13 CLIMATE ACTION
5 GENDER EQUALITY
11 SUSTAINABLE CITIES AND COMMUNITIES
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
8 DECENT WORK AND ECONOMIC GROWTH

Chambers Ireland Submission to the National Cyber Security Strategy 2019-2024 Mid-Term Review Consultation

February 2023

Chambers Ireland Perspective on the National Cyber Security Strategy

From a high level Chambers Ireland's view is that there are several fundamental and deep problems that exist within our national Cyber Security policy framework, the framing of this particular policy review lends insight into how this issue is being misframed.

Chapter 4, for example, of this consultation document mischaracterises the principle issue that we are facing as a country, it is not correct to say that there is "Increased Risk from Threat Actors", rather there is (belatedly) increase ***awareness*** of risks from threat actors. The risks were present and generally known in 2019 when the initial policy was formed, at least to those that had interest in the field and knowledge of it. Unfortunately, these risks were not apparent to those drafting our Cyber Security stance at that stage, and this is not to criticise the individuals involved but it strongly suggests that the scoping of the 2019 policy was deficient, and also supports the claim that the perspective of the Department of Communications in this, was limited.

From the standpoint of the business community, it appears the Department of Communications has taken a passive approach towards cybersecurity, as though the purpose of our national cyber security strategy was merely to meet our obligations under the Network and Information Systems Directive[1] rather than actually ensuring that our state's cyber security threats were minimised. These are very different roles, and should the National Cyber Security Strategy[2] refresh fail to reconfigure the National Cyber Security Centres goals, authority and resources to meet challenge of ensuring that our state's cyber security threats are minimised then our national vulnerabilities will persist.

[1] NIS Directive - ENISA - European Union

[2] National Cyber Security Strategy

Recent EU Law updates

It is welcome that the European Institutions are updating the original Directive through the Network and Information Systems 2 Directive[3], the Critical Entities Resilience Directive[4], and the proposed Cyber Resilience Act. The recognition of the need for deeper co-operation between members states is encouraging too, but the practicalities involved in delivering the aims of these directives are likely to be challenging in the Irish context. For example, talent generation and retention is likely to be extremely challenging for the Computer Security Incident Response Teams. Given our role as a hub for international software-as-a-service companies our state bodies are competing with such firms for the same small pool of talent. Moreover, anyone mission motivated for a role with the state is likely to see their skills rapidly atrophy in the absence of the form of persistent threats that are experienced by those active on the ground. State bodies have not been effective to date when it comes to building up Cyber Security professionals who have a deep knowledge of the networks they are managing and also the ground state of the threat environment.

Cyber Security Risks and the Irish Business Community

There are significant risks to Irish businesses and residents, both from large scale attacks such as the HSE incidents and the considerable risks that relate to misinformation campaigns. It is not reasonable to continue to assume that ours is a State that is too peripheral to be worth targeting – which seems to be the underlying assumption of much of our historical thinking regarding security. There is a tacit acknowledgement that with our shared history and border with Britain that there is a commensurate risk associated with their activities on this island, but that those

[3] NIS 2 Directive

[4] Critical Entities Resilience Directive

risks are not of an existential kind, ergo defence is a secondary concern for the state, particularly in the wake of the Good Friday Agreement.

Consequently, it seems as though our state response to Cyber Security operates from the premise that Ireland need only implement a risk-management response to Cyber Security events, as though Cyber Security risks are as stochastic as weather events. There are risks to Ireland, but these risks are ***security*** risks, they are non-independent. Attacks build upon the responses which we have had to the previous attacks. Should we continue to have a Cyber Security stance which is reactive and responsive to the attacks that have happened we will continuously be on the back foot because threat actors are deliberately carrying out these attacks and are planning these attacks.

The motivation that is inherent to Cyber Security threats means that we have to be proactive in our approach. This means that we need active surveillance of the threats, both at the state and the public level. We also need active responses to such threats (and this will need to be legislated for).

Our members are affected by Cyber Security risks in two distinct ways, through the direct effects of disruptive cyberattacks and the area of financially motivated cybercrime. Regarding cybercrime, commercial entities have a duty of care towards the business themselves and their customers to ensure that they have robust processes in place to reduce and ameliorate risk. Contracts often require Cyber Security insurance coverage, and this in turn leads to better practices being introduced in vulnerable sectors. The lack of digital skills in the workplace, particularly among medium sized businesses, is double edged. Inadequate technical skills can lead to Cyber Security vulnerabilities not being addressed, however the trend among our small to medium sized members has been to outsource much of their IT needs. The trend towards cloud email and CRM services to facilitate remote working and multiple devices etc. has inadvertently hardened many businesses that had been relying on only architecture like office mail servers, and we believe that this has been a net positive in terms of securing private businesses. Among larger scale firms [in terms of employee numbers], many or most (outside of sectors such as manufacturing) have extremely robust systems in place. Again, the changes induced by lockdowns and then requirements of flexible working have led most large employers to address their internal technical debt which was leaving them vulnerable.

