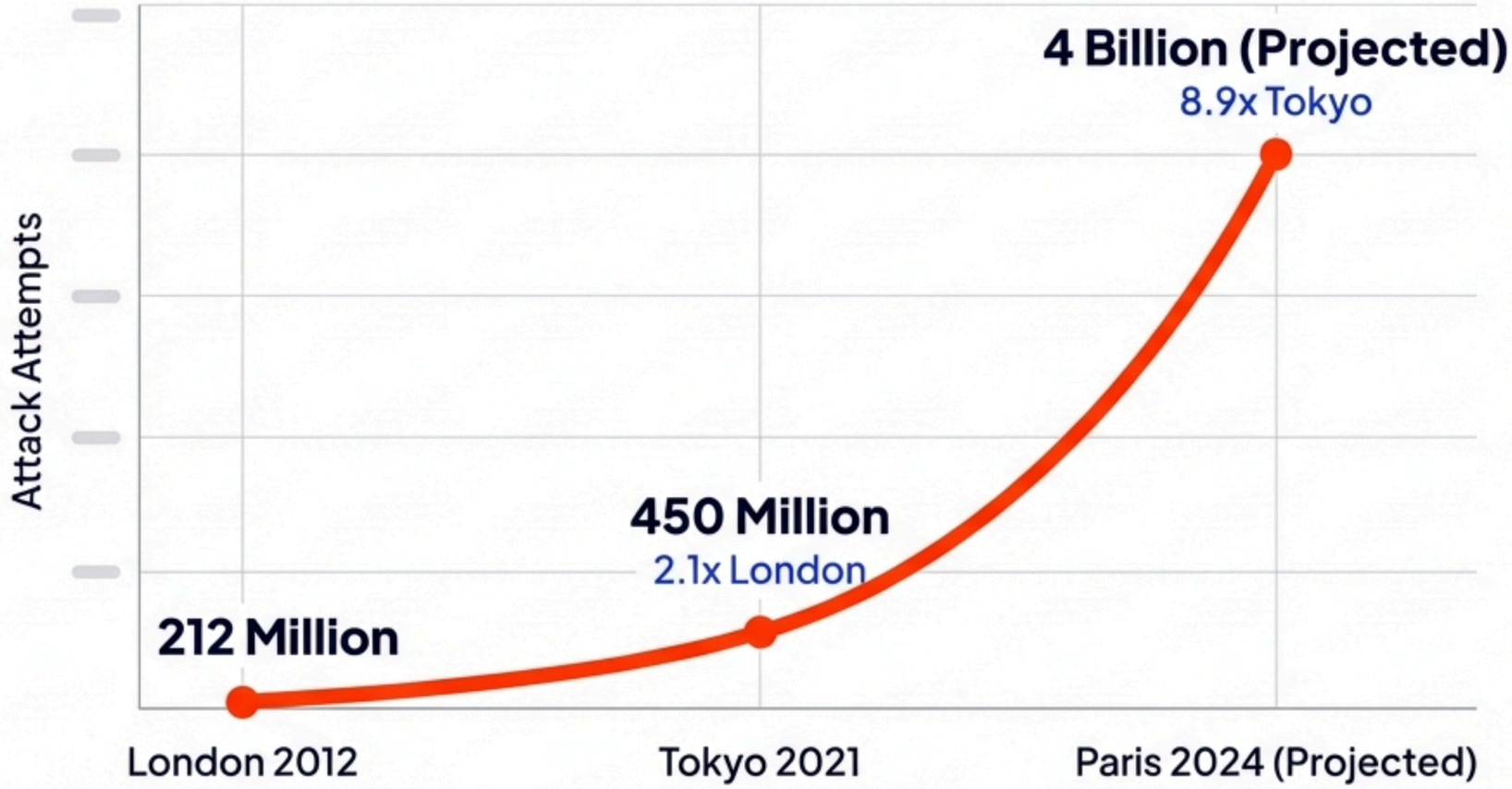

AT&T STADIUM

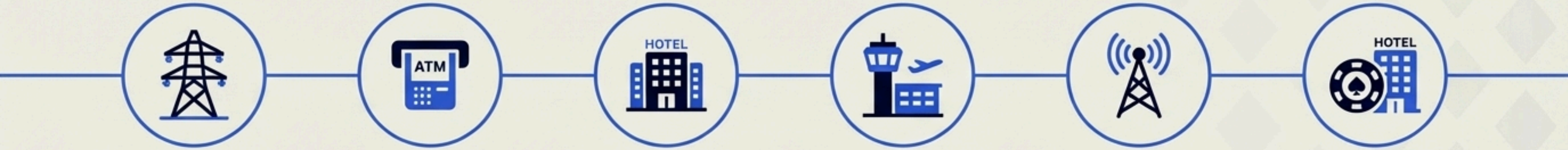
The Threat is Real, Documented, and Exponentially Growing.

