National Cyber Security Centre
a part of GCHQ

The Cyber Threat to Sports Organisations

Ensuring fair play online

The Cyber Threat to Sports Organisations

Contents

4 Forewords

5 Executive summary

6 Introduction

Source of statistics

How digitally reliant is sport?

8 Threat overview

Nature of the threat

Nation-state involvement

Major events

10 Attack trends

Trend 1: Business Email Compromise (BEC)

Trend 2: Cyber-enabled fraud

Trend 3: Ransomware

20 Venue security

Attack opportunities

Implementation of key technical controls

Venue security: mitigation

23 Risk management & industry trends

How important is cyber security and who provides leadership?

What is driving cyber risk management?

Risk management guidance

Forewords

Sports organisations are reliant on IT and technology to manage their office functions and, increasingly, their security systems at venues. As detailed in this report, cyber attacks can have a wide-range of impacts; from multi-million pound fraud to the loss of sensitive personal data. The NCSC is not just here to look after the IT systems of the UK government. We are committed to supporting the sports sector and we encourage you all to implement the guidance outlined in this report.

Ciaran Martin - Chief Executive Officer, NCSC

Cyber security is of ever-increasing importance to sports organisations, from grass roots clubs holding personal data through to national organisations hosting and participating in major international sporting events. Losing access to data, IT or technology can have a significant impact on sports organisations resulting in data breaches, fraudulent loss of funds and disruption to event delivery. Improving cyber security across the sports sector is critical. The British Olympic Association sees this report as a crucial first step, helping sports organisations to better understand the threat and highlighting practical steps that organisations should take to improve cyber security practices.

Rt Hon Sir Hugh Robertson, Chair of the British Olympic Association (BOA)

Executive Summary

- Sport is central to British life. It provides massive health, social and economic benefits to the nation, contributing billions of pounds to the UK economy each year. This power and profile make the sector a target for criminals and other cyber attackers.
- Cyber security is regarded as an important issue by sports organisations. Almost all those surveyed reviewed cyber security measures in preparation for compliance with the General Data Protection Regulation (GDPR). Statistically, this approach appears to have been successful at preventing mass data breaches.
- However, cyber attacks against sports organisations are very common, with 70% of those surveyed experiencing at least one attack per annum. This is significantly higher than the average across UK business.
- The primary cyber threat comes from cyber criminals with a financial motive. Criminal attacks typically take advantage of poor implementation of technical controls and normal human traits such as trust and ineffective password policies.
- There have been a small number of Hostile Nation-state attacks against sports organisations; typically, these attacks have exploited the same vulnerabilities used by criminals.
- The most common outcome of cyber attacks is unauthorised access to email accounts (Business Email Compromise) leading to fraud. Ransomware is also a significant issue in the sector.

The survey highlights the following key areas for sports organisations to review:

Email security

Good email technical controls are not routinely applied in the sports sector. Implementing measures such as anti-spoofing and multi-factor authentication can significantly reduce your cyber risk.

Staff empowerment

Under half of organisations provide staff training. Staff are an important line of defence and it is essential to encourage people to report any suspicious activity they spot.

Cyber risk management

Sports organisations are complicated. Survey results indicate that organisations would benefit from a holistic approach to Risk Management, looking beyond compliance (e.g. beyond GDPR) to ensure all cyber risks are considered across the IT estate.

Introduction

Sport is central to British life. It provides massive health, social and economic benefits to the nation, contributing to over £37 billion to the UK economy each year.

Unfortunately, this financial power makes the sector a target for criminals and other cyber attackers.

This report is designed to demystify the cyber threat to sports organisations by highlighting the cyber security issues that affect the sector on a daily basis: business email compromise, digital fraud, and venue security.

Along with descriptions of these common attack types, we include some statistics on their occurrence and suggestions for measures which will stop the vast majority of these attacks - or at least reduce their impact.

Sports organisations of all shapes and sizes will find this guide useful. From local clubs to national federations.

Source of statistics

The statistics contained in the report are primarily drawn from an Ipsos MORI survey, commissioned by the National Cyber Security Centre (NCSC). The survey explored experiences of cyber incidents and breaches, attitudes towards cyber security and its relation to physical security. All fieldwork was conducted in the spring of 2019.

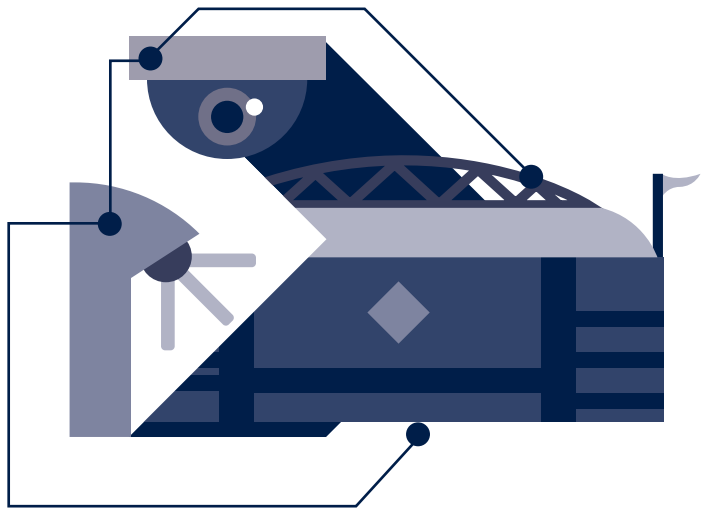
Ipsos MORI completed telephone surveys with 57 sporting organisations. This sample included sporting bodies and specific clubs, from sports such as football, rugby, tennis, cricket and athletics. This may seem a small sample size but, nonetheless, we feel it is sufficient to illustrate some trends and common challenges faced by this sector.

