2025 Voice of the CISO-rapport van Proofpoint onthult verhoogd AI-risico, recordhoogte CISO-burnouts en aanhoudend menselijk probleem in cybersecurity

73% van Nederlandse CISO's verwachten een materiële cyberaanval in het komende jaar, met menselijke risico's en GenAI-aangestuurd dataverlies als grootste zorgen

Amsterdam, 26 augustus 2025 – Proofpoint, Inc., een leidend cybersecurity- en compliancebedrijf, publiceert vandaag zijn vijfde jaarlijkse Voice of the CISO-rapport. Hierin worden de belangrijkste uitdagingen, verwachtingen en prioriteiten van Chief Information Security Officers (CISO's) wereldwijd onderzocht. Het rapport voor 2025, waarin 1.600 CISO's uit 16 landen zijn ondervraagd, belicht twee cruciale trends. Allereerst de toename van cyberaanvallen, die zorgt voor meer onrust onder CISO's, wat gepaard gaat met een groeiende bereidheid om losgeld te betalen wanneer zich incidenten voordoen. De tweede trend is de snelle opkomst van GenAI. Deze dwingt securityleiders om een evenwicht te vinden tussen innovatie en risico's, ondanks de toenemende bezorgdheid over blootstelling en misbruik van data.

Naarmate cyberdreigingen steeds vaker voorkomen en steeds complexer worden, maken CISO's zich steeds meer zorgen over het vermogen van hun organisatie om een ernstige aanval te weerstaan. 73% van de Nederlandse CISO's denkt dat ze het risico lopen om in de komende 12 maanden een ernstige cyberaanval te ondervinden. Toch zegt 58% dat ze niet voorbereid zijn om hierop te reageren. Vier op de vijf Nederlandse CISO's hebben het afgelopen jaar te maken gehad met aanzienlijk dataverlies, waarbij incidenten door insiders bovenaan de lijst van oorzaken staan. Volgens de enquêtegegevens schrijft 99% van de Nederlandse CISO's ten minste een deel van het dataverlies toe aan vertrekkende werknemers, een stijging van 67% ten opzichte van vorig jaar. Menselijk gedrag blijft dus een kritieke kwetsbaarheid. Op basis van de antwoorden op de enquête zegt 57% van de Nederlandse CISO's te overwegen om losgeld te betalen om datalekken te voorkomen of systemen te herstellen.

AI is snel naar voren gekomen als zowel een topprioriteit als een topzorg voor CISO's: 60% van de Nederlandse CISO's zegt dat het mogelijk maken van het gebruik van GenAI-tools een strategische prioriteit is voor de komende twee jaar, zelfs nu de beveiligingszorgen aanhouden. In de VS maakt 80% van de CISO's zich zorgen over mogelijk dataverlies van klanten via openbare GenAI-platforms. In Nederland werd deze zorg weerspiegeld in iets meer dan de helft (52%) van de respondenten. Naarmate de inzet van AI versnelt, verschuiven Nederlandse organisaties van beperking naar governance, waarbij 64% gebruiksrichtlijnen implementeert en 58% AI-gestuurde verdedigingen onderzoekt. Toch is het enthousiasme gedaald ten opzichte van het lokale hoogtepunt van 78% vorig jaar.

"De bevindingen van dit jaar onthullen een groeiende kloof tussen vertrouwen en capaciteit onder CISO's", aldus Patrick Joyce, global resident CISO bij Proofpoint. "Hoewel veel securityleiders optimistisch zijn over de cyberhouding van hun organisatie, vertelt de realiteit een ander verhaal. Toenemend dataverlies, tekortkomingen in gereedheid en aanhoudend menselijk risico blijven de veerkracht ondermijnen. Naarmate de adoptie van GenAI zowel kansen als dreigingen versnelt,

wordt CISO's gevraagd meer te doen met minder, ongekende complexiteit te navigeren en toch te beschermen wat het belangrijkst is. Het is duidelijk dat de rol van de CISO nog nooit zo cruciaal, en zo onder druk, is geweest."

Belangrijkste lokale bevindingen uit Proofpoint's 2025 Voice of the CISO-rapport zijn:

