BLOG REPORT

From The White House to The World Cup: Deepfakes Expose Sports' Data Vulnerability

TIAKI

From Politics to Play: Deepfakes' Expanding Reach

If the Chief of Staff to the US President can become victim to a deepfake attack, what's protecting you?

Deepfakes, spoofed texts, and AI voice clones are no longer just concepts from Hollywood spy movies; they've become everyday realities.

The Alarming Reality of AI Impersonation:

This week, the FBI launched an investigation into a sophisticated attempt to impersonate White House Chief of Staff Susie Wiles. The perpetrator used AI to clone her voice and spoofed access to her personal contact list, reaching out to governors, senators, and high-powered executives with incredibly convincing voice calls and messages. Even seasoned professionals were nearly tricked into engaging.

This wasn't a typical phishing email with obvious typos. Instead, it was a highly personalized and believable approach that almost deceived members of Congress.

Identifying the Red Flags

So, what gave it away?

- ★ The impersonator lacked basic knowledge that Wiles would possess.
- ★ They requested a cash transfer, a significant red flag in any scenario.
- ★ Their tone was uncharacteristically formal and stiff.
- ★ There were grammatical errors in messages, which would not be present in Wiles's communications.
- ★ The messages did not originate from her authentic phone number.

These behavioral red flags, including deviations in tone, timing, grammar, and the overall feel of a message, are crucial indicators that something was amiss.

The Widespread Threat

Imagine the potential damage if your CEO or another prominent figure in your sports organization were to be impersonated in a deepfake or scam. The technology is readily available, the tools are easy to use, and targeting can be as precise as using someone's personal phone contacts. AI can also create highly authentic interactions in any language. Not only is a ransomware attack in Finnish, Swedish, Italian or Japanese now effortless for the cybercriminal, AI even considers local cultural nuances into the attack plan. Let that sink in. And then ask yourself, “Is my organisation ready to thwart these types of attacks?”

AI has drastically lowered the barrier to entry for these malicious activities, simultaneously escalating the risks. This isn't solely a government issue or just a responsibility for Chief Information Security Officers (CISOs). This is a pervasive problem that affects everyone within an organization. Every organization must operate under the assumption that these tactics will be deployed against them. It's not a matter of "if," but "**when**."

Essential Safeguards

To mitigate these risks, consider these crucial steps:

- ★ **Secure personal and executive mobile devices.**
- ★ **Train staff to cultivate a healthy skepticism** toward anything that feels even slightly off.
- ★ **Always confirm voice requests through separate, secure channels.**
- ★ **Never rely solely on voice identification** to verify someone's identity.

Do you have any systems in place to verify the identity of callers or message senders within your organization?

The Alarming Rise of Synthetic Identities

The recent incident involving Susie Wiles underscores a critical shift in the cyber threat landscape. As Bob Carver, a prominent voice in cybersecurity, frequently highlights, the convergence of deepfake technology and ransomware tactics is creating a perfect storm for high-value targets.[1] Gone are the days when deepfakes were merely amusing curiosities or tools for entertainment. Today, they are sophisticated weapons in the hands of malicious actors, capable of wreaking havoc on reputations, financial stability, and operational integrity.[2]

The ease with which synthetic identities can be created is truly alarming. Unit 42, Palo Alto Networks' cyber threat intelligence and incident response team, demonstrated in their "False Face" report how a single researcher, with no prior experience and readily available tools, could create a real-time deepfake for job interviews in just over an hour.[3] This chilling revelation proves that the barrier to entry for deepfake creation is incredibly low, making this technology accessible to a wider range of threat actors, including those with nefarious intentions.

