Business

Unleashing humans and AI in the battle against new and current threats

Authored by:
Jan Aril Sigvartsen and **Stefan Månsby**
Senior Executive Advisors, Orange Business

May 2024

orange™ Business

Introduction

In the same way that the internet revolutionised the distribution of information, Artificial Intelligence (AI) is revolutionising human efficiency and precision at an unprecedented scale.

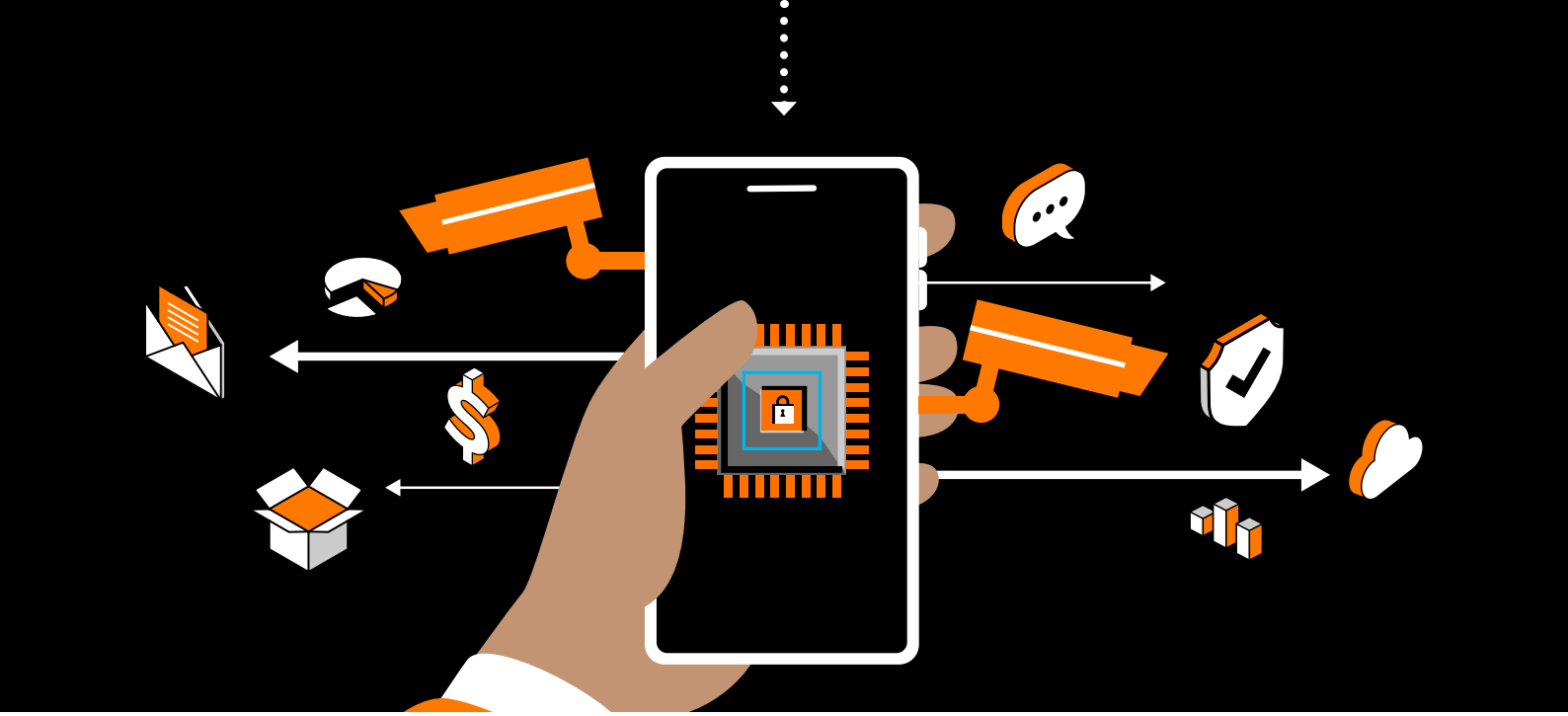
It's a transformation as significant and as pervasive as the internet's reshaping of communication and information access back in the day.

What's fascinating – and crucial to understand – is that AI is no longer simply enigmatic, over-hyped technology jargon. It's becoming an ingrained, assumed feature of everything we engineer or use. It's in the fabric of our daily lives, subtly yet significantly enhancing our capabilities and behaviours.

However, with great power comes great responsibility. While AI may be a powerful tool, capable of elevating human dignity by making us more efficient and precise, it also harbours the potential for misuse.

Why? Today, AI services are not just specialised tools for an elite with buying power: these services have become globally available, affordable, and simple enough for virtually anyone to use. Now, almost any person with a browser – whether an 8-year-old child or an accomplished engineer – can do what only hooded, tech-savvy talents in hacker groups could do in the past. This ubiquity of AI is giving superpowers to every human being on the planet: however, we will become victims of our own efficiency unless we can demonstrate innovation in our cybersecurity strategy equal to that taking place in the world around us.

How did we get to this point? AI algorithms have been around since 1995, but the advancement and widespread availability of hyper-scalable cloud computing have dramatically accelerated the growth and affordability of AI technologies. Coupled with highly user-friendly interfaces, these developments have led to a significant paradigm shift in various sectors, fundamentally altering the landscape and expectations across industries - including cyber security - due to the current state of AI. We can now leverage practically unlimited compute power – for good or bad - a concept that seemed like science fiction only a few years ago.



What this means in practical terms is that AI applications are now capable of doing anything that can be described through algorithms, something which takes us beyond serialization or ransomware attacks.

AI-enabled cybersecurity threats aim not merely at theft or extortion but to act as a puppet master that seeks to manipulate us all. In this scenario, paralysing attacks simultaneously targeting hundreds of different locations within a business could end up shaping how employees behave, take decisions and what they believe to be the 'truth'.

