FEATS OF STRENGTH

A Business-Focused Cybersecurity Magazine

2024 CYBER TRENDS

IN THIS ISSUE:

CASSIO GOLDSCHMIDT, SERVICETITAN
DOUG INNOCENTI, MOONPAY
KAREN HIGGINS-CARTER, GILBANE, INC.

Top 5 Cyber Trends for 2024

2024 Artificial Intelligence Cyber Trends

DECEMBER 2023

K logix

TABLE OF CONTENTS

2024 Cyber Trends *December 2023*

FROM THE *Editor*

Dear Readers,

As another year comes to a close, we wanted this issue of the magazine to reflect trends to look out for in 2024. In an article on page 6, we share the five top trends we predict, based on what our CISO and security expert community is telling us. These include the persistent hot topic of artificial intelligence, along with changes in threats, how to address changing regulations, the increase of cyber representation in the boardroom, and the importance of strong threat detection.

I predict some organizations may face tighter cybersecurity budgets in the coming year, causing them to rethink their investments and resource distribution. This is a great opportunity for security leaders to reevaluate their priorities and ensure they are addressing the most impactful areas that align strongly with business goals. To demonstrate this value and gain justification, CISOs will continue to communicate effectively with their business counterparts. An example of this is on page 4, Karen Higgins-Carter (EVP, Chief Information and Digital Officer, Gilbane, Inc.) states, "A mentor once told me that a risk is not the absence of a control. Framing the message in terms of how would the absence of that control impact the business can be a powerful way to communicate the value of our efforts."

We also feature Cassio Goldschmidt (CISO, ServiceTitan) on page 8. He reinforces the need to focus on strong communication as a CISO leader. He also discusses some top trends his team is concentrating on, as well as some areas of growth for the industry as a whole. These include right sizing identity and privileges, seamless transitions related to acquisitions, tokenization, and artificial intelligence.

On page 10, Doug Innocenti (CISO, MoonPay), talks about his deep investments in attaining certifications for industry regulations, something his team spent a great amount of time accomplishing. He also points out trends related to talent shortage and rising threats.

To dive deeper into AI, we wrote an article on page 12 that discusses 2024 AI cyber trends. Not only will more investments be made in harnessing the power and innovation surrounding AI, but CISOs and their teams will continue to spend time educating themselves on the topic.

I hope you enjoy reading!

Katie Haug

Feats of Strength Editor

VP, Marketing, K logix

Magazine Contributors

Katie Haug - Editor
VP Marketing, K logix

Kevin West - Editor
CEO, K logix

Emily Graumann - Graphics
Graphic Designer, K logix

About K logix

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication Feats of Strength. Through hundreds of CISO interviews, we extract trends in order to provide services that align business to information security.

PROFILES IN Confidence

KAREN HIGGINS-CARTER

Executive Vice President, Chief Information and Digital Officer

GILBANE, INC.

HEADQUARTERS: Providence, Rhode Island

EMPLOYEES: 3,100+

REVENUE: $6.3B annual revenue, Gilbane Building Company; $8.5B total development, Gilbane Development Company

Karen Higgins-Carter, CISSP, NACD.DC is an engineer by training who spent most of her career working in information technology. She mainly focused on roles in the financial industry, gaining deep exposure to cybersecurity as it relates to protecting data, maintaining trust with customers, and adhering to regulatory requirements. After 20 years in finance, Karen decided to make a transition to join Gilbane, Inc., a family-owned company that provides real estate development, global integrated construction, and facility management services.

Moving her career into a new industry was exciting for Karen, and she felt the transition to Gilbane would enable her to continue to grow professionally. She explains, “I felt from a values perspective, Gilbane made sense for me. It has a family-owned culture that really cares about people, and also a culture of safety, which is very similar to cybersecurity. Gilbane has built some of the largest and most complex projects on the planet. I am truly impressed by our team of experts, and how they build these complex buildings. From a technology perspective, it’s easy to work with stakeholders who know how to build things and also appreciate the need to manage risk.”

As the Executive Vice President, Chief Information and Digital Officer, Karen is responsible for optimizing the value of innovation, digital, analytics and AI, technology, and cybersecurity. The role was newly created one year ago to ensure a single point of accountability for these related areas in the company, with a focus on digital transformation at the center. The structure of her responsibilities is comfortable to Karen because risks related to digital strategies are cybersecurity in nature and to have one executive oversee those areas, it is easy to make risk-adjusted strategic plans and execute through a risk lens.

