"DOCTOR, HAVE I BEEN CLONED?"

Bill Palisano
President of Lincoln Archives

Probably not. But, there may be someone (or several people) out there in this (everything on-line, data intense, everything and everyone connected) world that for all intensive purposes is (are) you. They don't share your DNA. They don't look like you.

They don't sound like you. They really have nothing at all in common with you. Except, for your social security number and/or drivers license number and/or your medical identification number. Not going to happen to you, right? I hope not. But there's an old adage: "Hope is not a course of action." A year ago, I wrote an article in this journal about identity theft. A lot (I mean A REAL LOT) of things have happened in a year. Many reports/stats that have been published since, including:

1. In 2013, the health care industry experienced more data breaches than it ever had before, accounting for 44% of all breaches, according to the Identity Theft Resource Center. It was the first time that the medical industry surpassed all others, and stood in stark contrast to the financial services industry, which represented just 3.7% of the total.

2. According to a 2013 ID Experts data security survey of 91 healthcare organizations, 90% of respondents had experienced a data breach in the previous two years and 38% had had more than five incidents. Criminal attacks have doubled in the last four years, according to the survey.

So, what types of systems are being compromised? According to research and report: A SANS Analyst Whitepaper (entitled: "Healthcare Cyberthreat Report – Widespread Compromises Detected, Compliance Nightmare on Horizon" published 2/14, sponsored by Norse): 33% of malicious traffic passed through or was transmitted via VPN apps, 16% by firewalls, 7% by routers. Per the report: "The fact that security devices and applications are emitting the most malicious traffic... is particularly troubling." Also, the study reported that 7% came from radiology imaging s/w, 7% video conferencing systems, 3% from digital video systems ("most likely used for consults and remote procedures").

Who are the targets? The report also states: "...SANS estimates roughly a third of the provider organizations...represent small providers, either individual practices or small groups with fewer than 10 providers." So, although the majority of the targeted/ breached providers were large, still a high percentage of compromised practices were small practices. If you're a small practice, you too are in fact 'on the radar'.

OK so above info is on breaches. Some may/may not have led to Medical Identity Theft (at least not yet). Here are some stats/info on actual Medical Identity Theft (based on the "2013 Survey on Medical identity Theft" conducted by Ponemon Institute and sponsored by MIFA – Medical Identity Theft Fraud Alliance). This is a small sample:

1. The number of medical identity theft victims increased... a 19 percent increase over one year.

2. Medical identity theft can put victims' lives at risk... 50 percent are not aware that medical identity theft can create inaccuracies in their permanent medical records.

3. The most frequent medical consequence of a medical identity theft is that respondents lost trust and confidence in their healthcare provider (56 percent).

4. Individuals lack awareness of the seriousness of the crime... As a result, it seems they are slow to take steps to protect themselves and resolve the crime. In fact, 50 percent of respondents do not take any steps to protect themselves from future medical identity theft.

5. Resolution of the crime is time-consuming. The amount of time it takes to deal with the crime may discourage many victims from trying to resolve the theft and stop future incidents. Those who did try to resolve the incident say such activities consumed almost a year or more, according to 36 percent of respondents. Almost half (48 percent) of respondents say the crime is still not resolved.

6. Individuals rarely take steps to check their medical records. Specifically, 56 percent of respondents do not check their records to determine if the health information is accurate.

In any free enterprise economy, the laws of economics rule. Remember Macro Economics: Supply & Demand? Based on Ponemon's survey, if Medical ID Theft (demand) is up 19%, you'd think that cost (of ID's) would be way up too. Wrong. The pricing for your personal identity has gone DOWN on the black market. Per "The Office of the National Counterintelligence Executive" report: "How

"Doctor, have I been cloned?"

continued from page 10

Much Do You Cost On the Black Market? (http://www.ncix.gov/issues/cyber/identity_theft.php): "Your social security number, at $3, is less expensive than a McDonalds Happy Meal. That's a decline for cyber criminals, as last year the average cost of obtaining a U.S. Social Security Number was $5. Currently: Your mother's Maiden Name: $6" Why is this? My belief is this: based on the huge increases in attacks and actual breaches there's A LOT more supply out there; possibly out-stripping demand (for now). I'm not even going to get into the "Affordable Care Act" and how it could drive demand for stolen identities way, way up...

So, what am I seeing out there in response to the upward trend in attacks, breaches, and resultant Medical Identity Theft instances? A new 'suite' of services: Breach Reporting Services, and Breach Mitigation Services. The former refers to a service where client signs up, pays a (typically) low monthly fee (could be $10-$20). In the event of a suspected or actual breach, the BRS will do an interview to get all known facts/evidence, then advise as to whether or not mandated data breach reporting is required or not. If it is, they will do it for you. They know the laws, the regulations and they'll take this function completely 'off of your plate'. BMS's are a pro-active suite of services to lower the risk of a breach. These are more involved, and typically fairly expensive. The BMS works with the client, investigates, does many a risk analysis, identifies potential threats and potential solutions. Did I mention these can be typically quite expensive?

I'll leave you with a very relevant quote: "There's a shift taking place in the way many enterprise network defenders think about data breaches and cyberattacks," said Timothy P. Ryan, Kroll managing director and head of Cyber Security. "The sheer number of breaches that have recently occurred has caused companies to think more proactively about risk and mitigation. In short, it's no longer 'if it happens' but 'when it happens.' Companies are now thinking about their levels of risk in proactive ways. Previously, most organizations did their best to protect their network and dealt with breaches when they happened. Today, more executives are being forced to abandon their traditional 'crisis playbooks' as they face a proliferation of cybercrimes that require a more comprehensive yet nimble approach."