The Evolution of Cyber-Resilience: Navigating the Impact of AI on Firms

18 January 2024

Introduction

The contours of our digital landscape are undergoing profound shifts, with artificial intelligence (AI) requiring businesses to embrace a new technological era. Businesses are not just embracing AI for innovation, they are also grappling with the imperative to fortify cyber-resilience. This article explores the mid- and long-term implications of AI on firms' cyber-resilience postures, considering the challenges, opportunities, and strategic imperatives that business leaders must consider.

The Current Landscape: A World in Transition

As organisations race to adopt new technologies, the World Economic Forum's Global Cybersecurity Outlook 2024 provides a snapshot of the prevailing sentiments. The adoption of generative AI, a subset of artificial intelligence, raises concerns among executives. The majority believe that, in the next two years, generative AI will favour attackers over defenders. This apprehension is grounded in the perceived advancement of adversarial capabilities, with phishing, malware development, and deep fakes topping the list of concerns. There is a counter-balance to this viewpoint with some declaring AI the best defence against cyber-attacks.

Geopolitical and Technological Transitions

Beyond cybersecurity, AI's influence extends to geopolitics, as evidenced by the potential risks it poses in areas like misinformation and election security. These types of concerns support the heightening of AI concerns. While generative AI adds complexity to cyber threats, it is not the sole concern. The past five years have seen a doubling of malware infiltrations globally, reflecting the dynamic nature of cybercriminal activity amid geopolitical tensions.

The Rise of Large Language Models and Generative AI

The 2024 Global Cyber Outlook findings indicate a swift response from organisations to mitigate emerging risks associated with adopting new technologies. Large language models (LLMs) and generative AI have surged in prominence over the past year, with the cybersecurity sector being a notable beneficiary. Despite the fervour surrounding generative AI, the spectre of quantum technologies looms in the background, showcasing the perpetual need to address evolving threats.

© 2024 AI & Partners B.V.. All Rights Reserved

Continued Influence of Automation and Machine Learning

In 2022, industry leaders anticipated that automation and machine learning would significantly impact cybersecurity. Fast forward two years, and generative AI takes centre stage as the technology with the most substantial influence on cybersecurity. Industries such as cybersecurity, agriculture, banking, and insurance see generative AI as a pivotal force shaping their cyber-defence strategies.

The Dual Nature of Generative AI: Balancing Act of Cybersecurity

Generative AI is a transformative force, not only bolstering cybersecurity defences but also posing risks as a tool in the hands of cybercriminals. As with most technological advances, bad actors are finding a way to exploit for their gain. In general, these attack types are the same but amplified through the power of AI. For example, cybercriminals leverage generative AI chatbots to create sophisticated phishing emails and custom malware that is self-evolving, lowering the bar for executing complex and convincing campaigns Furthermore, AI enables these bad actors to target victims with highly personalised and unique attacks at scale. This necessitates a need for firms to be proactive.

Dark Web Trends and AI Misuse

The dark web's proliferation of discussions around generative AI in 2023 underscores its appeal to malicious actors. Hackers boasting about utilising ChatGPT and recreating malware strains signal a concerning trend. The threat landscape expands as generative AI assists in developing self-evolving malware, demonstrating the need for a proactive cybersecurity approach.

A Global Commitment: Government Action

At the time of writing the World Economic Forum’s Annual meeting is taking place in Davos and this year is dominated by AI. Business leaders are gaining an understanding on adopting AI and managing the associated risks.

This builds on recent AI developments by governments around the globe:

United Kingdom: Acknowledging the multifaceted concerns surrounding AI's impact on cybersecurity, the AI Safety Summit stands as a diplomatic breakthrough. UK Prime Minister Rishi Sunak's endorsement of the Bletchley Agreement reflects a commitment to address the risks posed by AI. The summit, coupled with the 'Capabilities and Risks from Frontier AI' paper, signals a global recognition of the need to navigate the challenges and opportunities presented by AI.

United States: The US Government’s Department for Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) unveiled an AI roadmap for cybersecurity. Covering:

- Using AI responsibly to support CISA’s missions
- Assessing and assuring AI systems
- Protecting critical infrastructure from malicious AI use
- Collaborating and communicating on key AI efforts
- Expanding AI expertise in the workforce
- Emphasising safe and ethical use of AI.