The areas where our members have the greatest concerns are those areas where they cannot control the risks they are exposed to. These external events are the ones which are most likely to have effects beyond the individual firm level and are where the state has both the greatest potential to reduce the risks that firms are exposed to, in part because it is vulnerabilities within the State that expose the rest of us to considerable risk.

Responsibility for addressing State associated risks

Presently the department which has the primary responsibility regarding Cyber Security is the Department of Communications. As we averred to earlier, Chambers Ireland holds that this has resulted in a misunderstanding of the kinds of risks to which we are exposed the vulnerability that the State itself exposes the rest of our society and our economy.

Other elements of Cyber Security rest with the Department of Justice (the prosecution of detected crimes), and some parts rest with the Department of Defence (those that pertain to other States attempting to undermine the security of our State), the Departments of Education and Children have special responsibilities relating to the risks to minors, the Department of Further and Higher Education has a role to play in skilling up the workforce to address the Cyber Security skills gaps in the workforce, and the Department of Enterprise will have increased responsibilities particularly in relation to Cyber Resilience with the upcoming act.

These distributed responsibilities are not atypical, however Chambers Ireland members are concerned that Ireland’s traditional stance, re: neutrality, has left us particularly vulnerable to the defence relevant threats. Our national stance on defence is predicated on there being no state level foreign that is both capable and interested in undermining our security, and that the security threats which we otherwise experienced can be dealt with through typical counterinsurgency means.

Chambers Ireland believe that our state needs to significantly harden its institutions to the external threats which we are vulnerable to, if state bodies are to avoid continuing to be a serious risk factor for the people that live and work on this island.

To deliver on that threat reduction agenda we believe that the Department of Defence should become the primary department that has responsibility for Cyber Security, at least for the next decade, so that the institutional attitude to Cyber Security can alter from being one which is focused on process, where we merely implement and action EU directives, to being one which probes where our State's resources are weak, and mandates the changes that are needed if we are to avoid persistent vulnerability.

Evidently all other Departments will need to address their internal vulnerabilities, and certain Departments (including Communications, Enterprise, Education, Expenditure and Reform will all have extensive roles to play within their areas of responsibility). However, the framing of this consultation strongly suggests that our current Cyber Security policy is inappropriate to the challenges that we face. This implies that the Department of Communications probably doesn't have a broad enough perspective on the underlying risks to meaningfully tackle them within the lifetime of this Strategy, and so why we believe that the core responsibility should move to Defence.

Limitations to the existing National Cyber Security Strategy

The vision of the current National Cyber Security Strategy is far too narrow and its objectives are similarly limited. It must shift towards an active stance that seeks to prevent our businesses and our people from being vulnerable to the Cyber Security threats that our State institutions expose them to.

Our members do not believe that the State is sufficiently active when it comes to many of the Cyber Security threats that our members experience. There is no significant state capacity to ameliorate the intellectual property and espionage threats for businesses and we suspect that the issues are even greater within the public services. There ought to be a stronger counterespionage programme in defence of state security. Our Critical National Infrastructure assessment should be part of a broader Critical National Risk assessment which takes a much broader view on how Cyber Security can impact our prosperity, our quality of life, and our way of living.

It is critical that our National Cyber Security Strategy is a component of our National Security Strategy and should not be independent of it, there are aligned threats. As a result, we concur with the arguments of the Report of the Commission for the Defence Forces[5] that we need to significantly strengthen both our intelligence and our cyber defence capabilities, and think that the creation of a Joint Cyber Defence Command has merit. However, the issue that the broader civil service has regarding attracting those with Cyber Security skills, or alternatively the development and retention of individuals with such high demand skills, is even greater within the Defence forces.

Our sense is that Ireland would do better to emulate the Estonian model of integrating individuals with Cyber Security skills within the Defence context. For a start, we need to ensure that we can independently respond to Cyber Security threats as the emerge without relying on the likes of the British National Cyber Security Centre – not least because of their relationship to GCHQ which may modify their response capacity.

