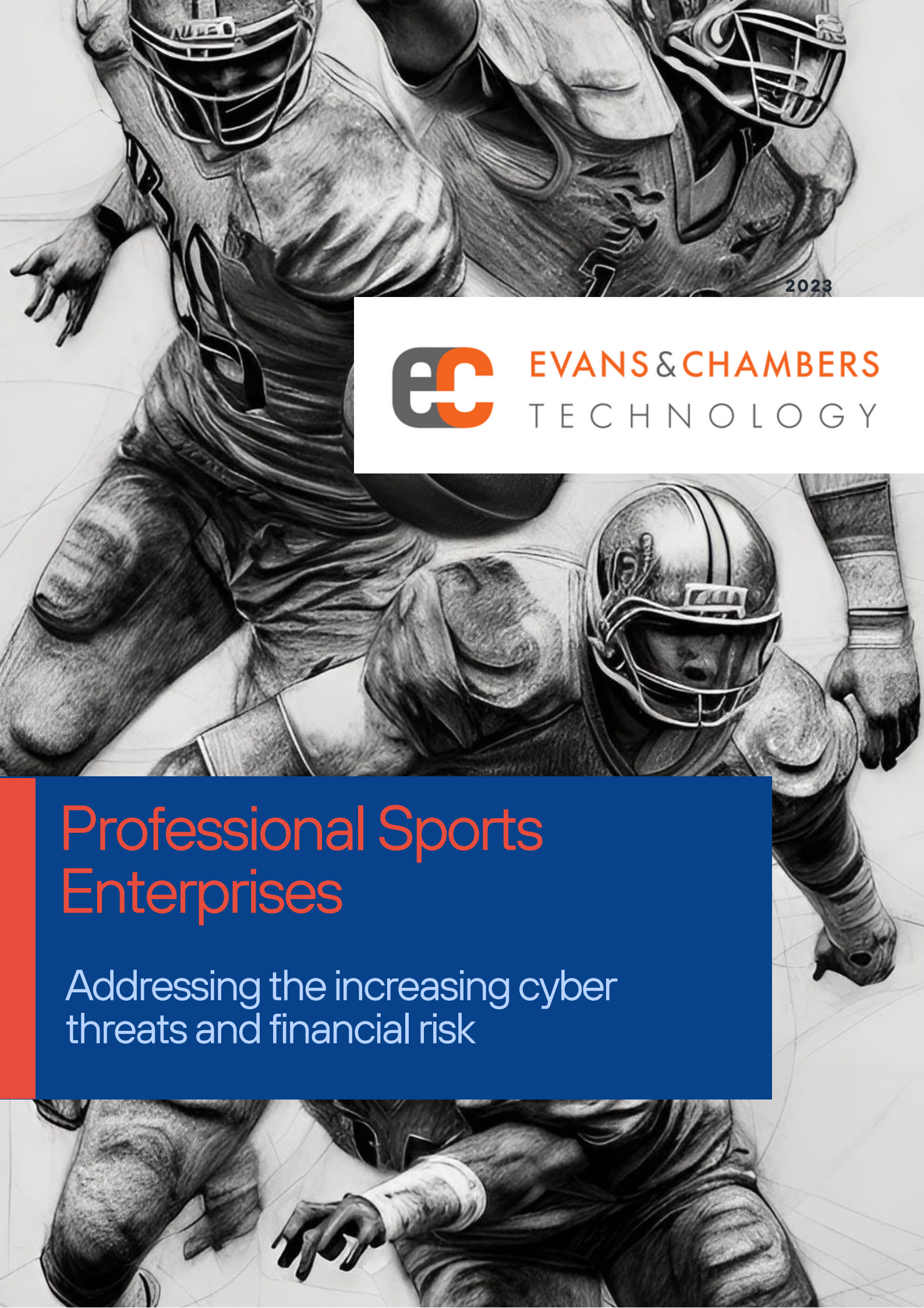


2023

EVANS & CHAMBERS TECHNOLOGY

Professional Sports Enterprises

Addressing the increasing cyber threats and financial risk

Table of Contents

Forward 3

Introduction 5

How Digitally Reliant are Sports Enteprises?

