Gids voor Risicobeheersing

BEDRIJFSCONTINUÏTEIT MANAGEMENT – WAT IS HET?

Introductie

Hoewel een verzekering de kosten kan compenseren die zijn gemaakt als gevolg van verstorende incidenten, is dit niet de enige beperking waarop u moet vertrouwen. Incidenten kunnen ook een impact hebben op gebieden die niet verzekerd zijn, zoals uw reputatie, aandelenkoers, consumenten- en marktvertrouwen, de kosten van het beheren van het incident, en onverwachte kosten.

Bedrijven moeten een robuust raamwerk voor Bedrijfscontinuïteit Management (BCM) implementeren dat helpt bij het identificeren en beperken van risico's voordat ze verstorend gaan werken, en dat ook een tijdig en effectief herstel mogelijk maakt wanneer ze dat wel doen.

Stel uzelf de vragen in dit document en overweeg hoe goed uw bedrijf is voorbereid om het hoofd te bieden aan verstoringen, het herstellen van verstoringen en een veerkrachtiger organisatie te worden in het proces.

Wat is Bedrijfscontinuïteit Management?

BCM is een managementactiviteit die zich richt op de prioritaire behoeften van het bedrijf.

Het bereidt oplossingen voor die helpen bij het tijdig detecteren, reageren op, beheren en herstellen van eventuele storingen; om de activiteiten voort te zetten tot een afgesproken niveau, ongeacht de aard van het incident.

BCM verbetert ook de organisatorische veerkracht van een bedrijf door:

- Risicobeheer dat helpt om de noodzaak om een BCM-plan in werking te stellen, te verminderen
- Een herstel- en responsstructuur om die risico's te beheersen die niet kunnen worden voorkomen of voorspeld, of waar mitigatie mislukt

Wat betekent dit voor u?

BCM betekent dat u weet welke onderdelen van uw bedrijf belangrijk voor u zijn, wat er zou gebeuren als u ze verliest, hoe u ze kunt verliezen en wanneer en hoe u ze weer aan de praat kunt krijgen.

Enkele voordelen van BCM zijn:

- Minder risico voor uw productiviteit, omzet, merknaam en reputatie
- Onderbroken operaties kunnen sneller weer online zijn
- Meer zichtbaarheid van belangrijke processen, risico's, toeleveringsketen en andere vitale afhankelijkheden
- Meer vertrouwen bij personeel, klanten en partners in uw vermogen om te presteren tijdens en na incidenten
- Het kan helpen bij het verminderen van contractuele en serviceniveau-inbreuken, en boetes
- Concurrentievoordeel
- Het is een goed verkoopargument en kan een voorwaarde zijn voor sommige nieuwe klanten
- Mogelijke verlaging van verzekeringspremies
- Het analyseren van de workflow en de onderlinge afhankelijkheden van activiteiten kan helpen bij het identificeren van risico's, inefficiënties, en beveiligings- en veiligheidsproblemen in alle delen van het bedrijf

Wie moet er bij BCM worden betrokken?

Naast het hebben van de benodigde middelen om het BCM-raamwerk op te bouwen en te onderhouden, is het belangrijk dat het bedrijf het senior management volledig hierin meeneemt; op deze manier zijn zowel personeel als management volledig betrokken bij BCM.

Management inkoop

Zorg ervoor dat het Senior Management Team (SMT) en senior belanghebbenden betrokken zijn bij BCM, aangezien het moet worden afgestemd op hun algemene bedrijfsdoelstellingen en -strategieën.

BCM Beleid

Er moet een formeel BCM-beleid worden opgesteld dat de SMT-eigendom van BCM erkent en de doelstellingen, reikwijdte en de rollen en verantwoordelijkheden van alle betrokkenen bij BCM definieert.

Rollen en verantwoordelijkheden: er zal een aantal rollen moeten worden gevormd, met duidelijke begeleiding en training voor elk:

- Een incident response (IR) team
- Een BCM-team - één team, of een 'gelaagd' aantal BCM-teams.
- Een BCM-coördinator / manager / lead
- Afdeling BCM-vertegenwoordigers

Wat is belangrijk voor uw bedrijf?