COMMUNICATING RESPONSIBLY AND EFFECTIVELY

Karen is responsible for reporting on cybersecurity to the executives and the board. She comments, “To effectively communicate, you must put yourself in the shoes of the audience and understand the responsibilities of the board. I sit on the board of another company, so I think about the board member perspective and how they are stewards of the company and its future. Boards care about the shareholder value over the long-term, ensuring there is the right strategy, resources, and risk management approach in place.”

She continues, “My advice to CISOs is to not speak in terms of technical controls and what you do every day, but communicate how cybersecurity risk is realized as any other type of business risk. In fact, we manage risks related to confidentiality, integrity, availability, and related control failures and those manifest themselves as operational risk, operational losses, reputation impacts, legal, and compliance risk. A mentor once told me that a risk is not the absence of a control. Framing the message in terms of how would the absence of that control impact the business can be a powerful way to communicate the value of our efforts.”

> *“My advice to CISOs is to not speak in terms of technical controls and what you do every day, but communicate how cybersecurity risk is realized as any other type of business risk.”*

When anticipating questions from board members, Karen suggests being prepared to speak on emerging risks, things they might have read about in the news and apply those to what is relevant to your own organization. When working with the board, Karen likes to share management's perspective and welcomes board insight and advice.

RISKS RELATED TO DIGITAL OFFERINGS

A top focus area for Karen and her team is to proactively mitigate and identify emerging risks related to digital offerings the organization is developing. It requires managing both how they compete with the digital offering, and how they concurrently manage risk in the offering.

She explains, "Our innovation team has developed a methodology for experiments and what we call the experiment canvas. Through that tool, we identify not only the potential of an idea, but some of the inherent cybersecurity risks we would need to control through the experimentation process."

Karen continues, "It's tempting to work with startups, but many are not 'enterprise ready' to safely manage sensitive data. It's important to balance the potential rewards of innovation and experiments with the cybersecurity risks. As a control function leader, you need to also serve as an enabler. You have to understand what the business goal is and how you enable success in a controlled way. With that in mind, you can come up with collaborative efforts to reach business strategies and goals while managing risk."

LEADERSHIP AND HIRING

Karen's team manages everything from innovation to cybersecurity, and to ensure she maintains effective leadership, she believes in being hands-on, which includes visiting actual construction sites in person, or the "frontline" as she calls it. She says, "I've been out to our construction sites on a regular basis over the past year. You learn a lot about how technology is used in the field. On our job sites, our teams are managing construction work performed by our trade partners. You really must walk in their shoes and experience their work environment to understand how technology is being leveraged, what the cyber risks are, and if shortcuts are being taken. It's important to bring their perspective into how to help them protect and manage risk."

When looking at the cybersecurity team and the abundant lack of talent in the industry as a whole, Karen believes in developing people to combat this skills gap. It comes down to efficient training, development, and coaching, in order to grow individual skillsets in the cybersecurity realm. Karen comments, "You're kidding yourself if you think you're going to hire yourself out of a skills gap, you have to develop it. You can find people who are good developers and encourage them to move into cyber. You can find people who are good process leaders who can help with the risk management aspects of cybersecurity because all controls operate within the context of a process. If you find a good process person and teach them about risk and enterprise risk management concepts, they can be helpful. Staffing cybersecurity teams can be a struggle if you're looking for a unicorn that doesn't exist. I find that part of my responsibility as a leader is to put together the team, that should collectively have all the skills. Then I can coach and develop the team in areas where individual team members may need support."

> *"Our innovation team has developed a methodology for experiments and what we call the experiment canvas. Through that tool, we identify not only the potential of an idea, but some of the inherent cybersecurity risks we would need to control through the experimentation process."*

TOP 5 2024 CYBERSECURITY TRENDS

What is in for 2024? Read where CISOs and security leaders will be investing their time and resources, and areas to focus on for the upcoming year.

By Katie Haug, VP, Marketing, K logix

1. Generative Artificial Intelligence Will Make an Impact

CISOs and security leaders who persistently track the evolution of artificial intelligence may gain a competitive advantage. Generative AI will continue to increase in sophistication, and adversaries will use complex tactics to conduct AI-powered attacks on organizations. These attacks may include automated malware or deepfakes. In turn, cybersecurity professionals will leverage AI-driven measures to detect and respond to threats in proactive ways that result in stronger effectiveness.