Threat Overview 6

Nature of the Threat

Nation-State Involvement

Major Events

Insider Threats

Attack Tendencies 8

Tendency 1: Ransome Ware

Tendency 2: Insider Threat

Tendency 3: Business Email Compromise

Tendency 4: Cyber Enable Fraud

Player Security 17

Venue Security 19

- Attack Opportunities
- Implementation of Key Technical Controls
- Venue Security: Mitigation

Sports Betting 22

- Nature of the Threat
- Nation-State Involvement
- Major Events

Risk Management & Industry Trends 24

- How Important is Cyber Security and Who Provides Leadership?
- What is Driving Cyber Risk Management
- Ten Cybersecurity Questions

Reliance on Technology

Professional sports organizations are reliant on IT, IoT and other technologies to enable fan and player engagement, venue operations and back office functions. This report details how cyber attacks can have a wide-range of impacts, from multi-million dollar frauds to the loss of sensitive personal data. Improving cyber security across the sports sector is critical. Losing access to data and systems can have a significant impact on sports teams.

10-8 Cyber has partnered with Evans & Chambers to look after the IT systems of professional sports team. We see this report as a crucial first step for team leadership to better understand the threat and highlight practical steps that should be taken to improve cyber security practices. We are committed to supporting your organization and we encourage you to call upon us.

Jamil Evans
President & CEO
Evans & Chambers

Gregory Crabb
Chief Executive Officer
10-8 Cyber

A High Value Target for Cyber Criminals

Professional sports are central to American life. They provide significant health, social, and economic benefits to the nation, contributing over $80 billon dollars to the US economy each year.

This power and profile make the sector a target for criminals and other cyber attackers.

- No league or event in global competitive sports has gone unaffected by a cyber event in the past decade. The NBA, NFL, MLB ,International Olympic Committee, and scores of others have endured a spectrum of cyberattacks event impacting event integrity, revenue, fans, stadium infrastructure, and personal security.

- As sporting event revenues increase and operations at sports stadiums become more dependent on data centers, cloud infrastructure, and IOT devices; the performance metrics and health data of athletes has become more vulnerable to illicit exposure or alteration. As a result, competitive sports has become increasingly vulnerable to cyberattacks.

- The primary threat comes from cyber criminals with a financial motive. These attacks take advantage of poor implementation of technical controls as well as human error such as insider access and ineffective password policies.

This report details the key attack types - from business email compromise to ransomware, from IoT hacking to player safety.

Cybersecurity risks are on the rise and many organizations need to initiate basic proactive measures to guard against them.

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

Common activities that increase cyber risks for Professional Sports Organizations:

- Accounts or pages on social media sites
- Unsupervised websites or blogs
- Personal information about your (customers, beneficiaries/service users) held electronically
- Personal information about your employees held electronically
- Unsupervised email address for your organization or its employees or volunteers
- Unguarded internal online business systems
- Storefronts to order, book or pay for services online
- A systems/database for sharing confidential, medical or performance data (players/athletes)
- Online banking for your organization
- Online sharing platforms (eg Strava)
- Discussing sensitive information during virtual meetings

Threat Overview

The Financial Damage a Multi-billion Dollar Corporation faces during an Incident

Estimating the financial damage inflicted by a cyber incident on a multibillion dollar corporation is a complex task that depends on multiple factors such as the type of incident, its severity, the company's response, and the potential long-term effects.

It is challenging to provide a specific estimate without additional information. However, factors such as lost revenue, compensation to affected parties, legal fees, and repetitional damage all contribute to the total financial loss.

Additionally, the stock market reaction and potential loss in market capitalization also play a significant role in determining the overall financial impact of a cyber breach incident.

Nature of a Cyber Threat

A cybersecurity attack is a deliberate and malicious attempt by an individual or group to compromise the confidentiality, integrity, or availability of a computer system, network, or data.

This can be achieved through various means, including viruses, malware, phishing scams, unauthorized access, and exploitation of vulnerabilities in software or hardware.

