Cybersecurity Awareness for NOCs and IFs

September 2020
Technology and Information Department

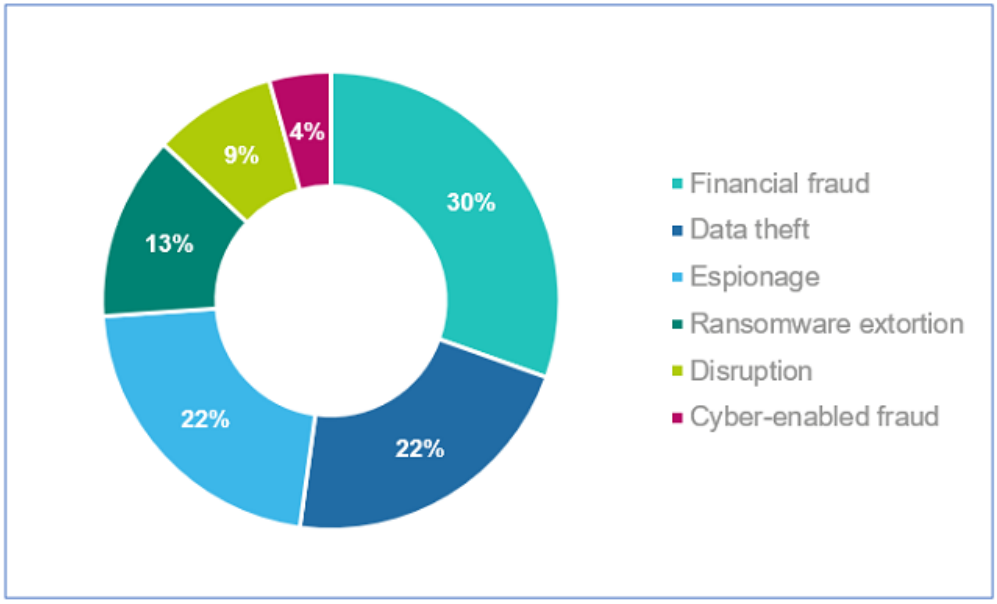
1. Introduction

The objective of this document is to provide some clear guidelines on cyber security and information security best practices that should be followed to prevent a negative impact on confidentiality, integrity and availability to IT services and data related NOCs and IFs. Cybersecurity and information security has become an increasing risk as Organisations continue to use and become more dependent on IT services.

Over the last months, the IOC has seen a number of attacks targeting the Olympic Movement involving the NOCs and IFs which include the compromise of NOC user mailboxes which have led to attempts made on financial fraud as well as a number of phishing campaigns leveraging the COVID-19 situation or the postponement of Tokyo 2020 Olympic Games in the aim of capturing user credentials to then be used by the malicious threat actors for their own personal gain.

As demonstrated in the report published by the UK's National Cyber Security Centre (NCSC) regarding cyber threats to the UK sports sector[1], sports related Organisations are heavily targeted by malicious individuals, criminal organisations and state sponsored hackers. Figure 1 shows their most common objectives.

Figure 1: Targeting of the sports sector globally (by campaign objective, 2017–20)



To protect your Organisation, your partners and the Olympic Movement, please read the following assessment and the related recommended guidelines.

2. Assessment

- Financially motivated cybercriminals pose the highest threat to sporting organizations through business email compromise (BEC), cyber-enabled fraud and ransomware attacks. Such campaigns were generally initiated using social engineering techniques.

- Cybercriminals are attracted to the large amounts of sensitive personal data held and significant financial transactions carried out by sporting organizations, and increasingly carry out cyber-enabled ticket scams during major events. Such criminals will likely also seek to target high-profile individuals representing sporting organizations for blackmail or extortion.

- Many operational technology (OT) systems at sporting venues are largely unpatched and open to remote management access. Less mature security practices, such as a lack of secure network design and weak user access controls, suggest a high threat from attackers with moderate capabilities.

