onsecurity

Understanding AI's impact on the cybersecurity landscape

Integrating, Automating & Innovation

CURRENT STATE OF AFFAIRS

2024 has marked a monumental degree of change, progression, and emerging challenges for the information technology sector.

One of the most poignant cybersecurity trends of the year centralised around the rise of cyber-inequity in lieu of progressive technology, with many small to medium sized businesses (SMB's) struggling to recover from critical cybersecurity breaches due to a lack of correct preventative measures.

Identified in the World Economic Forum's global security outlook, reports showed a clear differentiation between businesses with strong cybersecurity measures and those without.

These findings, interestingly, made evident a correlation between the size and data security, suggesting that SMB's invest less overall in their cybersecurity measures and therefore suffer more significantly from data breaches and attacks than their large enterprise counterparts.

onsecurity

Not only this, but heightened third party and supply chain risks became a focal point for the year, following a reported increase in third party data breaches. Further research uncovered that digital risks and supplier fraud were attributed to be major factors contributing to the supply chain risks faced by businesses, posing a stern reminder to IT professionals to remain vigilant of their entire cybersecurity ecosystem.

DATA BREACHES

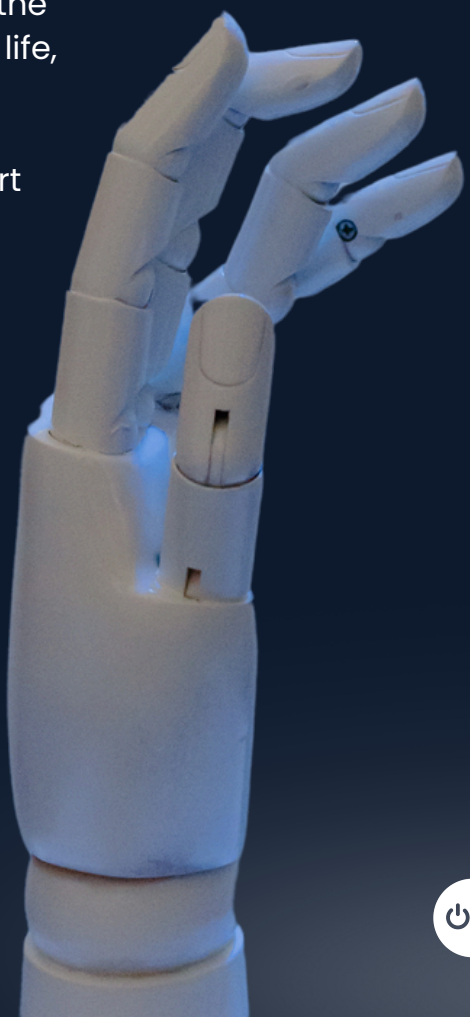
Data breaches were similarly reputable in 2024 due to their prolific likelihood, following advancements in both technological and cybercriminal intelligence. The World Economic Forum (Source: Global Security Outlook, World Economic Forum) emphasised the unrelenting risk of data breaches for businesses of any scale, with data breaches attributed as one of the greatest threats to any business in the digital age. The surmounting threat of data leak in turn added regulatory pressures for information technology professionals.

The EU's Cyber Resilience Act, and planned implementation of DORA for the EU fintech industry, are just some of the many newly enforceable regulatory guidelines introduced to minimise the risk of compromise. . While these new preventative measures may seem a bother, enforcement of their frameworks could inevitably save thousands of businesses from breaches,costly remediation efforts, and large legal fees- an optimistic note for many information security professionals.

Much of the industry's focus for 2024, however, has manifested itself in the emergence of publicly accessible AI technologies, and their interplay with existing understandings of artificial intelligence and machine learning. The immense capacity of AI technology has already opened doors of possibility for industry professionals regarding automation, yet how to best adopt artificial intelligence for the IT sector remains largely speculative.

One thing for certain can be taken from the current state of affairs in the technology sector: good cybersecurity posture is more critical than ever. The constant threat of data breaches by malicious actors looms over businesses of all sizes, while AI implementation for workplace automation gains wider acceptance. The contemporary digital landscape presents both unprecedented potential and significant risk for businesses of any size.

To shed light on an increasingly relevant topic, this comprehensive report will investigate the integration of AI technology with everyday life, and how automation interplays with information security. Utilising existing information on AI, as well as industry-expert knowledge, this paper hopes to offer best practices for AI implementation, including what to be cautious about, and how to navigate AI securely.



HOW IS AI AUTOMATING EVERYDAY LIVES?

Emerging technology, particularly surrounding AI, is automating human life constantly. We're all familiar with voice assistants, like Apple's Siri, or Amazon's Alexa. These technologies utilise artificial intelligence to instantly provide results for whatever query you might have, using chat transformers to turn this information into a conversational answer. Streaming services like Netflix optimise AI to give you tailored movie recommendations based on your previous watching habits, and many e-commerce stores now implement AI chatbots to assist you with any queries you may have. Whether we realise it or not, AI is already all around us, and being integrated constantly to enhance our digital experiences.

