coming up with "AI-first" use cases that are novel, and where the benefits and possible unintended consequences are yet to be understood. This is where impact assessments and responsible AI guidelines will become an invaluable tool in the value strategy and risk formulation of those use cases, particularly in the legal tech space where the stakes are high. — E*mili Budell-Rhodes, Director, Engineering Culture, LexisNexis*

We expect to see significant innovation in how organizations handle cyber incident response. Data breaches are at an all-time high, increasing by nearly 20% in the first nine months of 2023 over the entire year of 2022. The response process is onerous, but recent improvements in technology, coupled with enhanced regulatory reporting requirements around the world will require a paradigm shift in terms of readiness and effective response. In 2024, we will see AI leveraged to improve the incident response lifecycle:

- AI could help organizations create and integrate business continuity and disaster recovery plans.
- AI systems can provide analysis and threat identification that cybersecurity professionals can use to identify breach risks and take preventive security measures.
- AI models will increasingly be used to identify personal information in massive sets of both structured and unstructured data; reducing the time, effort, and resources required for incident response.
- Generative AI can be used to create breach-notification letters.
- Continuous improvement: Over time, predictive AI could use the information collected in the response to generate suggested security and privacy practice enhancements.

— *Joe Pirrotta, Director of Review Services, ProSearch*

In the upcoming year, a decisive showdown will unfold, determining whether AI emerges as a formidable threat actor or the ultimate guardian of cybersecurity. In a race against time, hackers and cybersecurity professionals are actively harnessing the power of AI to fortify their respective endeavors. In 2024, the culmination of this race will reveal whether AI stands as a potential menace or the most impactful emerging technology protecting our cybersecurity realm. — *Christopher Bray, SVP of Partner and eCommerce Sales, Sectigo*

AI and machine learning will be used in cyber offense and defense. In the coming year, we believe both attackers and defenders will leverage AI and machine learning tools to automate and improve their operations. On the offensive side, we can expect to see AI algorithms used to automate vulnerability scanning, phishing attacks and data exfiltration, making them more effective and harder to detect. On the defensive side, AI-powered solutions will likely be deployed to monitor networks for anomalous behavior, automatically update security protocols, and even take immediate action to neutralize threats. This tug-of-war between offensive and defensive AI use cases will then escalate, leading to a new cybersecurity "arms race." Companies and governments will need to invest heavily in cutting-edge technologies to keep up, and cybersecurity strategy will need to focus increasingly on AI-hardening and AI-driven threat detection and response. — *Chandrodaya Prasad, SonicWall Executive Vice President of Product Marketing*

2024 will be the year that the reliability of the digital record meets its demise as deep fakes fully undermine digital trust. Gone are the days when people could trust what they saw and heard. With the proliferation of deepfakes, every digital record whether that be a photo, video or voice recording could be a fake. Given our current reliance on digital records within our legal, security and digital systems, without a solution, we will witness the crumbling of our systems that rely

on biometrics to authenticate identity. Soon all forms of recording devices will have a built-in encrypted timestamp, acting as a watermark at the time of capture. These encrypted watermarks must be built upon the only unimpeachable form of encryption, PKI, to separate authentic images from deepfakes to re-establish digital trust in images, videos, and recordings. — *Christopher Bray, SVP of Partner and eCommerce Sales, Sectigo*

I think this will be the year of R&D, standing up ethics boards, thought leadership, and educating the legal market on how to use AI without introducing risks. AI is obviously one of the most powerful tools to date, but that also requires that we take a systematic approach to education and deployment of the technology. — *Matthew Rasmussen, Founder & CEO, ModeOne*

Artificial Intelligence (AI) is poised to transform the legal industry by 2024. Applications like document review and analysis, contract management, and legal research are already prevalent. However, emerging areas show even greater potential. One such area is predictive policing of corporate behavior, where AI forecasts legal issues based on company behavior, aiding proactive risk mitigation. AI-assisted Negotiations streamline contractual or settlement discussions. Real-time compliance advice offers up-to-date recommendations as laws evolve. Integration with emerging technologies combines AI with blockchain, IoT, and augmented reality. Mergers and acquisitions analysis benefit from AI's deeper assessments of legal, financial, and cultural risks. Ethical and privacy considerations are crucial for compliance. Lastly, AI offers interactive legal education, providing personalized training for legal professionals. Prioritizing AI implementation based on company needs is vital to avoid overwhelming solutions. — *Stefania Quintaje, Axiom*