The dark side of AI's coexistence with 'everything else'

Unlike application refactoring, business operating model transformation, or reshaping your integration landscape, using AI does not require you to upgrade anything – it is possible simply to tap into any value it may provide without modifying any of your technology, people, or processes.

However, at least 20% of any company's assets – consisting of technology, processes, and people – are defined as 'toxic': these are virtually impossible to upgrade unless you have access to almost unlimited resources. These can be a mix of integrations, applications, contracts and skillsets and your business processes may continue to work well – in fact, you may be a market leader - even if as many as 90% of your assets may be considered toxic.

Nevertheless, this is double-edged sword. Not only is AI supercharging an attacker's ability to exploit any current vulnerabilities, the introduction of AI-enabled support within businesses is also increasing new attack scenarios by an order of magnitude – this is the introduction of AI by 'the back door' and is therefore likely to be flying under your radar. So, whether you use AI in your organization – and no matter what your official digital or security stance on AI capabilities may be – any business will be vulnerable to both edges of the sword.

An additional and very significant concern relates to the volatile geo-political situation which gives any motivated individual the ability to use AI against you – in parallel or one step at a time: they may try to influence your decisions and behaviour based on what seems to be coming from your own data-driven insights, business processes, the recommendations of trusted advisors or the outputs from your own digital systems.

It's possible that dashboards may be altered, the security department may have changed something in your automated or non-automated compliance checks, or your own code repository may automatically introduce new, tailored vulnerabilities in your application portfolio. Or it could be that your project department may be staffed by biased individuals, or your procurement people may leave the door open to partners with a malicious, manipulative agenda.

Many companies now inadvertently become embroiled in a geopolitical war simply by doing what they have always done: providing their services and being present in certain regions. To emphasise: the bad actors participating in these geopolitical conflicts go beyond theft or extortion and aim at controlling human behaviour – something that must not only influence your approach to value creation but ultimately how you define your processes and technology landscape.

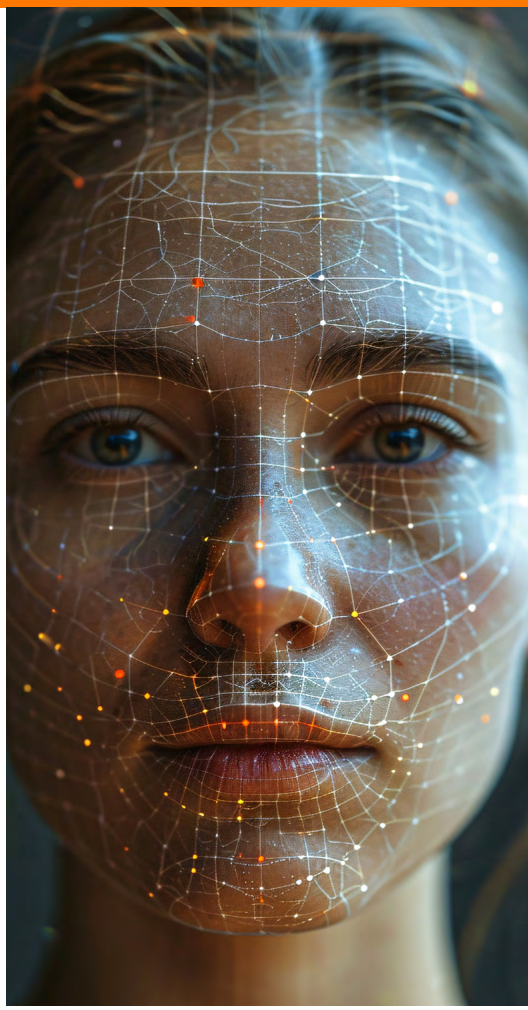
This presents a critical challenge for any business, any department, and any individual. It's not just about adopting AI; it's about understanding its implications upon the whole operating model – within and across any function, department, or division; then integrating it responsibly – and being acutely aware of the new vulnerabilities it introduces.

The looming dominance of AI may be hard to face for many individuals due to sentiment, outdated truths, or current identities; but, irrespective of your maturity level with AI or your opinions of it, the future is already on your doorstep.

Business

Recognizing and protecting against emerging threats

The continuous maturing of AI has brought to light a new breed of vulnerabilities that go far beyond traditional IT cybersecurity principles, and which target every individual and department in the organization.



Additionally, as most people are already digital cyborgs continuously hooked into cyberspace in their personal life, these attacks expand beyond individuals 'at work' to target employees on a 24/7 basis.

These threats represent new realities and scenarios that demand immediate attention and action. So, let's dissect these vulnerabilities and discuss how we might protect against potential AI exploits.

Deepfakes

AI's ability to create hyper-realistic video and audio recordings poses a significant threat. Imagine an AI impersonating not just a CEO or a public figure, but absolutely any individual, in order to disseminate false information or manipulate behaviour. This is not about creating videos of actors or politicians saying unheard of things or behaving absurdly, but changing one word, once sentence or making a small adjustment in behaviour to influence insights, recommendations, decisions, and other behaviours – one unnoticed step at a time.

To combat this, we need to consider a multi-faceted approach such as raising awareness about deepfakes, utilizing AI content detection tools, employing digital watermarking, and bolstering security with biometric authentication.

Phishing attacks

An AI-enabled attacker can craft highly personalised and convincing phishing content, mimicking the communication style and narrative of trusted contacts, colleagues, family members and friends. Protection against this sophisticated form of deception requires advanced email filtering, updated and regular security training that keeps pace with emerging trends, and implementation of multi-factor authentication principles to reduce the risk of breach.

Data and model poisoning

In the context of using AI positively to increase efficiency and precision, its reliance on data is its Achilles' heel. Manipulated data can skew the output of these algorithms, leading to malfunction or behaviour modification according to an attacker's design and intent. To shield against this, organizations should rigorously validate and cleanse data, restrict access to AI training datasets and maintain vigilant monitoring of model behaviour.