Organized Cyber Crime

Cyber organized crime against sports franchises is a growing threat, where cybercriminals target these organizations for financial gain or sensitive information. Hackers steal sensitive information such as confidential contracts or employee information. Additionally, sports franchises' websites and ticketing systems may also be targeted by fraudsters, who use phishing scams or card skimming to steal personal and financial information from fans. Sports franchises are particularly vulnerable to cybercrime due to their reliance on technology and their high-value target status.

Nation State Effect

A nation-state attack against a sports franchise is a cyber attack carried out by a government or government-sponsored group, with the intention of achieving political or strategic objectives. These attacks can be designed to steal sensitive information, disrupt normal operations, and compromise the franchise's computer systems and networks. The impact of such an attack can be significant, as sports franchises hold valuable information and assets, and are relied upon by fans, players, and employees. It is important for sports franchises to be aware of the threat posed by nation-state attacks and to implement robust cybersecurity measures to defend against them.

Attack Tendencies

Phishing

A type of online fraud in which an attacker attempts to trick a victim into providing sensitive information, such as login credentials or financial information, by posing as a trustworthy entity in an electronic communication, such as an email or text message. The attacker will often use social engineering tactics to convince the victim to click on a link that takes them to a fake website that looks legitimate, where they are prompted to enter personal information.

Credential Stuffing

A type of cyber attack in which an attacker uses a list of stolen usernames and passwords to automate login attempts on multiple websites. The attacker will use a program to repeatedly try the stolen credentials on different websites, in an attempt to gain access to an account.

Password Spraying

Password spraying is a type of cyber attack in which an attacker attempts to gain access to a large number of accounts by trying a small number of commonly used passwords against a large number of username or email addresses.

Information from the National Cyber Security Centre

Tendency One: Ransomware

Ransomware is a type of malware that encrypts files on a victim's computer and demands payment, usually in the form of cryptocurrency, for the decryption key. Once the malware is activated, it will typically lock the user out of their computer or encrypt their files, making them inaccessible. The attackers will then demand a ransom payment to restore access to the files or to the system.

What makes ransomware possible?

Typically ransomware is very hard to install onto a system. Although, there are many ways attackers can use to eliminate the difficulties and infect any computer system. Phishing emails that contain malicious files or attachments can potentially be the easiest way into a computer network.

Ransomware Mitigations

There are several steps that organizations and individuals can take to mitigate the risk of a ransomware attack:

- Use anti-virus and anti-malware software: use the software to detect and remove malware, including ransomware.
- Be cautious of unsolicited emails or phone calls. Do not open email attachments or click on links from unknown sources.
- Employee Education: Educate employees on the risks of a ransomware attack.
- Use endpoint protection: Use endpoint protection solutions to detect and block ransomware at the endpoint level.

By implementing these mitigations, organizations and individuals can significantly reduce their risk of a ransomware attack.

NFL Team Hit with a Devastating Ransomware Attack

Professional sports organizations are connected to a lot of people. The San Fransisco 49ers sent a formal apology to 20,930 people confirming a data breach by the ransomware group Blackbyte that affected the teams contracts, playbooks, and classified information.

While the team did not fully disclose the attacker deployed ransomware payloads, they continue to remediate the issue by restoring information on devices and security systems. On February 12, 2022, Blackbyte claimed responsibility for the attack and started leaking classified information to the general public.

Blackbyte published hundreds of megabytes of data stolen from the San Francisco 49ers. Although it is still unknown how much data was completely stolen from the attack in February, this is a warning to all sports organizations.

The 49ers organization stated, "We are also taking steps to help prevent something like this from occurring again, including additional measures to further enhance our security protocols and continued education and training to our employees."

Tendency Two: Insider Threat

An "Insider Threat" attack refers to an attack on an organization's network or systems that originates from within the organization. Insider threats can be unintentional or intentional, and they can take many forms, here are a few examples:

- Theft of confidential or sensitive data
- Misuse of company resources or intellectual property
- Insider trading or other financial crimes

What are the possible ways to mitigate insider threat attacks?

