



Rogier de Vrey, advocaat
en partner bij CMS, tevens
universitair docent bij de
Universiteit Utrecht



Bedrijfsgeheimen

Uw kroonjuwelen in de digitale informatiemaatschappij

Vijftig jaar geleden werd de waarde van een bedrijf uitsluitend bepaald op basis van haar fysieke kapitaal. Vandaag de dag is de waarde van de meest succesvolle bedrijven ter wereld gefundeerd op immateriële activa. Data wordt het ‘nieuwe goud’ genoemd. Deze – met name digitale – gegevens, zoals algoritmes, klantgegevens, productformules en technologie, hebben van nature een vertrouwelijk karakter.

Onderzoek: het lekken van bedrijfsgeheimen wordt meer en meer als bedreiging gezien

Volgens een wereldwijd onderzoek binnen het bedrijfsleven, in opdracht van CMS uitgevoerd door de Economist, is driekwart van de bedrijfstop van mening dat er moet worden geïnvesteerd in de bescherming van dergelijke bedrijfsgeheimen. Meer en meer komt de vertrouwelijkheid van kwetsbare informatie en technologie in het geding, nu transacties vaker online en grensoverschrijdend plaatsvinden, waarbij kans op een lek groot is. De kranten staan er vol van: van diefstal van honderden miljoenen euro's kostende bedrijfsgeheimen door Chinese spionnen tot de individuele ex-werknemer die er met de geheimen van zijn/haar ex-werkgever van door gaat. Dergelijke bedreigingen worden vergroot door de verandering in werkcultuur die door de pandemie is veroorzaakt. We werken meer thuis en meer digitaal.

Uit het onderzoek blijkt dat bijna de helft (45%) van de beursgenoteerde bedrijven faalt in het beschermen van bedrijfsgeheimen, ondanks de toenemende noodzaak om intellectueel eigendom te beschermen. Cybercriminaliteit (49%) en lekken door werknemers (48%) zijn de grootste risico's voor het verlies van handelsgeheimen. De wereldwijde kosten van diefstal van bedrijfsgeheimen lopen jaarlijks op tot meer dan € 1.4 biljoen (!). Executives verwachten

dat het risico op diefstal van bedrijfsgeheimen de komende vijf jaar nog verder zal stijgen.

Het onderzoek toont aan dat voor bedrijven een holistische aanpak het beste werkt ter bescherming van bedrijfsgeheimen. Daarbij moet een evenwicht worden gevonden tussen beperkingen en stimulansen, en, belangrijker nog, het betrekken van werknemers op alle niveaus. Zonder deze strategie blijft het beschermen van bedrijfsgeheimen voor velen een moeilijke strijd.

Wat is een bedrijfsgeheim?

Een bedrijfsgeheim is alle informatie die geheim is, een bepaalde waarde vertegenwoordigt en waarvoor “redelijke maatregelen” zijn getroffen om het geheim te houden. Deze voorwaarden zijn opgenomen in de Wet Bescherming Bedrijfsgeheimen (WBB, van kracht sinds 23 oktober 2018). Waar voor een octrooi wordt vereist dat het om een (technische) uitvinding gaat die nieuw en inventief is, is dat niet vereist voor een bedrijfsgeheim. Een bedrijfsgeheim ziet dus niet alleen op een (technische) uitvinding, maar ook bijvoorbeeld op vertrouwelijke klantgegevens, businessmethoden, productformules (het recept van Coca-Cola), software algoritmes en gegevens over productieprocessen.

Voordeel van een bedrijfsgeheimen is verder dat – zolang niemand anders het geheim ontdekt – er geen tijdslimiet aan de

bescherming is verbonden, terwijl een octrooi maximaal 20 jaar bescherming geeft. Verder is anders dan bij octrooiverlening, geen lang en kostbaar registratietraject nodig, en is een bedrijfsgeheim in principe te handhaven in de gehele EU (als aan de voorwaarden wordt voldaan).

Wat zijn de voorwaarden voor bescherming van bedrijfsgeheimen?

Om bescherming voor bedrijfsgeheimen te kunnen krijgen onder de WBB moet aan bepaalde voorwaarden worden voldaan. Voorwaarden waar organisaties vaak nog niet (volledig) aan voldoen. Allereerst is vaak onvoldoende bepaald en gedocumenteerd welke concrete informatie en technologie bedrijfsgeheim zijn. Identificeren wat de waardevolle geheime kennis is en dat vervolgens goed documenteren is noodzakelijk om later (als er een lek is) een goede bewijspositie te hebben en aanspraak op bescherming te kunnen maken.

