PLATFORM
INTEGRALE VEILIGHEID
HOGER ONDERWIJS

Een initiatief van de Vereniging Hogescholen en VSNU

KPMG

Aan de Vereniging Hogescholen & VSNU
Van de Stuurgroep Integrale Veiligheid Hoger Onderwijs (IV-HO)
15 juni 2020

Aanbieding sectoradvies:

‘Governance van Cybersecurity, Privacy & Kennisveiligheid HO – Pas toe of leg uit!’

Als Stuurgroep van het Platform Integrale Veiligheid Hoger Onderwijs geven wij richting aan de ontwikkeling van integrale veiligheid in het hoger onderwijs. In het platform werken onze mensen gezamenlijk aan dit actuele onderwerp. Zo hebben zij langs de bestuurlijke lijn geadviseerd aan de Minister OCW op het onderbreken en weer op gang brengen van het fysieke onderwijs n.a.v. de coronacrisis. Het hoger onderwijs heeft zich gelukkig weerbaar getoond en binnen korte tijd een historische omslag gemaakt naar online onderwijs en onderzoek.

Dat betekent ook dat we onze weerbaarheid op het gebied van cybersecurity en kennisveiligheid moeten vergroten. De ransomware-aanval op de Universiteit Maastricht ligt hierbij nog vers in het geheugen. Ook op het gebied van kennisveiligheid moeten we stappen zetten. Kennisdeling is van groot belang voor onze maatschappelijke en economische ontwikkeling, maar is ook interessant voor criminele organisaties en sommige buitenlandse mogendheden.

In de brief aan de Tweede Kamer van het ministerie van OCW van februari is een aantal maatregelen aangekondigd. Deze maatregelen liggen op technisch niveau: betere monitoring en detectie (SOC’s), daarnaast intensievere samenwerking, het vergroten van veiligheidsbewustzijn en audits.

Om ook invulling te geven aan het aspect van organisatieontwikkeling is in Platformverband onderzocht hoe de governance van Cybersecurity en Kennisveiligheid in de instellingen zelf ingericht zou kunnen worden om de bestuurbaarheid ervan te verbeteren. Vervolgens is met KPMG, de CISO’s en enkele ‘cyberprofessoren’ een expertopinie tot stand gekomen.

Deze Positon Paper bevat dus een expertopinie over de inrichting van de cybersecurityfunctie. in samenhang met de andere integrale veiligheidsgebieden. Het is een service-document en er gaat geen normerende werking vanuit. Het bevat een ideaalbeeld dat ter inspiratie wordt aangeboden. Uiteraard speelt schaalgrootte een rol en is de praktijk weerbarstig, maar wij hopen dat het paper zal bijdragen aan kennisontwikkeling en het goede gesprek in onze sector hoger onderwijs, met een duidelijk ideaalbeeld voor ogen.

Verzoek

Als Stuurgroep IV-HO willen wij onze collega-bestuurders van hoger onderwijsinstellingen uitnodigen om in koepelverband deze Position Paper te agenderen.

Bijlage(n):

Position Paper

PLATFORM
INTEGRALE VEILIGHEID
HOGER ONDERWIJS

Een initiatief van de Vereniging Hogescholen en VSNU

KPMG

POSITION PAPER

Definitieve versie, 20 april 2020

Inrichting governance van cybersecurity in het hoger onderwijs

Pas toe of leg uit!

Deze Position Paper is opgesteld vanuit het Platform Integrale Veiligheid Hoger Onderwijs (IV-HO)[1] en gaat in op de twee veiligheidsgebieden 'Cybersecurity & Privacy' en 'Kennisveiligheid', zoals beschreven in het 'Dreigingsbeeld Hoger Onderwijs'[2]. In deze paper hanteren wij voor de eenvoud de term 'cybersecurity' om de governance van deze veiligheidsgebieden te belichten. Integrale veiligheid[3] en zeker ook cybersecurity gaan als een saté-prikker dwars door andere beleidsterreinen heen en hebben raakvlakken met een veelvoud van hen, zoals HR, wet- en regelgeving, financiën en kwaliteit.

Voor de duidelijkheid: cybersecurity beslaat niet enkel de digitale bescherming van informatie, maar behelst ook de informatiebeveiligingsaspecten van kennis, privacy, fysieke beveiliging en continue beschikbaarheid van informatie en IT.

Waarom is een inhaalslag hard nodig?