2023 was a year that many woke up to the possibilities of AI usage and 2024 may be a pivotal year on how widely it is embraced. One trend that is likely to continue into 2024 is serious security breaches, both as bad actors use AI to become more precise in their attacks and also through taking advantage of increasing reliance by companies on third-party software services offering AI. — *Sarah Hutchins, partner, Parker Poe*

GenAI will continue to evolve, especially as offerings from major players like OpenAI (GPT), Anthropic (Claude), and Google (Bard/Gemini) are continually updated with newer models and more enhanced offerings. Legal software companies that try to incorporate these advancements into their offerings will need to be able to establish guardrails and safety measures to demonstrate they are making responsible use of AI. This will be particularly important as more guidelines are issued from regulatory bodies and guidance is provided from professional industry associations like the ABA. — *Amit Dungarani, Vice President, Partnerships & Strategic Initiatives, Casepoint*

Prepare for an election espionage extravaganza. With the upcoming U.S. Presidential election, nation-state cyber activity is expected to surge, targeting election infrastructure and influencing the outcome through disinformation campaigns and other tactics. In addition, there will be a wave of espionage and information theft. Think James Bond, but with more keyboards and fewer martinis. The election will be a prime target, with everything from disinformation campaigns to direct attacks on election infrastructure. It's going to be a wild ride. — *Bob Rudis, Vice President Data Science, GreyNoise Intelligence*

We've also heard reports of low adoption of AI, especially in corporate law settings. What steps can the industry take to either assuage the fears lawyers might have about AI or make it less unapproachable?

AI will continue to bring value to our everyday tasks, but we're going to see more advanced applications of the technology. AI will be embedded into applications in several ways: enabling users to interact naturally with the software to ask questions, automate tasks, gain insights, hunt for information more precisely and more. The most advanced solutions will act as co-pilots, not auto-pilots, ensuring that while productivity and efficiency is significantly improved, we don't lose human oversight and control. — *Ajith Samuel, Chief Product Officer, Exterro*

We must teach AI to work with us, not against us. We need frameworks, ethical-use policies, and strong governance to ensure the proper use of AI. Such structures are the first step in making those in the legal industry more comfortable with AI, leading to greater adoption. From there, any business — including a law firm — needs to discover where they might be using AI internally or within third-parties, and monitor it closely. Looking ahead, we expect to see an increasing number of vendors claim they can help control AI. Adopt with caution. It's still too early to know the unintentional consequences of AI use, and it's impossible to claim one can control it. We'll likely see a lot of overpromising, giving companies a false sense of security. — *Daniel Barber, CEO, DataGrail*

It remains important to stress that the systems are most effective to support the work of someone who is skilled at a task and not replace that individual. A more experienced practitioner should know how to work with a relative novice or less experienced practitioner to take less than final work and turn it into the final product. If lawyers gauge their expectations accordingly, they may be more willing to use the systems as intended. — *Richard Robbins, Epiq Managing Director, Applied Artificial Intelligence*

Corporate legal teams taking a cautious approach are valid — especially when they're considering using genAI with proprietary data. GenAI combined with proprietary data has the potential to significantly improve time-consuming workflows, enhancing team efficiency. That being said, organizations must understand how they will access this data as well as research the T&Cs of any solution or model being considered. Legal teams can consider the following four steps if they're looking to experiment with genAI:

1. **Problem Definition:** Legal teams should clearly identify the challenges they're looking to solve, outlining expected outcomes;
2. **AI Evaluation:** Assess whether genAI is the right tool for these challenges, considering its capabilities and constraints. There may be a more simple solution!;
3. **Cross-Functional Team Formation:** Create a task force of business users who can add expertise across technical questions and process development;
4. **Build vs. Buy:** Carefully decide between developing an in-house AI solution or procuring an external solution, with a focus on data security and operational fit.

