John Sileo

Cyber Security Expert & Hall of Fame Keynote Speaker

The Hacker's Blacklist: Critical Cybersecurity Threats & Solutions. To avoid becoming the next disastrous data-breach headline, you must foster a **healthy culture of security** that addresses both the technological ***and*** human elements of data defense. Change happens when you create **energy and buy-in** among the people who handle your mission-critical information. When it comes to the latest data security threats, you can't possibly do everything—but you must do the right things. This **cyber security training crash course** forges a high-level, non-technical path through the often confusing web of human decision making, cyber defense, mobile technology, IoT, social media and cloud computing—critical components of your success. This **highly-interactive presentation** builds on John's **experience losing everything** to cybercrime, continues with a **live hacking demo** of an audience member's smartphone and ends with an actionable **Roadmap of Next Steps**.

C-Level Cybersecurity: Building a Bulletproof Culture of Security. Security **awareness starts at the top**. Cybercriminals lust for your corporate data. Competitors bribe your disgruntled employee for a thumb drive full of confidential files. Social engineers exploit your executives' social media profiles – a veritable "how to" guide for network security access. Hackers "sniff" unprotected IP addresses and cloud traffic you didn't even know existed. Cyber extortionists encrypt your mission-critical data and demand a ransom. In the meantime, **you end up the next disastrous headline** – reputation damaged, customers fleeing. Cybercrime and corporate data breach are a huge financial cost and legal liability to organizations. **This does not have to be your fate.** As a leader, you must learn to cope with a wide range of cyber threats with little to no technical background, limited resources and almost no lead time. The answer lies in your **preparation and strength of culture**. This presentation aims at leaders looking to imbue their culture with **security strategies from the boardroom to the break room**. John leverages his work with clients like the Pentagon and Schwab to help you develop a prioritized punch list of critical action items.

Think Like a Spy: Personal Identity Theft Protection. Identity theft training is **no longer optional**. Every move you make in the digital world can be tracked, hacked, recorded and exploited. Threat sources like **smartphones, the Internet of Things (IoT), wearable technology, cloud computing and social media** have shifted the competitive landscape in favor of cyber-savvy users with strong identity theft training. Due to the power of personally identifying information (PII) and the rapid rate at which information is being compromised, we must leverage **the very latest prevention tools** to protect everything from our Social Security numbers to bank accounts, from passwords to confidential emails. John delivers these identity theft countermeasures in a highly interactive, disarmingly humorous presentation inspired by his personal loss of more than $300,000, his business and two years of his life to data theft. In ***Think Like a Spy***, John focuses specifically on identity theft prevention tools that apply to every individual in your audience.

The Art of Human Hacking: Social Engineering Self Defense. Anti-fraud and social engineering training only work when your people experience it in person. Human beings can be the weakest link or the strongest competitive advantage in the security and profitability of your information assets. But people are the most commonly underutilized, least expensive weapon in your fight against cybercrime. Social Engineering Training too often fails because of Death by PowerPoint. Fraud training needs to be engaging and interactive to be effective. To put it simply, this session makes security fun, so that it sticks. In this continually-interactive session, John goes deep into social engineering tools and tricks used to separate you from your critical data. By building System-1, Reflex-Based Awareness around how tools like social media, trust shortcuts, ego stroking, greed appeals, and cortisol flushing enable social engineers, John will dramatically reduce the human element of your threat footprint. By the time John finishes his entertaining closing story, your audience will be fully empowered to detect and deter social engineering, fraud and deception.