Instellingen voor hoger onderwijs zijn van nature open, kennis moet kunnen stromen. Er was hierdoor in het verleden dan ook weinig noodzaak tot een 'Fort Knox'-beveiliging en een volwassen cybersecurityfunctie. Het bewustzijn wat betreft informatie- en IT-gerelateerde risico's was traditioneel ook laag. Die tijden zijn veranderd; specifieke informatie heeft bij instellingen een hoge waarde en een uiterst vertrouwelijk karakter (de 'kroonjuwelen' zoals gevoelige persoonsgegevens), de beschikbaarheid van de informatie- en IT-voorzieningen is onmisbaar en de integriteit van onderzoeks- en studieresultaten is cruciaal.

Recente incidenten en een toenemend dreigingsniveau laten zien dat een flinke inhaalslag van de digitale weerbaarheid moet plaatsvinden. Cybersecurity gaat niet enkel over het voorkomen van incidenten, maar ook over het snel detecteren en herstellen van incidenten, en het organiseren hiervan.

De minister van OCW heeft in haar recente Kamerbrief aangegeven dat wordt geïnvesteerd in beveiligingsbewustzijn, monitoring (SURFcert, Security Operations Centers) en periodieke toetsing. Reeds in 2018 is het belang van cybersecurity en in de bredere zin integrale veiligheid binnen het hoger onderwijs onderkend door de vorming van het platform IV-HO.

---

1 Opgesteld door KPMG is samenwerking met de werkgroep IV-HO-governance. Wij bedanken de hoogleraren Cybersecurity Bibi van den Berg (UL) en Michel van Eeten (TU Delft) voor hun input en feedback. Deze Position Paper is niet bedoeld als weergave van hun standpunten. Tevens hebben de SCIPR-bestuursleden en CSC-voorzitters een conceptversie van feedback kunnen voorzien.

2 Het hoger onderwijs heeft zich in 2018 gecommitteerd aan het sectorbreed en in iedere instelling integraal organiseren en professionaliseren van het veiligheidsbeleid.

3 De andere integrale veiligheidsgebieden, te weten Sociale Veiligheid, Zorgwekkend gedrag & Radicalisering, Internationalisering, Integriteit, Gebouwveiligheid en Arbo & Milieu komen hier niet expliciet aan bod; wel zijn dezelfde principes van toepassing.

Deze Position Paper vormt de vervolgstap door een standpunt in te nemen over de organisatorische inrichting van cybersecurity en met name over de 'aanvoerder' om de inhaalslag invulling te geven.

Deze paper gaat derhalve in op de governance van cybersecurity[4]. Voor nadere detaillering verwijzen wij graag naar het 'Model Informatiebeveiligingsbeleid' van SCIPR. De organisatorische inrichting op de andere veiligheidsgebieden kan eenzelfde route volgen als beschreven in deze paper. Hieronder lichten wij de inrichting van cybersecurity als voorbeeld toe.

Waaraan dient de inrichting van effectieve governance te voldoen?

De juiste inrichting van de cybersecurityfuncties is van belang om risico's te analyseren, beleid en prioriteiten te bepalen, medewerkers voor te lichten, de juiste maatregelen te laten treffen en deze na periodieke evaluatie zo nodig bij te stellen. Cybersecurity is niet met een technische exercitie of compliance-checklist op een hoog niveau te krijgen, wel met risicomanagement, prioriteitstelling en een multidisciplinaire aanpak.

Een gedegen governance en strategische positionering van cybersecurity waarborgen aanvullend dat de geschikte technische en organisatorische maatregelen getroffen worden om de relevante risico's af te dekken, en dat deze gehandhaafd worden én blijven. Daarbij mag het geen onnodige bureaucratie introduceren of een negatieve kosten-batenverhouding opleveren. Instellingsbrede besluitvorming en rapportering over cybersecurity dient efficiënt te kunnen verlopen en nevengeschikt – en dus niet ondergeschikt – te zijn aan andere beleidsterreinen. Dit zorgt ervoor dat nieuwe onderzoeksprojecten, samenwerkingen, e.d. het minimum cybersecurityniveau niet kunnen ondermijnen.

Dit voorstel betreft niet louter een structuurkwestie (het 'harkje'); natuurlijk zijn ook de bijbehorende processen, bewustwording, cultuur en wijze van persoonlijk opereren en communiceren onontbeerlijk om een hoger cybersecurityniveau te bereiken. Belangrijke uitgangspunten zijn dat het bredere veiligheidsbeleid integraal is georganiseerd en dat de governance aansluit bij het besturingsmodel van onderwijsinstellingen.

Hoe past de CISO-functie in de organisatiestructuur? ('verticale ophanging')

Het CvB draagt de eindverantwoordelijkheid voor risico's van de gehele instelling, inclusief die van cybersecurity. Ondersteunend hieraan is het proces van *Enterprise Risicomanagement* (ERM) dat risico's identificeert en inzichtelijk maakt, voorstellen doet voor risicobeperking en (rest)risico's monitort.