Attack Volume Growth During Olympic-Scale Events



Attack volumes against host city infrastructure are growing at an accelerating rate. Dallas should prepare for a threat landscape at least an order of magnitude larger than any previous US-hosted event.

The Attacker's Playbook is Consistent: Target the Host City's Infrastructure.



2012 London Olympics

DDoS attack targets the **power grid** on Opening Ceremony day, requiring Cabinet-level emergency response.

2014 Brazil World Cup

Massive malware campaign targets **ATMs and financial systems**, with 87,776 attempts blocked.

2018 PyeongChang Olympics

Wiper malware attack uses a **hotel network** as a pivot point to disrupt event operations.

2021 Tokyo Olympics

Data breach at the **Ministry of Transportation** and Narita International Airport.

2022 Qatar World Cup

State-sponsored APT gains 12-month persistent access to a major **telecommunications provider**.

2023 Pre-Super Bowl LVIII

Ransomware attack on **MGM Resorts** causes a 10-day outage and ~$100 million in losses.

Every major sporting event in the past decade has experienced documented, significant attacks on the surrounding civil infrastructure.

CASE STUDY: PyeongChang 2018 — The Hotel Was the Weapon

The Target: Ski Resort Hotel in PyeongChang.

The Tactic: Lateral movement. Attackers compromised the hotel Wi-Fi 3 days before the Opening Ceremony to pivot into the Olympic Committee's core IT infrastructure.

The Impact: 300+ systems destroyed by "Olympic Destroyer" wiper malware. Wi-Fi crashed, websites went offline, ticketing and transportation apps failed.

The Lesson for Dallas: Your third-party vendors are a critical part of your attack surface. Attackers will use them as a strategic entry point to reach higher-value targets.

CASE STUDY: Las Vegas 2023 — The $100 Million Phone Call

“A 10-minute phone call gained administrator privileges.”

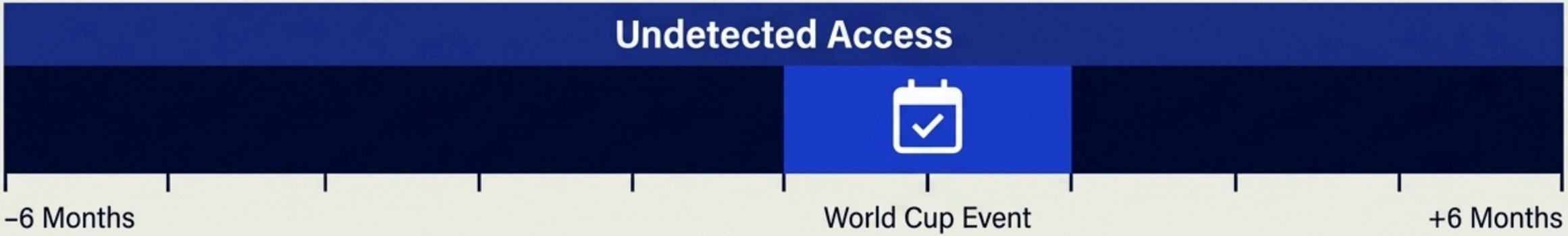
The Target: MGM Resorts (5 months before Super Bowl LVIII)

The Tactic: Vishing (Voice Phishing)
The Scattered Spider ransomware group impersonated an employee on a call to the IT help desk to gain access. No complex technical exploit was required.

The Impact: ~$100M in financial losses
10+ days of operational chaos: hotel reservations, digital room keys, POS systems, and ATMs were all disabled.

The Lesson for Dallas: Technical controls are meaningless if they can be bypassed by social engineering
Your help desk and employee training are front-line defenses.

CASE STUDY: Qatar 2022 — The Undetected Breach



"Remained undetected for 12+ months... throughout the entire World Cup."

The Target: A major telecommunications provider supporting the World Cup.

