

STROZ FRIEDBERG

DIGITAL RISK MANAGEMENT & INVESTIGATIONS

ERIN NEALY COX*

Executive Managing Director & Deputy General Counsel

Tel: 214.377.4556 | enealycox@strozfriedberg.com

RACHEL WOMACK, Vice President

Tel: 214.377.4554 | rwomack@strozfriedberg.com

Proud to be Recognized as a Dallas
2011 Texas' Best

★ Computer Forensics Firm

★ Individual Expert Witness*

★ Data Security/Recovery Provider

★ E-Discovery Company - National

CYBERCRIME & DATA BREACH— THE EQUAL OPPORTUNITY ENEMY

Every industry is taking heed of the surge in cybercrime and unrelenting reports of data breaches. A leading risk management practice is to operate under the assumption that a breach can happen, and more than likely, will happen to your organization. To that end, cybersecurity efforts must also shift from prevention tactics alone to robust detection capabilities. Having a ready-to-execute DATA BREACH PREPAREDNESS PLAN is essential to minimizing potential reputational and financial havoc of a cyber intrusion. As a helpful guide, the following high-level checklist addresses 33 tips over 3 phases of a breach.

1. Preparedness Plan

□ Create your data breach response plan and team. □ Define team roles and responsibilities. □ Outline steps necessary in the first 72 hours. □ Establish clear action-items and checklists to keep parties focused. □ Train staff to identify and report breaches. □ Consult security experts to audit and review your current security assessment. □ Examine third parties' security protocols. □ Track fast-changing data breach laws, privacy rules and notification mandates. □ Encrypt sensitive data. □ Map locations of critical data. □ Restrict access to information on a "need to know" basis. □ Review employee lists and purge old user accounts. □ Follow a data retention policy with a plan to destroy or dispose of unneeded data. □ Identify and secure computer systems from vulnerabilities like common attack vectors. □ Implement appropriate electronic and physical security.

2. Incident Response Plan

□ Seek expert forensic advice on the nature and scale of the incident. □ Change encryption keys and passwords immediately. □ Ensure data is no longer being compromised. □ Secure all data and systems. □ Isolate and preserve compromised data. □ Leave the computers' power on; disconnect from the networks if possible. □ Identify types of compromised data, affected parties and scope of the breach. □ Attempt to retrieve or neutralize compromised data. □ Identify the time frame for who needs to be contacted and how. □ Adhere to regulatory notification mandates and coinciding timeframes. □ Document your work. □ Determine when the clock starts ticking for potential notification rules. □ Consider notifying law enforcement, if you suspect criminal activity.

3. Post Assessment & Action Plan

□ Assess gaps and evaluate effectiveness of plans, procedures and staff training. □ Adjust security and response plans and processes; communicate and train accordingly. □ Stay current; test your plan often and remain aware of changing threats and laws. □ Maintain a breach report in accordance with regulatory standards. □ Continue to restore customer relations; monitor crisis communications and if applicable, track effectiveness of identity fraud monitoring vendors.