Statement of
Alan Brill
Senior Managing Director

Kroll®

before the

ERISA Advisory Council
to the
United States Department of Labor

June 7, 2016
Washington, DC

Statement of Alan Brill

CISSP, CFE, CIPP/US, FAAFS

Senior Managing Director, Kroll Cyber Security

before the ERISA Advisory Council to the United States Department of Labor

June 7, 2016

Table of Contents

Statement of Alan Brill[1]

CISSP, CFE, CIPP/US, FAAFS

Senior Managing Director

Kroll Cyber Security

before the

ERISA Advisory Council

to the

United States Department of Labor

June 7, 2016

Executive Summary:

Cyber security has become a matter of central importance to every organization that is part of the eco-structure of organizations that create, use and store personal and financial information for participants in pension plans.

Threats against cyber-resources now are a reality for even small to medium-size organizations. Hackers have found that small to medium-size organizations often have less effective security measures than do larger organizations (which often have more resources to devote to security) and that in many cases, once entry is gained into such organizations, the hackers can navigate to other organizations which have ineffective trust relationships. (This is how, as reported in the case of the Target data breach, the perpetrators started by breaching the security not of Target itself, but by compromising online credentials used a company that provided air conditioning and heating services for their stores.[2] From that company's network, they moved into the Target network and navigated to Target's point-of-sale system where they spread malware.)

Hackers also understand – as should firms involved in ERISA -- that physical location does not matter. Because of the global nature of the Internet, every organization is virtually next door to

[1] The material presented in this document represent the opinions of the author.

[2] See, for example, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

sophisticated gangs of cyber criminals. If you are connected to the Internet, the potential for being breached is a real one.[3]

As investigators who both carry out intensive analyses to understand how actual intrusions occur and consultants who assist organizations to develop cost-effective defensive measures to achieve a commercially reasonable level of cyber security, we understand the need for the development of guidance for organizations involved in processing pension-related data.

These organizations need guidance to enable them to assure themselves that they are operating a commercially reasonable program of cyber security. Certainly, the work done by the National Institute of Standards and Technology[4] (NIST) and the International Standards Organization[5] (ISO) represent a basis for such guidance, but developing and fielding those standards will take time, and time is not on our side. In addition, interpreting those standards to develop reasonable implementable controls for organizations that differ widely in structure, size, function and sophistication is no easy matter. Criminal elements are well aware that there is a huge gap between the existence of standards and their effective adoption across this broad range of companies. Cybercriminal organizations are currently attacking every kind of financial services organization. They are stealing personal information. They are inducing financial organizations to transfer large amounts of money to them. They are using malware to encrypt data and force victims to pay them ransoms with the hope that they will receive a decryption key.

In my testimony, after reviewing current threats and the importance of conducting a risk and threat assessment, I will pose a series of questions that an organization can ask of itself to immediately begin reducing risk by dealing with issues that are frequent causes of incidents, and which can be managed at low cost. I will also point out the growing importance of risk transfer through cyber-insurance, which is becoming an important aspect of an overall insurance program. None of this is meant to be a panacea – I don’t believe that one exists – but it is my

[3] Even organizations that have removed Internet access from portions of their systems infrastructure have been been victimized. A major breach of security at the U.S. Department of Defense involving a system not connected to the Internet was traced back to an infected flash memory device inserted into a laptop computer. See https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

[4] The overview of NIST’s Cybersecurity Framework may be viewed at http://www.nist.gov/cyberframework/

[5] The International Standards Organization has developed a set of standards (the ISO 27000 series of documents) focused on the development and implementation of an Information Security Management System (ISMS). See, for example, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

sincere hope that by eliminating some frequent causes of compromise, which can be done at a reasonable cost and with reasonable effort, we can, at the very least, provide a basis for mitigating frequently exploited security problems.

Good morning.

Let me begin by thanking the Council for allowing me to be with you this morning. My objective is to brief you on the cyber-security challenges facing both employers and the organizations that provide them with pension and ERISA-related services.

By background, I'm a Senior Managing Director[6] in the cyber security and investigations practice of Kroll, the international investigations and advisory services firm.[7] We provide investigative services and preventive services to clients around the world. We do not sell hardware or software, and are, in fact, vendor neutral in providing advice to our clients. Many of our people joined us from federal and state law enforcement agencies.