Daarnaast is het voor organisaties van belang om voldoende fysieke, digitale en organisatorische maatregelen te treffen om geheimhouding te garanderen. Bij fysieke maatregelen kan je denken aan beveiligingssystemen voor gebouwen, bewakingscamera's, afgesloten ruimten, of toegangssystemen op basis van een pasje, iris-scan of vingerafdruk. Op organisatorisch vlak is bijvoorbeeld een duidelijke en goed vindbare "Know-how Protection Policy" van belang, classificatie van informatie ("Confidential", "Strictly confidential", "Top secret"), trainingen en exit interviews voor werknemers.

Kortom, enerzijds een bepaald niveau van toezicht op de activiteiten van werknemers (en contractspartijen) en anderzijds een collaboratieve aanpak gericht op het duidelijk uitdragen van een bedrijfscultuur en invoering van innovatieve prikkels voor werknemers (denk aan een beloningsregeling voor

medewerkers die nieuwe bedrijfsgeheimen ontdekken of hiaten in de beveiliging aankaarten). Tenslotte is natuurlijk een passend cybersecurity beleid van belang, met toegang tot informatie op een need-to-know basis en zaken als een password beleid (met toegangsniveaus) en encryptie. Online-bedrijven zullen meer cyberbeveiligingsmaatregelen moeten nemen, terwijl productiebedrijven meer fysieke maatregelen moeten nemen op de fabrieksvloer.

Op juridisch vlak zijn NDA's, geheimhoudingsbepalingen in arbeidsovereenkomsten en overeenkomsten met derde partijen van belang. Ook valt te overwegen om bepaalde gedocumenteerde bedrijfsgeheimen te registreren bij IE-instanties zoals de WIPO en BBIE ("i-DEPOT") of een notaris.

Uiteindelijk is een holistische aanpak door geïntegreerde cybersecurity ('security by design') te combineren met het creëren van een bedrijfscultuur rondom bedrijfsgeheimen, de beste manier om bescherming van vitale en waardevolle bedrijfsinformatie te kunnen garanderen.

Optreden tegen diefstal (of misbruik) van bedrijfsgeheimen

Als dit huiswerk goed gedaan is, biedt de wetgeving op gebied van bedrijfsgeheimen (WBB) een goed wapen tegen diefstal en ongeautoriseerd gebruik. Bedrijfsgeheimen zijn in feite quasi-intellectuele eigendomsrechten geworden. De WBB biedt aan bedrijven een mooie toolkit om op te treden tegen partijen die op oneigenlijke wijze aan bedrijfsgeheimen komen. Zo is er de mogelijkheid een verbod te vorderen op gebruik van de bedrijfsgeheimen en kunnen producten worden vernietigd waarin de bedrijfsgeheimen zijn verwerkt of die (o.a. bij de productie) voordeel hebben gehad bij de ongeautoriseerde toegang tot bedrijfsgeheimen. Ook maatregelen als bewijsbeslag, schadevergoeding en recall

zijn mogelijk. Mocht het tot een procedure komen, dan zijn er tegenwoordig speciale voorzieningen om te voorkomen dat tijdens een procedure over bedrijfsgeheimen, deze informatie zijn vertrouwelijkheid verliest. Zo kan tijdens de procedure verzocht worden om bepaalde geheime informatie enkel onder geheimhouding toegankelijk te maken voor één persoon van de wederpartij en een advocaat, inclusief boetes op overtreding van geheimhouding (de zogenoemde 'confidentiality club'). Om als bedrijf goed van deze toolkit gebruik te kunnen maken is wel van belang dat er een uitgewerkt draaiboek ligt voor het geval een bedrijfsgeheim wordt gestolen of gelekt.

Tot slot

Waar innovatief ondernemerschap en het voorop lopen in digitale ontwikkelingen voor een bedrijf de voorsprong kan betekenen ten opzichte van zijn concurrentie, neemt het belang toe om de daarmee gepaard gaande bedrijfsgeheimen goed te beschermen tegen diefstal en ongeautoriseerd gebruik. Het is nog nooit zo belangrijk geweest om de juiste maatregelen te nemen om als organisatie succesvol te blijven. De aard van bedrijfsgeheimen brengt met zich mee dat goede voorbereidingen noodzakelijk zijn en dat het pas treffen van maatregelen als het gegevenslek zich voordoet, vaak te laat is. Start met het deugdelijk identificeren van uw bedrijfsgeheimen (audit-fase), implementeer vervolgens de noodzakelijke maatregelen en heb een draaiboek gereed (beschermingsfase). Controleer tenslotte, o.a. door trainingen en periodieke checks en updates, of de bescherming naar behoren blijft (check-up fase). Wordt een bedrijfsgeheim desondanks openbaar, dan biedt de WBB regelgeving de juiste mogelijkheden om op te treden. ■