WWBA news
Westchester Women's Bar Association
SEPTEMBER 2016
www.wwbany.org

# CYBERSECURITY FOR THE SMALL TO MEDIUM ENTERPRISE
## How to be Safe Without Going Broke

*Kenneth C. Citarella and Elizabeth M. Barnhard*

The stories occur every day and only get less encouraging. The computer networks of the world's largest, most sophisticated organizations are penetrated and corporate secrets or the personally identifying information of an enormous number of individuals get exposed. If international banks with seemingly limitless resources cannot protect themselves, what can the small to medium-sized organization be expected to do? You can help your clients reduce the potential damage to their businesses from data breaches.

Although it is true that there are some intruders that cannot be kept out, there is a great deal every entity can do to improve its cybersecurity without incurring great expense. First, of course, the decision must be made to improve cybersecurity. Without that basic commitment, nothing will happen. With it, a client can rationally decide what to do to minimize risk and manage costs. Since it is a matter of when, not if, a client's computer network will be penetrated, it is in a client's best interest to decide to improve cybersecurity.

First, the client must thoroughly understand what they do and how they do it. This is more difficult than it sounds for many smaller organizations. Emphasis is often on growth, service, profit or other parameters that measure the organization's success. There is often little managerial awareness of the sensitivity of the data collected, who has access to it, and how it is stored and processed. With the public's concern about security of personal information and the expanding patchwork of federal, state and local laws governing data security, small and medium-sized organizations ignore cybersecurity at their peril.

Suppose you represent a typical web-based start-up. The owners had a good idea for a niche business, enroll new customers online and over the phone, and make monthly charges against customer credit cards. Where is all this data? In one computer? In more than one? In notebooks or smartphones also? Who is in charge of collecting and organizing the data? Who deletes the records of former customers and when? These same questions exist for charitable organizations with regard to their donors. The security of none of these processes can be improved unless what actually happens is well understood first.

During the January to April tax season, W-2 Form scams abound. Typically, the scammer will send an email to someone in the payroll department that resembles, or "spoofs", the legitimate email address of a senior executive, and asks for copies of the W-2s of all employees. The domain name in the email address is usually off by just one letter that the reader's eye can easily overlook. For example, instead of johnsmith@reliablebusiness.com, it is johnsmith@reliablebusness.com. The employee responds to the email and everyone's personally identifying information is sent to the identity thief.

These two seemingly divergent examples make a common point. Cybersecurity and data breach prevention are not just issues of technology; human behavior plays a very significant role. Fortunately, the importance of human behavior also provides the opportunity for simple and inexpensive controls that can make a huge difference.

***"Although it is true that there are some intruders that cannot be kept out, there is a great deal every entity can do to improve its cybersecurity without incurring great expense."***

There is one guiding principle that must be accepted by clients seeking to improve their data security, regardless of their size or business operations complexity. Security is always inconvenient. But better to be inconvenienced than suffer permanent business damage from a data breach.

# CYBERSECURITY FOR THE SMALL TO MEDIUM ENTERPRISE
## How to be Safe Without Going Broke

Data security improvements must address both technological and human features. Neither can be sufficient on its own. Here are some quick and easy suggestions for clients (and law firms alike):

- Identify sensitive data: customer information, employee information, financial accounts, etc. Concentrate this information in as restrictive an environment as possible. Limit access only to those personnel who must have it.

- Identify all third party vendors, including Cloud vendors, who handle the client's data. Be sure the client always understands it owns the data and remains responsible for it. Inquire about the vendor's data security practices. Just letting the vendor know the client is concerned can make a big difference. Be sure the contract addresses responsibility for a data breach occurring at the vendor.

- Look for simple steps that can improve the security of a transaction. For example, never hit "Reply" to an email that provides instructions from a customer concerning sensitive data. Respond to the email by using the forwarding feature. This requires affirmatively typing in the customer's email address. This simple step will keep a client from falling prey to an email which spoofs a customer's email and which can result in a loss of customer data or funds. Any request that appears to come from a CEO or other supervisor that asks for sensitive data should be treated in the same manner. Typing the email address of the real CEO, for example, can prevent W-2s from heading out to parts unknown.

- Some industries, particularly small to medium size financial services firms, should use email "whitelist" practices. Most organizations, just like individuals, use a "blacklist" practice. This means all incoming emails are accepted until the user decides to block them as spam or other unwanted material; hence, a blacklist of rejecting domain names. A whitelist is the exact opposite. All emails are rejected, or at least quarantined for closer review, unless they are on a pre-approved list of acceptable domain names. This is another excellent way for a client to defend against spoof attacks.

- Make sure the client's firewall and anti-malware are up to date. If the client has any type of network, they probably have an IT vendor who monitors such matters for them. Be sure they are doing their job. If the client's IT department is really just a few separate computers which only share data via email or an internet service like Dropbox, each device must have current anti-malware and an up to date operating system. All preferences must be set for automatic updating.

- Consider bringing in an outside security vendor for a review of the client's practices. Counsel should contract the security vendor, so that privilege applies. Discuss ahead of time precisely what the security vendor should look at, how much time will be expended, the deliverables and the cost. No client likes to spend money pre-emptively, but even just a few hours and modest fee can make a huge difference.

Considering that the average cost of a personally identifying information data breach can be as much as $150 per record according to a recent study, and that funds transferred in response to a spoof attack are likely never to be recovered, these modest preventive steps, which are really just a burglar alarm for the 21st Century, are a wise investment.

***"Cybersecurity and data breach prevention are not just issues of technology; human behavior plays a very significant role."***


***Kenneth C. Citarella***
*Guidepost*
*Senior Managing Director,*
*Investigations and Cyber Forensics*
*415 Madison Avenue*
*New York, NY 10017*
*212.817.6732 (o)*
*212.817.6728 (f)*
*kcitarella@guidepostsolutions.com*



***Elizabeth M. Barnhard***
*Leason Ellis LLP*
*Of Counsel*
*One Barker Avenue*
*Fifth Floor*
*White Plains, NY 10601*
*914.821.3074 (o)*
*914.288.0023 (f)*
*barnhard@leasonellis.com*