Looking at my work and the work of more than 50 cyber security professionals in our U.S. cyber investigations group, where a lot of our work is with organizations in different parts of the financial services community, I can definitively tell you that the cyber risks faced by both employers and services organizations are more severe and significant than in the past, and certainly more important than when I last had the opportunity to brief this Council. We analyze both individual cases involving data breaches and trends that we see across breaches. We publish these in our annual Data Breach Trends Report[8], a publication we make freely available to assist companies with their determinations of how to protect their sensitive data. The 2015 report offers the following key insights:

- *Human errors — accidental exposure, lost devices, and other non-malicious forms of data loss — were at the root of 60 percent of cases.*
- *Current and former employees along with related third parties accounted for almost 70 percent of data breaches.*
- *Hacking gets the headlines, but 58 percent of breaches considered malicious or non-accidental resulted from stolen data, such as from laptop thefts.*
- *In the age of digital hype, the threat of a breach via paper records was still surprisingly strong at 32 percent of the cases.*

[6] http://www.kroll.com/en-us/who-we-are/kroll-experts/alan-brill

[7] See www.kroll.com

[8] http://www.kroll.com/data-breach-trends-report

We also look at fraud-relate risks on a global basis and publish our results annually.[9]

Introduction

Many organizations fail to recognize that the information that they use every day and which they routinely receive and store in the course of their business, have substantial value in the criminal underworld. Whether it is information that provides information on people's bank accounts or information that would help an identity thief to carry out some other scheme, that business information can be turned into cash by a hacker. As an example, with just the name on a checking account and access to the routing information and the account number (the same information needed to initiate a pension payment) I can carry out a number of schemes, from printing and negotiating physical checks to initiating "electronic check" funds transfers.

It's interesting that in the world of cyber-criminals, there is as much specialization as there is in other fields of endeavor. Those who specialize in actually hacking into your system and stealing the data are often not the ones who will use it to actually carry out a fraud or money theft. The data thieves typically sell the data to exploiters, who actually commit the frauds. They operate through online marketplaces, usually on what's called the "dark web." These marketplaces are quite organized, with purchaser feedback so that the sellers of stolen data get rated by the other criminals that buy their data. I've actually seen some cases in which the sellers offer holiday specials ("buy 1,000 credit cards, get 100 free!")

One of the facts of today's world is that if you hold data that the cyber-crooks want, it doesn't matter where you are – on the Internet, everyone is next door to the crooks – or how large or small your company is. The thieves know that small and medium size businesses often don't have adequate cyber-security in place. They are easy targets, and (particularly since the hackers can use largely automated tools) they are worth attacking.

In this briefing, I'd like to report to you on the kinds of threats that the organizations – both employers and service providers – that make up the ERISA eco-structure -- are up against; some questions to ask to help achieve a commercially reasonable level of cyber-security; the need for top level recognition of the problem; the need for planning; and the role of risk transfer through cyber-insurance. Of course, I am reporting on trends. The particular issues that any specific

[9] http://www.kroll.com/global-fraud-report

organization faces are unique, and each organization has to evaluate the risks and responses that are right for them.

Looking at Current Risks

As you can imagine, risks are constantly evolving. Some are very high-tech. Some rely on specific security failures on the part of the victim. Some are very low-tech, but still work very well. Remember that cyber criminals today are not out for some sort of award for being the most technologically sophisticated. They work for criminal organizations that operate like any other businesses. These organizations are bottom-line oriented, and will use whatever techniques actually work.

In other cases, the criminals may work for the victim organization, and the risks associated with crimes committed by employees, contractors and vendors should not be underestimated. Insider cyber-crimes are still alive and well, and represent a potentially significant risk to many financial services organization.

Here are some of the risks we've been seeing at organizations in the financial services sector:

Ransomware

Imagine suddenly getting a message on your screen telling you one of several things:

- You have been caught by an "FBI computer program" with illegal content on your computer, and the data on your computer has therefore been encrypted. Payment of an online "fine" will get you the code to decrypt it.
- A criminal has encrypted your entire hard drive. Only a payment will make your data available to you again.

This is happening all too often as criminals figure out that mass distribution of the malware that encrypts the hard drive content and receipt of lots of small payments (averaging $200-300) is a very effective business model, particularly if you are overseas in a country unlikely to have any interest in extraditing you if you are ever identified. Add to this the proportion of users who never back up their data files, and you have a real problem.

At corporations, the malware that underlies the damage can quickly spread through a corporate network with disasterous results. When hundreds – or thousands – of machines and key databases are encrypted, it may be difficult for that organization to continue to operate. The motivation to pay ransoms that can soar to hundreds of thousands of dollars is strong.

As investigators, we can sometimes decrypt the data, sometimes not. But what victims forget when they send their payment to the perpetrators is that they are dealing with criminals, who may well decide not to send a decryption code when they receive the money.

The bad guys even helping the victims understand exactly how to pay the ransom – they include instructions to make it easier to give in to their demands. For criminals demanding payment in the virtual currency Bitcoin, they include instructions on how to buy and transfer this virtual currency. Others are very happy with prepaid credit cards, and will tell victims exactly what kind of card they like and which stores sell them. The FBI has even published a brochure on the ransomware problem[10] urging victims not to pay the ransom, although there is no question but that the pressure to do so in hopes of regaining access to critical data can be overwhelming.