Het CvB belegt het informatie- en risico-eigenaarschap in de (1e) lijn en mandateert beleidsmakers en functionele experts in de beleidsstaf (2e lijn) om hen te helpen die risico's tot een acceptabel niveau te reduceren – dus niet om verantwoordelijkheid voor risico's of cybersecurity te nemen! Die 1e lijn bestaat uit het management in de faculteiten of instituten, maar ook in de ondersteunende diensten. Daar hoort ook het eigenaarschap voor cybersecurity te liggen.

4 NB: Voor privacy bestaat de wettelijke functie van Functionaris Gegevensbescherming (FG), die onafhankelijk toezicht houdt op en adviseert over privacy (vanuit de 3e lijn). Hierdoor is naast de formele FG-functie ook een rol weggelegd voor een Privacy Officer (vanuit de 2e lijn), die vergelijkbaar is met die van de CISO (m.a.w. voor privacybeleid, inrichten privacyrisicomanagementsysteem, inbrengen expertise, ondersteunen DPIA's, e.d.).

De aanvoerder voor cybersecurity is de CISO of Chief Information Security Officer. De CISO is de 2e lijn: de gemandateerde beleidsmaker, cyberrisicomanager en expertmatig adviseur van de 1e lijn. Dus niet de IT-specialist die beveiligingsmaatregelen treft. De CISO is op instellingsniveau beleidsvoorbereidend, ondersteunt de organisatie met hun lijnverantwoordelijkheid voor risicoanalyses van processen, projecten en inkopen, geeft expertadvies aan de 1e lijn en is één van crisismanagers bij incidenten. Een CISO rapporteert periodiek aan het CvB en de RvT over de voortgang op het jaarplan, risico's en een aantal kritieke indicatoren, zoals incidenten en veiligheidsbewustzijn. Het bestuur kan alleen met een goed overzicht de risico's overzien en op onderbouwde wijze de juiste keuzes maken. Ook vormt de CISO het interne én externe aanspreekpunt voor cybersecuritykwesties.

Grote instellingen beschikken daarnaast ook over een onafhankelijke interne auditfunctie (3e lijn) die de relatie tussen informatie/risico-eigenaren in de 1e lijn en beleidsmakers (2e lijn) monitort op effectiviteit. De meeste onderwijsinstellingen missen veelal een onafhankelijk orgaan dat de naleving van beleid en effectiviteit van het samenspel tussen 1e en 2e lijn toetst en vaststelt of de 2e lijn relevante risico's voor de organisatie ophaalt en monitort. Zij kunnen deze toetsende rol dan extern laten invullen, of die verwachten vanuit Raad van Toezicht, inspectie, Autoriteit Persoonsgegevens of accountant. De drie verdedigingslijnen zijn geadopteerd uit de private sector, waar dit zg. '*three lines of defence*'-model de de-facto standaard is voor organisatorische inrichting van risicobeheersing.

HO-instellingen zijn bijzondere instituten, waar het adopteren van dergelijke corporate governanceprincipes uit het bedrijfsleven naast een organisatorische aanpassing ook een cultuurverandering vraagt. Met het CvB als beleidsbepaler varen de faculteiten, instituten en hun decanen/directies deels een eigenstandige koers. Ze beschikken over beleidsvrijheid en eigen budget, beheren gebouwen en laboratoria, bepalen hun aanname-beleid, e.d. Om de gehele instelling op het minimaal vereiste cybersecurityniveau te laten opereren is het noodzakelijk dat de governance van cybersecurity alle organisatieonderdelen bereikt en betrekt. De decentrale mindset waarin deze faculteiten en instituten leven geldt niet voor IT en cybersecurity; zij zijn technisch te zeer met elkaar verweven. Een lokaal aangeschafte cloudtoepassing of een zelfstandig met internet verbonden lab kan niet alleen de kroonjuwelen van eigen onderzoek aantasten, maar maakt de gehele instelling kwetsbaar en kan ernstige verstoringen en datalekken veroorzaken.

De CISO heeft derhalve behoefte aan ondersteuning en voelsprieten in dergelijke organisatieonderdelen. Die voelsprieten zullen geformaliseerd moeten worden, bijvoorbeeld als een aangestelde '*Integrale Veiligheid liaison*', die adviseert en niet optreedt als politieagent. Deze IV-liaison moet de faculteit goed kennen (en anders-om) en affiniteit hebben met de veiligheidsgebieden. Verantwoordelijkheid, bevoegdheid en taken van deze functie dienen expliciet beschreven te zijn, evenals de functionele relatie met de IV-verantwoordelijken, zoals de CISO. Maar bovenal moeten de IV-liaisons voldoende tijd en aanzien hebben om betrokken te zijn bij projecten en ontwikkelingen die spelen en dienen zij naleving van cybersecuritybeleid te stimuleren. De CISO zal op regelmatige basis moeten overleggen met deze IV-liaisons om in de gehele organisatie geworteld te blijven.