Manipulation of recommendations and decision making

There's a risk that AI could be used to create biased or manipulated datasets, leading to flawed business insights or swaying human decision-making. To safeguard against this, transparency in AI decision-making processes is crucial: organisations must implement robust data analysis protocols and, importantly, maintain human oversight – especially in the absence of AI governance.

You should strongly consider implementing more advanced AI governance functions and an approach based on continuous improvement that reverse engineers AI-supported decisions, recommendations, and influence. This should include model explainability and transparency, establishing human accountability and responsibility, and ensuring regulatory compliance is expanded to include alignment with your own tailored ethics and standards.

Intriguing and malicious content generation

The capability of an AI-enabled attacker to generate spam, fake reviews, fake messages, and fraudulent documents poses a threat to business reputation and integrity. Countermeasures could include deploying AI content detection systems, establishing rigorous content verification processes, and upholding legal measures against fraud.

Supercharged AI-powered hacking

In the wrong hands, AI can help an attacker to research, identify and exploit vulnerabilities at an unprecedented scale and efficiency by simultaneously launching multi-dimensional attacks targeting hundreds of business processes, individuals or digital assets and integrations.

To defend against this, organisations should consider employing AI-driven security systems for threat detection and automating continuous security audits and checks. They should also conduct red team/ blue team exercises using AI tools and rigorously apply the latest security patches.

Avoiding the creation of toxic assets and technology debt is now more crucial than ever to avoid infections and breaches by those with malicious agendas.

Automated social engineering

AI can enable an attacker to engage in highly personalised social engineering attacks based on data harvested from various sources.

When combined with other exploits, this can be a formidable attack vector. Counterstrategies might include enhanced employee training, deploying behavioural analytics to detect unusual patterns, and advocating for minimal personal data sharing online.

However, understanding these vulnerabilities is just the starting point. We must also recognise more specific activities an AI-enabled attacker might perform. AI-powered password cracking, automated exploit code generation, model poisoning, and data fabrication should be squarely on our radar. These are not just tools to disrupt business operations; they can be leveraged for financial gain or geopolitical manoeuvring.

In essence, our approach to security must evolve in tandem with the deep integration of AI into our organizational fabric. It's not just about building higher walls; it's about fundamentally rethinking how those walls are constructed, monitored, and maintained. This requires a blend of technological acumen, strategic foresight, and an unwavering commitment to ethical practices.

The future of cybersecurity in an AI-dominated world is not merely a technological challenge; it's a test of our collective ability to adapt, innovate, and ethically navigate this new digital frontier, one which should make your cybersecurity strategy as innovative as your – or any attacker's – innovation strategy.

Cybersecurity risks tailored by business departments and functions

In an era where old vulnerabilities can be exploited with superpowers and new vulnerabilities rise with the maturity of AI, it's imperative for different departments to tailor their cybersecurity strategy to how they intend to operate and behave.

Marketing

Cybersecurity risk	Scenario	Reflection
AI-Enhanced Spear Phishing	In the digital bazaar, AI crafts phishing emails with uncanny precision, targeting marketers. These aren't your grandfather's scams; they're tailored, convincing, and dangerously effective.	A reminder that in AI, as in magic, the hand is quicker than the eye. Be sceptical, verify twice.
Deepfake Deception	The digital stage is set for a performance in which AI-generated deepfakes of CEOs demand marketing data. This is the modern-day Trojan Horse; taking advantage of thoroughly misplaced trust in visuals and audio.	The onus is on us to question reality, a lesson as old as skepticism itself.
Content Sabotage	AI, the trickster, alters online content, embedding malicious seeds in the fertile grounds of our digital campaigns, waiting to sprout chaos.	Like a magician's illusion, the danger lies in what you don't see. Be vigilant.
Behavioural Manipulation	With AI analysing behaviour, marketing staff are targeted with unsettling precision, as if the AI knows them better than they know themselves.	An echo of the sentiment that understanding does not imply benevolence. Watch closely.
Ad Fraud Mirage	Here, AI-driven bots mimic human engagement, creating a mirage of ad success. Real money chasing fake clicks; a fool's errand.	A costly reminder that not all that glitters is gold. Question the value.
Competitive Intelligence Heist	AI, the modern-day cat burglar, stealthily scrapes away the hard-earned data of marketing campaigns, leaving behind no trace.	In this digital heist, awareness is our security system. Activate it.
Automated Social Engineering	AI-powered bots masquerade as customers, weaving convincing narratives to extract marketing secrets. The wolf in digital clothing.	Remember, in the garden of technology, not every voice seeks to enlighten.
SEO Poisoning	AI subtly manipulates the web's signposts, leading visitors astray. A digital sleight of hand redirecting traffic to the shadows.	The map is not the territory. Ensure your signposts are secure.
Brand Impersonation	In the theatre of social media, AI-generated impostors take the stage, mimicking brand voices to spread disinformation. The masquerade is convincing.	A call to be discerning viewers, questioning the authenticity of the performance.
Credential Stuffing Phantom	Like phantoms, AI-driven attacks slip through digital cracks, attempting thousands of key combinations to unlock marketing treasures.	The door may be digital, but the lock is real. Fortify it.