Ryan Spelman, Managing Director of Cyber Risk at K logix comments, “Everyone in cyber understands the pressure to prepare for both sides of AI – how attackers plan to use it and how their teams should integrate it into their security programs. There are some impactful emerging capabilities of AI that could identify and thwart vulnerabilities including anomaly detection in cybersecurity tools, endpoint detection and response tools, and natural language processing. To better prepare we recommend organizations set and meet internal benchmarks around their approach to AI, policies and procedures should be established with respect to AI, and investment considerations when evaluating AI solutions must be in place.”

2. Sophisticated Phishing Attacks Will Continue, More Investments In Employee Training

Employees will remain constant targets, continuing to emphasize the need for internal training programs around cyber education and awareness. The 2023 Phishing Report revealed a 47.2% surge in phishing attacks last year, and this trend is expected to continue. Boards and corporate executives are becoming more educated and aware, as direct financial loss from successful phishing attacks increased by 76% in 2022 according to the 2023 State of the Phish Report.

The market for cybersecurity awareness and training is greatly expanding, with an anticipated doubling in value by 2026, going from $5.6 billion to over $10 billion (Cybersecurity Ventures). The annual Verizon Data Breach Investigations Report (DBIR) found that 74% of data breaches involved a human element, with phishing (a.k.a. social engineering) being one of the most prevalent attack vectors.

3. Changing Regulations Will Persistent, But With Opportunities For Competitive Advantages

In the United States, regulations from governing bodies such as the SEC will continue to make updates and in turn greatly influence cybersecurity programs. For example, the new SEC Cybersecurity ruling focuses on risk management strategy, cyber threat governance, and disclosure of material cybersecurity incidents. The idea is that transparency and awareness will increase, thereby protecting the interests of investors, companies, and markets alike.

Although staying up to date requires a lot of work, according to Gartner, by 2024 less than 10% of organizations will have successfully weaponized privacy as a competitive advantage. Having a privacy program that is strongly aligned with cybersecurity not only helps build trust with customers and partners, but it enables a proactive approach to cyber.

4. Cyber To Receive Increased Representation In Boardrooms

In 2024, it will be more important than ever for CISOs to be strongly aligned with their executive counterparts, mainly boardroom members. According to K logix CISO trends, only 62% of CISOs believe their boardrooms are adequately educated about cybersecurity.

Cybersecurity was in the news more in 2023 than any other year, making it an unavoidable topic. CISOs had opportunities to continue to educate their boards on the importance of a proactive, strategic approach to cybersecurity. According to a forecast by Gartner, by 2026 about 70% of corporate boards will have incorporated at least one individual with specialized knowledge and proficiency in cyber.

Kevin West, CEO of K logix comments, “The increased relevance of cybersecurity has enabled CISOs to become strategic leaders among their business counterparts. While many are still working on achieving this position, 2024 will give them more opportunities to solidify cyber’s role within an organization. I encourage CISOs to ensure that executives understand why a strong and strategic cybersecurity program enhances trust with customer, employees and partners, and enables efficiency while reducing overall risk.”

5. Threat Detection And Monitoring To Reign Top Priority And Focus Area

Searchlight Cyber March 2023 report found that 93% of CISOs are concerned with dark web threats, but 21% of CISOs have no threat intelligence capability at all. While most security teams report that have some threat intel built into their tools, 2024 will be the year for CISOs to use threat intel data effectively and ensure it is operationalized.

Sydney Solomon, a threat intel expert at K logix states, “Effective cyber threat intelligence is timely, accurate, and provides information relevant to an organization’s specific goals and industry. With an understanding of adversaries’ targets, resources, and capabilities organizations can make strategic decisions that seek to stay one step ahead of the threats. Threat informed defense will be key in 2024 to support proactive remediation of gaps, implement stronger defenses, and make smarter decisions about how to invest resources.”

CASSIO GOLDSCHMIDT

CISO
SERVICETITAN

HEADQUARTERS: Glendale, California

EMPLOYEES: 2,500+

REVENUE: Private Company

PROFILES IN *Confidence*

Cassio Goldschmidt has over 20 years of experience, working across all sized organizations from Fortune 500 companies to startups. He has built security programs from the ground up, positively impacting organizations and strengthening their security programs.

