Drs. Alex Hoogteijling RE CISA MBCI

Datamanagement in relatie tot BCM

Bij datamanagement in relatie tot bedrijfscontinuïteitsmanagement (BCM) wordt al gauw gedacht aan het maken van back-ups en het herstellen van data. Binnen BCM speelt datamanagement echter een veel grotere rol en kan het zelfs worden ingezet om calamiteiten te voorkomen.

Het BCM-proces richt zich op het versterken van het weerstandsvermogen en de veerkracht van organisaties ter voorbereiding op bedreigingen die de bedrijfsvoering kunnen verstoren, zoals brand, ICT-uitval of stroomstoring. In dit managementproces worden continuïteitsbedreigingen geïdentificeerd en wordt de impact hiervan op de bedrijfsvoering geanalyseerd. Dit leidt, afhankelijk van onder andere de risicobereidheid van een organisatie, tot de implementatie van continuïteitsmaatregelen (preventief, detectief, repressief en/of correctief) om bijvoorbeeld de kans op verstoringen en de gevolgen hiervan te verlagen of de verstoringsduur te verkorten.
Enkele voorbeelden van continuïteitsmaatregelen zijn het implementeren van een noodstroomvoorziening, het documenteren en testen van noodprocedures en het redundant (dubbel) uitvoeren van ICT-systemen. Of dergelijke maatregelen afdoende zijn dient periodiek te worden beoordeeld via management reviews en internal audits. Bevindingen uit dergelijke controles zouden idealiter moeten leiden tot correctieve maatregelen op het gebied van bedrijfscontinuïteit.

Dataverslaving
Aangezien organisaties in toenemende mate afhankelijk zijn van ICT en informatie, is het niet meer dan logisch dat continuïteitsmaatregelen zich ook richten op de beschikbaarheid van betrouwbare informatie in geval van een calamiteit. Vroeger beperkte dit zich tot het maken van een back-up van slechts een selectie van data op een tape (onder andere vanwege de kostprijs van tapes en de lange tijdsduur voor het maken van back-ups). Deze tapes werden niet eens altijd dagelijks extern opgeslagen. Het terugplaatsen van data werd bovendien slechts sporadisch getest.
In het huidige tijdperk van virtualisatie en cloud computing is er nauwelijks meer een drempel om data real-time op meerdere plaatsen tegelijk op te slaan. Zelfs voor particulieren is dit routine geworden dankzij diensten als iCloud, OneDrive en Dropbox.
Wij beschouwen het tegenwoordig als vanzelfsprekend dat wij overal en altijd bij onze data kunnen. Je zou zelfs kunnen stellen dat wij hier verslaafd aan zijn geraakt. Zodra zich hierin ook maar even een verstoring voordoet weten we ons geen raad. We schakelen dan massaal over naar een afwachtende modus totdat de ICT-problemen weer zijn verholpen. Creativiteit om toch het werk op een alternatieve wijze voort te zetten is dan vaak ver te zoeken.
Men is zelfs zo gewend geraakt aan digitale informatie-(verwerking) dat het terugvallen op 'papieren workarounds' in veel gevallen ondenkbaar is geworden. Zo is bij verzekeraars het claimafwikkelingsproces en de verzekerdenadministratie tegenwoordig in hoge mate gedigitaliseerd. Informatie zoals polissen, claimaanvragen, klantendossiers en claimbeoordelingscriteria zijn vaak niet eens meer op papier beschikbaar. Bij ICT-uitval of andersoortige verstoring waarbij deze data tijdelijk ontoegankelijk is ligt de gehele bedrijfsvoering stil, wat vervolgens voor een enorme improductiviteit zorgt. Daar komt nog eens de schade als gevolg van omzetderving, negatieve publiciteit en eventuele claims voor het niet of te laat nakomen van afspraken bovenop. Dit probleem doet zich niet alleen voor bij dienstenleveranciers, maar ook bij productiebedrijven. Het primaire productieproces valt bij veel bedrijven al snel stil als informatie over bijvoorbeeld bestelorders, productieplanningen en voorraden niet beschikbaar is.

