
We the People
Of the United States,
in Order to form a more perfect Union,
establish Justice, insure domestic Tranquility,
provide for the common defence,
promote the general Welfare, and secure
the Blessings of Liberty to ourselves and
our Posterity, do ordain and establish this
Constitution for the United States of America.
SIGNATURE OF BEARER / SIGNATURE DU TITULAIRE / FIRMA DEL TITULAR
PASSPORT
PASSEPORT
PASAPORTE
USA
UNITED STATES OF AMERICA
P
USA
547017342
SU
JIMMY ZHIGANG
UNITED STATES OF AMERICA
02 Jan 1979
CHINA
M
31 May 2016
United States
Department of State
30 May 2026
SEE PAGE 27
USA
P<USASU<<JIMMY<ZHIGANG<<<<<<<<<<<<<<<<<<<<<<
5470173429USA7901025M2605306571997038<474536

JIMMY ZHIGANG SU

(672) 533-2028 Jimmy.Su@binance.com

Dr. Su is an experienced and passionate global Cyber Security executive with a demonstrated track record of aligning security with business objectives and delivering world-class level cybersecurity capabilities across products and enterprise. He has delivered exceptional results from both the security of business and business of security settings. He has an excellent track record in building and leading highly motivated and productive teams in both start-up and large-scale organizations. Binance is the largest cryptocurrency exchange in the world by both trading volume and active accounts. It has more than 277 million registered users in over 180 countries. Dr. Su is the Chief Security Officer at Binance. In his role, he is responsible for developing the technology, processes, and team that safely store the world's largest holdings of cryptocurrency.

JD.COM (NASDAQ: JD) is China's largest ecommerce company by revenue and a member of the Fortune Global 500. At JD.COM, Jimmy led a global team based in Mountain View and Beijing that focused on account security, data security, Red Team, IoT security, Cloud security, AI security, Big Data analytics, blockchain-based security applications, enterprise security, incident response, and security deception. His team was responsible for the risk control and data security of over 300 million active JD customers. Successful accomplishments include building security teams, driving secure product development, managing technology risk, and achieving regulatory compliance.

Jimmy has successfully led development of numerous information security products from concept through production. His work at FireEye focused on the development of large-scale Windows, mobile, and Javascript exploit kit malware classification and clustering both in the Cloud and on the appliance. He led a team including data scientists, developers, and QAs from the initial prototype development to the deployment in all FireEye core products including NX, EX, FX, AX, and mobile in two years. He led the effort to add real-time malware detection capabilities to the end-point product. The mobile product won the CRN Enterprise App Award for Security. He also worked on credentials phishing detection, which had been deployed in production on ETP (Cloud) and EX (appliance). Out of FireEye's $797 million annual billings in 2016, $542 million (68%) of them in products and subscription services rely on key detection engines built by his team. These detection engines account for more than 85% of malware detections in FireEye products.

Work Experience:

March 2020-current | Binance, Vancouver, BC | Chief Security Officer at Binance

- Jimmy's team is responsible for both information security and IT at Binance. The team is focused on identifying and mitigating cyber and physical risks facing Binance's global operations. Areas include security of the trading platform, corporate infrastructure, risk control, SDL (Security Development Lifecycle), Red Team, security governance, as well as diverse product offerings including Binance Pay, Web3 wallet, and others.

January 2017-March 2020 | JD.COM, Mountain View, CA and Beijing, China | Senior Director of Information Security at JD.COM

- Jimmy's team is responsible for ensuring the security of JD's corporate infrastructure, as well as diverse product offerings including JD Mall, JD Cloud, JD Finance, smart speakers, smart refrigerator, fully automated warehouse, and others. His team also leads security policy definition, red-team exercises, vendor security reviews, security product evaluations, security risk evaluation and compliance.
- Lead all advanced research at JD security including account security, data security, IoT security, Cloud security, AI security, Big Data analytics, blockchain-based security applications, enterprise security, incident response, and security deception.
- Lead end-to-end process from concept to production on multiple deliveries including real-time bot detection, account anomaly detection, credential stuffing detection, coupon fraud detection, dynamic analysis using sandbox, and transparent data encryption.
- Built the Red Team from ground up with world class white hat hackers, including multiple members of the 2018 and 2019 DEFCon World Finals CTF team, Microsoft bounty program Hall of Fame member, Apple bounty program Hall of Fame member, Google bounty program Hall of Fame member, and China's youngest White Hat hacker.

Lead the Red Team in finding over one hundred critical vulnerabilities in both JD's internal and external facing systems. Work closely with different business units to fix these vulnerabilities in a timely manner to prevent losses.

