

A Conversation with



Steven J. Kuperschmid, Esq.

Partner & Co-Chair, Cybersecurity and Data Privacy Practice Group



Richard M. Frankel, Esq.

**Of Counsel, Cybersecurity and Data Privacy Practice Group
Former FBI Special Agent with Over 25 Years of
Distinguished Public Service**

Introduction

The recent data breach affecting the Federal Bureau of Investigation has raised significant concerns across both the public and private sectors. The attack, believed to have been carried out by the notorious hacking group, ShinyHunters, in apparent retaliation for a Public Service Announcement published by the FBI's Internet Crime Complaint Center describing the gang as cybercriminals who use coercive tactics, harassment, and swatting, underscores a troubling new dynamic: cybercriminal organizations are no longer merely evading law enforcement—they are striking back. When even the nation's premier law enforcement agency falls victim to such an attack, it highlights both the evolving sophistication of threat actors and the vulnerabilities that exist within even the most security-conscious organizations.

To help our clients understand the implications of this incident and what lessons can be drawn for their own cybersecurity posture, I sat down with my colleague, Richard M. Frankel, Of Counsel, in our Cybersecurity and Data Privacy Practice Group. Rich brings a unique perspective to this discussion, having served more than 25 years with the FBI, including as Special Agent In-Charge of several FBI field divisions and as the Associate Director of National Intelligence and Senior FBI Representative to the Office of the Director of National Intelligence. His career has been devoted to understanding, investigating, and defending against exactly the types of complex, coordinated attacks that this breach represents.

The following Q&A addresses the key questions businesses should be asking in the wake of this incident.

Q&A with Richard M. Frankel

Question - Rich, given your extensive experience within the FBI, what is your initial reaction to this breach, and how significant is it in the broader landscape of cybersecurity incidents?

Answer - This breach is extraordinarily significant—not because of the specific data that may have been compromised, but because of what it represents. The FBI is not just any organization; it is the lead federal agency for investigating cyberattacks and the repository of some of the nation's most sensitive law enforcement and intelligence information. If threat actors can penetrate the FBI's defenses, it sends a clear message to all of us: no organization is immune. For businesses, this should serve as a wake-up call. The sophistication of today's adversaries—whether nation-state actors, organized criminal enterprises, or advanced persistent threat groups—has reached a level where traditional security measures are often insufficient.

Question - What do we know—or can we reasonably infer—about the nature of this attack? What techniques might the threat actors have employed?

Answer - While the full details are still emerging, attacks of this magnitude against high-value government targets typically involve a combination of advanced techniques. Some reports indicate it may have been a vulnerability in the Oracle system that supported the FBI's jobs website. According to these reports, ShinyHunters utilized a similar vulnerability in the past against a national business. Additionally, we often see spear-phishing campaigns targeting employees with access to sensitive systems, exploitation of zero-day vulnerabilities, and supply chain compromises where attackers infiltrate a trusted vendor or software provider to gain access to the ultimate target. Nation-state actors, in particular, have demonstrated patience—sometimes maintaining persistent access within a network for months or even years before executing their objectives. Businesses should understand that these same techniques are increasingly being deployed against the private sector.

Question - The hacking group ShinyHunters has been identified as the suspected perpetrators, and this attack is believed to be retribution for FBI operations against them. What can you tell us about this group and what does their involvement suggest?

Answer - ShinyHunters is a notorious cybercriminal group that has been responsible for some of the most significant data breaches in recent years. They emerged around 2020 and quickly established themselves as one of the most prolific and capable threat actors in the cybercriminal ecosystem. The group has targeted major companies including Microsoft, AT&T, Ticketmaster, and numerous others, stealing and selling hundreds of millions of user records on dark web marketplaces. The FBI has been actively pursuing ShinyHunters, and if this attack is indeed retribution for those efforts, it represents a deeply troubling escalation. We are seeing a criminal organization not merely evading law enforcement but actively striking back against it. This sends a chilling message and demonstrates that these groups have both the capability and the audacity to target even the most formidable adversaries. For businesses, this underscores that threat actors are becoming increasingly bold, and organizations that cooperate with law enforcement investigations may themselves become targets for retaliation.