The 2025 Unit 42 Global Incident Response Report further emphasizes this escalating threat. It details a shifting threat landscape characterized by faster, more complex attacks, with **70% of incidents now spanning three or more attack surfaces**.[4] **The report highlights the rise of disruptive extortion, supply chain vulnerabilities, insider threats, and AI-assisted attacks**. AI, once seen as a tool for progress, is now being weaponized to amplify cyberattacks, from crafting highly personalized phishing emails to automating real-time communication that is nearly indistinguishable from human interaction.[5] This includes AI-driven phishing and **vishing (voice phishing) attacks**, where AI-generated voices perfectly mimic real individuals, making it incredibly difficult to discern authenticity.[6]

Why Sports Is a Prime Target

The sports industry, a multi-billion dollar global phenomenon, presents a uniquely attractive target for deepfake attacks due to several inherent vulnerabilities:

---

[1] Predictions for 2025 from cybersecurity experts - Global Security Mag Online
[2] Combat Deepfakes in Financial Services | Ping Identity
[3] False Face: Unit 42 Demonstrates the Alarming Ease of Synthetic Identity Creation
[4] Trends, threats and expert takeaways. Insights from the “2025 Unit 42 Global Incident Response Report.” - Palo Alto Networks
[5] Most Common AI-Powered Cyberattacks | CrowdStrike
[6] VUMC employees: Beware of 'vhishing' AI-generated voice phishing scams - VUMC News

- ★ **High-Profile Individuals and Brands:** From the Head of FIFA, the Head of the Olympics, and Premier League club owners, to star athletes like LeBron James or Lionel Messi, the sports world is populated by globally recognized figures. A deepfake of a prominent sports leader making a controversial statement, admitting to doping, or endorsing a fraudulent scheme could cause immediate and irreversible reputational damage, trigger financial markets and sports betting markets instability, and erode fan trust. Similarly, a deepfake of a popular athlete promoting a fake product or engaging in scandalous behavior could devastate their personal brand and endorsement deals.
    - The Ponemon Institute's recent survey revealed that **42% of executives and board members have been targeted by fake images or videos, with 66% expecting a future deepfake attack.**[7] This risk is amplified for high-profile sports figures whose every move is scrutinized.

- ★ **Emotional Investment and Fan Engagement:** Sports thrives on emotion and passionate fan engagement. This emotional connection can be expertly exploited by deepfakers to spread misinformation, incite unrest, or manipulate public opinion. Imagine a deepfake video showing a beloved team's owner announcing a shocking relocation, or a renowned coach revealing sensitive team tactics – the fallout could be immediate and widespread, impacting not only the team's image but also their financial stability and fan base loyalty.

- ★ **Fragmented Ecosystem:** The sports industry is a complex web of interconnected entities: governing bodies, leagues, teams, athletes, sponsors, broadcasters, ticketing platforms, merchandise retailers, and a myriad of third-party vendors. This highly fragmented ecosystem creates numerous entry points for attackers. Each entity represents a potential weak link in the overall cybersecurity posture.

- ★ **Immature Cybersecurity Resiliency & Leadership:** While some major sports organizations have invested in cybersecurity, many still lag behind other industries in terms of their overall cyber resiliency and dedicated leadership. Smaller clubs, regional leagues, and individual athlete management groups often lack the resources, expertise, and strategic focus to adequately defend against sophisticated AI-powered threats. This often stems from a perception that cybersecurity is an IT problem rather than a fundamental business risk.

- ★ **Lack of 3rd Party Audits and Oversight:** The interconnected nature of the sports supply chain means that vulnerabilities in one third-party vendor can expose the entire network. Yet, comprehensive and regular third-party security audits are not yet a universal standard. This lack of oversight allows weaknesses to persist, creating ripe opportunities for attackers to leverage deepfakes for social engineering, financial fraud, or data exfiltration.

The Vulnerability of the Sports Ticketing Supply Chain

The sports ticketing supply chain is particularly susceptible to deepfake attacks and associated cyber threats. This multi-layered system, involving primary ticket vendors, secondary marketplaces, payment processors, and event venues, is a rich target for criminals.

