EDWARDS WILDMAN

CLIENT ADVISORY

edwardswildman.com

January 2014

An Edwards Wildman Privacy & Data Protection Client Advisory

Every Company is a Potential "Target" of a Breach: What is a Company to do?

By: Theodore P. Augustinos and Mark E. Schreiber

Recent events involving widely-publicized data breaches, at respected retailers with significant resources to address information privacy and security challenges, are a wake-up call for any business. If such prominent organizations are under attack and have difficulty protecting the security of their customer's information, what can any businesses do? Here are four suggestions.

1. Re-Arm against Threats

   First, we must keep in mind that the complete story of these recent events has not yet been written. Highly sophisticated attacks have, in prior events, overcome some of the state-of-the art safeguards, and the countermeasures, forensic expert tell us, are not yet entirely up to the task. Nevertheless, recent research on data security incidents teaches us that most breaches involve some basic failure or simple mistake. According to one industry study, 97% of reported malicious data breaches were avoidable. In addition to the big breaches in the news, the Massachusetts Office of Consumer Affairs and Business Regulations reported a record number of reported breaches in 2013, up 30% from the prior record in 2012, according to the Boston Business Journal.

   Current events may be a good reminder to re-arm against potential threats: re-visit technical and administrative safeguards, and re-educate, re-train and re-sensitize personnel.

   A new "Cyber Streetwise" cyber security website was launched last week by the UK government to assist business in protecting against data breaches, and free materials are available at the FTC. Both sites are worth reviewing. The UK site includes basic advice to businesses and individuals, including tips on IT security password management, wireless networking, online banking and website security.

   Companies should certainly take this opportunity to review the well known and publicized data security basics: maintain and check firewalls; enable logging on all servers; back up log files; encrypt portable devices, other media and backups; control the ability to download and export data; and segregate and compartmentalize sensitive databases. While DNS queries, Domain Generation Algorithms, and so-called "Magic Packets" may be beyond many executives' common vocabulary, the IT departments of most companies will grasp these terms. As threats develop, so do defenses, and the next generation of anti-malware techniques and software is now becoming available. Companies should continually explore available improvements and upgrades to security systems to implement and maintain the appropriate level of defenses against an attack. Many forensic consultants offer frequent, excellent and free webinars on data security issues to help monitor recent developments, techniques and resources for defending against cyber-attacks and other data security risks.

2. Address Vendor Relationships

   Another message of the recent events may be that vendor management should be on the front lines of every company's defense against data breaches. Industry studies identify vendors as a source of perhaps a third or more of data breaches and thus a vulnerability for

many companies. Vendor relationships, including those with data and payment processors; records management and storage facilities; legal, accounting and other professional services firms; and other relationships, must be carefully scrutinized for their compliance profile, capabilities and culture in order to maintain adequate defenses against a potential attack through those avenues. Companies should view third parties that touch their personal data as potential sources of vulnerability for a breach. Due diligence on vendor engagements is critical, and vendor contacts must incorporate appropriate contractual protections, representations, warrantees and indemnifications, as well as audit and reporting rights. After engagement, vendors should be monitored and revisited, and audited as appropriate, just as each company should continually monitor and revisit its own security apparatus and protocols to insure that security is keeping up with evolving business needs, uses of information, and the relevant threat environment.

3. Review Response Plan

   This is also a good time for companies to review incident response protocols, make sure the response team is in place, and consider testing the breach or crisis management workings in a "tabletop" or mock breach scenario. It is usually helpful for IT personnel to work with forensics teams in advance to establish procedures for responding to particular threats, in order to improve the possibility of immediate identification, prompt remediation, and investigation of the effect and scope of the incident. Legal, public relations and other internal and external resources should be well prepared to address the various, and sometimes conflicting, compliance obligations that are usually triggered by a data security incident, including the timing and content requirements for notifications.

