COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

Transforming the Cyber-Security Paradigm

By John Reed Stark
Compliance Week Columnist

When my daughter comes home from school with a cold, it is not her fault. No one can protect her from catching a cold; they are inevitable. The same goes for data breaches.

Every company can experience a data breach—and probably already has! That is why companies need to shift cyber-security practices away from prevention and detection and into a paradigm of incident response. Traditional data breach protections do not detect quickly enough, or act nimbly enough, to counter today's sophisticated and clandestine data breaches.

John Reed Stark
Columnist

Yet, so many companies remain unwilling to recalibrate cyber-security into a more effective archetype of response. Why?

David Fontaine, CEO of Corporate Risk Holdings (parent company of Kroll) believes that because cyber-security threats have suddenly become so complex, sophisticated, and transnational, companies are struggling to stay current. Fontaine notes, "When a data breach hits the headlines, there is an instinctive reaction that somebody screwed up and left a door unlocked. This only further fuels the fire that breached companies must redouble fortification and detection. That might be true, but the reality is that companies, above all else, should pivot their attention and focus to data breach response."

In other words, when companies trying to prevent data breaches rely too much upon customary protections of intrusion detection and firewalls, they are just as misguided as parents trying to prevent their kids from catching colds by relying upon hand-washing and multiple clothing layers. The smarter method for combating data breaches (like colds) is to focus efforts and preparation on how to contain, treat, and cure the problem, as fast and as painlessly as possible. Company executives should preach this realism, rather than the fantasy of ironclad security.

Welcome to the new paradigm of cyber-security: where technological infrastructure has expanded dramatically; where data-points reside on multiple platforms (including employee devices, vendor networks, and the cloud); and where data breaches don't define victim companies; how companies respond to them does.

Of course, traditional cyber-security measures such as periodic risk assessments; antivirus, software patching, encryption, and a manifold response plan are important cyber-security measures. But everyone knows that already. Let's focus on what everyone does not already know.

Ever Heard of EDRs?

Recently, a wave of dedicated incident response solutions known as "endpoint detection and response" or "EDR" tools have come into being. Typically installed within a swath of IT equipment including domain controllers, database servers, and workstations, the real-time "intelligence feeding" of EDR tools will likely become a corporate cyber-security standard.

For instance, most internal investigations kick off with manual data acquisition, file-system forensics, and log file analysis on data aggregated and collected after the suspected breach. By providing continuous monitoring and recording of activity on endpoints and servers, EDR tools reduce the need for such after-the-fact data collections. EDR tools decrease the cost, complexity, and time of internal investigations and regulatory response, while simultaneously accelerating the identification of root causes and attack vectors of data breaches.

EDR technologies also provide a richer depth of behavior-based anomaly recognition and better visibility into threats of all varieties, not just malware. For example, by providing instant aggregate threat information and decreasing the "dwell time" of targeted attacks, EDR solutions enhance enterprise visibility and help counter internal threats and malfeasance.

An 'Incident Response' Approach to Cyber-Insurance

Companies should better incorporate data breach response when considering enterprise risk management such as insurance transfer mechanisms. Traditionally, purchasing insurance coverage begins with a policy review, a risk breakdown, and a range of other risk-related analytics. Purchasing cyber-insurance is much different, however, because no standard policies exist and the cyber-insurance market remains in its infancy, leading many companies to forego available policies and rely upon their more traditional policies of general liability and property. This is backwards thinking.

Instead, management should undertake an approach towards its insurance calculus based more upon data breach response, identifying insurance gaps before procurement. How? By analyzing the typical cyber-incident response workflow that would follow a cyber-attack (digital forensic analysis; data exfiltration review; litigation; regulatory response; customer notification and credit monitoring; law enforcement liaison; remediation; and so forth). By analyzing the realities and economics of data breach response workflow, a company can then collaborate with its insurance agents and originators to allocate risk appropriately and determine, before any cyber-attack occurs, which workflow tasks will trigger coverage; which will fall outside of coverage; and which might be uninsurable.

> Conventional cyber-security fortification and defense measures need to make way for EDRs; otherwise companies risk a sluggish, incomplete and piecemeal data breach investigation.