Voordat herstelplannen worden geïmplementeerd, is het van cruciaal belang om te weten wat de belangrijkste bedrijfsonderdelen zijn en wat de SMT-prioriteiten zijn.

Om te begrijpen wat belangrijk is voor het bedrijf, moet u weten hoe het hele bedrijf werkt.

Wat doet u?

U moet eerst samenwerken met de SMT om akkoord te gaan:

- Wat de belangrijkste producten / diensten zijn voor uw bedrijf
- Wat de impact van hun verlies in de loop van de tijd zou zijn - productiviteit, omzet, reputatie, invloed op de effecten stroomopwaarts / stroomafwaarts in het bedrijf, klantvertrouwen, en personeel
- Wie de belangrijkste klanten, partners en andere belanghebbenden zijn
- Hoe klanten en concurrenten zullen reageren op verstoring
- De belangrijkste tijden van het jaar waarin het bedrijf opereert en wanneer de vraag / productie hoger is
- Een tijdlijn voor herstel - wanneer moet elk worden hersteld na een storing, in welke volgorde en in welke mate

De term voor dit werk is een 'business impact analyse (BIA)' en moet beginnen met deze strategische visie van SMT.

Hoe doet u het?

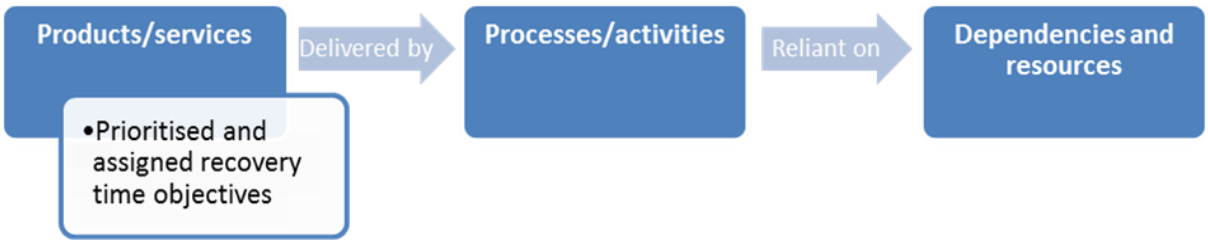
Gewapend met deze SMT-visie op de herstelprioriteiten, moet u een grondig begrip krijgen van hoe het bedrijf werkt en wat de verschillende onderlinge afhankelijkheden zijn. Ga naar degenen in het bedrijf die begrijpen hoe dit alles wordt geleverd en bepaal van hen:

- Welke activiteiten en processen zijn betrokken bij het leveren van producten / diensten
- Welke middelen en afhankelijkheden zijn vereist om deze activiteiten / processen mogelijk te maken
- Hoe vormen verschillende bedreigingen een risico voor deze afhankelijkheden en middelen
- Wat kan worden gedaan om de risicogebeurtenissen die bij hen optreden te minimaliseren
- Wat kan worden gedaan om herstel mogelijk te maken in het geval dat risicobeperking mislukt of ontbreekt

Wat heeft u nodig om het te doen?

Alle bedrijven hebben afhankelijkheden waarop wordt vertrouwd om de productie / service te behouden.
De identificatie en beoordeling hiervan zal de sleutel zijn tot het succes van uw BCM-regelingen. Deze kunnen zijn:

- Gebouwen
- (Nuts)/Voorzieningen
- Uitrusting, machinerieën
- Speciaal gereedschap, mallen etc
- IT, gegevens
- Telefonie
- Leveranciers/partners
- Voorraad, verbruiksartikelen
- Transport
- Teams/personeel
- Zusterbedrijven
- Papieren documenten



