Published on *The National Law Review* https://natlawreview.com

Data Breach Preparedness: A Critical Risk Management Priority for Small and Mid-Sized Businesses

Article By:

Joseph J. Lazzarotti

After hearing a lot lately about big companies suffering data breaches, it is important to remember that, according to inc.com, half of all cyberattacks target small to mid-sized businesses (SMBs). Based on a 2016 State of SMB Cybersecurity Report, CNBC reported that in the prior 12 months half of all SMBs in the U.S. had been hacked. This makes sense when one considers FBI reporting (pdf) that an average of 4,000 ransomware attacks happen every day in the U.S., as observed in statements from SEC Commissioner Luis A. Aguilar, who in October 2015 said that:

> *Cybersecurity is clearly a concern that the entire business community shares, but it represents an especially pernicious threat to smaller businesses. The reason is simple: Small and midsize businesses are not just targets of cybercrime; they are its principal target.*

Clearly, SMBs need to address this significant risk to their businesses. Strong IT safeguards are part of the solution, but not a silver bullet. Administrative and physical safeguards also are needed, such as access management policies, awareness training, equipment inventory, and vendor assessment and management programs. But even the best safeguards cannot prevent all breaches. Thus, SMBs need to be prepared for responding to the inevitable – that they will experience a data breach of some kind. Below are three key steps SMBs should take to improve their level of breach response preparedness.

Understand your risks and vulnerabilities

- Not all SMBs are created equal, at least with respect to inherent business risk of a cyber breach. Factors such as the type of business, jurisdictions in which business is conducted, and the amount and nature of the personal information involved in the business (payment card data, health data, SSNs, etc.) drive this risk.

- Core competencies may be lacking. That is, members of the organization's IT staff may be very adept at systems management, but significantly lacking when it comes to the latest

cybersecurity tools and attack methodologies to provide competent leadership and execution.

Develop and practice an “Incident Response Plan”

- Identify the internal team (*e.g.,* leadership, IT, in-house counsel, and HR). These are the persons in the business who will direct the response to the incident. They will need to make quick, informed and prudent decisions that likely will be critical to the success of the response process, and possibly the future of the business.

- Identify the external team (*e.g.,* outside legal counsel, forensic investigator, and public relations). Having external members of the team identified ahead of time can be vital to the success of any preparedness plan. When a breach happens, valuable time can be lost trying to identify, evaluate, and engage third-party service providers necessary for the response.

- Take into account all legal and contractual obligations that may affect the response process.

- Clarify the roles and responsibilities of the team members at key points in the response process – discovering the incident, investigation, coordination with law enforcement, remediation, notification, third party inquiries, compliance, and reevaluation. This should include a well-defined decision making process to facilitate good choices and avoid delays.

- Practice, practice, practice. It is likely that members added to the response team do not have first-hand experience with helping to coordinate a breach response. And, even a well-drafted plan does not give persons charged with implementing the plan a feel for what is involved. Once an SMB creates its plan, it should gather its internal and external breach response team members to simulate a breach in action in order to help members gain valuable experience with navigating the issues in a breach response, as well as working with each other.

Create awareness throughout the organization.

- Educate employees on how to recognize attacks and other forms of data breach.

- Instruct employees on what to do immediately if they believe an attack has occurred (*e.g.,* who to notify IT, how to disconnect from the network).

- Instruct employees on what *not* to do (*e.g.,* deleting system files, attempting to restore the system to an earlier date).

All breach notification laws mandate that notification, if required, must be made without unreasonable delay. In some cases, notification can be required in as few as 15 days or even 72 hours. Thus, in all cases, SMBs have to act fast, sometimes very fast, making decisions that can have significant reputational implications for the business, as well as shape compliance and legal risks. Preparedness can make all the difference in the success of an SMB’s response to a data breach.

National Law Review, Volumess VII, Number 257