Should Ireland move towards the Estonian model it would allow for better integration between those who have the skills which the state needs and industry, which is where such people are most likely to find employment. It is unlikely that the state will have the resources to maintain an Incident Response Team at the highest level of readiness and skills development unless such people are working on such problems on a daily basis. We cannot rely on steady progression of defence recruits in the way that Estonia (arising from conscription) but we should make it easier for those that wish to participate in the Reserves to take an IT/Cyber Defence track, and have appropriate requirements and pathways for onboarding such talent. This way we could develop

[5] Report of the Commission on the Defence Forces

the teamwork and skills that are needed for the crises we are certain to encounter through exercises without having to compete on the open market in terms of salaries.

We could also develop a security clearance regime which would allow those within the private sector to contract into state bodies where there is a mismatch between civil service workforce plans and the conditions that individuals are likely to encounter when delivering similar projects and services in the private sector.

There is also a need for a much more active and effective counterespionage/intelligence response, to deal with Cyber Crime events. Much of the attitude towards Cyber Crime is that it is Criminal in nature, ergo it ought to the be Gardaí who deal with it, and it is 'Cyber' so it's criminality is novel in some essential way. Rather the novel element of is often that it is simply being carried out from another jurisdiction[6]. This creates a number of problems for our institutions, firstly the Gardaí struggle to maintain talent in this area as much as any other State body. Moreover, those that do work within this space for the Gardaí are often directed towards Child Sex Abuse Material which is a realm of activity which has an enormous burn-out rate and is rarely somewhere that individuals can persist in over the long run. Secondly, given the challenge of prosecuting Cyber Crime cases, and the extra-jurisdictional nature of the threats, crime agencies are actively incentivised to not record these effectively unprosecutable crimes. This suggests that the response to Cyber Crime needs to be of a different kind to other forms of crime, and our contention is that Ireland should shift away from a Cyber Crime approach to events and towards a more proactive Threat Analysis approach coupled with Active Cyber Defence.

Our exiting strategy amplifies our vulnerabilities

We know from our members, many of whom came to the State's aid in response to the HSE attacks, that the Cyber Security vulnerabilities of our State institutions are vast, and that the

[6] Cybercrime: Current Threats and Responses - A review of the research literature

attack surface is so porous that in some ways the HSE attackers went about their business the hard way – there were far easier pathways to accomplishing their aims, and many of those pathways remain open to future attackers.

The response of our members when the HSE was attacked was often to volunteer their own cybersecurity, and other IT generalist professionals to help get their local hospitals up and running. This was an ad hoc response, reliant on both good will and capacity. Good will can continue to be assumed as a given, however it is not clear that capacity to help can always be relied upon. A set of attacks that targets the private sector in combination with public sector attacks would result in an extremely diminished capacity to assist state bodies that are compromised.

In preparation for the next attack we **must** alter entirely how we address these challenges. Currently the stance of state bodies is at once distributed and centralised in the worst possible ways. No one is responsible for Cyber Security within our state institutions because everyone is responsible for security, meanwhile no one is empowered to make the necessary changes if the systems are to be strengthened, and no one can require action by another entity even if that body is exposing others to risk.

As a case in point, the National Cyber Security Centre has an advisory role for other state institutions. They can make a request of the National Cyber Security Centre to help inform their decision making with regard to cybersecurity, however they can’t mandate what the threat response must be, nor whether the threat response is effective. There are few institutions where individuals and employees are incentivised to actively highlight where procedures are ineffective or are creating vulnerabilities. This is true across all fields of endeavour, but is particularly true of bodies where the principal accounting officer also has a final say over human resources and staffing issues. As a result, Chambers Ireland believes that State bodies are uniquely vulnerable to creating systems architecture that are vulnerable to Cyber Security threats, and so expose the rest of us to a considerable extent.

We need the National Cyber Security Centre to have the remit to actively pursue vulnerabilities within other state institutions’ systems and that vulnerabilities which are discovered are published to firstly ensure that the body involved remedies the vulnerability, and secondly allows other bodies to learn from the errors of their peers. There shouldn't need to be a request to consult about an issue, rather sysadmins and Secretaries General should shiver when they receive an unsolicited email from the National Cyber Security Centre's red team.

The current attitude of state bodies to cybersecurity suggests that there is an unfounded belief in security through obscurity; State institutions seem to rely on them being too small, and Ireland too irrelevant, for such organisations to be targeted – at this stage, such an intuition has proven to be demonstrably false – we are both vulnerable to attack from abroad, and a location it is easy to conduct operations from. Ireland needs to accept these facts and then fully readdress what our response to Cyber Security is.