AI isn't just improving upon the novel things in life, however. In fact, in the past few years AI technology has been broadly adopted by enterprise businesses of all different sectors, whether it be to improve the quality of communications, introduce customer service chatbots, or analyse data trends.. Within every business, irrespective of the sector, AI will interplay closely with IT operations and procedures. While IT focuses on using technology to process information, AI aims to enhance technology to be more intelligent and time-efficient, saving businesses the hassle of outdated manual procedures.

AI AND SECURITY

The adoption of AI technology into the IT sector has been a topic of great contemplation for many professionals. AI can effortlessly automate tasks through pattern recognition algorithms, offering numerous benefits surrounding the maintenance of good cybersecurity for businesses without the often time consuming inclusion of third party tools.

A key example is AI's frequent implementation into incident response plans. With a wealth of AI tools and third-party plugins available from Open AI's ChatGPT to Google's AI Bard, businesses have no shortage of options when selecting which AI tool will best suit their security goals. Using network traffic information, threat intelligence feeds, and security event logs, these AI plugins can analyse patterns and sift through huge amounts of data to identify indicators of compromise, unauthorised access attempts, or behavioural irregularities.

What's more, AI can also automate incident responses and generate a report based off of these findings, accelerating alert investigations by an average of 55% (Source: IBM, AI Cybersecurity). This expedited investigation process in turn means faster remediation and, relievingly, less damage done by malicious hackers.

onsecurity

AI, due to its efficiency and ability to perform several manual tasks in an automated manner, is also relatively economical and an accessible option for many SMB's. Recent reports of cyber-inequity have stirred conversation surrounding affordable cybersecurity for small businesses, and, in many cases, AI offers a budget-conscious solution for many. AI has also drastically reduced the risk of human error in cybersecurity, with its ability to learn information and enact it swiftly unparalleled by even some of the best computer scientists. The introduction of AI to the IT sector has certainly caused a great deal of progression and optimised cybersecurity practices for many, but as professionals how much can we actually rely on AI to identify and remediate constantly evolving risks?

This is the concern shadowing the widespread adoption of AI technology, and a question that cannot be objectively answered due to how rapidly AI is progressing. While AI has the potential to completely transform cybersecurity practices for the better, it is important to remember that even AI itself needs security measures, and introducing it on a wide scale naturally comes with as much risk as reward. There are limitations to AI's ability surrounding the identification of risks that only the nuance of professional human logic can aptly tackle, with a fundamental flaw in AI technology pertaining to the incorrect flagging of benign issues as "threats". However, by using artificial intelligence technology to supplement an existing human cybersecurity team instead of replacing it, businesses can reap huge benefits from all it has to offer, while minimising the risk of false positives and possible complications.

USING AI BEST PRACTICES

The risks of AI usage shouldn't dissuade you from exploring such an exciting piece of technology, but you should certainly educate yourself on best practices before adopting its use, particularly in a business setting. With informed application and correct education, AI can benefit your business significantly, optimising operational procedures and improving security practices.

1. Our foundational advice for anyone considering AI implementation would be to start by outlining your limitations, and how AI can optimise your workflow to overcome these. It could be that you introduce an automated scanner for vulnerabilities, or a customer chatbot. Remember to keep it measurable: anything you cannot track or maintain regularly could do more harm than good.

2. Before any launch of AI, assuring excellent data management and using high-quality data is utmost important. Due to AI's constantly progressing condition, poor data management is an all-too-easy way for malicious hackers to breach your business. Analyse your organisational data and run regular maintenance to ensure the AI has everything it needs to work efficiently, without leaking any personal information.

3. On the same note, check any AI-generated code to ensure it is reliable. Testing it to ensure it meets the criteria is always a good way to overcome this!

4. While it's tempting to just copy and paste all the details you might need when working with AI, be incredibly apprehensive of inputting sensitive information into any software. Additionally, you should treat any outputted information with a degree of caution. AI is generally accurate in its output, but many chat-transformers have been known to fabricate information or misunderstand user's requests.

5. Train and educate employees on AI usage and, similarly, the ways in which it can be maliciously used against your business. Demonstrate to team members AI-generated content and the security threats it can pose if misutilised, and take time to cover responsible AI usage for the protection of sensitive information.

AI PREDICTIONS FROM ONSECURITY'S VP OF ENGINEERING:

Mike Oram, VP of Engineering at OnSecurity, believes that AI integration into cybersecurity is still in its early stages. With his extensive experience in cybersecurity and risk management, Mike has witnessed significant evolution in the industry over the years. However, he notes that the pace of development is accelerating as both technology and cyber threats become more sophisticated.

"AI has already begun revolutionising the cybersecurity landscape, but will undoubtedly continue to do so for years to come. As threats become increasingly common and more sophisticated, AI's ability to process vast amounts of data and identify patterns will be invaluable. It won't be long before AI-powered systems can autonomously detect and respond to threats in real-time.

Beyond detection, AI will also enable predictive analytics, allowing us to anticipate emerging threats and proactively mitigate risks. OnSecurity is already using AI to automate routine tasks, freeing up our security professionals to focus on more strategic and complex challenges. While AI will undoubtedly enhance our capabilities, it's essential to remember that it's a tool, not a replacement for human expertise. The future of cybersecurity will be defined by a symbiotic relationship between AI and humans."

Mike Oram, VP of Engineering at OnSecurity

onsecurity


onsecurity