NLdigital

Cyber Chain Resilience Consortium

Whitepaper

Cybersecurity naar de **bestuurderskamer**

Hoe CIO's, CISO's en IT-managers cybersecurity structureel op de agenda krijgen.

Cybersecurity: de sleutel ligt bij jullie

Cybersecurity is geen puur IT onderwerp. Het raakt reputatie, continuïteit, juridische aansprakelijkheid en klantvertrouwen. Toch blijft het voor veel bestuurders een ver-van-hun-bed-show, iets wat ze 'overlaten aan de IT'. Maar die tijd is voorbij. Digitale veiligheid is zó verweven met de bedrijfsvoering dat de verantwoordelijkheid ervan niet meer alleen technisch ingestoken kan worden.

De Cyber Security Raad zegt het treffend in haar handreiking: "Cybersecurity is niet slechts een technische uitdaging, maar een structureel en strategisch vraagstuk dat de gehele organisatie raakt." Met de juiste aanpak kan cybersecurity zich ontwikkelen van kostenpost naar strategische troef.

Ga snel naar...

Een solide basis in vier stappen:

Cybersecurity is geen IT-issue. Het is een strategisch bedrijfsrisico dat vraagt om leiderschap, structuur en samenwerking. **Start het gesprek zo snel mogelijk.** Doe dit met taal die landt, inzichten die richting geven en een structuur die werkt:

1

Praat vanuit business continuïteit

Stop met het bespreken van technische onderwerpen. Maak inzichtelijk wat een dag stilstand kost en wat het kost om dat te voorkomen.

Gebruik de NIS2-deadline

2

De inwerkingtreding van de NIS2 in 2026.
Gebruik de tijd om voor te bereiden

3

Werk aan de cultuur

Zorg voor een omgeving waarin fouten gemeld durven worden.
Een veilige meldcultuur is je beste detectiesysteem.

Bouw een interne security community

4

Security is niet alleen van de security officer, maar van iedereen.
Hoe meer medewerkers bijdragen aan beveiliging hoe weerbaarder een organisatie wordt.

Start met het opzetten van een security community waarin je iedereen samenbrengt die actief wil bijdragen aan security. Dit zijn de cyber-champions van de organisatie.

Organisaties die dit consequent doen, creëren geen papieren veiligheid, maar échte cyber-weerbaarheid: met een cultuur van heldere taal, gedeeld eigenaarschap en actie die ertoe doet.

In dit whitepaper lees hoe je dit verder op kan pakken

1. **De urgentie:** waarom dit nu op de agenda moet

Om het bestuur te overtuigen van de urgentie, moet de context helder zijn. We zien vier grote krachten die nu samenkomen:

Geavanceerdere aanvallen

Cyberdreigingen zijn groter, slimmer en sneller dan ooit. De opkomst van AI versnelt en vergroot de schaal van aanvallen alleen maar. Wat vroeger mensenwerk was, is nu geautomatiseerd, denk bijvoorbeeld aan het geautomatiseerd vinden van zwakke systemen van organisaties en het volledig personaliseren van phishing.

Geopolitieke spanningen

Cybersecurity raakt de nationale veiligheid. Spanningen in de wereld vertalen zich direct naar digitale dreigingen voor Nederlandse bedrijven. Sabotage en spionage door statelijke actoren zijn reële risico´s geworden, hiervoor wordt steeds vaker gebruikgemaakt van aanvallen op toeleveranciers. Ook bedrijven die geen directe betrokkenheid bij nationale veiligheid hebben, kunnen gericht als springplank naar een andere organisatie worden aangevallen.

Verplichtende wetgeving (zoals NIS2 en DORA)

EU-wetgeving zoals de cyberbeveiligingsewet (NIS2), DORA en CRA dwingen organisaties om structureel werk te maken van security. Bestuurders krijgen niet alleen een grotere verantwoordelijkheid, maar ook juridische aansprakelijkheid. Vrijblijvendheid maakt daardoor plaats voor verplichting.

Digitale afhankelijkheid

De meeste aanvallen komen tegenwoordig binnen via leveranciers, of ketenpartners. Ook voor organisaties die hun eigen beveiliging redelijk op orde hebben, blijkt ketenweerbaarheid een ingewikkeld vraagstuk.Grote opdrachtgevers eisen steeds vaker dat hun leveranciers ‘in control’ zijn. Als je je security niet op orde hebt, verlies je dus ook contracten (“*License to Operate*”).

