Opening Statement

Interviewer:
Goedemorgen en welkom. Allereerst dank ik u hartelijk voor uw bereidheid om aan dit interview deel te nemen. Mijn naam is Imane Akhyar en ik ben masterstudent Information Studies aan de Universiteit van Amsterdam. Dit interview is onderdeel van mijn scriptieonderzoek bij Kouters van der Meer. Het onderzoek richt zich op de vraag hoe kunstmatige intelligentie effectief kan worden geïntegreerd in het cybersecurity-risicomanagement binnen financiële instellingen.

Het gesprek zal ongeveer 60 minuten duren maar ik denk dat we al na 30 minuten klaar zijn. Alle antwoorden worden volledig geanonimiseerd en strikt vertrouwelijk behandeld. U bent uiteraard vrij om een vraag over te slaan of het interview op elk gewenst moment te beëindigen.

Heeft u op dit moment nog vragen voordat we van start gaan?

Respondent:
Nee, alles is wel duidelijk.

Sectie 1: Achtergrond van de geïnterviewde

Interviewer:

Voordat ik verder ga wil ik nog kort uitleggen dat het interview uit twee delen bestaat, namelijk de introductie vragen en de kernvragen. Als eerst begin ik met de introductie vragen:

Q1.1: Kunt u kort iets over uzelf vertellen en uw rol binnen de organisatie?

Respondent

Mijn naam is [Naam] en ik ben sinds januari werkzaam als directeur binnen [Naam Bedrijf]. Binnen onze organisatie ben ik specifiek verantwoordelijk voor het bedienen van klanten in de financiële sector, met name banken. Voordat ik deze rol op mij nam, werkte ik als auditor, waar ik veel ervaring heb opgedaan op het gebied van toezicht, controle en risicobeoordeling. Deze achtergrond helpt mij nu om klanten goed te adviseren over governance- en risicovraagstukken, zeker in relatie tot nieuwe technologieën zoals kunstmatige intelligentie. En sindskort behoor ik ook tot de AI-groep van het bedrijf.

Interviewer:
Q1.2: Hoeveel ervaring heeft u met cybersecurity, risicomanagement of AI?

Respondent:

Ik heb bijna tien jaar ervaring als IT-auditor, met een focus op technologie risico's binnen verschillende organisaties. Vanuit die rol ben ik veel bezig geweest met cybersecurity en risicomanagement in brede zin. Hoewel AI daar tot voor kort nog niet centraal in stond, zie ik dat het nu steeds relevanter wordt. Daarom ben ik inmiddels ook aangesloten bij een AI-werkgroep binnen onze organisatie, waarin we onderzoeken hoe we AI op een verantwoorde en effectieve manier kunnen toepassen. Die combinatie van achtergrond in technologie en risicobeheersing helpt me om de risico's en kansen van AI goed te kunnen overzien. Daarnaast heb ik afgelopen jaar een aantal scripties begeleid over AI en risicomanagement.

Interviewer:
Q1.3 In hoeverre bent u bekend met LLMs of andere AI-technologieën in uw werkcontext?

Respondent:
Ik heb vooral ervaring met ChatGPT en zie dat dit ook binnen onze organisatie en bij klanten veel wordt gebruikt. Zelf maak ik gebruik van de betaalde versie, die ik erg goed vind. Daarnaast hoor ik ook positieve verhalen over andere modellen, zoals Claude. We bevinden ons nog in een verkennende fase, maar ik zie dat er veel wordt geëxperimenteerd en samengewerkt met bestaande tools. Wel blijft er een zekere terughoudendheid: ik stel mezelf vaak de vraag hoe betrouwbaar de output is, en of de inputdata wel voldoende gecontroleerd is. Dat soort vragen komen steeds vaker naar voren, zeker bij kritieke toepassingen.

Interviewer:
En als laatst:
Q1.4 Bent u bekend met regelgeving zoals DORA of de AI Act?