Supporting the entire World Cup event.

The Tactic: Advanced Persistent Threat (APT)

China-linked group BlackTech APT used a rootkit to gain access 6 months before the tournament and maintained it for over a year.

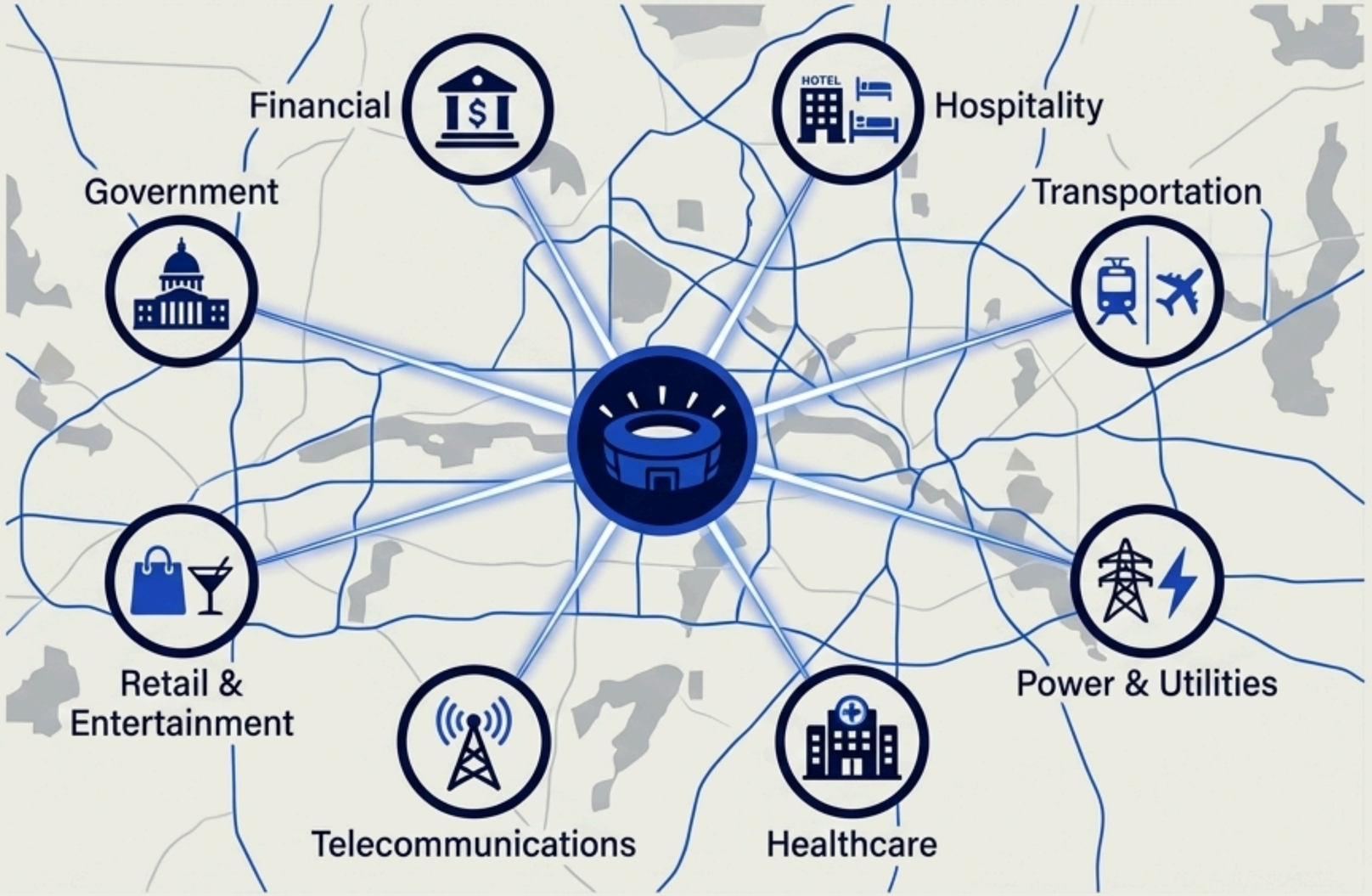
The Impact: Complete, persistent access.

For intelligence gathering throughout the entire event, bypassing Qatar's $1.1 billion cybersecurity investment.

