

STATEMENT OF ALAN BRILL, CISSP, CFE, CIPP

**Senior Managing Director
Kroll, Inc.
600 Third Avenue, New York NY**

**Before the United States Department of Labor
Advisory Council on Employee Welfare and Pension Benefit Plans**

**Privacy and Security Issues Affecting Employee Benefit Plans
July 20, 2011**

My name is Alan Brill. I am a Senior Managing Director in the Computer Forensics and Information Security Practice of Kroll. We apply our knowledge of information security, digital forensics, investigations and business to help organizations make high-risk, high-value decisions. One of the focuses of our work over the past decade has been in understanding and helping clients to cope with the issue of protecting sensitive personal data and responding where a breach is suspected or is known to have occurred. We maintain offices in dozens of countries and have the opportunity to see these issues as they are occurring and evolving across the world.

I'd like to discuss the lessons we've learned in dealing with hundreds of incidents and hopefully preventing many times that number. In an environment where resources are limited, and security must compete with other potential uses for available funds, we can't afford to fall victim to easily preventable incidents. We're fortunate in that there are lessons to be learned, not only from the actual experiences of organizations like Kroll, but from work done in other industries, including financial services, health care and credit card processing.

In our society, we have reached a point where we understand that the incredible benefits available through information technology and the global Internet are not without cost. Cost to us as a society, and cost to us as individuals.

It is a reality that for every new technology, there is a percentage of the population that's up to no good. They look for ways to exploit the technology for their own benefit, regardless of whether doing so is legal or moral. And in the past, they often got away with it. Laws recognizing various forms of computer-related abuse as a crime often lag behind the ability of the wrongdoers to take advantage of the technology-law gap. I believe that we would all agree that Information technology advances at the speed of light – after all, aren't most of the gadgets we buy superceded by new models before we can unpack them? But while the technology advances at the speed of light, the laws protecting and overseeing that technology advance at the speed of legislation.

One of the areas of greatest concern to individuals, businesses and government agencies today concerns the protection of sensitive personal, financial and health-related information. I venture to say that few of you here today have not at least gotten a letter saying that some of your data had been compromised. Only a few weeks ago, I had a credit card transaction turned down. When I called the bank, they told me they had received word that my card number was among thousands stolen in a cyber-theft incident. So they decided to invalidate my card and give me one with a new number. Hundreds of millions of data breach notices have gone out. This number is not, as far as we can tell at Kroll, decreasing. It appears that the number of organizations being targeted for information theft is increasing. The cyber-criminals are recognizing the value (to them) of attacking small to medium size businesses in both large and small cities. These targets are often less protected than major companies in large markets. But a small to medium size business can be a lucrative target. Perhaps a quick wire transfer fraud would only net you a few hundred thousand dollars rather than a few million, or a few thousand identities or credit cards rather than hundreds of thousands, but you can accomplish these attacks quickly, and from wherever in the world you are. The late Senator Everett Dirksen is quoted as saying "a billion here, a billion there, pretty soon you're into real money." That's true for the attacks on small to medium businesses. The numbers add up very quickly.

Of necessity, the proper calculation, payment and accounting for retirement income requires storage of an enormous amount of highly sensitive data for extended periods – perhaps during an individual's working life and retirement years. There's the data about the recipients, of course, and spouses or others who may be potential beneficiaries. There's often detailed banking information, necessary to implement direct deposits. But it is also necessary to consider the nature of an important segment of the population whose information we are discussing.

Our older population has been identified by many as being particularly vulnerable to frauds of all kinds. When it comes to technology-driven frauds like identity theft, unauthorized bank transfers, email scams, telephone-based scams, it has been widely reported that our senior citizens are being targeted.

From the viewpoint of a cyber-criminal, senior citizens are great targets. They often have money on the form of their life's savings and also often have good credit ratings. They are often not very computer-literate, and may be more likely to fall for various phishing schemes. They certainly didn't grow up in the world of social media, and where anyone can put anything on the Internet and make it look – at least outwardly – legitimate.

Put all of this together, and you have something of a perfect storm of risk. Large amounts of sensitive information – including financial information – about a population that may be less able to defend itself.

What does this mean in terms of the topic of today's hearing on the privacy and security issues affecting employee benefit plans?

