Hector Monsegur

Hector Monsegur is a cybersecurity professional and former member of Anonymous and LulzSec who speaks to organisations about cyber risk, hacking culture, and the realities of digital security.

- Former member of Anonymous and hacking group LulzSec.
- Pleaded guilty to multiple U.S. federal cybercrime offenses under a cooperation agreement.
- Cooperation with authorities enabled the identification and arrest of co-conspirators and the prevention or mitigation of further cyberattacks.
- Sentenced to time served and supervised release in Manhattan federal court.
- Has worked in legitimate cybersecurity roles, including penetration testing and cyber risk and research positions.
- Co-host of the “Hacker and the Fed” podcast with former FBI special agent Chris Tarbell.

Hector Monsegur's 2026 Biography

Key speaking topics

- Cybersecurity risk and threat landscape
- Hacker tactics and attack methodologies
- Organised hacktivism and cybercrime networks
- Insider perspectives on Anonymous and LulzSec
- Law enforcement cooperation in cyber investigations
- Corporate vulnerability and digital resilience
- Ethical pathways in cybersecurity careers

Ideal for

- Chief Information Security Officers and security teams
- Boards and senior leadership teams overseeing cyber risk
- Risk, compliance, and governance professionals
- Technology and cybersecurity conferences

Audience outcomes

- Clear understanding of how high-profile cyberattacks are planned and executed
- Insight into vulnerabilities commonly exploited by attackers
- Greater awareness of organisational cyber risk exposure
- Perspective on the legal and operational consequences of cybercrime
- Informed discussion around prevention, detection, and response

AVAILABLE FOR

- Speaking

HECTOR'S SPEAKING THEMES

- Cybersecurity
- Future of Technology
- Political Risk & Policy
- Risk Management
- Supply Chain Resilience

Why organisations work with Hector Monsegur

- First-hand experience of organised cybercrime and federal investigation processes
- Direct insight into attacker mindset and operational methods
- Practical relevance for organisations managing cyber risk
- Ability to translate complex security issues into accessible business language

Biography

Hector Monsegur brings direct, first-hand insight into cyber risk, hacking culture, and digital vulnerability. As a former participant in high-profile cyberattacks linked to Anonymous and LulzSec, he understands how coordinated attacks are planned, executed, and exploited at scale.

U.S. federal authorities charged Monsegur with multiple hacking and fraud-related conspiracies and aggravated identity theft. He entered a guilty plea under a cooperation agreement, assisting investigators in identifying co-conspirators and preventing or mitigating further cyberattacks targeting corporate and government systems.

Following his sentencing in Manhattan federal court, Monsegur transitioned into legitimate cybersecurity work. He has held roles in penetration testing and cyber risk and research, applying his technical expertise to help organisations understand weaknesses before adversaries do.

Monsegur also co-hosts the “Hacker and the Fed” podcast with former FBI special agent Chris Tarbell, exploring cybercrime investigations and the evolving threat landscape. His experience spans both sides of cyber operations, offering senior leaders and security professionals an unfiltered perspective on attacker mindset, law enforcement response, and organisational exposure.

Raised in New York City’s Lower East Side public housing and largely self-taught in computing, Monsegur’s journey underscores the accessibility of cyber capability and the realities of digital risk. For organisations navigating complex cybersecurity challenges, his background provides practical insight into how threats emerge, escalate, and can be addressed.

Hector Monsegur's 2026 talks & topics

From High School Dropout to Hacker to FBI Informant

An autobiographical lecture tracing Hector’s journey from leaving high school to becoming a hacker, an FBI informant, and ultimately transitioning into legitimate cybersecurity work.

Key takeaways:

- Insight into the realities behind federal indictments and what the process involves
- First-hand perspective on Anonymous, high-profile hacks, and global cyber campaigns

- A candid exploration of informant culture, accountability, and life after hacking

---

The Hackers Manifesto: The A–Z on Hacking

A comprehensive exploration of hacking culture, motivations, tools, and operations, drawing on historical context and real-world examples.

Key takeaways:

- Understanding what makes hacking appealing and how targets are chosen
- Overview of hacktivism, state-sponsored hacking, and high-profile cases including Sony, Visa, MasterCard, and government systems
- Practical insight into how hacking tools, hardware, and software are used in real attacks

---

The State of Security

An examination of current cybersecurity challenges, including supply chain vulnerabilities, backup recovery issues, and lessons from major incidents.

Key takeaways:

- Why supply chain attacks such as SolarWinds remain relevant
- The risks and limitations of backup and recovery strategies
- Practical measures for maintaining a safer online environment

---

Storage and Recovery: Risks, Reward and Redundancy

A focused discussion on storage and recovery strategies, the challenges they present, and the shortcomings of widely adopted solutions.

Key takeaways:

- Key risks associated with storage and recovery systems
- Common deficiencies in current recovery solutions
- Considerations for strengthening resilience and redundancy

Cybersecurity: A Human Problem, Not a Systems Problem

A talk centred on the human element in cybersecurity, using real-world stories to examine how error, disinformation, and social engineering expose organisations to risk.

Key takeaways:

- How human error creates vulnerabilities within organisations
- The impact of social engineering and disinformation
- Practical approaches to reducing people-related security risks

Security Best Practices

An overview of general security topics, current software and trends in cyberspace, and perspectives from both offensive and defensive security roles.

Key takeaways:

- Awareness of popular software and emerging cybersecurity trends
- Insight from black hat and red team experience
- Directional view of where security and hacking are heading

Hector Monsegur's Videos

What Hector Monsegur's clients say

Hector was great! Our attendees really had positive feedback about his talk and wanted him to stay on stage longer!! He was very professional and easy to work with!

ISACA