

## **STATEMENT OF SETH GEFTIC**

**Senior Manager, Federal Solutions**

**RSA, The Security Division of EMC**

**174 Middlesex Turnpike, Bedford, MA 01730**

**Before the United States Department of Labor**

**Advisory Council on Employee Welfare and Pension Benefit Plans**

**September 1, 2011**

My name is Seth Geftic. I lead the Federal Solutions group at RSA, The Security Division of EMC. RSA is the premier provider of security, risk and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments. Today, RSA's Identity Protection and Verification group protects more than 8,000 organizations and 250 million online identities and has secured more than 20 billion transactions across a number of industries. In particular, the financial services industry is where we have our largest presence. Specifically, this includes many retail banks in the United States, which is one of the segments most targeted by cybercrime as well as many of the largest employee welfare and pension benefit plan providers.

In addition to providing technology solutions for our customers, RSA is also recognized for our advanced research and thought leadership in the cybercrime arena. One example of this is the RSA Anti-Fraud Command Center. The RSA Anti-Fraud Command Center is on the forefront of new threat detection and cybercrime intelligence, achieving several milestones including the shutdown of more than 450,000 phishing attacks and 80,000 Trojan attacks across 185 countries. In addition, the RSA Anti-Fraud



Command Center helped launch the first commercial anti-phishing and anti-Trojan services in the industry.

In many respects, the types of attacks perpetrated against employee welfare and pension benefit plan providers are not drastically different than those that target other financial services providers and industries outside of financial services. Like traditional crime, they all usually involve a motive, an opportunity and a means. The first thing to understand is the motivation of a cybercriminal.

Why is the data that is available in employee welfare and pension benefit plans so valuable to a cybercriminal? First, as the old saying goes “because that is where the money is.” The features and functionality introduced by many pension plan providers have made conducting business easier and more convenient for their customers. Unfortunately, the features introduced are also available to any cybercriminal who has taken over a user’s account. This gives them the ability to “cash out” an account with more speed and ease than in the past.

In addition to stealing available funds, these types of accounts are targeted because there is a wealth of sensitive personally identifiable information (commonly referred to as PII) that is typically stored in user’s accounts as well as in the plan provider’s databases. As part of its normal lifecycle, this information is passed along to third parties and within different internal areas of an organization. The more this data is in transit and the more locations it is stored, the higher the propensity to have that information fall into the wrong hands. This could happen due to an attack or simply due to a mistake on behalf of the party handling the data.

Personally identifiable information has a fairly broad utility to a cybercriminal. First, it can be used to commit multiple types of fraud or identity theft, and does not change, even if compromised. Second, the value of personal data to a cybercriminal is much higher than a credit card or bank account number alone. For example, the average selling price for a U.S. credit card in the cybercriminal underground is around \$1.50. But when that single card is sold with a full identity profile, the value can be up to ten times more.

Today, organizations continue to migrate new services to the Internet and store data in electronic format as a way to reduce costs and provide more convenient, self-service options to their users. Despite the security measures taken by some organizations, data breaches, fraud, and cybercrime continue to increase at alarming rates. In addition, cybercriminals are more organized and adaptive than ever; they have the most advanced technologies at their disposal and use sophisticated economic models in the operation of their business. One way cybercriminals are able to innovate and grow is by utilizing the Cybercrime Underground.

For more than five years, an underground network of cybercriminals has been growing in size and sophistication. Employing ingenious strategies and complex technological capabilities, they have been preying on financial services and other organizations and their customers to steal account numbers, credit card numbers, personally identifiable information (PII), and other data that they can use to commit fraud or sell to other criminals in a thriving black market often referred to as the Cybercrime Underground.

The once-popular hacker stereotype of a lone, alienated techno-nerd breaking into an organization's IT systems for fun has given way to a truly frightening reality of coordinated groups of innovative cybercriminals who communicate frequently and strike aggressively. They rely on a range of advanced attack methods and social engineering techniques to steal sensitive data and then cash out in a market where demand is well-publicized and fraudsters are well compensated. While cybercriminals evolved their methods and grew their networks to attack financial services and other organizations and work around security measures that have been implemented, no such gradual escalation is required when targeting new industries and smaller organizations with less protection. The infrastructure exists and the methods are proven – and they are gradually seeking out new targets to attack.