Moet de CISO buiten IT worden gepositioneerd? ('horizontale ophanging')

In veel instellingen voor hoger onderwijs rapporteert de CISO aan de IT-directeur of aan de CIO, zowel functioneel als hiërarchisch. Alhoewel dat vanuit het verleden logisch verklaarbaar is en soms goed gedijt, is dit geen duurzame oplossing. De CISO schrijft beleid en risico- en compliancegebaseerde prioriteiten voor die ten dele door de IT-organisatie vertaald en ten uitvoer moeten worden gebracht. Ook ziet de CISO toe op de afhandeling van cybersecurity-incidenten die onder andere in de IT-organisatie kunnen zijn ontstaan. Dit maakt dat de CISO onafhankelijk van de IT-directeur c.q. de CIO moet kunnen functioneren. Het advies van de CISO aan het CvB moet soms anders kunnen zijn dan of zelfs tegenstrijdig kunnen zijn met dat van de IT-verantwoordelijke. Wanneer de CISO onder IT ressorteert, is er geen sprake van zg. '*countervailing power*' met voldoende checks & balances – er ontbreekt een gezonde tegenstelling van belangen. Kortom, een volwaardige CISO behoort buiten de IT-organisatie en het CIO Office gepositioneerd te zijn.

De CISO heeft natuurlijk een thuishaven en leidinggevende nodig, niet iedere beleids- of integrale veiligheidsfunctie kan tenslotte rechtstreeks onder het bestuur hangen. Een logische positie voor deze functie is bij één van de stafdiensten, bij andere 2e-lijnsfuncties. De CISO geniet daarbij nog steeds de vrijheid om het CvB onafhankelijk en (on)gevraagd te adviseren over beleid, om onderzoek te doen naar incidenten en om prioriteit te vragen voor nieuwe risico's. Bovendien kan de functie zo ook goed worden gesitueerd samen met de andere integrale veiligheidsgebieden; deze dienen samen te komen in een multidisciplinair integraal veiligheidsoverleg of bestuurlijk platform. De positionering van de CISO en de functionele lijn met andere (2e-lijns)staffuncties is essentieel voor het effectief kunnen uitvoeren van deze functie, net als een constructieve werkrelatie met de technische cybersecurityfuncties in de IT-organisatie.

"CISO's moeten CvB duidelijk maken dat cybersecurity veel meer is dan een IT-vraagstuk alleen."

Bibi van den Berg (hoogleraar Cyber Security Governance, Universiteit Leiden)

Hoe invulling te geven aan de eisen aan de CISO-functie?

De invulling van de CISO-functie kent verschillende taakgebieden op strategisch, tactisch en operationeel gebied die uiteenlopende, multidisciplinaire competenties vereisen. Belangrijke competenties betreffen in ieder geval het op bestuurlijk niveau en op managementniveau afstemmen over risicomanagement- en handhavingsvraagstukken en het uitdragen van noodzakelijke vervolgstappen. Natuurlijk moeten er naast een krachtige bestuurlijke en organisatorische focus ook een goede relatie en goede communicatie met de IT-organisatie zijn – zonder de technische oplossing te veel voor te schrijven. Deze combinatie van competenties is schaars en gewild. Duurzame aandacht, passende inbedding én inschaling van deze functie in de organisatie helpt om CISO's vast te houden.

De CISO-functie behelst meerdere rollen die door verschillende individuen of door één persoon kunnen worden uitgevoerd. Ook zijn enkele rollen heel duidelijk niet onderdeel van de CISO-functie: de Functionaris Gegevensbescherming (FG) gezien diens positionering en onafhankelijkheid; de technische security manager die zich bezighoudt met de inrichting van cybersecuritymaatregelen omdat die rol niet past naast die van beleidsmaker. Het is wel essentieel dat de CISO intensief samenwerkt met deze rollen om de (gepercipieerde)

afstand tussen de lines of defence klein te houden. Rollen die wel in de CISO-functie[5] passen (en momenteel nog niet zijn opgenomen in het functiehuis) zijn onder andere[6]: beleidsmaker cybersecurity, informatierisico-manager, adviseur veiligheidsbewustzijn en eventueel Privacy Officer (afzonderlijk van de FG).