In answering that question, I'm relying on the collective experience of my colleagues and myself at Kroll. We are often the people who get the call when something terrible has happened, or is suspected, in terms of a network intrusion or data theft. We can carry out the investigation, perform the computer forensics, and, if necessary, help in the notification of those whose data was stolen and whose identities may be at-risk.

I wish I could tell the Council that there was a simple solution – use this software or hardware and the problem will disappear – but I can't. As you can imagine, there are many causes of intrusions into systems. Some involve insiders stealing data. Others involve external entities – cyber-criminals – exploiting security deficiencies to gain access to a system. Some involve thoughtless acts – failing to shred sensitive material and throwing it into a paper recycling bin instead – while others are highly technical. But I think there are lessons to be learned from the hundreds of incidents that we have helped to investigate and remediate.

Lessons Learned.

One of the hardest things to tell an organization is that the intrusion event was completely preventable. That happens more often than you might imagine. Some quick examples may illustrate my point:

- A financial organization lost tens of thousands of records because an older system which was scheduled to be replaced wasn't. Because of economic conditions, the company decided to postpone replacing the system for a year. But everyone assumed that it wouldn't need maintenance. They got hit with an attack that sent data base code in the form of internet requests – the stuff you type into your browser. The old application was not protected by a small piece of software called an application-level firewall that would have filtered out that embedded code. It wasn't there, so the system read the code, executed it, and transmitted thousands of records to someone without any authorization. Installing what is literally a free, open source program – which took about 90 minutes – completely stopped the data loss.
- Another company sent backup tapes offsite every day. One day, while the driver of the pickup van was in a building collecting another company's tapes, the van was broken into, and the box containing our client's tapes was stolen. Unfortunately, even though their backup software had the capability to fully encrypt the tapes with a strong encryption system, they hadn't bothered to turn on that feature of the software. The tapes, as a result, were completely readable. This was a totally preventable release.
- In another recent case, we discovered that a cyber-criminal talked a telephone support person into providing credentials to enter a company's online system. Not only did they get a user ID and password, but they obtained the code needed to download a digital certificate that vouched for their identity. This is called a "social engineering" attack, since it involves more of the skills of the old-fashioned confidence artist to talk someone into doing something they shouldn't. Again, something that shouldn't have happened.

Other cases we see may not be preventable in a technical sense, but demonstrate another frequently encountered problem. Maintaining more data than is needed for longer than it is required. Put simply, we often encounter organizations that hate to get rid of data. If you remember any accounting classes you may have taken where the instructor talked about inventory models like FIFL (First in, First Out) and LIFO (Last In, First Out), I have to tell you that as we investigate many cases of cyber-intrusion and data theft, the model they seem to follow is one we call "FISH" which stands for "First In, Still Here."

The data retention problem has several aspects that the Council should be aware of. First, organizations often collect data that they don't actually need. Only a couple of years ago, I had a case that was of this kind. They collected a lot of data that we discovered was used nowhere in the company's business

processes. When we asked why they collected it, they told us that they had always collected it. It actually seemed to come as a revelation to the technology people in the company that much of the data they carefully collected, edited and stored wasn't actually ever used. Some of this data was of a kind that would be very helpful to a cyber-criminal stealing identities. And, as you might have guessed, these data elements were among those stolen. Data that is collected and stored, but isn't used or needed represents 100% risk and 0% value.

In another case, a high-tech company had its e-commerce site hacked. The hackers got the credit card data for several years of transactions. When we investigated, we asked why they kept credit card numbers and related data for years – and didn't give their customers the ability to opt in or out of storing such information – they said that it wasn't something they actually thought about. Yet our analysis showed that among the credit cards stolen were some that hadn't been used in years. Someone bought an item 3 years ago and never bought anything else. The return period for an item in their store was 90 days. We asked what the purpose of holding the credit card data forever, and they responded with “well, if they ever return, we have their credit card numbers.” I suspect the victims would have preferred to have the right to determine whether they wanted those numbers stored forever. I also had a recent case where an individual discovered a charge on their credit card that came from a company they hadn't dealt with in years – a charge for renewal of software that this person didn't want to renew. He knew that the information that the software company had included a credit card expiration date that had passed more than a year earlier. The vendor knew that the bank in question renewed cards most frequently for 3 years and didn't change the card number, so they just added three years, and an expiration date of 09/2010 became 09/2013 and the charge went through. The bank reversed it, but the point is that even old and apparently outdated information can have value and be misused. So the other lesson is that once data is no longer needed, don't keep it, or at least put it into less accessible protected storage.