- **Vertrouwen versus realiteit: CISO's bereiden zich voor op aanvallen te midden van toenemend dataverlies en tekortkomingen in gereedheid.** In 2025 voelt 73% van de ondervraagde Nederlandse CISO's het gevaar een materiële cyberaanval te ervaren in de komende 12 maanden (een stijging van 63% vorig jaar), maar geeft 58% toe dat hun organisatie onvoorbereid is om te reageren. Vier op de vijf Nederlandse CISO's (81%) ervoeren het afgelopen jaar materieel dataverlies (een stijging van 45% in 2024) ondanks dat de meerderheid vertrouwen uitsprak in hun cybersecuritycultuur.
- **Aanvallen vanuit alle hoeken, hetzelfde gevolg.** Nederlandse CISO's worden geconfronteerd met een steeds gefragmenteerder dreigingslandschap zonder één dominant risico. Insiderdreigingen, e-mailfraude, malware en ransomware zijn allemaal topzorgen. Ondanks de gevarieerde tactieken leiden de meeste aanvallen tot hetzelfde resultaat: dataverlies. Gezien het risico zegt 57% van de Nederlandse CISO's dat ze zouden overwegen losgeld te betalen om systemen te herstellen of datalekken te voorkomen.
- **Data loopt niet vanzelf de deur uit.** 99% van de Nederlandse CISO's die dataverlies hebben ervaren, zegt dat vertrekkende werknemers een rol speelden. Dit is een stijging van 67% ten opzichte van vorig jaar. Ondanks de bijna universele adoptie van Data Loss Prevention (DLP)-tools, zegt een derde dat hun data onvoldoende beschermd blijft. Naarmate GenAI versnelt, rangschikt 59% van de Nederlandse CISO's informatiebescherming en -governance nu als een topprioriteit, wat een verschuiving naar dynamische, contextbewuste security teweegbrengt.
- **Het menselijke probleem blijft bestaan.** Menselijke fouten blijven de grootste kwetsbaarheid op het gebied van cybersecurity in 2025, waarbij 53% van de Nederlandse CISO's mensen als hun grootste risico noemt, ondanks dat 56% gelooft dat werknemers de beste praktijken op het gebied van cybersecurity begrijpen. Deze kloof benadrukt een kritieke kloof: bewustzijn alleen is niet genoeg. 41% van de Nederlandse organisaties mist nog steeds toegewijde middelen voor insiderrisico's om de kloof tussen kennis en gedrag te overbruggen.
- **Vriend of vijand? AI's tweesnijdend zwaard.** De snelle opkomst van GenAI vergroot de zorgen over menselijk risico. 52% van de Nederlandse CISO's maakt zich zorgen over dataverlies van klanten via openbare GenAI-tools, waarbij samenwerkingsplatforms en GenAI-chatbots worden gezien als de grootste securitydreigingen. Desondanks zegt 60% dat het mogelijk maken van veilig GenAI-gebruik een topprioriteit is – wat een verschuiving van beperking naar governance benadrukt. De meesten reageren met veiligheidsmaatregelen: 64% heeft gebruiksrichtlijnen geïmplementeerd en 58% onderzoekt AI-gestuurde verdedigingen, hoewel het enthousiasme is afgenomen van 78% vorig jaar. Iets

minder dan de helft (49%) beperkt het gebruik van GenAI-tools door werknemers volledig.
- **Bestuursafstemming neemt af naarmate de CISO-druk toeneemt.** De afstemming van het bestuur met Nederlandse CISO's is gedaald van een hoogtepunt van 80% in 2024 naar 59% dit jaar. Toch is aanzienlijke downtime naar voren gekomen als de grootste zorg van besturen na een cyberaanval – gevolgd door verstoring van de bedrijfsvoering en verlies van klanten.
- **Ander jaar, dezelfde druk.** Nederlandse CISO's blijven geconfronteerd worden met toenemende druk in het licht van toenemende dreigingen en beperkte middelen: 55% meldt buitensporige verwachtingen, en 56% zegt dat ze het afgelopen jaar burnouts hebben ervaren of gezien, beide stijgingen van respectievelijk 51% en 43% ten opzichte van vorig jaar. Hoewel 64% nu zegt dat hun organisaties stappen hebben ondernomen om hen te beschermen tegen persoonlijke aansprakelijkheid, heeft 45% nog steeds het gevoel dat ze de middelen missen om hun cybersecuritydoelen te bereiken.

"Artificial intelligence is van concept naar kern gegaan en transformeert hoe zowel verdedigers als tegenstanders opereren", aldus Ryan Kalember, chief strategy officer bij Proofpoint. "CISO's staan nu voor een dubbele verantwoordelijkheid: AI benutten om hun securityhouding te versterken en tegelijkertijd het ethische en verantwoorde gebruik ervan te waarborgen. Deze evenwichtsoefening plaatst hen in het centrum van strategische besluitvorming. Maar AI is slechts een van de vele krachten die de CISO-rol hervormen. Naarmate de dreigingen intensiveren en omgevingen complexer worden, heroverwegen organisaties hoe cybersecurityleiderschap er in de huidige onderneming echt uitziet."

Om het 2025 Voice of the CISO-rapport te downloaden, bezoekt u: [LINK]

Methodologie
Het 2025 Voice of the CISO-rapport biedt een belangrijk perspectief op de stand van zaken op het gebied van cyberbeveiliging vanuit het oogpunt van degenen die zich in de frontlinie bevinden bij het beschermen van mensen en het verdedigen van data. Door meer dan 1.600 CISO's van organisaties met 1.000 of meer werknemers in verschillende sectoren te ondervragen, meet de enquête ook de veranderingen in de afstemming tussen securityleiders en hun raden van bestuur, en onderzoekt hoe hun relatie de securityprioriteiten beïnvloedt. Gedurende het eerste kwartaal van 2025 werden 100 CISO's geïnterviewd in elke markt uit de volgende 16 landen: Nederland, de Verenigde Staten, Canada, Brazilië, Mexico, het Verenigd Koninkrijk, Frankrijk, Duitsland, Italië, Spanje, de Verenigde Arabische Emiraten, het Koninkrijk Saoedi-Arabië, Australië, Japan, Singapore en India.

Over Proofpoint Inc.
Proofpoint, Inc. is een toonaangevend cybersecurity-bedrijf dat de belangrijkste activa en grootste risico's van organisaties beschermt: hun werknemers. Proofpoint helpt bedrijven over de hele wereld met zijn geïntegreerde suite van cloud-oplossingen om gerichte bedreigingen te stoppen, hun data te beschermen en hun gebruikers minder vatbaar te maken voor cyber- aanvallen. Toonaangevende organisaties van elke omvang,

inclusief 85 procent van de Fortune 100, vertrouwen op Proofpoints mensgerichte oplossingen voor security en compliance om hun belangrijkste security- en compliance-risico's te beperken. Dit geldt voor e-mail, cloud, sociale media en het web. Meer informatie is beschikbaar op www.proofpoint.com.

Volg Proofpoint: X | LinkedIn | YouTube