- JD's first three Blackhat briefings on the world stage of hacker conference on kernel exploit generation
- JD's first three papers ever accepted to DEFCon 2018 on AI security
- JD's first best paper award in CCS, one of the top four security conferences
- Ten patents in both China and US in the areas of data security, container security, and risk control

December 2012-January 2017 | FireEye Inc, Milpitas, CA (joined through acquisition of Ensighta by FireEye) | Promotion path: Staff Engineer -> Senior Staff Engineer -> Manager of the Advanced Threat Research Group -> Director of Data Science

- Director for real-time malware detection using machine learning on the end-point HX product.
- Director for improving malware detection efficacy using novel classification and clustering techniques across all FireEye's core products including NX, EX, AX, FX, and mobile. **Winner of FireEye's Above and Beyond award for Q4 2015 after the release of this detection engine in NX.**
- Director for credentials phishing detection on EX and ETP.
- Director for FireEye's multi-million Android and iOS mobile security product. Coordinated with Marketing, Product Management, and TechOps to handle multiple successful releases. Managed both developers and QAs from prototype development to current product.
- Lead developer on the similarity analysis of Android apps in the mobile security product line. Developed patent pending techniques for malware classification and clustering. Product has analyzed over three million Android apps in the Cloud.
- Lead developer on the Android app crawler for both Google Play and third-party markets. Crawler has retrieved and indexed over two million Android apps.
- Published 15 FireEye threat research blogs on mobile security to establish thought leadership in this space.
- Patent granted on malware classification using similarity analysis

January 2011-December 2012 | Ensighta Inc, Berkeley, CA | Senior Scientist

- PI and principal developer on project for scalable security audits of program binaries in the Cloud through a Web service named BitTurner.
- PI and principal developer on project for similarity analysis of Android applications using feature hashing on Dalvik bytecode.
- PI and principal developer on project for security audit and code hardening of third-party program binaries. Led the team at Ensighta from proposal writing to implementation.

August 2002-December 2010 | University of California, Berkeley, CA | Research Assistant

- Worked with Professor Yelick on Titanium. Titanium is a Java based parallel programming language. Project involves compiler optimizations for explicitly parallel programs.
- Worked on communication optimizations for irregular structured problems and performance counter libraries.
- Developed static analysis on enforcing sequential consistency of Titanium programs
- Developed performance debugging tool for Titanium programs by looking at performance statistics of runs with small number of processors to predict performance bottlenecks in large processor configurations.

Education

PhD Computer Science**,** University of California, Berkeley. **Thesis**: *Raising the Level of Abstraction in Parallel Computing*

M.S. Computer Science**,** University of California, Berkeley. **Thesis**: *Automatic Support for Irregular Computations in a High-Level Language* (Perfect GRE score 2400)

B.S. EECS**,** University of California, Berkeley. (Highest Honors, GPA 4.0)

Job Description: Chief Information Security Officer

Overview

The Chief Information Security Officer (**CISO**) is a senior management and Controlled Function within an ADGM FSRA-regulated firm The CISO is responsible for establishing and maintaining a robust information and cyber security framework. The CISO ensures that the firm's systems, data, and digital infrastructure are protected against internal and external threats, in line with regulatory requirements and best practices.

Key Responsibilities

1. **Information and Cyber Security Governance**

    - Develop and implement the firm's information security strategy, policies, and procedures, ensuring alignment with FSRA requirements and international best practices (e.g., ISO 27001).
    - Establish and maintain a risk-based information security framework that supports the confidentiality, integrity, and availability of the firm's systems and data.
    - Regularly assess the firm's technology and cyber risks, report findings to senior management, and provide recommendations for mitigation.

2. **Threat Detection and Incident Response**

    - Monitor the firm's technology environment for cyber threats, vulnerabilities, and breaches, and ensure timely incident response and recovery procedures are in place.
    - Maintain and regularly test a documented incident response plan and business continuity plan, including procedures for regulatory notification of material security incidents.
    - Lead investigations and root cause analyses of cyber incidents and recommend corrective actions.

3. **System and Data Protection Controls**

    - Ensure that robust access controls, encryption standards, and network protections are implemented and maintained across the firm's infrastructure.
    - Oversee third-party vendor risk assessments, particularly for outsourced IT services, cloud computing, and data storage providers, in accordance with FSRA outsourcing rules.

- Ensure compliance with data retention, data residency, and privacy obligations relevant to client and business data.

4. **Training, Awareness, and Culture**

   - Develop and deliver ongoing security awareness training to employees, management, and consultants to foster a strong information security culture.
   - Promote adherence to internal cyber hygiene standards and ensure that all staff understand their responsibilities in maintaining information security.

5. **Regulatory Engagement and Oversight**

   - Liaise with the FSRA on matters related to cybersecurity and technology risk management, and ensure that all regulatory obligations and expectations are met.
   - As a Controlled Function, the CISO must meet fit and proper requirements.
   - The CISO holds personal accountability for the adequacy and effectiveness of the firm's information security framework and may be subject to regulatory scrutiny or action in the event of systemic failure or negligence.