Eight respondents also completed in-depth, telephone interviews which lasted approximately 1 hour. The qualitative sample was made up of a mixture of sporting bodies and associations.

How digitally reliant is sport?

Like most of the UK economy, sport is highly reliant on digital technology. Sport is played in large venues with networked security systems controlling essential functions such as turnstiles and security cameras. Sports clubs and organisations hold a significant amount of sensitive personal data and process millions of financial transactions every year

The Ipsos MORI report revealed that almost all sports organisations have a website, social media account, and hold digital records containing personal information about customers, staff and volunteers. Over 80% of respondents had online business systems and offered customers the opportunity to make bookings, payments or purchases via the internet.

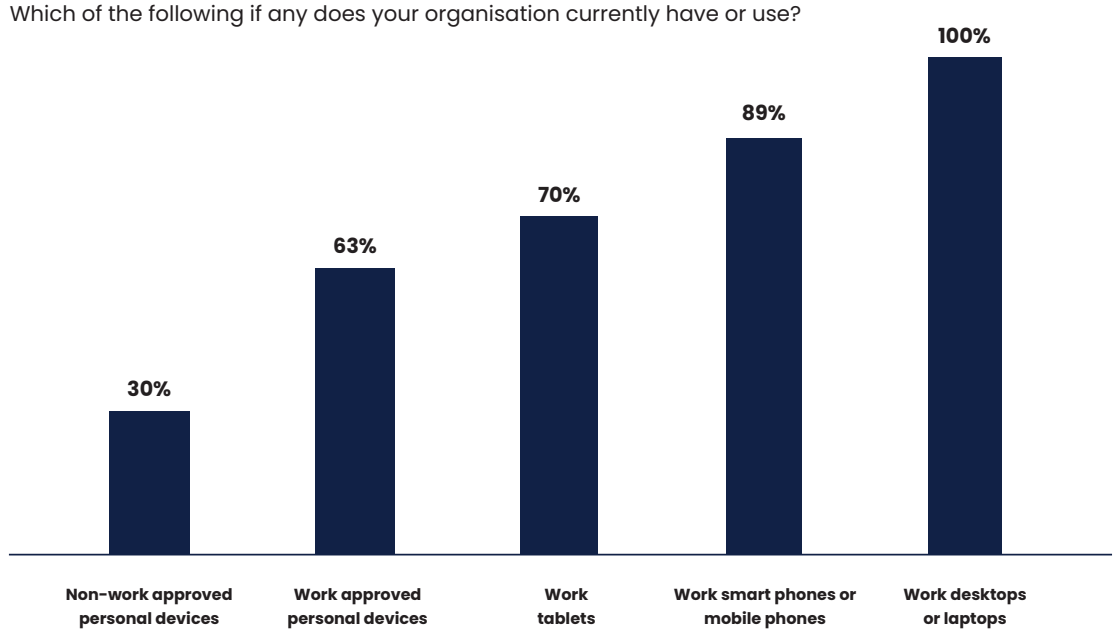


Sports organisations conduct a lot of activity online and the vast majority hold personal information on customers/employees

Which of the following if any does your organisation currently have or use?

Accounts or pages on social media sites	96%
A website or blog	95%
Personal information about your (customers/ beneficiaries/service users) held electronically	95%
Personal information about your employees held electronically	95%
Email addresses for your organisation or its employees or volunteers	93%
Internal online business systems	88%
The ability for customers to order, book or pay for services online	82%
A systems/database for sharing confidential, medical or performance data (players or athletes)	77%
An online bank account your organisation or your clients pay into	74%
An online sharing platform (eg Strava)	40%

Which of the following if any does your organisation currently have or use?



Threat Overview

At least
70%
of sports organisations have experienced a cyber incident or breach

30%
of organisations recorded over 5 incidents in the last 12 months

NCSC research indicates that the cyber threat to the UK sports sector is significant.

At least 70% of the sports organisations we surveyed have experienced at least one cyber incident or harmful cyber activity. This compares to 32% across general UK business, according to the DCMS annual breaches survey.

Around 30% of incidents resulted in direct financial damage to the victims, with costs varying considerably from under £500 through to over £100,000 per incident. The average cost was more than £10,000 per incident.

Beyond direct financial costs, 41% of breaches or attacks resulted in new measures being put in place to prevent further incidents.

Nature of the threat

The primary cyber threat to sports organisations comes from cyber criminals with a financial motive. Survey data, quantitative research and the NCSC's own incident data suggests that almost all criminal attacks are conducted using commonly available tools and techniques which don't need a lot of technical knowledge to be effective. These include phishing, password spraying and credential stuffing.

These low level attacks often take advantage of poorly-implemented security controls. For instance, ineffective password policies and known software bugs that aren't patched. They also exploit normal human traits such as trust, in order to gain unauthorised access to accounts or business systems. The outcome of these 'commodity' attacks varies, but often results in Business Email Compromise (BEC) or the delivery of malware.