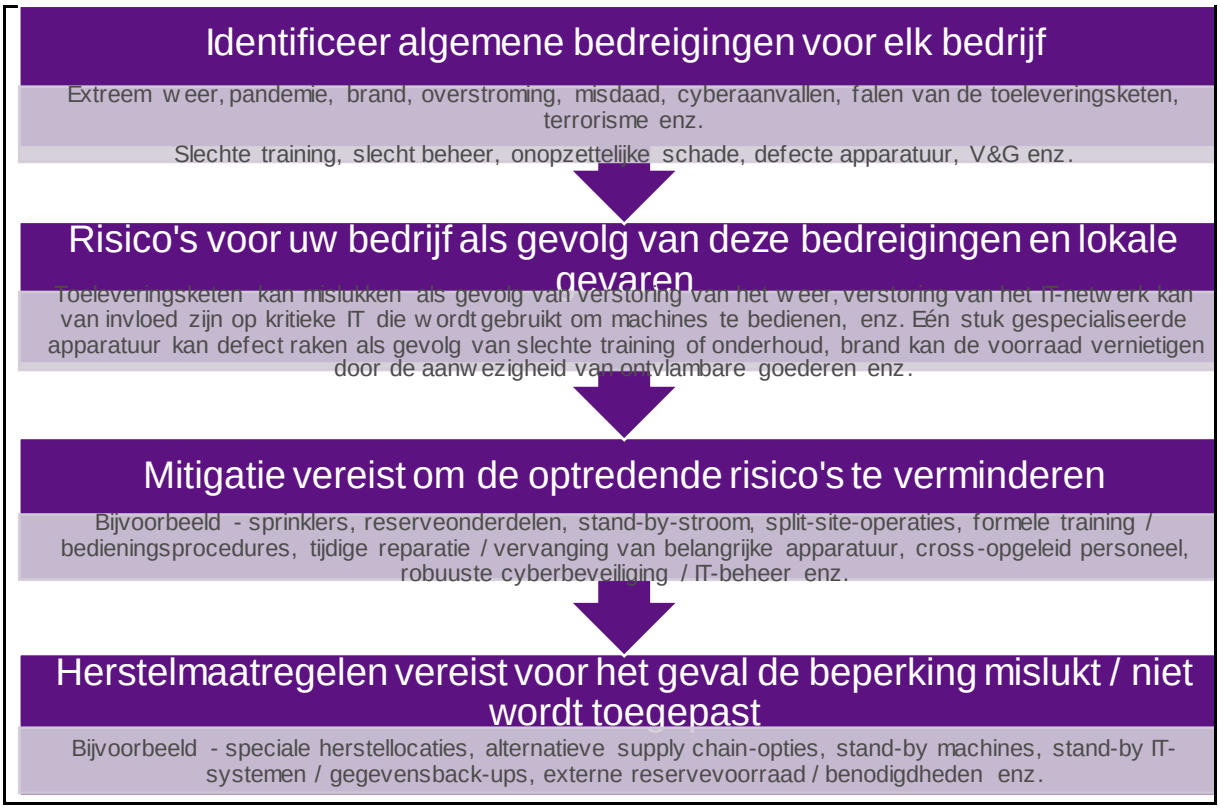
Wat zou er mis kunnen gaan?

Zelfs de kleinste en soms meest onverwachte dingen kunnen escaleren en tot aanzienlijke verstoringen leiden. Dit zijn vaak zaken die niet waren te voorspellen en des te meer reden geven om een herstelplan te hebben.

Gebruik uw bestaande risicobeheerprocessen om eventuele risico's te identificeren en te registreren:

- Oorzaak verstoring van het bedrijf
- Herstel na verstoring

Als u eenmaal weet wat moet worden beschermd, is een typisch proces om risico's te identificeren:



Typische maatregelen om het optreden van risicogebeurtenissen te verminderen zijn onder meer:

- Vroegtijdige waarschuwingsdetectie - IT, brand, overstroming etc.
- Meerdere vestigingen, dubbele leveranciers enz
- Stand-by elektrische stroom, AC-eenheden
- Tweevoudige kabelinvoerpunten
- Gespiegelde of cloudgebaseerde IT-systemen
- Fysieke en cyberveiligheidsmaatregelen
- V&S-conformiteit
- Sprinklers en brandbestrijding

Wat als u uw gebouw, IT of toeleverancier verliest?