Sales

Cybersecurity risk	Scenario	Reflection
AI-Powered Identity Theft	AI algorithms, masquerading as digital chameleons, analyse public data to impersonate clients, weaving a web of deceit aimed at unauthorised transactions.	A stark reminder that in the digital realm, identities are fragile constructs. Question everything.
Automated Spear Phishing Precision	Like a magician using misdirection, AI crafts emails that bypass the critical eye, targeting sales personnel with uncanny accuracy to pilfer sensitive data.	An invitation to look beyond the surface, for the devil is in the details.
Deepfake Audiovisual Deception	The stage is set for deception as AI-generated deepfakes of clients or executives command actions, blurring the lines between reality and fabrication.	In this era of digital illusions, skepticism is our guiding star.
Predictive Analytics for Espionage	AI, the silent observer, uses data to unveil vulnerabilities within sales strategies, turning information into a weapon against itself.	Awareness that knowledge, while power, can also be an Achilles' heel.
Data Poisoning of CRM Systems	In a twist of fate, AI inputs false leads and customer interactions into CRM systems, leading sales astray in a maze of misinformation.	In this era of digital illusions, skepticism is our guiding star.
Credential Stuffing Automation	With the relentless efficiency of a machine, AI attempts to unlock the gates to sales databases, armed with a trove of stolen credentials.	A cautionary tale of the digital breadcrumbs we follow. Guard them wisely.
Competitive Intelligence Subterfuge	AI, the stealthy spy, scrapes and analyses sales tactics and customer feedback, turning the sales department's open book against them.	The digital keys to the kingdom are under siege; fortify your defenses.
Malware Customized for Sales Software	Tailor-made by AI, malware seeks out vulnerabilities in sales-specific software, a digital Trojan horse within the walls of CRM systems.	In the marketplace of ideas, some are shopping for your secrets. Lock them up.
AI-Generated Fake Client Orders	The mirage of lucrative deals lures sales into a trap, as AI crafts convincing but fraudulent orders, leading to financial and reputational ruin.	A reminder that even the mightiest walls have cracks. Inspect them often.
Social Engineering Bots	Like wolves in sheep's clothing, AI-driven bots engage in conversations, mimicking human queries to elicit sensitive sales information or manipulate actions.	In the desert of desire, mirages can seem real. Quench your thirst with caution.

HR

Cybersecurity risk	Scenario	Reflection
AI-Driven Identity Verification Fraud	AI algorithms manipulate digital footprints to create seemingly legitimate identities, tricking HR systems into onboarding non-existent employees.	A digital Pandora's Box opens, reminding us that not all that is verifiable is true. Doubt, then verify.
Automated Phishing Campaigns	Using AI, attackers craft highly personalized phishing emails targeting HR staff, mimicking internal communications to steal sensitive employee data.	In the shadow of familiarity, deception finds its roots. Be wary of the familiar turned peculiar.
Deepfake Interview Scams	Attackers use AI-generated deepfake videos to impersonate job candidates during remote interviews, aiming to gain access to corporate networks or sensitive information.	A testament to the idea that seeing isn't believing. Challenge the expected.
Data Poisoning of AI Recruitment Tools	AI-driven recruitment tools are fed false data, leading to biased hiring decisions or exploitation of system vulnerabilities for unauthorized access.	A mirror reflecting our own biases . Question the input; question the output.
Credential Stuffing on HR Platforms	AI algorithms automate attempts to access HR systems using stolen credentials, seeking personal data or financial information.	An automated siege on digital fortresses; the password is mightier than the sword. Strengthen it.
Social Engineering by AI Bots	AI-powered chatbots engage HR personnel in conversations designed to elicit confidential information under the guise of routine queries or IT support.	A conversation with a machine, masquerading as insight, seeks to deceive. Engage critically.
AI-Enhanced Background Check Manipulation	AI tools create false digital histories or erase negative information about candidates, misleading background verification processes.	In the digital age, the past is malleable. Verify, then trust.
Competitive Intelligence Gathering	Competitors deploy AI to analyse job postings and employee updates, inferring strategic moves or talent weaknesses.	What's shared freely becomes the weapon of the observer. Guard your insights like treasures.
Psychological Profiling Gone Awry	AI tools intended to assess candidate suitability are manipulated to exclude qualified individuals based on biases in training data, leading to legal and reputational risks.	The tool that measures can also mislead. Beware the biases that lie beneath.
Fake Employee Feedback and Reviews	AI-generated submissions flood platforms with fake employee feedback and performance reviews, impacting morale and decision-making.	In the digital chorus of feedback, discerning the genuine from the fake requires a keen ear. Listen wisely.

Application Development

Cybersecurity risk	Scenario	Reflection
AI-Driven Code Injection	AI algorithms fine-tune the art of crafting code that blends seamlessly into the application's fabric, only to unravel it from within, stealing data or compromising functionality.	A digital trojan horse, reminding us that not all is as it seems. Verify, then trust.
Automated Vulnerability Discovery	With relentless efficiency, AI scours application code, unearthing vulnerabilities faster than developers can patch them, opening gates to unauthorized access.	An arms race in the digital domain; speed in patching is of the essence.
Intelligent Phishing Attacks on Developers	AI, mimicking the digital nuances of trusted colleagues, sends phishing communications to developers, seeking to extract sensitive access credentials or inject malicious code.	Familiarity breeds complacency: skepticism is the antidote.
Deepfake Manipulation in Developer Communications	AI-generated deepfakes of team leaders or key stakeholders instruct developers on malicious updates, blending deception with authority.	In the echo chamber of digital communications, question the source.
AI-Powered Bug Exploitation	AI algorithms, trained on pattern recognition, sift through digital traces left by developers, piecing together enough information to reconstruct proprietary source code.	The digital footprint is larger than we think. Guard it jealously.
Manipulation of AI-Based Testing Tools	Competitors employ AI to analyse publicly available code commits and developer discussions, gaining insights into new features or technologies before they're officially released.	In the open forum of innovation, silence is sometimes golden.
Automated Exploit Generation	AI systems generate and deploy exploits against newly released applications at a pace that overwhelms traditional security measures, demanding a new level of agility in response.	The shield must evolve as quickly as the sword. Stay nimble.
Bias Injection in Machine Learning Models	Subtle manipulations by AI introduce biases into machine learning models used in applications, leading to skewed results and potential harm to users or reputational damage.	The integrity of the model is paramount; watch closely for unintended influences.