Respondent:
Ja, ik ben bekend met de GDPR en de AI Act, en zie dat die steeds meer invloed hebben op hoe organisaties AI inzetten. Er is veel overlap tussen verschillende regelgeving, wat het belangrijk maakt om dit goed te doorleven bij het opstellen van intern beleid. Bijvoorbeeld: mag iets wel volgens de AI Act of juist niet? Dat zijn afwegingen die je vroegtijdig moet maken. In onze organisatie zie ik dat proportionaliteit een belangrijk uitgangspunt is. We zijn geen grote techspeler, maar willen wél op een verantwoorde manier kunnen verantwoorden hoe we AI inzetten. Daarom betrekken we soms ook externe juridische experts om na te gaan of ons gebruik binnen de wettelijke kaders past

Sectie 2: Thematische verdieping

Interviewer:
Nou top dat waren de introductievragen. De volgende vragen gaan over componenten van het framework. Dit zijn meer inhoudelijke vragen over de onderwerpen en de laatste twee vragen gaan over het voorlopige framework.
Q2.1: Op welke punten binnen cybersecurity en risicomanagement kunnen AI-modellen de meeste waarde bieden? En dan heb ik het specifiek over de financiële sector.

Respondent:
Ik denk dat vooral in het verwerken van hele grote datasets veel winst te behalen is, zodat je beter inzicht krijgt en niet alles zelf hoeft te doen. Ik denk dat als je het op de juiste en veilige wijze inzet, het mankracht bespaart en veel meer inzicht kan opleveren. Wel met de kanttekening dat er ook steeds meer data komt, en dat het misschien lastig is om altijd volledig inzicht te hebben. Ik denk eigenlijk dat dat misschien helemaal niet mogelijk zal zijn, maar ik denk wel dat het daarbij heel goed helpt. Bij risicomanagement denk ik dat het efficiënter inrichten van processen en het automatiseren daarvan, bijvoorbeeld dat alle rapportages automatisch gaan, heel nuttig kan zijn. Toevallig hadden we vorige week een klant met een heel mooi dashboard voor managementinformatie, uit allerlei fancy PowerBID's. Ik vroeg toen: 'Wat is de bron en is die volledig?' Daar kwam eigenlijk helemaal geen antwoord op. Dan loop je ertegenaan: waar komt de data vandaan en hoe weten we of de data juist is?

Interviewer:
Wat hier dus ook uithaal is dat de bron van de data een grote rol speelt hierin.
Q2.2: Zijn er bepaalde AI-tools waarvan je denkt dat ze heel handig zijn, bijvoorbeeld ChatGPT?
Ik heb eigenlijk vooral ervaring met ChatGPT en die zie ik ook het meest om me heen. Verder heb ik niet veel andere AI-tools gebruikt. Ik hoor wel goede verhalen over de betaalde versie en denk dat die ook heel handig kan zijn voor binnen de organisatie zelf. Als we het hier zouden gebruiken, we werken in een Microsoft-omgeving , dan zal CoPilot ook wel goed gaan. Maar ik ben nog steeds enigszins huiverig of alles wel klopt. Ik stel mezelf echt veel vragen. Ik denk soms: hoe weten we dit nou zeker? En als iemand iets invoert en er komt een antwoord uit, hoe weten we dan zeker dat dat antwoord juist is.

Interviewer:
In eerdere interviews kwam het onderwerp toezicht op het gebruik van AI-systemen regelmatig naar voren. Sommige organisaties hebben daar al expliciet beleid voor opgesteld, terwijl anderen vooral het belang benadrukten van logisch nadenken en gezond verstand in het gebruik ervan.

Q2.2: Hoe wordt in uw organisatie toezicht gehouden op AI-systemen?

Respondent:
Op dit moment zijn we nog bezig met het opbouwen van onze governance rondom AI. Er is binnen de organisatie wel al een breder Maatschappij- & Veiligheidsbeleid, maar we merken dat AI een eigen benadering vraagt. Daarom zijn we bezig met het opstellen van een apart AI-beleid, los van dat bestaande kader.