Zoals aangegeven, is een CISO niet eindverantwoordelijk voor cybersecurity; de CISO is ook geen risico-eigenaar. De CISO (of iemand uit diens team) dient betrokken te zijn bij belangrijke projecten, inkopen en samenwerkingsverbanden. Derhalve ligt het budget voor cybersecurityactiviteiten en -projecten in de lijn respectievelijk bij opdrachtgevers, mits de als kritiek geclassificeerde cybersecurityprojecten ook daadwerkelijk worden uitgevoerd. Deze vorm van prioriteren en budgetteren dient verankerd te zijn in de planning- en controlcyclus en in het projectportfoliomanagement. Bovendien moet de CISO toereikend eigen budget hebben voor de strategische en tactische processen, zoals het opstellen van een meerjarenroadmap cybersecurity, het laten uitvoeren van technische (hack)testen en (SURF)audits, het inhuren van advies of het opschroeven van het veiligheidsbewustzijn van medewerkers en studenten. Bovendien dient dit budget ook toereikend te zijn om tijdelijk medewerkers uit andere organisatieonderdelen toe te wijzen om beveiligingsprojecten gerealiseerd te krijgen.

“Voor de CISO geldt: budget hebben is invloed hebben.”

Michel van Eeten (hoogleraar Governance of Cyber Security, TU Delft)

Welke aanbevelingen leiden tot succes?

Wij raden bestuurders van hoger onderwijsinstellingen aan:

- Organiseer cybersecurity integraal met andere veiligheidsgebieden op basis van risicomanagementprincipes.
- Positioneer de CISO-functie passend in de organisatie (als zuivere 2e-lijnsfunctie en in de relevante gremia). Voor sommige instellingen zal een ‘Leg uit’-optie met overbruggingsperiode en groeipad nodig zijn. Dit geldt bijvoorbeeld vanwege de huidige organisatiestructuur of -omvang en een reeds functionerende constellatie, waarin de CISO nog vanuit de 1e lijn opereert. Desondanks kunnen onze overige aanbevelingen onverkort worden opgevolgd.
- Rust de CISO uit met mandaat, budget en capaciteit om de jaarplandoelen te kunnen bereiken.
- Organiseer cybersecurityfuncties in de functiehuizen voor universiteiten en hogescholen en zorg voor adequate inschaling van de CISO-functie in het instellingsfunctiehuis om CISO met de benodigde competenties te kunnen aantrekken en behouden.
- Geef duurzame aandacht aan cybersecurity en investeer in de relatie met de CISO.
- Regel periodieke rapportage van de CISO aan het CvB (minimaal kwartaallijks) en de RvT (minimaal jaarlijks).
- Bewaak de balans in volwassenheid tussen het kwartet organisatie – mensen – processen – techniek in de voortgang van cybersecurity.

5 In kleinere organisaties kunnen verschillende IV-rollen door één persoon of een klein team worden ingevuld.
6 Voor de detailinvulling van de CISO-functie (en overige informatiebeveiligingsfuncties) verwijzen wij naar de hieronder vermelde publicatie over ‘Beroepsprofielen Informatiebeveiliging 2.0’.

- Draag zorg voor een vorm van informatiegovernance; de cybersecurityfunctie kan alleen goed functioneren als er zicht is op (minimaal) de kroonjuwelen, alsmede het eigenaarschap en informatiemanagement daarvan zijn ingericht.
- Stel een meerjarenplan op om het gewenste niveau voor de verschillende integrale veiligheidsgebieden te behalen én te borgen.
- Start gezamenlijk sectorbrede initiatieven op het gebied van cybersecurity, zoals het inkopen van producten of diensten (b.v. managed Security Operations Centers), het uitwisselen van kennis en personeel, e.d.

Referenties:

- Model voor Informatiebeveiligingsbeleid SCIPR
- Dreigingsbeeld IV-HO
- Cyberdreigingsbeeld hoger onderwijs
- Beroepsprofielen Informatiebeveiliging
- SURFaudit
- Cybersecurity white paper

PLATFORM
INTEGRALE VEILIGHEID
HOGER ONDERWIJS

Een initiatief van de Vereniging Hogescholen en VSNU

KPMG

POSITION PAPER

Definitive version, 20 april 2020

Cybersecurity governance in Higher Education

Comply or explain!

This Position Paper has been drawn up by the Platform for Integrated Security in Higher Education (IV-HO)[1] and it addresses the two areas 'Cybersecurity & Privacy' and 'Knowledge Security', as described in the 'Threat Analysis Report for Higher Education'[2]. In this paper, for the sake of simplicity, we use the term 'Cybersecurity' to elucidate the governance of these security areas. Integrated Security[3], and especially Cybersecurity, cuts through several other policy areas and overlaps with many of them, such as HR, legislation and regulations, finance and quality.

