Key Takeaways from Anatomy of a Data Breach Webinar

Insights from Featured Speakers:

Will McKeen
Special Agent, FBI Cyber Crimes Task Force

James Mignacca
Chief Executive Officer, Cavelo

Ben Tercha
Chief Operating Officer, Omega Systems

Anatomy of a Data Breach

Speakers from Omega and Cavelo – joined by a special guest from the FBI's Cyber Division – break down the current cybersecurity threat landscape and review considerations and recommendations for businesses to follow before, during and after a data breach.

***Responses have been edited and streamlined to allow for easier reading.*

Omega Systems
omegasystemscorp.com

Cavelo
cavelo.com

What's Included?

The Threat Landscape

Q: The FBI has developed a robust network of task forces and operations centers focused on combatting cyber crimes. Can you tell us about what you're seeing in the public sector of late in terms of threat actors and adversaries?

A: The cyber threats we encounter include traditional actors engaged in financially motivated fraud, such as business email compromises and cyber-enabled frauds, as well as more advanced malware actors. Ransomware remains a significant and increasing concern for the FBI. Moreover, we also handle cases involving malicious insiders and romance scam actors.

- Will McKeen, FBI

Q : Can you explain risks and vulnerabilities that we are discovering more frequently in the private sector?

A : We're witnessing cyber threats like business email compromise, account impersonation, reward resource hijacking and vulnerability exploitation. Business email compromise is occurring weekly, emphasizing the importance of strong defenses. Recently, a manufacturer vulnerability was leaked before its official release, leading to a rush to patch systems before cybercriminals exploit them in customer environments. Securing the systems before malicious actors target them has become a race.

- Ben Tercha, Omega Systems

Q : What does it mean to have a “limitless attack surface” and how that’s opened up businesses to more risk factors?

A : Over the past 5 to 10 years, the shift to cloud adoption has significantly changed the cybersecurity landscape. Previously, data was stored in one location, protected by firewalls, but now, with multiple cloud providers, data is distributed, creating a more extensive attack surface.

The increase in remote work due to COVID-19 has further complicated the situation. Traditional security measures like monitoring north-to-south traffic are no longer sufficient, as everything is distributed. The attack surface has expanded with the use of mobile devices and multiple endpoints. Data is the critical asset to protect, and it is now scattered across various devices and cloud services, making it challenging to track and secure.

To address this complex attack surface, a multidimensional approach is required, focusing on identifying the riskiest areas and remediation to reduce the risk of data breaches.

- James Mignacca, Cavelo

Pre-Breach: Vulnerabilities & Risk Factors

Technical & Human Risk Factors

Q: What are some of the technical layers and components of a security program that are designed to prevent data compromise?

A: Firewalls with UTM features are effective for safeguarding office environments, but with the shift to remote work, endpoint protection has become crucial. Implementing EDR with 24/7 SOC monitoring helps contain threats. Additionally, MFA and trusted device models are vital for cloud services to restrict access based on health criteria and ownership. Zero-trust policy is also gaining popularity, necessitating customized implementations. Routine security awareness training and phishing simulations are also critical.

- Ben Tercha

Q: What's the FBI's perspective on user awareness training and how businesses should be educating their users on current threats?

A: Many companies neglect security awareness training as a selling point, but for the FBI, cybersecurity is central to our culture. We prioritize data protection and trust - even if it means delaying payment verification for security. We gladly conduct tabletop exercises and breach awareness programs with private firms. We aim to have cyber-trained agents accessible within an hour's drive of every American for rapid incident response.

Ongoing cybersecurity education is vital, and we regularly run phishing campaigns to enhance employee awareness. Collaborating with law enforcement and outside counsel fortifies our defenses. We consider cybersecurity not just a job requirement, but a compelling factor for potential clients.

- Will McKeen

Pre-Breach: Vulnerabilities & Risk Factors

Understanding the Financial Impact

Q: How can technical gaps be measured in a way that lets companies actually calculate the financial cost of a potential breach?

A: Quantifying potential breaches and liabilities is important for Board-level comprehension, as decision-makers think in financial terms. It's impossible to have zero risk, so it's crucial to educate people about the inherent risks of doing business online. Risk management involves determining acceptable and unacceptable risk levels, which may change over time. Regular reviews, often quarterly, help monitor and address risks. Many companies are now utilizing cybersecurity insurance to further mitigate their risks. By explaining cybersecurity in financial terms that the Board understands, organizations can get more funding and work on preventing data breaches.

- James Mignacca

Q: Once a cyber incident happens, what does the FBI do to attempt to recover these funds? Is the FBI solely focused on catching the “bad guy?”

A: When a breach occurs, we prioritize protecting the victim from further harm. Our Rapid Response and Asset Recovery Teams work to help victims reclaim their funds. Within 72 hours, we achieve over 75% success in fund recovery, especially within the US. While we prefer using banking channels for swift recovery, seizure warrants might be necessary, leading to longer processes. In cases like a $47 million business email compromise, we successfully recovered most funds through traditional banking, but some were converted into cryptocurrency. Dealing with cryptocurrency is more challenging, and we rely on legal processes to retrieve those funds. Our ultimate goal is to identify and catch the perpetrators behind the cybercrime.