Cybersecurity is niet louter een technische uitdaging, maar een kernonderdeel van risicomanagement. Bestuurders moeten kunnen sturen op weerbaarheid, net als op financiële gezondheid. De risico’s zijn niet alleen technisch of tijdelijk, maar raken fundamentele pijlers van de bedrijfsvoering. Denk aan operationeel stilvallen, reputatieschade, omzetverlies, juridische claims en uiteindelijk zelfs het voortbestaan van de organisatie.

Toch wordt digitale veiligheid in veel organisaties nog ad hoc benaderd. Security komt vaak pas in beeld na een incident of audit. Daarmee loopt men achter de feiten aan. Proactieve, structurele inbedding van security in governance, budgetcyclus en strategievorming is essentieel om de regie te houden. Veiligheid beschrijft altijd een momentopname, en vereist blijvende aandacht en investeringen om actueel te blijven.

2. **De kloof tussen IT en bestuur:** waarom praten we langs elkaar heen?

Veel bestuurders zien cybersecurity nog steeds als een IT-aangelegenheid: "Onze IT'er regelt dat." Die houding is deels te verklaren. Het onderwerp voelt technisch en complex, en IT-afdelingen communiceren vaak niet in de taal van de board. IT spreekt in tools, de board in risico's. Deze kloof leidt tot ruis, misverstanden en gemiste kansen.

IT zegt:

"We moeten patchen vanwege CVE-2024-xyz en de firewall upgraden."

De board denkt:

"Wat kost dit? Wat is het risico? Heb ik controle? Wat gebeurt er als we dit wel of niet doen?"

Ze willen vooral niet verrast worden door verantwoordelijkheden die ze niet (kunnen) controleren.

Bestuurders nemen strategische besluiten over cybersecurity, maar missen vaak de kennis om de juiste vragen te stellen of effectieve kaders te geven. De opdracht is dan óf te vaag ("We moeten iets aan security awareness doen"), óf te specifiek zonder inzicht in effectiviteit ("Iedereen moet een e-learning volgen").

Vervolgens komt het middenmanagement in actie zonder dat ze altijd begrijpen wat het doel is of hoe het bijdraagt aan het grotere geheel. Dat leidt tot uitvoer zonder impact.
De rol van CIO's, CISO's en IT-managers is cruciaal in deze vertaling. Zij moeten niet alleen 'omhoog' uitleg geven in begrijpelijke taal, maar ook 'zijwaarts' en 'naar beneden' ondersteunen. Niet met technische metrics, maar met antwoorden die aansluiten op de vragen van het bestuur én praktische begeleiding voor de uitvoering.

En het werkt pas echt als het van twee kanten komt: ook bestuurders moeten hun rol pakken. Zij moeten leren welke vragen ze moeten stellen, wat hun verantwoordelijkheid is (geen “los het maar op”) en hoe ze sturing geven aan security. Alleen zo landt een besluit niet op papier, maar in de praktijk.

3. Hoe krijg je het wél **op de agenda**?

Veel organisaties worstelen met het agenderen van security. Hier zijn vier strategieën aangedragen door experts om de impasse te doorbreken:

Strategie 1: Praat vanuit bedrijfsrisico’s

Stop met praten over tools en begin over bedrijfsrisico’s.

Niet:

"We hebben een nieuwe back-up server nodig."

Maar:

"Als we geraakt worden door ransom-ware, liggen we drie weken stil. Dat kost ons €200.000 en klant X. Met deze investering zouden we binnen vier uur weer online zijn."

Gebruik 'praatplaten' of infographics.
Bestuurders zijn visueel ingesteld, maak het dus tastbaar. Een simpele visual die risico en oplossing toont, werkt beter dan een technisch diagram.

Strategie 2: Richt je op de quick wins

Veel bestuurders schrikken van de kosten om alles maximaal veilig te maken. Door te richten op cyberweerbaarheid is veiligheid meer kosten efficiënt.

Richt je op beveiligingsmaatregelen met een hoog rendement (lage kosten met hoge effectiviteit, de quick wins) en vul dat aan met maatregelen om adequaat te reageren op een aanval. Denk aan een goed incident en crisisproces. Dit maakt je veel flexibeler en cyberweerbaarder met lagere kosten.

“Ga ervan uit dat we gehackt worden.
Hoe zorgen we dat we dan overleven?”