Financially motivated attacks have typically leveraged on email phishing to gain access to user credential where systems have weak authentication with no multi-factor authentication allowing threat actors to maliciously access and amend data for the purpose of financial fraud.

The most common impact of such attacks has been business email compromise (BEC) leading to financial fraud.

Such criminals likely also have a high intent to target the sports sector's networked OT systems with disruptive ransomware, particularly as successful attack does not require the capabilities of a highly sophisticated threat actor.

3. Mitigation Recommendations

Sporting organisations face a wide range of cyber threats due to their high public profiles, the perception that these organisations are often very wealthy and the significance of major sporting events to many states' international relations. As such, sporting organisations should seek to understand their cyber threat profile and identify the key cyber threat groups that may be motivated to target their organisation and people, to build a proportionate and prioritised response to their threat environment. A Cyber and Information security risk assessment on the sporting organisation would be a recommended approach as a means to gain visibility on the most critical risks that require immediate attention for remediation.

The following sections provide some guidance on the type of cyber threats that should be reviewed for mitigation actions as they have been identified as common or reoccurring related to previous incidents that have tracked and monitored through press media and threat intelligence services.

3.1. Business Email Compromise: mitigations

- Use multi-factor authentication such as physical MFA tokens or mobile apps such as Microsoft Authenticator to reduce the impact of password compromises. Refer to the NCSC guidance on Multi-factor authentication for online services and setting up two-factor authentication (2FA)

- Make sure your users are using good and complex passwords and that they are managing them properly. Encourage the usage of password management tools, which allows to securely store all passwords in an encrypted format.

- Consider a Conditional Access policy to help reduce the impact of BEC. All major providers have user guides to help you design, build and manage your approach.

3.2. Cyber-enabled fraud: mitigations

- Make your staff aware about cyber threats and train them on identifying malicious e-mails and reporting security incidents. Consider running phishing tests to assess staff awareness level and to train your users in properly detecting malicious e-mails.

- Widen your defenses to include more technical measures to block malicious e-mails. For more information refer to the NCSC guidance on defending your organisation from phishing attacks

- Use effective anti-spoofing controls on your domains (such as for payment pages on websites and email domains) to reduce threat actors' ability to send fake emails purporting to represent legitimate organisations. For more information refer to the NCSC guidance on Email security and anti-spoofing.

3.3. Ransomware: mitigations

- Protect your devices and networks by keeping them up to date: use the latest supported versions, apply security patches promptly, use antivirus and scan regularly to guard against known malware threats. For more information refer to the NCSC guidance on mitigating malware and ransomware attacks.

- Keep safe backups of important files and business-critical data. Even if you decide to pay the ransom, there is no guarantee that you will get access to your computer, or your files. For more information refer to the NCSC guidance on mitigating malware and ransomware attacks.

- Segregate networks as sets: network segmentation (or segregation), involves splitting up a network into various network segments. This greatly increases the difficulty for an attacker to reach their goal once in the network, as their point of entry may not have any means of reaching the target data or system (e.g. If venue CCTV is compromised the attacker cannot easily reach the main cooperate IT network and vice versa). Systems and data that do not need to communicate or interact with each other should be separated into different network segments, and only allow users to access a segment where needed.

3.4. General cybersecurity: mitigations

- Make sure your Organisation documents and information are stored, protected and transmitted through your standard and controlled IT environment and tools (Microsoft 365, internal servers, etc.).
- Properly manage your privileged accesses as administrators accounts, systems and service accounts as they highly sensitive and as they provide access to a large number of resources.
- Consider using digital signature technologies to allow identifying legitimate e-mails and documents.
- Where possible, make sure activity logging is activated. In case of security incident, it will allow you to investigate what happen.

[1] http://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf

[2] http://www.darkreading.com/attacks-breaches/nba-players-financial-data-exposed-in-bec-email-scam/d/d-id/1325637