FEATS OF STRENGTH

A Business-Focused Cybersecurity Magazine

ARTIFICIAL INTELLIGENCE: FRIEND OR FOE?

IN THIS ISSUE:

JUNE 2023

IK logix

TABLE OF CONTENTS

Artificial Intelligence *June 2023*

FROM THE *Editor*

Dear Readers,

Artificial Intelligence and the security surrounding it has been top of mind for our community, and we felt this was a good opportunity to include articles and CISO interviews to help provide guidance. It is an exciting topic because AI technology has the potential to revolutionize the way we work. There are some amazing innovations that come with AI, however it's important for organizations and security leaders to thoroughly understand both the benefits and risks.

We've found the numerous advantages when leveraging AI tools are only realized when there is a strategy in place with strong processes and parameters. AI has the potential to help organizations move faster and increase their security measures. However, similar to when everyone rushed to move to the cloud when workers went fully remote, many security protocols were overlooked, causing cracks in protections against threats.

It is important to consider the risks associated with AI, namely bad actors who are able to exploit this technology. It's vital that organizations understand the persistent and evolving risks associated with AI tools so they can better prepare themselves. In this issue of the magazine, we discuss all of this in detail. Some of the K logix team spent months researching and staying up to date on AI in order to produce content that talks to some of the challenges and confusion out there. We also spoke with four CISOs who share their thoughts and approaches on AI.

What we found was similar across our experts and the CISOs we interviewed - AI is a great opportunity but needs to be approached with caution. We hope you enjoy reading this issue of the magazine.

Kevin West

CEO, 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.

CARLOS CONG

DEPUTY CISO
PAYCHEX

HEADQUARTERS: Rochester, NY

EMPLOYEES: 16,000+

REVENUE: $4.61 Billion

PROFILES IN *Confidence*

Carlos Cong has worked in technology for over 20 years and always been passionate about security because of the great responsibility in protecting data and availability for organizations. As part of his charge in his current role as Director of Enterprise Security at Paychex, Carlos helps protect the $4 billion company with over 700,000 customers across the globe. He says he wakes up everyday energized to tackle new risks and concerns on the horizon, mainly because he is able to work with an incredible team of talented people.

Carlos came to Paychex over ten years ago and instantly knew he would enjoy working here because he was surrounded by passionate, like-minded individuals. Over the last ten years he has had opportunities to work across technology roles, which naturally progressed into his current role working on the security side of the business. Looking back over his tenure so far at the organization, Carlos says it is exciting to see how much his work has helped modernize their environment, everything from the data center to the network, security, and beyond.

He comments, “Right now I directly oversee the Cyber Fusion Center, which includes security intelligence, detection, hunting, insider threat security, incident response, digital forensics, security assessment of vulnerability management, application security, the 24x7 security operations center, and our cyber awareness and response management program. I also serve as a Deputy CISO, Chief of Staff for our CISO, so I help to lead the security engineering, program management, and risk and compliance pillars as well within the organization.”

He continues, “I’ve been working full time in security for a little over one year. Even though I’ve been at Paychex for ten years, I haven’t been in security the entire time. When I first came to Paychex, I was on the Enterprise Technology Services team, which included a very close partnership with security, leading security initiatives lockstep with the team, and driving new technology innovation in all types of different areas. When I officially led security, I had a good grasp on the various pillars within security, but there was a lot of learning to be done and I had to spend a good six months doing a lot of research, talking to colleagues, working with my team and truly getting grounded and understanding all the various pillars, the feedback loops, the frameworks that we needed to put in place in order to scale. We’ve been hard at work doing that since.”

FOCUS AREAS – THREATS, AI, PREVENTION

Like most security practitioners, Carlos says he is focused on addressing threats in proactive and efficient ways. He explains, “Things like ransomware, data exfiltration, prevention and response are definitely always top of mind. Plus we are focused on our ability to rapidly respond to zero-day vulnerabilities and just general vulnerabilities in the environment. There’s a series of different strategies that we have out there.”

“AI comes with innovation and opportunity, but it’s so early on in its creation that you don’t know how the adversaries are going to take something that was meant to propel society forward, and potentially weaponize it. And we already see evidence of that.”

From an AI perspective, Carlos considers it an emerging risk. He comments, "AI comes with innovation and opportunity, but it's so early on in its creation that you don't know how the adversaries are going to take something that was meant to propel society forward, and potentially weaponize it. And we already see evidence of that. You read articles about how ChatGPT and others could develop malware in them. Intellectual property is getting lost. We're doing a lot of research. We're working with various industry partners to see exactly how this is going to apply to Paychex from an AI perspective."

He continues, "In the prevention bucket, there are several different things that we're hyper-focused on, obviously identity management, zero trust, and least privilege access. Everything from the end user all the way through our workloads and applications, making sure the environment is appropriately segmented, making sure we have the appropriate detections and controls in place to prevent not only the spray and pray bad actors, but also the more mature sophisticated ones that like to slow crawl in your environment. Tactics being used are becoming more and more difficult to detect and we have to stay ahead of those things faster. Weaponization is happening daily, and we must have a processing framework in place to keep up with all these different tactics and techniques, and we have a good practice around that. Because we're continuously doing intelligence gathering and seeing how things out there in the wild apply to our environment, it's a continuous cycle, and it's never ending. I don't anticipate it to slow down. In fact, I anticipate it to speed up, and that's really what we're preparing for."