As I said earlier, I recognize that ERISA-related sensitive personal data will often be relevant and have to be stored and processed over an extended period of years. But during that period, the risk factors are changing. As those whose data is being stored by public and private entities involved in the processing of long-term employee data, what expectation should we have about the security of our information? Recognizing that there is no such thing as 100% security, what should the organizations collecting, storing and using such data do to protect it, and what should they do if it is compromised?

Right now, there are a maze of state and federal laws that come into play when sensitive data is compromised. The dozens of laws are often very different. For example, a breach notification letter that meets the needs of some states is a direct violation of the notification laws of another state. The obvious result is a level of confusion, extra work to get the notifications right – a real issue for companies that operate on a nationwide basis – and extra costs.

In terms of avoiding incidents, which is certainly preferable to investigating them after they occur, there is much that could be done. The Federal Financial Institutions Examination Counsel – FFIEC – recently issued revised guidelines for online authentication of individuals. How do you know who's on the other end of a communication line, whether it's a phone line or an Internet connection? To over-simplify what the financial institution regulators have been saying for years, the point is that a User-ID and Password isn't enough. That's a good rule.

In the health care industry, there are obvious comparisons with HIPAA and HITECH. From my viewpoint, one of the key elements involved in the implementation of those laws is the requirement for employee training. Across the board, we find that employees receive very little training on data security. Training is no panacea, certainly, but it can and does help. So do things like making data security a specific and stated part of employees job descriptions. An item on data security that is part of an employee's annual performance review also helps to make the need for security more real to people.

There has been good work done by the credit card industry. The card issuers, who everyone acknowledges are competitors, understood that security was an issue that affected their industry and that having multiple sets of guidelines or rules simply wouldn't work. They came up with a uniform set of principles for protection of data – which are really pretty simple to understand – and a mechanism for enforcing those rules depending on the volume of credit card transactions that an organization processes. These rules – called the Payment Card Industry Data Security Standard – are an indication of how competitors with a common security problem can get together and agree on guidelines that affect each of them. I believe it is a model that could serve the organizations in the employee benefits plan field well. Let me be clear – establishment of baseline security standards will not eliminate cybercrime any more than the PCI standards eliminated identity theft from credit card issuers. But if we can set a standard, and provide mechanisms for compliance measurement – including both self-assessments and external assessments where appropriate – I believe we can have a marked impact on the problem.

Doing things in a way that protects information stored in computer systems doesn't have to be expensive. For example, NIST provides excellent guides showing how to configure computer servers to be highly secure. These guides are free and available on the Internet. It's a matter of taking the time to get them, review them and implement the parts that make sense for a given organization. Making sure that software is updated with patches as manufacturers identify security vulnerabilities and provide new code to repair those security holes has become a real issue. Failure to patch means that you're running with known security problems. That's generally not something you want to do. I mentioned earlier the case in which we were able to use an open source web application firewall to stop a data breach. Knowing that such software can stop the kinds of code-injection attacks that have been so prevalent.

Building defense into our employee benefit systems isn't simply a matter of good security, It's a matter of good business. Breaches are very expensive, not only in financial terms, but in reputational damage as well. To say nothing of the terrible consequences to a retiree who discovers that a hacker has redirected their retirement payment to the hacker's own bank account. For a senior citizen who is completely dependent on that payment, the results – even a short period while the matter is investigated and a correct payment made – can be devastating. Ultimately, the cost of playing fast and loose with employee benefit and retirement data isn't the cost to the company that did so. The cost is paid by the retiree who didn't get their payment, and who can't pay their rent or pay for a renewal of a needed prescription.

I'm not suggesting a revolutionary change. I'm suggesting that the Council look at the successes in the financial community and the credit card community of having common standards and an expectation that those standards would be met. Uniform national laws on breach notification would certainly bring some order out of the chaos caused by dozens of different laws. Remember, it is not about the technology, or the Internet, or even the retirement and benefit plan organizations. It's about the individuals who rely on the employee benefits industry to protect their data and their benefits. What we recommend, and what we do, we do for them.

On behalf of myself and my colleagues at Kroll, I want to thank the Council for permitting me to offer our views on this important subject.