Cyber Security

# AVOID A CYBER SECURITY OWN GOAL

Lisa Ventura, CEO of the UK Cyber Security Association presents a guide to successfully tackling the growing cyber threat.

**WORDS:** LISA VENTURA

**In the busy world of football issues such as cyber security can often be put on the back burner. However, football clubs worldwide are just as susceptible to cyber-attacks as any other organisation and business - perhaps even more so.**

The data held by many football clubs is often seen as extremely lucrative, and this year alone the football world has been subjected to several cyber-attacks. Firstly, a wiki-leaks style hack published revelations from player contracts by Football Leaks, and recently FIFA confirmed that their computer systems have been hacked not just once, but twice.

### Why are football clubs being targeted by hackers?

Today, football clubs are effectively retail, hospitality and global entertainment companies, but many are only investing small amounts compared to organisations in other industries when it comes to defending against cyber-attacks. With the sheer breadth of football club operations stretching across many different industries, this makes them prime targets to a wide range of cyber-attacks. It is therefore important that football clubs take cyber security seriously and invest in their security infrastructure. But just how can football clubs secure themselves against the growing cyber threat?

### Types of cyber attacks for football clubs to watch out for

There are two main types of cyber-attacks that are often aimed at football clubs. While there are many kinds out there including trojans, malware and ransomware, it is often a Distributed Denial of Service (DDoS) attack or social engineering ("spearphishing") attack that is leveraged against them.

The high profile of football clubs makes their websites and social media channels a very attractive commodity to cyber criminals, and this is where DDoS attacks can come in. While many of these attacks are not related to the club or the sport in general, many high-profile organisations are used by activists, terrorists and extremists to promote their causes and to get their messages to a wider audience.

In addition to DDoS attacks social engineering, or "spearphishing" is also being increasingly used against football clubs leading to data breaches. It relies on the behaviour of the initial victim, requiring them to be very trusting, therefore attacks of this nature are better designed to "trick" the victim into allowing access to data. Football clubs need to have a greater awareness of the dangers they face and how to protect their services, customers, employees and brands from harm and reputational damage.

Many football clubs also hold more types of confidential and sensitive information such as the medical details of players and data relating to children. Financial and personal data is still a huge commodity for cyber criminals with the European General Data Protection Regulation (GDPR) placing increasing obligations for football clubs to secure personal data that is held by them, even if that data is processed and held by a third party. Clubs are increasingly becoming subject to other data protection legislation, especially as they engage with fans worldwide. For example, under Chinese cyber security legislation personal information that is generated or collected in China is to be stored domestically.

Football clubs also hold a significant amount of internal correspondence that is sensitive or confidential, and this will often have a large value to cyber criminals. For example, cyber criminals will often be interested in players' salaries and contract information and negotiations, clubs' transfer dealings, commercial leads and other sensitive or potentially damaging internal correspondence such as disciplinary information and HR documentations. If this data gets into the hands of cyber criminals and is made public it can often lead to reputational damage, be highly embarrassing or have a financial impact. If the club is listed, it could even have a market impact.

**"While many of these attacks are not related to the club or the sport in general, many high-profile organisations are used by activists, terrorists and extremists to promote their causes and to get their messages to a wider audience"**

**How can football clubs protect themselves from cyber attacks?**
There are many ways that football clubs can protect themselves against cyber-attacks, starting with a review of all the personal data they hold. GDPR won't be enough, since football clubs hold large amounts of fans' financial and personal data through ticketing and retail operations. What's more, fan engagement through social media channels should also be covered, as these channels pose a significant risk to data held.

The first step for any football club is to acknowledge that these threats are real and do exist, and to ensure accountability and leadership at Board level which cascades down. A full cyber security audit should be conducted, which requires a thorough understanding of what data is held where, along with a full understanding of the range of business-critical systems that are in operation at football clubs and training and awareness raising amongst all staff of the impact to the club if these were attacked.

Many studies show that exploiting users (i.e. humans) can often bypass expensive technical defences, so an affective cyber security strategy must encompass people, processes and technology in order for it to be successful. Cyber security is not just an IT issue, it is everyone's responsibility, and education amongst all departments and members of staff is key to guarding against cyber-attacks. Having a good IT architecture and basic IT hygiene, such as ensuring all software patches and updates are installed regularly, will often mitigate most cyber-attacks.

Preparing for the worst is always the right thing to do. Despite the best efforts of your cyber security procedures, policy and IT department determined or lucky cyber attackers will always stand a chance of getting through. The damage from a cyber attack often comes from organisations handling an attack or data breach badly, so preparing for the worst, both in terms of a business and media response and technical response is key to ensuring football clubs are resilient in the face of a cyber-attack. ■

**About the author – Lisa Ventura**
Lisa Ventura is the CEO and Founder of the UK Cyber Security Association, a membership association that is solely dedicated to individuals and companies who actively work in cyber security in the UK. She has over 10 years' experience in the cyber security industry and is passionate about raising awareness of being more cyber aware in business to help prevent cyber-attacks and cyber fraud.

**About the UK Cyber Security Association**
The UK Cyber Security Association (UKCSA) is a new membership organisation responsible for providing centralised contact for resources within the cyber security industry across the UK. It exists to support individuals and companies within the industry and works towards a specific set of objectives to promote the importance of cyber security for businesses and individuals.
**www.cybersecurityintelligence.com**

## CYBER-ATTACKS: 5 STEPS TO PROTECTION

There are five key things that all football clubs should do to help protect themselves from cyber-attacks:

**1. Ensure your systems are always up to date:** While there are many valid reasons why football clubs struggle to keep their systems up to date including the cost of this, ensuring you are running the latest version of Windows, Mac OS and other software is crucial. By updating your systems on a regular basis major issues are often fixed, and you are less likely to be compromised by a cyber-attack.

**2. Back up, back up, back up and back up again**: Backing up the data held by football clubs was previously a laborious process, but cloud storage solutions today are affordable, simple and fast. There are huge benefits to storing your data on the cloud and while there is still a small risk that these can still be compromised, your data will be protected against certain types of cyber-attacks such as ransomware. It is vital you make complete back-ups of your company files and data on a regular basis.

**3. Knowledge is key: Educate your staff:** The more training and awareness that your staff have of cyber fraud, the better equipped they will be to safeguard against potential attacks. With football clubs being more reliant and dependent on the internet than ever before, it is vital that you train all your staff to be cyber aware at a minimum.

**4. Conduct regular risk assessments:** There is much you can do to help protect your systems and business from cyber fraud internally but having regular risk assessments undertaken by a professional may highlight any areas that may have been overlooked. Cyber Essentials is a great place to start for this.

**5. Introduce a password policy:** Insecure passwords can often be a football club's weakest link, so review these regularly. Introduce a password policy that forces your employees to change their passwords frequently.■