EXECUTIVE SUPPORT & SERVANT LEADERSHIP

Having executive support is important to Carlos, and he says his team is fortunate to have an executive team that is fully supportive of their program. He explains, "We have the full backing of the organization when it comes down to needing to address certain risks that we have, even including our legal teams. So, it's really a true company effort, but we have our challenges too, just like the rest of the world. Everybody has budget pressures and there are decisions that we all have to make. The good news about having a risk priority is that we know where our 'true norths' are, and it makes it so much easier to speak with the data and prioritize things."

Carlos considers himself a servant leader. He comments, "I have a few core things that are principles in mind that my team is very well familiar with. Things like doing what's best for the business, customer or employee, those

"We have the full backing of the organization when it comes down to needing to address certain risks that we have, even including our legal teams. So, it's really a true company effort, but we have our challenges too, just like the rest of the world."

should always inform our approach from the front. Another focus is to always advocate for your team and carry the flag for security. Step up and step in. Basically, meaning if there's a time and a place where you feel like the team is struggling in any way, we should be able to step in and assist and provide whatever knowledge or inputs is needed at the time, and then pull up and push out is more about advocating for your employees. Just making sure that you're aware of their career goals and aspirations, and then helping them navigate how to achieve them. And that goes back to our career journey framework that allows employees to really navigate and map out exactly what the opportunities are within security and then how to get there."

To continue and grow as a leader Carlos takes advantage of professional development opportunities. He also learns from his executive management, taking their feedback and engaging with them on a regular basis. He continues, "Industry peers are important to learn from as well, especially taking feedback from them. It's key for me to make sure I'm showing up the right way, continuously learning, doing a lot of reading in terms of research in the space and just keeping abreast of what's new and what's emerging. So, there's a variety of things that I try to do to continuously develop because it's incredibly important. I don't like to ever feel like I'm stagnant in any way because if I am then that means the organization isn't moving the way that it could or should."

The CISO's Guide to Artificial Intelligence

By Sydney Solomon, Senior Cybersecurity Consultant, K logix

ChatGPT has made Artificial Intelligence (AI) a widespread topic of conversation in cybersecurity circles and there is certainly much to be said on the topic. ChatGPT is an application of Natural Language Processing (NLP), a subfield of AI. As NLP capabilities advance, there are many ways NLP can be used in cybersecurity tools to enhance detection capabilities, reduce manual tasks, and improve visibility of vulnerabilities, which this article will explore in more depth.

THE BASICS

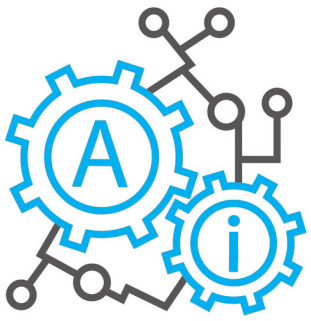
To examine NLP's cybersecurity applications, there are a few key terms to understand at a high-level, starting, at the very top, with AI. AI is a broad concept that refers to a machine simulating human intelligence. Researchers seek to achieve this by training machines to learn the way humans learn. An example of this is machine learning (ML), where the AI algorithm is trained to learn patterns from data. The two primary ways an AI algorithm is taught to do this are 1) supervised learning and 2) unsupervised learning*.

- Supervised learning: AI algorithms that are trained on labeled data to derive patterns can be used to label new data. An example would be using historical incidents to identify new incidents.
- Unsupervised learning: AI algorithms that try to derive patterns from unlabeled data. Examples include categorization (such as clustering) and anomaly detection.

The next term, deep learning (DL), is a ML technique that utilizes neural networks to derive patterns from data*. Neural networks, inspired by the design of the human brain, are layers of inputs and outputs. Each layer consists of a bunch of nodes that perform an evaluation function on an input. The output of that function is then passed onto the next layer which conducts another evaluation. This goes through however many layers until a final output is reached.* NLP is a subfield of AI that uses various ML techniques, including DL, that strives to teach a machine to analyze and understand language (semantics and syntax).

NLP'S APPLICATIONS IN CYBERSECURITY

Anomaly detection in cybersecurity tools establishes a baseline of what normal traffic looks like at an organization and then alerts on any variants. To do this, it is using an AI algorithm that is deriving patterns from the data via unsupervised learning. A challenge with this process is that the AI algorithm can generate many false positives, causing alert fatigue among analysts. Applying NLP techniques to anomaly detection could reduce the number of false positives, minimizing the need for manual review. Leveraging NLP to analyze logs, which are partially written in natural language, an Intrusion Detection System would have added data points to identify a security incident more accurately.



Endpoint detection and response tools (EDR) filter and analyze activity on the endpoint to detect and

prevent a malicious threat. Its predecessor, anti-virus tools, filtered threats based on a list of known malicious signatures, which is an example of an AI algorithm that detects patterns using supervised learning. Legacy anti-virus tools could detect known threats but could not detect new types of threats. To address that gap, EDR tools today filter on additional datasets, like anomalous traffic patterns, and conduct dynamic malware analysis, which is when the tool runs suspicious activity in a controlled environment to observe behavior. While EDR tools can identify new threats, it can be time-consuming and visibility gaps may persist. NLP can further advance the EDR space by implementing fast-filtering methods, such as analyzing printable strings in the malware code, to detect indications of malware.

