April 16, 2013

CORPORATE COUNSEL

The War On Cybercrime: How Far Can You Go?

Gabriel Ramsey, Mark Mermelstein, and James Hsiao

Cybercrime is neither rare nor isolated these days. You no longer need to be a major bank, retailer, credit card company, social media site, or government to become a target. Every company with an online presence, or even a connection to the Internet, has become fair game.

Symantec has reported that, year over year, malicious Internet attacks are steadily increasing. Their most recently released report (2012), showed that in 2011, these attacks had increased by over 81 percent, and unique malicious software ("malware") variants increased by 41 percent, compared with 2010. It is no longer a question of whether a company will be hacked, but when. Attacks are also increasingly "targeted." For example, in January The New York Times was targeted through a technique called "spear-phishing," where innocuous-looking email or social media messages were tailored to individual employees and designed to install code that could access, monitor, or steal information.

Obvious targets, such as financial institutions, credit card companies, and defense contractors, have often already "hardened" their defenses. Thus, cyberattacks have steadily increased against other targets, such as cloud services providers—where reams of data can be accessed through a single attack—less obvious commercial targets holding valuable information, and companies in the supply chain with access to a primary target's systems through authenticated connections. Becoming an attack vector against a primary target can be extraordinarily costly, with significant reputational implications.

Given the potential loss of the most sensitive assets, information, and trade secrets, and the collateral risks of such an incident, companies must develop an integrated, proactive strategy involving technological features, law enforcement partnerships, and private legal enforcement, to prevent, respond to, and deter the massive and growing problem of cybercrime.

Integrated Defenses, Planning, and Investigative Capabilities

Network security historically consisted of a firewall between the Internet and internal networks. Like a proverbial Great Wall, the "crunchy" exterior protected the "soft" interior from the marauding horde. As the chief security officer of the Times recognized in the attack on the newspaper, attackers "no longer go after [the] firewall," but instead "go after individuals." With targeted techniques, companies must assume that computers will become compromised and cannot rely on security software and hardware to stop attackers. For example, in the Times attack, the attackers installed 45 pieces of custom malware, but antivirus software was only able to detect a single instance. Therefore, companies must implement multi-tiered security throughout their networks, not simply border checkpoints, and educate employees to create a security-aware culture. Companies should widely deploy the strongest commercially viable encryption to protect their data.

Gabriel Ramsey

Mark Mermelstein

But security technology and awareness alone are not enough. Companies must build investigative capabilities into their technological presence, rather than trying to "bolt them on" as an afterthought. Proper investigation can provide intelligence about methodology, techniques, and attack patterns, provide guidance as to potential future attacks, or lead to the identities of the attackers. Evidence-gathering protocols established on the front end can pay dividends on the back end. For example, monitoring intrusions may involve "honeypots"—traps that appear to be legitimate network nodes—which isolate attackers and afford time to investigate attacks as they occur.

Built-in data markers, extensive logging, and methods of parsing this mountain of information are also important. Breach response plans should include securing compromised systems without alerting the attacker, cloning of compromised machines to maintain forensics, and tracing of connections to determine the true origins of attacks. Given the sophistication and motivation of the adversaries, security firms, such as CrowdStrike, have responded to this need by offering sophisticated proactive monitoring, investigation and intelligence services, and also offensive techniques such as surveillance and reconnaissance, counter-espionage, and denial-and-deception.

Whether handled in-house or outsourced, these strategies raise legal implications that potential cybercrime victims need to understand if they are going to seriously consider the more aggressive of these approaches.

Proactive Engagement

What can a company do with information about an attack or an attacker?

Collaborate With the Government: Companies can opt to collaborate with law enforcement. The U.S. Attorney's Office, for example, created a National Security Cyber Specialist Network, with a designated assistant U.S. attorney in every U.S. Attorney's office to act as a centralized resource to deal with cybercriminals, especially when there may be national security concerns. Criminal prosecution via referral to the government is just one law enforcement option. Other agencies, such as state attorneys general or public consumer protection agencies, may bring civil enforcement actions that have the advantage of a lower burden of proof and can rely upon flexible state consumer protection laws.

Successful partnerships with law enforcement maximize the relative strengths of the private and public sectors. They rely heavily upon a company's ability to diligently collect and present technical information about the cybercrime

event and the government's ability to investigate and track down the perpetrators. For example, law enforcement has the ability to use subterfuge and enlist the aid of foreign law enforcement to track down the perpetrators, use extradition treaties to get them to the United States, and then use threats of incarceration and promises of leniency to convince them to identify others. In addition, law enforcement can use asset forfeiture laws to seize criminal instrumentalities and proceeds for the benefit of victims.

