Meeting with Joint Oireachtas Committee on Transport and Communications Networks

Wednesday 26 May 2021

Opening Statement by Minister of State Ossian Smyth, T.D.

Chairman,

We meet today against the backdrop of the significant ransomware attack on the HSE that has very seriously impacted on the ability of our hospitals and wider health services to provide essential services to our citizens and on the frontline staff in the health service who have been working under extraordinary pressure over the last 14 months since the start of the pandemic.

Ransomware Incident Response

The National Cyber Security Centre has been supporting the HSE in dealing with the ransomware attack since the NCSC was notified of the incident early on the morning of Friday 14 May. Following this notification, the NCSC immediately activated its National Critical Cyber Incident Response Plan.

Since that initial contact, the NCSC has been working intensively to support the HSE and external contractors in the response to the incident and to restore essential services as quickly as possible. From the outset the NCSC has liaised with EU and other international partners to share information and to ensure that the HSE had immediate access to international cyber supports.

While steady progress is being made with regard to bringing systems and services back online, the HSE is best placed to provide updates on the restoration of services and is doing so on an ongoing basis.

The NCSC has also worked with the HSE and external experts to identify the technical details of the malware used in this incident, so that it can share these details with both its constituent bodies and wider, through advisories. The NCSC has issued public advice in relation to the cyber-attack on the HSE as well as general guidance on ransomware attacks. This information is available on the NCSC website and will be updated as required.

A dedicated team in the NCSC has also been providing specific guidance to its constituents, including Government Departments and agencies, together with operators of essential services, on appropriate measures they can take to reduce the risk of further ransomware incidents on their networks. Staff at the NCSC have been in direct contact with the operators of essential services and this will continue throughout the coming days.

The National Cyber Security Centre

I would like to provide the Committee with some information on the role and functions of the National Cyber Security Centre, including how it supports hundreds of organisations across the Irish public and private sectors, as those individual organisations seek to mitigate the risk of a cyber-attack.

The NCSC was established by Government Decision with a broad remit across the cyber security of Government ICT and critical national infrastructure.

It acts as a central contact point in the event of a government or nation-wide cyber security incident affecting the State. The NCSC also coordinates and supports the response to significant incidents, with the lead role being taken by the entity affected by the incident.

The Computer Security Incident Response Team (CSIRT) is the team within the NCSC that leads in responding to cyber security incidents. The CSIRT has achieved international accreditation. It is this team that engages with the affected body to support it in addressing a threat.

Information sharing is a key component of the work of the NCSC whereby it acts a source of expert advice and guidance, but also as a 'clearing house' for information. That is to say it takes in threat intelligence data, trends and risks data, from national, global and local sources, analyses them, and makes sure that those people who need that data get it, either to protect their own systems, or to assist them in carrying out their statutory roles. The NCSC is in regular and frequent communication with international counterparts and the exchange of information is a two-way street.

The NCSC also supports public bodies, operators of essential services and digital service providers to improve their cyber security posture and fulfil their obligations under the European Network and Information Security Directive. The NCSC takes a very proactive role to supporting these important bodies in continually building

their cyber security resilience through a range of initiatives, including by hosting seminars and workshops.

Resources

There has been a deal of commentary on the level of funding and resources allocated to the NCSC and to cyber security across Government. It is important to recall that in considering the overall resources available to the State in preventing, mitigating and managing cyber-attacks the principal investment made by the State is the very substantial investment made by individual Government Departments and public sector bodies in their own IT security infrastructure and IT security staff. In the case of Government Departments and non-commercial State bodies this money is funded from the exchequer and is many multiples of the figure of €5m quoted in commentary over the last two weeks.

The NCSC team is made up of highly skilled, specialist technical civilian staff, with skillsets in areas such as computer science, software engineering, malware analysis, information technology forensics, cryptography, software development, and cyber security compliance, as well as general cyber security skills. The expertise and competence of the NCSC team has been very much in evidence over these past 13 days in how the team has supported the HSE in dealing with the attack.

NCSC had a staff complement of 29 at the start of 2021. In addition to payroll costs, the NCSC has funding of €5.1 million available to it this year, compared with €1.7 million in 2020. I would stress again, however, that the principal investment in cyber security is in the form of the collective investment made by individual organisations.

Recognising that the environment in which the NCSC operates is extremely dynamic, a detailed capacity review of the NCSC is being undertaken to inform Government as to how the NCSC needs to evolve going forward. This capacity review is being carried out by an expert international consultancy and is due to report in the coming weeks in line with the timeline for completion of this work of Q2 2021 set out in the 2019 National Cyber Security Strategy.

I will consider the report of the capacity review and its recommendations together with Minster Ryan. Government consideration may also be required having regard to the focus of the report. It will inform the future development of the NCSC and will indicate the extent of any additional resources required to deliver its mandate,

the objectives under the 2019 Strategy and other emerging obligations arising at EU level.

Ireland's National Cyber Security Strategy 2019-2024

As I have outlined, the NCSC is working with stakeholders to strengthen cyber security across Government networks and critical national infrastructure. Ireland's National Cyber Security Strategy for the period 2019-2024 sets out an ambitious programme of measures to further develop Ireland's cyber security capacity. The key themes of the strategy are to **Protect,** to **Develop** and to **Engage**. This involves:

- the **Protection** of the State, its people, and its critical national infrastructure from threats in the cyber security realm,
- the **Development** of the Capacity of the State, of research institutions, of businesses and of citizens, and
- **Engagement** by the State, nationally and internationally, in a strategic manner, supporting a free, open, peaceful and secure cyber space.

An inter-Departmental Committee chaired by my Department oversees the implementation of the National Cyber Security Strategy. The Committee meets quarterly to review progress. To date good progress has been made in delivering the 20 measures in the five-year strategy. The capacity review will feed into decisions to be taken to ensure that this ambitious strategy is delivered in full.

Finally I want to put on record my gratitude to the HSE staff, the NCSC, external contractors, An Garda Siochana, staff from the Office of the Government CIO, international partners and others who have been engaged 24/7 in dealing with this appalling criminal attack.

I would be happy to take questions from the Committee with regard to the role and functions of the NCSC, though there may be questions that it would not be possible or appropriate to address in a public forum, in particular where doing so could disclose information which might assist criminals to identify potential vulnerabilities in IT security arrangements.

Thank you

ENDS