Bloomberg BNA

Corporate Law & Accountability Report™

Data Breaches

GCs Now 'Quarterbacks' of Cyber Incident Responses: John Reed Stark

Bloomberg BNA's Yin Wilczek recently posed questions to John Reed Stark, president of John Reed Stark Consulting LLC, a firm that advises clients on data breaches, cybersecurity, cybercrime and incident response. In the era of cyber events, Stark suggests that the general counsel now is the "most logical and effective quarterback" for data breach responses.

BLOOMBERG BNA: In the age of cyber breaches, how has the role of general counsel changed? What are some emerging/top concerns for general counsel (GC) with respect to cyber incidents?

John Reed Stark: The GC, alone or with outside counsel, has quietly emerged as the most logical and effective quarterback of data breach response.

Incident response workflow requires careful legal navigation because the legal ramifications of any failure can be calamitous or even fatal for any public or private company. So many incident response issues are critical to the very survival of a company, so the GC should lead investigative workflow, commanding the investigation and remediation for the C-suite and sharing with senior management the ultimate responsibility for key decisions. Just like any other independent and thorough investigation, the work relating to a cyber-attack will involve a team of lawyers with different skill sets and expertise (e.g. regulatory; e-discovery; data breach response; privacy; white-collar defense; litigation; law enforcement liaison; and the list goes on).

Virtually every aspect of an incident response is rife with delicate and complex legal issues. For instance, consider the dramatically competing constituencies during an incident response. On one hand, there are the FBI, Secret Service, U.S. Air Force Office of Special Investigations, and other law enforcement agencies who want to help find the intruders, and on the other hand, there are the myriad attorneys general and other state regulatory agencies who will be issuing requests and demanding answers about the safety of the personally identifiable information or so called "PII" of their respective citizenries. The GC should lead the creation of the rules, practices and procedures that govern the sharing of intelligence with government agencies.

In addition to the governmental investigations and litigation, the list of civil liabilities after a cyber-attack

John Reed Stark

John Reed Stark is president of John Reed Stark Consulting LLC. Before forming his own firm, Mr. Stark served for over five years as managing director (three as head of the Washington, D.C., office) of a global digital risk management firm, leading cybersecurity, incident response and digital compliance engagements for corporations and regulated entities. Before that, Mr. Stark served for 15 years as an SEC enforcement attorney leading cyber-related projects, investigations and a broad range of substantial and pioneering SEC enforcement actions, including 11 years as founder and chief of the SEC Office of Internet Enforcement. He also concurrently served for 15 years as an adjunct professor at Georgetown University Law School teaching a law and technology course and 10 years as a guest instructor teaching an annual law enforcement and technology in-service lecture at the FBI Academy. Read his blog on CybersecurityDocket.com entitled, *Stark on IR*.

is almost endless, including shareholder lawsuits for cybersecurity and data breach disclosure failures; declines in a company's stock price; and management negligence. There may also be consumer/customer driven class action lawsuits against companies falling victim to cyber-attacks, alleging a failure to adhere to cyber security ''best practices.''

Most importantly, with respect to cyber-attack investigations, attorney-client privilege will arguably apply to the work product from the digital forensic investigators hired by outside counsel. This is not done to hide information; rather it helps protect against inaccurate information getting released in an uncontrolled fashion and allows for more careful deliberation and preparation for litigation or government investigation/prosecution, two scenarios more and more likely nowadays. Along these lines, the digital forensics, malware reverse engineering, exfiltration analysis, logging review and the rest of the typical incident response workflow should all be done at the direction of counsel.

For instance, after a data breach, law enforcement agencies may request forensic images of impacted systems or may want to attach a recording appliance to a victim company's network in hope of capturing traces of attacker activity, should an attacker return to the company. These requests raise a host of legal issues, including whether providing information to law enforcement could violate the privacy of customers or result in a waiver of the attorney-client privilege.

Interestingly, law firms are only beginning to respond to the need for incident response by forming specialized data breach response legal practice groups. But my take is that the incident response practice area is where the Foreign Corrupt Practices Act was 10 or 15 years ago. In fact, I predict that in just a few years, data breach response practice groups of law firms will not only be a leading revenue generator for law firms but will be the leading growth area for large law firms as well.

BBNA: What can GCs do now to better tackle such incidents?

Stark: The best place for a GC to begin a review of a company's incident response capabilities is with a review of the company's cybersecurity policies and procedures. It is a good starting point to facilitate meaningful legal guidance relating to a company's cybersecurity risks and vulnerabilities.