Strategie 3: Maak het tastbaar (storytelling & simulaties)

Het Neighbouring Effect:
Bestuurders beseffen de urgentie vaak pas echt als een concurrent of een bedrijf in de regio gehackt wordt. Gebruik die voorbeelden. “Heb je gehoord wat er bij bedrijf X is gebeurd? Dat kan ons ook overkomen.” En als iemand van hen bereid is er zelf over te komen vertellen wordt het nog tastbaarder.

Crisis Simulaties:
Organiseer een Tabletop Exercise → Zet het bestuur aan tafel en speel een hack na. Wat doen ze? Wie bellen ze? Als ze merken dat ze geen plan hebben, ontstaat de urgentie vanzelf.

Strategie 4: De 'brandbrief' op één A4

Soms is een schok nodig. Een bondige, duidelijke memo werkt.
Geen jargon, maar duidelijke taal:

> *"We testen onze back-ups nooit.”*
> *“Als het misgaat, weten we niet of we kunnen herstellen.”*
> *“Een halve dag testen kan het verlies van onze organisatie besparen!”*

Koppel dit aan bestuurlijke aansprakelijkheid en reputatieschade. De ervaring leert dat bestuurders snel in actie komen als ze zwart-op-wit zien dat ze (persoonlijk) risico lopen of contracten schenden.

Deze strategieën helpen om security structureel op de agenda te krijgen. Niet als IT-issue, maar als boardroom prioriteit om de organisatie operationeel te houden.

4. **Best practices** uit de praktijk

Organisaties die cybersecurity succesvol agenderen, doen dat met heldere taal, concrete acties en strategisch leiderschap:

Spreek in impact:

→ Geen technische afkortingen, maar:
“Als dit systeem faalt, verliezen we klant X” *of:*
“dan komt onze organisatie tenminste X dagen stil liggen”.

Integreer security in je cultuur:

Start bij onboarding met training en het schetsen van heldere verwachtingen.
→ Hoe kan iedereen bijdragen aan onze cyberweerbaarheid?

Simuleer aanvallen:

De kennis en ervaring uit een crisisoefening van 3 uur zegt meer dan 30 pagina’s ongetest beleid.

Stel eigenaarschap scherp:

Weet wie waarvoor verantwoordelijk is en toets dat regelmatig.

Gebruik peer stories:

Een mkb-ondernemer die gehackt werd en een week offline lag, overtuigt sneller dan een prachtige risico-analyse.

5. **Hoe nu verder:** waar begin je morgen?

CISO's, CIO's en IT-managers die hun uitdagingen niet op de bestuurstafel terugzien lopen het risico roepende in de woestijn te worden. Start daarom het gesprek zo snel mogelijk en doe dit met taal die landt, inzichten die richting geven, en een structuur die werkt.

Gebruik deze whitepaper als katalysator.

- ☑ Organiseer een crisisoefening.
- ☑ Stem je communicatiestijl af op je publiek.
- ☑ Betrek de juiste mensen.
- ☑ Gebruik actuele wetgeving als brug naar het gesprek.
- ☑ Wijs je bestuurders op de Handreiking Cybersecurity voor Bestuurders en Bedrijfseigenaren van de Cyber Security Raad.

En bovenal: **neem het voortouw en wees die strategische partner die zorgt voor rust, richting en robuustheid, juist als het spannend wordt.**

"Vervang angst en jargon door oefening en eigenaarschap: cybersecurity is uiteindelijk mensenwerk."

Dit whitepaper is opgesteld door CCRC & NLdigital, op basis van:

- De handreiking “Cybersecurity is niet slechts een technische uitdaging, maar een structureel en strategisch vraagstuk dat de gehele organisatie raakt." uitgegeven door de Cyber Security Raad
- Interviews met CISO’s, experts en bestuurders;
- Input gegeven door bezoekers op de Cybersec beurs 2025;
- De scriptie Inside the SME Security Decision - An exploration of leadership engagement in building cyber-resilient small and medium-sized enterprises door Yoran Koenders voor de TU Delft, uitgevoerd in opdracht van CCRC.

Cyber Chain Resilience Consortium

CCRC richt zich op het verhogen van de cyberweerbaarheid van organisaties door het laagdrempelig kunnen uitvoeren van cyber oefeningen voor en met de keten.

NLdigital

NLdigital is dé brancheverenigingen van de digitale sector. Samen met partners ontwikkelen en leveren ze de producten en diensten die Nederland nodig heeft om digitaal vooruit te komen