I saw a recent estimate putting the criminal's profits from ransomware at some $500 million a year and another claiming that the first study substantially understated those profits. That's a pretty good deal for a low-overhead scam with little chance of being prosecuted!

Data Theft

This is the cybercrime that is the first in the public's mind. The criminals are out to steal data, whether that consists of credit card data, banking data, or valuable intellectual property (like bids for large projects that are soon to be tendered or plans for military hardware). If you've ever received a notification from a company you deal with, or from your credit card issuer telling you that your information "may have been compromised," you, like most Americans, have data that's probably out there somewhere on the Dark Net. But statistics tell us that most people who receive these notices don't actually experience identity or financial theft. That's partly because the card brands have gotten very good at identifying suspicious transactions and their ability to quickly cancel cards that they believe were compromised.

For the most part, a consumer will not have responsibility for funds charged on a stolen card, but they still get the inconvenience of not having a card while new ones are issued. The new cards

[10] file:///C:/Users/abrill/Downloads/Ransomware_Trifold_e-version-2.pdf

with chips are very useful for reducing theft when they are used in a merchant terminal, although it is acknowledged that adding a PIN – as is common in most of the world – would provide much more protection than just a chip and signature. And the chip cards don't provide high-level protection for transactions in which card data is provided over the Internet, where they are no better than cards without chips.

Preventing data theft requires implementing security at a commercially reasonable level. In my experience, getting to the right level involves at the very least doing the basics, but even more importantly, getting attention to the problem and buy-in from the highest levels of the organization – generally, this means the Board. If a company is not serious about cyber-security, it is more likely to become a victim. Many companies have never carried out an organized risk assessment. Many simply believe that their IT managers (or outsourced IT services) are on top of the problem. And many have learned the hard way that the risks were there, and that criminals have exploited them.

A final point about data theft is that there are dozens of state and federal laws and regulations requiring consumer notification under many circumstances when a breach is detected. Other countries are also adopting mandatory notification laws, which can represent an additional challenge for global organizations. Many companies offer affected consumers credit monitoring with either one or three credit bureaus. But it is interesting that statistics show that less than a third of consumers offered credit monitoring services actually take advantage and sign up for them.

Data Manipulation

One of the most worrying predictions is that attackers may move from just stealing data to changing it. What do you do when your bills start going out wrong, either under-billing or over-billing your clients? What does a hospital do when it becomes evident that patient's electronic medical records are wrong – wrong blood types, wrong lab test results? What will happen to a firm's reputation when the electronic funds transfers that represent pension payments turn out wrong, with some recipients receiving massive overpayments, and others getting almost nothing. Aside from the very real damage done to pension recipients who depend on those payments for basic needs, the reputational damage to the company involved can be huge.

More directly to today's hearing, what if a company in the employee benefits field discovers that the employee's benefits history and records in its databases have somehow become incorrect, and there is no correct backup? Attacks of this kind can be devastating. And attacks directed against decision support system can cause important business decisions to be based on false and inaccurate data.

It's likely that companies are going to be increasingly focused on data integrity – making sure

that their key information remains accurate and that it hasn't been subject to unauthorized changes. One technology that appears to hold great promise for helping to assure the integrity of data involved the use of the recordkeeping technology underlying the virtual currency "Bitcoin." While that currency has been the subject of a great deal of criticism, the ledger system – called a blockchain[11] – is exciting. It's currently being used for authenticating securities transactions and is the subject of a great deal of investment, research and planning throughout the financial services community.

Pass-Through Attacks

There's a term that's become fairly well known over the past few years – "SWATting". This happens when someone calls the police and makes a report that causes a SWAT team to descend on a person's home or business, bursting in with guns drawn and treating completely innocent people as dangerous, armed felons.

The equivalent in the cyber-world is to either take control of computers at an organization and use them to conduct an attack on another organization (so that it's traced to a company that's actually another victim but seems to be a perpetrator) or by taking control of a server within an organization and using that compromised server to store and transmit material like child pornography. With millions of U.S. computers compromised by malware to act as what are called "zombies" doing the bidding of a criminal (sometimes called a "bot herder") who often rents out the use of his or her botnet to other criminal enterprises, to attack their enemies.

[1111] The subject of virtual currencies, how they work and the risk associated with them are the subject of an article I wrote with my colleague, Lonnie Keene, for NATO's Defense Against Terrorism Review, and may be found at http://www.coedat.nato.int/publication/datr/volumes/datr9.pdf

These attacks can bring negative publicity or even litigation, and unless a company is diligent in monitoring and protecting its networks, this is a very real threat.

Distributed Denial-of-Service Attacks

Distributed Denial of Service (DDoS) attacks have been around a long time. Basically, they operate by flooding a company's Internet-facing servers with so much useless traffic that the system fails. Many organizations have been knocked off-line by these attacks. Working with your internet provider is key to preventing, recognizing and defeating DDoS attacks. Activist organizations like Anonymous use these attacks to further their various campaigns.

