tijdsgebonden risicos vangen in metaforen

maart 2020

Arno Nuijten en Mark van Twist

Interne auditors rapporteren over risico's, zodat de organisatie een beeld heeft wat haar te wachten staat en tijdig actie kan ondernemen. Maar juist de tijdsdimensie ontbreekt in de manier waarop auditors over risico's rapporteren. In deze bijdrage verkennen wij het gebruik van metaforen om de tijdsgebonden risico's in de IT-systemen van een organisatie te benoemen.

Het signaleren van en rapporteren over risico's staat centraal in de werkzaamheden van interne auditors. Voor de duiding en opvolging van risico's wordt vaak gebruik gemaakt van de formule 'kans x impact' van een gebeurtenis. Hierbij blijft een wezenlijk kenmerk van risico's naar ons idee buiten beeld, namelijk hoe de temporele dimensie van risico's zich ontwikkelt. Een risico kan zich heel plotseling voordoen en dan ineens veel schade veroorzaken, maar kan ook juist een heel geleidelijk proces op gang brengen waarvan de schade langzaam steeds groter wordt. Verder kan het bijvoorbeeld zijn dat de aanvangsschade heel hoog is en de vervolgschade klein, of juist andersom.

Ook de kans dat een risico zich manifesteert is allerminst een statisch gegeven, maar wordt bijvoorbeeld gevormd door het menselijk handelen in de organisatie, onbedoelde fouten, olifantenpaadjes, ongelukkige timing en het onderdrukken van symptomen wanneer risico's zich aandienen. Zeker bij de snelheid van hedendaagse IT-systemen kunnen risico's zich razendsnel ontwikkelen en neemt het belang van de tijdsdimensie dus verder toe.

Meer taal nodig

Kortom, we hebben meer taal nodig om tijdsspecifiek over risico's te rapporteren, bijvoorbeeld over risico's die de organisatie loopt in haar vitale IT-systemen. Behalve de kans en de impact is ook de manier waarop deze zich in de tijd manifesteren relevant. In het auditvak hebben we maar heel weinig woorden om risico's door de tijd te typeren. Een mogelijkheid om nieuwe taal te ontwikkelen op dit vlak is metaforen aan een andere discipline te ontlenen. Dat kan bijvoorbeeld door IT-systemen als 'vitale functies' te zien die wezenlijk zijn voor het gezond functioneren van de organisatie en risico's te beschouwen in termen van pijnprikkels die hieruit voortvloeien.

In deze bijdrage gaan wij op zoek naar woorden die tot uitdrukking kunnen brengen hoe risico's zich in de loop der tijd kunnen ontwikkelen. We zijn daarbij op zoek gegaan naar krachtige metaforen die kunnen helpen om symptomen te herkennen, gebeurtenissen in de tijd te plaatsen en daarmee behulpzaam te zijn om op het juiste moment de juiste interventie te plegen. We hebben niet de illusie een volledige taxonomie te schetsen van de tijdspatronen waarin risico's zich kunnen ontwikkelen. Wel beogen we enkele herkenbare metaforen aan te reiken die in de praktijk van auditors bruikbaar kunnen zijn in de communicatie met het management. Om die reden lichten we een en ander steeds toe aan de hand van anekdotes die ontleend zijn aan onze praktijk.

De migraineaanval in de organisatie – poging tot uitstel van pijn verhoogt de kans dat ernstige risico's optreden

Anekdote:
Het klantinformatiesysteem lijkt zo nu en dan even te haperen, maar 'besluit' gelukkig telkens weer om de ingevoerde queries te presenteren aan de gebruikers. De doorgewinterde gebruikers weten dat dit een aankondiging is dat het systeem binnen niet al te lange tijd 'down' kan gaan. Dat gebeurt wel vaker in een periode van drukte. Een reden dus om nog even wat extra werk te verzetten dat niet mag blijven liggen. En zeker op de momenten dat het systeem weer even de snelheid te pakken heeft, gaat iedereen er weer tegenaan, nu het nog kan. Een storing zou nu wel heel slecht uitkomen. De systeembeheerder ziet inmiddels serieuze foutmeldingen op zijn scherm: delen van 'het geheugen' zijn slecht toegankelijk en geven 'time-out'-meldingen, 'buffers lopen vol'. Gebruikers beginnen te bellen om ondersteuning en maken massaal schermafdrukken, zodat ze nog kunnen redden waar ze mee bezig waren. Het systeem gaat plat.