Cassio is currently the CISO of ServiceTitan, a company that provides service visit and construction project software for trade organizations. He has served as their CISO for over five years and continues to enjoy his work because of the strong organizational leadership in place and commitment to cybersecurity. Cassio says he joined because of the mission of the organization, built by two individuals who identified a lack of technology in an underserved industry. The company had about 600 employees when Cassio started and now has over 2,500 employees, something he attributes to their strong culture.

When joining the organization, Cassio was technically the first hire in security, although there were security efforts from the engineering team before he joined. He explains, "There was no central security team before I joined, so I was responsible for a completely blank page. I was focused on building the team, figuring out who we needed to hire, identifying the first projects that we were going to tackle, and understanding how to communicate and interact with all the other teams. And quite frankly, this can be very scary for a lot of CISOs. But because I've built programs from the ground up before, I had a good blueprint of what to execute. However, I always make sure that when I'm building a program, I aim to create a replica of what I've done in the past; instead, I tailor it to the company I'm working for and their specific needs."

FOCUSING ON STRONG COMMUNICATION

Armed with a Bachelors in Computer Science, Masters in Software Engineering, and an MBA, Cassio felt prepared to help ServiceTitan grow and strengthen their security practice. Not only did he need to ensure the right security processes and procedures were in place, but he also knew it was vital to solidify strong relationships with executives and employees across the organization. This was important in order to gain key buy-in and build awareness about the security program goals and projects.

He comments, "When communicating with upper management, it's important to understand the technical side, while also understanding the needs of the business and not only the executives that are running the company, but also putting myself in the customer's shoes, working with sales, working with customer support, and so on. This helps give assurance that I will be focused on making sure our customers have peace of mind when working with our organization."

He continues, "Something I found interesting when I started hiring was that my first team member was somebody with information security background and also an MBA. And the next hire also had an MBA and was somebody with a technical background. That is incredibly rare, but I think that was a huge advantage for us in order to have people who were not only technically savvy, but always knew how to talk to the business."

The most important thing to Cassio was to build a culture of security that includes executive presence and influence. He relies on connecting with people and educating in a way that helps them understand the importance of security. He says, "You have to use empathy and appeal to the emotional side of things, and also show that you are not doing this because it's your own agenda. It's really all about the company goals and priorities, and to show that you have nothing but the best intentions in mind. It sounds super simple, but it's really hard to create those relationships and bring people to your side, and create this culture in the first place, but that is the number one thing that all CISOs should be doing because as people say, it takes a village."

"I've worked in my teams' shoes. I love to listen to people because their work is always changing. And understanding, listening, and knowing that they have a voice is very important."

CURRENT INITIATIVES AND INDUSTRY TRENDS

Cassio's current initiatives include full verification of machines and identities and right sizing privileges. Cassio says the days of having different roles and different tools is coming to an end and we are going to see more of right sizing privileges, meaning dynamically providing privileges based on needs and looking at logs to understand what kind of privileges people had and didn't use.

Another area of focus is around acquisitions and ensuring there is technical and procedural alignment between ServiceTitan and any organizations they acquire. This means expanding services to the acquired organization with things like their Bug Bounty program. The biggest focus in any acquisition is keeping security consistent to make sure practices, tools, and other areas are effective and properly covered.

In general, for the cybersecurity industry, Cassio sees access to tokens as something to look out for. He explains, "Instead of stealing data and terabytes going through routers and so on, these days if somebody gets an API token and copies it on a piece of paper, it doesn't even pass through your DLP. A former employee or attacker can get a discrete amount of data on demand as long as they want, especially if you know the tokens are not properly refreshed, or API queues are not properly rotated. So as people move to the cloud, you see more and more of these kinds of interactions using machine to machine credentials or API tokens and so on. And I don't think most of the CISOs actually see the problem with that."

Another relevant trend in the industry is Artificial Intelligence (AI), something Cassio has been studying and has been up to date on for many years. He has published articles on the topic, talking about generative AI and how it impacts business, and written papers on AI and the risk for business, to name a few. Cassio attends conferences on a regular basis, many with tracks or focus areas on AI that he chooses to actively participate in. He also received an AI certification from Microsoft. It is important he stays up to date on AI because of its impact on the cybersecurity industry. By self-learning and contributing to the community, Cassio not only educates himself, but he also spreads his knowledge with the broader industry of security professionals.