- Will McKeen

Incident Response: The Immediate Aftermath

Technical Response

Q: Where do companies fall short when it comes to breach response?

A: During a cyberattack, stopping the threat actors and containing the attack is a priority. However, customers often overlook the crucial step of discovery and forensics, which is essential to understand the extent of the breach, access points and data compromised to prevent future attacks effectively.

- Ben Tercha

Regulatory Reporting & Disclosure

Q: What role does the FBI play interacting with regulators?

A: During FBI incident responses, cybercrime victims are treated respectfully without blame or involvement of regulators. The FBI's role is to find digital evidence and protect the identities of victims. Regulators are not part of the process to maintain a supportive relationship and encourage cooperation.

- Will McKeen

Q: Where should firms registered with the SEC focus their time and attention ahead of the final regulations (expected October 2023)?

A: Companies must adopt a multidimensional view of risk management and demonstrate compliance through best practices to meet SEC requirements. The reporting aspect, especially for material breaches, may pose potential havoc and recordkeeping challenges. While there may be ongoing debates and revisions, overall, it is a positive development.

- James Mignacca

Third-Party Risks

Q: What do regulators and other stakeholders expect to see in today's cyber climate with regard to third-party data access and management?

A: Taking a holistic view of the attack surface is crucial for organizations. Third parties with access to sensitive data or systems are part of the organization's attack surface and should be treated accordingly. Continuous automation is gaining importance, and some companies even demand regular risk management reports from their vendors. Recognizing that the organization's security depends on its weakest link highlights the importance of carefully evaluating and handling third-party risks. Extending the attack surface to include third-party vendors and considering them as vital parts of the security strategy is a practical and effective approach.

- James Mignacca

Q: How can businesses balance the benefits and advantages of outsourcing/co-sourcing functions of their company with the level of incurred risk (as a result of that relationship)?

A: Thoroughly assessing and managing third-party risks is crucial, as the level of risk incurred through these relationships directly impacts the organization's security. This involves diligent vendor management, evaluating their access to systems and data and verifying their cyber controls, policies and insurance coverage. Additionally, third-party independent audits like ISO or SOC 2 can provide valuable insights. Technical controls, such as restricting data access and using remote PCs, can further protect sensitive information. The focus remains on risk management, intolerance and partnering with the right vendors. A rigorous vendor management process ensures only reliable partners gain access to networks and data, enhancing overall security measures.

- Ben Tercha

New Threats Emerging

Q: What cyber trends do you expect to see over the next 12-24 months?

A: Although there were fewer cyber incidents in 2022 compared to 2021, hackers made billions more in that year, indicating that cyber incidents are becoming more damaging. The democratization of cybercrime has led to various actors being capable of causing significant harm. This includes nation-states with different motivations and criminal groups, particularly targeting South America, with a rise in bank fraud in Brazil. Additionally, AI is changing the effectiveness of scams, making it harder to identify phishing emails with poorly written content as AI can now create more convincing messages. The evolving attack surface and advancements in AI pose new security challenges, and organizations must seek more training and expertise to counter these emerging threats.

- Will McKeen

Q: What are your thoughts on how new AI tools (like ChatGPT and others) are going to impact security and compliance down the line?

A: AI and quantum computing are expected to significantly impact cybersecurity. While AI can enhance cyberattacks' speed and effectiveness, quantum computing could break conventional encryption methods. The linear model of cyberattacks by human hackers may shift to automated and more frequent attacks due to AI. Penetration tests may become more standardized as AI automates scanning and spear-phishing. Human involvement in attacks may decrease over time.

To counter these threats, organizations must adopt best practices, awareness training and comply with regulations. Compliance, though seen as a nuisance by some, is necessary to safeguard against future AI-driven cyber threats. Preparing for the changing cybersecurity landscape is crucial, given the potential dangers AI and quantum computing present.

- James Mignacca

Thinking Ahead: Post-Breach Reflection & Futureproofing

Q : For businesses that don't have the budget/resources to implement a comprehensive cyber risk management program, what's the single most important control to implement or enhance that will help protect them from the threat of a data breach?

A : In modern cybersecurity, there's no single most important control. With technology advancements and sophisticated attackers, a combination of measures is necessary. Prioritizing user security and comprehending the value of data are crucial for effective protection.

- Ben Tercha

A : Prioritize high-risk areas, safeguard valuable data and align budget allocation with compliance and risk management efforts. For a more effective and cost-efficient security strategy, understand where your data is to aid breach prevention and compliance.

- James Mignacca

A : Limit data access, regularly review access permissions, conduct threat assessments and implement best practices like zero trust networks. Identifying high-risk areas helps allocate budget for tools that target the most likely sources of infection, maximizing chances of detection and minimizing potential damage.

- Will McKeen

omega systems

w: www.omegasystemscorp.com
p: 610-678-7002
e: connect@omegasystemscorp.com

cavelo

w: www.cavelo.com
p: 1-844-422-8356
e: info@cavelo.com