CASE STUDY

"At COE Security, we build, operate, and transfer world-class security solutions, empowering businesses with resilience and trust."

Joseph Henderson

COE SECURITY LLC

USA | BRAZIL | UAE | INDIA

CASE STUDY

ENHANCING ENTERPRISE SECURITY THROUGH SOCIAL ENGINEERING TESTING

COE SECURITY

Measurable Impact Our Security in Numbers

- 1,500+ Global Engagements
- 95% Client Satisfaction
- 10+ Years of Cybersecurity Excellence
- 15K+ Critical Vulnerabilities Identified
- 1M+ Security Incidents Managed
- $350M+ Costs Saved
- $2.5B+ Transactions Secured
- 24/7/365 Threat Monitoring & Response
- Proactive Threat Hunting
- Cutting-Edge Security Technologies
- Dedicated Security Advisors
- Zero-Day Exploit Mitigation
- Incident Response Planning & Execution
- Security Awareness Training
- Customizable Security Solutions

Client Profile

A gobal technology company handling sensitive intellectual property, customer data, and financial records wanted to evaluate its employees' awareness and susceptibility to social engineering attacks. With the rise in phishing, vishing, impersonation, and pretexting attacks, the company sought to test its workforce against real-world social engineering threats and improve its security culture.

Challenges Faced

Before undergoing Social Engineering Testing, the company identified several concerns:

- Increased phishing attempts targeting employees and executives.
- Weak employee awareness, leading to clicking on malicious links and sharing credentials.
- High-risk executives (C-suite & finance teams) targeted by business email compromise (BEC) scams.
- Insufficient security training, leaving employees vulnerable to pretexting and vishing attacks.
- Lack of reporting culture, where employees failed to report suspicious interactions.
- Weak verification processes, allowing attackers to manipulate employees into granting unauthorized access.

Our Approach

To thoroughly assess the company's security defenses, we conducted a multi-layered Red Team assessment, simulating real-world adversarial tactics to test cyber resilience.

We're Hiring!

COE SECURITY

Compliance & Regulatory Mastery

- ISO 45001
- HIPAA & HITRUST
- NIST & NIST 800-171
- ISO 27001
- PCI DSS
- CMMC
- CIS Controls
- SOC 2
- CCPA & NYDFS
- EU CRA
- FedRAMP
- GDPR
- UK Cyber Essentials
- Essential Eight - Australia

We're Hiring!

Scoping & Threat Modeling

- Target groups – Identifying employees, executives, IT teams, and customer service representatives.
- Attack scenarios based on real-world tactics, including phishing, vishing, pretexting, baiting, and physical impersonation.
- Rules of engagement, ensuring a realistic but controlled testing environment.
- Compliance considerations, aligning with ISO 27001, GDPR, PCI DSS, and internal security policies.

Security Testing Execution

• Phishing Campaigns – Testing employee responses to targeted emails.
• Vishing Attacks – Conducting phone-based manipulations to extract sensitive data.
• Pretexting Attacks – Impersonating others to gain unauthorized access.
• Business Email Compromise (BEC) – Testing susceptibility to CEO fraud or fake wire transfers.
• Baiting Attacks – Using malicious USB drives to track employee curiosity.
• Tailgating & Physical Impersonation – Attempting unauthorized physical access.
• Smishing Attacks – Sending fraudulent SMS messages.
• Social Media Exploitation – Evaluating the exposure of sensitive data through online sharing.

Findings & Risk Assessment

- Attack success rates, showing how many employees fell for social engineering attempts.
- High-risk individuals, identifying employees who were most susceptible to manipulation.
- Behavioral patterns, analyzing why employees engaged with malicious content.

COE SECURITY

Our Cybersecurity Arsenal: Beyond Protection- We Build Resilience

- Application Penetration Testing (Thick/Thin)
- Mobile Application Penetration Testing
- API Penetration Testing
- Network Penetration Testing
- Operational Technology Security Testing
- Cloud Penetration Testing
- AI & LLM Security Audit and Pen Testing
- Red Teaming & Social Engineering Services
- Product & Hardware Penetration Testing
- IoT Security
- Security Operations Center Services (24/7)
- Custom Security Services

We're Hiring!

- Security awareness gaps, highlighting weaknesses in training and reporting procedures.
- A prioritized remediation roadmap, providing practical steps to strengthen security awareness.

Remediation Support & Secure Hardware Development Best Practices

- Targeted employee awareness training, using real examples from the engagement.
- Phishing simulation exercises, ensuring employees could recognize future threats.
- Incident reporting improvements, encouraging employees to report suspicious interactions.
- Multi-factor authentication (MFA) enforcement, reducing the risk of credential-based attacks.
- Verification protocol enhancements, strengthening identity verification processes.
- Executive security training, helping C-suite members recognize BEC and deepfake scams.

Results

- Reduced phishing susceptibility by 60% through targeted training.
- Increased security reporting by 75%, creating a more proactive security culture.
- Implemented stronger verification procedures, reducing pretexting and impersonation risks.
- Enhanced MFA adoption, securing high-risk accounts from unauthorized access.

COE SECURITY

Industries We Protect with Cutting-Edge Security



- Financial Services
- Healthcare
- Retail
- E-commerce
- Government
- Cryptocurrency
- Blockchain Technology
- Automotive
- Transportation/Logistics
- Energy & Utilities
- Hospitality/Tourism
- Entertainment/Media
- Manufacturing
- Education
- Telecommunications
- HiTech & Information Technology

We're Hiring!

Conclusion

By leveraging our Social Engineering Testing services, we helped the company identify human security vulnerabilities, improve employee awareness, and build a strong security culture. Our real-world attack simulations provided valuable insights, ensuring employees were better prepared against sophisticated social engineering threats.

COE Security LLC

COE Security is a leading cybersecurity services provider, offering comprehensive solutions to address the evolving threat landscape. We have a proven track record of helping organizations of all sizes mitigate risks, strengthen defenses, and recover from cyberattacks. Our team of experienced cybersecurity professionals possesses deep expertise in the latest technologies and best practices, enabling us to deliver tailored solutions that meet your unique security needs.

"Peace of mind in a world of cyber threats. That's what we deliver."

Joseph Henderson

COE SECURITY