He comments, "I think AI has potential to become a big headache, especially with attacks such as business e-mail compromise. If AI understands the entire communication going on between two people, it can get in the middle of this communication and start acting as the person you're communicating with. None of the solutions we have out there are going to be able to detect these kinds of things properly. But there's also a lot of things that AI is going to help us prevent. And I think it's really a great thing that came to the industry and will help us tremendously in the future."

LEADERSHIP

Cassio prides himself on providing his team autonomy and the ability to speak up and contribute their own ideas. He comments, "I've worked in my teams' shoes. I love to listen to people because their work is always changing. And understanding, listening, and knowing that they have a voice is very important. Building relationships across business teams is also very important. It's really important to build those bridges not only internally, but also externally, speaking in conferences, collaborating with the community, which I try to do as much as I can. I can really bring the best back to the company and help the team grow. I am always focused on our people and that they get the education they deserve."

To keep growing on a personal and professional level, Cassio engages with all aspects of the cybersecurity community. He talks and meets with other CISOs at many industry conferences and has created a strong network of collaborators amongst his peers. This helps him address challenges, discuss industry trends, and continue to learn from people who are going through the same experiences he is.

Cassio also works with startups and VCs to expand his knowledge and learn from new-to-market security companies. He says, "There are a lot of startups, they're very innovative and they're doing things differently in solving problems that big companies have been focused on. When you talk with a startup and you become part of their customer advisory board, you can influence their solutions in order to work in your type of environment. I spend several hours during the week talking with startups and also VCs."

DOUG INNOCENTI

CISO
MOONPAY

HEADQUARTERS: Miami, FL

EMPLOYEES: 300

REVENUE: Private Company

Doug Innocenti has a strong IT and security background in the banking industry, working a combined 28 years at Legacy First Union, Wachovia, and Wells Fargo (which acquired Wachovia in 2008). He then worked at Navan (formerly TripActions) before landing at his current organization, MoonPay.

Doug says security has been ingrained into everything he has done throughout his career, giving him wide exposure to many aspects of the industry. He became passionate about security projects early on, so his career naturally moved from IT-focused roles to more security-focused roles.

At MoonPay, Doug had an opportunity to combine his financial services background with his passion for working at innovative, forward-thinking organizations. MoonPay is a Web3 infrastructure company building end-to-end solutions for payments, custody, world class design, and enterprise-scale digital asset and smart contracts minting.

“Coming to MoonPay was almost like coming home for me,” he said. “I’ve always loved innovation, building new technologies, and working at the cutting edge of new tech. When I saw what MoonPay was doing, it was the perfect model of what I was looking for and interested in. I had an opportunity to help move the needle forward for the next level of technology and expand the fintech space. I feel that I’m at the cornerstone of something new and innovative.”

He initially joined MoonPay as Director of Information Technology, running the IT program and working on projects like building the foundations of a zero-trust model, hardening corporate systems, and laying the foundation for the overall security controls. At the time, his team partnered with the security team, which made his move into the CISO role a seamless next step.

As CISO of MoonPay, Doug oversees the strategy, architecture, and governance for IT and security, and is also in charge of implementing and integrating SaaS, contact center, support, and infrastructure platforms. He considers his role a strong combination of information technology and security.

“I have different teams that handle a lot of the traditional IT engineering, and I have my cyber defense team, I have my security operations team, I have my technical operations team, and so on,” he said. “The way I look at things is that all of us are responsible for security. I hold them all accountable for how they are going to ensure they’re not only implementing secure and robust systems, but they’re also caring for the overall topology of security at MoonPay.”

FOCUS ON STRONG 2024 INITIATIVES

MoonPay recently earned its ISO 27001 certification, a large accomplishment considering the amount of work and time Doug and his team invested over the better part of the past year. The benefits of this certification will help MoonPay improve overall program maturity while continuing to reduce risk in a proactive manner. Doug says his team is also working on finalizing their SOC 2

> *“The way I look at things is that all of us are responsible for security. I hold them all accountable for how they are going to ensure they’re not only implementing secure and robust systems, but they’re also caring for the overall topology of security at MoonPay.”*

Type 2 certification. They finished their SOC Type 1 earlier this year, and their Type 2 will soon close out after nine months of evidence.

As Doug's team moves into 2024, they plan to achieve their ISO 27018 for PII data in the cloud environment.