One concern with the emergence of tools like ChatGPT is that phishing emails will be harder to detect as malicious actors can utilize ChatGPT to write targeted phishing emails with perfect grammar. Email protection tools can adapt to this new threat by utilizing NLP to identify the types of emails malicious actors may send and unusual communication patterns. For example, a malicious email may read differently from how employees at that company would compose an email. Most email protection tools on the market today make use of NLP techniques and as that realm of AI advances so will the tools' ability to accurately identify a threat.

NLP can also be used to identify vulnerabilities. Developers, for example, can use NLP tools, like ChatGPT, to identify vulnerabilities in their code. Additionally, NLP capabilities can augment existing vulnerability management tools by scanning specification documents. Specification documents provide an overview of the software / system / product in question, such as its purpose, a list of features, code design and use requirements. Scanning these documents can provide clues indicating where vulnerabilities may exist. A vulnerability scanning system that utilizes NLP capabilities could provide a more vivid picture of vulnerabilities on the network.

CONCLUSION

While the article covers some of the ways AI NLP capabilities can enhance an organization's cybersecurity toolset, there are many more applications. K logix can provide guidance to organizations on how AI is changing cybersecurity and the threat landscape as well as how organizations can prepare. For more information, please contact one of our experts: info@klogixsecurity.com.

*There are other forms of machine-learning that fall outside of these two categories.

* It should be noted that while DL is generally categorized under ML, the distinction between the two is not always clear-cut.

*With DL, the patterns and goals can be abstract, and, thus, it is not always fully known to humans how the machine solves its problem.

Sources:

https://www.youtube.com/watch?v=aircAruvnKk.
https://www.youtube.com/watch?v=gQmXAKD4_3o%2C
www.securityinfowatch.com/cybersecurity/article/21114214/a-brief-history-of-machine-learning-in-cybersecurity
Li, Dr. Albert Zhichun, and David Barton. "A Brief History of Machine Learning in Cybersecurity." Security Info Watch.
https://doi.org/10.1007/s10207-021-00553-8
www.proofpoint.com/us/blog/engineering-insights/leveraging-ml-to-detect-ai-generated-phishing-emails
www.insights.sei.cmu.edu/blog/artificial-intelligence-in-practice-securing-your-code-using-natural-language-processing/.

JACOB COMBS

Chief Product Security Officer/Senior Director Medical Device Cybersecurity

INSULET

HEADQUARTERS: Acton, MA

EMPLOYEES: 2,500+

REVENUE: $1.3 Billion

PROFILES IN *Confidence*

Jacob's career in technology and security has spanned many different industries including telecommunications, defense, financial services, and healthcare. He explains, "I've worked across different critical infrastructure sectors that have extremely high requirements for cybersecurity. This gave me an abundance of experience because I'm not formally trained in cybersecurity, I had to learn by doing to succeed in those industries. And in doing so I realized my love for identifying and mitigating cybersecurity risk."

Jacob is currently the Chief Product Security Officer/ Senior Director Medical Device Cybersecurity at Insulet, an innovative medical device company improving the lives of people with diabetes and other conditions through its Omnipod delivery system.

SECURITY BY DESIGN & KEY RESPONSIBILITIES

As Chief Product Security Officer/Senior Director Medical Device Cybersecurity, Jacob and his team's responsibilities include security of Insulet's Omnipod 5 Automated Insulin Delivery system, as well as legacy medical device products. His team ensures strong security is holistically designed into their products from start to finish. He explains, "We have a large ecosystem that's built around the devices we manufacture and sell. And we are laser focused on security by design, especially when it comes to security architecture, risk management and testing, across embedded devices, mobile applications, cloud services, and data. Along with that comes the global risk management of these products across the full product lifecycle especially from a cybersecurity perspective."

With a continually changing landscape of global regulatory requirements, Jacob ensures his team keeps the organization's devices and patients safe across the globe by managing privacy and ensuring their data is protected.

Jacob continues, "Different product platforms may move into different territories, use different technologies, or integrate with data differently. We have to build a secure ecosystem around our product that gives the business the ability to be agile and address patient needs as they arise. Since security is built into the product, the business can pivot quickly to meet market or regulatory demands."

BUILDING FROM A RISK MANAGEMENT PERSPECTIVE

Insulet's mission is to build security into products using a risk-based approach. Jacob makes sure all stakeholders align to this mission from not just a technical perspective, but also how security protects patients and positively impacts the business.

To achieve this, Jacob says it starts with securing a seat at the table. He believes in regularly meeting with executives and the board to inform them on the status of the security strategy, the current security posture of the products, and how the security program is faring in regard to regulatory changes. Providing risk-level information and how it impacts the company and product lines is vital. Aligning cybersecurity risk to business goals such as the security of next generation products, builds strong communication lines and ensures leadership understands the value of security. He comments, "The foundation is all about risk. I always approach issues and proposals from a risk perspective, talking in terms of business opportunity, brand equity, or customers satisfaction.

"We have to build a secure ecosystem around our product that gives the business the ability to be agile and address patient needs as they arise."

I express it in the terms that mean the most to the to our customers."

Having a business-focused approach enforces positive dialogue that goes beyond technical jargon and instead emphasizes the importance of security's impact on the overall business. Jacob says this also builds credibility for what security is delivering for the business and results in stronger buy-in for future projects or initiatives.

