Position Paper on 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.

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.

---

[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.

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 institutional level for preparing Security policy, supporting the organisation with their

[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.).

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 function[5] (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.

[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.

- 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.
- 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