Whether an attack is targeted at a customer's account or an internal employee's account, often the method to achieve access is through social engineering. Social engineering is not a new concept. It's been around since well before computers even existed. However, these techniques have been adapted for the modern age of digital crime. Social engineering tactics use superficial cues to exploit trust, pique human interest, and evoke a strong emotion such as fear, curiosity, or excitement that hinders the victim's ability to think logically, and elicits an immediate response.

By preying on strong human emotions, cybercriminals are able to circumvent otherwise effective technology-based security measures such as firewalls, encryption, anti-virus, spam filters, and even strong authentication and to gain access to systems to steal identities, funds, information, and corporate and government secrets. And, while there is no “technology” at play – social engineering uses no software or “hacking” technology – don’t be fooled: social engineering tactics are sophisticated and rooted in the fundamentals of complex human psychology.

One of the most common social engineering methods still very popular among cybercriminals is a phishing email – a message designed to appear as though it originated from a legitimate person or entity. The purpose is to trick users to click on a link within the email which then directs them to a fraudulent website designed by the criminal that prompts victims to provide their account information as well as other personally identifiable information. In an even more convincing attack, email accounts are hijacked and are used for sending out phony messages to the victim’s contact list. By doing this, criminals can make victims think that these emails are from the actual email account owner, and therefore are more likely to be trusted. Friends and associates trust the source, open the malicious links, and download malicious software (commonly referred to as malware) to their computers. Today’s online social engineer is nothing more than a con man who uses digital methods – such as email – to swindle people’s personal data or to trick them into clicking on a malicious link that downloads malware onto their computers or networks.

Today, with the enormous popularity and growing use of social networking, social engineers have extended this tactic to sites such as Facebook, LinkedIn, and Twitter. They prey on the trust a user has for those within their social circle. For example, when a user on a social networking site receives a message from someone within their network with instructions to view a file or video, the user is more likely to respond to the request since it appears to have come from a trusted source. Additionally, cybercriminals have started to recognize the value of enterprise credentials and proprietary information – moving beyond the data collected and used to commit traditional identity theft.

To exacerbate the problem, not only are cybercriminals getting better at exploiting human behavior for social engineering attacks, they are also increasingly effective at spreading malicious software onto users’ machines. Today’s malware is very sophisticated – capable of stealing personal and financial data

and take over accounts. Types of malware that might be familiar to users include Trojans and Spyware. For just a few hundred dollars, criminals can purchase advanced malware kits in the Cybercrime Underground which gives them the ability to conduct attacks that are much more sophisticated than they could have created on their own.

The malware that is commonly seen used to breach financial institutions is very sophisticated and offers a wide range of features. Some of these include the ability to sit undetected on a user's machine and collect login credentials (and other security information) for all accounts (not just banking accounts) that the user accesses. Other features include the ability to automatically sneak into a user's online account and transfer funds to another account which they control. Then some of the most advanced tools for sale on the black market today have the ability to grab Microsoft Office files and emails from a user's Outlook account. These capabilities are usually completely automated, easily bypass password security checkpoints and go undetected by many standard security tools. For example, the Zeus Trojan, the malware most widely used by criminals to target financial institutions, is detected less than 40% of the time by the major anti-virus engines.

Malware developers in the underground often configure their tools to steal information from a wide variety of companies. But more often, the malware is customized with a list of trigger website addresses designed to attack a specific organization or set of organizations, as is often the case at larger benefit and pension plan providers. In this case, the malware is only activated when a user accesses one of the websites on the list. At this point, the attacker's plan is to gain access to a user's account and drain the account of money and possibly steal as much valuable data they can about that user. If the attacker is unable to directly access a user's account, they will find the least path of resistance. For example, a cybercriminal could utilize the phone channel and socially engineering a customer service representative to reset the passwords on a user's account.