To further solidify the secure by design approach, Jacob says it is important to implement organizational policies around security in product development. He explains, "By engaging early with product development teams using structured and rigorous security assessments, security requirements and design are baked into the product from the beginning. Building this cybersecurity muscle within the organization ensures that secure design happens from the beginning on every single new feature or new product being developed. It has been quite effective in finding issues early and designing a strong security foundation. The business case for security by design is undeniable."

FOCUSING ON MATURITY AND COMMUNICATION

The top focus area for Jacob and his team is expanding and maturing many of the product security policies and procedures that have been developed over his tenure. Launching an innovative medical device is hectic and processes must be regularly updated to ensure their efficiency and effectiveness. Jacob comments, "It is important to iterate over your processes to ensure you are moving from baseline maturity to the next level. In an area like vulnerability management where a baseline process only tracks vulnerabilities, the next level would be ensuring that product development teams are decreasing their time to patch identified vulnerabilities. By maturing these processes during the development and maintenance lifecycles, we are making sure security patches are delivered to the field at a much faster rate. This protects our customers and our business."

Security automation is also something Jacob plans to continue to invest in. He says, "In the medical device industry, our quality standards require rigorous design verification processes. Since these processes statically verify requirements, we have designed into the system, they are a ripe target for automation. The product security organization continues to expand its automation capabilities and I have worked tirelessly to build automation into our DNA. I target security engineers with software development backgrounds and require that automated test cases accompany every security requirement that emerges from our security risk assessments."

He continues, "The last area I'm focused on this year is continually re-evangelizing security. I create training presentations for both technical and non-technical groups within the business. I believe it is important to speak with teams at all levels of the business to bring them up to speed on regulatory changes as well as the modern security landscape. Continuous training and communication ensures that security risk is part of the decision-making process."

"There's a lot of thinking, analysis, review, communication, and collaboration that has to happen to enable secure product delivery at scale."

KEEPING UP WITH REGULATIONS AND TRANSFORMATION

Jacob says he faces two main challenges, both very common across the medical device industry. The first is addressing increased scrutiny from regulators. He jokes that he used to read interesting fiction books for his own enjoyment, but now only reads articles and books covering standards, laws and regulations. He said to be successful in his role, you must always stay up to speed on any changes coming from regulators. He has developed a forward-looking product security program, so they are ahead of the curve when any new regulations are published.

The second challenge, similarly faced by many industries, is security's ability to keep pace with business transformation. Businesses are growing rapidly, expanding their product lines, adding regions, and often undergoing digital transformations at the same time. Jacob comments, "Our products are leading growth in the diabetes technology market and the demand continues to be high. So being able to scale and keep up with that increased demand from a security by design perspective is key. There's a lot of thinking, analysis, review, communication, and collaboration that has to happen to enable secure product delivery at scale."

PROFILES IN *Confidence*

HUGH TOWER-PIERCE

CISO

MILLENNIUM TRUST COMPANY

HEADQUARTERS: Oak Brook, IL

EMPLOYEES: 1,000+

TOTAL ASSETS UNDER CUSTODY: $55 Billion

Hugh Tower-Pierce has over 23 years of experience in both technical and people management roles, with the majority of his career spent working in health insurance, health/tech and financial-related businesses.

Hugh currently serves as Chief Information Security Officer (CISO) for Millennium Trust Company, a leading provider of health, wealth, retirement, and benefits solutions, serving over 5 million customers nationwide. He has been in this role for four months and pursued the position because of the unique opportunity to work at a company that helps people plan, save, and invest. Due to his background in both finance and healthcare, Hugh felt this company and role would give him exposure to familiar verticals, but also introduce a new set of security challenges and opportunities to explore.

Organizational support is important to Hugh, as he believes a security program is more successful when it is backed by not only the executives, but across the business as an intrinsic part of the company's culture and shared goals.

RESPONSIBILITIES & FOCUS AREAS

Hugh is responsible for typical security program areas including security operations, incident response, governance and policy, due diligence (inbound and outbound), application security, identity, and compliance. To accomplish the security program goals while continuing to support the business, Hugh has identified major focus areas including assessments, identity, and application security.

For assessments, Hugh notes, "We spend a lot of time on the assessment piece. There is a lot of due diligence for acquisitions, which take time, and we focus on assessments related to compliance like PCI, SOC, and HIPAA. The due diligence we do on vendors looks conceptually and procedurally similar to customer assessments, which also relate to compliance assessments."

Application security is another area of attention. "We are partnering on customer identity issues, and also focusing on how authentication works across multiple product areas, the architecture of products between our mobile and web properties, and making sure we engage with our product team," says Hugh. To ensure security is baked into the SDLC, Hugh focuses on transparency, engaging with the product teams on an on-going basis. This results in better communication and more understanding in the value of security as part of the development process, avoiding any surprises or delays.

One challenge Hugh and his team face is security inherent to acquisition activity the organization has been involved in. Hugh explains, "There's some version of independent environments that present strategic and tactical challenges. You must think through them from a security and business perspective when it comes to both the user and employee experience and having a common set of standards across those environments. If we acquire a business, we must make sure we are looking at the distinct risk challenges and how we can operate as one company and apply one set of standards across the board. There must be a consistent security strategy to support this kind of rapid growth."