Possible ways to mitigate insider threat attacks include:

- Implementing security awareness and training programs for employees to educate them about potential threats and best practices for security.
- Conducting background checks on employees and contractors to identify potential risks.
- Regularly conducting security assessments and audits to identify vulnerabilities.

What makes an insider threat cybersecurity attack possible?

An insider threat attack is possible due to several factors including:

- Lack of security awareness and training for employees. Without proper training, employees may inadvertently fail prey to social engineering attacks.
- Insufficient incident response plans. Without a plan in place to respond to a security breach, organizations may struggle to contain the damage and prevent further attacks.
- Personal or financial problems of employees. Some employees may turn to insider threats due to personal or financial problems.

Overall, an insider threat attack can happen due to a combination of factors, it is very important for organizations to have a comprehensive security strategy in place to mitigate the risks and detect and respond to insider threats.

NFL Teams Worried about Potentially Losing Draft Picks and Playbooks

Back in 2020, during Covid, the NFL moved their operations online ahead of the 2020 draft in late April. The Baltimore Ravens were preparing for the draft by talking about their picks via zoom. John Harbraugh said this is a concern, he would not want opposing coaches and teams knowing who they may select in the draft. Furthermore, he would not want other teams knowing their playbook as well.

He is not alone, teams all around the country do not know how to react if opposing teams were to see their drat boards. Los Angeles Rams operating chief officer Kevin Demoff said the security aspect is a critical focus for teams heading into the draft.

Demoff said, "How do you make sure your conversations are protected? Hacking into a team's draft room on zoom is probably a lot different. That would be my biggest concern just from an encryption standpoint of how do you have these conversations confidentially?" Like Demoff, managers and coaches all around the league are very concerned about this issue. How do teams ensure online safety at a time with everything being online?

For sports organizations around the country and the world, technology is becoming more and more prevalent. Staying safe online from threats and opposing teams is of utmost concern. Draft boards and playbooks are just the start of what threat actors and opposing coaches can steal from a team.

Tendency Three: Business Email Compromise

A type of cyber attack in which an attacker targets an organization by compromising the email account of an employee, typically an executive or someone in a financial role, and uses it to request fraudulent wire transfers or sensitive information.

How can a business email be compromised?

There are many ways a business email can be compromised, here are a few:

- Malware: An attacker may use malware, To steal login credentials or gain access to the email account.
- Weak Passwords: An attacker may use a brute force attack to guess an employee's password if it is weak or easily guessable.
- Third-Party Breaches: An attacker may gain access to the email account through a third-party service provider that has been breached.

It's important for organizations to implement security measures to help them prevent these types of issues.

What Makes a Business Email Compromise Possible?

Hundreds of business emails become compromised everyday. Here are a few of the biggest reasons why:

- Lack of security measures: An organization that does not have robust security measures in place, such as 2FA.
- Lack of employee education: Employees are not educated on the risks of email compromise and how to recognize and avoid suspicious emails.
- Lack of monitoring and auditing: An organization that does not regularly monitor and audit email accounts for suspicious activity may not detect a compromise until it's too late.

By implementing strong security measures against email compromise, organizations can reduce the likelihood of a successful attack and respond quickly if a compromise does occur.

NBA Team losses contracts, negation details, and player data

Ransomware hits the National Basketball Association. The Houston Rockets have announced they detected system failures within their organization. The Rockets have called in forensic experts to help mitigate the issue. They have reported this maybe harder than they think. They have said, no employee, player or manager has been very much affected.

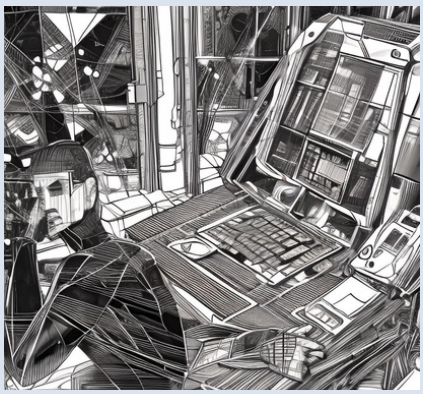
The initial report indicates the attacker attempted to place a ransomware attack on the Rockets computer systems, but failed. Once the Rockets found out about this problem they started the investigation. The closing reports say the hacker proved to be unsuccessful in terms of a big win. Although, minor damage definitely has occurred.