De anekdote laat een patroon zien waarlangs risico's zich in de tijd ontwikkelen totdat een grenswaarde wordt overschreden, uitmondend in een migraineachtige situatie waarin de informatieverwerking, en daarmee het normaal functioneren van de organisatie, tot stilstand komt en niets anders rest dan de tijd te nemen voor herstel zodat normale 'informatie-uitwisseling' weer mogelijk wordt. In deze anekdote dienen symptomen in het functioneren van het informatiesysteem zich aan als 'voorbode' voor het plat gaan van het systeem. Zoals slaperigheid, prikkelbaarheid, vermoeidheid en slechte concentratie doorgaans als aankondiging dienen van een migraineaanval. Dit lokt vaak uit tot de neiging om 'nog snel even' allerlei belangrijke zaken af te werken nu het nog kan en vooralsnog te trachten om de symptomen te onderdrukken. Juist deze handelswijze, gedomineerd door de naderende impact van migraine, verhoogt de kans dat de migraine uiteindelijk toeslaat en werkt derhalve averechts. Het wegnemen of verminderen van de factoren die bijdragen aan de migraine zou meer effectief geweest zijn.

In de beschreven anekdote zou het gebruik van een metafoor als de migraineaanval in de auditrapportages naar ons idee uitnodigen om in een eerder stadium acties te ondernemen die het gebruik en daarmee de belasting van het informatiesysteem enigszins temperen. Daarmee creëer je de gelegenheid om gericht te werken aan technische en organisatorische factoren die het probleem in het informatiesysteem veroorzaken.

Secundaire 'pijn op de borst' in de organisatie – waarschuwing dat vitale functies worden veronachtzaamd

Anekdote:
Het bedrijf heeft een historie van vele overnames van collegabedrijfjes. De krachtsinspanning om de grootste en de sterkste te worden is tekenend voor de ambitie van dit bedrijf. Vanwege deze historie en de snelheid die ermee gepaard gaat, is de interne bedrijfsvoering van deze organisatie belast met een versnipperd landschap aan informatiesysteempjes en IT-functionarissen die deze systemen beheren. Signalen dat de overnamedrift beter zou kunnen worden getemperd om de interne organisatie op orde te brengen, vinden niet echt een voedingsbodem. Het noodzakelijke onderhoud op deze informatiesystemen waarop 'de techneuten' van het bedrijf attenderen, sneuvelt in de prioriteiten van alledag om juist nieuwe koppelingen te realiseren met systemen van overnamekandidaten. Het realiseren van dergelijke koppelingen lijkt steeds moeizamer te gaan en steeds meer tijd in beslag te nemen. De organisatie heeft inmiddels besloten om een externe IT-leverancier in de arm te nemen en de IT-functionarissen en de verantwoordelijkheid voor de informatiesystemen daar onder te brengen. De juristen van het bedrijf zijn druk doende een scherp contract op te stellen, zodat de leverancier kan worden aangesproken bij onvoldoende prestaties en ook het onderhandelen van de prijs gaat op scherp.

De problemen in de IT-systemen van dit bedrijf zijn meer de zijdelingse uiting van een naastgelegen – veel ernstiger – probleem en zijn daarom te beschouwen als een 'secundaire pijn'. De pijn op de borst staat niet op zichzelf, maar wijst op een probleem met een naastgelegen vitale functie: het hart. In het streven naar efficiëntie en beheersing zoeken organisaties hun toevlucht tot standaardisatie en bundeling. We standaardiseren processen zodat ondoelmatige varianten worden weggesneden. En we creëren dienstencentra of besteden activiteiten uit aan die ene partij. Zo ontstaat de beweging dat ook de bijbehorende risico's zich clusteren op dergelijke vitale plaatsen. Net als bij het dichtslibben van de bloedtoevoer van het hart zijn het juist de reeds bestaande vernauwingen die zorgen voor verdere vernauwingen op diezelfde plaats. Risico's klonteren samen op plaatsen waar ze het meeste schade aanrichten.