AI POTENTIAL & RISKS

Hugh believes there is a huge potential for business opportunities, occurring across both big and small use cases when it comes to AI. He explained, "The individual could benefit on a day-to-day basis with small but frequent use of AI for particular tasks, while there are also opportunities at a larger scale doing such things as data analysis to optimize services. Regardless of what security issues or risk may surround AI, we must adapt to it."

He also acknowledges what to look out for, and comments, "One of the main things to be aware of is the potential for data leakage which may exist as an acute concern

when early in adoption lifecycle. Right now, because of the way companies have been slow to react, lots of people are using generative AI services outside of any framework. The resulting fear is that this unmanaged use can lead to data exposure. At Millennium Trust we're taking steps to manage these risks while investigating how best to incorporate AI services to the benefit of our employees' productivity and value we provide clients. Beyond data leakage, there are ethical and bias concerns with AI. Broadly speaking many organizations are finding themselves behind already, with their workers using it in an ad hoc fashion, and companies scrambling to identify what their specific opportunities and risks are."

Hugh also believes vendors are late to enter the AI discussion. He describes an 'AI arms race,' and has been in discussions with security tooling vendors about AI-related threats. However, he feels most don't have strong answers yet, they're still late in identifying what those risks might be to their products. An outcome of this might be that AI resistance or AI features become part of the vendor selection criteria. Hugh plans to continue to bring the topic up with vendors and ensure he remains vigilant with research and trending data around AI.

LEADERSHIP APPROACH

"My philosophy is that if I can hire and develop good people and give them the space they need, they tend to succeed. I will always make sure I'm there as a safety net if something happens, so I can provide a more hands-on approach or guidance as needed. I am normally naturally calm and like to bring stability to situations, which I've found helps in certain types of work like incident response. I also prioritize trust, a big factor in how I lead and build a team," Hugh says.

As a part of his own growth, Hugh discovered the importance of self-awareness and vulnerability as a way to connect with others and develop as a better leader. He focuses on receiving feedback in a non-defensive way and leaving (professional) fear at the door to continue to develop as a leader. He emphasizes being authentic and honest with people and staying grounded as much as possible. Mentorship has always been important, and Hugh believes in seeking the help and guidance of others to better oneself, as well as providing mentorship to those who can learn from his perspective, experience, and skills.

Activities outside of work also help ensure Hugh is a strong and successful leader. Long distance running in the 50-to-100-mile range helps him spend time outside and process the variety of interesting or challenging issues that come with the job. He's found that the extreme physical and mental effort involved tends to strip away and identify the things in life that are truly inconsequential, leaving only the things that matter. In gaining this kind of perspective, it helps Hugh refine his priorities, whether that be at work or within his personal life.

COMMUNICATING WITH EXECUTIVES

As a security leader who interacts with many non-technical

"In discussions with leadership, and other non-technical executives, I try to meet them where they are and offer them as much as they're interested in engaging on risk and security, while avoiding too many technical terms."

people, Hugh says he must ensure he understands what the business is doing in terms of priority. He explains, "When I'm talking to someone on the finance, product, sales, or customer service team, it's important to empathize with what their challenges are, what they're trying to solve, and what the term "success" means to them. It's also important to interact with them from the perspective of the business, and not only focus on security. As a security team we can't operate in a vacuum, we don't exist in the company just to practice security for its own sake; we exist to enable our colleagues to do what they need to get done in a safe way and to foster trust with our customers."

He continues, "In discussions with leadership, and other non-technical executives, I try to meet them where they are and offer them as much as they're interested in engaging on risk and security, while avoiding too many technical terms. I try to put myself in their shoes and meet them on common ground. Security needs to have a positive perception in the company so that we can be most likely to succeed doing our part to foster business growth. It's important to me that we are viewed as partners rather than a source of friction. We must give the right level of feedback and provide trusted and informed counsel on risk where we need to, to mitigate that risk and help continue to build success."

The Positive Side of AI

How to leverage AI to prevent threats

By Ryan Spelman, Managing Director, Cyber Risk, K logix

OVERVIEW OF ARTIFICIAL INTELLIGENCE

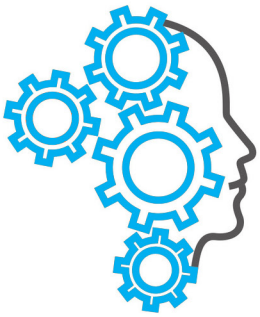
In this day and age, Artificial Intelligence (AI) has become more prevalent in society. AI is essentially the development of systems to execute tasks that would normally be done manually by a human being. From vacuums to Siri, AI has allowed us to live in a more hands-free world where numerous tasks have been automated for us. It has not only automated countless tedious tasks to provide convenience in our lives, but it also has helped make our lives a lot easier. With the touch of a button, our entire houses could be cleaned, and with the sound of our voice, we can receive directions to any destination. But despite the numerous capabilities AI has allotted us, it can accomplish even more feats in the realm of cybersecurity.

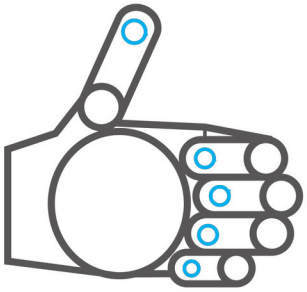
Cybersecurity is a constantly moving target as those in the field work relentlessly to protect against and mitigate the threats of tomorrow. Now, with the introduction and development of AI, a wide array of new and complex threats has also risen, such as deepfake technology; AI products that, "aren't fully ready," with a "number of issues that need to be sorted"; and a number of other methods and vulnerabilities that threat actors look to exploit. For this reason, organizations have needed to work tirelessly to defend against this new threat landscape.