First and foremost, cybersecurity is a business imperative, yet too often cybersecurity is too far down on a C-suite priority list—or because it is so complex, simply delegated to lower level technical personnel. There should be a commitment from the top down, both culturally and financially, to rigorous cybersecurity, and C-level accountability should be a part of the day-to-day business focus. The GC should review current reporting lines and assigned areas of responsibility to ensure they make sense. Given the responsibilities and accountability needed to execute an incident response plan, the right employees, possessing the appropriate skill sets, should be adequately empowered. One important check is to make sure that the individual charged with overseeing cyber-defense is not the same person who reports up the chain about breaches and who would oversee any response—it can create too much of a conflict. The best practice is to have an incident response group that is separate and apart from information technology infrastructure and reports to the GC—just like any other internal investigative group, an incident response team should have credibility and independence.

In cybersecurity, most companies allocate significant resources to fortifying their networks and to denying access to cyber-attackers. However, it is now a cliché, well founded in reality, that data breaches are inevitable. Along those lines, just like a fire evacuation plan for a building, a company should have a plan in place to respond to data breaches: an art form less about security science and more akin to incident response. Due to the absence of such a plan, many organizations unfortunately allow what could have been a relatively contained incident to become a major corporate catastrophe because they neither thought through all of the elements necessary for an effective response nor put the necessary mechanisms in place to ensure these elements were addressed in their plans.

Similarly, the critical importance of a business continuity plan in the event of a natural disaster is widely recognized and accepted. Yet, too often, such plans are not evaluated in the context of assessing cybersecurity risks. The GC may want to take ownership and ensure the properly interwoven connectivity of a company's incident response plan and disaster recovery plan.

Another area for the GC to check is whether incident response is competently staffed. Competition for talent in the information security space is intense, while the pressure on IT security senior executives is infinite and exhausting. Moreover, despite their rapidly rising salaries, turnover remains constant and there is a serious shortage of experienced and capable IT senior executives, especially chief information security officers. Relatedly, when a company loses key senior IT security personnel, it is not only a red flag but also an opportunity for a GC to examine succession plans and to obtain an unbiased, albeit possibly disgruntled, view of any cybersecurity flaws. The art and the benefit of the exit interview is lost on so many companies today—too often because departing employees are dismissed as resentful and unreliable. In the case of a resigning IT executive, a proper exit interview may reveal critical cybersecurity and incident response weaknesses.

The GC also needs to inquire whether the company is keeping up with cybersecurity threats. Not all companies face the same cybersecurity risks. There is no ''one size fits all'' approach. Companies that house and maintain large amounts of personal information and data need to tailor any defense, mitigation and response plans accordingly. By taking steps to ensure that information flow about data breaches within the industry and the latest intelligence about rising threats are considered by management on an ongoing basis, companies can stay current on the latest threats and prepare accordingly—preparedness is the key.

The GC may also want to review information technology and security budgeting with the chief financial officer. Most budgeting at companies is conducted annually and planned carefully and thoughtfully before execution—yet cybersecurity budgetary priorities can shift very quickly. Thus, a one-year budgetary cycle might not be swift or agile enough to manage rapidly emerging cyber-threats. Moreover, the average cost of a data breach continues to increase.

Also, the most significant cybersecurity vulnerability at any company will always be its employees. If employees do not adhere to cybersecurity rules and requirements, an attacker's exploit becomes all the more effective and capable of doing damage. GCs should take note of the frequency and efficacy of the firms' cyber-safety training programs. It is important to determine who participates in the training and how the company handles policy violations, especially violations by senior executives, whom studies have shown are typically the least compliant with cybersecurity policies.

BBNA: What are steps they can take to safeguard against future breaches?

Stark: There are five important areas that immediately come to mind. The first area is data mapping.

Every cyber-attack response begins with the simple notion of preservation, i.e. collecting and preserving, in a forensically sound and evidentiary unassailable manner, any ESI [electronically stored information], devices, logs, etc. that could become relevant to the cyber-attack.

Preservation is a critical workstream during a cyber-attack because incident responders will be scrutinizing every byte of data, including any fragments, artifacts or remnants left by the attacker in all sectors of any relevant device, including deleted recoverable files, unallocated and slack space or the boot sector. These artifacts can include: Internet addresses; computer names; malicious file names; system registry data; user account names; and network protocols.