© 2024 AI & Partners B.V.. All Rights Reserved

European Union: Starting with the foundation of GDPR regulations, the European Union has demonstrated a commitment to values in shaping new technologies. The General Data Protection Regulation, implemented on May 25, 2018, marked a significant stride in building trust, a cornerstone for the enduring relationship between people and companies. The EU's sustainable approach to technologies provides a competitive edge by embracing change aligned with the Union's values.

As transformative technologies like AI emerge, ethical and legal considerations come to the forefront, including issues related to liability and potential biases in decision-making. The EU recognises the necessity to ensure the development and application of AI within an appropriate framework that fosters innovation while upholding the Union's values, fundamental rights, and ethical principles such as accountability and transparency.

With GDPR as the foundation, the EU has positioned itself as a global leader in addressing the ethical dimensions of AI. The recently introduced EU AI Act signifies a pivotal moment, ushering in sweeping changes. This comprehensive and mandatory regulatory framework holds the potential to impact numerous businesses within the EU or those established in third countries where AI systems operate within the EU. As part of this framework, businesses leveraging AI are required to conduct assessments to determine the risk category of their systems, with varying obligations based on the level of risk. From banning unacceptable risks to imposing strict requirements on high-risk systems and transparency measures for lower-risk ones, the EU's proposed five-tiered risk framework aims to establish proportionate regulations for AI providers and users.

In essence, the EU, having laid the foundation with GDPR and now advancing with the EU AI Act, is well-positioned to lead the global discourse on the ethical governance of AI.

AI Skills and Cybersecurity: Bridging the Gap

As organisations adopt AI to bolster their cyber defences, the need for a skilled workforce proficient in both cybersecurity and AI becomes paramount.

The Challenge of the AI-Cybersecurity Skills Gap

The rapid integration of AI into cybersecurity strategies unveils a gap in skills within the workforce. Traditional cybersecurity professionals may find themselves grappling with the intricacies of AI-powered threats, necessitating a bridge between cybersecurity proficiency and AI skill sets. The evolving threat landscape demands not only a comprehensive understanding of traditional cyber threats but also the ability to navigate the complexities introduced by AI. These are additional challenges which build on the well documented global cybersecurity talent shortages.

To address this, organizations can analyse the skills gap, implement AI-focused training, encourage collaboration, recruit AI-savvy professionals, and foster continuous learning.

Then to advance the agenda organisations can leverage the pivotal role of AI in powering personalised training platforms, simulations, and automated threat detection, contributing to enhanced cybersecurity skills.

AI in the Cybersecurity Cycle: A Strategic Overview

Cybersecurity is a corporate strategic issue and not just an IT problem. Therefore, we must consider the impact of AI across the cybersecurity cycle of Govern, Prepare, Manage and Follow-up:

© 2024 AI & Partners B.V.. All Rights Reserved

Govern

As organisations face stiffer cybersecurity requirements, AI emerges as a potent ally to help organisations in their quest for enhanced cyber resilience.

Firstly, AI can augment cybersecurity team's analysis and recommendations. This is critical to breaking the Board (Business Leadership) v CISO (security teams) gap in understanding, and helps to provide improved Organisational Context (commitment, strategy, awareness), Oversight and inform a fit for purpose Risk Management Strategy.

Secondly, AI has the potential to contribute to the assessment, management and control of Cybersecurity Supply Chain intricacies. A growing area of cybersecurity concern given the number of supply chain breaches.

Thirdly, AI can be utilised to assess controls around key cyber security artefacts and help to identify strengths and gaps.

Finally, AI can bolster an organisations threat intelligence, whether from an industry, application or jurisdiction perspective. AI will support with up to date insight and information as well as prioritisation of the threats against an organisations level of risk

Verdict: Underutilised, with a growing need for action. Expect greater adoption in the near term.

Prepare

Cyber risk management has lagged behind other digital transformations, leaving many companies uncertain about how to identify and manage digital risks, resulting in latent untapped potential.