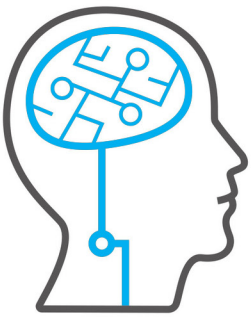
LEVERAGING AI TO PREVENT THREATS

Although AI may have come with new methods for an organization to be compromised, it has also brought a revolutionized way of mitigating and fighting against yesterday's threat, and the threats that are to come. Due to the numerous methodologies a threat actor leverages to compromise an organization's environment, there is not a one-size-fits-all solution. This is where AI can make a difference. For example, SentinelOne has unveiled, "a revolutionary threat-hunting platform that integrates multiple layers of AI technology to deliver unparalleled security capabilities and real-time, autonomous response to attacks across the entire enterprise," which would help organizations significantly increase their security measures. AI has also created additional benefits to reduce the chances of threat actors successfully gaining unauthorized access to an environment, such as:

- "Avoids Human Error" which is the cause of many







compromises within organizations

- "Identifies Possible Vulnerabilities Around the Clock" which would help companies address threats in a quicker and more efficient timeframe
- "Able to Utilize Huge Amounts of Data" which would allow the enterprise to analyze larger amounts of information for potential risks and threats

UNIQUE ASPECTS OF AI

Overall, AI has critical capabilities that can assist organizations in protecting it's data, assets, and customers. These different capabilities are what makes AI so unique, and the three that can have the most significant impacts are machine learning, robotics, and self-awareness, as they provide users with a more sophisticated approach to security to help prevent threats and elevate security measures.

Through machine learning, AI can:

- Monitor and learn patterns of internal users
- Analyze honeypots to learn new types of attacks threat actors may utilize
- Ingest information from cybersecurity forums to learn new attack types
- Investigate methodologies of threat actors attempting to attack the organization's environment

Through robotics, AI can:

- Provide enhanced physical security for an organization's offices, sites and data centers
- Replace legacy systems in the environment that are more susceptible to attacks
- Reduce insider threat as machines can manage sensitive data
- Can replace metal detectors at entry points of facilities to thoroughly scan individuals

Through self-awareness, AI can:

- Improve biometrics used for access control management (e.g., pressure when typing, position of finger when using print scanners)
- Understand behaviors of employees (e.g., how long they review certain web pages, how they alternate between windows on the screen)
- Make decisions on how to respond to different actions taken in the environment (e.g., unauthorized access)
- Reduce the threat of Deepfake technology by thoroughly analyzing the voices of individuals to confirm their identity

The general idea here is that even though hackers and other threat actors can exploit the innovative technology of AI, it can also be used to greatly increase security measures for organizations, and, for lack of a better term, drastically change the game. AI has the potential to take security to new heights and reduce threats across the board.

PROFILES IN *Confidence*

GERNETTE WRIGHT

IT Security Officer
SCHNEIDER ELECTRIC

HEADQUARTERS: Rueil-Malmaison, France

EMPLOYEES: 130,000

REVENUE: $34.17 Billion

Gernette Wright has over 25 years of experience transforming and building cyber security and information systems. He began his career on the technical side of IT, working in various roles around systems administration, and infrastructure management, before moving into more security-focused roles serving as Senior Manager for Security Operations, VP of Information Security and most recently IT Information Security Officer. He explains, "Before I took on security-specific roles, I knew I wanted to understand more than infrastructure operations. The challenging technical aspects brought me into security, the ability to be a part of business enablement keeps me here. I've always resonated with the idea that what we are doing has a bigger purpose."

Over one year into his role as IT Security Officer for the Americas at Schneider Electric, working with the R-CISO, Gernette is responsible for maintaining enterprise-wide information security risk and privacy while upholding the necessary security to support business needs. Gernette breaks his responsibilities down into three specific areas.

The first area of responsibility is internal and external footprints – with responsibilities for areas ranging from incident management to internal security governance. This requires a business mindset to understand both what the security goals are in relation to their footprints, but also aligning those to the what the business is trying to accomplish.

The second area is vendor and customer contractual responsibilities, from the cybersecurity compliance perspective. His team looks at contract language that comes in to make sure it has the proper cybersecurity protocols and language in place. This area also brings with it some level of customer-facing responsibilities that requires interacting with customers to answer any questions on internal security programs and articulate requirements and standards as a company to ensure both parties are protected and also happy. Sometimes that means adopting languages from both parties and finding middle ground.

The third, and the main area where Gernette spends the majority of this time is around the company's M&A information security remediation activities. Gernette comments, "We often acquire companies that are young in their security journey. Part of the process includes a formal security assessment. While going through their remediation program, I try to understand what they're currently doing to see what can be adopted and/or enhanced in order to implement our set of security standards so they meet our level of security. Sometimes they have to build a program from the ground up and sometimes there is some type of program partly built and needs to be matured. I believe it's key to ensure their program is tailored to how they work but also ensure our standard framework is followed to help them mature their security program. Although the goal is meet Schneider's standards, this is their program so my approach is to lead them to a solution, never to just throw something at them and insist that it be implemented."

