NACD Directorship
Boardroom Intelligence

VIEWPOINT

Cyber Extortion: What to Do When Your Data is Being Held for Ransom

by **Mark E. Robinson** and **Cynthia J. Larose** | March 10, 2015

Imagine you are the IT systems administrator of a large corporation. Coffee in hand, you sit down one morning and log in. You receive a message that there has been an intrusion into the corporate database, a large amount of sensitive data has been stolen, and your backup in the cloud has been compromised. BUT "U R Datta WilL B REstoReD" once you pay "BiTCoiNS U.S.$50,000" to the anonymous cyber-extortionists. If you refuse, your data will be sold or publicly released. You are instructed not to involve police. The amount demanded is short money, you notice. Better to pay and move forward than risk the potentially catastrophic consequences.

The value of the kidnapped data is immeasurable: trade secrets, client and customer information, personal financial information, compromising emails between top executives. The list goes on. You owe a duty to all of these stakeholders to protect the company's most sensitive information and to resolve this crisis with the least damage possible. Should you quietly pay the ransom and hope the extortionists return the company's crown jewels? Or should you take a hard line, call the authorities, and refuse to submit to cyber terrorist threats that may or may not be real, lest you become a compliant target for future extortions?

Those at Banque Cantonale de Geneve likely considered these gut-wrenching questions when they were victimized by hacking group Rex Mundi. On January 9, 2015, Rex Mundi demanded 10,000 euros in exchange for hijacked emails. The bank refused, and Rex Mundi subsequently released the data to the public. Fortunately, it turned out that the leaked data (the hackers were semi-bluffing) consisted only of clients' inquiries, not accounts. However, the damage to the bank's reputationwas immeasurable. It had a "reputation for helping clients conceal information from tax authorities" and had just struck a deal with Swiss authorities to pay fines for helping wealthy Americans avoid taxes. The extortionists struck when the bank's reputation was already on the line and the resulting reputational damage arguably may have been worse than had truly sensitive information been released.

So how can companies protect themselves from cyber extortion and how should they respond to such threats?

Companies should start by assembling a data breach response team consisting of the relevant personnel, starting with IT/technical, legal, forensic, and PR professionals. This group must convene, anticipate, and prepare responses to potential data breach, cyber extortion, hacktivist and other nightmare scenarios. There are two critical steps companies can take to embark on this process.

1. Identify and protect the company's crown jewels—the most sensitive data—and ensure that information is safeguarded to the maximum extent possible. This means developing a comprehensive risk management plan that includes robust border control as to all points of entry, including within your own company as well as third party vendors and business partners with network access. There also must be active network monitoring for external intrusions but also unusual activity within the network. More and more, hackers are lying in wait within the system, plotting their attack and exit, deviating from the traditional "smash and grab" route of simply stealing personally identifiable information and then receding into the nether regions of the dark web. Password protection is no longer enough, meaning that companies need to employ multi-factor identification with constantly changing access codes. There also needs to be fortress-like back-up and tested disaster recovery systems, regular penetration testing and all attendant good cyber hygiene practices.
2. The sad truth is that you need to assume that whatever you do to protect the crown jewels is not going to work. Your defenses, no matter how robust or state of the art, will eventually be compromised. Begin to plan accordingly. For the cyber extortion exercise, just like every other significant risk, company management needs a well thought-out plan. The dilemma of "pay or don't pay" needs to be debated internally in advance, and the response options need to be clearly laid out. Decisions, tradeoffs, and pros and cons cannot be discussed for the first time when there's a gun pressed to the company's head.

You will quickly find that there is no win/win answer. The best option is to choose the least damaging of the bad options based on all the facts and circumstances. Policies like "Never negotiate with terrorists" and "Never trade arms for hostages" all sound good on paper until the terrorists kill the hostages, or in this case, destroy—or, perhaps worse, publicly release—the kidnapped data.

Unfortunately, cyber extortion happens all the time and frequently goes unreported. If you cave and pay, you may become easy prey. If you don't pay the ransom and instead go to the authorities, you may suffer economic consequences far greater than the often short money demanded in the first place. These evolving forms of cyberattack are threats that can never be eliminated. The best defense is proactive, thoughtful and intelligent preparation on all fronts.

Mark E. Robinston serves as co-chair of the Mintz Levin's national white collar defense and investigations practice and is a nationally recognized authority in government investigations and enforcement and cybersecurity defense. Mark represents, advises, and defends public and private sector clients in connection with internal investigations, regulatory enforcement actions, commercial litigation, and large-scale data breaches. Cynthia J. Larose is chair of the Mintz Levin's Privacy & Security Practice and has extensive experience in privacy, data security, and information management matters, including state, federal, and international laws and regulations on the use and transfer of information, behavioral advertising, data security breach compliance and incident response, data breach incident response planning, as well as data transfers in the context of mergers and acquisitions and technology transactions. The authors acknowledge the work of Mintz Levin litigation associate Jane Haviland in researching and helping to develop the content of this article.

Originally appeared on NACDonline.org on March 10, 2015.