— *Kelly Griswold, CEO, Onna*

The low adoption of AI in corporate law settings can be attributed to various factors including skepticism, lack of understanding, and concerns about the implications for legal practice. We cannot exclude that a lack of clear legislation and the speed of AI's evolution does not help anyone to fix processes or minimize risks associated with the technology. To overcome these challenges, we can gradually integrate AI by educating lawyers about its benefits through workshops, seminars, and training sessions. Identifying early adopters within each team and leveraging internal resources can champion innovation and build trust. Collaboration between lawyers and tech departments is crucial to develop customized, user-friendly solutions. Internal study groups can verify and refine AI solutions. By taking these steps, the legal industry can help lawyers overcome their apprehension towards AI, leading to greater adoption and more efficient, effective legal practices. — *Stefania Quintaje, Axiom*

End users should generally not directly engage with generative AI and instead need this kind of rigorous quality assurance. Otherwise, each individual end user could proceed in conflicting and contradictory directions, driving teamwork dysfunction, inconsistent results, and slow contracting. The goal should be a hybrid approach of gen AI mixed with human-designed rules to create elaborate insights into contracting, predict most negotiating issues and solutions ahead of time, and better discern whether prevailing conditions align with objectives. You can have your cake and eat it, too. — *Jason Mark Anderman, Axiom*

We must measure and build trust in what's new and we are well equipped to do so. Taking eDiscovery as an example, the key to assuaging fears and making it more approachable is to remember two things:

1. An incremental approach to adoption is possible. Gaining trust by using AI assistants and chatbots available to help with personal administrative activities could be a precursor to using AI tools in the course of generating work product. Using AI in workflows that give legal professionals opportunities to validate, train, and refine results will help with the adoption of AI assistance.
2. We are already well prepared to measure the performance of AI technologies. While the technology is evolving, math is still math. So, using the process of document review as an example, continuing to conduct statistical sampling, and validating workflows and performance using precision and recall metrics is crucial.

— *Dr. Gina Taranto, Director of Applied Sciences, ProSearch*

Low adoption rates of AI by lawyers are not surprising, especially in corporate law. Lawyers tend to be risk-averse given the nature of their role/profession, especially where risk management/minimization is critical in a corporate legal department. While GenAI is still all the buzz, there are still a lot of questions around data privacy, IP, security, and general reliability of the technology, especially as negative headlines call attention to attorneys getting sanctioned for ill-advised use of GenAI. That said, companies will generally follow the lead of their peers. A number of leading Fortune 500 companies are actively exploring AI — and specifically GenAI — in a very methodical way. They are starting by forming cross-disciplinary committees with stakeholders from legal, IT, various business owners/lines, HR, and more to explore specific use cases, safeguards, and ways to explore the technology, while balancing needs, offerings, and risk. The key to getting higher adoption rates is education, frank discussions with your peers and colleagues, and talking to the software vendor community to understand what they are offering and how they differentiate their approach to the issues. — *Amit Dungarani, Vice President, Partnerships & Strategic Initiatives, Casepoint*

Are we approaching AI overload? Have those who are going to adopt it already done so. Is there too much hype?

We are high on the hype curve, with the inevitable “trough of disillusionment” likely arriving in mid to late 2024. That said, as product suppliers continue to provide major advantages in the tools they offer by leveraging AI, there will be steady increased adoption and benefit for the next several years. — *Tony Donofrio, CTO, Veritext Legal Solutions*

There is certainly a lot of hype, but I don’t think we’re anywhere close to seeing who will adopt it. It can feel like AI is already everywhere because it was all anyone could talk about in 2023, but there are a number of more risk-averse industries — and segments within industries — that are taking a more cautious approach. I think we should expect to see use cases expand dramatically as people grow more comfortable and as parameters and ethical use policies are put into place. — *Daniel Barber, CEO, DataGrail*

We have reached AI overload. There is too much hype. The last year has been dominated by fascination with technology and consideration of what it might be. It has been time for initial experiments. Now we will learn from those experiments and for the leaders, move to adoption. We need to focus less on technology for the sake of technology and get back to the problems we want to solve. — *Richard Robbins, Epiq Managing Director, Applied Artificial Intelligence*

The question of whether we are approaching an ‘AI overload’ or if the hype around AI has outstripped its practical utility is a topic of ongoing debate. While AI has been subject to significant hype, it’s also true that it has brought about substantial improvements and efficiencies in various fields. The challenge lies in discerning realistic applications from overhyped promises. Concerns about ethics, privacy, and regulatory compliance also contribute to slower AI adoption. Clearer guidelines and standards can address these concerns and provide organizations with more confidence in adopting AI. The key is for organizations to focus on realistic, practical applications of AI that align with their specific needs and capabilities, rather than succumbing solely to the hype. — *Stefania Quintaje, Axiom*