- ★ **Financial Incentives:** Billions of dollars exchange hands annually in the ticketing market. Deepfakes can be used for sophisticated fraud schemes, such as impersonating a ticketing platform

[7] New Study from Ponemon Institute Spotlights the Escalating Threat and Financial Impact of Deepfake Attacks on Businesses and Executives

executive to authorize fraudulent transactions or a venue manager to release sensitive fan data.[8] The FBI's warning about "malicious text and voice messaging campaigns" impersonating senior U.S. government officials, often utilizing AI-generated voice messages, directly applies to the financial transactions prevalent in ticketing.

★ **Data Richness:** Ticketing platforms hold vast amounts of personal and financial data on millions of fans. A successful deepfake-driven phishing campaign could lead to mass credential harvesting, enabling account takeovers and further financial fraud.

★ **Fragmentation and Interdependencies:** The ticketing supply chain is a prime example of the fragmented sports ecosystem. A breach in a third-party payment gateway or a small-scale reseller, enabled by a deepfake-powered social engineering attack, could have cascading effects throughout the entire chain, impacting fan trust and event operations.

★ **"Commodity" Attacks and Social Engineering:** As the National Cyber Security Centre (NCSC) in the UK highlighted in their report on cyber threats to sports organizations, most criminal attacks utilize commonly available tools and techniques, often exploiting "normal human traits such as trust." Deepfakes elevate these social engineering attacks to an entirely new level of sophistication, making it much harder for individuals within the ticketing supply chain to detect and thwart fraudulent requests or communications.

Top 10 Strategic Steps for Sports to Reduce Deepfake Risk

To combat this escalating threat, sports properties, regulators, and stars must adopt a proactive and comprehensive cybersecurity strategy. These recommendations are specifically tailored to the unique context of the sports industry:

1. **Elevate Deepfake Threat to the C-Suite & Board Level:** Cybersecurity, particularly deepfake risk, must be a top-down priority. Sports organizations need dedicated Chief Information Security Officers (CISOs) or equivalent roles with direct reporting lines to the CEO and Board.[16] This ensures adequate budget, resources, and strategic oversight for robust security programs.
    - *Data Point: A recent Ponemon Institute study found that only 48% of organizations incorporate the risk of cyber threats against executives in their cybersecurity strategies, despite 42% of executives having been targeted by deepfakes.*

2. **Implement Advanced AI-Powered Deepfake Detection & Verification Tools:** Invest in and deploy cutting-edge AI-powered solutions capable of real-time deepfake detection for video, audio, and images. These tools should be integrated into communication platforms, social media monitoring, and internal verification processes.
    - *Data Point: The market for AI in cybersecurity is projected to grow significantly, with a CAGR of over 20% in the coming years, indicating increasing sophistication in detection capabilities.[9]*

[8] Deepfakes Targeting Benefits with AI-Generated Claims
[9] Artificial Intelligence in Cybersecurity Market Share, Forecast | Growth Analysis & Opportunities [2030]

3. **Mandate Multi-Factor Authentication (MFA) and Biometric Verification (where appropriate):** Beyond basic MFA, explore advanced biometric verification for high-privilege access, sensitive transactions, and critical communications. This adds a crucial layer of defense against deepfake-enabled impersonation.
    - *Sports Context: For instance, for team owner approvals of major transfers or financial transactions, a voice biometric verification on top of traditional MFA could be implemented.*

4. **Conduct Regular, Sports-Specific Deepfake Awareness & Training Programs:** Develop tailored training modules for all staff, from front office to field staff and athletes, on recognizing deepfake threats. Use real-world sports deepfake examples (even hypothetical ones) to make the training relevant and impactful. Focus on identifying subtle cues in voice, video, and text that may indicate manipulation.
    - *Sports Context: Training could involve simulated deepfake calls from a "league official" or "team manager" requesting sensitive information.*

5. **Establish Robust Third-Party Risk Management & Audit Protocols:** Given the fragmented nature of the sports industry, mandate rigorous security audits and contractual obligations for all third-party vendors, especially those handling sensitive data or critical operations (e.g., ticketing platforms, broadcasting partners, athlete management agencies).
    - *Data Point: Unit 42 reports indicate that supply chain vulnerabilities are a growing concern, with attackers increasingly exploiting weaknesses in third-party ecosystems.*[10]

