
Why cybercrime matters to general counsel

February 2011

*Breaches underscore
need for active role*

At a glance

Cybercrime is a force to be reckoned with that calls for the attention of general counsel

General counsel are often the last to arrive at the cyber scene of crime

GCs can become appropriately involved in cyber issues at the right time and ensure the cyber risk is properly mitigated



Introduction

General counsel involvement in cybercrime is increasingly critical to protecting the organization and its intellectual property from the significant (and successful) nature of the cyber threat. By virtue of their pivotal role within the company, general counsel need to arrive at the scene of the crime early, remain involved continuously, and be prepared to act quickly in the event the company comes under one such silent, yet potentially catastrophic, attack.

Cybercrime: a force to be reckoned with

One message is clear from the near decade-long explosion in data breaches resulting in the theft and sale of more than a hundred million credit and debit card numbers: Cyber criminals are successfully compromising systems of companies in every industry and stealing their key assets. These breaches have a significant, and potentially devastating, impact on a company's reputation or financial position. Almost certainly, the breaches open the company to litigation or regulatory investigations when customers' personal information is compromised. Companies are required to afford certain levels of protection to various types of personal information under any number of state and federal statutes. As a result,

the compromise of such information can lead to class action lawsuits or regulator inquiries.

As a result, one would expect the general counsel to be the first in command to navigate the issues associated with data breaches and cybercrime events. But the general counsel is often one of the last to arrive at the scene of the crime. Issues related to cybercrime and data breaches remain buried deep in information security and information technology (IT) within an organization, unlikely to surface even in the gravest of circumstances. This is the case even among leading organizations that recognize that the strategic importance of protecting the confidentiality, integrity, and accessibility of information transcends a strictly IT responsibility.

Why should general counsel care about cybercrime? Why are they often the last in line to hear about these issues in their company? How does the delay in the general counsel's involvement open companies up to further litigation risk and financial exposure? This article answers these questions and concludes with practical tips for general counsel.

Laying the Groundwork

Cybersecurity is not just an IT issue

In the past 18 months, there have been a series of 'first-ers' relating to cyber issues, which have elevated cybersecurity to a national priority. President Obama has created a new office on cybersecurity, appointed a cybersecurity coordinator, and publicly acknowledged that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."¹ Shortly after the creation of this office, the Administration released its Cyberspace Policy Review, which addressed the critical importance of making cybersecurity a national priority.² To highlight one statistic, the report stated that "industry estimates of losses from intellectual property to data theft in 2008 range as high as \$1 trillion."³ Further, in October 2010, the first-ever US Cyber Command—designed to protect Department of Defense networks—became operational under four-star general Keith Alexander.

Similarly, on the private sector side, several significant 'first-ers' have elevated cybersecurity concerns beyond the IT world. A criminal hacker from Miami was sentenced in March 2010 to 20 years imprisonment for his role in the biggest hacking and identity theft case ever prosecuted by the Department of Justice. In that incident, more than 170 million credit and debit card numbers from over 14 retail and credit card processors were stolen or put at risk of being stolen.⁴

What was eye-opening was that these crimes were committed by kids who have self-taught computer skills and who were under the influence of illegal recreational drugs. This underscored the ease with which cyber criminals can access and successfully penetrate the private sector's systems and the vast amounts of personal information they contain.

The following month, several companies acknowledged cyber attacks on their systems by entities in China groups that were targeting intellectual property and other sensitive data. A number of months later, security researchers discovered the first-ever sophisticated worm (known as "Stuxnet") targeted at shutting down specific sensitive industrial control systems. Both the perpetrators in this type of attack (state sponsored-adversaries, rather than malicious individual hackers) and the target (industrial control systems) were firsts. The sophistication and dedication of the state-sponsored adversary entered public consciousness.

Clearly, cybersecurity issues now reside within the sphere of senior public policy and business leadership, rather than solely within the IT world.

System compromises create legal obligations

The second reason general counsel should care about cybercrime is that cyber intrusions and other types of system compromises create legal obligations. State data breach notification statutes are a good example. Legal obligations under

1 <http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>

2 http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

3 *Id.* at 12.

4 <http://www.justice.gov/usao/nj/press/press/files/pdffiles/dojgonzalez0326rel.pdf>.

Hackers often leave a number of ‘back-doors’—rendering the system vulnerable to re-entry.

many of these statutes arise not when personal data is stolen and misused by an unauthorized individual, but rather when a system is compromised and personal information is potentially at risk of being stolen and misused. Under Maryland statute 14-3504, for example, companies are required to conduct a “reasonable and prompt investigation” when a breach has occurred that compromises the security, confidentiality, or integrity of personal information maintained by the business.⁵

Here, the distinction between system compromise and data compromise is critical. It is the event of a system compromise that creates a legal obligation to conduct an investigation of the compromise, not the event of data being stolen and/or misused. Often, the general counsel’s office is informed of the data breach, if it is informed at all, only after an investigation has been underway and the IT department or an external investigation team has confirmed that data has been stolen from the system and misused, or is likely to be misused.