We vinden het belangrijk dat medewerkers actief worden meegenomen in dat beleid, zodat het niet alleen een document is op SharePoint dat niemand leest. Toezicht moet voor ons niet alleen formeel zijn, maar ook gedragen worden in de praktijk. Daarom betrekken we verschillende disciplines in het opstellen ervan en kijken we ook hoe we kennisdeling en bewustwording over AI kunnen vergroten. Het is echt nog in ontwikkeling, maar er wordt serieus werk van gemaakt.

Interviewer:

Helder, dank u. U gaf dus aan dat het toezicht op AI nog in ontwikkeling is en dat er gewerkt wordt aan een apart AI-beleid. Een belangrijk aspect daarbij is natuurlijk de rol van wet- en regelgeving.

Q2.3: Hoe beïnvloeden GDPR, DORA, NIS2 of de AI Act het gebruik van LLMs in uw organisatie?

Respondent:
Ja, vanzelfsprekend is er wel wat overlap tussen die verschillende regelgevingen. Daarom is het ook zo belangrijk om ze goed te doorlopen voordat je met AI aan de slag gaat. Als je een beleidsstuk opstelt, moet je echt vooraf nagaan: mag dit op basis van GDPR? En hoe zit het met de AI Act? Ik heb vorig jaar een project gedaan waarbij dat ook aan de orde kwam, en daarin bleek dat proportionaliteit een heel belangrijk uitgangspunt is. Dat geldt hier bij ons net zo. We zijn natuurlijk geen grote speler als Microsoft, maar we willen wél op een verantwoorde manier kunnen uitleggen waarom we iets doen, en hoe we dat vastleggen. We willen er met een goed gevoel naar terug kunnen kijken dat we dit met zorg en bewustzijn hebben ingericht.

Het vraagt wel om samenwerking. Het is niet iets wat je even in je eentje bedenkt of oplegt. Het is echt een gezamenlijke verantwoordelijkheid om beleid te maken dat past bij de regelgeving én bij onze organisatie. Dat is nog wel een uitdaging, maar wel eentje waar we ons actief mee bezighouden.

Interviewer:

Verder heb ik nog een aantal vragen over ethiek en privacy. Dat zijn natuurlijk twee termen doe best vaak terug komen bij het gebruik van AI.

Q2.4: Welke ethische risico's ziet u bij de inzet van LLMs?

Respondent:
Er zijn zeker ethische risico's. Een belangrijk punt is de kwaliteit en herkomst van de data die gebruikt wordt om LLMs te trainen, daar is niet altijd transparantie over. Je weet soms

niet precies waarop een model is gebaseerd, en dat maakt het lastig om de betrouwbaarheid van de uitkomsten goed in te schatten.

Daarnaast zie ik het risico dat mensen te afhankelijk worden van AI. Het gevaar bestaat dat je als gebruiker je eigen kritisch denkvermogen verliest en gewoon klakkeloos overneemt wat een model teruggeeft. Terwijl je juist moet blijven nadenken: klopt dit? Begrijp ik wat hier staat? Zeker als het om complexe of beleidsmatige informatie gaat, is dat cruciaal.

Wat ik ook merk in de praktijk, is dat er bij medewerkers steeds vaker zorgen ontstaan over de inzet van AI, bijvoorbeeld dat hun werk deels of helemaal wordt overgenomen. Die angst leeft ook bij LLM-toepassingen. Het roept vragen op over werkzekerheid, rolveranderingen en toekomstbestendigheid van functies. Dat zijn thema's waar je als organisatie ook aandacht voor moet hebben, en die je mee moet nemen in je ethische afwegingen.

Interviewer:

En vaak willen organisaties wel profiteren van de snelheid en efficiëntie van AI, maar tegelijkertijd de controle behouden over wat ermee gebeurt.

