HEALTH, SAFETY AND CYBERTHREATS

Croner-i
HR • Tax • H&S • Audit & Accounting

ABOUT CYBERSPACE AND CYBERATTACKS

Cyberspace is the term used to describe the electronic medium of digital networks used to store, modify and communicate information. It includes the internet as well as other systems used to support businesses.

We can state with some confidence that cyberspace is an integral part of modern society, and its associated systems bring many benefits to businesses in terms of efficiencies and effectiveness.

However, we can also state with some confidence that cyberattacks are becoming the number one threat to many organisations, particularly as the world becomes more connected through cloud services and the Internet of Things.

For those responsible for an organisation's health and safety management functions, cyberattacks may not be high on the agenda of risks to be managed. However, as the Health and Safety Executive's (HSE) business plan for 2018/19 notes, "cybersecurity is becoming a bigger issue across all sectors". One of its key strategic priorities is to ensure the threat from cybersecurity is adequately addressed in high-hazard businesses.

WHAT ARE CYBERTHREATS?

There are a number of potential "hostile" or "threat actors" who intend to use cyberspace for malicious purposes, be this for terrorism activity, other forms of crime, or state or industrial espionage.

These threat actors include criminals, terrorists, so-called "hacktivists" and even foreign states. Obviously, their relative resources, capabilities and motivations will vary depending on the particular profile.

It is often thought, from a cybersecurity perspective, that threat actors are typically outsiders to the organisation. However, such activity may also be perpetrated by insiders, former insiders, or outsiders working in collusion with an insider. This will include both direct employees and those from the supply chain with access to relevant systems.

The motivations for cyberattacks can be complex but include ideological reasons, personal financial reward, revenge, need (e.g. debt), conveying a political message, and so on.

For a successful attack, there needs to be an intersection of:

- capability — whether the attacker has the skills and resources required to mount an attack
- intent — if the target has value to the attacker and furthers their mission or objectives
- opportunity – are there weaknesses that can be exploited to execute the attack? These could be both technical and human weaknesses, e.g. via a targeted phishing campaign.

HOW DO CYBERATTACKS WORK?

There are several methods of cyberattack that threat actors utilise. The UK National Cyber Security Centre (NCSC) at www.ncsc.gov.uk publishes detailed information on the various methods used but, in summary, the most common attacks are as follows.

- **Phishing attack** — Where the threat actor poses as a trusted third party by email and requests personal data. This can also be used as a way to deliver documents which, when opened and with macros enabled, can download and install further malicious software. This is often the first stage in a more complex attack process which gives attackers an initial foothold in the IT systems.
- **Ransom attack** — Where the threat actor (hacker) compromises one or more systems, encrypting the data and blocking an organisation's access until a ransom is paid (ransomware). An example of this is the WannaCry attack which crippled the NHS in May 2017 – an attack the FBI recently attributed to the North Korean Government.
- **Distributed Denial of Service (DDoS) attack** — Where high volumes of data or traffic are sent to a site or system to deliberately overload it and make it unavailable. This can also come with a ransom demand, though not always.
- **Virus or malware attack** — These include Trojans, viruses and worms entering the system unexpectedly, e.g. through email attachments or when a certain link is clicked on. They run software that steals data, installs ransomware, or destroys information on the system.
- **Password attack** — There are two key areas of password attacks: a) where someone has reused their password on another system (say Yahoo mail, or other public website) – if this system is hacked, the password can be easily tested against other systems or websites; b) weak passwords, which can often easily be guessed by running computer programs that test thousands of passwords per second.

It is worth noting that in its most recent report on cyberthreats to UK business, the NCSC highlights the threat posed by the supply chain. This includes compromises to managed service providers (to gain access to data) and the exploitation of products prior to their supply.

THE HEALTH AND SAFETY CONTEXT

No matter how an attack occurs, the consequences to an organisation can involve significant financial loss and reputational damage. It can also result in other risks materialising, including those related to health and safety.

From a health and safety context, cyberattacks can be grouped into three distinct areas, as follows:

1. Attacks on Industrial Automation Control Systems (IACS) resulting in physical risks
2. Attacks resulting in the loss, unauthorised access, destruction, or other unintended use of electronic information and data
3. Attacks resulting in the disruption of operations, caused by the loss or interruption of electronic systems and networks such as Building Management Systems

Attacks on IACS

Industrial Automation Control Systems can include electrical, control and instrumentation systems, emergency shutdown systems, and fire and gas systems. All have safety critical applications.

In early 2017, the HSE published Cyber Security for Industrial Automation and Control Systems. Aimed at major hazard workplaces, the publication recognises that threats can originate not only from system networks but also software upgrades, maintenance activities and unauthorised access.

The document notes that IACS are increasingly merging with corporate systems and, together with the increased use of non-proprietary systems, “has led to modern IACS becoming potentially more vulnerable to cyberattack”.