Wire Transfer E-Mail Frauds

One of the specific attacks that we have been seeing with increasing frequency in recent months is the use of falsified emails purporting to be from a senior corporate executive – most often the CEO or CFO – directed at someone in a company's accounting department designed to induce them to make a wire transfer to an account controlled by the criminals. They are very good at crafting realistic appearing emails, and have been surprisingly successful in doing this, and all too often, the funds, once transferred, are gone for good. This is a low-tech attack – it's essentially a very specialized version of Social Engineering, in which a perpetrator tries to talk an employee into performing an unauthorized act, but it works.

Phishing, Spear Phishing, and "Vishing"

Sending various types of false emails, attachments, instant messages and other forms of communication is a problem that's been around a long time, but is still with us because these attacks are still so effective. A high percentage of malware infections can be traced back to a person opening an attachment to an email that looks safe, but isn't. One launched, the malware can rapidly spread through an organization and be very difficult to remove. Spear phishing, by the way, it the term given to phishing attacks that are customized to support fraud against a specific targeted company. Email may contain company logos. They may seem to come from internal sources. They can be very effective.

Malware writers are very talented. They can create an attachment to an email that appears to be a word file – and that actually looks like one when opened, but which also contains a "dropper" that loads malware onto the targeted machine. They can also establish a website that looks innocuous (or looks like a legitimate site) which will automatically load malware on anyone who visits the site. (These are referred to as "watering hole" sites, and the malware infections are sometimes called "drive-by attacks.")

And one kind of attack that's often overlooked is called "Vishing" or voice-mail phishing. This involves leaving messages on employees voice mail asking them to call a number controlled by the criminals or to either visit a website or respond to a phishing message in their email, and purporting to come from a senior company official.

URL Theft

There's no question that a company's internet names are valuable, as it is how we reach the destinations on the internet that we want to visit. But even organizations as large and sophisticated as the New York Times have had hackers re-route traffic away from their real web servers and redirected them to servers controlled by criminals[12].

There are specific mechanisms by which a URL can be transferred from one owner to another. The bad guys are experts at manipulating these processes. The solution is to go to your URL registrar, and lock your account. This makes it virtually impossible for your URL to be hijacked without your knowledge. This can very often be done online. When I did it for my personal URLs, it took me about 5 minutes and was very easy.

Changing Attack Modalities and Increased Risk

Years ago, it was common for cyber-attackers to strike quickly, steal data and get out. Now, it is common that hackers want to break into your network and remain there for months or years, stealing data without being noticed. Unfortunately, they are often successful. While the time to carry out a successful penetration of an organization's system may be measured in hours or days, the time between the beginning of the intrusion until it is noticed by the victim is often measured in months. This new strategy on the part of cyber-criminals, often called "Advanced Persistent Threats" (or "APTs") represent a continuing danger.[13]

[12] http://www.latimes.com/business/technology/la-fi-tn-melbourne-it-discovers-breach-that-took-down-nytimescom-20130827-story.html

[13] For a background on Advanced Persistent Threat attacks, see my article in NATO's Defense Against Terrorism Review journal at http://www.coedat.nato.int/publication/datr/volume6/03-How_Cyberterrorists_Could_Be_Living_Inside_Your_Systems.pdf

Moving Toward Commercially Reasonable Cyber Security by Asking the Right Questions

When we analyze the hundreds of actual cases that are brought to us every year, we see some incidents that would have been very difficult to prevent, but we also encounter many others that could have and should have been avoided.

Every organization must ultimately determine what the “right” level – the *commercially reasonable* level -- of cyber-security is for them, based on an assessment of risks and threats that they face. But we find that incidents – sometimes serious incidents – are traceable to very basic issues that can be fixed for little or no cost. It seems that there are some basic questions that every employer and service provider executive should be asking of its IT people, internal auditors and risk managers. Here are some of the key issues that you have to consider:

Do you need the data you collect and store?

It’s really difficult to hear from a company that has just lost a lot of data in a hacking case that the data that was stolen was either data that they collected but never actually used, or that it was old data, still containing sensitive personal information, but of no real value to the victimized corporation. These companies now have to deal with the financial and reputational damage of a breach where the data should never have been collected or should have been wiped from the company’s records when it became valueless. Unfortunately, theft of data that shouldn’t have been there happens all too often.

In some cases, we’ve seen that managers are shocked to discover what data was stored in their systems. Photos contained GPS metadata. Some software packages defaulted to collect more data (and metadata) that was actually needed, and no one took the time to actually understand the application’s data collection and change the defaults to avoid collecting and storing data that isn’t needed. Collecting and storing unneeded sensitive data represents 0% value and 100% risk.