Gathering the data and devices relating to a cyber-attack is the first and one of the most critical steps of an incident response. The most effective investigative methodology of a cyber-attack is one based on targeted incident response practices and does not solely rely on ''signature detection'' technologies, such as antivirus software. Rather, careful investigators employ an iterative process of digital forensics, malware reverse engineering, monitoring and scanning. As analysis of known or suspected compromised systems identifies new so-called Indicators of Compromise (IOCs), investigators will examine network traffic and logs, in addition to scanning hosts for these IOCs. When this effort discovers additional systems, those systems are forensically imaged and analyzed, and the process repeats. Armed with the information gathered during this phase of ''lather, rinse, repeat,'' a victim company can begin efforts to remediate the malware, rebuild compromised systems, reset compromised account credentials, block IP addresses and properly initiate network and host monitoring in an effort to detect additional attempts by the attacker to regain access.

Preservation is also critical because investigators will likely need to scour all ESI in search of PII. The search for PII is necessary to determine whether the attacker exfiltrated (removed from a corporate IT environment) any data containing personal information relating to any individuals, who may require notice of the cyber-attack, credit monitoring services and other remedial action. Finally, just about every cyber-attack response also involves the forensic imaging and reviewing of e-mails and other relevant communications from laptop computers, desktop computers, network servers, backup tapes, mobile devices, iPads and other systems.

Yet, preserving ESI after a cyber-attack can quickly become a challenging, costly and resource-intensive task. Most companies have ESI in so many locations (both physical and virtual) that, after a cyber-attack, it becomes an onerous struggle to locate and preserve relevant ESI and to piece together information about sometimes complex and disparate systems—all under the intense pressure of an active digital forensic investigation (with serious consequences for error or omission). Relatedly, it can sometimes take days after learning of a cyber-attack before a company realizes that it maintains an electronic purging process that deletes data (such as relevant logging information) on a regular schedule. Without having proactively made the effort to map information sources, assets and their key characteristics, these purging schedules can become unintended and latent causes of spoliation.

GCs should probe a company's data practices because where information relevant to identifying and describing potentially accessed/target/exfiltrated systems has never been data-mapped, establishing a strong and effective incident response plan for addressing cybersecurity risks can become challenging. Without any sort of responsible system overview or asset classification exercise, companies not only make mistakes in their cyber incident response plans, but companies can also make mistakes when applying available resources for security.

In addition, GCs should press to identify and understand the most critical pieces of company information. Otherwise, GCs become unnecessarily hamstrung during litigation and law enforcement/regulatory response. Mapping should make it faster and simpler for the GC to identify the company's most valuable intellectual property assets and consumer/customer-based informational assets, and how that data is currently being protected. Rapid access to, and a solid understanding of, the location of data assets can become critically important during a data breach response. For instance, whether data is maintained internally, at a third-party data center (in the U.S. or overseas), or in a cloud-based environment are all-important for a GC to appreciate first-hand. Asking these and other similar questions will help a GC better understand the company's posture with respect to securing its virtual assets and inform what additional steps, if any, management can take to improve such practices.

The second area is cyber insurance.

Just like with other hazards of doing business, today's public and private companies have begun taking into account cybersecurity concerns when considering overall enterprise risk management and insurance risk transfer mechanisms. Clearly, cyber insurance will eventually become yet another basic element of a company's insurance coverage, just like property insurance for companies and health insurance for individuals.

Interestingly, companies who maintain cyber insurance might also have the best cybersecurity policies and practices—probably because before obtaining cyber insurance coverage, a company is typically subjected to a fairly rigorous review by the proposed insurance company. Just like the physical exam typically required by insurance companies before issuing life insurance, which can prompt better personal wellness practices, a cyber insurance exam might trigger or prompt better corporate cybersecurity wellness.

A number of different types of insurance policies have the potential to be implicated in the event of a cyber-attack—or at least to be subject to a request for defense costs and/or indemnity. Factors depend on the nature of the breach, the relationship of the parties, the type of the information at issue (such as personal information, intellectual property, trade secrets, and e-mails), the precise form of the operative policy and, if related to third-party liability claims, the allegations asserted and the type of damages sought.

Yet while the market for cyber insurance continues to evolve and grow dramatically, there still has not materialized any form of standardized cyber insurance policy language, and whether standard property casualty provisions even cover losses relating to cyber incidents often remains an open question. Stand-alone cyber insurance policies offer broader coverage and should be explored by every GC, along with an evaluation of the sufficiency of the company's directors and officers liability insurance program.

But the question of how to design a stand-alone cyber insurance policy is a difficult one. The actuarial challenges of predicting/gauging both the probability and the impact of a cyber-attack can, in turn, make it difficult to match a cyber insurance policy with the unique risk profiles of today's global and technologically sophisticated companies; these are difficulties faced not only by insurance analysts but also by even the most experienced executive teams. Cyber-attack damages are so multifaceted and unique—much more so than fire, flood, health and other more traditional insurance scenarios and models—that there is no normal distribution of cyber-attack outcomes on which to base the probabilities of future effects. As a result, there are now a dizzying array of cyber insurance products in the marketplace, each with its own insurer-drafted terms and conditions, which can vary dramatically from insurer to insurer—some effective and comprehensive and others replete with loopholes, exclusions and other troubling features.

Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption and network damage. A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection. Many companies forego available policies, however, citing as rationales the perceived high cost of those policies, confusion about what they cover, and uncertainty that their organizations will suffer a cyber attack.

Traditionally, purchasing insurance coverage begins with a policy review, a risk breakdown and a range of other risk-related analytics. GCs should, however, make sure management also considers a different approach towards that calculus.

GCs should work with senior executives to review actual cyber-attacks, analyzing and scrutinizing the typical cyber-incident response workflow and so-called ''workstreams'' that follow most cyber-attacks. By analyzing and revisiting the realities and economics of these workstreams, a company can then collaborate with its insurance sales representatives and originators to allocate risk responsibly and determine, before any cyber-attack occurs, which workstream costs will trigger coverage; which workstream costs will be outside of coverage; and which workstream costs might be uninsurable.

It is also crucial that GCs conduct the necessary due diligence to be sure that the cyber insurance carrier their company uses has a good claims paying and claims handling history and has a proven history of rapid and supportive response. When a cyber attack occurs, too often there are doubts as to coverage, which can impact incident response.

Whatever the type of insurance held by a company, an insurance claim will undoubtedly follow, and insurance adjusters will scrutinize all invoices pertaining to all relevant workflows and will require briefings and documentation regarding all investigative efforts. For maximum objectivity, credibility and defensibility, rather than the company itself, the independent digital forensic firm investigating the breach—at the direction of counsel—should lead any briefings with insurance carriers.

As an aside, GCs should make sure that during any sort of data breach response, a professional on the incident response team, preferably counsel, will maintain carefully written documentation of all efforts of the response. This will help later on when gathering the ''documentation package'' to present to an inquisitive insurance adjuster when seeking an insurance reimbursement for the costs of the breach.

The third area is the implementation and installation of an Endpoint Detection and Response Tool.

Typically installed within an entire attack vector including domain controllers, database servers and user workstations, GCs should explore with information technology personnel the deployment of the real-time ''intelligence feeding'' of a so-called Endpoint Detection and Response (EDR) tool. EDR deployment will improve a company's ability to detect and respond to outsider and insider threats; enhance its speed and flexibility to contain any future attack or anomaly; and help a company manage data threats more effectively overall. EDRs will also boost the swiftness and precision of a GC's regulatory response workflow.

The fourth area is physical security.

Contrary to many popular notions of cyber-attacks, cyber-attacks can sometimes begin with a physical breach. For instance, when an outsider attempts to surreptitiously gather fodder for a social engineering scheme (such as a spearfishing campaign), or when an insider (such as a so-called ''bad leaver'') gains access to a company's network and wreaks havoc, without initially using malware or other clandestine technological means.

Hence, GCs should understand the physical security of facilities, including management's plans for reception and entry checkpoints; ID scanner and other access records; video or still footage; physical logs; and even elevator and garage records.

The fifth and final area is that the GC cannot respond to an incident without a lot of specialized help.

When a company experiences a cyber-attack, the company will likely need to hire an expert and experienced digital forensics/data breach response firm to investigate for several reasons. First, very few companies employ the kind of personnel who have the technological expertise to understand and remediate today's cyber-attacks. Second, like any company in a crisis, engaging an independent and objective investigator not only insures integrity in the response but also creates a defensible record if challenged later on (e.g. by regulators, class action lawyers, partners, customers, etc.). Finally, as I mentioned earlier, if the digital forensics/data breach response firm is engaged by outside counsel, a company can (arguably) maintain and secure the attorney-client privilege for the reports and other investigative documents pertaining to the attack.

Given the scarce number of firms who can truly investigate a cyber-attack, especially those with malware reverse engineering expertise, it makes sense to search for a firm before experiencing a cyber-attack.

A quick side note on malware: GCs should realize the term ''malware'' is often misunderstood. The term ''malware'' is often defined as software designed to interfere with a computer's normal functioning, such as viruses (which can wreak havoc on a system by deleting files or directory information); spyware (which can gather data from a user's system without the user knowing it.); worms (which can replicate themselves in order to spread to other computers—unlike a computer virus, a worm does not need to attach itself to an existing program); or Trojan horses (which are non-self-replicating programs containing malicious code that, when executed, can carry out an attacker's actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm).