In most cases, attacks are not targeted, sport organisations just happen to be victims of mass campaigns. However, major losses have been experienced by sports organisations as a result of bespoke attacks, where criminals have harvested information before undertaking fraudulent financial transactions.

Approximately
30%
of these incidents caused direct financial damage, averaging £10,000 per incident

The biggest single loss was over
£4m
(excluded from averages)

Nation-state involvement

Broadly speaking, the NCSC assesses that there is a remote chance of nation-states targeting the sport sector. However, there have been a small number of highly targeted incidents where nation-states have conducted cyber attacks against sports organisations.

The most high profile attacks were conducted by Russian Military Intelligence (GRU) against the World Anti-Doping Agency, in August 2016. The GRU stole confidential medical files from WADA's Anti-Doping Administration and Management System, then leaked sensitive information onto the internet.

The WADA hack was part of a wider campaign of malicious activity against sporting bodies likely conducted in retaliation for its athletes being banned from competing under the Russian flag. Consequently, we assess that the Russian threat to sports organisations is focussed on a small subgroup of organisations that hold, or have access to, sensitive athlete data. The likelihood of this threat materialising will increase if Russia's relationship with host countries or sporting institutions deteriorates in the run up to a major sporting event.

Major events

We assess that organisations which host major sporting events face a higher cyber threat than the industry average. The 2018 Winter Olympics in Pyeongchang were hit with an advanced and wide-ranging series of cyber attacks, reportedly causing disruption to the opening ceremony and the event's website. These activities were almost certainly conducted by a nation-state, with intent to disrupt the games.

It should be noted that major sporting events also face a heightened criminal threat. Quantitative research indicates that major events are targeted by cyber-enabled crime, such as 'spear phishing', and cyber-dependent crimes such as ticketing scams.

Attack trends

Attack types defined

Phishing

Phishing describes a type of social engineering where attackers trick users to 'do the wrong thing', such as disclosing information or clicking a bad link. Phishing can be conducted via a text message, social media, or by phone, but these days most people use the term 'phishing' to describe attacks that arrive by email. Email is an ideal delivery method for phishing attacks as it can reach users directly and hide among the huge number of benign emails that busy users receive. In a targeted campaign, an attacker may use information about your employees or company to make their messages even more persuasive and realistic. This is usually referred to as 'spear phishing'.

Credential stuffing

Credential stuffing takes advantage of the fact that people often use the same username and password combinations for more than one online account. By fraudulently gaining valid combinations for one site, and successfully using them on other sites, an attacker can access many legitimate accounts with a single set of credentials. The primary motivation is financial, but it can lead to identity theft.

Password spraying

Lists of a small number of common passwords are used in what's known as a 'brute force attack' on large numbers of accounts. These attacks are successful because for any large set of users, there will likely be some who are using very common passwords. These attacks can slip under the radar of security monitoring, which looks at each account in isolation.

Attack Trends - Percentage of organisations reporting attack activity

Access or business disruption	Website or online services taken offline	8%
	Temporary loss of access to files or networks	12%
	Distributed denial of service	14%
Data and systems breaches	Permanent loss of files	4%
	Software of systems corrupted or damaged	8%
	Personal data was altered, destroyed or taken	8%
	Unauthorised access or hacking into business systems	12%
	Malware: ransomware/spyware/virtues	39%
Fraud and Phishing	Hacking or attempting hacking of bank accounts	5%
	People impersonating the organisation in emails	30%
	Staff directed to fraudulent websites	61%
	Fraudulent emails, text messages or phone calls	75%

Trend 1: Business Email Compromise (BEC)

Research indicates that Business Email Compromise (BEC) is the biggest cyber threat to sports organisations.

BEC involves attackers seeking to gain access to official business email addresses, which they then use to engineer such things as fraudulent payments or data theft.

The primary motivation for BEC is financial gain. According to Action Fraud, BEC is one of the fastest growing cybercrime operations out there. It's 'low cost-high return' model is doubtless what attracts criminals.

How business email is compromised

BEC activity can be highly targeted and involve many layers. Techniques such as 'spear phishing', combined with phone calls and spoofed emails, are all deployed in order to obtain usernames and passwords from staff. Attacks are often aimed at users who have senior roles or can authorise financial transactions.

Business Email Compromise can also come about through industrial-scale technical attacks, such as credential stuffing and password spraying (see Attack types defined).
The outcomes of successful opportunistic attacks frequently involve auto-forward rules being put in place on a compromised email account, to steal sensitive information.

Once access has been achieved, attackers operate indiscriminately and may steal thousands of emails, before any tangible impact is identified by the victim.

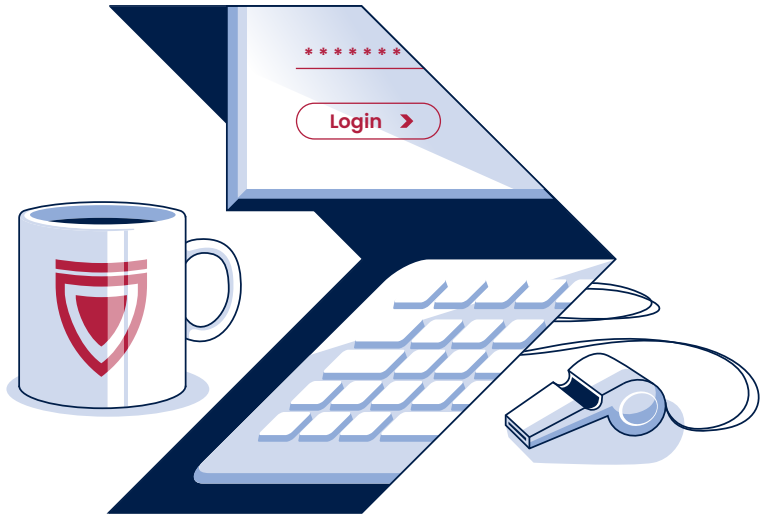
What makes Business Email Compromise possible?