To put this in clear terms: Cybersecurity not only relates to the digital protection of information, but also encompasses the aspects of information security relating to knowledge, privacy, physical security and the continuous availability of information and IT.

Why does higher education need to catch up urgently?

Higher education institutions are by their very nature open: they are places where knowledge has to flow freely. In the past there was no need for any kind of 'Fort Knox' type of security and a mature Cybersecurity function. Traditionally, there was only a low level of awareness of information- and IT-related risks. However, times have changed; specific information within institutions has a high value and is extremely confidential (the 'crown jewels', such as personal data), the availability of information and IT facilities is essential, and the integrity of both research and study results crucial.

Recent incidents and a rising threat levels show that there is some serious catching up required within the field of cyber resilience. Cybersecurity is not only about preventing incidents, but also about rapidly detecting of and responding to incidents, and organising this capability.

1 Written by KPMG in conjunction with the IV-HO Governance working group. We are grateful to Cybersecurity professors Bibi van den Berg (UL) and Michel van Eeten (TU Delft) for their input and feedback. This Position Paper is not intended as a reflection of their views. The board members of the SCIPR (SURF Community for Information Security and Privacy) and the chairs of the CSC (Coordinating SURF Contacts) meetings have also given feedback on a draft version of this paper.

2 *Dreigingsbeeld Hoger Onderwijs*. In 2018, higher education institutions committed to organising and professionalising an Integrated Security policy both sector-wide and within each institution.

3 The other areas of Integrated Security, namely Social Safety & Security, Alarming Behaviour & Radicalisation, Internationalisation, Integrity, Building Security, and Working Conditions & Environment, do not fall explicitly within the remit of this Position Paper, although the same principles apply in these areas.

The Minister of Education, Culture and Science stated in her recent letter to Parliament that investments will be made in security awareness, monitoring (SURFcert, Security Operations Centres) and regular testing. The importance of Cybersecurity, and Integrated Security in a broader sense, within higher education has been recognised since 2018, as evidenced by the establishment of the IV-HO (Integrated Security in Higher Education) platform.

This Position Paper lays the basis for how Cybersecurity should be organised and in particular regarding the positioning and role of the Chief Information Security Officer as leader for accomplishing the transition needed.

This paper exemplifies the governance of Cybersecurity[4]. For further details, please refer to the 'Model Information Security Policy' produced by SCIPR (SURF Community for Information Security and Privacy). The organisational structure in the other security areas can follow the same path as described in this paper. The organisation of Cybersecurity is explained below as an example.

What conditions are necessary for effective governance?

Cybersecurity functions need to be organised correctly in order to analyse risks, determine policy and priorities, inform staff, implement appropriate measures and adjust these measures where necessary following regular evaluations. Cybersecurity strictly approaching as a technical exercise or compliance checklist is insufficient to raise Cybersecurity to a higher level; what is needed is risk management, priority setting and a multidisciplinary approach.

Proper governance and strategic positioning of Cybersecurity also ensure that the appropriate technical and organisational measures are taken to cover the relevant risks, and that these measures are applied, upheld and enforced. It is important to avoid introducing unnecessary bureaucracy or causing any negative cost-benefit effects. Institution-wide decision-making and reporting on Cybersecurity should be efficient and equivalent – therefore not subordinate – to other policy domains. This will ensure that new research projects, partnerships, etc. cannot undermine the minimum level of Cybersecurity required.

This proposal is not just a structural issue; the related processes, awareness, culture and manner of personal operation and communication are, of course, also indispensable to achieve a higher level of Cybersecurity. Important basic principles are that the broader Security policy must be organised in an integrated way and that the governance must be in line with the operational model applicable for educational institutions.

How does the CISO function fit within the organisational structure? ('vertical positioning')

The Executive Board has ultimate responsibility for the risks of the whole institution, including the risks of Cybersecurity. The Board is supported in this by the process of Enterprise Risk Management (ERM), which identifies and clarifies risks, puts forward proposals for risk mitigation and monitors (residual) risks.

The Executive Board delegates the information and risk ownership within the 1st line (of the three lines of defence), and mandates policymakers and functional experts within the policy-making staff (2nd line) to assist them in reducing these risks to an acceptable level –not to assume responsibility for risks or Cybersecurity! The 1st line comprises the management of the faculties or institutes, but also of the support functions. This is where the responsibility for proper Cybersecurity belongs.