Traditional IT and Cloud Operations

Cybersecurity risk	Scenario	Reflection
AI-Enabled Access Anomaly Detection Evasion	AI algorithms adeptly mimic normal user behaviour, evading detection while infiltrating cloud environments, blurring the lines between legitimate access and covert operations.	A reminder that in the cloud, appearances can deceive. Vigilance must penetrate beyond the surface.
Automated Cloud Service Exploitation	AI tools tirelessly probe cloud services for vulnerabilities, launching attacks at machine speed when weaknesses are detected, leaving little time for human intervention.	The cloud's expanse is vast; our defenses must be both broad and swift.
Intelligent Data Exfiltration	With precision, AI identifies and siphons off sensitive data from the cloud, navigating through networks with minimal detection, orchestrating a silent heist of information.	In the digital ether, data whispers secrets. Guard them well.
AI-Powered Phishing Attacks on Administrators	AI crafts convincing phishing messages targeting cloud administrators, exploiting trusted relationships to gain elevated access or deploy malicious cloud configurations.	Trust, while a virtue, can be weaponised. Approach digital trust with caution
Deepfake Manipulation in Cloud Security Training	AI-generated deepfakes impersonate security experts or senior IT staff in training materials, disseminating misleading or harmful security practices among the team.	In training, as in practice, the source of wisdom matters. Authenticate and verify.
Manipulation of AI Cloud Security Tools	Subtly altering the behaviour of AI-based security tools, attackers induce false negatives or disable alerts, creating blind spots in the cloud's defensive perimeter.	The tools that guard us can be turned against us. Ensure integrity through redundancy and verification.
AI-Facilitated Insider Threat Amplification	AI algorithms augment the capabilities of malicious insiders, automating the theft or sabotage of cloud resources with enhanced efficiency and discretion.	An insider's betrayal, amplified by AI, reminds us that the human element remains our greatest vulnerability.
Configuration Drift Exploitation	Leveraging AI, attackers exploit minor, unnoticed deviations in cloud configurations to establish footholds, turning seemingly innocuous settings into gateways for attack.	Especially in the cloud, the devil is in the details. Continuous monitoring is key.
AI-Assisted Cloud Infrastructure Mapping	AI systematically maps cloud infrastructure, uncovering hidden APIs, data storage, and inter-service communications to identify unconventional attack vectors.	Knowledge is power and, in the cloud, understanding our architecture is the first line of defense.
Automated Compliance Evasion	AI algorithms dynamically alter cloud workloads and data handling practices to evade compliance checks, risking regulatory penalties and compromising data security.	Compliance is not just a hurdle but a safeguard. Automation must align with governance.

DevOps and DevSecOps specific teams

Cybersecurity risk	Scenario	Reflection
AI-Enhanced Code Injection	AI tools evolve to craft and inject malicious code into the CI/CD pipeline, seamlessly integrating it into deployments, turning every update into a potential trojan horse.	A reminder that the tools we build to automate can also be taught to betray. Scrutiny is paramount.
Automated Vulnerability Scanning Evasion	AI algorithms fine-tune attack vectors to slip past automated vulnerability scans in DevOps pipelines, exploiting the gap between scan schedules and patch deployments.	The race between scanning and exploitation narrows, demanding not just speed but foresight.
Intelligent Configuration Drift	AI-driven scripts subtly alter infrastructure-as-code configurations, inducing drift that opens security gaps, masked by the complexity of rapid deployments.	In the flux of continuous deployment, constancy is a virtue. Watch the watchmen.
AI-Powered Phishing for DevOps Credentials	Leveraging data mining and social engineering, AI crafts highly personalized phishing campaigns targeting DevOps teams, aiming to compromise pipeline integrity from within.	In the digital web of trust, skepticism is the thread that holds firm.
Deepfake Deception in Code Reviews	AI-generated deepfakes impersonate trusted developers or security advisors during code reviews, recommending malicious commits or dismissing critical vulnerabilities.	Even familiar faces may mask unfamiliar intents. Verify beyond doubt.
Manipulation of Machine Learning Models	AI algorithms subtly inject biases or vulnerabilities into machine learning models during the development phase, compromising applications before they reach production.	A trojan horse of a different breed—hidden not in code, but in the data that shapes it.
Automated Compliance Evasion in DevSecOps	AI dynamically alters application behaviour to temporarily comply with security audits, only to revert to non-compliant operations post-review, exploiting regulatory loopholes.	Compliance is not a checkbox but a continuum. Continuous monitoring matches continuous deception.
AI-Assisted Insider Threats in DevOps	Malicious insiders use AI to accelerate and obfuscate the exfiltration of proprietary code or sensitive data, exploiting their access to development environments with precision.	The human element, augmented by AI, remains the most unpredictable variable. Guard against it judiciously.
Cloud Infrastructure Discovery and Attack	AI algorithms systematically map and analyse cloud-based DevOps environments, identifying undocumented services or exposed ports to launch targeted attacks.	In the cloud, visibility is both a shield and a sword. Illuminate your digital landscape.
Supply Chain Compromise through AI	AI-driven analysis identifies and targets weak links in the software supply chain, inserting malicious code into dependencies, compromising applications from their foundations.	The chain is only as strong as its weakest link—AI finds it with unnerving efficiency. Fortify accordingly.