Q2.4a: Is er volgens u altijd menselijke controle nodig, of kunnen bepaalde beslissingen ook volledig geautomatiseerd worden?

Respondent:
Ik ben van mening dat er altijd een vorm van menselijke controle nodig is, zeker bij belangrijke of gevoelige output zoals beleidsdocumenten, rapportages of adviezen. Bij simpele taken zoals bijvoorbeeld vertalingen kun je AI misschien prima zelfstandig iets laten doen, maar zodra het inhoudelijk of strategisch wordt, moet er echt iemand meekijken.Je kunt AI gebruiken als hulpmiddel, maar het mag nooit de eindverantwoordelijkheid overnemen. Mensen moeten begrijpen wat er gegenereerd is en bereid zijn dat te corrigeren of aan te passen waar nodig. Uiteindelijk leveren wij iets op aan de klant, en dan moet je zeker weten dat alles klopt. Er moet dus altijd nog een laatste controle plaatsvinden, zodat je met vertrouwen achter de kwaliteit van het werk kunt staan.

Interviewer:
U benoemt meerdere keren hoe belangrijk de herkomst en betrouwbaarheid van data is.
Q2.5: Hoe belangrijk is volgens u de datakwaliteit en -controle in AI-toepassingen zoals LLMs?

Respondent:
Dat is ontzettend belangrijk. De input data moet aan bepaalde voorwaarden voldoen voordat je het verantwoord kunt gebruiken in AI-toepassingen. Als je niet weet waar de data vandaan komt, of hoe die tot stand is gekomen, dan wordt het heel lastig om op de uitkomsten te vertrouwen. Zeker bij modellen die grote hoeveelheden tekst of informatie genereren, is het cruciaal om te begrijpen wat de basis is waarop het model zijn voorspellingen of output baseert. Tegelijkertijd moet je daar ook realistisch in blijven. Je kunt niet elke dataset volledig doorlichten of handmatig controleren, zeker niet als je met beperkte middelen werkt. Daarom is het belangrijk om een proportionele aanpak te hanteren: je moet kritisch zijn, maar ook werkbaar blijven. Het draait om bewustwording, duidelijke spelregels en goed risicomanagement bij het gebruik van data in AI-context.

Interviewer: Naast de data is het ook belangrijk dat de LLMs op de juiste manier, binnen het bedrijf, worden gebrukikt.

Q2.6: Hoe wordt gecontroleerd hoe LLMs worden ingezet of aangepast?

Respondent:
We zitten nog in de beginfase van het ontwikkelen van controlemechanismen rondom het gebruik van LLMs, maar wat we nu al doen, is sterk inzetten op educatie en bewustwording. Binnen onze organisatie hebben we een gebruikersgroep waarin mensen ervaringen uitwisselen, vragen stellen en risico's bespreken. Die kennisdeling is ontzettend waardevol.

Daarnaast organiseren we regelmatig interne kennissessies om collega's bewust te maken van zowel de kansen als de risico's van AI. Niet iedereen heeft een technische achtergrond, dus het is belangrijk dat mensen begrijpen wat een LLM precies doet, waar je op moet letten bij gebruik, en hoe je verantwoord omgaat met input en output. We geloven dat goed geïnformeerde medewerkers uiteindelijk de beste eerste controlelaag vormen. Dus in plaats van alles dicht te timmeren met technische restricties, leggen we nu de nadruk op training, open dialoog en gezamenlijke leermomenten. Dat vormt de basis van onze aanpak.

Interviewer: Dat waren dan de inhoudelijke vragen. De volgende twee vragen gaan over het voorlopige framework.

Q2.7: Wat is volgens u nodig om vertrouwen te hebben in een AI-ondersteund framework voor cybersecurity-risicomanagement?

Respondent:
Om vertrouwen te hebben in een AI-framework, is het belangrijk dat duidelijk is waar het begint. Start je bij beleid of juist bij een technische risicoanalyse? Die volgorde bepaalt hoe de onderdelen logisch op elkaar aansluiten. Als dat onduidelijk is, wordt het lastig om het framework goed toe te passen.