Ongeacht de maatregelen die zijn genomen om het optreden van risicogebeurtenissen te verminderen, zullen er altijd gebeurtenissen zijn die niet kunnen worden voorspeld of voorkomen, met dit in gedachten is het belangrijk dat de vereiste herstelmaatregelen aanwezig zijn.

Om uw herstelvermogen te verbeteren, moet u rekening houden met twee belangrijke gebieden:

- Bouw herstelregelingen - implementeer maatregelen om tijdig te herstellen
- Ontwerp een formele antwoordstructuur om het gebruik van die regelingen te beheren

In plaats van een hersteloplossing te hebben voor het verlies van een bepaald product of dienst, is het vaak beter om te focussen op de afhankelijkheid. Meestal heeft u beproefde regelingen nodig voor herstel na het verlies van:

Gebouwen en nutsvoorzieningen / faciliteiten

De gebouwen omvatten de belangrijkste bedrijfsruimten, maar ook opslagruimten en parkeerplaatsen - alles dat belangrijk is voor het bedrijf. Ze kunnen buiten gebruik worden gesteld vanwege brand of overstroming, maar ook vanwege activiteiten op aangrenzende sites of een incident waardoor de toegang tot de site onmogelijk is, ook al is deze operationeel.

Typische oplossingen zijn het maximaliseren van activiteiten op meerdere locaties, het verplaatsen van personeel naar alternatieve locaties, het overdragen van werk naar andere locaties / bedrijven, het gebruik van de marktplaats / andere bedrijven om te helpen, veerkrachtige elektrische / andere faciliteiten en natuurlijk goede huishoudings- en onderhoudsregimes.

Personeel

Personeel staat centraal in het geval van verlies van afhankelijkheden, maar houd rekening met de niet-beschikbaarheid van grote aantallen personeelsleden zelf (pandemie, slecht weer, vervoersproblemen enz.) en het verlies van belangrijke personeelsleden.

Oplossingen omvatten het uitvoeren van belangrijke activiteiten op meerdere locaties, het op korte termijn opstellen van bekwaam personeel, het trainen van personeel, het overdragen van werk aan anderen en personeel dat thuis / op afstand werkt.

IT en Communicatie

De meeste bedrijven zijn afhankelijk van IT en data. IT kan complex zijn, is meestal kritiek en vaak niet in uw handen om het probleem op te lossen. IT en gegevens kunnen in het hele bedrijf worden gebruikt, of lokaal om een machine te laten draaien. Hoewel cyberaanvallen een veelbesproken bedreiging voor IT zijn, zijn er nog steeds veel storingen die te wijten zijn aan slecht begrip en beheer van IT, uitval van IT-componenten, fysieke schade veroorzaakt door brand of overstroming, kabels die worden doorgesneden (of gestolen) en zo verder.

Typische oplossingen zijn onder meer het gebruik van 'cloud'-systemen, off-site stand-by IT-systemen die zich in verschillende stadia van stand-by bevinden, handmatige oplossingen en goed allround IT- en IT-beveiligingsbeheer. IT en gegevens kunnen worden gehost binnen het bedrijf of door een derde partij, maar u moet er toch voor zorgen dat herstelmaatregelen voldoen aan de zakelijke behoeften.

Uitrusting/machinerieën

Dit kunnen machines en apparatuur zijn die worden gebruikt in een productiefaciliteit, een magazijnoperatie of elk ander bedrijf met een apparatuurbehoefte als onderdeel van de operatie. Denk ook aan speciale stellingen of gereedschappen die nodig zijn om naast de apparatuur / productielijn te werken. Verstoring kan bijvoorbeeld worden veroorzaakt door uitval, slechte training / bediening / onderhoud, afhankelijkheid van enkele storingspunten, en brand.

Oplossingen kunnen een combinatie zijn van het gebruik van reservecapaciteit op en buiten de locatie, werk overdragen aan andere bedrijven / locaties, goede procedures voor onderhoud en reparatie, de mogelijkheid om

te zorgen voor tijdige vervanging van defecte machines / componenten door leveranciers (waar levertijden niet herstelbehoeften van het bedrijf overschrijden).