The problem that surfaces when the general counsel is brought to the table at this stage, or not brought to the table at all, is two-fold. First, if the investigation has been performed independently by an internal or external investigation team and not at the direction of counsel, the results of the investigation, both preliminary and final, will not be privileged. When the company is later sued by any number of external parties or investigated by

regulators, the initial reports will not enjoy the benefits of a privileged status and will be available for use by the company’s adversaries.

Second, the IT department may be aware of the system breach but choose not to investigate it either further or fully. Both decisions can leave the company exposed. Often, the IT department will remediate the discovered problem without further investigation to save time or resources, and often under the belief that this ‘band-aid’ remediation has cured the problem. Other times, the IT staff will take some additional investigatory steps and mistakenly believe they have fully ‘scoped’ the intrusion. In both situations, the company is left exposed, either because of a likely repeat offense or in terms of legal liability. (Note that state statutes can require a full investigation at the system compromise stage.) Hackers often leave a number of ‘back-doors’—rendering the system vulnerable to re-entry. Without a full and complete investigation that identifies and remediates the methods of entry, criminals are likely to return.

In sum, some cybercrime incidents—especially those that put sensitive data at risk—trigger legal obligations that require in-house counsel involvement. Counsel should be involved at the time the incident is detected, rather than after the compromise has been partially or fully investigated, to enjoy the full benefits of privilege that are important in any litigation and to ensure that a full and complete investigation occurs within the appropriate environment.

⁵ Md. Code §§ 14-3501 et seq.

Recent large-scale data breaches have cost companies well into the hundreds of millions of dollars.

Moreover, the importance of attaching privilege to cybercrime incidents involving sensitive data cannot be overstated. Cyber forensic investigations are messy. Until the investigation is over, the facts of how the compromise occurred, whether and how much data was taken out of the environment, and whether the cyber attack is ongoing are likely to be under constant flux. Lawsuits from customers, banks, regulators, and other third parties are frequent, if not expected. Protecting these investigative reports through privilege when litigation is anticipated can greatly assist the victim company in managing its litigation risk.

Cyber attacks can have catastrophic effects on a company

The third, and perhaps most obvious, reason why general counsel should care about cyber issues is that cyber intrusions expose companies to significant financial, legal, and reputational risks. Recent large-scale data breaches have cost companies well into the hundreds of millions of dollars in responding to the incident and resulting fines and litigation. Recent state-sponsored attacks have revealed the successful stealing of sensitive intellectual property from private companies. Lost laptops containing unencrypted health-related information have resulted in class action lawsuits and regulator enforcement actions. Losing data—even the risk of loss—poses significant financial and litigation risks for companies.

Less frequently reported are cyber incidents that put a company's own existence at risk. For example, system breaches that result in loss of business customer data for service providers, such as cloud providers and other Internet-related service providers, could be catastrophic. Often in these cases, one of the selling points of the service is the security of the provider's systems. Once these have been compromised, customers—especially business customers—may sever ties with the provider and choose a competitor.

While in-house counsel is often brought to the table when the cyber issue has resulted in some level of appreciable damage, it must ensure that it is in a proper position to advise the company about the ensuing risks throughout the process and not just when the catastrophe is imminent.

You have certain legal rights as a cybercrime victim

Finally, general counsel should be aware of their rights as cybercrime victims; this knowledge can assist them in the immediate aftermath of a computer incident. While the Computer Fraud and Abuse Act, (Title 18, United States Code, Section 1030) is well known for its use in prosecuting perpetrators of hacking crimes, a key civil provision was added in 1996 that affords certain rights to victims of computer intrusions. In particular, section (g) provides that an individual who suffers damage or loss as a result of a violation of the Act “may maintain

Common parlance in the cybercrime world creates a language barrier for general counsel—rendering them less likely to become informed.

a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.”⁶

The injunctive provisions of this section assist a victim in retrieving stolen data as the result of a system compromise and preventing its dissemination. For example, employers can use this section to obtain injunction relief against former employees who improperly access the employer’s computer system and gain access to information that may be used to compete against the employer.

If general counsel are not made aware of cyber incidents in their organization and at the appropriate time, however, they are unable to take advantage of the significant legal rights afforded to cybercrime victims.

Why are general counsel the last to find out?