The Houston Rockets have also said they have lost over 500 gigabytes of data. This includes financial records, medical records and contract information. The attacker said the information will not be handed back to them until they pay the ransom. Is this really a win for the franchise? You have to pay to win?

The investigation remains in full swing, but early forensics reports indicate no sensitive data appears to have escaped from the system, according to InfoSecurity Magazine. Take the Houstons Rockets from example, even if the attack is called "minor", losing 500 gigabytes of classified information is not good for an organization.

Tendency Four: Cyber Enabled Fraud

Cyber enabled fraud in sports franchises refers to the use of technology and the internet to commit financial crimes within the context of sports organizations. This can include hacking into computer systems to steal sensitive information, using phishing scams to steal login credentials, or using other methods to steal money from the franchise. These types of fraud can have a significant financial impact on a sports franchise and can also damage its reputation if the public becomes aware of the breach.



What makes Cyber Enabled Fraud Possible

Cyber enabled fraud is becoming more and more possible not because the applications they use and buy from are becoming very overwhelming for security systems. The widespread use of technology, the ease of access to tools and information, and the anonymity of the internet are just a couple of examples of how technology is growing faster than the security measures can cover them all.

Cyber Enabled Fraud Mitigations

To mitigate the risk of cyber enabled fraud, its important for organizations and individuals to be aware of the risks and take appropriate measures to protect themselves, such as keeping software and operating systems up to date for example. Additionally, organizations should implement robust cybersecurity measures such as firewalls, intrusion detection systems and employee education.

Sports Referee Software Hacked Personal Information

A major company that providers software for sports referees, ArbiterSports, got attacked by a ransomware attack. During July of last year, over 540,000 referees were hacked of their personal information from this site. The company said that despite blocking and detecting multiple attacks that the breachers tried to steal encrypted data, they still managed to steal a copy of its backups.

ArbiterSports had backups containing sensitive data about users who registered on their site. "The passwords and Social Security numbers were encrypted in the file, but the unauthorized party was able to decrypt the data." the company said. The information included, email addresses, dates of birth, social security numbers, usernames and passwords.

The site said, the ransomware hackers reached out and demanded a hight price for the information back. In exchange, for the money they would delete the information they had gotten. The company said its paid the ransom demand and "obtained confirmation that the unauthorized party deleted the files." There is no guarantee that the hackers did not make a copy of the data before deleting it.

Right after the attack, no employee at ArbiterSports was too available for questions. The company since the breach said they have tightened up their practices and security. They would like to ensure their registered referees should not fear sharing their information again.

Player Security

Player cybersecurity in sports refers to the measures taken to protect the digital and personal information of athletes, hacking and other forms of online exploitation. This can include measures such as using secure networks and devices, implementing strong passwords and two factor authentication, and providing training to players on how to recognize and prevent cyber threats. Additionally, teams and leagues may also implement cybersecurity protocols to protect sensitive data such as financial information, game plans and scouting reports.

How could a cybersecurity attack ruin a players reputation?

A cybersecurity attack could ruin a player's reputation in a number of ways:

- Scandal: if a player is targeted by a cyber attack that results in the release of information about illegal or unethical behavior. It could damage their reputation and cause the loss of sponsorships and endorsements.
- Financial loss: If a player's financial information is stolen or compromised as a result of a cyber attack, it could lead to financial loss and damage their reputation.
- Injury of personal relationship: If a players personal relationship is targeted in a cyber attack, it can ruin their reputation and cause them to lose that trust and support of friends, family and fans.
- False accusations: A cyber attack can sometimes plant false accusations and information about a player which can harm their reputation and career.

Overall, players need to take steps to protect themselves from cyber threats and have a plan in place in case they do fall victim to an attack.

What makes a player cybersecurity attack possible?