The Lesson for Dallas: Sophisticated adversaries aren't just attacking during the event.

They are establishing access *now*. The battle has already begun.

The Dallas-Fort Worth Attack Surface is Vast and Interconnected



- **9** Matches | **39-Day** Event Window
- **500,000+** Expected Visitors
- **130,000+** Hotel Rooms
- **Major Hubs**:** DFW International Airport, Texas Capital Bank, Baylor Medical Center, AT&T Headquarters

Most Probable Threats Facing Dallas Infrastructure Sectors.

Attacker Profile	Hospitality	Financial	Healthcare	Transportation	Telecom	Power
State-Sponsored (Russia, China, etc.) Highest Capability. Motive: Intelligence, Disruption.	LOW THREAT	LOW THREAT	LOW THREAT	MODERATE THREAT	HIGH THREAT	HIGH THREAT
Ransomware Groups (Scattered Spider, LockBit) Highest Probability. Motive: Financial Gain.	HIGH THREAT	MODERATE THREAT	HIGH THREAT	LOW THREAT	LOW THREAT	LOW THREAT
Organized Crime (Financial Fraud) Motive: Direct Theft.	MODERATE THREAT	HIGH THREAT	LOW THREAT	LOW THREAT	LOW THREAT	LOW THREAT
Hacktivists (Anonymous, etc.) Motive: Political Messaging.	LOW THREAT	LOW THREAT	LOW THREAT	MODERATE THREAT	LOW THREAT	MODERATE THREAT

Dallas 2026: Projecting the Scale of the Cyber Event

Projected Attack Attempts

8-10 Billion

Total malicious security events projected during the 39-day World Cup period, based on the growth trajectory from London to Paris.

Peak Daily Attack Rate

200-250 Million

Projected number of attacks per day during high-profile matches.

Most Likely Scenarios

1. **Hotel-to-Event Infrastructure Pivot** (PyeongChang Precedent)

2. **Ransomware** targeting **DART** or **Hospitals** (MGM Precedent)

3. **Power Grid DDoS** during a high-profile match (London Precedent)

4. **Telecom provider breach** for long-term intelligence (Qatar Precedent)

The question is not *if* attacks will happen. They are inevitable. The question is how you prepare.

VULNERABILITY

RESILIENCE

Based on years of major event analysis, a clear framework for defense has emerged. It requires a strategic shift from a reactive security posture to a proactive, event-driven resilience plan. The next five months are the critical window to build this resilience.

The Framework for a Resilient Dallas 2026

IMMEDIATE ACTIONS (Now - March 2026)

- Conduct a World Cup-specific Risk Assessment.
- Run a Tabletop Exercise using historical precedents (MGM, PyeongChang).
- Assess Third-Party & Vendor Risk.
- Strengthen Access Controls (MFA, Privileged Access).

SHORT-TERM ACTIONS (March - May 2026)

- Establish Coordination with law enforcement (FBI, CISA) and industry ISACs.
- Update and Test Incident Response & Business Continuity Plans.
- Conduct targeted Security Awareness Training (World Cup-themed phishing).
- Accelerate Vulnerability Management and patching.

DURING EVENT (June 11 - July 19, 2026)

- Activate 24/7 Enhanced Monitoring (SOC Operations).
- Implement a Change Freeze on critical systems.
- Maintain Daily Communication and intelligence sharing.
- Ensure Backup & Resilience systems are on hot standby.

Focus Area: Your Security is Only as Strong as Your Weakest Vendor

The PyeongChang 2018 attack proved that hospitality and event support vendors are not just targets, but strategic vectors.

Inventory & Assess
Map all vendors with network access or those handling critical data. Use a vendor security questionnaire to assess their posture.

Segment
Isolate vendor networks from your core business operations. Guest Wi-Fi must be completely air-gapped from property management systems.

Contract
Mandate specific security controls and incident notification SLAs in your vendor contracts for the World Cup period.

Monitor
Actively monitor all vendor connections for unusual activity.

Intrusion

A Local Partner for a Global Event.

Take the Next Step Toward a Secure World Cup 2026.

Our expert team can provide a confidential, no-obligation readiness assessment tailored to your organization and industry. This assessment will:

- Identify your specific risks based on the World Cup threat landscape.
- Benchmark your current security posture against event best practices.
- Provide a prioritized roadmap of actionable recommendations.

Request Your Confidential Readiness Assessment