The rise of Business Email Compromise has been facilitated in part by the increased popularity of Software-as-a-Service (SaaS) solutions, such as Office 365 and G Suite. SaaS normally offers access from anywhere as default, meaning anyone can logon with a valid username and password combination. This is great for the organisations using these services as it's cheap, convenient and flexible. However, it's important to do what you can to secure your organisation's accounts, so it doesn't end up causing more problems than it solves.

One of the best technical controls to reduce the risk of BEC is multi-factor authentication (MFA). MFA provides an extra layer of security for online services, preventing attackers from accessing them with passwords alone.

Survey results indicate that 51% of sports organisations already use MFA on some services, this is a key action area.

Research indicates that IT professionals often meet resistance from senior management when attempting to implement MFA. This may be due to concerns about harming the business by putting security 'blockers' in the way of working practices. So it is important to shape solutions that fit the business, such as implementing Conditional Access controls (see below) to ensure MFA fits your business context. Low staff awareness may also contribute to lack of adoption of MFA (see Cyber-enabled Fraud below).



Office 365 payment fraud targeting a Premier League football club

The Managing Director (MD) of a Premier League football club was the victim of a 'spear phishing' attack. When he clicked on the email, he was diverted to a spoofed Office 365 login page where he entered his credentials, unwittingly passing his email address and password to unidentified cyber criminals.

During the transfer window, the football club agreed a transfer with a European club worth almost £1 million. However, the cyber criminals were using the MD's credentials to monitor account activity and identified the impending transfer as an opportunity to monetise their attack. The attackers assumed the identity of the MD and communicated with the European club. Simultaneously they created a false email account and pretended to be the European club in communications with the real MD. At this point the football clubs thought they were talking to each other, but both were talking to the cyber criminals.

The cyber criminals sent an amended payment request to the MD, changing the real bank details to an account they had control of. The transaction was approved and the Premier League club almost lost £1 million. Fortunately, the payment did not go through. The cyber criminals' account had a fraud marker against it and the bank refused the payment. This highlighted the attempted fraud to the FA and the victim club.

Office 365 account compromise affecting a UK sporting body

An organisation that holds athlete performance data had been using Office 365 as its corporate email for several years. When a member of staff received an unusual auto reply from a colleague, they reported it to their IT team as suspicious. Investigations revealed that for several months the colleague's email account (and eight others) had been compromised by an unexplained rule that was auto-forwarding emails to one of three suspicious external email accounts.

Approximately 10,000 emails were found to have been sent to the external email accounts, many of these contained personal data and the Information Commissioner's Office (ICO) was notified immediately. The organisation was able to employ specialist legal and forensic advice provided through its Cyber Insurance policy, although there was significant cost to the organisation in terms of diverting internal resources and policy excess costs.

Because of the length of time from the initial breach, there was not a complete set of audit logs, and forensic investigations were unable to identify the source of the breach. However, to advise affected parties of the breach, the organisation had to contact well over 100 individuals whose sensitive data had been stolen.

The organisation did have a policy of enforcing strong passwords, but at the time of the incident had not enabled MFA for Office 365. Following the incident, the company implemented MFA for all Office 365 accounts and for other online applications processing sensitive data.

Business Email Compromise: mitigations

- Use multi-factor authentication 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)
- 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.

Trend 2: Cyber-enabled fraud

Cyber-enabled fraud is fraud which cyber technology facilitated. This can be contrasted with the situation where cyber is used to commit the crime itself.

In addition to BEC (see above), common cyber-enabled crimes include mandate fraud, CEO fraud, conveyancing fraud and invoice fraud. Across UK business, £2.3 billion was reportedly lost to payment diversion fraud alone, in 2018/19.

Survey results indicate that 75% of sports organisations have received fraudulent emails, text messages or phone calls. 61% have also identified staff being directed to fraudulent or fake websites. As with BEC, the primary motivation behind cyber-enabled fraud is financial.

'Email spoofing' plays an important role in cyber-enabled fraud. Spoofing is the use of a forged sender address on an email, to convince the recipient the email is genuine. Another technique favoured by fraudsters is 'typo squatting.' This is the creation of a website that looks like a genuine brand. For example a web site using gooogle.com rather than google.com. These are subtle techniques, used to redirect the victim, or convince them they are engaging with a genuine partner or company.

First line of defence

Only 46% of surveyed organisations have staff training, education and awareness programmes in place for cyber security. However, a mere 2% of sports organisations identified prevention of fraud as a primary cyber security objective.

Email spoofing

Not using available technical controls to prevent email spoofing may also contribute to the prevalence of cyber-enabled fraud.

At least 30% of surveyed organisations indicated that they had experienced people fraudulently impersonating the organisation in emails. Despite this, very few of the surveyed sports organisations have configured the three technical anti-spoofing controls recommended by the NCSC. These are, Sender Policy Framework (SPF), Domain-Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC).