Transport

Transportvereisten kunnen eigendom zijn van het bedrijf of een derde partij. Ze kunnen vracht en verplaatsingen tussen locaties of binnen de locatie omvatten (bijvoorbeeld vorkheftrucks). Verstoring kan betrekking hebben op het transport zelf, brandstoftekorten, de infrastructuur (wegen, toegang, spoor, vracht enz.) of de chauffeurs / afhandelaars.

Typische maatregelen zijn onder meer het hebben van een vloot van verschillende soorten voertuigen, crosstraining van chauffeurs, leveranciers van transport, het stallen van voertuigen op een goede afstand van elkaar enz.

Verbruiksartikelen / voorraad

Verbruiksartikelen en voorraad omvatten inkomende artikelen die nodig zijn als onderdeel van het productieproces, benodigdheden om machines te laten werken (zoals smeerolie), evenals afgewerkte producten die klaar zijn om vanaf de locatie te worden verzonden. Verlies van één van beide kan te wijten zijn aan slechte opslag en behandeling, ongedierte, brand, overstroming, of een probleem met de toeleveringsketen.

Maatregelen zijn onder meer het reserveren van inkomende voorraad en gereed product die elders kunnen worden gebruikt wanneer de productie wordt onderbroken (op en buiten de locatie), veilige opslag, en beveiliging van meerdere toeleveringsketens.

Toeleveringsketen / belanghebbenden

Veel bedrijven zijn afhankelijk van een toeleveringsketen. Supply chains zijn een afhankelijkheid waar u weinig controle over heeft, dus het is belangrijk om te begrijpen waar de kwetsbaarheden in de supply chain zitten. Leveranciers kunnen uw bedrijf om vele redenen in de steek laten, waaronder het falen van hun eigen leveranciers, gebrek aan grondstoffen, tekort aan arbeidskrachten, fysieke schade aan hun gebouwen, en cyberaanvallen.

Oplossingen omvatten het behouden van overzicht en goede relaties met alle elementen van de toeleveringsketen, het gebruik van parallelle leveranciers, ervoor zorgen dat er tijdig naar alternatieve leveranciers kan worden overgeschakeld, en het vasthouden van voorraden on- en off-site om stilstand van leveranciers op te vangen.

Papieren records / bestanden

Sommige bedrijven vertrouwen op papieren documenten en papieren dossiers - als een service voor anderen (bijvoorbeeld scannen, opslag van bestanden) of om naar te verwijzen als onderdeel van de bedrijfsvoering.

Herstelmaatregelen omvatten het onderhoud van veilige, "brand - en overstromingsvrije" opslagoplossingen, off-site duplicatie, en het scannen van records op veerkrachtige IT-systemen, waardoor het risico aanzienlijk wordt verminderd.

Hoe reageert u op een verstorend incident?

Het belang van tijdige en passende communicatie kan niet genoeg worden benadrukt - escalatie en tijdige melding van gebeurtenissen kunnen de sleutel zijn tot versneld herstel van het bedrijf.

Nu u weet wat de hersteloplossingen zijn, hoe gaat u ze beheren? Hoe gaat u reageren en de oplossingen in werking stellen - en wie zal dit doen? Een systeem en plan om de eerste respons en het herstel te beheren, moet het volgende omvatten:

- Incidentdetectiesystemen en escalatieprotocollen, met de mogelijkheid om op elk moment te communiceren
- Formele, competente en getrainde responsteams
- Maatregelen om het gebruik van uw herstelregelingen te ondersteunen
- Een BCM-plan (en alle ondersteunende documenten) waarin alle responsacties formeel worden beschreven

Incident detectie

Voor een effectieve reactie moet u incidenten kunnen identificeren terwijl ze zich voordoen. De juiste mensen moeten onmiddellijk weten of er zich een incident heeft voorgedaan - binnen en buiten werktijd.