It’s time for companies to go on a data diet. Don’t collect information unless there is either a documentable legal requirement for the data, or a demonstrable business process in which it is actually used. The excuse of “but that’s the way we’ve always done it” doesn’t constitute justification. If this excuse is offered, consider it even more reason to determine whether you’re storing sensitive data that you don’t need or use. Similarly, once information is no longer needed (assuming that there is no legal or regulatory requirement to keep it) it should be deleted. But because this is a decision that can have both operational and legal consequences, prudence dictates that data retention and destruction policies be reviewed by counsel before implementation.

Do you know where your data is?

This used to be an easy question. The data would be on the hard drive of my laptop computer, or of my desktop computer, or perhaps on a server that my organization owns and operates. But the world has changed, and data can now be stored in Internet-accessed storage facilities ranging from services like Dropbox or a personal Google Drive, to enterprise solutions involving Storage as a Service from vendors like Microsoft, IBM or Amazon. In many cases, these vendors have dozens of physical sites, and in some cases, those sites may be located in different countries. Given the differences in privacy laws between nations, particularly at this time where the former process for data transport out of the European Union – the Department of Commerce's Safe Harbor system -- has been invalidated and new processes are in flux, it can be very important to know where your data is stored. Customers or government agencies may have rules limiting storage to a particular nation or nations. If this is the case, can your storage vendor tell you with certainty where your data is actually residing? It is anticipated that this will become a more critical issue as cases work through the courts and they consider whether an organization can avoid having to produce evidence by storing it in another jurisdiction.

None of this should suggest that you should not use cloud storage and processing services. Services like Amazon and other major cloud providers spend many millions of dollars on security, and have large security teams monitoring their systems continuously. But you do need to understand how their protection fits into your overall security program, and whether their contracts appropriately protect your interests. You can also increase your level of protection where cloud storage is involved by encrypting stored files and keeping the keys within your organization. If you do this, even if the cloud provider is compromised, your data will still be encrypted.

This is clearly an area where IT professionals should be availing themselves of expert assistance from legal counsel and information security professionals.

By the way, when it comes to backup, you may want to keep it walled off from your regular network so that should you be hit with ransomware, it is not able to also affect your backup.

Are you covered by specific standards?

Depending on your industry, you may be covered by specific standards, and this includes most financial services providers. If an organization stores healthcare-related data, additional rules apply. For any organization storing specialized data – such as criminal records or social services data, additional state laws may define data security regulations. For international organizations, increasing numbers of countries are putting data breach notification, data retention and trans-border data transfer rules in place. This is another issue that should be carefully discussed with counsel in establishing business processes and company standards and procedures.

Does your technical security match up with your systems architecture?

Over the years, I've seen companies grow far faster than their data security. Security that may work when you're a tiny business may become insufficient as your organization grows. As a manager, you have to avoid taking the easy route of assuming that whoever is responsible for our information technology has done an adequate job of securing your data against today's risks. Management can't avoid the ultimate responsibility when a breach occurs, so it makes sense to pay attention before an incident. We've found that IT managers will often tell us either that they either assumed everything was allright or that they just didn't know how to build the right security into their systems, or they knew, but couldn't get the budget or other resources to put the controls in place. This is not an activity where either guessing or hoping for the best is the right course of action – you have to know definitively what you are doing, and whether that represents a commercially reasonable position in light of risks and resource availability.

Another aspect of this is to focus on potential security issues that are associated with "smart" devices you plan to make part of your company's technology base. It's easy to forget, for example, that many "copiers" also can serve as network printers or fax machines. They may have either a hard drive or solid state drive. If this is not recognized and storage cleared before getting rid of the machine, sensitive information can be placed at significant risk without the organization even knowing it. This applies to any device with data storage capabilities. For example, a drugstore donated its old computers to an educational organization. They believed there was not data on the hard drive, but the data was only "deleted" and was still on the drive, and was “unerased” using free software, exposing thousands of customer’s prescriptions and insurance information. The company, it turned out, didn’t take the time to be certain that the data was actually and irrevocably wiped from storage. There are various ways this can be done, but without careful consideration and management of the process, data may remain and be subject to theft.

As more and more devices connect to the Internet, it seems clear that the Internet of Things will become increasingly important in organizations’ overall security planning.

Also, one of the lessons we’ve learned in dealing with hundreds of breach incidents is to recommend that you set your systems to maintain logs. Keep them for an extended period. Too often, when we’re trying to figure out what happened and whether data was actually stolen, the log files that would support our investigation are either turned off or kept for so short a period that by the time we are called in, they have been overwritten. Storage for logs is no longer terribly expensive, and without those logs, any investigation is going to be more difficult and time consuming. Comprehensive logging is one of the best investments you can make.

Are you patched?