Player cybersecurity attacks are much more common that you think. If a player has too much public information, lack of awareness and if an attack is targeting professional player information. That could all lead to a possible loss of reputation and personal information. The most common ways players can be targeted include account takeovers and social media impersonation.

What are the possible ways to mitigate cybersecurity attacks against players?

Players also need to know that there are ways they can negate their losses, even if they get into a potential cyber crime.

- Being cautious of phishing scams: Players should be cautious of phishing scam and not click on any links or provide personal information unless they are certain it is legitimate.
- Keeping personal information private: Players should be careful about the personal information they share online and limit the amount of personal information they have available on social media and other public platforms.
- Having cyber insurance: Teams and leagues can also consider purchasing cyber insurance, which can help them recover from a cyber attack and minimize the damage to the team and the players.

These are some of the most effective ways to reduce the risk of cyber threats and minimize the damage in case an attack does occur.

Venue Security

Venue cybersecurity refers to the measures taken to protect the digital infrastructure of venues such as stadiums, concert halls, and other public gather spaces from cyber threats. These measures may include protecting against hacking, data breaches, and other types of cyber attacks.

This includes protecting various types of technology that are used in these venues, such as WiFi networks, point of sale systems, ticketing systems, and other digital infrastructure. It also involves protecting the personal data of guests and employees, such as credit card information, contact information and other sensitive data.

Venue cybersecurity is important as venues are often a target for cyber criminals due to the number of people present in them and the sensitive information they hold, like credit card information and personal data.

Protecting the infrastructure of these venues can prevent financial loss, reputational damage and most importantly protect the guests personal data.

What makes venue cybersecurity attacks possible?

There are several factors that can make venue cybersecurity attacks possible:

- Outdated software and systems: Venues may have outdated software and systems that are vulnerable to known exploits.
- Lack of monitoring and logging: Venues may not have proper monitoring and logging in place.
- Human error: Employees may inadvertently open malicious emails or click on links in emails.

By understanding these factors, venues can take steps to mitigate the risk of a cyber attack, such as updating software and systems, implementing strong access controls, and having incident response plans in place.

What are possible ways to mitigate venue cybersecurity attacks?

Possible ways to mitigate venue cybersecurity attacks include:

- Regularly monitoring and analyzing network activity for unusual or suspicious patterns.
- Keeping software and security systems up-to-date with the latest patches and updates.
- Regularly backing up important data and maintaining disaster recovery plans.
- Conducting regular security assessments and penetration testing to identify and address vulnerabilities.

How could a Venue cybersecurity attack ruin a franchises reputation?

A venue cyber security attack can ruin a franchise's reputation in several ways:

- Loss of customer trust: If a cybersecurity attack results in the loss of personal, and financial information for customers, it can lead to a loss of trust and confidence in the franchise.
- Financial Loss: Cybersecurity attacks can also result in financial loss for the franchise as they may have to pay for damages, compensation, and legal fees.
- Reduced ticket sales: If the cyber attack causes the cancellation of the event, it can result in the loss of revenue from ticket sales which can be a major blow to the franchise.
- Game fixing: If cyber attacks leads to games fixing, it can harm the integrity of the game and damage the reputation of the franchise and the league.

Overall, a cybersecurity attack on a venue can have a significant impact on a franchise's reputation and financial stability. it is important for franchises to implement strong security measures in their venues, regularly monitor and update them, and have incident response plans in place to minimize the damage in case an attack does occur.

Sports Betting

What is Sports Betting and how can that affect Sports Franchises?

Sports betting refers to the activity of placing wagers on the outcome of a sporting event. Sports betting can affect sports franchises in several ways:

- Increase the risk of cyber attack: Gamblers and gambling organizations have a great incentive to obtain confidential information about the medical status of players, game playbooks, and player trades.
- Legal issues; Sports franchises may also face legal issues if they are found to be involved in illegal sports betting activities, and this can also lead to fines and penalties

The legalization of sports betting has the potential to bring new revenue streams to sports franchises, but it also comes with a number of risks and challenges that need to be carefully considered and managed.

What makes a betting cybersecurity attack possible?