6. **Develop a Rapid Deepfake Incident Response Plan:** Create a clear, actionable plan specifically for deepfake attacks. This includes protocols for immediate verification, public communication strategies (debunking, issuing warnings), legal counsel involvement, and coordinated action with law enforcement and cybersecurity experts.
    - *Sports Context: A rapid response plan is crucial for managing potential reputational damage during a live event or major announcement.*

7. **Implement Strong Data Governance and Access Controls:** Minimize the amount of sensitive data publicly available and strictly control access to critical systems and information. Regularly review and revoke unnecessary access privileges. This reduces the "training data" available for deepfake creation and limits the impact of a successful breach.
    - *Sports Context: Limiting access to athlete medical records, contract details, or proprietary scouting reports is paramount.*

8. **Foster a Culture of Skepticism and Verification:** Encourage a "verify, then trust" mindset across the entire organization. Implement internal verification procedures for all high-stakes communications, especially those involving financial transactions or sensitive information.
    - *Sports Context: For example, an athletic director should always verify a transfer request via a pre-arranged, secure channel before acting on it.*

[10] The Biggest Security Risks in Your Supply Chain in 2025 | UpGuard

9. **Engage with Cybersecurity Intelligence & Threat Sharing Platforms:** Actively participate in industry-specific cybersecurity intelligence sharing groups and collaborate with national and international cybersecurity agencies and digital-data-AI partners. This enables sports organizations to stay ahead of emerging threats and learn from attacks targeting similar entities.
    - *Data Point: Collaborative intelligence sharing is increasingly seen as a critical component of effective cybersecurity, as highlighted in the 2025 Unit 42 Global Incident Response Report.*

10. **Explore and Implement Blockchain and Digital Watermarking Solutions for Media Authenticity:** Investigate emerging technologies like blockchain for verifying the authenticity of official sports media content and digital watermarking to identify and trace manipulated footage. This can help broadcasters and fans distinguish genuine content from deepfakes.
    - *Sports Context: Official league announcements, significant player interviews, or critical game footage could be digitally watermarked to ensure their provenance.*

Conclusion

The embarrassing breaking news about the deepfake attack on Susie Wiles is a loud and clear alarm bell. For the sports industry, often seen as a realm of entertainment and passion, it's a critical moment to recognize the profound and growing threat posed by AI-powered deepfakes.

By embracing proactive cybersecurity measures, investing in advanced technologies, fostering a culture of vigilance, and prioritizing comprehensive risk management, sports organizations can protect their high-profile individuals, safeguard their invaluable data, and preserve the trust of their global fan base in an increasingly deceptive digital world.

The game has changed; it's time for sports to play a stronger defence.

About the Author:

David Andrew
Founder & Managing Partner
www.tiaki.ai
david.andrew@tiaki.ai

David is the Founder & Managing Partner at TIAKI, a niche consulting practice helping executive leadership in sport make confident, informed decisions on their risks, investments and business outcomes powered by secure 'data-at-scale'. He collaborates with bold and determined leaders in the sports ecosystem to define their data, AI and cybersecurity strategies to deliver sustainable value.

David's vision for TIAKI is to empower sports franchise CEOs, leadership teams, sports media broadcasters and investors in the global sports industry with strategic advisory frameworks to deliver secure, pioneering digital fan experiences and new ecosystem business models to achieve breakthrough returns.

David has over 20 years of strategy and technology enabled business transformation experience, providing consulting expertise in cloud native technologies, data strategy, digital business enablement and cybersecurity strategy. He is passionate about helping talented leadership teams succeed in securely growing their differentiated business models in the data-driven, digital sports economy.

Based in Stockholm, David previously worked for IBM Consulting, EY, Accenture Strategy and Orange Business. He studied Chemistry at Durham University and holds an MBA from Trinity College, Dublin Business School.