However, the definition of malware is actually far broader. In the context of a cyber-attack, malware means any sort of program or file that is used by attackers to infiltrate a computer system. Like the screwdriver a burglar uses to gain unlawful entry into a company's headquarters, legitimate software can actually be malware. For example, during an ''Advanced Persistent Threat'' or ''APT'' attack, attackers will often use ''RAR'' files as containers for transporting exfiltrated information, yet RAR files have a broad range of legitimate uses and can be used in the context of general corporate activities.

Thus, reverse engineering malware, which can be hiding in plain sight, is both an art and a science. Forensic investigators, incident responders, security engineers, and IT administrators employ a broad range of practical skills to examine malicious programs that target, access and infect corporate computer systems. Understanding the capabilities of malware is not only critical for responding to information security incidents, but it is also critical to an organization's ability to derive threat intelligence and to fortify defenses.

Yet, malware reverse engineering is costly, with hourly rates more akin to a law firm partner's rather than information technology specialists. Even finding a specialist with reverse malware engineering skills can quickly become a challenge—educational institutions are only just beginning to graduate individuals with malware skills and most malware specialists are self-taught or are ''home-grown'' within digital forensic firms. Thus, GCs should bear in mind that without a competent digital forensics firm, staffed with digital forensic examiners who are skilled at malware reverse-engineering, its executives may end up feeling like a homeowner with a rapidly flooding basement—yet no plumber to help find the leak and plug it up.

BBNA: What are some GC best practices in incident response investigations?

Stark: For starters, the first cardinal rule of incident response is to communicate openly and with transparency to victims. Even if a company does not have the answers, which at an early stage of an incident response is actually quite typical, companies need to keep communication lines friendly, consistent, frequent, responsive, considerate and wide open.

Like every data breach response, at the outset there are far more questions than answers and circumstances can change dramatically at any time. Being victimized is a scary thing for people, and when data breach victims are not treated honestly, thoughtfully and openly, and communication is poor, inconsistent and robotic, the frustration of victims multiplies exponentially.

Every data breach impacts multiple constituencies—customers, partners, employees, vendors, regulators—and every one of those constituencies wants and deserves answers. What can often be even worse than a data breach itself, is the failure to respond in an appropriate manner, which includes reaching out thoughtfully and openly to possible victims.

Next, be mindful of whom to blame. When my eight-year-old daughter comes home from school with a bad cold, I don't blame my daughter. I don't blame her teacher. I don't blame her school. Why? Because protecting my daughter from a cold during the school year is simply not possible and I am not so arrogant as to think I can do the impossible. The same goes for data breaches.

Every entity on this planet, government or private sector, can experience a data breach at any time (and probably already has). Data breaches don't define victim companies—how they respond to data breaches does. GCs should guide their company executives by preaching this kind of realism, rather than the fantasy of ironclad security.

Finally, GCs should approach data breaches like any other internal investigation—mandating the same notions of independence, neutrality and impartiality. For maximum objectivity, credibility and defensibility, rather than the company itself, the independent digital forensic firm investigating the breach, at the direction of counsel, can even lead any briefings with constituencies (including board members, customers, vendors, employees, partners, media, etc.).

BBNA: Are there other issues GCs should be aware of stemming from a cyber incident?

Stark: One over-arching issue is that the role of the GC after a data breach is a challenging one because, unfortunately, the public's view of cyber-attack victims is less about understanding and sympathy, and more about anger and vilification.

Given in particular the 47 or so separate state privacy regulatory regimes, together with a growing range of federal agency jurisdiction, instead of accepting a helping hand, cyber-attack victims are accepting service of process of multiple subpoenas. The world of incident response is an upside-down one: Rather than being treated like criminal victims, companies experiencing data breaches are often treated like criminals themselves, becoming defendants in federal and state enforcement actions, class actions and other proceedings.

Formerly looked upon as the problem of the IT director, cybersecurity has quickly evolved into a GC issue and responsibility, which the GC needs to understand and oversee. In the aftermath of a corporate cyber-attack, GCs and the companies they govern are subjected to immediate public scrutiny and, in many cases, unwarranted criticism.

But cybersecurity engagement for GCs does not mean that they should obtain computer science degrees or personally supervise firewall implementation and intrusion detection system rollouts. GCs can lead incident responses first by becoming actively involved in ensuring the organizations they counsel are not only adequately addressing cybersecurity, but are also engaging in careful, thoughtful, independent and systematic incident response. Second, and most importantly, by approaching the subject in much the same way they approach other areas of risk under their purview: with vigorous, skeptical, intelligent and methodical inquiry.

ISSN 2330-6300