While much of the attack scenarios discussed previously have focused on customer's accounts, we have increasingly seen the division between the consumer and the enterprise is slowly disappearing.

Consumers are also employees, and employees conduct personal business and check personal email accounts from corporate workstations. Similarly, as organizations make access available to a wider array

of resources over the Web via technologies such as SSL VPNs, the variety of computers touching the corporate network expands to include personal machines such as the family computer and even mobile devices.

The dual use of computers for personal and business purposes opens the door for Trojan infections on corporate-issued endpoints and the opportunity for cyber criminals to capture additional data such as VPN credentials that enable access to corporate applications like webmail accounts and other internal resources. As a result, organizations are facing an increased risk of data loss.

Little attention has been focused on the crossover impact and potential risks malware could pose to the enterprise. As organizations, particularly larger ones, have advanced Security Operations programs with clearly defined policies and multiple technologies in place to protect both networks and end users, there is a sense of whether existing security measures are “good enough” to prevent against the threat of cyber attacks. However, the rapid evolution of criminal sophistication has created possible gaps with the current security controls and policies designed to protect corporate resources and monitor employee behavior.

Below are two examples of how a cybercriminal could compromise a benefits and pension plan for financial gain.

- An attacker sends a user a “phishing” email. This is an email that appears to be from their actual benefits provider but is in fact a fake. The email explains to the user that their account needs to be updated immediately and they should log in to ensure their benefits don’t expire. Once the user clicks on the email, it takes them to a site that looks like the legitimate site. However, when the user attempts to access their account, instead of typing their username and password into their benefits site, they are in fact handing them over to an attacker. With the user’s login credentials in hand, the attacker is now free to access the account to transfer funds or steal personal data.

Many of these attacks are automated and built with “delay pages” in between that might send a message to the user such as, “The server is busy. Please try your request later.” This is to prevent a user from becoming suspicious.

Attacks similar to the one that was just described have been around for several years and are not very difficult for skilled attackers. However, attacks like these are still quite popular among cybercriminals to steal financial and personal data. In fact, in July 2011, RSA's Anti-Fraud Command Center detected more than 25,000 unique phishing attacks, the highest number ever recorded by RSA in a single month. In 2010, RSA witnessed a 27 percent increase in global phishing attacks from the previous year.

- In another example, the office manager at a non-profit organization receives an email with an attachment (Note: these types of targeted attack emails are often referred to as “spear phishing”). The fake email was received with an email header announcing “Your package has arrived.” Utilizing social engineering techniques, the employee is convinced the email is legitimate and opens the attachment without giving it much thought. Once opened, the user finds information about a fictitious package shipment scheduled to arrive. What the user fails to recognize though is that after clicking on the link or opening the attachment, the user gets served up with the latest version of the attackers malware on their computer – and most likely without even knowing it. Once activated, the malware steals the user’s login credentials, and the attacker is able to access the employer’s payroll system. This gives the attacker the ability to add several fictitious employees to the payroll system. The fictitious employees however are actually real people that are commonly referred to as “mules” in the cybercrime industry. They act as conduits between the compromised account and the criminal’s account. Another way of thinking about them is to see them as a money launderer. Often mules are willing accomplices, but other times, they’ve been scammed, often via “work at home” job opportunities, into collaborating with the criminals. In this case, not too long after the employee at the non-profit opened the email, the firm had over \$100,000 stolen from their bank account.

These types of attacks are not uncommon and often smaller firms, like the one from this example are targeted. Why? Because generally they are less aware of the threats that exist, have weaker defenses and are more likely to assume that this is a problem that only exists for larger organizations.

Now that some attack scenarios have been outlined the obvious question would be, “What can we do about these attacks?” Unfortunately, there is no “silver bullet” technology that exists. The best defense is the practice of “layered security” also referred to as “defense-in-depth”. The techniques and technologies described below have been used for over five years in the financial services sector and have also been widely adopted in many other sectors including healthcare, retail, and government.