In 2023, Taylor Swift shared trending search rankings with large AI language models — in other words, AI is big news. This recent attention comes somewhat late as AI is already being integrated into pillars of our society in ways that will soon make it “too big to fail.” While this does not necessarily mean mass adoption and regular personal usage, it does mean that interactions with AI are already, and sometimes unknowingly, part of daily life. As AI marches forward, so too

does a patchwork of AI regulation. Teams will need to monitor these regulatory updates to ensure compliance of their own AI practices. Companies will continue to find new and innovative ways to integrate AI into their business models. As this trend accelerates, it's important these companies develop compliance policies and direct the appropriate employees on use parameters while accounting for the accuracy and security of their data. As more legal departments use AI, a reevaluation of bar guidance on ethics is likely necessary next year. — *Sarah Hutchins, partner, Parker Poe*

AI is here and not going away! The hype is concerning because there is too much ambiguity surrounding the term "AI." Artificial Intelligence is being used broadly to include both Gen AI and machine learning technologies that have long been employed in legal. But hype away people — the techies are hard at work building AI solutions that are going to revolutionize our world! — *Brian Meegan, Director of Sales and Marketing, ProSearch*

No. Even a year after the release of ChatGPT, it still continues to be a hot topic. We are just at the cusp. The AI revolution is still in the early stages and will reveal a hockey stick growth pattern over the coming decade in terms of advancement and usage. While we may move onto the "next thing" in media coverage and conversation like we have with blockchain, cryptocurrencies, the metaverse, and so many other technologies, this moment seems different given how transformative and, frankly, useful this technology can be in everyday life. — *Amit Dungarani, Vice President, Partnerships & Strategic Initiatives, Casepoint*

In the Fall of 2023, President Biden signed an Executive Order on AI that has some thresholds and reporting requirements to be met. What impact will that EO have in 2024?

President Biden's Executive Order signals a desire to create a sweeping regulatory framework. It is but one of a collection of frameworks being assembled around the world. The Bletchley Declaration, a policy agenda focused on AI risk, was signed by representatives of 29 countries, including the United States and China just after the Biden Executive Order. Expect that 2024 will bring an array of new legal constructs that we will, as a society, need to contend with. It remains to be seen whether regulation will dampen the explosive growth we have seen in this arena. — *Richard Robbins, Epiq Managing Director, Applied Artificial Intelligence*

President Biden's Executive Order on Artificial Intelligence is poised to have significant impacts in 2024 across sectors including healthcare, corporate law, and technology. The Order establishes strict standards and reporting requirements for AI safety, security, and trustworthiness, aiming to promote responsible development and use of AI technologies. Although specific rules are yet to be defined, the Order's implementation under President Biden's mandate will be critical for observing a tangible impact. Developers of powerful AI systems will be required to share safety test results and critical information with the U.S. government, leading to more stringent safety protocols in AI development. The Order's focus on privacy and civil liberties risks associated with AI is likely to result in enhanced measures for the lawful and secure collection and utilization of data. Federal departments and agencies will implement AI governance structures, appointing Chief AI Officers and AI Governance Boards, potentially inspiring similar models in corporate settings. Furthermore, fostering international cooperation, particularly with the EU, is crucial. Collaborative efforts can prevent privacy discrepancies that have plagued organizations and companies in the past, impacting global AI standards and practices. Organizations across sectors should anticipate the need to adapt to these standards and practices to ensure compliance and responsible usage of AI technologies. — *Stefania Quintaje, Axiom*

The Executive Order stands as a warning shot, with the value of raising awareness of the potential misuse and abuse of the technology. There will be more tangible operational impacts for firms and corporations as state and federal privacy and cybersecurity rules emerge. — T*ony Donofrio, CTO, Veritext Legal Solutions*

Absent federal legislation, the Executive Order on AI directed government agencies to vet future AI products for potential national or economic security risks. Agencies such as the FTC, Consumer Financial Protection Agency, EEOC, NIST, and dozens of others are already focused on practical ways to monitor AI systems and ensuring fairness, consumer privacy and safety. — *Ryan Costello, Head of Data Privacy, ProSearch*

President Biden's executive order establishes an initial framework for regulating and governing the development and deployment of AI tools. As we head into 2024, companies developing any foundation AI model that "poses a serious risk to national security, national economic security, or national public health and safety," must notify the federal government, according to the White House. That notification will include when companies are training the model. The order also lays out standards that will be set up by the National Institute of Standards and Technology regarding an AI systems' security and safety. Companies in industries like software development, housing, health care, and education should begin carefully assessing how AI is used in their business given these additional requirements from various regulatory agencies. These reviews, for example, should scrutinize the overall system for vulnerabilities. — *Sarah Hutchins, partner, Parker Poe*

Speaking of regulations, will we finally see national legislation on cybersecurity and/or data privacy in 2024? More state laws?