"I really think it's going to identify and allow us to extend our overall security posture along with the traditional things that every CISO is looking at right now when it comes to zero trust and defenses around the perimeters," he said.

To accomplish these certifications, Doug leverages his own team along with auditor partners who help level up and ensure they are meeting specific criteria. His internal team takes the lead on day-to-day work that needs to be done to deliver compliance, and in turn the auditors help them deliver on those.

In the past two years, Doug and his team have worked tirelessly on retooling their environment to better understand what investments they have, sunset anything they are not using, and ensure their strategy aligns with the products in their environment.

"Functionally, I think we're in a really great space," he said. "We're going to spend the next year making sure we're getting the most out of the platforms we have, and optimizing them so that we're positioned for our continued growth as an organization."

To ensure executives remain up to date on security plans and goals, Doug has employed a strong communication strategy to share data upstream in a productive and proactive manner.

"On a weekly basis, I produce reports from my team and myself that roll out to the executive team, so we are constantly sharing our security posture, what is underway, what we need to look out for, and what our next steps would be," he said. "This is all combined with our ongoing OKRs at a company level, to really ensure that we're communicating everything upstream on a weekly and a biweekly basis. And really, the culture itself at MoonPay, and the ability to communicate and share information so widely, ensures that not only the executive staff, but the company as a whole is aware of what's going on and how we're delivering to help support not just MoonPay but the employees with staying safe."

TRENDING AREAS AND CHALLENGES

The limited talent pool in information security is something Doug believes to be an ongoing challenge for the industry. Although he feels lucky to have limited attrition within his security team, he says there is always a need to continuously bolster the skill sets of his team members.

"We're focused on leveling up the skill sets of the team in conjunction with completing their daily work," he said. "I'm focused on reinforcing the need to grow their skills, to grow their certifications, and ensure they're continuing to uplift themselves and the program. It's a balancing act, but I've been lucky enough to have a great team that's been able to deliver on both of those."

The changing landscape of threats continues to be a challenge faced by many, and Doug believes teams must be dynamic in their approach to keep pace and ensure their organizations remain secure.

"Staying ahead of threats is all about having the right tooling, the right places to monitor the perimeters around, not just our platform itself, but our endpoints, our corporate systems, and having the right proactive monitoring and notifications in place," he said. "And then obviously the ability to review those on a daily, weekly, monthly, quarterly basis to identify the trends."

Artificial Intelligence (AI) poses another challenge, something Doug and his team are staying informed about in order to better understand the changing market.

"AI is an ongoing challenge for all CISOs to consider, and not only looking at what it's doing but also the fact that it changes the landscape of how you see cyber defense," he said. "The ability for AI to do things that individuals were doing before, but also protecting the data that we have, is important. We need to make sure that if we're using AI, the data we're producing into those large language models are being secured and protected, which is an area we've done a tremendous amount of work on. I think it's evolving and moving faster than anything I've seen in my career. The simple TDoS or DDoS attacks of the past were easy to deal with. Now you're dealing with things that you wouldn't even have fathomed five years ago."

2024 Artificial Intelligence Trends

Leveraging AI to mitigate threats and capitalize on innovation

By Emily Graumann, Marketing, K logix

2024 will be an even bigger year for Artificial Intelligence (AI), with more people harnessing its powerful potential, and the presence of stronger, more widespread possibilities. With this technology comes a plethora of both benefits and risks, the former utilized by cybersecurity teams and the latter exploited by cybercriminals in a stiff and innovative arms race. It is important for security leaders to be vigilant against new threats, as well as up to date on the abilities of AI and rising trends.

We identified key things to look out for in 2024 as it relates to AI:

