The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

September 2013 © 2013 The Metropolitan Corporate Counsel, Inc. Volume 21, No. 9

# Four Stages Of Cyber Risk Management

**Joshua Gold**

ANDERSON KILL

In case anyone had not noticed that the severity of data breaches keeps reaching ever-more unnerving levels, a friendly reminder recently arrived in the form of federal indictments unsealed against a group of alleged cyber criminals. The alleged cyber gang's hit list included the NASDAQ, major retailers and an array of other large businesses, including a slew of financial institutions. The alleged cyber gang had amassed an impressive haul over a period of years, stealing hundreds of millions of dollars and more than 150 million financial account and credit card numbers. This is on the heels of news that cyber thieves stole $45 million from ATMs in a coordinated plot spanning numerous countries.

But as most now know, it is not just large financial institutions and retailers that are targeted. Small and medium-sized businesses are prime targets for cyber thieves these days, based on the perception that they are the weakest security link in the chain. While that perception may be debatable, the risks are real for businesses of every size and industry – as well as universities, hospitals, key national infrastructure entities and the military.

Some hackers are mercenaries. Some are nationals. All pose a serious threat. A few months ago, a report was released indicating that computer hackers in Asia accessed and copied several U.S. weapons designs. Other cyber attacks have sought to degrade data or shut down key infrastructure altogether.

Joshua Gold

The indictments unsealed in New Jersey remind us all that sound security compels us to continually reevaluate and evolve to keep pace with both new and modified cyber threats. As demonstrated by the hundreds of millions of dollars pilfered by the alleged cyber gang, even financial institutions, which employ some of the best and most cutting-edge data security measures in the world, are susceptible to sophisticated cyber attacks.

The bottom line is this: if you have information worth stealing or oversee infrastructure worth meddling with, you are in the crosshairs of cyber criminals worldwide, every day.

Whether you are counsel to a financial institution, a large retailer, a small services business, the Defense Department, or a university, you and your organization are well advised to manage data breach and hacking risks to the fullest extent possible through a combination of advance planning and risk transfer. Planning should encompass not only avoiding a breach but also handling a breach should your best efforts at prevention fail.

Coping with cyber risk can be divided into four stages: disclosure, prevention, crisis management and insurance coverage. Below, we consider each in turn.

### 1. Know Your Disclosure Responsibilities And Meet Them

Full and fair disclosure of risks is the first vital step in risk management, as failure to disclose may create a mare's nest of liabilities when a breach does occur. To do this right, review guidance about what and how much detail should be disclosed to investors, customers and other stakeholders. Organizations should comport themselves with the letter and spirit of guidance from the Securities and Exchange Commission and the Federal Financial Institutions Examination Council concerning data security issues and risks. The focus on this issue will only get larger going forward. Lawmakers recently asked the SEC to beef up disclosure responsibilities about cyber risks and preparedness for the benefit of investors. Remember also that disclosure may have to go beyond just assessing and disclosing the risks of data theft. Depending upon the risk profile of the entity, disclosures and risk assessments may very well have to address data destruction and alteration.

### 2. Develop One Plan To Avoid A Breach And Another To Handle A Breach

*Avoiding A Breach*

In-house lawyers, risk managers and IT departments must now work in tandem to develop and refine plans to avert a cyber-data breach and to handle one should a breach occur. It is advisable (if not quasi-mandatory for certain businesses) to involve someone from senior management in this team effort. Preparedness for a data breach is key.

Perform due diligence on all vendors used to host and manage data, including cloud computing firms. Negotiate clear and reasonable protections into vendor and cloud contracts.

Understand the use and know the identity of sub-contractors hired by third-party computer and cloud vendors. Sub-contracting is prevalent now. Make sure you know where the data is housed and by whom (e.g., is it being hosted in the U.S. or in some other country?).

Assessing cybersecurity of third parties and business partners is always a tricky situation. Often, for security purposes, the

***Joshua Gold*** *is a Shareholder in the New York office in the law firm of Anderson Kill. Mr. Gold regularly represents policyholders in insurance coverage matters and disputes concerning liability, arbitration, time element insurance, electronic data, and other property-casualty insurance coverage issues.*

***Please email the author at jgold@andersonkill.com with questions about this article.***

counterparty understandably does not want to reveal in great detail its specific security measures. At the same time, the party putting trust in those security measures is not comfortable doing so sight unseen. Accordingly, smart planning should budget for the use of security assessment firms for vendors and cloud firms. This can comprise a core part of your due diligence.

To avoid potential liability and other unwelcome attention, update privacy disclosures to customers and others when third-party data is shared with or entrusted to third parties.

