Auteur: Fook Hwa Tan is Chief Quality Officer bij Northwave. Hij is te bereiken via fookhwa.tan@northwave-security.com.

The GREAT 'Risk Reset werd gehouden in Congrescentrum Spant! In Bussum.

The GREAT 'Risk' Reset

Op 16 november 2022 was er een grote bijeenkomst van audit-, compliance-, risk- en security professionals: The GREAT 'Risk'Reset. Het evenement was georganiseerd door ISACA in samenwerking met NOREA, IIA en PvIB. Het was alweer de derde keer dat de conferentie gehouden werd. Door COVID-19 was het lange tijd niet mogelijk zoveel mensen bijeen te brengen om met elkaar te netwerken en kennis te delen. Ondanks vele webinars de laatste jaren was het nu weer prettig om fysiek bijeen te komen.

Het Risk Event, zoals de bijeenkomst in de volksmond wordt genoemd, wordt georganiseerd om professionals bij elkaar te brengen rond het onderwerp risk. Na meer dan twee jaar COVID-19 kon eindelijk weer een groots evenement georganiseerd worden voor meer dan 450 deelnemers. Dat is ook de reden voor de keuze van het thema: The Great 'Risk' Reset. Heeft deze periode van lockdowns, testen en thuiswerken ook in het risicolandschap veel veranderd? Het was de vraag die de sprekers probeerden te beantwoorden en de vraag waarop deelnemers graag een antwoord wilden.

Keynotes en tracks

Het event werd gehouden in Congrescentrum Spant! in Bussum. De conferentie had naast de keynotes, waar iedereen bij elkaar was, ook vier tracks waaruit deelnemers konden kiezen. De onderwerpen van de tracks waren: IT Risk, Emerging Risk, Corporate Risk en Supplier Risk. Hieronder volgt een korte terugblik op de behandelde onderwerpen.

De keynotes gingen over circles of trust, cyber mythe en privacy in de praktijk. Vanuit de circles of trust werd aangegeven uit te zoeken welke stakeholders je hebt en hoe je deze moet beheer-

sen. In de cyber mythe presentatie werd getracht de FUD (Fear, Uncertainty and Doubt) te halen en cybersecurity weer in een positief licht te brengen. Met privacy in de praktijk probeerde de spreker aan te geven dat ondanks de vage wetsteksten organisaties best heel praktisch met privacy om kunnen gaan.

IT Risk track

In de IT Risk track werd gesproken over risico's met betrekking tot cybersecurity, DevOps, Cloud, softwareontwikkeling, purple teaming en human risk. De verschillende sprekers gaven een verscheidenheid aan risico's weer die een connectie hebben met IT. In de afgelopen jaren zijn organisaties door Citrix, aan het begin van 2020, en vervolgens door het thuiswerken als gevolg van COVID-19 versneld verder gaan digitaliseren. Met deze digitale transformatie zijn ook nieuwe risico's geïdentificeerd. De discussie was ook in hoeverre deze risico's nieuw zijn of bekende fenomenen met een iets andere prioriteit. We zien dat IT en digitalisering nog meer boardlevel agendapunten zijn geworden. Dit ofwel door het verder automatiseren van processen ofwel door de toename van cyberaanvallen.

Emerging Risk Track

Bij de Emerging Risk track kwamen nieuwe risico's aan de orde, zoals deepfakes, web 3.0 (DeFi, blockchain, metaverse), ransomware en model risk. Het begon met de beschrijving van risico's met betrekking tot deepfakes. Hoe kunnen we echt van nep onderscheiden? Wat doet het met een medewerker van wie deepfake porno video's of foto's rondgaan op het internet? Wat moet een organisatie hieraan doen, wanneer zij een reputatie wil hooghouden?
Hiernaast werd ook ingegaan op de vele mogelijkheden van de metaverse. Dit zou op afstand werken of ondersteund werken verder kunnen bevorderen. Maar hoe weten we wat echt is en hoe controleren we de berekeningen die zijn gemaakt? Verder werd ook ingegaan op hoe we risico's zouden moeten definiëren in een genetwerkte wereld, waarbij meer naar de impact op bedrijfsfuncties zou moeten worden gekeken in plaats van naar de organisatie als geheel. De context waarin een risico wordt geïdentificeerd zal moeten bepalen hoe het beoordeeld, geëvalueerd en behandeld dient te worden.

Ransomware als opkomend risico werd behandeld op een manier waarbij de deelnemers werden meegenomen in het gehele proces van initiële infectie tot aan de onderhandelingen over het losgeld en het verkrijgen van de decryptor sleutel om alle data weer terug te krijgen. Ook kwam in deze track een interessant verhaal aan bod over de klimaatgevolgen van de benodigde capaciteit voor het minen van cryptovaluta. Voorbeelden werden gegeven van hoe door aanpassingen aan algoritmes de benodigde capaciteit aan rekenkracht kan worden gereduceerd. Dit betekent weer een afname in energiebehoefte van de datacenters die deze capaciteit leveren. Milieubewust leven door te investeren in groene crypto? Iets om over na te denken.

Corporate Risk track

Risico's met betrekking tot Avg, algoritmes, ethiek, interne audit, gedrag en EU-wetgeving vormden de basis van de sessies binnen de Corporate Risk track. Vanuit wet- en regelgeving werd bekeken met welke nieuwe risico's organisaties rekening moeten houden. Maar er werd ook gekeken naar de kansen die de nieuwe ontwikkelingen met zich meebrengen. Een van de sprekers behandelde hoe haar organisatie omgaat met behavioural risk. Ze ging in op het identificeren van dit soort risico's en het beheersen hiervan door te sturen op de gewenste cultuur. Ook werd ingegaan op de kansen en mogelijkheden door het gebruik van algoritmes. Deze algoritmes zullen een verdere transitie in de samenleving teweegbrengen met betrekking tot slimmer werken, mobiliteit, geneeskunde en onderwijs. Vanuit het perspectief van een interne audit werd gekeken naar een overzicht van risico's voor het nieuwe jaar 2023.

Supplier Risk track

De vierde track ging over de Supplier Risk, een onderwerp waarover in de markt veel gesproken wordt. Sprekers bespraken risicomanagement met betrekking tot derden, gebruik van AI, leveranciersmanagement, statelijke actoren, circles of trust en nationale ketens. Hierbij werd duidelijk weergegeven dat een organisatie niet alléén functioneert en zeker rekening moet houden met stakeholders in de gehele keten. De vraag was hoever gaat de keten en hoe diepgaand moet je daarbij onderzoeken? In hoeverre vertrouw je op de organisaties waarmee je samenwerkt en hoeveel controle moet je hierbij uitvoeren? Van software tot hardware tot producten en diensten moet je weten wat je verwacht van een leverancier. Dit moet je niet eenmaal toetsen, maar continu.

Conclusie: prioriteit bepalen

Vele risico's zijn de revue gepasseerd, waarbij veelal nieuwe perspectieven werden gegeven op bestaande en bekende risico's. Ik denk dat uiteindelijk de boodschap was dat de wereld is veranderd en dat daarmee het landschap aan risico's is veranderd. Hierbij wordt eenieder aangemoedigd om voor de eigen organisatie te bepalen welk risico prioriteit heeft en daarbij een keuze te maken welk risico behandeld dient te worden in 2023!