In de beschreven anekdote heeft de organisatie zichzelf een 'ongezonde' gewoonte eigen gemaakt door de bedrijfsvoering – het hart van de organisatie – te veronachtzamen en signalen te negeren. De problemen werden afgewenteld op een kleine groep 'techneuten' die uiteindelijk werden overgedragen aan die ene leverancier die ook nog eens de

duimschroeven werd aangedraaid en die dus kunst- en vliegwerk moet verrichten om de dienstverlening op peil te houden. Alle risico's werden hiermee samengebracht bij die ene leverancier wiens falen vitale gevolgen voor de organisatie zou hebben.

Het gebruik van de metafoor van de secundaire 'pijn op de borst' in de auditrapportages toont dat problemen in de IT-systemen worden veroorzaakt door de gewoonte om bedrijfsvoeringaspecten te negeren bij bedrijfsovernames. De organisatie zal deze ongezonde gewoonte moeten bijstellen en meer terughoudend moeten worden om risico's bij een enkele externe partij te beleggen.

Hoge bloeddruk in de organisatie – sluipmoordenaar die uiteindelijk een beroerte kan veroorzaken

Anekdote:
De productie ligt stil vanwege problemen met het CAD/CAM-systeem. Razendsnel wordt de IT-beheerder opgetrommeld om het informatiesysteem en daarmee de productie weer operationeel te krijgen. Er is een probleem met een verkeerd geïnstalleerde patch van de toepassing. Een volledige herinstallatie zou een lange periode van stilstand vragen, dus daarom wordt gewerkt met een work-around om deze 'brand te blussen'. En zo gaat het al tijden: de beheerders zijn voortdurend bezig met brandjes blussen, maar binnen de kortste keren steken de problemen de kop weer op, op andere plaatsen in de organisatie. Het rennen van incident naar incident verhindert dat er tijd en rust wordt gevonden om de samenhang tussen de incidenten en daarmee het onderliggende probleem te onderzoeken, en een structurele oplossing te implementeren.

In het streven naar snelle oplossingen voor acute problemen zoeken organisaties hun toevlucht tot incidentmanagement en komen daarbij 'net niet toe' aan het aanpakken van de problemen. Ze houden daarmee het patroon van het voortdurend oplaaien van incidenten in stand. Medewerkers die graag 'brandweerman' spelen kunnen zich koesteren in deze drukke en dankbare bezigheid. De spanning bouwt zich echter in de loop van de tijd op. Hoge bloeddruk is een sluipmoordenaar die niet meteen acute problemen oproept en die zonder pijnstillers heel lang valt uit te houden. Op termijn kan hoge bloeddruk echter via symptomen van drukkende en knellende pijn voor grote problemen zorgen. Zoals bij een beroerte, waarbij een ogenschijnlijk onbeduidend klein incident (bloedpropje) onverwacht grote gevolgen kan hebben en vitale hersenfuncties kan beschadigen.

Het gebruik van deze metafoor zou in de beschreven anekdote uitnodigen om incidenten, noodreparaties en kleine succesjes te onderscheiden van problemen, structurele oplossingen en grote successen. Planmatige aanpak van problemen in plaats van de waan van het moment. Investeren in extra capaciteit om de druk op de organisatie te verminderen. Maar bovenal: het doorbreken van gewoonten die de problemen aanwakkeren.

Clusterhoofdpijn in de organisatie – uitschakeling door het plotsklaps optreden van snijdende, haast ondraaglijke pijn

Anekdote:
Door onhandige politieke beslissingen heeft het land waar uw organisatie is gevestigd, zich de woede op de hals gehaald van een buitenlandse mogendheid die bekendstaat om de cyber attacks die zij eerder heeft gepleegd. De dreiging van een DDOS-aanval op uw systemen is daarmee meer prominent dan ooit. Echter, het is niet duidelijk of juist uw organisatie of die van een andere partij gaat worden aangevallen. U moet voorbereid zijn op de gebeurtenis, maar hoe precies is nog de vraag.