DMARC is underutilised, with less than 33% of surveyed companies configuring the protocol.

What makes cyber-enabled fraud possible?

Cyber-enabled fraud often relies upon social engineering (normally phishing) to trick staff into making mistakes. It's essential to empower and encourage people to report any suspicious activity they spot. Also, to recognise that no amount of staff vigilance can ever stop all attacks, so you need to support your team with appropriate technical and business-focussed defences.

Payment fraud affecting a UK Racecourse

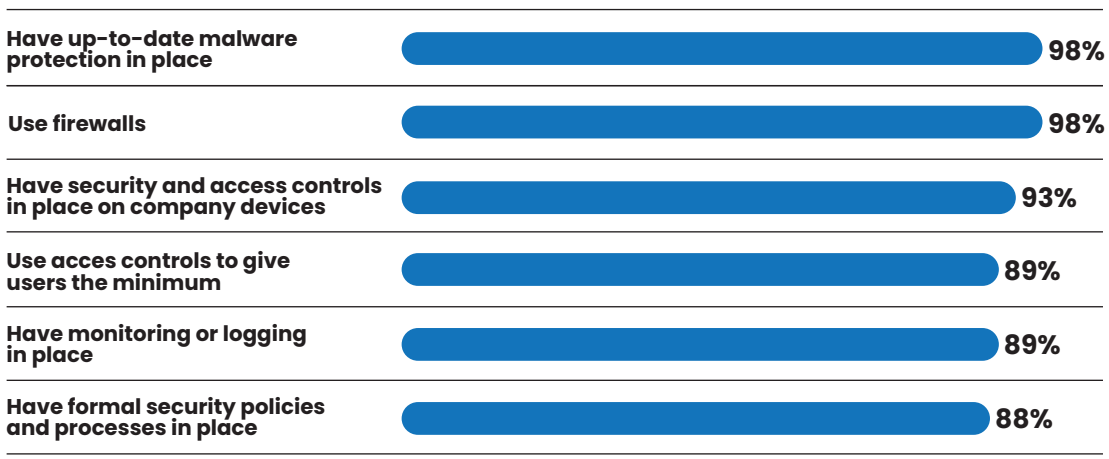
A member of staff at a UK Racecourse identified an item of grounds keeping equipment for sale on eBay. They exchanged numerous messages with the seller and the member of staff was convinced that both the seller and the equipment were legitimate. The seller asked for the staff member's email address to send more photographs of the item.

The parties agreed a price of over £15,000 and that the transaction would be completed via eBay. At this point the seller sent the member of staff bank transfer details via an eBay message, this diverted the member of staff to a spoofed version of eBay. The payment page looked legitimate and the member of staff believed they had confirmed this via an eBay customer services chat window; they went through with the purchase via bank transfer. The member of staff later realised that they had been tricked into a false transaction. The payment could not be recovered, resulting in a significant financial loss.

Cyber-enabled fraud: mitigations

- Typical defences against phishing often rely exclusively on users being able to spot phishing emails, an approach that will only have limited success. Instead, you should widen your defences to include more technical measures. For more information refer to the NCSC guidance on defending your organisation from phishing attacks
- Use effective anti-spoofing controls on your domains, making it difficult for fake emails to be sent from your organisation's domains. For more information refer to the NCSC guidance on Email security and anti-spoofing.

Implementation Security Controls (Business Systems)



Graphic 4: Implementation of security controls

Trend 3: Ransomware

Ransomware is a type of malware that prevents you from accessing your computer (or data that is stored on your computer). Whilst ransomware is less common than BEC and cyber-enabled fraud, the business impact of ransomware attacks can be disastrous.

Approximately 40% of attacks on sports organisations involved malware. A quarter of these involved ransomware.

Since 2018, ransomware attacks have been growing in impact. The criminals carrying out the attacks are taking more time to analyse victim networks and understand the 'value' of the target organisation.

Using network analysis and lateral movement within the victim's network, attackers try to ensure they have maximum impact on the victim organisation - potentially denying access to business-critical files and systems.

Ransomware affecting an English Football League club

An English Football League (EFL) club suffered a significant ransomware attack, which crippled their corporate and security systems. They were asked to pay a 400-bitcoin ransom which they declined. The attack encrypted almost all the club's end user devices, resulting in the loss of locally stored data. Several servers were also affected, leaving the club unable to use their corporate email. The stadium CCTV and turnstiles were non-operational, which almost resulted in a fixture cancellation.

The attack vector remains unknown, but the initial infection was likely enabled by either a phishing email or remote access via the CCTV system. All systems at the stadium were connected to one network (VLAN). This meant that the infection spread across the estate quickly.

The attack cost the club several hundred thousand pounds from lost income and remediation.

After recovering, the club identified the following factors:

- The IT estate had grown organically and very few security controls were in place
- Networks should be segmented to limit the impact of attacks
- They did not have an emergency response plan and had not conducted response exercises
- They had not recognised how digital/cyber reliant their business was, therefore, cyber security investment was low

The club subsequently recruited a new IT manager and have upgraded their systems and processes to minimise the risk of future attacks causing such significant damage.