Legal and procurement

Cybersecurity risk	Scenario	Reflection
AI-Driven Contract Tampering	AI algorithms subtly alter terms in digital contracts, exploiting legal ambiguities or introducing clauses beneficial to adversaries, all in the guise of routine updates or corrections.	A testament to the notion that the devil is in the details—and AI may well be holding the pen.
Automated Legal Research Manipulation	AI tools, trusted to sift through precedents and statutes, are compromised to omit critical legal information or highlight unfavourable cases, skewing legal strategies and advice.	In the realm of law, as in logic, the foundation of our conclusions is only as solid as the data we consult.
Intelligent Phishing Attacks on Legal Staff	Using data analysis to understand the communication patterns of legal departments, AI crafts highly convincing phishing emails that mimic internal or client communications, aiming to extract sensitive information.	Familiarity breeds vulnerability: a sceptical eye is our best defense.
Deepfake Deception in Negotiations	AI-generated deepfakes impersonate key stakeholders in contract negotiations or legal discussions, misrepresenting positions or agreeing to unfavourable terms.	In the digital age, seeing and hearing are no longer believing. Authenticate rigorously.
Manipulation of Procurement Bidding Processes	AI analyses historical bidding data to predict future tenders, allowing adversaries to subtly manipulate procurement processes or outmanoeuvre competitors with uncanny precision.	A reminder that in procurement, transparency is a double-edged sword. Handle with care.
AI-Powered Analysis of Legal Vulnerabilities	Competitors use AI to analyse public and leaked documents, identifying legal vulnerabilities or strategies in litigation, thereby gaining an unfair advantage in court or negotiations.	The walls have ears, and now, they have AI. Protect your legal strategies as you would your trade secrets.
Automated Compliance Evasion	AI dynamically alters the operation of software or services to meet compliance checks on paper while actually operating outside regulatory guidelines, complicating legal oversight and accountability.	Compliance is not a checkbox; it's a commitment. Continuous monitoring is key.
Insider Threat Amplification in Legal Departments	AI enhances the capabilities of malicious insiders within legal or procurement teams, automating theft or sabotage of sensitive documents and contracts with precision.	The human factor, augmented by AI, underscores the need for comprehensive access controls and vigilance.
AI-Enhanced Forgery of Legal Documents	Sophisticated AI algorithms generate forgeries of legal documents, signatures, or seals with high accuracy, challenging the integrity of legal processes and documentation.	Trust in the authenticity of legal documents is foundational; digital verification technologies are crucial.
Supply Chain Risk Analysis Manipulation	AI manipulated by adversaries skews risk analyses, downplaying the vulnerabilities or risks associated with certain suppliers or contracts, leading to misguided trust and potential breaches.	In supply chain management, an informed decision is a safe one. Ensure your AI tools haven't been compromised.

Financial department

Cybersecurity risk	Scenario	Reflection
AI-Powered Fraud Detection Evasion	AI algorithms learn to mimic normal transaction patterns so closely that fraudulent activity slips through unnoticed, exploiting the very tools designed to protect financial integrity.	The sharper the tool, the more precise the evasion. Constantly refine and question detection models.
Automated Phishing Attacks on Finance Staff	AI crafts highly personalized phishing emails targeting finance personnel, using detailed analysis of their digital footprint to bypass traditional vigilance and security training.	In the age of AI, skepticism is a virtue. Train eyes to see beyond the surface.
Deepfake Manipulation in Financial Communications	AI-generated deepfake audio and video convincingly impersonate C-suite executives or trusted clients, requesting unauthorized transfers or disclosing sensitive financial information.	Trust but verify. In digital communication, authenticity must be authenticated.
AI-Driven Insider Trading Strategies	AI analyses market data and internal financial reports with unprecedented depth, identifying patterns to exploit for insider trading, well beyond human capability.	The line between analysis and exploitation blurs with AI. Guard your data.
Manipulation of Algorithmic Trading Systems	Malicious AI introduces subtle, manipulative data into the market, swaying algorithmic trading systems to make detrimental trades or manipulate market conditions.	The market is a sea, AI the current. Navigate with caution, knowing what moves beneath the surface.
AI-Enhanced Embezzlement Tactics	Using AI to automate and conceal unauthorized financial transactions, culprits siphon off funds with a complexity and scale previously unattainable by human actors alone.	Vigilance in oversight is paramount; AI can mask the footsteps of financial malfeasance.
Financial Forecast Manipulation	AI tools subtly skew financial forecasting models, leading to overly optimistic or pessimistic projections, which can misguide strategic investment and budgeting decisions.	In forecasting, question the wind that shapes the sails. Ensure models are robust and data is clean.
Compromise of Automated Compliance Reporting	AI algorithms adjust financial reporting data just enough to evade detection by compliance systems, presenting a façade of regulatory conformity while engaging in risky or illicit activities.	Compliance is not just ticking boxes; it's ensuring the spirit of the law is followed. Monitor closely.
AI-Facilitated Ransomware in Financial Systems	Advanced AI customizes ransomware attacks to target specific financial systems, learning from each interaction to improve its chances of success and evasion from security measures.	In the dance of attack and defence, AI steps deftly. Prepare to meet it step for step.
Disinformation Campaigns Affecting Stock Prices	AI-driven disinformation campaigns manipulate stock prices by spreading false financial news about companies, exploiting the rapid response of markets to perceived threats or opportunities.	The truth is the first casualty in the war on information. Fact-check rigorously.

