Security 101: Paper Documents

By: Jim Mottola
Director oforensic Investigations –
Risk Mitigation Services,
Sobel & Co.

As businesses we are seemingly in an informational twilight zone, where important data is stored in both the digital and physical world. Not unlike the character Henry Bemis (Burgess Meredith) from episode 8, of the Twilight Zone, Time Enough to Last, there is no telling, short of an apocalypse, how long paper documents, in his case books will be around. So until the transition to an entirely digital environment is complete, we will remain attentive to protecting Personally Identifiable Information (PI) in both worlds.

According to the NIST Guidance for Protecting the Confidentiality of PII, it is defined as:

"any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

The most interesting part of this definition is in regards to the phrase, “linked or linkable to an individual”. So while one document, in itself may not provide a fraudster all the information needed to commit identity theft, it may provide a key piece. The New Jersey Identity Theft Prevention Act mirrors the NIST definition for PII, while also making organizations responsible when it pertains to Garden State resident data.

The statute addresses the need to protect information as a result of identity theft and data breach elements “regardless of the physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed, or electromagnetically transmitted.” Again, with almost every state having its own data breach statue, it is presumable that businesses holding data for residents of other states must meet other legal requirements.

Now let's approach this from a practical standpoint, borrowing a quote cited by NIST, from McGeorge Bundy, "If we guard our toothbrushes and diamonds with equal zeal, we will lose fewer toothbrushes and more diamonds." In this case, let's give paper the attention it deserves, and for organizations looking to initiate a program of operational security, this is a great jumping off point. However, let's not lose something more valuable, in the mean while.

To begin with paper documents, unlike information in digital formats are usually hiding in plain site, which are both a blessing and a curse, but easy enough to address:

Shred it! Shred it! Shred it!

Really, do we need to state the obvious? The answer is yes. It is easy enough, and should be part of every business process; either outsourced such through secure shredding services or commercially available machines, ranging from $45.00 and beyond. Above all, your paper documents should be shredded via cross cuts process.

What do I Shred?

Any piece of information contained in the NIST and NJ Identity Theft statute. Yes, that may mean culling the paper a bit, if expense is an issue, or make it easy for employees and give them a wide birth to shred it and forget it. Most companies dispose of paper in an Eco-friendly manner, so you can protect information and save the planet. I would also encourage business owners to allow employees to shred documents at work once a year, especially during tax preparation season, when we, as consumers usually toss out important data in the trash. Look at it this way, with the average consumer losing about 8 hours of their time as a result of identity theft, it is just one more day they will be productive at work, rather than at home contacting credit reporting and financial institutions.

When do I Shred it?

Retention policies including timelines for destruction of sensitive data, should be part of every business, based upon regulatory industry compliance and the IRS Guidelines for Small Businesses. Of course, consulting your tax adviser is usually the best course of action.

How do I store paper?

Yes, as you guessed it, filing cabinets are not totally disappearing from the work place; however, increasingly both businesses big and small are scanning and retaining these documents digitally. Again, it depends on your ability to pay someone or do it yourself. If retaining paper in its digital format, you should determine which information is important PII, segregate it and secure it, via lock and key.

What can employees do?

As I have touched upon before, clean desk policies, which include clearing our desks off at the end of the day, securing important information in a locked draw or cabinet go a long way to protecting information and getting everyone to think about protection of data. I am also a big fan of locks on office doors, while the most critical data should be secured, the out box or some ongoing project documents may need to be left out until the next day.

Is there anything else?

Office Machines: Copiers, Fax, Printers, etc. are other places where information, can be left unattended overnight. So it should be the responsibility of the last person leaving the office to take a quick look around those areas before locking up on the way out. I can't emphasize enough how important this is especially, when most of our offices are cleaned after business hours, when no one is around. Yes, we would like to trust that our cleaning services people have been vetted through a background check of some sort; however, given the right opportunity, they or someone else may decide to take advantage of an opportunity that was within our ability to prevent.