Time to Spin Off Incident Response

When the same employee charged with overseeing cyber-defense also oversees data breach response, a conflict of interest inevitably arises. A cyber-security para-

Reprinted from Compliance Week, November 2015

digm premised upon incident response segregates incident response from cyber-security, because a more independent investigative team is going to be far more reliable than a cyber-security team who may ultimately bare blame for the breach.

Like any internal investigation, the most important aspect of data breach investigations is independence. Independence lends credibility, objectivity, and integrity to a result while also creating a defensible record if challenged later on (by regulators, class action lawyers, partners, customers, and so forth).

Counsel as Quarterback

Rather than the typical corporate reporting scheme, where data breach response personnel report to the COO, CIO, or CISO, the incident response team should instead report to the general counsel.

Malware reverse engineering results, exfiltration analysis, logging review, digital forensics exploration and the rest should all be cloaked with the protections of attorney-client privilege and work product. This is not done to hide information; rather the privilege helps protect against releasing inaccurate information in an uncontrolled fashion and allows for more careful preparation for litigation or government investigation, two scenarios more and more likely nowadays.

Moreover, every aspect of an incident response is rife with complex legal issues. For instance, consider the many competing constituencies during an incident response. On one hand, there might be FBI, Secret Service, U.S. Air Force, and other law enforcement agencies trying to lock up the intruders. On the other hand, there are myriad attorneys general and other regulatory agencies issuing requests and demanding answers about the safety of the personal information of their respective citizenries.

Also, law enforcement agencies may request forensic images of impacted systems, or may ask to attach a recording appliance to a victim company's network in hope of capturing traces of possible future attacker activity. These requests raise a host of legal issues, including whether providing information to law enforcement could violate customer privacy or inadvertently waive the attorney-client privilege.

Finally, in addition to the governmental investigations and litigation, the list of civil liabilities after a cyber-attack is almost endless, including shareholder lawsuits for cyber-security and data breach disclosure failures; declines in a company's stock price; and management negligence as well as customer-driven class-action lawsuits alleging failures to adhere to cyber-security "best practices."

Given that the legal ramifications of data breach response failure can be calamitous or even fatal, the response side of the cyber-security paradigm should shift. This same model already applies when investigating corruption, bribery, and other criminal behavior, where the GC, not the COO, CISO, or CIO, quarterbacks investigative workflow; superintends remedial efforts; and governs intelligence sharing. An independent data breach SWAT team, under the direction of the GC, also reduces the scraps that can arise between compliance, operations and legal, especially relating to the GC's disclosure obligations, including disclosures to shareholders (via the SEC), the states and law enforcement.

A Necessary Paradigm Shift

Today's cyber-security paradigm needs to shift dramatically. Conventional cyber-security fortification and defense measures need to make way for EDRs; otherwise companies risk a sluggish, incomplete and piecemeal data breach investigation. Customized cyber-insurance policies, created by way of a reverse gap analysis, need to supplement general liability and property insurance coverage; otherwise, companies risk financial peril, even bankruptcy. And cyber-security departments need to reorganize data breach response under the purview of the GC; otherwise, given the post-data breach rush to the courthouse, companies risk a liability implosion.

In short, today's companies need to get with the virtual program. Philosophies of prevention and detection are no longer the master ethos of strong cyber-security. Doctrines of defend and respond have taken their place. ■

John Reed Stark is president of John Reed Stark Consulting, a firm that advises companies and corporate boards on data breach response, cyber-security and digital compliance. Stark's experience with data breaches touches upon all aspects of cyber-incident response, especially during early phases of crisis management, and forensic analysis.

Stark's lengthy career includes: almost 20 years with the SEC's Division of Enforcement; over five years as managing director of an international cyber-security and data breach response firm; and an early stint as special assistant U.S. attorney in Washington, D.C.

Stark also served as adjunct professor at Georgetown University Law School where he taught a course on cyber-crime for 15 years. He has given numerous lectures on cyber-crime at the FBI Academy in Quantico and has authored several articles on law and technology.

He can be reached at john.reedstark@complianceweek.com.