It is not surprising that issues related to cybercrime remain hidden deep within the IT departments of organizations. Cybercrime concerns unauthorized access to networks and computers, and IT is about protecting these systems and networks. Cybercrime issues and investigations are highly technical. Technical phrases such as ‘zero-day,’ ‘malware,’ ‘sys admin rights,’ ‘stolen credentials,’ and ‘back doors,’ are common parlance in the cybercrime world and have little meaning to those other than IT security professionals. This creates a language barrier not often found, or as deeply entrenched, in other non-cyber investigations, such as more common fraud investigations. Because

of this language barrier, general counsel (and other C-level executives) are less likely to become informed about the nature and scope of cyber risks to their company than about other kinds of risks.

Just as the technical language barrier may impede lawyers from becoming fully informed of cyber risks, the IT staff often has its own reasons for not broadcasting the exposure it faces from cyber attacks. The purpose of IT professionals is to secure systems. A common, and at times accurate, inference of a successful cybercrime attack on a system is that someone within the IT department did not do his or her job right. Any cyber forensic investigator will confirm that working with the IT department in the aftermath of a breach is very tense, as staff is often fearful of losing their jobs. As a result, there is little incentive for those within the department to share with those external to the department any system compromise or data breach.

These factors—technical language barriers by lawyers and fear of job security from IT staff—create a set of impediments that ultimately leave in-house counsel far removed from the cyber scene of crime.

What are some practical tips for how general counsel can become appropriately involved in cybercrime matters?

General counsel can take certain steps to overcome these hurdles and to ensure they are involved in a proper and timely manner with these events, which carry such enormous risk for their companies.

⁶ 18 U.S.C. Section 1030(g).

1. Become informed about cyber issues. If generations that came of age without today's technological wizardry can learn email, instant messaging, and VOIP video conferencing, general counsels can become informed about cyber issues. Ask your IT staff for an introductory training session. Participate in any number of conferences with introductory sessions on cybersecurity and information technology for non-IT professionals. Get over the technical hurdle.
2. Understand the cyber trends in your industry. The second step in becoming informed is to learn about and understand the trends that affect your industry and your organization. Law enforcement, trade associations, security companies, and public-private sector sharing organizations are pushing out information about cyber attacks, issues, and risks. Key into the messages that are relevant to your industry and your organization.
3. Establish an information security council. Establish a multi-department council that brings together information technology and information security with legal, risk, and compliance. Hold monthly or quarterly meetings. Such a council will create an ongoing dialogue within your organization to discuss the threats facing your company and industry.
4. Establish an incident response plan and test it periodically. The first 48 hours after a compromise is detected is the critical period in determining whether your organization will weather the storm or go down in flames. An incident response plan is the first step in being prepared and responding appropriately. To be effective, these plans need to be tested on a periodic basis.
5. Establish clear guidance on what kinds of incidents need to be reported to legal and when. The IT staff needs clear instructions and an understanding of what kinds of incidents merit escalation and when. Without such guidance, general counsel risk the possibility that the IT staff will over report to them, which could desensitize general counsel to the risks. Lack of appropriate guidance can also lead to underreporting, which brings all of the attendant risks outlined earlier.
6. Review legal remedies available to cybercrime victims. Understand civil remedies that may be available to your organization and in what circumstances they apply. Injunctive relief needs to be applied for quickly. Know how to act fast and whom to contact.
7. Have a cyber forensic investigator on retainer. Cyber investigations require special skill and expertise. Having someone available to be on-site in 24-48 hours if needed can determine whether your organization is able to prevent sensitive targeted data from leaving your system.

Final thoughts

The impact of technological advancement is dramatic and far-reaching. Of course, much of this change is good for business, opening new doors, ventures, and opportunities. But through those doors can also tread hackers bent on criminal activity that can damage, perhaps even plunder, a business. For general counsel, that means involvement is critical to protecting the organization and its intellectual property from these significant threats.

No longer a matter exclusively for the IT department, cybercrime today requires that general counsel get to the scene of the crime early, remain involved continuously, and be prepared to act quickly in the event the company comes under one such silent, yet potentially catastrophic, attack. It's a pivotal role and one that leading general counsel will embrace to the betterment of the company, its employees, and its customers.

**To have a deeper conversation about how
this issue may impact your business,
please contact:**

Kimberly Peretti
Director
PwC
703 918 1500
kimberly.k.peretti@us.pwc.com

Shane Sims
Director
PwC
703 918 6219
shane.sims@us.pwc.com

Ed Gibson
Director
PwC
703 918 3550
ed.gibson@us.pwc.com

David Burg
Principal
PwC
703 918 1067
david.b.burg@us.pwc.com

About PwC

PwC global Forensic Services team of experienced professionals is dedicated to meeting the challenges caused by fraud allegations, financial crimes and other irregularities.