Wat ik daarnaast essentieel vind, is een duidelijke koppeling met risk assessment. Je moet eerst weten welke risico's relevant zijn in jouw context voordat je passende maatregelen kunt bepalen. Die stap mis ik nu nog; zonder die analyse krijg je al snel generieke controles die niet altijd aansluiten bij de praktijk.

Het framework moet ook flexibel genoeg zijn om toegepast te worden binnen verschillende typen organisaties, wat werkt bij een grootbank, niet per se bij een kleinere partij. En tot slot: toetsing. Het zou moeten benoemen hoe het gevalideerd wordt, door wie en op basis van welke criteria. Alleen dan blijft het framework actueel en bruikbaar.

Q2.8: Welke onderdelen van het framework vindt u het meest relevant of juist problematisch? Mist u bepaalde elementen of ziet u mogelijkheden voor verbetering?

Respondent:
Wat ik heel sterk vond aan het framework is dat het meerdere relevante thema's aangestipt, zoals data, lifecycle, governance en ethiek. Maar er zijn ook elementen die wat mij betreft verder versterkt mogen worden. Een belangrijk punt is educatie. In de praktijk zie ik dat kennis over AI heel ongelijk verdeeld is binnen organisaties. Sommige medewerkers zijn

digitaal vaardig en experimenteren volop, terwijl anderen nauwelijks weten wat een LLM eigenlijk doet. Als je dan een framework ontwikkelt dat moet bijdragen aan verantwoorde implementatie van AI, dan moet daar een duidelijke educatieve component in zitten. Niet alleen eenmalige trainingen, maar structureel: onboarding, herhaal sessies en toegankelijke documentatie. AI-literacy moet echt een basisvoorwaarde worden.

Daarnaast mis ik aandacht voor kennisdeling als structureel onderdeel. AI ontwikkelt zich snel, en organisaties leren veel al doende. Het zou mooi zijn als het framework stimuleert dat ervaringen, successen en fouten actief worden gedeeld, binnen teams, tussen afdelingen, of zelfs over organisaties heen. Zo bouw je collectieve intelligentie op en voorkom je dat iedereen opnieuw het wiel moet uitvinden. En als laatste zou ik voorstellen om expliciet onderscheid te maken tussen de ‘run’-kant en de ‘change’-kant van AI-inzet. Dus enerzijds het dagelijks gebruik (run) en anderzijds de verandering, innovatie of implementatie (change). Die twee vragen om verschillende vormen van governance, risico-inschatting en betrokkenheid van mensen. Door dat onderscheid in het framework op te nemen, sluit het beter aan bij hoe organisaties daadwerkelijk werken.

Interviewer:

U heeft een aantal waardevolle punten benoemd, zoals het belang van een duidelijke start en koppeling met risk assessment, maar ook de noodzaak van flexibiliteit en toetsbaarheid. Bij de vorige interviews kwam educatie ook al naar, dus die zal ik zeker verwerken in het framework.

Dan zijn we hiermee aan het einde gekomen van het interview. Zoals gezegd ga ik de resultaten uit dit gesprek verwerken in de verdere ontwikkeling van het AI-framework. Op basis van alle interviews volgt er een aangepaste versie, die ik in de tweede week van juni met u zal delen via een korte Google-survey. Die bevat vijf à zes eenvoudige, gesloten vragen om het framework te valideren, en zal voorzien zijn van een duidelijke deadline aan het einde van diezelfde week.

Nogmaals dank voor uw tijd en waardevolle inzichten, ik heb er echt veel aan gehad! Zoals eerder aangegeven worden alle antwoorden volledig geanonimiseerd en uitsluitend gebruikt voor mijn scriptie. Na afronding worden de gegevens verwijderd en nergens anders voor gebruikt.