VIEWS & VISIONS

A publication of Bowles Rice LLP

Summer 2015

Seven Steps to Cyber Security

John Sileo, President and CEO
The Sileo Group

John Sileo's identity was stolen from his business and used to embezzle $300,000 from his clients. While the thief covered his crimes using Mr. Sileo's identity, John and his business were held legally and financially responsible for the felonies committed. The breach destroyed John's company and consumed two years of his life as he fought to stay out of jail.

In response, John made it his mission to help organizations and individuals protect the data that underlies their wealth. Combining real-world experience with years of study, John became an award-winning author, trusted advisor and keynote speaker on identity theft, cyber security, online privacy and digital fraud.

He is President and CEO of The Sileo Group, a think-tank devoted to helping organizations secure the data that drives their profits, and whose clients include the Pentagon, Visa, Homeland Security and Pfizer. John graduated from Harvard University with honors.

Everybody wants your data. To Facebook, you are information inventory that can be aggregated, shared and sold. To competitors, you are one poorly configured firewall from handing over the recipe to your secret sauce. And to the data spies sitting at the table next to you in Starbucks, you are one unencrypted wireless connection away from wishing you had paid better attention to this article.

Every business is under assault by forces that want access to customer databases, employee records, intellectual property and, ultimately, your bottom line. Research is screaming at us – more than 80 percent of businesses surveyed have already experienced at least one breach and have no idea of how to stop a repeat performance. Combine this with the average cost to repair data loss, a stunning $6.7 million per incident (according to the Ponemon Institute), and you have a profit-driven mandate to change the way you protect information inside of your organization.

But as entrepreneurs who already stretch every resource to the limit just to stay in the game, you need to do more with less. Here are a handful of the most common high-risk data theft situations and *7 Survival Strategies* to inexpensively decrease your exposure:

1. **Start with the humans.** One of the costliest data security mistakes I see companies make is to only approach data privacy from the perspective of the company. This ignores a crucial reality: *All privacy is personal*. In other words, no one in your organization will care about data security, privacy policies, intellectual property protection or data breach until they understand what it has to do with them.

   Strategy: Give your people the tools to protect themselves personally from identity theft. In addition to showing them that you care (a good employee retention strategy), you are developing a privacy language that can be applied to business. Once they understand opting out, encryption and identity monitoring from a personal standpoint, it's a short leap to apply that to your customer databases and intellectual property.

2. **Immunize against social engineering**. The root cause of most data loss is not technology; it's a human being who makes a costly miscalculation out of fear, obligation, confusion, bribery or sense of urgency. Social engineering is the craft of manipulating information out of you or your staff by pushing buttons that elicit automatic responses. Data thieves push these buttons for highly profitable ends, including spear-phishing, social networking fraud, unauthorized building access and computer hacking.

   Strategy: Immunize your workforce against social engineering. First, when asked for information, they should immediately apply a healthy dose of professional skepticism. Train them to automatically assume that the requestor is a spy of some sort. Second, teach them to take control of the situation. If they didn't initiate the transfer of information (e.g., the credit card company called, not vice versa), have them stop and think before they share. Finally, during this moment of hesitation, empower them to ask a series of aggressive questions aimed at exposing fraud. To see fraud training in action, visit **www.Sileo.com/fraud-training-101**.

3. **Stop broadcasting your digital data**. There are two main sources of wireless data leakage: the weakly encrypted wireless router in your office and the unprotected wireless connection you use to access the Internet in an airport, hotel or café. Both connections are constantly sniffed for unencrypted data being sent from your computer to the web.

   Strategy: Have a security professional configure the wireless router in your

office to utilize WPA-2 encryption or better. If possible, implement MAC-specific addressing and mask your SSID. Don't try to do this yourself. Instead, just hand a qualified technician this paragraph and continue to do what you do best while the technician earns your wisely spent dollars. While the technician is there, have him or her do a security audit of your network.

To protect yourself while surfing on the road, purchase a high-speed USB modem from one of the major carriers (Verizon, Sprint, AT&T) and stop using other people's free or fee hot spots. Unlike hot spot transmissions, these devices are encrypted and will give you Internet access from anywhere you can make a call.

4. **Eliminate the inside spy.** Chances are you don't perform a serious background check before hiring a new employee. That is short-sighted, as most of the worst data theft ends up being an "inside job" where a dishonest employee siphons information out the back door when no one is looking. Many employees who are dishonest now were also dishonest in the past, which is why they no longer work for their former employer.

   Strategy: Invest in a comprehensive background check before you hire, rather than wasting multiples of your investment cleaning up after a thief steals valuable data assets. Follow up on the prospect's references and ask for some that aren't on the application. Investigating someone's background will give you the knowledge necessary to let your gut-level instinct go to work and will discourage dishonest applicants from going further in the process.

5. **Don't let your mobile data walk away**. In the most trusted research studies, 36-50 percent of all major data breaches originate with the loss of a laptop or mobile computing device (smart phone, etc.). Mobility, consequently, is a double-edged sword, but it's a sword that we're probably not going to give up easily.

   Strategy: Utilize the security professional mentioned above to implement strong passwords, whole disk encryption and remote data wiping capabilities. Set your screen saver to engage after five minutes

of inactivity and check the box that requires you to enter your password upon re-entry. This will help keep unwanted users out of your system. Finally, lock this goldmine of data down when you aren't using it. Either carry the computer on your person in a backpack, store it in the hotel room safe or lock it in an office or fire safe when not using it. Physical security is the most overlooked, most effective form of protection.

6. **Spend a day in your dumpster.** You have probably already purchased at least one shredder to destroy sensitive documents before they are thrown out. The problem tends to be that no one in the business uses it consistently.

   Strategy: Take a day to pretend that you are your fiercest competitor and sort through all of the trash going out the door for sensitive documents. Did you find old invoices, credit card receipts, bank statements, customer lists, trade secrets, employee records or otherwise compromising information? It's not uncommon to find these sources of data theft, and parading them before your staff is a great way to drive the importance of privacy home. If your employees know that you conduct occasional "dumpster audits" to see what company intelligence they are unsafely throwing away, they will think twice about failing to shred the next document.

7. **Anticipate the clouds**. Cloud computing (when you store your data on other people's servers), is quickly becoming a major threat to the security of organizational data. Whether an employee is posting sensitive corporate info on their Facebook page (which Facebook has the right to distribute as they see fit) or you are storing customer data in a poorly protected, non-compliant server farm, you will ultimately be held responsible when that data is breached.

   Strategy: Spend a few minutes evaluating your business's use of cloud computing by asking these questions: Do you understand the cloud service provider's privacy policy (e.g. that the government reserves the right to subpoena your Gmails for use in a court of law)? Do you agree to transfer ownership or control of rights in any way when you accept the provider's terms of service (which you do every time you log into the service)? What happens if the cloud provider (Salesforce.com, Google Apps) goes out of business or is bought out? Is your data stored locally or in another country that would be interested in stealing your secrets (e.g., China, Iran, Russia)? Are you violating any compliance laws by hosting customer data on servers that you don't own and, ultimately, don't control? If you are bound by HIPAA, SOX, GLB, Red Flags or other forms of legislation, you're probably pushing the edges of compliance.

By taking these simple steps, you will begin starving data thieves of the information they literally take to the bank. This is a cost-effective, incremental process of making your business a less attractive target. But it doesn't start working until you do.