Security and Compliance

Cybersecurity risk	Scenario	Reflection
AI-Compromised Security Protocols	AI algorithms manipulate security protocols in the guise of enhanced protection, introducing flaws that are exploited to bypass security measures, leaving systems vulnerable.	In the arms race of cybersecurity, question the allegiance of your tools. Vigilance is key.
Deepfake Disinformation Campaigns	AI-generated deepfakes target security teams with false alerts or misinformation, diverting attention from real threats or undermining trust in legitimate communications.	In the digital echo chamber, trust but verify. The integrity of communication is paramount.
AI-Powered Phishing Attacks on Compliance Data	Utilizing natural language processing, AI crafts highly convincing phishing emails targeting compliance officers, aiming to extract sensitive audit data or manipulate compliance reports.	The pen is mightier in the age of AI; guard your data like state secrets.
Automated Vulnerability Discovery and Exploitation	AI systems scan for and exploit vulnerabilities at a pace and depth beyond human capacity, leveraging these for attacks before patches can be applied or detected.	The digital battleground shifts with the winds of AI; adapt your defenses accordingly.
Manipulation of Behaviour-Based Security Systems	AI subtly alters behaviour patterns within monitored systems, gradually desensitizing security protocols to unauthorized activities, effectively blinding detection mechanisms.	The wolf in sheep's clothing; AI can cloak malice in normalcy. Educate your systems to see through the disguise.
AI-Driven Insider Threat Amplification	Enhanced by AI, insider threats become more sophisticated, using algorithms to mask unauthorized activities or exfiltrate data undetected, exploiting systemic trust.	The threat within grows in the shadow of AI; shine a light with continuous monitoring and anomaly detection.
Evasion of Machine Learning-Based Security Tools	Malicious AI evolves to outmaneuver machine learning-based security tools, continuously adapting to avoid detection and exploiting weaknesses in AI-driven defense mechanisms.	As AI defenses rise, so do AI offenses. Foster an environment of perpetual learning and adaptation.
AI-Enabled Regulatory Evasion	Organizations use AI to skirt the edges of regulatory compliance, dynamically altering operations to appear compliant while engaging in practices that violate the spirit of regulations.	In the dance of compliance, AI steps lightly. Ensure your partner dances to the right tune.
Misinformation Attacks on Security Policies	AI-generated misinformation campaigns internally undermine trust in security policies and procedures, leading to decreased adherence and increased vulnerability.	The foundation of security is trust; protect it from the termites of disinformation.
Compromise of AI Ethics and Compliance Algorithms	AI designed to monitor ethical compliance and decision-making within organizations is tampered with, leading to skewed ethical guidelines and compromised compliance monitoring.	Ethics in AI requires a foundation of trust; build it with bricks of transparency and audits.

As seen from some of the scenarios, one stark difference between past technological trends and the rapidly evolving landscape of Artificial Intelligence is the way security must now be intricately tailored to align with the unique operations of each department within a business.

This is a break from the industry tailored yet lowest common denominator and (often) manual checklists conducted by interview in non-real time.

This paradigm shift signifies a departure from the traditional model where security was centralised and uniformly applied across an organization. Instead, we're moving towards a model where security becomes decentralised, with each department, division, or team not only becoming responsible for their specialised cybersecurity risks but also actively predicting, preparing and managing them. This approach, while novel to many companies operating on the principles of the past, aligns with the notion of failing fast and adapting in step with the global innovation race.

For businesses, this means staying constantly educated about the latest developments in AI capabilities and its associated threats; both for toxic assets, technology debt and the new scenarios. It necessitates investing in continuous exploration, development and advancement in security measures specifically designed to combat AI-related risks.

Moreover, fostering a security-conscious culture where continuous training and awareness is woven into daily operations becomes imperative. Collaborating with different breeds of cybersecurity experts and industry peers to share knowledge and develop best practices tailored to individual operational models is no longer optional; it's essential, not only to safeguard your business, but to foster business growth, and maintain a relevant and positive brand reputation.

Looking at the broader dimension of cyberdefense, here are a few MUST-do's:

Implementing a modern – up2date, up2speed - cybersecurity approach

Upgrading to cyberdefense solutions that leverage AI and machine learning is crucial and will enable security to be tailored to the business unit's mode of operation. These solutions can detect anomalies and patterns that indicate AI-generated attacks, offering a proactive cyberdefense stance.

Fostering a culture of security awareness

If you aspire to have a resilient workforce able to recognise and respond to new threats, including sophisticated AI-driven attacks like phishing, deepfakes and individual manipulation, then frequent staff training is essential. Radically, this means that automatically trusting what seems to come from your security department is no longer sufficient to ensure the operational security necessary for an individual department's success.

Establishing data governance protocols

Controlling and monitoring data flows within the organization is key to ensuring data integrity and preventing data poisoning. Additionally, it is important to introduce the principles of explainability and transparency if you want to be able to reverse engineer in real time your decision support systems, any decision made using AI or any insight attributed to a business function or individual.

Developing a digital authentication framework

Incorporating multi-factor authentication and biometrics can safeguard against unauthorised access, particularly from deepfake technologies; but the digital industry will have changed in the time it has taken you to read this whitepaper, so keep exploring.

Encouraging responsible and sustainable AI use

Defining ethical guidelines for AI usage within your organisation is crucial to prevent internal misuse or misunderstandings (good intent gone wrong) and to maintain ethical standards tailored to the perceptions - in terms of services, employee behaviour and brand recognition – you wish your stakeholders to have of your business.

Adopting AI detection tools

Investing in technologies specifically designed to detect AI-generated content is a step towards smarter, AI-aware cybersecurity practices. This can not only help your employees leverage the opportunity of global reach but can also safeguard your operating model against behaviour manipulation and prevent your brand becoming associated with malicious or unacceptable geo-political or malicious behaviours.

Evolving to real-time predictive and proactive Incident Response capabilities

Having a robust plan and the capability to respond to breaches – especially those involving AI – not merely quickly but in milliseconds, is crucial in minimising damage. Now that any individual has affordable, straightforward access to hyper-scalable compute power, it is no longer enough to take a human-based reactive approach to security incidents: instead, you must implement a governance framework base on predictive, real-time response.

Securing Intellectual Property

Utilising advanced digital watermarking (invisible, robust or forensic) and other IP protection methods is vital to guard against the unauthorised use of AI in replicating or modifying proprietary material.

Statistically, existing methods of managing this risk are insufficient to protect against AI-enabled attackers so you need to change your approach, explore new methods, and step up your game.

Monitoring regulatory compliance

Keeping abreast with regulations around data privacy and AI, such as GDPR or the AI act, is essential for compliance and protection against liabilities.