Data privacy is a bipartisan issue — there's an even mixture of red and blue states that have data privacy laws — but I'd place my bet on more State Privacy Laws before a federal law. There are too many contrasting interests at play holding up a federal law, and the system moves so slowly, especially as we inch closer to the next presidential election. But, all is not lost. Given that Gartner predicts that 75% of the world's population will be protected by data privacy laws by 2024, we can assume that the majority of U.S. citizens will be included in that statistic in the near future thanks to state laws. Most state-level laws don't go quite as far as the CCPA — and not nearly as far as the GDPR — but these state-level privacy laws tend to have a similar baseline of provisions. Knowing how each law impacts business practices is crucial. Organizations can use these areas of overlap to build the foundation of a broadly compliant data privacy program. — *Daniel Barber, CEO, DataGrail*

I do not believe that we are well served by our patchwork quilt of state laws pertaining to cybersecurity and data privacy. The compliance burdens placed on organizations that are active across the nation are enormous. That said, heading into an election year, it is difficult to see meaningful progress being made to address this need until after the current election cycle. — *Richard Robbins, Epiq Managing Director, Applied Artificial Intelligence*

Regulatory changes such as the rise of digital trust will become more robust. Digital Trust refers to the level of confidence that individuals and businesses have in the security, privacy, and reliability of digital transactions and interactions. It is one of the most important "movements" worldwide because it helps build customer loyalty and drives revenue growth. The loss of brand value is a huge component in the valuation of every company, but some don't understand this threat and how the chief information security officer/chief technical officer (CISO/CTO) needs to be heard seriously. — *Oscar Chavez-Arrieta, SonicWall Executive Vice President of Latin America*

In 2024, incoming cybersecurity regulations will force businesses to be more transparent about their breaches and attacks. Forthcoming legislation such as the EU's NIS2 Directive and the Cyber Resilience Act will impose more stringent standards for cyber protection and establish clear reporting timelines in the event of a breach. As these directives take effect, businesses will be made to share with their partners and suppliers early identifications of system vulnerabilities or face fines. The aim of this is to prevent cybercriminals from inflicting widespread damage across multiple businesses. In 2024, it will be crucial to optimize the transparency afforded by these regulations, and by dragging cybercriminals out into the open, authorities can more effectively curtail their illicit activity. — *Bobby Cornwell, Vice President Strategic Partner Enablement & Integration at SonicWall*

The Year of Transparency, for better or worse. In 2024, organizations will be forced to spill the beans about their cyber breaches. This will be driven by regulatory changes, a spate of punishing breaches at well-recognized organizations (at least one of which will likely impact a major financial services firm and cause major market distress for days), and the realization that transparency is key to maintaining trust and stability. So, get ready for companies to air their dirty laundry in public. — *Bob Rudis, Vice President Data Science, GreyNoise Intelligence*

We've also seen federal agencies such as the FTC get involved in data breach reporting. What impact will those regulations have in 2024 and will other agencies get more involved (*i.e.*, DOJ)?

I wouldn't be surprised to see the FTC slap more fines or get more involved. Ransomware and data breaches continue to pose some of the biggest threats to a business. The government may continue using the proverbial "stick" to encourage businesses to enhance their cybersecurity and data privacy practices. — *Daniel Barber, CEO, DataGrail*

The proposed amendments to the Health Breach Notification Rule (HBNR) by the FTC signify an expansion of breach notification scope and requirements. These amendments clarify breaches, redefine personal health record related entities, and update notice methods. A potential consequence of these amendments is an increase in FTC investigations and more vigorous enforcement actions, leading to higher incident response costs for companies striving to comply with the enhanced notice requirements. As regulatory attention escalates, businesses can expect augmented compliance costs. The involvement of multiple federal agencies hints at a move toward standardizing cybersecurity and data privacy practices across sectors. Such efforts can harmonize compliance obligations, facilitating understanding and adherence for businesses navigating the complex landscape of regulations. — *Stefania Quintaje, Axiom*

