Dick Brandt (voormalig CISO PostNL) en Johan Bakker (voormalig CISO KPN) hebben beiden meer dan 25 jaar ervaring in het bedrijfsleven, volop opererend op het grensvlak van techniek en business. Beiden zijn vanuit een technische achtergrond meer dan 10 jaar geleden in het information security werkveld begonnen om vervolgens door te groeien tot CISO van een multinational. Dick en Johan zijn nu beiden actief als zelfstandig ondernemer (advies en consultancy) en hebben tevens samen de CISO Masterclass BV opgericht, waar ze als docenten hun opgedane kennis en ervaring overdragen aan toekomstige en zittende CISO's. Zij zijn te bereiken via dick.brandt@cisomasterclass.nl en johan.bakker@cisomasterclass.nl.

SUCCESVOL OPEREREN OP HET GRENSVLAK VAN TECHNIEK EN BUSINESS

Succesvol Information Security Management staat of valt bij de mate van aansluiting en draagvlak die de "information security verantwoordelijke" weet te vinden bij "de business." De Chief Information Security Officer (CISO) opereert op het grensvlak van techniek en business en dat is in de praktijk niet altijd eenvoudig. CISO's met een technische achtergrond hanteren doorgaans een analytische insteek, communiceren probleem- en oplossingsgericht en hebben een andere risicobeleving dan de business.

De business wil niet van de CISO horen hoe iets werkt, maar wil begrijpen wat het hen oplevert!

Binnen een technische (ICT) omgeving is dit de norm en werkt dit constructief. Echter, om succesvol te zijn binnen zijn of haar organisatie, moet de CISO zich ook soepel kunnen bewegen in de wereld van de business; de business begrijpen, de taal spreken en security kunnen verkopen. Van hem of haar wordt dus veelzijdigheid verwacht.

Alleen wanneer information security zichtbaar de organisatiedoelstellingen ondersteunt en de business daadwerkelijk helpt haar strategie te realiseren, zal er draagvlak binnen de organisatie ontstaan en wordt security niet ervaren als last maar als 'enabler'.

De samenhang doorgronden

De CISO zal dus de samenhang van die twee werelden moeten doorgronden en die kennis moeten gebruiken om een win-win situatie voor beide werelden te creëren. Hiermee voegt de CISO waarde toe aan het bedrijf of de organisatie en groeit het draagvlak voor information security als geheel en voor zijn of haar positie in het bijzonder.

Hoe dit het beste gedaan wordt, verschilt per sector, organisatie en organisatiecultuur. Het is doorgaans een proces van vallen en opstaan, waarbij er voortdurend lessen geleerd kunnen worden uit de opgedane ervaringen en opnieuw richting kan worden gekozen.

De eigen business begrijpen

Eén uitgangspunt is echter voor alle sectoren, organisaties en organisatieculturen hetzelfde; om effectief met managers en bestuurders te communiceren, en daarmee invloed uit te kunnen oefenen, zal de security professional de wereld van de business moeten doorgronden, hun management cultuur en drives moeten begrijpen en hun taal moeten spreken. De CISO moet zich als één van hen onder hen kunnen bewegen.

Om de business van binnen uit te kunnen ondersteunen, moeten zaken als de marktbenadering, businessdoelen, de waardeketen, het verdienmodel, de jaarrekening en de businessuitdagingen bekend terrein zijn.

Een schaap met vijf poten

Verder zal hij om invloed uit te kunnen oefenen, zich, naast de voor de hand liggende soft skills, moeten verdiepen en bekwamen in zaken als organisatiekunde en managementvaardigheden en daarnaast een zekere organisatiesensitiviteit moeten ontwikkelen om binnen de heersende organisatiecultuur te kunnen opereren.

Een CISO moet in staat zijn de information security strategie over de business strategie heen te kunnen leggen en zo te formuleren dat de bijdrage van information security aan het realiseren van de business strategie voor iedereen binnen de organisatie helder is.

Herkenbare business doelen

De securitydoelen en het beleid kunnen zodoende herkenbaar voor de organisatie worden geformuleerd, dat de discussie over nut en noodzaak grotendeels vermeden wordt en het draagvlak toeneemt. Voor de business herkenbare doelen zijn zaken als:

- **strategische waarde**
- **bijdrage aan de business doelen**
- **reputatie, merkwaarde of concurrentiekracht**
- **kostenverlaging of omzetverhoging**

Let op: De business wil niet van de CISO horen hoe iets werkt, maar wil begrijpen wat het hen oplevert! En als de CISO de bijdrage van het security beleid en de implementatie ervan niet in bovengenoemde termen kan uitdrukken, dan is er iets mis met of de inhoud of zijn of haar wijze van communiceren.

Wat te doen als CISO?

Het voorgaande suggereert bijna dat iedere CISO een volledige MBA opleiding zou moeten volgen; bij een aantal grote multinationals is dit overigens al de norm. In de praktijk is binnen de meeste organisaties MBA-niveau nog niet nodig of niet haalbaar. Wel moet iedere CISO zich verdiepen en bekwamen in de hier besproken kennis en vaardigheden, om hem of haar in staat te stellen als een volwaardige partner van de business te opereren.