One layer of defense-in-depth security is utilizing strong authentication, or more simply, a way to authenticate a user beyond a username and password. Strong authentication techniques could include issuing security devices, such as a token, or implementing risk-based authentication. A risk-based approach includes looking at a wide variety of factors about a user’s interaction with a site and determines if anything appears to be unusual or suspicious. Factors that could look suspicious could include the location of the user, the time of day they are accessing their account, the machine they are accessing their account from, or suspicious transactions or activities (i.e., adding multiple new payees at one time). In the case of the phishing attack mentioned previously, there is a good chance that even if an attacker stole a user’s password, they would still be blocked from accessing their account due to the increased protection from strong authentication. This is because something about the attacker would have seemed out of the ordinary, perhaps their location, and they would have been asked to provide more information before getting access to the user’s account. Since the attacker would not necessarily have this information, the attack has become much more difficult.

In order to better understand fraud trends and spot suspicious activity, many businesses have increased their collaboration with other organizations and industries to share information and specific details about known attacks. For example, our RSA eFraudNetwork™ community, which is embedded into many of our products, gives our customers a way to anonymously share fraudulent identifiers so that if another organization sees a similar attack, they will know to increase their defenses. This way if an attacker is spotted by one organization they would also be more likely to be caught by all other organizations within the network. This type of collaboration can also exist outside of technology in the form of industry education groups, such as the Financial Service Information Sharing and Analysis Center (FS-ISAC), the Anti-Phishing Working Group (APWG). With the increased interest in the realm of cyber security, many

more resources are available to businesses and consumers to learn about new trends and share insight with other organizations.

Another method that is commonly utilized is employing fraud protection services that specialize in blocking and shutting down attacks. Often, once an attack is identified, organizations are powerless to stop the attack against their customers. The longer these attacks remain active, the greater the cost to an organization and their customers. For example, a standard phishing attack costs an organization about \$400 per victim. This is why monitoring services that specialize in detecting phishing and Trojan attacks and working on behalf of organizations to block access and shut them down are so important. The ability to reduce an attacker's window of opportunity from a matter of days to a matter of hours will greatly limit the impact on an organization and its customers. Additionally, it allows organizations the ability to outsource these specific security skill sets that may otherwise not exist in-house.

A third solution often utilized by financial institutions is the use of identity verification services. These consumer authentication and fraud prevention services confirm a user's identity by utilizing "knowledge-based" authentication. This includes asking users "top-of-mind" questions that are formed based on information contained public, commercially and internally available data sources. Most importantly, the questions are formed based on information that cannot be easily guessed and is not readily available on the Internet. Many financial institutions have deployed these types of services to assure the identities of a user seeking to sign up for a new account or service or attempting to access their accounts via the Call Center where security is often lacking compared to its online counterpart.

Often technology solutions are not bought directly by benefit and pension providers from a vendor. Instead, much of this is outsourced to third party integrators. It is important for organizations to vet these integrators and platform providers to ensure they are offering the proper level of security. Whether the security tools chosen are acquired directly from a vendor or a platform provider, it is important to understand that their security layers need to be implemented properly. So often organizations suffer a breach only to realize later that the technology they have already purchased and deployed was simply not being utilized properly. Worse yet, organizations often knowingly ignore recommended best practices because they don't feel that they would be targeted.

While a strong security posture certainly is critical in reducing risk and the cost associated with a cyber attack, social engineering tactics are designed to bypass the technical aspects of a security strategy and exploit the weakest link in an organization's security – the human user. One way to combat this is to increase security education and awareness campaigns. Since human beings are often the first, and weakest, line of defense in an organization, their ability to spot social engineering techniques and practice proper security hygiene can go a long way in helping to thwart attacks. This doesn't mean that criminals can't adapt their methods to a user's knowledge or launch sophisticated social engineering attacks that are harder to detect; however, those organizations and users that remain uneducated are the weakest prey and are the "lowest hanging fruit" for the cybercriminal.

Training users with examples of what to look for in a social engineering scam is a good way to help users identify social engineering attacks. Training should include clues that warn of a phishing email such as threatening or other strong emotion-invoking messaging. Users of all levels need to be trained.