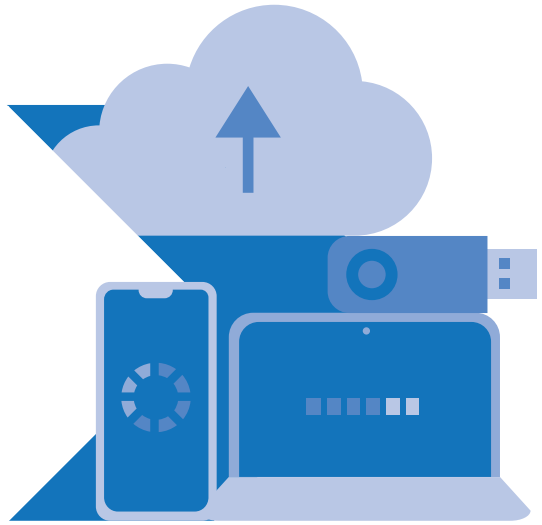
What makes ransomware possible?

Basic security controls such as antivirus, firewalls and user access controls are typically implemented by sports organisations (see Graphic 4).

However, 21% of surveyed companies do not have a patching strategy and 25% do not back up their data.

Patching is the business of ensuring your software and device operating systems are always kept up to date. This is an essential defence against ransomware, as ransomware often takes advantage of vulnerabilities for which patches already exist.

Equally, a lack of data backups increases the business impact of ransomware by making recovery more difficult and costly.



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.
- Keep safe backups of important files. 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 protecting your organisation from ransomware.
- 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.

Venue Security

90%

of head offices were based at the organisation's primary event venue

75%

of respondents agreed that cyber security was as important as physical security at their main venue

94%

stated that revenue from hosted events is important or very important to their business model

The ransomware case study highlights that modern sports venues rely upon complicated 'systems of systems,' combining normal office networks with internet-connected industrial control systems and physical security hardware.

Research suggests that venues tend to develop their IT estates over time, responding to emerging business needs, but without necessarily following a planned security architecture. This makes it difficult to fully understand all the ways an attacker can gain unauthorised access to systems or accounts.

The most common non-office systems in venues were CCTV (100%), payment systems (98%), turnstiles (90%) and industrial controls systems (ICS - 56%). These systems play a key role in event delivery, the revenue from which is central to the business model of 94% of those surveyed.

However, survey results indicate that security controls to protect stadium systems are less mature than those used for general business systems.

The following security themes were identified:

Attack opportunities

Unpatched systems

Around a third of surveyed companies do not have a patching strategy in place for their industrial controls systems, CCTV, turnstiles, and payment systems. This may reflect the fact that these systems are remotely administered (see below) or that systems are difficult to patch and in some cases impossible.

Unpatched systems offer a security weakness that attackers can exploit with basic off-the-shelf capabilities. It's important to understand and manage this risk, particularly where patching is impossible. Patching remains the single most significant thing you can do to secure your technology.

Remote access

Survey results indicate that 56% of CCTV, payment systems and turnstiles are remotely accessible by third parties. This offers attackers a potentially easy route into the network.

Remote access is not inherently bad for security, but it should be limited through security controls that make unauthorised logins difficult. Equally, authorised access should be limited to the system that the third-party is supporting (see Network segmentation below).

The survey results indicate that security controls are not universally in place, potentially leaving these systems open to unauthorised access using brute force password attacks, password spraying, and in some cases default login details such as 'Admin' and 'password'.

Impact amplifiers

User access controls

User access controls are present on most industrial control systems, CCTV, payment systems and turnstiles.

However, around 20% of companies do not use separate accounts for each user on their CCTV and payments systems. This rises to around 30% for CCTV and industrial controls systems.

These statistics are also reflected in the unnecessary use of administrative accounts, which allow fully privileged access to systems, when 'normal user' accesses would suffice. Sharing of accounts and the use of privileged accesses increases the risk of account misuse and gives attackers a better chance of acquiring privileged access through hacking.

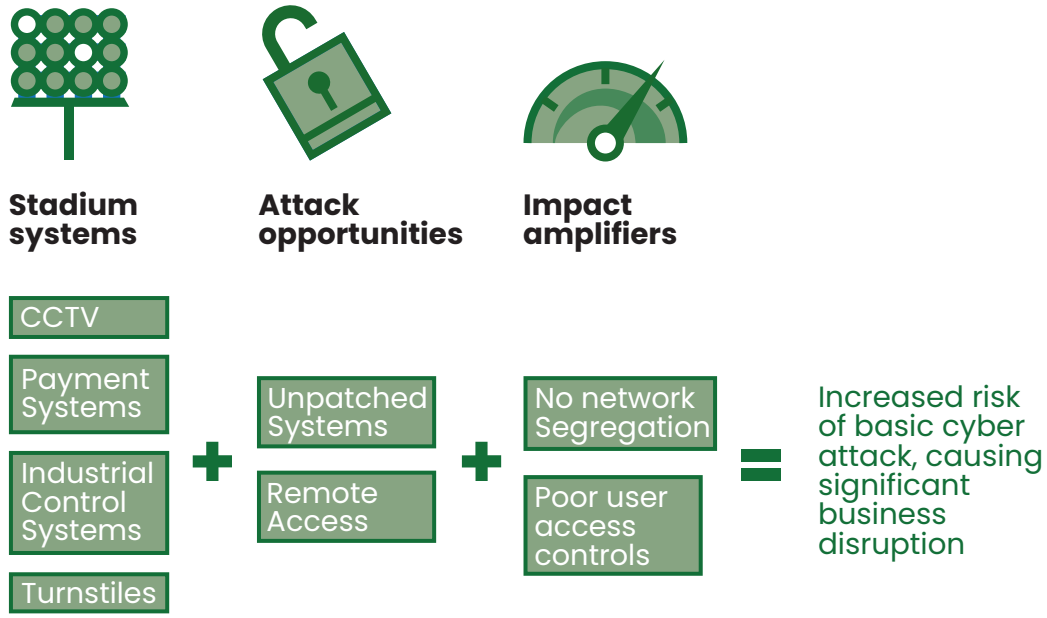
Network segmentation

Network segmentation makes it much harder for an attacker to reach their goal once inside the target network. It's essential for preventing breaches of individual systems spreading across an organisation.