Crisismanagementdata
Niet alleen voor het continueren van de bedrijfsvoering zijn organisaties in grote mate afhankelijk van informatietoegang, maar ook voor het managen van de calamiteit zelf en de crisiscommunicatie hieromtrent. Het tijdsaspect speelt daarbij een belangrijke rol. In het eerste uur direct na een calamiteit dienen namelijk meteen al belangrijke besluiten te worden genomen. Ook verwachten stakeholders zoals medewerkers, klanten, businesspartners en media direct geïnformeerd te worden. Informatie die hiervoor benodigd is wordt vaak gebundeld in een bedrijfscontinuïteitsplan. Zo'n bedrijfscontinuïteitsplan bevat onder meer gedocumenteerde noodprocedures, recovery (herstel) procedures, workaroundformulieren, crisiscommunicatieprotocollen, contactgegevens van belangrijke stakeholders (waaronder toeleveranciers) en checklists voor specifieke crisisscenario's.
Dergelijke informatie dient in geval van een calamiteit natuurlijk wel beschikbaar te zijn. Hier moet Internal Audit bijzonder alert op zijn. Het komt namelijk nogal eens voor dat een bedrijfscontinuïteitsplan verloren gaat in de calamiteit of dat de digitale versie alleen benaderbaar is voor een beperkt aantal personen dat vanwege de calamiteit hier niet direct bij kan. Dit is een beetje te vergelijken met het maken van een back-up, maar deze in dezelfde ruimte bewaren als de primaire databestanden.

Voorkom datalekkage
Tijdens calamiteiten zijn organisaties kwetsbaarder voor fouten en misbruik waardoor zich, bovenop de bestaande crisissituatie, nieuwe ongewenste gebeurtenissen kunnen voordoen. Denk daarbij aan diefstal van laptops, USB-sticks of complete servers met bedrijfs-, privacy, of medisch gevoelige informatie uit een bedrijfspand dat is getroffen door een brand. Dat bedrijfskapitaal (waaronder data) verloren is gegaan als gevolg van de calamiteit is op zich al een ramp. Hier biedt een schadeverzekering in sommige gevallen echter nog enige pijnverlichting. Maar als vertrouwelijke dossiers ineens op straat liggen, dan heb je als organisatie toch het een en ander uit te leggen. Dit is dan een crisis bovenop een crisis.
In een bedrijfscontinuïteitsplan dienen dus instructies te zijn opgenomen rondom het beveiligen van een getroffen vestiging zodra overheidshulpdiensten de locatie hebben verlaten. Denk daarbij aan het plaatsen van hekken, het inzetten van beveiligers en het veiligstellen van informatiedragers (digitaal en papier). Internal Audit dient vast te stellen of

In perioden van verstoringen moeten internal auditors alert zijn op data integriteitsissue

dergelijke instructies in het bedrijfscontinuïteitsplan zijn opgenomen. Helemaal mooi zou het zijn als internal auditors ten tijde van een calamiteit ook ingezet worden om het crisisteam scherp te houden en te checken of alle instructies ook worden nageleefd.
De internal auditor kan bij een calamiteit er bijvoorbeeld op toezien dat informatiedragers die ogenschijnlijk als verloren beschouwd kunnen worden, niet argeloos bij het grofvuil worden geplaatst. Het is namelijk goed mogelijk dat de data hierop nog door gespecialiseerde salvagebedrijven kan worden hersteld. Indien dit niet meer het geval is dient de informatiedrager definitief te worden vernietigd zodat eventueel misbruik hiervan ook echt niet meer mogelijk is.
Het risico op ongewenste verspreiding van data doet zich overigens niet alleen direct na een calamiteit voor. Ook in de daaropvolgende periode waarin noodproductie- en herstelactiviteiten plaatsvinden bestaat dit risico. Tijdens een noodproductie- of uitwijksituatie ontbreekt het namelijk vaak aan adequate informatiebeveiligings- en controlemaatregelen. Ook wordt gewerkt volgens noodprocedures waarmee niet iedereen even bekend is. Dit alles leidt tot een verhoogde kans op procedurele fouten, onjuiste of onvolledige informatieverwerking, beveiligingsincidenten door misbruik van de situatie en mogelijk zelfs lekken van informatie of diefstal hiervan.

Van belang is dat een organisatie zich bewust is van dergelijke risico's en hieraan in het bedrijfscontinuïteitsplan ook aandacht besteedt. Hier is weer een belangrijke controlerende rol voor de internal auditor weggelegd. Zo dient bij een tijdelijke verruiming van bevoegdheden erop toegezien te worden dat hier geen misbruik van wordt gemaakt. Dit zou bijvoorbeeld het geval kunnen zijn bij het versneld inkopen van vervangende bedrijfsmiddelen waarbij bepaalde controlestappen uit de reguliere inkoopprocedure worden overgeslagen. Bij terugkeer naar de business-as-usualsituatie, moet een organisatie dergelijke brede bevoegdheden weer inperken, workaroundprocedures beëindigen en controls weer heractiveren.