4. Anticipate an Incident

   As we know with breach incidents, it's not a matter of if, but when. Realistic simulations and drills incorporating unexpected data and factual scenarios, as noted, are a useful way to assess your company's readiness, even if you have been fortunate to avoid a recent, actual incident. Make sure your standby response team is on red alert, with adequate resources, decision making, capability and preparedness to respond to an incident as promptly and accurately as possible. Review available resources, many of which are free, to stay current on legal and regulatory compliance in all applicable jurisdictions, including a global data breach guide published by the World Law Group. Frank, ongoing discussions with privacy and IT security personnel, C-Suite executives and even boards of directors will help improve the company's information security profile and increase its chances against these persistent and growing cyberthreats.

For more information, please contact the authors of this advisory Theodore P. Augustinos, Partner, +1 860 541 7710, taugustinos@edwardswildman.com, Mark E. Schreiber, Partner, +1 617 239 0585, mschreiber@edwardswildman.com or one of the attorneys listed below:

Mark E. Schreiber, Partner, Chair, Privacy and Data Protection Group Steering Committee	+1 617 239 0585	Boston	mschreiber@edwardswildman.com
Theodore P. Augustinos, Partner, Steering Committee, Privacy and Data Protection Group	+1 860 541 7710	Hartford	taugustinos@edwardswildman.com
Laurie A. Kamaiko, Partner, Steering Committee, Privacy and Data Protection Group	+1 212 912 2768	New York	lkamaiko@edwardswildman.com
Barry J. Bendes, Partner	+1 212 912 2911	New York	bbendes@edwardswildman.com
Michael P. Bennett, Partner	+1 312 201 2679	Chicago	mbennett@edwardswildman.com
Nicholas Bolter, Partner	+44 (0) 20 7556 4380	London	nbolter@edwardswildman.com
Kenneth Choy, Partner	+852 2116 6653	Hong Kong	kchoy@edwardswildman.com
Mark Deem, Partner	+44 (0) 20 7556 4425	London	mdeem@edwardswildman.com
Ben Goodger, Partner	+44 (0) 20 7556 4188	London	bgoodger@edwardswildman.com
Edwin M. Larkin, Partner	+1 212 912 2762	New York	elarkin@edwardswildman.com
Sarah Pearce, Partner	+44 (0) 20 7556 4503	London	spearce@edwardswildman.com
Ronie M. Schmelz, Partner	+1 310 860 8708	Los Angeles	rschmelz@edwardswildman.com
Stephen M. Prignano, Partner	+1 401 276 6670	Providence	sprignano@edwardswildman.com
Thomas J. Smedinghoff, Partner	+1 312 201 2021	Chicago	tsmedinghoff@edwardswildman.com
David S. Szabo, Partner	+1 617 239 0414	Boston	dszabo@edwardswildman.com
David L. Anderson, Counsel	+1 310 860 8710	Los Angeles	danderson@edwardswildman.com
Patrick J. Concannon, Counsel	+1 617 239 0419	Boston	pconcannon@edwardswildman.com
Karen L Booth, Associate	+1 860 541 7714	Hartford	kbooth@edwardswildman.com
Jonny McDonald, Associate	+44 (0) 20 7556 4620	London	jmcdonald@edwardswildman.com
Ari Moskowitz, Associate	+1 202 939 7934	Washington, D.C.	amoskowitz@edwardswildman.com
Matthew Murphy, Associate	+1 401 276 6497	Providence	mmurphy@edwardswildman.com
Patrick Peng, Associate	+852 3150 1936	Hong Knon	ppeng@edwardswildman.com
Erin Pfaff, Associate	+1 310 860 8717	Los Angeles	epfaff@edwardswildman.com
Nicholas Secara	+1 212 912 2785	New York	nsecara@edwardswildman.com
Ajita Shah, Associate	+44 (0) 20 7556 4385	London	ashah@edwardswildman.com
Nora A Valenza-Frost, Associate	+1 212 912 2763	New York	nvalenza-frost@edwardswildman.com

EDWARDS WILDMAN