Here are the factors that can make a sports betting cybersecurity attack possible:

- Weak security measures: If Sports betting website or app has weak security measures, such as poor encryption or a lack of two-factor authentication.
- Insider access: An employee or vendor with access to the betting system can also be the cause of a cyber attack.
- Malware: Attackers can also use malware such as trojans or keyloggers to steal sensitive information and disrupt the operations of a betting website or app.

Overall, It is important for sports betting website to have rock solid security measures.

What makes a betting cybersecurity attack possible?

A cybersecurity attack in sports betting can ruin a franchise's reputation in several ways:

- Damage to the brand: If a cybersecurity attack results in negative publicity it can damage the reputation and image of the franchise and its brand.
- Financial loss: Attacks can also result in financial loss for the franchise, as they may have to pay for damages, compensation, and legal fees.
- Reduced sponsorship opportunities: If a franchise suffers a cyber attack, it can lead to reduced sponsorship opportunities as companies may be less likely to associate with a franchise that has been associated with a cyber attack.

What are possible ways to mitigate cybersecurity attacks in sports betting?

There are several ways to mitigate cybersecurity attacks in sports betting:

- Penetration testing: Hiring ethical hackers to perform penetration testing can help identify vulnerabilities in the system and fix them before they can be exploited by attackers.
- Compliance: Adhering to industry standards and regulations, such as PCI DSS, can help ensure that the system is secure and minimize the risk of a cyber attack.
- Insurance: Having cyber insurance can provide financial protection in case of a cyber attack and help cover costs such as legal fees, investigations, and data recovery.

It's important for sports betting websites and apps to regularly monitor and update their security measures, have an incident response plan, and educate employees and vendors about cyber threats

Risk Management & Industry Trends

Cybersecurity should be a priority for leadership

Too often, sports franchises share sensitive information such as financial data and personal information of players and fans as a result of weak cybersecurity infrastructure.
When a hacker obtains sensitive information, the result can lead to damage to the organizations public image, loss of revenue, and legal consequences. Cyber attacks can also target operational systems, causing major disruption to the day-to-day activities of the franchise. With the increasing digitalization of the sports industry, sports franchises must prioritize cybersecurity to protect themselves and their stakeholders.

Personnel who should be engaged in cybersecurity dicussions

Ownership is a huge part of sports that nobody sees. They make trades, work with the team and deal with the money. As those are huge roles to have, over recent years sports franchises ownership should also be engaging in cyber risk management discussions as they are ultimately responsible for the overall well-being and success of the franchise. They should have multiple people involved in these discussions including, The CEO or President, The Chief Information Officer (CIO), The Chief Technology Officer (CTO), The Chief Financial Officer (CFO), and the legal department. Additionally, external consultants such as cybersecurity experts, auditors, and insurance brokers should be involved in these discussions to provide impartial advice and recommendations on risk management strategies. These people are the backbone to having a successful cybersecurity infrastructure day in and day out.

Cybersecurity Questions Professional Sports Franchises need to consider

1. Do we have a complete inventory of hardware and software assets?
2. Do we have a comprehensive security plan in place, and is it regularly updated to keep pace with emerging threats?
3. Have we implemented strong passwords and multi-factor authentication for all of our systems and accounts?
4. Are we regularly backing up and securely storing our critical data and information?
5. Do we have a clear and effective incident response plan in case of a cyber attack or data breach?
6. Are all employees, contractors, and vendors aware of our cybersecurity policies and procedures and trained on how to identify and report potential threats?
7. Are we regularly monitoring our systems and networks for unusual activity or potential breaches?
8. Have we conducted a risk assessment to identify potential vulnerabilities and address them in a timely manner?
9. Are we using encryption to protect sensitive information and data both in transit and at rest?
10. Have we considered and planned for the potential financial and reputational impacts of a data breach or cyber attack, and do we have adequate insurance coverage in place?

.

Get in touch

Evans & Chambers
202-768-7330
Jamil@EvansChambers.com
www.EvansChambers.com

10-8 Cyber, LLC
703-776-0846
Gregory.S.Crabb@TenEightCyber.com
www.TenEightCyber.com