Sommige hiervan zijn voor de hand liggend, zoals brand- / rookdetectie, lekdetectie, een gebouwbeheersysteem enzovoort, maar denk ook aan inbraken, uitval van belangrijke machines, verlies van IT / elektrische stroom buiten werkuren - hoe wordt dit gecommuniceerd?

Response teams

Responsteams moeten worden bemand door mensen met de juiste kennis, vaardigheden en autoriteit. Stem reactieteams af op bestaande managementstructuren in het hele bedrijf. Voor veel bedrijven is het volgende gebruikelijk:

Lokale incidentresponsteams (IR) - beheer het incident

Verantwoordelijk voor de onmiddellijke reactie op verstorende incidenten zoals brand, lekkage, IT-uitval enzovoort. Ze zijn vaak verantwoordelijk voor het uitvoeren van evacuaties, onmiddellijke reactie en communicatie, en waarschuwen het BCM-team terwijl ze het incident zelf beheren en oplossen, in plaats van het herstel.

BCM-teams / herstelteams - beheer het herstel

Afhankelijk van de grootte en structuur van uw bedrijf, geeft u misschien de voorkeur aan een gelaagde BCM-teambenadering - bijvoorbeeld Bronze, Silver en Gold Teams. Vaak zal het IR-team een incident kunnen beheren zonder activering van het BCM-plan, maar als het incident erger wordt en waarschijnlijk langer zal duren, informeert het IR-team het BCM-team dat vervolgens het BCM-plan zal oproepen en de verdere communicatie en herstelmaatregelen zal beheren.

Crisismanagementteam (CM) - beheer de crisis

Er moet een CM-team van senior leden zijn dat zou bijeenkomen als de gebeurtenissen op een punt waren gekomen waarop het hele bedrijf gevaar liep en gebeurtenissen niet konden worden beperkt door BCM-regelingen alleen – kortom, een crisis.

Staf en teams die betrokken zijn bij herstel, maar geen deel uitmaken van de IR / BCM-teams

Er zullen medewerkers zijn die niet in de responsteams zitten die verantwoordelijk zijn voor het opzetten van alternatieve gebouwen en het wisselen van IT-systemen, zoals facilitaire teams, beveiligingspersoneel en IT-teams. Zorg dat dit allemaal wordt gecoördineerd!

Commandocentrum

Hoewel voorzieningen voor conferentiegesprekken een goede manier zijn om een BCM-teamvergadering te organiseren, kan er een tijd komen dat het BCM-team een veilige plek nodig heeft om af te spreken, zowel binnen als buiten de locatie (op geschikte afstand).

Escalatie en communicatie

Alle responsteams moeten duidelijke escalatiepaden hebben, waarbij elk lid onmiddellijk toegang heeft tot de relevante contactgegevens (vermeld op hun telefoon is vaak het beste) voor alle belangrijke contacten (intern en extern).

De eerste persoon die op de hoogte is van een incident, kan een personeelslid zijn. Zorg dat hij weet wat hij moet doen en hoe hij contact kan opnemen met het IR Team / lijnmanager, ook buiten werktijd.

Zorg dat u alle vormen van communicatie hebt overwogen en in staat bent om ten minste één ervan effectief te gebruiken zonder afhankelijk te zijn van de site of IT die mogelijk is getroffen.

Media

Bedenk hoe er met de media wordt omgegaan en hoe de berichtgeving in de media over het incident zal worden gecontroleerd. Identificeer wie in het bedrijf mediavragen in en uitgaande berichten zal beheren.

Welzijn van het personeel

De impact op het welzijn en het welzijn van het personeel tijdens en na een verstorend incident kan een even grote impact hebben op het bedrijf als de financiële impact. Het is dan belangrijk om de impact van incidenten op het fysieke en mentale welzijn van uw personeel in overweging te nemen en te monitoren. Besteed aandacht aan de communicatie met het personeel, aangezien deze vaak over het hoofd wordt gezien.

