

CYBERSECURITY – THE NEW AND DYNAMIC HOT TOPIC

Samantha Fletcher Watts - Director and Head of Compliance
DMS Investment Management Services (Europe) Ltd.



Cybersecurity is a hot topic definitely here to stay for the foreseeable future but alongside the systems and IT infrastructure it governs, this is a topic that evolves and develops on a daily basis. There are numerous drivers of cyber attacks, political, hactivism, a new hacker cutting their cyber teeth and sometimes is just a lottery. Cyber attacks and incidents also come in many forms and many remain unidentified for long periods of time, particularly where they involve the theft of data. The data remains and a copy is taken therefore nothing is missed.

There has been a certain level of acceptance that every organisation will ultimately fall victim to some form of cyber event and with it a focus from the regulators of not only implementing effective controls and monitoring tools but also mandatory reporting requirements. The SEC, CFTC, FCA and the Central Bank of Ireland have all issued guidance and best practice documents outlining their expectations in this regard.

At a pan European level we have seen the NIS directive which came into force in August 2016, with Member States having until May 2018 to implement. In Ireland this implementation will be overseen by the Department of Communications, Energy and Natural Resources. The Directive establishes a framework for network and information systems to be prepared to respond to a Cyber event and the aim is to create a cybersecurity standard across all Member States. The Directive applies to those organisations

operating essential services and digital service providers. Essential services is considered to include energy, transport, banking, healthcare.

What can an organisation do to protect itself – some key steps:

- Identify critical systems and those containing confidential and sensitive data and prioritise these systems and their gateways for enhanced protection;
- Penetration testing and cybersecurity risk assessments by external parties are worth considering;
- Appointment of a Chief Information Security Officer who has a mandate for Cybersecurity and access to adequate resources and budget;
- Training and awareness of all staff;
- Don't forget mobile devices, home laptops and tablets etc;
- Have a clear incident management plan in place.

Training and education cannot be emphasized enough, employees are one of the key gatekeepers of the system and therefore they are also any organisations weakest link. Training and education around cybersecurity, in relation to levels of defense, some scare tactics regarding what a cyber event could realistically mean for the business and its employees and a constant awareness and vigilance programme all help to enhance and strengthen system based controls and protections.

Ultimately if or should I say when you are the victim of a cyberattack the impact is directly affected by your reactions in the initial stages it is therefore imperative that following notification of an attack you are not working out how to address but have in place a detailed incident management plan to guide you in addressing the issue and mitigating risk for your clients, your business and your employees. Know what external assistance will be required and who you will request this from, know who will make the key decisions required, know who will form the core incident management committee and what part each committee member will be required to fulfill.