Within the domain of Cybersecurity the CISO (Chief Information Security Officer) has the lead positioned in the 2nd line as the mandated policymaker, Cyber Risk manager and expert adviser for the 1st line. Consequently, the CISO cannot be the IT specialist who implements security measures. The CISO is responsible at the

4 NB: For privacy issues, there is the statutory position of a Data Protection Officer (DPO). The DPO independently monitors and advises on privacy (from the 3rd line of defence). As well as the formal DPO position, there is also a role for a Privacy Officer (from the 2nd line of defence), a position that is comparable to the CISO (in other words, this role is concerned with Privacy policy, organising the privacy risk management system, contributing expertise, supporting Data Protection Impact Assessments, etc.).

institutional level for preparing Security policy, supporting the organisation with their responsibility for performing risk analyses of key processes, projects and purchases and providing expert advice to the 1st line, and is one of the crisis managers in the event of an incident. On a regular basis the CISO reports to the Executive Board and Board of Governors on the progress of the annual plan, changes in risk levels and a number of critical indicators, such as incidents and security awareness. The Board can only effectively oversee the risks, and make the right, well-informed choices if it has sufficient and balanced overview of the risks. The CISO is also the internal and external point of contact for Cybersecurity issues.

Large institutions also have an independent Internal Audit function (3rd line), which monitors the effectiveness of the relationship between information/risk owners in the 1st line and policymakers (2nd line). Most educational institutions lack an independent body that checks the compliance with policy and the effectiveness of the interaction between the 1st and 2nd lines, and determines whether the 2nd line is identifying and monitoring the relevant risks for the organisation. They can hire an external party to validate compliance, or expect it to be organised by the Board of Governors, the Inspectorate of Education, the Data Protection Authority or the accountant. The 'three lines of defence' model have been adopted from the private sector, where this model is the *de facto* standard for how risk management should be structured within an organisation.

Higher education institutions are a unique type of organisations, where adopting such corporate governance principles from the private sector requires both an organisational and a cultural change. While the Executive Board determines policy, the faculties and their deans/MTs have a high degree of autonomy in setting their own direction. They have freedom of policy and their own budget; they manage buildings and laboratories, define their own hiring policy, etc. For the entire institution to operate at least at the minimum required level of Cybersecurity, the governance of Cybersecurity must reach and involve all parts of the organisation. The decentralised mindset in which these faculties and institutes generally operate does not apply in the case of IT and Cybersecurity; they are technically highly interconnected. A locally purchased cloud application or a lab with an independent internet connection can impact not only the 'crown jewels' of its own research, but also makes the whole institution vulnerable and can cause serious disruptions and data breaches.

For this reason, the CISO needs support and personal contacts in these organisational units. These personal contacts will have to be formalised, for example as an appointed 'Integrated Security Liaison', who advises rather than engages in policing. This Integrated Security Liaison needs to know the faculty well (and vice versa) and have affinity with the various (integrated) security areas. The responsibilities, authorities and tasks associated with this role must be defined clearly and explicitly; the same applies to the functional relationship with the people who are responsible for Integrated Security, such as the CISO. But above all, the Integrated Security Liaisons must have sufficient time and standing to be involved in current projects and developments and must also promote the compliance with the Cybersecurity policy. The CISO will need to have regular discussions with the Integrated Security Liaisons in order to stay rooted in the organisation as a whole.

Does the CISO need to be positioned outside of IT? ('horizontal positioning')

In many higher education institutions, the CISO reports to the IT Director or CIO, in terms of both function and hierarchy. While this may have a logical explanation based on past history and may sometimes be very successful, it is not a good long-term solution. The CISO has the task of prescribing policy and risk- and compliance-based priorities, which often must be translated and implemented by the IT organisation. The CISO also oversees the handling of Cybersecurity incidents that could have originated in the IT organisation. This means that the CISO must be able to operate independently of the IT Director or CIO. It must be possible for the CISO's advice to the Executive Board to sometimes differ from – or even conflict with – that of the head of IT. If the CISO resides within IT, there is a lack of countervailing power with sufficient checks and balances; there is no segregation of duties or healthy conflict of interests. In short, to be fully effective, a CISO must be positioned outside the IT organisation and the CIO Office.
The CISO obviously needs to have a base and a manager, because not every policymaking function or Integrated Security function can be report directly to the Executive Board. A logical position for this function is in one of the staff departments, with other 2nd line functions. The CISO will then still have the freedom to give the Executive Board independent, solicited or unsolicited security advice, to investigate incidents and to request priority for new risks. It also allows the function to be conveniently situated together with the other Integrated Security areas; these must be combined in a multidisciplinary Integrated Security Boar or Platform. The positioning of the CISO and the functional alignment with other staff functions (in the 2nd line) is essential for the effective performance of this function, along with a constructive working relationship with the technical Cybersecurity functions within the IT organisation.