ADDRESSING CHALLENGES

Threat prevention, particularly ransomware, is a constant challenge for Gernette and his peers, because of the ever-evolving nature and need to constantly be up to date on the latest TTP's. He ensures he is always learning and educating himself to better protect his organization and lead security programs with confidence.

Addressing regulations is another challenge, as frameworks and policies are modified and security teams must keep up to meet compliance mandates. Gernette says, "There's a variety of privacy and security frameworks coming out with updates like CSF 2.0. As an industry it is sometimes hard to staff adequately for response to push those changes through, especially if you were already going through a gap remediation in the last version."

Security staffing is also a challenge across most organizations and Gernette believes that will continue with

particular security skillsets being harder to find, especially on the governance side. He says cybersecurity jobs revolve around risk mitigation which involves looking at data, something that is not glamorous and can be tedious, leading to burn out and the lack of interest in pursuing this line of work.

POSITIVES AND NEGATIVES OF ARTIFICIAL INTELLIGENCE

Gernette is excited about the advances in AI, he made the point that AI is not new as it has existed in various technologies for quite some time, such as chatbots, facial recognition, speech recognition, etc. He says it is the advances in large language models powering generative AI such as ChatGPT which are revolutionizing our work and personal lives. Although AI brings many innovative transformations, Gernette warns about the fast rate at which AI is entering the market and if policies and regulations can actually keep up with this. He says, "AI is going to change how we do things, and the way we function. Much like the internet, it's going to be transformative. In the context of work there will be many of positives; one area that comes to mind is staffing. There is always a need in our industry for SOC analysts, AI could help augment some of those higher skillsets needed for forensics and eyes on glass. Imagine if a Tier 1 SOC Analyst could conduct an end-to-end forensics on day #1 just by typing a contextual question into an AI backed search bar or reduce false positives. That would transform staffing and operations in the SOC. This is the type of application of AI that will benefit other areas such as vulnerability management and malware detection and prevention, among others, and improve operations in our cybersecurity space."

However, Gernette says like Newton's Third Law, everything has an equal and opposite reaction, and there are also some negative effects of AI. He comments, "As we learned during the pandemic, there was a mass rush to accommodate remote employees and because of the speed of implementation, proper considerations around security controls weren't taken. The speed that companies are adopting AI might mean businesses may forgo a thorough vetting and testing of critical controls in order to go to market sooner. As we've learned, it's hard to go back and put security in place after the fact. The companies putting AI products out there must make sure they are designing with security and privacy in mind before they go to market."

He continues, "On the cyber defense side, an area of concern is phishing. We've developed our awareness training to teach our employees to be cognizant of spelling, grammar, and email address correctness, however with AI, those emails could be written perfectly. The effectiveness of our standard AT training will become greatly reduced or obsolete; we will need to re-tool ourselves and create better ways to educate our user community. We also need to be aware of the privacy challenges with the use of AI. The US has been slow to adopt privacy regulations, but proper legislation is needed to safeguard privacy information and choices. AI systems needs lots of data for its predictive algorithm, which raises concerns about systems abilities to pull in feeds from many different places, processing, access, and storage of that information."

"I believe in mentorship, there's always someone who is smarter and more experienced than you."

LEADERSHIP STYLE & COMMUNICATION

Gernette leads with a democratic type of style, coaching his team members to achieve their goals, while including them in important discussions so they feel valued. He explains, "I involve my team as much as I can, I believe better decisions and work products are a result of joint conversations from cumulative voices and opinions. As an employee, I like to feel valued and that my work and efforts are appreciated, and putting myself in others shoes, I feel they'd want the same."

In past roles Gernette has presented to boards, something he believes must be approached with strong communication and an open mind. He comments, "I try to get to know the board before I present to them so I can understand how they digest information and what they're looking for. You don't need to be technical with boards, but there is value in showing certain metrics, so they understand what you're actually doing and represent cyber posture of the organization. I present from a business perspective to make sure the information is not falling on deaf ears. It's great if you're able to reuse an existing format and tailor that to your style, but in cases where that does not exist, one approach I've taken is use the board audit-subcommittee as a sounding board. I outline what I'm thinking and then ask them for input to fine tune, and I've found this fostered engagement and they feel invested in security. This may not work for every situation or everyone, but given the accessibility and size of the organization, it was an approach that worked well for me at that time."

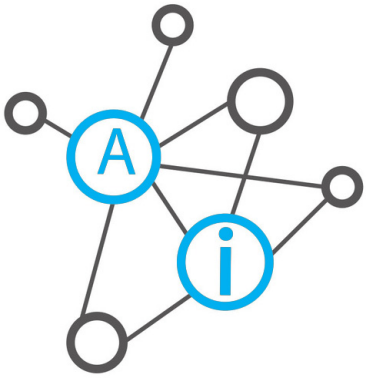
GROWING AND LEARNING

Gernette is passionate about education and the need to expose yourself to relevant information to stay up to date through upskilling. He attends industry and leadership conferences to improve his communication, hear from other leaders, and network with the larger community. Having a mentor is very important to his growth, he explains, "I believe in mentorship, there's always someone who is smarter and more experienced than you. It's important to find that person to take advantage of their experience and advice and also be a sounding board for my challenges and goals. I've had a few mentors in my career, and they have been a huge part of my growth. I believe it's important to remain teachable in everything I do, to know when to listen and when to talk, whether it's someone from a different part of the business, in a meeting with peers, work social event, etc. You'd be surprised what you learn by just observing and listening."