Firstly, an organisations Assets & Data is a critical area for them to understand as part of their Cyber Incident Response Plan. AI is able to offer complete, accurate inventories of devices, applications and users. This is valuable in identifying the high-risk assets and then supporting the tailored treatment of those assts.

Secondly, expanding upon the previous point about identifying Data and Assets, AI-driven systems have the capability to anticipate potential breach points, allowing strategic allocation of resources and tools to vulnerable areas. This is in addition to AI automating certain incident response activities such as vulnerability scanning and patch management. Utilising prescriptive insights from AI analysis enables the optimisation and enhancement of controls and processes, ultimately bolstering an organisation's cyber resilience.

Thirdly, A pivotal arena where AI can make substantial contributions is in streamlining cybersecurity training and awareness initiatives across organisations. Recognised as the linchpin of cyber defence, effective training becomes even more formidable when augmented by AI-driven tools, offering personalised and targeted learning experiences.

Finally, AI's capabilities can be harnessed for testing and simulation, ensuring organisations are well-prepared to face evolving cyber threats.

Verdict: Growing area of influence. In the mid-term expect the introduction of solutions to play catch up to other digital transformation, while areas such as Identity Access Management (IAM) leverage AI to improve security. Cybersecurity Education will lead the way.

© 2024 AI & Partners B.V.. All Rights Reserved

Manage

The Manage phase is more than just the Technical response to a cyber incident. This considers, Instant-set up (effectively knowing and instigating the playbook), Technical Response and the often-over-looked Management Coordination.

Firstly, it is in Technical Response where we witness the current zenith of AI's impact of handling cybersecurity incidents:

This is most notable in the Identification phase where AI enables analysts to sift through the noise of alerts and detect attacks more efficiently. The analysis of diverse datasets enables the creation of a deep understanding of normal activity, facilitating proactive threat hunting. Moreover, AI reinforces the Zero-Trust model by triggering user access revocation upon detecting suspicious behaviour. Solutions such as Security Operations Centre (SOC) are increasingly becoming AI powered. This should be seen as augmenting capability with the need for human supervision remaining.

This influence extends to containment efforts, showcasing the potential for AI to autonomously respond to emerging threats.

Cautionary Tale: Though Technical Response is a bright area for cybersecurity, we have to note the following:

1. Uncontrolled use of generative AI query's within organisations is potentially harvesting a treasure trove of information for bad actors to utilise against / target particular organisations
2. As generative AI develops we will better understand bad-actors ability to leverage and scale for misuses

Secondly, the Management Coordination activities are generally underserved, but companies are beginning to offer solutions to produce notification information, and track incidents which will better serve this space

Verdict: In the medium to long term, AI's impact is set to rise, with dynamic and automated threat identification reaching its pinnacle. As AI matures, expect a growing impact on the efficacy of remaining technical elements, including containment, eradication, and recovery.

Follow-up

There are pockets of AI being utilised in this phase.

Firstly, Lessons Learned are being automated, with the creation of incident response reports, and advanced solutions are converting raw data from recent attacks into threat intelligence. This activity supports a closed-feedback loop upstream in the cybersecurity cycle, which along with human augmentation is accelerating cyber responses.

Secondly, there a number of emerging tools which can be utilised to better identify, prioritise, track and resource cybersecurity improvement programmes. This will lead to organisations generating better results from cybersecurity investment and tackle the 'effectiveness' problem of cybersecurity investments.

Verdict: Opportunity for organisations to leverage AI powered technologies to improve their overall cyber investments and effectiveness.

© 2024 AI & Partners B.V.. All Rights Reserved

Strategic Imperatives for Business Leaders

As businesses grapple with the transformative influence of AI on cyber-resilience, a roadmap emerges for business leaders to navigate this dynamic landscape. The following strategic imperatives provide a set of actions to take now:

Understand the risks for your business: Conduct a Holistic Cybersecurity Assessment

Conducting a comprehensive cybersecurity assessment tailored to your organisation is essential. Break down barriers between the board and cybersecurity experts with an accelerated assessment in the language of the board. Ensure coverage across the entire cybersecurity cycle, addressing both management and technical aspects for effective risk management. A narrow approach is simply ineffective.