However, this alone will not be enough: you will need to focus on data management capabilities as human checklists and compliance by interview may potentially become outdated within hours or days. Instead, you should build real-time compliance verification mechanisms able to match the pace of innovation.

Engaging in industry collaboration

Participating in industry groups and think tanks that have a genuine in how these scenarios impact your organisation and sharing knowledge on emerging threats and defenses is vital. First and foremost, it's not about discussing T-shirt sized solutions, but about raising awareness, and reflecting on and exploring alternative principles and approaches. Based on these informed discussions, you will be able to tailor these solutions to your own needs – either independently or together with your partner ecosystems.

The double-edged sword – the combination of AI-enabled attackers with the integration of AI into business operations – demands a multifaceted approach to building new cybersecurity capabilities in your operating model. It requires not just technological solutions but a profound shift in organisational culture and practices.

The tailored approach to cybersecurity described above, one that is adapted to the unique needs and operational models of each business entity, is critical in navigating the potential transformations brought about by AI.

"Consequently, it's not just about defending against new risks; it's about reshaping your cybersecurity strategies to be as dynamic and intelligent as the AI technologies the rest of the world – and hopefully also yourself – is exploring and embracing."

The new Cybersecurity kids on the block

As you strive to enhance your Cybersecurity capabilities and simultaneously exploit the myriad business opportunities presented by AI, it becomes crucial to deploy roles that serve as a bridge –between current cybersecurity practices, which may be robust yet traditional, and the innovative, AI-infused practices that are rapidly becoming indispensable.

The roles you introduce within your organization should be tailored to facilitate this transition, melding the tried-and-true with the cutting-edge – simply making Cybersecurity as agile as innovation allows everything else to be.

Job Role	Responsibilities	Rationale
Cybersecurity Analyst	Monitor network traffic for anomalies, investigate security breaches, and assess the risks associated with generative AI applications.	A foundational role for identifying and responding to immediate threats.
AI Security Specialist	Evaluate the security aspects of AI deployments within the company, develop defenses against AI-powered threats, and oversee the safe integration of AI tools.	Specialized in understanding AI-related threats and ensuring AI tools are used securely.
Data Protection Officer	Ensure compliance with data privacy laws, assess data handling related to AI outputs, and manage data privacy risks.	Essential for maintaining trust and adherence to privacy regulations in the age of AI.
AI Ethicist	Develop ethical guidelines for AI use, audit AI-powered systems for compliance with ethical standards, and advocate for responsible AI practices.	To ensure AI is deployed responsibly, in line with societal values and ethical considerations.
DevSecOps Engineer	Integrate security at every stage of software development and deployment, including AI-driven systems, to enable secure continuous delivery.	Bridges development, operations, and security to expedite secure deployment of AI applications.
AI Research and Development Lead	Explore and pilot cutting-edge AI technologies for both enhancing cybersecurity measures and identifying new business opportunities.	Drives innovation and ensures the company stays ahead of technology trends.
AI Governance Coordinator	Oversee AI governance frameworks, ensuring transparency, accountability, and regulatory compliance across all AI-powered initiatives.	Guarantees that AI deployments are controlled and compliant with internal and external standards.
Business Intelligence Analyst	Use AI to analyse market trends, customer data, and competitive information to inform strategic decision-making and identify new business opportunities.	Translates AI capabilities into actionable business insights.
Training and Awareness Manager	Develop and manage a cybersecurity awareness program that includes education on AI risks and opportunities, ensuring all employees are informed and vigilant.	Empowers employees to be the first line of defense and leverage AI effectively.
Threat Intelligence Specialist	Collect and analyse information on potential threats, including those posed by generative AI, to inform defense strategies and business risk assessments.	Proactive in identifying emerging threats and enabling informed decision-making.

These are the roles we can imagine today. However, as AI becomes an embedded part of daily operations, a host of new roles will become commonplace.

For example, the role of an AI Threat Predictor will become essential. This individual would be tasked with the complex and critical job of foreseeing potential AI-related security breaches, not just in their current forms but in ever-evolving, increasingly sophisticated scenarios.

As we enter the age of quantum computing, what about the Quantum Cryptologist. This person's role would delve into the intricacies of quantum computing, an area where traditional cryptography might falter, ensuring that our data remains secure against AI-driven decryption methods that we can barely fathom today.

Then there's the CyberImmunity Architect. This role moves beyond the traditional concept of cybersecurity into a realm where systems are designed to be inherently immune to Cyberthreats, a kind of digital prophylaxis against the myriad of dangers in the Cyberworld.

We shouldn't overlook the Behavioural Forensics Analyst. This professional would dissect and understand the nuanced behaviour of AI systems, especially those that mimic human behaviours. This analysis is crucial in identifying and mitigating risks that such human-like AI systems might pose.

The Autonomous Response Coordinator speaks to the need for rapid, intelligent responses to security threats. This would be a role that coordinates AI-driven security systems, ensuring they respond effectively and ethically to threats in real-time, without human intervention.

A CyberLegislation Advisor would be pivotal in shaping the legal landscape. As AI challenges our current legal frameworks, this advisor's role would be to guide legislation that addresses the unique challenges posed by AI, from privacy concerns to ethical dilemmas.

Then there's the Data Sovereignty Strategist. In an age where data is king, this strategist would navigate the complex waters of data ownership and jurisdiction, particularly crucial as AI blurs geographical boundaries and traditional jurisdictions.

Lastly, as also mentioned in the table above, the AI Security Ethicist. This is perhaps one of the most critical roles. As AI becomes more integrated into our lives, the ethical considerations surrounding its use and misuse become paramount. This ethicist would be at the forefront of defining and upholding the moral compass in the AI landscape.

In essence, as we march forward into this brave new world of AI, these roles – and likely many others we haven't yet envisioned – will become essential to navigate the complex, intertwined realms of technology, security, ethics, and law.

You've got everything to lose and everything to win!
Be predictive and be proactive – the future is now!