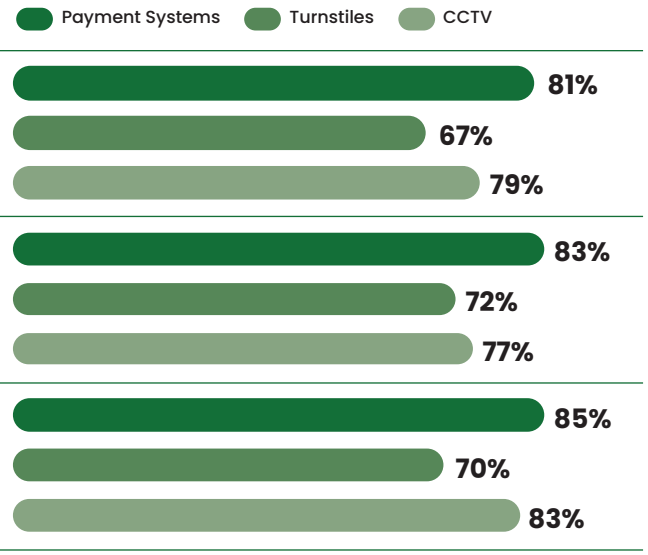
However, around 30% of CCTV, payment systems and turnstiles are not kept on a segmented network.

This means that attackers could use poorly protected systems (see Patching & Remote Access) as a route to access the critical business systems that underpin day to day operations.

For example, an attacker could gain access to a poorly protected or unpatched CCTV system and use it as a starting point to reach an organisation's main office network. Alternatively, the attack could work from your office network to your CCTV.



Impact Amplifiers



Venue security: 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.
- Restrict intruders' ability to move freely around your systems and networks. Pay particular attention to potentially vulnerable entry points e.g. third-party systems with onward access to your core network. Protect high privilege (admin) accounts and do not use them when a lower privilege account is sufficient. For more information refer to the NCSC guidance on preventing lateral movement.
- Operating your venue will almost certainly rely on third parties. The NCSC's guidance on supply chain security will help you assess the third parties you do business with.
- A 'Stadium Cybersecurity Best Practices Guide' is available to all members of the Cyber information Sharing Partnership (CiSP) - search CiSP on the NCSC website.

Risk Management & Industry Trends

How important is cyber security and who provides leadership?

Almost three quarters of those questioned by our poll believe that cyber security is a high priority for their organisation.

However, only a small proportion of those responsible for cyber security recognise it as their primary role. In most cases cyber security is part of a wider IT or general security remit.

Cyber security decisions are typically made at board level, with almost half of respondents being board members.

What is driving cyber risk management?

The implementation of GDPR in May 2018 appears to be driving organisational approaches to cyber security in the sports sector.

Almost all (96%) surveyed organisations reviewed their cyber security practices in preparation for GDPR, and protecting personal data was identified as the main reason to reduce cyber security risks.

Prioritisation of personal data protection appears to have been successful. Only 8% of surveyed organisations had experienced a personal data breach in the previous 12 months.

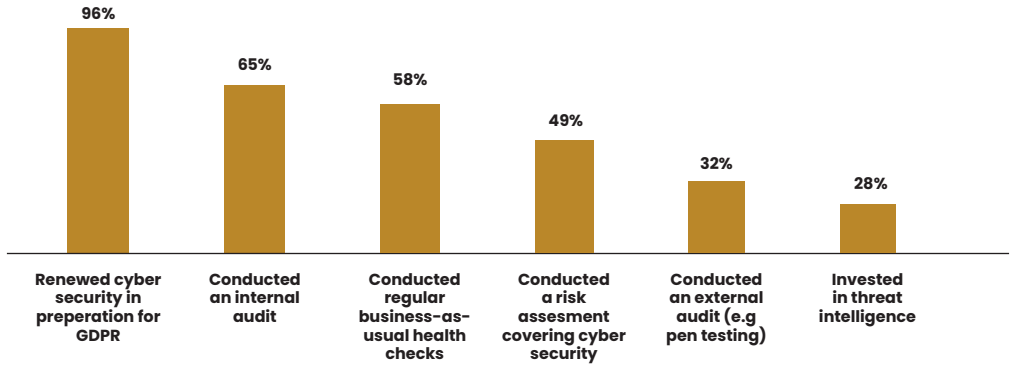
Beyond GDPR preparation, risk management was much patchier. 65% of surveyed companies have conducted an internal audit to identify their cyber risks, around 50% have conducted a cyber security risks assessment. Only one third have conducted an external audit.

The risk management impetus provided by GDPR preparations is reflected in the perception of cyber security priorities. Protecting personal data was cited by over half of the respondents as the main driver for reducing cyber attacks.