In 2024 we'll see corporate legal and compliance departments expand their sphere of operations to include managing the risk of organizational data as a result of the increased scrutiny and enforcement actions due to data breaches.. Specifically, companies are going to need to take a more holistic approach to managing the risk data poses due to data breach (as well as non-compliance with global and local privacy regulations and even litigation). Increased use of AI further reinforces the need for a comprehensive approach to ensure data is stored, used, managed, protected and defensibly disposed in an ethical and compliant manner. — *Ajith Samuel, Chief Product Officer, Exterro*

Companies will need to consider their breach reporting requirements even earlier and as part of their initial response to a breach. Some regulated entities have already been dealing with immediate regulatory notification requirements, but recent law changes have expanded impacted companies. It is increasingly important to prepare for a security breach ahead of time with the establishment and practicing of your incident response plan. Companies should know who they need to notify and when, under law or contract, before an incident happens — devoting precious resources to that review in the wake of an incident when systems are down and communication is strained is definitely not a best practice. Developing a notification plan that aligns with current requirements should be a regular — and at least annual — practice. — *Sarah Hutchins, partner, Parker Poe*

DOJ will continue to play a central role in investigating cybersecurity incidents and data breaches. One outcome of the wave of government-focused data breaches we saw in 2023 are the new cybersecurity rules proposed for the Federal Acquisition Regulation (FAR). One of those proposed rules, Cyber Threat and Incident Reporting and Information Sharing, expands the requirements for government contractors for incident reporting. The rule requires contractors to "'immediately and thoroughly investigate all indicators that a security incident may have occurred and submit information using the CISA incident reporting portal … within eight hours of discovery … [and to] update the submission every 72 hours thereafter until the Contractor, the agency, and/or any investigating agencies have completed all eradication or remediation activities." In addition, the rule will require the contractor to grant "full access" to CISA and the FBI to applicable contractor information, systems and personnel in response to a security incident reported by the contractor or a security incident identified by the government. This will expand the government's ability to thoroughly investigate data breaches. — *Amy Hilbert, Executive Vice President, Public Sector, Casepoint*

The new SEC requirement for "… registrants to disclose material cybersecurity incidents they experience…" will create an additional level of transparency about the number of cybersecurity incidents that are made public. As more incidents are made public, companies will start to realize cybersecurity incidents are not uncommon. The awareness of these incidents and the ability to learn from them will have long-term benefits including stronger cybersecurity practices and

technology innovation. Consider the Target and Home Depot breaches of 2013 and 2014, respectively. Both companies survived, and other companies and security teams learned from these incidents and innovated their security practices as a result. — *Matt McKeever, CISO & Head of Cloud Engineering, LexisNexis Legal & Professional*

Toward the end of 2023, we still saw reports of cyber theft in law firms and other companies. What new types of cyber theft will we see in 2024, And what new defenses can be put in place against them?

In 2024, the cybersecurity landscape is poised to witness the emergence of new types of cyber threats, necessitating the adoption of innovative defensive strategies. While many threats are already a reality, three noteworthy ones include:

1. The integration of Artificial Intelligence (AI) in business operations opens up potential vulnerabilities, especially in safeguarding customer data and protecting intellectual property. Risks such as data poisoning, evasion attacks, and privacy issues become more pronounced.
2. SMS Phishing serves as a growing vector for cyberattacks, as cybercriminals continuously adapt and devise new methods to overcome traditional defenses.
3. Cloud platform breaches maintain their relevance, as the adoption of cloud technology continues to surge. The widespread use of cloud platforms introduces the risk of major breaches, amplifying the need for robust security measures.