Prepare your business: Create & Maintain a Cybersecurity Incident Response Plan

Cyberattacks are inevitable (when not if), and regulators are introducing stricter accountability and penalties, meaning proactive preparation is crucial. Develop and maintain a business-led Cybersecurity Incident Response Plan (CIRP) covering both management and technical aspects. Meeting regulatory requirements and minimising financial, reputational, and operational impacts ultimately strengthening your bottom line.

Prepare for the EU AI Act: Understand the Impact on operating in the EU

Anticipate sweeping changes introduced by the EU AI Act. Businesses must understand the comprehensive and mandatory regime's potential impact. Assessing the risk category of AI systems and complying with transparency requirements will be essential. As the EU leads the global debate on AI ethics and regulation, businesses must align with the Union's values and fundamental rights.

Bridging the AI-cybersecurity skills gap: Conduct a Cybersecurity Skills Gap Analysis

Addressing the skills gap requires a holistic approach. Perform a cybersecurity skills gap analysis to pinpoint specific gaps in workforce proficiency concerning AI and cybersecurity integration. This analysis enables strategic investment in tailored training programmes, ensuring cybersecurity professionals possess essential skills to combat AI-powered threats.

Optimise your investments in cybersecurity: Review Your Cybersecurity Investments

Reviewing cybersecurity investments goes beyond financial considerations. Align resources with evolving risks, technology, and critically your organisation's cyber risk appetite. Optimise spending to achieve goals effectively and combat the evolving cybersecurity threat landscape.

Conclusion: Navigating the AI-Cybersecurity Landscape

Organisations find themselves at a critical juncture, with the transformative potential of AI offering unprecedented opportunities, yet demanding a vigilant and proactive approach. AI will undoubtedly contribute to enhancing an organisation's cybersecurity resilience; however, it cannot eliminate the operational and technical intricacies inherent in cybersecurity. As businesses traverse the intricate landscape of AI's mid- and long-term implications on cyber-resilience, the strategic imperatives outlined here serve as a compass. By embracing these imperatives, business leaders can not only navigate the challenges but also harness the full potential of AI in securing the digital future.

© 2024 AI & Partners B.V.. All Rights Reserved

About Temple Avenue Group: Temple Avenue Group is a professional services firm that specialises in Transformation Consulting & Training for service companies, your trusted partner in bolstering your cybersecurity defences. Take proactive steps to secure your organisation with our comprehensive cybersecurity consultancy offerings:

1. Assess - CRC360 Accelerated Cybersecurity Assessment: Gain an independent & accelerated assessment of your cyber resilience. A structured approach, providing informative insight, with a clear plan for action.
2. Prepare - Cyber Incident Response Planning: Development of your organisations Cyber Incident Response Plan (CIRP), helping you to prepare, manage and follow-up post incidents.
3. Manage – Coordinated Cyber Management Response: Incident Management tailored to your needs. Efficiently navigate and mitigate cybersecurity incidents under the expert guidance of Temple Avenue Group.
4. Improve – Cyber Programme Delivery: Drive the successful implementation of your cyber improvement programme. Let us assess the market to optimise your investments, ensuring maximum impact on your cybersecurity measures.

Get in touch with Temple Avenue Group:

Email: Consult@templeavenuegroup.com

Empower your organisation to thrive in the digital landscape with Temple Avenue Group's tailored cybersecurity expertise. Act now to fortify your defences and stay ahead of evolving cyber threats.

© 2024 AI & Partners B.V.. All Rights Reserved

AI & Partners

Amsterdam - London - Singapore

About **AI & Partners**:

Your trusted advisor for EU AI Act Compliance. Unlock the full potential of artificial intelligence while ensuring compliance with the EU AI Act by partnering with AI & Partners, a leading professional services firm. We specialize in providing comprehensive and tailored solutions for companies' subject to the EU AI Act, guiding them through the intricacies of regulatory requirements and enabling responsible and accountable AI practices. At AI & Partners, we understand the challenges and opportunities that the EU AI Act presents for organizations leveraging AI technologies. Our team of seasoned experts combines in-depth knowledge of AI systems, regulatory frameworks, and industry specific requirements to deliver strategic guidance and practical solutions that align with your business objectives.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

© 2024 AI & Partners B.V.. All Rights Reserved