One of the alleged leaders of ShinyHunters was arrested by the Dutch National Police. He is separately being investigated on suspicion of ordering two murders abroad. The Dutch High Tech Crime Unit executed the arrest under Dutch law.

The Dutch National Police, fully supported by the FBI, moved quickly to protect victims and preserve critical evidence.

Question - What are the potential consequences of this breach for national security and ongoing investigations?

Answer - The consequences could be far-reaching. ShinyHunters had stolen sensitive data, including Social Security numbers, dates of birth, phone numbers, addresses and emergency contact information, relating to thousands of FBI agents, staff and individuals who had applied for positions with the FBI.

ShinyHunters compromised the FBI's jobs website, the main portal for prospective employees to learn about the FBI and initiate the application process. The FBI is "aggressively" investigating the breach, including whether the hackers got into third-party software or the FBI's own internal systems. Depending on what data was accessed, we could be looking at compromised investigations, burned sources and methods, and the exposure of sensitive information about individuals who have cooperated with law enforcement. The retaliatory nature of this attack adds another dimension—if ShinyHunters accessed information about the FBI's operations against their group or other cybercriminal organizations, it could compromise ongoing investigations and potentially endanger personnel involved in those efforts. Perhaps equally concerning is the potential chilling effect on future cooperation, informants, witnesses, and partner organizations may be more reluctant to share information if they perceive the FBI cannot adequately protect that data.

The hackers at ShinyHunters used a new vulnerability with Oracle PeopleSoft, a human resources management program used mainly by large organizations, universities, governments, and corporations to manage human resources, finance, supply chain, and student administration, among others. In June 2026, ShinyHunters identified a Java deserialization vulnerability in Oracle's PeopleSoft Environment Management Hub servlet that allowed them to achieve web shell deployment on vulnerable servers. This attack on Oracle bears similarities to this breach involving the FBI, in that both incidents involved the exploitation of Oracle-related enterprise vulnerabilities, highlighting the significant risks posed by unpatched vulnerabilities in widely deployed enterprise platforms.

Question - For businesses that may have shared information with the FBI—whether through cyber incident reporting, participation in public-private partnerships, or as part of investigations—what should they be concerned about?

Answer - This is an important concern. Many businesses have proactively engaged with the FBI, sharing threat intelligence or reporting cyber incidents as encouraged by federal guidelines and, increasingly, required by regulation. Companies should conduct an internal review to understand what information they may have shared with the Bureau and assess whether that information, if compromised, could create additional risk. This might include details about their network architecture, vulnerability assessments, incident response capabilities, or information about specific threat actors targeting their systems. I would recommend that affected organizations consult with legal counsel to understand their notification obligations and consider enhanced monitoring for any unusual activity that might suggest adversaries are using compromised information.

Question - What lessons should businesses take away from this incident regarding their own cybersecurity programs?

Answer - The most important lesson is that cybersecurity must be viewed as an ongoing process, not a destination. The FBI has substantial resources, talented personnel, and sophisticated technology—and yet a breach occurred. Organizations must adopt a mindset that assumes adversaries will eventually penetrate their defenses, and plan accordingly. This means implementing defense-in-depth strategies, segmenting networks to limit lateral movement, deploying robust detection and monitoring capabilities, and having well-rehearsed incident response plans. Additionally, organizations should prioritize identity and access management, including multi-factor authentication and the principle of least privilege. Human factors remain critical—ongoing security awareness training can help prevent the social engineering attacks that often serve as initial entry points.

Question - Supply chain security has been a major focus since incidents like SolarWinds. How does this breach factor into that conversation?