Reactieplannen – algemeen

Met alle overeengekomen herstelregelingen en een structuur die tijdige reacties en communicatie mogelijk maakt, moet u nu de acties en referentiedetails formaliseren en verzamelen in reactieplannen. Dit kan zijn:

- IR-plannen. De inhoud van een IR-plan zal per organisatie verschillen en specifiek zijn voor scenario's zoals verlies van IT, brandevacuatie, bommeldingen, en chemische lekkages. De focus zal liggen op het beheersen van het incident zelf.
- BCM-plannen. Het doel van het BCM-plan moet zijn om het BCM-team (of teams als u een gelaagde BCM-teamstructuur heeft) een gebruiksvriendelijk document te bieden dat alle acties en referentie-informatie bevat die nodig zijn in het geval van langdurige bedrijfsonderbreking
- Individuele reactieplannen van het team. Teams die zijn geïdentificeerd voor herstel / verhuizing hebben mogelijk hun eigen 'one pager' nodig om hen de details te geven die ze nodig hebben voor hun deel van het herstel
- IT-DR-plannen. Het technische plan waarin wordt beschreven hoe u IT kunt herstellen. Dit kan eigendom zijn van het IT-team, maar moet worden opgesteld en afgestemd op de BCM-plannen
- CM-plannen. Dit kan ook deel uitmaken van het BCM-plan, waarin de SMT-reactie op gebeurtenissen die buiten de reikwijdte van het BCM-plan vallen (datalek, ongunstige publiciteit, verlies van klant / geld en schade op meerdere locaties) wordt beschreven
- Overige noodplannen en technische plannen. Naast plannen voor onmiddellijke respons op incidenten, kan er ook behoefte zijn aan specifieke noodplannen / -procedures voor incidenten die veel voorkomen of die een zeer specifiek soort respons vereisen, zoals uitval van apparatuur, herstel van gegevensback-ups, terugroepen van producten enz.

Inhoud BCM-plan

De focus van een BCM-plan zal afhangen van of het een BCM-plan op één siteniveau is, of dat het een overkoepelend BCM-plan op Silver / Gold-niveau is. Plannen op een hoger niveau zullen minder operationele details bevatten, met meer details over de bredere strategische respons en ondersteuning voor de operationele BCM-plannen op een lager niveau.

De inhoud moet alle acties, contactgegevens en referentie-informatie bevatten die het BC-team nodig heeft om het beheer van het herstel te ondersteunen.

Plannen moeten formeel zijn (ondertekend door de SMT), gebruiksvriendelijk, te allen tijde beschikbaar voor degenen die ze nodig hebben, flexibel zijn om allerlei incidenten te beheren en gebaseerd zijn op een gedegen business impact analyse (BIA).

Hoe bewijst u dat herstelmaatregelen werken?

U mag nooit van uw hersteloplossingen uitgaan - beproefde en geteste plannen zullen uw bereidheid om deze te gebruiken bevestigen en vertrouwen geven dat zij geschikt zijn voor het beoogde doel.

Nu herstel- en responsregelingen zijn overeengekomen, en er een BCM-plan is opgesteld, moet u nu bewijzen dat ze geschikt zijn voor het beoogde doel door ze te testen en te oefenen.

Testen en trainen

Enkele voordelen van een test of oefening zijn dat deze:

- Verbetert de bekendheid van BCM Teams met plannen en herstelmaatregelen
- Maakt betwisting / bevestiging van herstelmaatregelen en plannen mogelijk
- Identificeert hiaten en acties die nodig zijn om de veerkracht en het herstelvermogen te verbeteren
- Bevestigt beschikbaarheid van personeel, belangrijke contacten, documentatie / plannen, middelen, stand-by sites etc.
- Verhoogt het bewustzijn bij het personeel, niet alleen bij de responsteams en belanghebbenden
- Verhoogt het vertrouwen van responsteams, medewerkers, klanten (bestaande en toekomstige) en verzekeraars

Het hele jaar door moet een programma van tests en oefeningen worden opgesteld. Dit kan zijn:

- Desktopoefeningen
- Live repetities
- Live en technische test van herstelregelingen
- Communicatietests

Hoe houdt u het BC-raamwerk actueel?

Zorg dat de moeite en het goede werk dat nodig is om een BCM-raamwerk op te zetten, niet verloren gaat - houd het actueel.