AI-Enabled Cyberattacks And Sophisticated Phishing

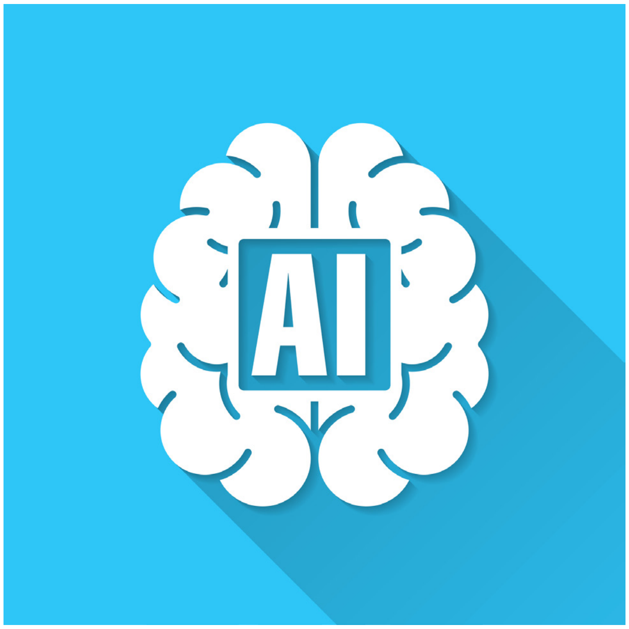
AI has become a mainstay in the toolbelt of cybercriminals, particularly to aid in launching social-engineering attacks. This includes the creation of phishing messages with more effective messaging to trick victims. According to Forbes on Blackberry's recent research, "top concerns for misuse of ChatGPT revolve around social engineering (creating highly convincing and difficult-to-detect phishing emails) and skilling up less experienced hackers to become more effective with their attacks." Gone may be the days of being able to identify these malicious messages by grammatical mistakes or awkward phrasing, and with generative AI in the hands of cybercriminals, a greater volume of attacks can be created in less time, with a higher success rate than ever before. Direct financial loss from successful phishing attacks increased by 76% in 2022 according to Proofpoint's 2023 State of the Phish Report.

Password Hacking And Deepfakes

AI technology is used by cybercriminals to improve their algorithms for password hacking, leading to faster and more accurate predicting. Because of the profitability of this endeavor, cybercriminals may concentrate a larger amount of their focus on password hacking. Other AI-enabled threats include deepfakes—content that has been digitally altered to mimic individuals, often high-profile leaders, politicians, and executives who have no shortage of audio and visual content to manipulate, to maliciously disseminate false information. AI's ability to distort and transform this content is used in this way by cybercriminals often in addition to social engineering attacks and extortion.

Penetration Testing

Fortunately, not all recent AI trends are harmful. This technology has proven the potential to be a major asset in penetration testing. AI can be used intentionally to explore the defenses of software and networks. Through this process, organizations will be able to identify their weaknesses more efficiently, before hackers get the chance to find and exploit them.



AI as Resource for Protection

Even with the risks AI can pose, it is also important to realize the benefits of this technology. Harnessing these advantages is essential for combating new challenges in the cybersecurity landscape. AI can be extremely useful to security teams through its capability to analyze large amounts of incident-related information. This can help teams better understand the data and take action against the threat. AI is also useful in flagging suspicious activity, emails, and login attempts to prevent potential breaches. Additionally, threat monitoring by AI is a technology that cannot be matched. AI can detect attacks more effectively and accurately than humans, and AI produces fewer false-positive results. In utilizing these qualities, the time and energy of a security team can be conserved, and the detected attack can be addressed in a manner faster than ever before.

The Growth and Potential of AI Continues to Explode

AI is here to stay. And not only that, it has also become a priority for organizations to learn about and understand. According to Forbes, 76% of enterprises have prioritized AI and machine learning in their IT budgets, and Blackberry found that “the majority (82%) of IT decision-makers plan to invest in AI-driven cybersecurity in the next two years and almost half (48%) plan to invest before the end of 2023.” The market for this technology also continues to increase. Recent research estimated the global market for AI-based cybersecurity products was about $15 billion in 2021 and will surge to roughly $135 billion by 2030 (Morgan Stanley). When thinking of how far AI has come, it is only fair to believe the potential benefits and potential risks of this technology will continue to evolve. Moving forward, security leaders must dedicate themselves to being watchful against the ways AI can be weaponized, as well as being receptive to the potential of AI to improve their industry and offer answers to these new threats.

Sources:

Forbes, “How AI Is Disrupting And Transforming The Cybersecurity Landscape”

Morgan Stanley, “AI and Cybersecurity: A New Era”

Core to Cloud, “How AI is Revolutionizing Cybersecurity: Trends and Implications”

Blackberry, “ChatGPT May Already Be Used in Nation State Cyberattacks, Say IT Decision Makers in BlackBerry Global Research”

CNET, “The Biggest AI Trends in Cybersecurity”

CSO, “Emerging cyber threats in 2023 from AI to quantum to data poisoning”

Proofpoint, “2023 State of the Phish Report”

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM

2024 CYBER TRENDS

FEATS OF STRENGTH
DECEMBER 2023