Encryption should be used as much as possible – notwithstanding that it is a subject of much debate. Some argue the term is misleading, some argue that semantics aside, encryption is often unnecessary, and others complain that encryption is expensive in certain contexts (such as cloud computing), while others argue that some low levels of encryption are worthless from a security standpoint. While the debate probably warrants its own article, for purposes of risk management, it is better to err on the side of encryption, even if it's more expensive to do so. A security breach involving data that is well encrypted may lead to significantly smaller losses and notification costs. It may also lead to decreased potential liability and less negative press where the data is disclosed by third parties through hacking or otherwise.

A solid cybersecurity plan also requires regular and updated training. Training employees how to safeguard data and avoid breaches at the point of hire is good, but training should not end there. Ideally, regular retraining of employees regarding data security procedures (including the basics like password protection) should be implemented – especially for those employees who have access to financial account records, health information or very sensitive information such as national defense data or key infrastructure data. Given that security threats and scams are varied and change with the times, regular retraining is a good idea to build into any security protocol.

Have computer data fully mapped. Like any good inventory, this will tell an organization what data it has and where. This also helps guard against so-called rogue cloud computing (situations where data is on the cloud without the knowledge of lead individuals in the IT department).

In your contracts with third-party vendors and cloud firms, make sure that you 1) have rights for periodic security audits, 2) have thought up-front about termination of data hosting and associated costs and obligations for removing data from the host's servers, and 3) have express rights to be notified in the event of a security incident aimed at your data or aimed at the host more generally.

*Advance Planning For Handling A Breach*

If an organization suffers a security breach and has no plan in place for handling it, that entity is already behind the eight ball.

Key elements of a data security incident plan include the assignment of individuals and resources charged with responding to an incident, including compliance with state notification laws; cooperating with the Federal Trade Commission (FTC), state attorneys general, and other law enforcement; coordination of work with computer forensic firms that assess the breach and advise on averting further disclosures and plugging holes; coordination of work with in-house and outside counsel to address potential liability associated with a breach; customer relations; investor relations; insurance company communications and notifications; and post-mortem assessments to avert future security incidents. Having such a team in place will reduce delays in responding comprehensively to a data breach.

## 3. Risk Transfer Through Insurance

As part of a risk management plan for cybersecurity, it is critical that businesses figure out their insurance needs. This is easier said than done, because the cyber insurance market remains in a state of flux. The insurance marketplace has expanded greatly for dedicated cyber insurance policies for both "first-party" risks (e.g., breach notification costs) and "third-party" risks (e.g., class action litigation defense and indemnity), with lots of different insurance companies all over the world getting in on the action.

Insurance coverage can be purchased for a variety of different losses emanating from a cyber incident, including for the costs of defending class action suits, indemnifying those who have a stake in the disclosed information, and responding to law enforcement agencies and the FTC. Insurance coverage is also available for investigating cyber breaches and complying with state notification laws. There is also insurance coverage for time element losses, where cyber incidents affect business income due to the hacking of a system.

Historically, many different types of insurance policies have provided some measure of coverage for cyber-related perils. All-risk property policies, general liability policies, and crime insurance policies often contain some level of insurance coverage for computer-related losses. Business package policies also occasionally cover data losses and other related perils. Indeed, one insurance coverage case we handled for a policyholder after it was hacked and had customer information stolen involved coverage under both a general liability policy and a commercial crime policy. The policyholder recovered its loss in full after the general liability company paid without objection and after we prevailed in court against the commercial crime insurance company.

In more recent years, however, the insurance industry has added exclusions to avoid claims under many business insurance policies and push policyholders toward buying separate insurance policies. This makes the insurance purchase more challenging when a business is deciding how best to cover cyber threats. Policyholders are well advised to pick carefully as they determine what coverage they already have under more standard business insurance policies and what coverage they need to purchase to cover potential gaps thanks to new exclusions and new cyber threats.

The good news is that the insurance market for policyholders shopping for cyber-specialty policies is more competitive than it ever has been, and this means more flexibility and coverage options than was the case five years ago. Despite this, insurance policies and terms are still unnecessarily complicated, and businesses would be well advised to closely examine policy forms so that they are making the smartest choices.

## 4. Don't Stand Pat

The risk profiles of most businesses and organizations are changing rapidly due to ever-evolving cyber threats. Make sure your risk management processes and insurance policies keep up with these changes too. Most insurance coverage can be tailored to expressly cover the policyholder's risk profile. The bottom line is that the insurance coverage should match the cyber exposure of the policyholder so that coverage is in place when needed the most.