Naast regelmatige tests en oefeningen, moeten BCM-plannen, herstelmaatregelen en responsteams regelmatig worden herzien en bijgewerkt om te voldoen aan de veranderende vorm en behoeften van het bedrijf.

Beoordeling

Alle elementen van het BCM-raamwerk moeten formeel worden beoordeeld door de SMT en de belangrijkste belanghebbenden om zeker te zijn dat ze nog steeds geschikt en up-to-date zijn. Dit omvat onder meer een herziening van het BCM-beleid, BIA, BCM-plannen, herstelregelingen en testrapporten. Niet alleen jaarlijks, maar na elke belangrijke wijziging.

Er moeten regelingen zijn om te zorgen dat belangrijke afhankelijkheden worden gehandhaafd, op tijd gerepareerd, onderhevig aan passend onderhoud, en onderhevig aan adequate veiligheidsmaatregelen. Hetzelfde geldt voor herstelregelingen (stand-by-locaties, reserveapparatuur enz.). Zorg ook dat belangrijke leveranciers worden onderworpen aan periodieke controles zodat ze een veerkrachtig niveau behouden waarmee u vertrouwd bent.

Bestuur / toezicht

Hoewel de BCM-coördinator/manager verantwoordelijk kan zijn voor het uitvoeren van veel van het bovenstaande werk, is de SMT verantwoordelijk dat dit gebeurt. Zoals eerder uiteengezet, moeten ze formeel worden betrokken bij de beoordeling van de plannen en moeten ze ook een audit- / toezichtprogramma plannen om te zorgen dat het BC-beleid effectief is.

Veranderingsmanagement

Goede veranderingsmanagementprocedures betekenen dat veranderingen op risico / impact kunnen worden beoordeeld voordat ze worden geïmplementeerd, met minder risico op veranderingen in de operatie of in herstelregelingen.

Bewustwording van het personeel

Betrokkenheid bij het personeel en hen bewust maken van het BCM-plan en hun verantwoordelijkheden is essentieel om BCM onderdeel te maken van de dagelijkse operatie en om een alert en capabel personeelsbestand te behouden in tijden van verstoring.

BCM verankeren en continu verbeteren

Aangezien BCM-beheer in het hele bedrijf wordt geïmplementeerd, kan de SMT het in alle bedrijfsonderdelen integreren door te zorgen dat het in overeenstemming is met strategische doelstellingen en bedrijfswaarden. Als dit effectief wordt gedaan, blijft BCM in vorm terwijl het bedrijf zich ontwikkeld door constante en soms onverwachte veranderingen.

Hoe kunnen we nog meer helpen?

Neem voor meer hulp en begeleiding contact op met uw makelaar.

Andere bronnen, websites en publicaties zijn onder meer:

- Het Business Continuity Institute (BCI) is een Britse instantie voor best practice in het VK, hoewel het een wereldwijde vertegenwoordiging heeft - www.thebci.org.
- Om u verder te helpen, werkt RSA samen met de RISCAuthority die een BCM-planningstool heeft ontwikkeld genaamd Robust ©. Dit is beschikbaar via de RISCAuthority - https://robust.riscauthority.co.uk/
- De RISCAuthority heeft ook andere bronnen om te gebruiken - https://www.riscauthority.co.uk/free-document-library/ (klik vervolgens op Business Continuity)
- Continuity Central is een goede bron voor begeleiding, tips en nieuws www.continuitycentral.com
- De Business Continuity Good Practice Guidelines (GPG) 2018-editie - beschikbaar via de BCI-link hierboven. Er is ook een gratis, lichtere versie beschikbaar op hun website
- ISO 22301: 2019 - Veiligheid en veerkracht. BCM-systemen - https://www.bsigroup.com/iso-22301-business-continuity
- Diverse ISO- en BS-publicaties gewijd aan continuïteit van diensten en IT - beschikbaar op https://www.bsigroup.com
- Geautomatiseerde online tools van derden die kunnen worden gebruikt om een BC-plan en ondersteunend raamwerk te produceren