Executives, in particular, tend to be easy or "soft" targets, often untrained and unaware of social engineering tactics, and more vulnerable to more sophisticated, targeted attacks because of the access that they have to highly sensitive corporate information and systems.

One of the most effective methods of reducing the impact of social engineering-based cyber attacks is embedded training that actually "test" people in real-time with live examples of phishing – and micro video games that give people the opportunity to have fun as they "practice" identifying potential scams.

Regardless of the type of training, at a minimum, organizations need to establish best practices for avoiding processes that are abused by social engineering scams – and update these best practices as the social engineers adapt and evolve their tactics. Social engineering attacks are becoming more of a problem not just among consumers, but in the workplace as well. Forty-five percent of employees state they have received some form of phishing email in their corporate inbox. In the end, user education and awareness are crucial and part of the first lines of defense in diminishing the impact of social engineering-based cyber attacks.

In order to defend against attacks aimed at the enterprise, security officers not only need to understand the methods but also the motivations of attack. First, they must understand what their “crown jewels” are - the most sensitive data within their environment. Second, they must understand where that data is and how it can be accessed. Then, they must provide controls to protect that data whether it is at rest or in-transit. The more sensitive and important the piece of data, the more focus needs to be spent to ensure its protection. CISOs and other security professionals need to ask several important questions such as:

- What is the value of my data that is potentially being put at risk?
- How much do I know about my remote employees’ activities?
- How can I be sure it is a legitimate employee performing the activities I am monitoring and not a cybercriminal?
- How much insight do I have to what data is flowing in and out of my network? Do I have tools such as network monitoring and data loss prevention solutions that can help provide insight and protection? Do I have analytical tools to research attacks after they have happened?
- What level of education is necessary to provide to my employees about online threats and the risk their activities pose to the organization? Have we provided this level of training?
- Is the most sensitive data in my environment encrypted? Is it protected by strict access controls and strong authentication?
- Do I collect and analyze logs of all security events that occur in my environment?

These are just some of the questions that CISOs need to be asking as part of assessing their established policies and controls and to identify any gaps that may exist in their current infrastructure. Once these controls and policies are established, the work is not done. They need to be continuously monitored to ensure they are being met. Often, organizations employ enterprise Governance, Risk and Compliance tools to help keep track of their environment and their controls. These tools help determine what their security posture is at a given moment, what vulnerabilities exist, what remediation efforts need to occur, and how they are tracking versus any regulation and guidance for which they are subject to adherence.

If the Council is looking at others with respect to defining policy, I would recommend referring to policy created in the financial industry, which has been working on creating frameworks to secure online transactions for several years. Specifically, I would refer to the Federal Financial Institutions Examination Council (FFIEC) Guidance issued in 2005 (*Authentication in an Internet Banking Environment*, [http://www.ffiec.gov/pdf/authentication\\_guidance.pdf](http://www.ffiec.gov/pdf/authentication_guidance.pdf)) which mandated increased account protection without committing to a specific technology. In June 2011, the FFIEC issued a supplement to the original guidance. According to the FFIEC, “The purpose of the supplement is to reinforce the risk-management framework described in the original guidance and update the FFIEC member agencies' supervisory expectations regarding customer authentication, layered security, and other controls in the increasingly hostile online environment.” (*Federal Financial Institutions Examination Council. (2011). FFIEC Releases Supplemental Guidance on Internet Banking Authentication [Press release]. Retrieved from <http://www.ffiec.gov/press/pr062811.htm>*)

Not only has the FFIEC Guidance created a framework to secure transactions and defend against cybercrime, but it did so in a way which allowed the financial industry to choose a security strategy that is appropriate given their level of risk, user acceptance and corporate resources. When creating policy in the security space, this is a key tenement. Otherwise, the policy could end up mandating security that has become outdated or simply doesn't address the specific security needs of the implementing organization.

On behalf of myself and my colleagues at RSA, The Security Division of EMC, I want to thank the Council for allowing me the opportunity to speak about these important issues. Even though we have just scratched the surface of the threat landscape and the security countermeasures that can be implemented, we hope that our insight and collaboration with the Council will help spread awareness and increase the general level of protection for the American public.