One of the most basic techniques that hackers use to successfully gain access to a system is to find and exploit a security hole that was known to the manufacturer, and for which software patches to fix it were available – but never installed. Unpatched systems are a tremendous risk. Unless there is a specific reason, patches should generally be installed. If there is a reason not to install a patch, such as the patch causing problems with a specific program you’re using, it’s vital to both recognize the risk and consider alternative controls.

There is a second problem that we’ve seen: the use of programs that have passed their “end-of-life” dates and for which the manufacturer no longer provides security patches. Hackers can and do attack these systems knowing that if they can get in, it is very unlikely that a patch will be provided. We generally urge companies to upgrade to supported versions of software.

Have you removed all default passwords?

A second common hacking technique involves the use of default passwords. Whether it is a password for an application, a hardware device like a router, or for a user account, using default passwords is not a good idea. With the advent of the Internet of Things, recent news reports have shown that using a default password on devices like smart thermostats, baby monitors, or even refrigerators can open the door to an attack. In a business, a new appliance in the break room which uses a default password can represent an invitation for a hacker to establish a beachhead inside your network.

Is Your Data Encrypted?

In general, storing and transmitting data in an encrypted form is recognized as a best practice, and it is. However, it's important to understand that it may not, under all circumstances, be practical to do this. Where an organization makes use of application systems licensed from various software manufacturers, an end-user may not be able to implement encryption until such a capability is built into the applications. The issue is complicated when stored data is used by multiple applications, perhaps developed by different manufacturers, but using a common data storage format. Unless all of the applications using the data can deal with specific encryption methodologies, a given organization may be functionally unable to implement encryption for stored and/or transmitted data. In such cases, there may be other controls that can, at least in part, compensate for the lack of encryption.

But to simply equate an unencrypted file with inappropriate security is overly simplistic. It is vital to understand the specific technology and software environment, the options realistically available to the company, and the overall system of controls as they are actually implemented to form a basis for understand the organization's capability in regard to using encryption.

Are authorized users properly authorized?

When we investigate cyber incidents, we look at log files to seek evidence of exactly what happened. It is not unusual to see that an incident involved what is apparently an authorized user. But it may turn out to be a user who is no longer employed, but whose account is still active. Or it may be someone who no longer actually needed access to the data stolen. It may be that the user's password was weak. It may be that the user employed the same password at many sites, one of which was compromised. It may be that for some reason, an employee shared their password with someone else. Or it may be that someone was given access to data that they did not actually need, and that data was compromised. It can even show that there are unauthorized accounts, installed and used by a hostile party.

How often do you audit your user records to be certain that:

- Every account is associated with one and only one person (no shared accounts)
- Every user account is associated with a current employee who actually needs access to the data they are authorized to see.
- To the extent possible, access is granted on the basis of access to specific fields, or to specific ranges within a database. For example, a worker may only need access to the last four digits of someone's social security number, not the whole thing, or only have access to employee records of those companies they support, not all employees of all companies.
- You have a process in place and working to rapidly remove access when someone leaves the organization, and to change access as an employee's needs change,
- You have a process in place to provide individual accounts to temporary employees/contractors and vendors, and to delete those accounts when no longer needed.

Data access should be viewed as an important aspect of information governance. Without a governance process, it becomes hard to effectively limit access or to audit that access, both regularly and when an incident makes such a review necessary.

Have you "hardened" your hardware?

On devices ranging from laptop or desktop computers to servers to routers, there are many options made available by the manufacturer to configure the devices. Some of these have security consequences. What settings are right for you?

Fortunately, the Information Technology Laboratory ("ITL") of the U.S. National Institute of Standards and Technology ("NIST") offers the Security Configuration Checklists Program.[14] ITL describes this program:

> "Vulnerabilities in IT products are discovered on a daily basis and many 'ready-to-use' exploits are widely available on the Internet. Because IT products are often intended for a variety of audiences, restrictive security controls are usually not enabled by default by the product vendor, so many IT products are immediately vulnerable "out-of-the-box." It is a complicated, arduous, and time-consuming task for even experienced system administrators to identify a reasonable set of security settings for many IT products. While the solutions to IT security are complex, one basic and effective tool is the security configuration checklist."

[14] http://csrc.nist.gov/groups/SNS/checklists/

> This is a free program that enables you to select the configuration options that will strengthen – or “harden” – your technology devices against hackers.

Have you trained your staff?

People make mistakes. They click on things they shouldn’t click on. They open email messages best left unopened and deleted. They visit websites that may contain so-called “drive-by” or “watering hole” malware. They may plug a memory stick that they found in the parking lot or an employee rest room into their computer with the intention of finding the owner.(One technique used by hackers is to drop an infected memory stick in or near a company’s premises hoping that someone will connect the device to a computer on the network to begin to attack it.) Any of these can start a devastating chain of infection within an organization.