De beschreven situatie kan worden uitgedrukt in de metafoor van de clusterhoofdpijn. Een zeer plotselinge, snijdende ondraaglijke pijn die het ingewikkeld maakt om de symptomen te zien en die zich manifesteert in specifieke delen van het hoofd en lichaam. De clusterhoofdpijn is immens en u weet dat het u kan overkomen, maar u weet niet wanneer het u gaat treffen. Het enige wat u kunt doen is u prepareren voor het geval dat deze extreme pijn toeslaat (voldoende pure zuurstof onder persdruk binnen handbereik hebben).

Het gebruiken van de metafoor van de clusterhoofdpijn in de auditrapportages zou in de beschreven anekdote uitnodigen om de meest vitale onderdelen van de organisatie te beschermen tegen de verwoestende externe impact, en nauwgezet alle beschikbare informatie te monitoren. U heeft voor zover bekend geen invloed op de kans dat de clusterhoofdpijn u treft, het enige wat u kunt doen is de schade beperken als het gebeurt.

Consequenties voor de interne auditor

In dit artikel hebben we een aantal – in dit geval medische – metaforen geïntroduceerd die bruikbaar kunnen zijn in de communicatie met het management over het tijdsgebonden gedrag van risico's in een organisatie. Dat gedrag ontstaat veelal uit een cyclisch patroon waarin actoren (mensen en systemen) in een organisatie op elkaar reageren, waardoor risico's zich in de tijd volgens een herkenbaar patroon ontwikkelen. Concepten uit een ander domein dan dat van de auditor kunnen helpen om het besef van tijd (urgentie, korte termijn versus lange termijn) onderdeel te maken van de rapportage over risico's. Dit maakt het mogelijk om symptomen van een risicopatroon vroegtijdig als zodanig te herkennen en te acteren op de onderliggende problemen en patronen, in plaats van te reageren op de individuele symptomen. Het herhalend karakter in die symptomen kan behulpzaam zijn voor de auditor bij de timing van zijn boodschap met het oog op het herkennen en doorbreken van het patroon dat zich aftekent.

Migraine, pijn op de borst, hoge bloeddruk, clusterhoofdpijn: het gebruik van dergelijke metaforen kan helpen om een meer verfijnde communicatie over het optreden van risico's door de tijd te duiden, en daarmee de ontwikkeling van een geëigende aanpak daarvoor. Daarmee kunnen ze ook behulpzaam zijn voor organisaties om het tijdsaspect te incorporeren in de acties die zij nemen om risico's in overeenstemming te houden met de organisatiedoelen. Bij een risico gaat het om 'kans x impact', maar veel valt er niet te doen met dit inzicht zonder goed begrip van hoe dat risico zich kan en zal manifesteren in de tijd…

Prof. dr. A.L.P. (Arno) Nuijten RE CISA CIA | Bijzonder hoogleraar bij *Open Universiteit en ESAA*

Arno Nuijten is bijzonder hoogleraar Behavioral IT Governance aan de Open Universiteit en initiatiefnemer van het expertisecentrum Behavioral Risk binnen Erasmus School of Accounting and Assurance (ESAA). Tevens was hij wetenschappelijk directeur van de IT Auditing & Advisory-opleiding aan ESAA en organiseert hij nationaal en internationaal onderzoeksinitiatieven op het snijpunt van risicogedrag, IT en interne audit.

Prof. dr. M.J.W. (Mark) van Twist | Directeur bij *Erasmus Universiteit Rotterdam, opleiding Internal Auditing & Advisory*

Mark van Twist is hoogleraar bestuurs- en beleidsadvisering op het grensvlak van publiek en privaat aan de Erasmus Universiteit Rotterdam en wetenschappelijk directeur van de Internal Auditing & Advisory-opleiding aan Erasmus School of Accounting & Assurance (ESAA). Daarnaast is hij onder meer voorzitter van de Orde van Organisatie Adviseurs (OOA).