ChatGPT in the Workplace

Why to limit employee use, and what it means to your business

By Shreeji Patel, Senior Cybersecurity Consultant, K logix



ChatGPT, as a large language model, has shown to be an impressive tool for various tasks such as natural language processing, text generation, and language translation. However, its increasing use in various domains has raised concerns about the potential risks and challenges it may pose in terms of privacy, security, ethical, and legal considerations. This article aims to discuss these risks and concerns by providing real-world examples of such risks.

One of the primary concerns regarding ChatGPT is the potential privacy risks it poses. With the vast amount of data it processes and stores, there is a high likelihood that personal information could be exposed or misused. In addition, the model's capability to generate text based on the given input raises concerns about the protection of sensitive data such as health records, financial information, and other confidential data. OpenAI released a new version of ChatGPT which had access to a massive dataset of internet text, including social media posts, news articles, and personal blogs. The model's ability to generate coherent responses led to concerns about its potential misuse for fake news and propaganda campaigns.

Another significant risk associated with ChatGPT is the potential security risks. The model's capability to generate text based on the given input can be misused to create convincing phishing emails or social engineering attacks. By utilizing ChatGPT, threat actors are able to enhance the communication skills, which they typically lack in their phishing emails. ChatGPT creates phishing emails that possess coherence, conversational flow, and a striking similarity to genuine messages at no cost, thereby granting even the most basic cybercriminals the ability to heighten the effectiveness of their social engineering attacks. If these generated messages are sent to unsuspecting users, they could be used to steal sensitive information, compromise systems, or infect devices with malware.

Phishing emails or social engineering attacks are examples of how ChatGPT poses an external threat. However, ChatGPT can also poses an internal threat. Samsung's semiconductor division allowed its engineers to use ChatGPT to check source code. However, the events that followed were appalling. According to Economist Korea, three Samsung employees accidentally revealed Samsung's sensitive corporate data, potentially giving OpenAI and its competitors insights about its technology. Firstly, an employee discovered a bug in the source code of the download program for the semiconductor plant measurement database and requested ChatGPT's help to resolve the issue. Secondly, another employee used ChatGPT to enhance the test sequence for a program that identifies yield and faulty chips. Lastly, an employee recorded an internal company meeting on their smartphone, transcribed it with a speech recognition application, and utilized ChatGPT to generate meeting minutes. All three of these individuals are currently under

investigation for disciplinary action. This example highlights the security concerns in utilizing ChatGPT and importance of implementing robust security protocols to protect the sensitive data used by ChatGPT.

Another significant concern associated with ChatGPT is the ethical and legal considerations regarding the potential misuse of the model. The model's capability to generate realistic human-like responses raises ethical concerns about its potential use in deepfake technology, disinformation campaigns, and other malicious activities. The model's training data could potentially contain biases that could be reflected in the generated output. This could lead to unfair and discriminatory outcomes, particularly in sensitive domains such as hiring or legal proceedings. Additionally, there are also legal liability risks associated to by utilizing ChatGPT. The model is capable of generating content, including text, images, and videos, which can be used for a variety of purposes. However, if the generated content violates copyright laws or infringes on someone's intellectual property rights, the user of ChatGPT could be held legally liable.

Although ChatGPT has shown significant potential in various domains, its increasing use raises concerns about the potential risks and challenges it may pose. Here are five best practices for organizations to consider while allowing its employees to use ChatGPT:

1. **Establish clear guidelines by defining Acceptable Use:** Organizations should establish clear guidelines for the use of ChatGPT to ensure that employees understand what is and is not appropriate use. This can include guidelines around language, confidentiality, and data security.

2. **Provide training and support:** Employees should be trained on how to effectively use ChatGPT and given ongoing support to ensure they are using the tool in the most productive and efficient way. This can include training on how to ask effective questions, how to interpret responses, and how to verify information.

3. **Monitor usage:** Organizations should monitor usage of ChatGPT to ensure that it is being used appropriately and that employees are not engaging in inappropriate behavior. This can include monitoring for offensive language, inappropriate content, and misuse of data.

4. **Protect data privacy:** Organizations should take steps to protect the privacy and security of data being used in ChatGPT. This can include using secure communication channels, limiting access to sensitive data, and ensuring that data is only used for authorized purposes. Additionally, identify which data tiers can be authorized to insert into ChatGPT.

5. **Continuously evaluate and update policies:** Organizations should continuously evaluate and update the guidelines for ChatGPT usage. This can help ensure that the policies remain relevant and effective in meeting the organization's security standards and addressing any emerging issues or concerns.

In conclusion, ChatGPT can be a powerful tool for organizations to enhance communication, productivity, and innovation. However, organizations must also consider the potential risks and challenges that come with using such a tool. Data privacy, security, legal liability, and bias are some of the key areas of concern that organizations need to be considered when allowing its employees to use ChatGPT. Additionally, organizations must implement the best practices outlined above to ensure ChatGPT is being utilized safely by its employees.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM

ARTIFICIAL INTELLIGENCE: FRIEND OR FOE?

FEATS OF STRENGTH
JUNE 2023