Training helps, and while it is certainly not a guarantee of complete security, it’s very hard to justify not providing your people with instruction, and providing it on a regular basis. One training formula that we’ve seen calls for a combination of annual in-person training (or specific online training) and monthly newsletters. Another process that can help is to modify your employee evaluation system to include a specific item requiring every employee to participate in a cyber-security awareness program, and to use that item to review the employee’s compliance with your cyber-security rules. We’ve found that including an item on cyber-security as part of an organization’s annual employee evaluation process makes it more personal for employees and can motivate good behavior. But remember that people are imperfect, and you have to have monitoring systems and effective reporting mechanisms to deal with errors that people can and will make.

One of the tools that has been successfully used by many organizations is to put in place restrictions on the types of attachments that can be passed through your email system. Executable files and files that can hide executables – such as .zip files – can be blocked from most users, so they can’t accidentally click on them. Where a user actually needs to receive these files, they can be funneled through a special email account or through monitoring software where they can be checked and released to the user.

Have you considered mobile security?

As people travel, they want to take their access to data with them. This causes security issues. Are people using unauthorized cloud storage services that they – not the company – controls? If so, that's almost a guaranteed issue at some point. The data moves to the custody and control of an individual employee or contractor – without authorization and without the organization being able to control that data. Make no mistake – it may be convenient, but if it results in a breach, your organization is 100% responsible for it. You need rules about how and where data is to be stored, and what is available to remote users.

It's also vital to remember that particularly as you travel, WiFi and even cellular sites may belong to hackers. You want to have a rule that online access from mobile devices must go through a VPN – a virtual private network – that will provide encryption from the mobile device to a secure network access point. You can run your own, or you can subscribe to access an inexpensive commercial VPN. The problem is severe enough that the UN Interregional Crime and Justice Research Institute (UNICRI) published[15] a paper that I co-authored with a Kroll colleague in their *Freedom From Fear* magazine entitled "Will hackers be competing in the Olympics?" Our conclusion was, between false WiFi sites and potentially false cell towers, there will be a lot of mobile device hacking at the games, and this is a growing problem. Don't fall victim to mobile security failures by ignoring the problem.

Have you thought about conference line security?

One final issue to think about involves the use of telephone conference lines. Many of us regularly dial into conference calls where highly sensitive information is discussed. There are cases on record of former employees continuing to dial into calls after they leave an organization, and listening in. Fortunately, this is an easy problem to deal with. If you hold sensitive scheduled conference calls, you should change the access code when an authorized participant will no longer be participating. There are also various useful commands, like finding out how many people are dialed in, or locking the call so that additional people can't connect to the conference. Each system differs, but you should know the capabilities available to you.[16]

There are obviously many other steps you can take, some more complex and some more expensive, but you should think of these as basics that you should be considering. An important

[15] http://f3magazine.unicri.it/?p=894

[16] For more details on this problem, see my article in SC magazine, http://www.scmagazine.com/whos-listening-to-your-conference-calls/article/213663/

resource to review in this regard is the Critical Security Controls list (known as the "Top 20" list) from the SANS Institute.[17]

What about organizations you work with?

Companies working in the pension/ERISA field almost never work alone. They may have partners that provide a wide range of services. There are technology providers that may support cloud services or which maintain software. With actuaries, consultants, and other professionals, any given organization exists as part of a network of organizations. How effectively do the organizations you work with protect the sensitive data with which you entrust them? If you are given sensitive data by an individual or employer, and there is an incident at one of the companies with which you share that data, you will be responsible. So finding out how they protect the data, and the extent to which your contracts with them protect you has become vital.

There is a model for dealing with this issue, and we find it in the regulations that healthcare organizations in the U.S. must follow – HIPAA and HITECH. Health care providers that contract with other organizations must have them complete "Business Associates" compliance documentation. As the Department of Health and Human Services describes it[18], *"The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate."* I believe that in considering recommendations to the Secretary, the Council should consider the Business Associate concept – not to adopt as is, but rather as a starting point for consideration of how to protect employees data as it moves between organizations.

The Need for Top Level Attention

In looking across hundreds of cyber incidents over more than 40 years, one thing has remained constant. Top level managers always seem shocked when their company is hit with a serious incident. We investigate and find that a pretty high proportion of the cases were preventable, but the appropriate controls weren't in place, either because the IT managers didn't give it a high priority (often because it doesn't seem important to top management) or because they couldn't

[17] https://www.sans.org/critical-security-controls
[18] http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/

get the resources (people, money, etc.) that they asked for to strengthen security. Of course, when we look at their requests, sometimes they are wildly inappropriate – clearly excessive in light of risks and needs -- but sometimes they were very reasonable, and simply didn't make it through the company's budgeting process.

What is amazing is that everyone knows that cyber-security is important – a high percentage of people have been notified at some point that their data has been compromised – but executives don't translate that into action when it comes to their own organizations. They often either ignore the issue or simply take the word of their IT executives that everything is fine when it comes to security.