Nazorg datamanagement
Bij herstel van data en terugkeer naar de reguliere gang van zaken dient nog wel goed gecheckt te worden of alle data ook juist en volledig zijn hersteld. Naast technische verificatie hiervan is een gebruikersacceptatietest geen overbodige luxe. Internal Audit zal in perioden waarin zich verstoringen

hebben voorgedaan alert moeten zijn op data-integriteitsissues. Indien toch data verloren is gegaan, is reproductie hiervan wellicht mogelijk via andere bronsystemen, papieren dossiers, poststukken en e-mails. In een uiterst geval zal een organisatie ook gegevens opnieuw moeten opvragen bij businesspartners of klanten.
Overigens dient niet alleen de recovery van primaire data te worden geverifieerd maar ook die van instellingen rondom toegangsbeveiliging, logging, functiescheiding, et cetera. Onder tijdsdruk kan het namelijk gebeuren dat vergeten wordt de standaard inlogcredentials van een 'admin' account van een nieuw aangeschafte server aan te passen. Ongeautoriseerde personen zouden zich zo toegang kunnen verschaffen en ongewenste handelingen kunnen verrichten waaronder het aanpassen van beveiligingsinstellingen, datadiefstal, sabotage en het bewerken van transacties.
Na herstel van systemen en data zal een eventuele achterstand in de informatieverwerking moeten worden weggewerkt. Informatie die tijdens de crisissituatie als workaround tijdelijk is vastgelegd op papieren formulieren of spreadsheets, dient overgezet te worden in de herstelde bedrijfsapplicaties. Dit is een foutgevoelig proces dat ook nog eens verstoord kan worden doordat gebruikers weer hun reguliere werkzaamheden in de applicaties uitvoeren. De kans op conflicten of dubbele invoer wordt hierdoor vergroot. Idealiter zou eerst de informatie volledig moeten zijn bijgewerkt voordat de applicatie wordt vrijgegeven voor gebruik. Het is denkbaar dat dit geduld niet altijd kan worden opgebracht.

Inzet big data bij BCM
Datamanagement bij BCM is niet alleen belangrijk met het oog op herstellen, verwerken en beveiligen van informatie, maar het kan ook worden ingezet bij het bestrijden van calamiteiten. Vooral ICT-verstoringen kunnen hierdoor worden beperkt. Door het analyseren van data afkomstig van verschillende sensoren en early warning systems, kan nog tijdig worden ingegrepen indien bijvoorbeeld een harde schijf dreigt te crashen of een server oververhit dreigt te raken. In de praktijk wordt al volop gebruiktgemaakt van dergelijke analyses voor het inplannen van onderhoud aan apparatuur en technische installaties.
Voor het voorkomen van andere type verstoringen wordt big data op dit moment nog niet of nauwelijks ingezet, terwijl hier toch wel degelijk mogelijkheden voor zijn. Denk bijvoorbeeld aan productieverstoringen als gevolg van problemen bij een toeleverancier. Een brand bij een leverancier is lastig voorspelbaar, maar veel andere problemen hebben een langere aanloopperiode waarvoor soms ook data beschikbaar is. Denk daarbij aan financiële problemen bij een leverancier, het niet kunnen leveren vanwege een boycot, levering vanuit een conflictgebied of staking door personeel. Door analyse van data uit diverse bronnen (nieuwsberichten, kredietbeoordelaars, betalingsgedrag uit eigen administratie) kan een organisatie dergelijke problemen bij toeleveranciers mogelijk eerder zien aankomen.
Ervaringsgegevens van verstoringen die zich hebben voorgedaan kunnen ten slotte worden gebruikt voor het verder verbeteren van analyses zodat organisaties de kans op toekomstige verstoringen nauwkeuriger kunnen inschatten.

Conclusie
Datamanagement en de rol van Internal Audit hierin is van essentieel belang voor bedrijfscontinuïteitsmanagement. Zowel in de voorbereiding op calamiteiten als de afwikkeling daarvan. Indien men hier steken laat vallen dan kan dat resulteren in een crisis bovenop een crisis. Het gaat daarbij om meer dan alleen het tijdelijk niet beschikbaar zijn van vitale data. Denk bijvoorbeeld aan het lekken van bedrijfs-, privacy, of medisch gevoelige informatie doordat informatiedragers na een calamiteit niet zijn veiliggesteld of beveiligingsinstellingen niet juist zijn geconfigureerd op uitwijkapparatuur. Tijdens crisissituaties is er bovendien een verhoogde kans op procedurele fouten, onjuiste/onvolledige informatieverwerking en misbruik van de situatie.
Internal Audit zou bij het implementeren van bedrijfscontinuïteitsmanagement de beheersmaatregelen rondom dergelijke datamanagementrisico's moeten beoordelen. Tijdens een daadwerkelijke calamiteit kunnen zij het crisisteam ondersteunen door te verifiëren of recovery van data en configuraties correct heeft plaatsgevonden en of afgesproken noodprocedures met bijbehorende controls daadwerkelijk worden nageleefd. <<

Big data kan ook worden ingezet bij het bestrijden van calamiteiten

Alex Hoogteijling is directeur en consultant bedrijfscontinuiteit bij Hoogteijling Management Consultancy. Hij is specialist op het gebied van business continuity management. alexhoogteijling@bcmspecialist.nl