A successful law enforcement referral program takes advanced planning and development. If they work out their strategy in advance, victims can not only benefit from the attackers being criminally prosecuted but also position themselves for monetary restitution arising out of government actions. However, there are challenges as well. Some are manageable, such as potential privacy issues regarding data sharing. Others are thornier, such as maintaining control in any situation where government enforcement is involved. Those who invite the government into their lives had better be sure their own house is in order. Certainly, understanding when to refer matters to law enforcement and having a vast array of relationships with law enforcement is an invaluable tool to have in the cybercrime-fighting tool-belt.

Investigate and Enforce Through Civil Litigation: Cybercrimes also violate civil laws; laws such as the Computer Fraud and Abuse Act, Electronic Communications Privacy Act, and state malware and hacking statutes may be enforced. Litigants may use intellectual property regimes such as trade secret, copyright, or trademark law to address data theft or misleading activities. Even the oldest common law regimes such as trespass, conversion, unjust enrichment, or nuisance can be valuable in combating cybercrime. Civil enforcement may have advantages of control, flexibility, and speed that the government may not have, a lower burden of proof, and a more focused goal of protecting a particular victim (rather than the public at large).

Also, a private investigation and civil litigation program may allow more focused development of information about threats targeting a particular company. An effective civil litigation program requires a team that is steeped in the cybercrime ecosystem, understands both the legal and technical issues including the limits on so-called "cyber-sleuthing," and that understands risk management techniques. The team must also have strong relationships in the private and public sectors and understand how to navigate a complex international environment that may involve issues of sovereignty, competing policies, and competing laws.

In the simplest form, armed with technical data and leads, a victim can initiate civil "John Doe" cases to avail itself of discovery mechanisms and the leverage that a legal proceeding can bring, to better develop identification of perpetrators. This may simply result in more robust law enforcement referrals. However, even sophisticated cybercriminals can be found. With some investment, it is certainly possible to identify perpetrators and pursue them for damages, injunctions, deterrence, or even with the goal of very loud and very public attribution. Civil litigation can also be used to dismantle technical infrastructure used to carry out attacks, even if perpetrators cannot be identified. In recent years, Microsoft has dismantled a number of malicious "botnets" through this means.

"Hacking Back"? While some cybercrime victims pay ransom or protection money to cybercriminals that have already infiltrated their system—ostensibly to avoid further harm—other frustrated companies are starting to explore the idea of going on the offensive against cybercriminals with so-called "hacking back" or "active defense." This strategy can be employed either to deter cybercriminals or to further investigations. The "offensive," however, implicates technological, legal, and ethical issues. Indeed, active countermeasures may be vulnerable under the same laws used to pursue cybercriminals. It is a rare organization that has the technical expertise necessary to go toe-to-toe with cybercriminals who can carry out advanced targeted attacks. Without the right technical resources, the right partnerships, and a firm understanding of the law, such efforts may be risky as well as difficult. Nonetheless, the mere fact that there is widespread and serious debate on this topic signals a shift in the discourse about dealing with malicious actors, protecting valuable assets in the information economy, and preserving the integrity of the Internet.

Cybercrime is a massive and growing problem. The stakes are high, and the problem is not going away. Companies cannot ignore the threats, not least because the regulatory and litigation environment—from Securities and Exchange Commission rules and Federal Trade Commission regulations to breach notification laws and class action suits—now require increased attention. Potential victims must be aware of the threats and proactively organize and implement an affirmative strategy. To do otherwise risks substantial exposure and substantial loss and will embolden the adversaries. No one can afford that outcome.

Gabriel Ramsey and Mark Mermelstein are partners at Orrick, Herrington & Sutcliffe. James Hsiao is an associate at Orrick. Ramsey has significant experience combating cybercrime, trade secret misappropriation, and technical abuses and threats. Mermelstein, a former L.A. County public defender, focuses his practice on the representation of white-collar criminal defendants and victims of crimes such as cybercrime. Hsiao, a former technology professional who has dealt with information security issues, focuses on litigation matters involving a myriad of areas such as securities, white-collar, and Internet issues.

Mark Mermelstein
Partner, White Collar & Corporate Investigations
Orrick, Herrington & Sutcliffe
(213) 612-2204
mmermelstein@orrick.com

Gabriel Ramsey
Partner, Intellectual Property
Orrick, Herrington & Sutcliffe
(650) 614-7361
gramsey@orrick.com