Fortunately, there is a recognition on the part of regulators like the Securities and Exchange Commission that cyber-breaches can be reportable events that can result in regulatory actions and substantial fines, or state governments which enforce breach notification laws, or enforcement agencies like the Federal Trade Commission which, as was affirmed by the Third Circuit Court of Appeals in the Wyndham case, has enforcement power as relates to consumer damage caused by data breaches, that cyber security is the responsibility of management and oversight by the Board of Directors.

If an organization's Board has not undertaken a specific program to understand their cyber-risk and the company's response to those risks or which does not require regular reports from management on the state of information security may find their inaction challenged by regulators, enforcement agencies or shareholder litigation. Boards must take the initiative to act in this area, and not wait to react after a problem occurs.

The Need for Planning

As we look across companies that we work with worldwide, the key differentiator between companies that recover well from a data breach incident and those that do not is the extent to which the risk of a breach was recognized and a plan was developed, tested and regularly updated.

Having a written breach plan is vital. Data breaches are crises, and you don't want to be forced to develop your crisis response plan in the middle of a crisis. You should also pre-identify resources that you may need from outside your organization. These resources include forensic and investigative specialists, specialist legal counsel and crisis communication organizations. Companies with cyber-insurance (discussed below) should coordinate their planning with their insurers.

Many of the companies that write cyber-policies have pre-identified panels of experts that the insurers have pre-vetted and which they have pre-approved to provide services under their policies. While exceptions can be made, it is generally preferable to work within their panels, as the carriers will accept their work and have often pre-negotiated special rates for these services. It is a good idea to pre-select one or two firms in each category and pre-contract with them, so that when a need arises, all that's required is a simple work order as opposed to having to negotiate a contract during a crisis. Of course, it's vital to make sure that legal issues (like a specialist law firm's license to practice in relevant states, or state laws requiring investigators to hold valid private investigator licenses) are adequately covered in the planning process.

It is also important to test your plans. These tests can take the form of table top exercises, generally facilitated by specialists in developing and running such exercises. Knowing that those with responsibilities under a plan are prepared to carry out their assigned tasks, and that there are alternates in place (and trained) should a designated person be unavailable is very important.

Risk Management and Cyber-Insurance

Cyber-incidents are part of an organization's overall threat profile. A risk assessment (which forms the basis for a risk management plan) is a basic part of doing business. Many cyber-security frameworks, from HIPAA to the NIST standards are based on a threat and risk assessment. In dealing with risk, one of the important components involves transferring risk through insurance.

A significant number of insurance carriers have developed a range of insurance products covering data breaches and other forms of cyber-crime. Financial services firms and those holding significant amounts of personal information – and that would include many firms in the ERISA field – should at the very least have a conversation with their risk managers and insurance brokers to determine whether cyber-insurance is right for them, what it would cover (and not cover) and costs. Be aware that most insurers will need to know about your systems and existing protections in order for their underwriting specialists to understand your risks and controls, and to develop a cost and coverage model for you.

Conclusion

There’s no question that cyber-security has become a serious issue in all parts of our economy, or that the financial sector has been a leader in recognizing and responding to the challenges.

The development of cyber security guidelines to assist organizations that are part of the ERISA eco-structure would be extremely helpful and enable employers, insurers and vendors in the field to have a benchmark against which they can measure their cyber security efforts. Certainly, the work done by NIST will be very helpful in this regard, but it is my experience that it will also be important for firms in this space to contribute anonymized copies of their standards and policy/procedures for the benefit of all. I believe that this Council can serve an important role in collecting and making the contributed material available to the industry.

In terms of the guidance that could be made available by the Secretary, it’s important to recognize the wide range of organizational size, sophistication and resources that can reasonably be directed to cyber security.

A good model to look at is the cyber-security guidance that on June 15, 2016 will become a requirement under Department of Defense acquisition regulations.

This can be found at *https://www.gpo.gov/fdsys/pkg/FR-2016-05-16/pdf/2016-11001.pdf*.

My objective today was, in part, to provide some questions by which organizations can begin the process of self-assessment of their cyber-security readiness. It is compatible with those new regulations and should provide a basis for immediate risk reduction. It is, I believe, a good place to start.

I hope my participation in this hearing has been of help to the Council, and that it will be of help to the industry.

I have submitted written remarks to supplement my testimony here today, and respectfully request that those remarks be made a part of the minutes of this meeting.

I stand ready now, or at the Council’s convenience to answer questions or provide further information.

Thank you for giving me the opportunity to once again brief the Council.

Alan Brill, CISSP, CFE, CIPP/US, FAAFS
Senior Managing Director
Kroll Cyber Security
300 Harmon Meadow Blvd. Suite 305
Secaucus NJ 07094
Email: abrill@kroll.com
www.krollcybersecurity.com
www.kroll.com