To counter these threats, organizations need to invest in advanced technologies, such as AI-driven threat detection systems and multi-factor authentication. Additionally, implementing comprehensive employee training programs, conducting regular security assessments, and staying up-to-date with emerging cybersecurity best practices are paramount for maintaining effective defenses. — *Stefania Quintaje, Axiom*

Social Engineering exploits will continue to be the most prevalent cyber theft risk for firms and corporations in 2024, with third-party systems exploits being second place. More firms will be exposed to Ransomware attacks as hackers continue to become more sophisticated in their phishing schemes. AI will play a role both in advancing the hacker's exploit toolkit as well as the cyber security defense toolkit, with a game of AI spy vs. spy emerging by the end of 2024. — *Tony Donofrio, CTO, Veritext Legal Solutions*

We will witness continued and significant advances in artificial intelligence, which will have both positive and negative impacts on cyber theft. Cybercriminals will become more sophisticated in their approach to phishing attacks, leveraging AI to design targeted and convincing attacks through multiple channels such as email, messaging, and voicemail. However, businesses and law firms can also take advantage of improvements in AI to implement advanced security measures to protect their data and assets. Thanks to the investment in AI made by the tech industry, it will be possible to detect unusual activity and quickly adapt to new threats. This investment will enable businesses to take advantage of new machine learning algorithms that have been added to security software. These algorithms can identify patterns and behaviors that are indicative of potential security threats. Businesses can use AI-powered tools to monitor their networks, detect anomalies, and respond promptly to security incidents. — *Oliver Silva, Director of Enterprise Accounts, Casepoint*

Phishing attempts are rampant over SMS text messaging, Telemessage, WhatsApp, and other mainstream messaging applications. Companies need to be thinking on how to be able to quickly identify these vulnerabilities in their corporate systems, how to monitor, remediate, and triage these threats. — *Matthew Rasmussen, Founder & CEO, ModeOne*

On the e-discovery front, what, if any, new developments will 2024 bring?

I expect that e-discovery platforms will continue to be enhanced to incorporate generative artificial intelligence features in line with announcements made from leading participants. There will be more beta programs and then generally released offerings. The better approaches will successfully harmonize more traditional machine learning approaches with newer capabilities. The ability to more effectively search for concepts instead of lists of words will lead to better

review overall. Summarization capabilities will be received as increasingly valuable. While the technology should allow for reviewers to be more efficient, suppliers will need to do a good job of offering solutions that are reasonably priced to make sense to clients. — *Richard Robbins, Epiq Managing Director, Applied Artificial Intelligence*

In 2024, e-discovery is set to undergo further advancements, characterized by several prominent trends. The adoption of Software as a Service (SaaS) and cloud-based solutions will continue to rise, offering scalability and cost-effectiveness to legal professionals. Managing both structured and unstructured data will gain greater attention, with structured data being favored for its ease of organization and management. The increasing complexity of e-discovery stems from the expanding volume and diversity of data, requiring efficient handling solutions. Artificial Intelligence (AI) will play an increasingly integral role in e-discovery review, providing enhanced efficiency in managing large data sets. Predictive coding and Early Case Assessment (ECA) automation are also gaining traction, streamlining the review process and reducing costs. Collaboration within organizations will be prioritized, while an acute focus on the return on investment (ROI) of e-discovery technologies will prevail amidst economic uncertainties. — *Stefania Quintaje, Axiom*

Generative AI in e-discovery review and analysis has ushered in a new era of practical applications that can generate significant business value for law firms and corporations. This technology has the potential to revolutionize the legal industry by enriching the way attorneys and legal technologists perform e-discovery. However, the successful integration and adoption of GenAI workflows require a deep understanding of its capabilities and limitations. Consequently, there will be increased demand for domain experts in GenAI workflow integration, prompt engineering, and training. The trailblazers who embraced this technology in 2023 established a profound understanding of its potential, positioning them as experts in this emerging field. They will drive market demand for their skills and knowledge as the legal technology community embraces the possibilities of Generative AI. — *Oliver Silva, Director of Enterprise Accounts, Casepoint*

Gen Z is leading the way to the depreciation of traditional email communications in business. Texting, WhatsApp, Slack, Teams, and others are becoming the mainstream form of communications so businesses need to be mindful of that heading into 2024 when building out their data classification, data privacy, and legal hold strategies. — *Matthew Rasmussen, Founder & CEO, ModeOne*

*****

Steve Salkin, Esq. is the Editor-in-Chief of *Cybersecurity Law & Strategy* and Law Journal Newsletters. He can be reached at ssalkin@alm.com or on LinkedIn @stevesalkin.

This article appeared in Cybersecurity Law & Strategy, an ALM publication for privacy and security professionals, Chief Information Security Officers, Chief Information Officers, Chief Technology Officers, Corporate Counsel, Internet and Tech Practitioners, In-House Counsel. Visit the website to learn more.