Business continuity, protecting the organisation's reputation and complying with the law were secondary drivers. Despite the high number of fraud-related cyber attacks that organisations experience, prevention of fraud and theft was not perceived to be a primary objective.

Graphic 9: Main reasons for reducing cyber risk

Cyber Risk Management processes used by organisations



Main reasons for organisations reducing cyber risk

47%

'strongly agreed' that they had identified data/ assets that could be targeted in cyber attacks

33%

'strongly agreed' that they had the right software and hardware in place to help protect the organisation from cyber attacks

28%

stated that revenue from hosted events is important or very important to their business model

25%

stated that revenue from hosted events is included or aligned to all our work systems and processes

Risk management performed for compliance reasons such as GDPR is sometimes described as 'defensive risk management'. This approach has limitations and can cause an excessive focus on protecting the organisation from being fined.

Defensive risk management is about being able to show that you haven't been negligent; the emphasis is on proving that something has been done. This is understandable, but it can mean that people focus on the wrong things, and do not identify and prioritise the security measures that would actually make their organisation safer.

It is likely that a tight focus on GDPR, rather than a more holistic approach to cyber security, has led to a lack of confidence among sports organisations that they have identified and mitigated cyber risks. For example, the survey results indicate that cyber-enabled fraud is one of the most common outcomes of cyber attacks. However, prevention of fraud was only cited as a primary cyber security objective by 2% of respondents.

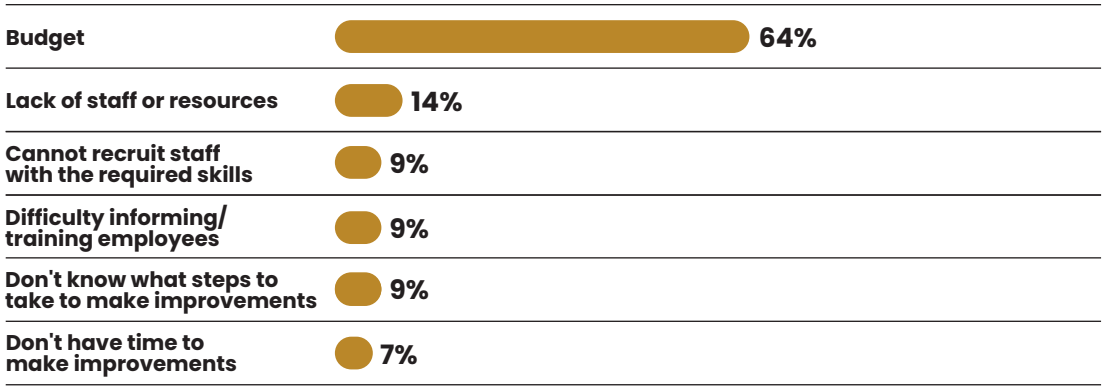
The survey findings regarding GDPR may also be indicative of budgetary pressures. Research suggests that GDPR preparation released money that would not normally be available to cyber security teams, allowing them to improve data protection practices. This is backed up by further research which suggests that 'budget' is the biggest cyber blocker for most sports organisations.

Risk Management Guidance

Risk management is about making informed decisions that balance an organisation's goals.

In the context of a sporting organisation, this is to balance cyber security against other forms of security, and indeed other organisational activities, such as running high-quality events, and outreach to young people. In this context, it is important to ground your risk management in what your organisation specifically cares about. You should start any risk management exercise by asking yourself, what specific eventualities are you trying to avoid? Once you have this clear understanding, the next stage is to consider how those eventualities could be realised. Advice on where to start is available in the risk management section of the Board Toolkit. The NCSC's 'Cyber security for major events' guide also provides basic, practical guidance. Both are available on the NCSC website.

What are the biggest blockers preventing further cyber security measures being implemented?



Actions checklist

Board Level

1 **Put risk on the agenda:** Discussions of what your organisation values, and what you're doing to protect it should be part of normal business.

Make time to cover these issues at your management meetings or weekly catch-ups. Find out where cyber security threats sit in the priority list, when compared to physical threats. The steps you take to reduce the risk to your business should be proportionate to the risks you face, and of course, affordable.

2 **Business Continuity:** Prepare your business for the most common cyber security threats by developing plans to handle those incidents most likely to occur. The best way to test your staff's understanding of what's required during an incident is through exercising.Consider using the NCSC's new Exercise in a Box product to test your organisation's resilience and preparedness.

3 **Cyber Awareness:** Empower your staff by helping them to understand why and how your organisation could be attacked online, and what they can do to help protect against these attacks. This will help them play their part in keeping the organisation safe.

IT Practitioners

4 **Make basic attacks more difficult:** Implement Multi-Factor Authentication (MFA) for important services such as email accounts. MFA buys a lot of additional security for relatively little effort. Organisations of all sizes can use MFA to protect their information and finances, and the services they rely on for day-to-day business. You should also consider the application of other technologies to manage accessto important services, such as conditional access and role-based monitoring.

5 **Reduce the password burden:** Review how your organisation uses passwords. To take some pressure off your staff, use technical security controls like blacklisting common passwords and allowing the use of password managers. Consider how you can identify or mitigate common password attacks such as brute forcing, before harm is done.

The Cyber Threat to Sports Organisations

@NCSC

National Cyber Security Centre

@cyberhq

Designed and created by Agent Marketing Ltd.
agentmarketing.co.uk