"CISOs must make it very clear to the Executive Board that Cybersecurity is much more than just an IT issue."

Bibi van den Berg (Professor of Cybersecurity Governance, Leiden University)

How should the requirements of the CISO function be fulfilled?

Fulfilling the CISO function involves several different task areas at strategic, tactical and operational levels, which require a variety of multidisciplinary competences. Important competences include in any event: achieving agreement at administrative and management levels about risk management and enforcement issues, and implementing the necessary subsequent steps. This strong administrative and organisational focus must naturally be combined with a good relationship and good communication with the IT organisation – but without imposing technical solutions to an excessive degree. This combination of competences is scarce and in great demand. Retaining CISOs can be facilitated by giving sustained attention to the function and ensuring that it is properly integrated and has an appropriate salary classification within the organisation.

The CISO function incorporates multiple roles that can be fulfilled by different individuals or by a single person. A number of roles are also very clearly not part of the CISO function: the legally required Data Protection Officer (DPO), in view of his/her positioning and independence; and the technical security manager, whose task it is to organise Cybersecurity measures as this role is not compatible with the role of policymaker. However, it is essential that the CISO should collaborate intensively with these roles in order to minimise the distance (or

perceived distance) between the lines of defence. Roles that do actually fit within the CISO[5] function (and are currently not yet included in the job classification system) are, for example[6]: Cybersecurity policymaker, Information Risk manager, security awareness consultant and possibly Privacy Officer (separate from the DPO).

As explained above, the CISO does not bear the final responsibility for Cybersecurity, and is also not the risk owner. The CISO (or someone from his/her team) must be involved in important projects, procurement and collaborations. The budget for Cybersecurity activities and projects therefore lies within the line or with sponsors, provided that the Cybersecurity projects classified as critical are actually executed. This form of prioritisation and budgeting must be anchored in the planning and control cycle and in the project portfolio management. Additionally, the CISO must have an adequate budget of his/her own for the strategic and tactical processes, such as formulating a multi-annual Cybersecurity roadmap, commissioning technical tests (for hacking and other issues) and audits (including SURFaudits[7]), hiring temporary consultants, or raising the security awareness of staff and students. This budget must also be sufficient to temporarily assign staff from other organisational units to realise security projects.

"For the CISO, having budget means having influence."

Michel van Eeten (Professor of Governance of Cybersecurity, Delft University of Technology)

What recommendations will yield a successful outcome?

We advise the following recommendations for administrators of higher education institutions:

- Organise Cybersecurity in conjuction with other security areas on the basis of risk management principles.
- Position the CISO function appropriately in the organisation (as a purely 2nd line function and in the relevant bodies). For some institutions, an 'Explain' option with a transitional period and growth path will be required. This will be needed, for example, because of the current organisational structure or size and an already well-functioning constellation, in which the CISO still operates from the 1st line. Nevertheless, our other recommendations can still be followed in full.
- Equip the CISO with the necessary mandate, budget and capacity to achieve the objectives in its annual plan.
- Organise Cybersecurity functions in the job classification systems for Higher Education, and ensure that the salary scale of the CISO function in the institution's job classification system is sufficient to attract and retain a CISO with the required competences.
- Give sustained attention to Cybersecurity and invest in the relationship with the CISO.
- Organise periodic reporting by the CISO to the Executive Board (at least quarterly) and the Board of Governors (at least annually).
- Monitor the balance of maturity between the quartet of 'organisation – people – processes – technology' in the progress of Cybersecurity.

5 In smaller organisations it is possible for different Integrated Security roles to be fulfilled by a single person or a small team.
6 For the detailed description of the CISO function (and other information security functions), please see the publication on 'Professional Profiles in Information Security 2.0' shown in the References below.
7 SURF, the collaborative organisation for ICT in Dutch education and research.

- Introduce a form of Information Governance; the Cybersecurity function can only function well if there is a clear view of (at least) the 'crown jewels', and if their ownership and information management have been well organised.
- Formulate a multi-annual plan for the purpose of both achieving and safeguarding the desired level for the various Integrated Security areas.
- Introduce joint sector-wide initiatives in the area of Cybersecurity, such as the procurement of products or services (e.g. managed Security Operations Centres), exchanging knowledge and staff, etc.

References:

- Model for Information Security policy (SCIPR (SURF Community for Information Security and Privacy)
- Threat Analysis Report: Integrated Security in Higher Education
- Cyber Threat Analysis Report for Higher Education
- Professional Profiles for Information Security
- SURFaudit
- Cybersecurity white paper