Answer - Supply chain risk continues to be one of the most challenging aspects of cybersecurity. Organizations are only as secure as the weakest link in their ecosystem of vendors, partners, and service providers. While we do not yet know if this breach involved a supply chain compromise, it is a technique that sophisticated adversaries favor precisely because it allows them to bypass direct defenses. Businesses should conduct thorough due diligence on their vendors, include robust security requirements in contracts, maintain visibility into what access third parties have to their systems, and implement monitoring to detect anomalous activity from vendor connections. The days of implicit trust are over; verification must be continuous.

Question - From a governance perspective, what should boards of directors and C-suite executives be asking their security teams in light of this incident?

Answer - Boards and executives should be asking several critical questions. First, what are our crown jewels—the data and systems that, if compromised, would cause the greatest harm—and how are we protecting them? Second, do we have adequate visibility into our network to detect sophisticated, persistent threats, not just commodity malware? Third, when was our incident response plan last tested, and are we confident it would hold up against an advanced adversary? Fourth, what is our exposure through third-party vendors and partners? And fifth, are we meeting our legal and regulatory obligations regarding cybersecurity, including the new SEC disclosure requirements? Cybersecurity is no longer solely an IT issue—it is a board-level risk management concern, and oversight must be commensurate with the threat.

Question - How do you expect the regulatory landscape to evolve in response to incidents like this?

Answer - We are already seeing a significant shift toward more prescriptive cybersecurity regulations and mandatory incident reporting requirements. The Department of War and the Department of Commerce and other cabinet-level departments, and various regulatory agencies are implementing increasingly stringent cybersecurity requirements and guidance, not to mention the ever-changing regulatory landscape at the state level. The Cyber Incident Reporting for Critical Infrastructure Act, SEC cybersecurity disclosure rules, state privacy laws with security requirements, and sector-specific regulations are all raising the compliance bar. High-profile incidents involving government agencies tend to accelerate this trend, as policymakers face pressure to demonstrate action. Businesses should expect continued regulatory expansion and should proactively work to build mature, well-documented cybersecurity programs that can withstand regulatory scrutiny. Those who view compliance as a ceiling rather than a floor will find themselves increasingly exposed.

Question - Finally, despite this incident, should businesses continue to engage with the FBI and other law enforcement agencies on cybersecurity matters?

Answer - Absolutely. While this breach is concerning, it does not change the fundamental value of public-private partnership in combating cyber threats. The FBI and other agencies possess threat intelligence, technical capabilities, and investigative resources that can be invaluable to businesses facing a cyber incident. Reporting incidents and sharing threat information helps not only the individual organization but the broader ecosystem—information shared about one attack can help protect countless others. Always, when there is a cyber incident affecting you or your business, file a report with the FBI's Internet Crime Complaint Center through its website at www.ic3.gov. I would encourage businesses to maintain and strengthen those relationships while being thoughtful about what information they share and how. The FBI will undoubtedly learn from this incident and emerge with strengthened defenses. Disengaging from law enforcement partnership would only benefit the adversaries we are all working to defeat.

Conclusion

The FBI data breach serves as a stark reminder that cybersecurity is an arms race with no finish line. If our nation's foremost law enforcement agency can be targeted successfully, every organization must take seriously the threats they face. The question is not whether your organization will be targeted, but whether you will be prepared when it happens.

The attorneys in Ruskin Moscou Faltischek's Cybersecurity and Data Privacy Practice Group work closely with clients to assess their current cybersecurity posture, develop and test incident response plans, navigate the complex regulatory landscape, and respond effectively when incidents occur. If you have questions about how this breach may affect your organization or would like to discuss strengthening your cybersecurity program, please do not hesitate to reach out.

Steven J. Kuperschmid, Esq.
Partner & Co-Chair, Cybersecurity and Data Privacy Practice Group
(516) 663-6686
skuperschmid@rmfpc.com

Richard M. Frankel, Esq.
Of Counsel, Cybersecurity and Data Privacy Practice Group
Former FBI Special Agent – Over 25 years of Distinguished Public Service
(516) 663-6534
rfrankel@rmfpc.com

***RMF Law Clerk Nilufar Shahpanahi contributed to the drafting of this article.**