An attack on an IACS could have significant safety implications. For instance, in December 2014, a malicious actor infiltrated a German steel facility. The adversary used a spear phishing email to gain access to the corporate network and then moved into the plant network. According to reports, the adversary showed knowledge in IACS and was able to cause multiple components of the system to fail.

They specifically targeted critical process components, succeeding in preventing a blast furnace from initiating its security settings when it should, which resulted in massive physical damage. This could have become a safety critical event, given the hazardous nature of the processes and materials involved.

Attacks on sensitive data

A cyberattack could have serious repercussions even in organisations that are not major hazard industries. Health and safety management systems can create considerable volumes of documentation containing sensitive business-related information, as well as personal data relating to employees or other persons.

Personal data can include information on accident/incident reporting forms, occupational health reports, and so on. With ever-increasing use of online reporting systems and outsourced occupational health services, the potential for cyberattack is clear.

The recently introduced General Data Protection Regulations (GDPR) requires the duty holder to hold personal data securely, and states that data shall be “processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing”.

Failure to protect sensitive health and safety data and its subsequent loss or theft could incur investigation and prosecution by the Information Commissioner’s Office – which can impose fines up to €20 million or 4% of an organisation’s turnover.

There may also be data relating to health and safety that is commercially sensitive, which the organisation may wish to keep out of the public domain. Accessing this data unauthorised and releasing it may cause considerable commercial and reputational damage to the organisation. In addition to the above, other consequences of the loss of general health and safety information could include the following:

- Resources may have to be invested to replace lost documentation and information (e.g. undertaking risk assessments again)
- Weakened defence against prosecution or civil litigation, due to an inability to provide evidence of previous good health and safety management because of permanently lost documentation
- Lost historical data that could assist in identifying and developing future risk control measures, leaving a knowledge gap

Preventing access to databases containing vital safety information due to a cyberattack must also be considered. For example, organisations interacting with the public often use databases detailing potentially violent service users. If access to this database is compromised, it could create additional risks to employees.

Attacks on BMS

The third area with possible health and safety implications can be described as operational. Building Management Systems (BMS), either standalone or integrated, can form part of many health and safety risk control systems. These systems control several environmental factors (e.g. ventilation, lighting, power, fire and security systems, etc).

As an example, many organisations now use automated access control systems as a security measure, to protect employees and prevent unauthorised access to certain premises. A cyberattack has the potential to override such systems, putting employees at risk from anyone gaining unauthorised access.

Similarly, a breakdown in communication systems such as those for lone workers may again put employees at increased risk.

THE H&S PRACTITIONER'S ROLE IN CYBER SAFETY

It is worth noting that the NCSC guidance, HSE publication and ICO guidance all focus on the overall management system required to ensure "cyber safety", and do not in any way suggest health and safety practitioners (or other risk specialists) should be experts in cybersecurity.

Just as most health and safety practitioners work from an advisory position to enable others within the organisation to manage risks, cybersecurity may need the input of a competent cyber risk specialist to support those with responsibility for managing systems.

The role of the health and safety practitioner is to assist in identifying the systems used directly for health and safety management — or that could have an impact on health and safety should they be attacked — and to work with IT security specialists to ensure they remain secure.

What's important is the partnership between the business and the IT security function to fully consider the risks. This is usually done through three lenses:

- **confidentiality** – what is the impact if the data in the systems is stolen or published?
- **integrity** – what is the impact if someone changes the system (a big area for health and safety and control systems)?
- **availability** – what is the impact if the system goes offline for a period of time? Can the business operate without it, and if so for how long?

With all of the above, organisations should define a sensible set of functional and technical controls to best mitigate the risks.

Croner-i

HR • Tax • H&S • Audit & Accounting

Further information

- National Crime Agency, www.nationalcrimeagency.gov.uk

This organisation works to protect the public from the most serious threats from organised crime. See the 2017-2018 report The Cyber Threat to UK Business, published in conjunction with the NCSC.

- National Cyber Security Centre, www.ncsc.gov.uk

The NSCS was set up to protect the UK from cyberattacks, manage major incidents and improve security through technological advancement and advice. It offers a wealth of guidance, services and resources for businesses, as well as weekly threat reports on current threat intelligence.

Publisher
Croner-i, 240 Blackfriars Road, London, SE1 8NW, United Kingdom.

Disclaimer

Every effort is made to ensure the accuracy of the information contained in this publication. Subscribers entering into transactions on the basis of such information should seek the services of a competent professional adviser as this publication is sold with the understanding that the publisher is not engaged in rendering legal or accounting advice or other professional services. The publisher, and the authors, consultants and editors, expressly disclaim all and any liability and responsibility to any person, whether a purchaser or reader of this publication or not, in respect of anything, and of the consequences of anything, done or omitted to be done by any such person in reliance, whether wholly or partially, upon the whole or any part of the contents of this publication.

Find out more **0800 231 5199**