ANMTA

2015 Spring Conference

May 14, 2015, Albuquerque, New Mexico

Electronic Banking

Presented by: Nathan Paden, C.P.A.

Bolinger, Segars, Gilbert & Moss, L.L.P.

Electronic Banking

Today we will discuss some of the advantages of electronic banking as well as common pitfalls, crime trends, internal control deficiencies, insurance coverage, and other problems relating to electronic banking and payment processing.

Electronic Banking

Most of us understand the advantages to Electronic Banking. The biggest of which is simply convenience.

24 hour access, not having to physically go to the bank, efficiency, etc.

New innovations, paying via an email account, transferring money with your cell phone through an app, even via a text message.

Electronic Banking

The biggest pitfall that most of us fall into is thinking that our money is safe.

That's what banks are for, right? To keep our money safe.

Electronic Banking

In the past, thieves stole money from the bank, not from individual account holders.

In the past, thieves physically took the money and everyone knew what was happening immediately.

That has changed. Thieves are now stealing from individual account holders who often don't even realize what is happening until it is too late.

Electronic Banking

According to a recent report by McAfee, a part of Intel Security, they estimate that the likely annual cost to the global economy from cybercrime is more than $400 billion!

Most companies underestimate how much risk they face from cybercrime and how quickly this risk can grow.

Electronic Banking

Most cybercrime incidents go unreported.

When a major US bank lost several million dollars in a cyber-incident it publicly denied any loss, even when law enforcement and intelligence officials confirmed it in private. Few of the biggest cybercriminals have been caught or, in many cases, even identified.

Electronic Banking

These crimes are carried out by professional gangs, some with significant organizational abilities. There are several cybercrime groups in the former Soviet Union that have “nation-state level” capacity. These groups have repeatedly shown that they can overcome almost any cyber defense. Financial crime in cyberspace now occurs at an industrial scale.

Electronic Banking

Cybercrime produces high returns at low risk and (relatively) low cost for the hackers.

Companies and individuals make decisions on how to manage the potential for loss from cybercrime by deciding how much risk the are willing to accept and how much they are willing to spend to reduce that risk.

Electronic Banking

In a case that became known as Trident Breach, hackers stole $70 million from the payroll accounts of some 400 American companies and organizations – all from the safety of their homes in Eastern Europe.

Electronic Banking

In the Trident Breach case, the hackers were able to get their hands on the cash by turning people into money mules.

They created some 3000 money mules, many of them unwitting Americans, by luring them into work-at-home jobs requiring "employees" to open bank accounts.

Electronic Banking

Often mules will open a bank account one day and the first transaction to hit the account will be a fraudulent EFT from a victim's bank.

Generally, these deposits range from $7,000 - $9,000.

Immediately after the money hits the account the mule will transfer the money electronically or withdraw the money in cash.

Electronic Banking

“The first money mule activity we started seeing was people who would receive an email saying, ‘You can get a work-at-home job’ and the work-at-home job would be something like transaction manager for an international company,” said Prof. Gary Warner of the University of Alabama at Birmingham, who teaches a program that combines computer forensics and justice studies.

Electronic Banking

Warner said the hackers transferred cash from business payroll-type "ACH" (Automated Clearing House) accounts to the mule accounts and the mules sent the cash by Western Union or MoneyGram to Eastern Europe, taking an eight or ten percent commission.

Electronic Banking

Warner said that when the banks started to get wise to the hackers' work-at-home schemes and set up roadblocks, the hackers then recruited dozens of students, mainly from southern Russia, to be a new breed of money mule.

Electronic Banking

The hackers obtained fake passports for the students, U.S. J1 work/study visas, and packed their new mules off to the United States. The students opened multiple bank accounts, mainly in the New York area, where they received stolen cash. Then, just as the mules before them had, they wired the cash back to their bosses.

Electronic Banking

This type of fraud is growing more and more common and is going to continue to get worse.

Referred to as a fraudulent electronic funds transfer (EFT) transaction.

Electronic Banking

First, a cybercriminal uses a software tool to gain control of the victim's computer from a remote computer. Often without the user even knowing they are infected. The criminal then uses an EFT to move most, if not all, of the money in the victim's bank account to one under his or her control, often costing the victim tens, if not hundreds, of thousands of dollars.

Electronic Banking

The increasing scope of this fraud prompted the FDIC to issue an alert warning about it in 2010.

According to the FDIC alert, the number of frauds has increased, as well as the size of losses, resulting from cyber thieves' stealing login credentials and using them to carry out unauthorized EFTs, which include Automated Clearing House (ACH) transactions and wire transfers.

Electronic Banking

"But wait, we are just a small company in a small town, this kind of thing doesn't happen here."

A 2011 study by Javelin Research showed that Cybercrime Losses by Small and Medium Sized Businesses (SMBs) go well beyond previously reported data.

Electronic Banking

SMBs have become an attractive target for cybercriminals because they tend to have more money than individuals, yet they seldom have the time, skills, or finances to build defenses that are as effective as those of larger businesses, Javelin states.

Electronic Banking

According to Javelin's "2011 Small Business Owners Identity Fraud Report,"

Fraud targeted at SMBs and their owners totaled more than $8 billion in 2010. Banks, merchants, and other providers absorbed at least $5.43 billion of that loss, while the cost to victims was $2.61 billion.

Electronic Banking

The losses include not only the financial losses themselves, but also costs associated with data theft, such as attorney fees, time to repair the damages, and the cost of opening new accounts, etc.

Electronic Banking

Javelin also found that SMB owners sustain greater losses through fraud than their online consumer counterparts.

"For SMBs, there's no 'zero liability' agreement with creditors as there is for most consumers, SMBs may be held liable for fraud losses, at a huge cost to their businesses."

Electronic Banking

“Wait a second, my money is covered by FDIC, if it is stolen I’ll just file a claim and get my money back right?”

Nope. While in most cases, individuals are covered from Cyber-Fraud losses under Federal Reserve Regulation E, many banks do not protect “Commercial” account holders from losses.

www.yourmoneyisnotsafeinthebank.org

(That is a real URL)

Electronic Banking

“Well, we’ve got insurance coverage for that don’t we?”

Don’t be so sure, many companies have insurance coverage for electronic records, network downtime, etc., but often these policies are geared toward liability if someone steals information from you rather than someone stealing money out of your bank account.

I would strongly encourage you to verify your coverage specific to cyber theft.

Electronic Banking

Even if you do have insurance coverage, dealing with the aftermath of cyber theft is costly.

Disruption of normal payment processes, closing and opening new bank accounts, stress on banking relationships, cleaning your network of malware, possibly weakening internal controls while temporary payment methods are in place, etc. are all issues that have to be dealt with as a result of experiencing cyber theft.

Electronic Banking

To understand how to safeguard against EFT fraud, you need to understand how it typically works.

The next several slides were taken from an article in the Journal of Accountancy in October 2010.

http://www.journalofaccountancy.com/Issues/2010/Oct/20092174

Electronic Banking

The scheme has basically three steps: (1) illicitly acquire the login credentials, (2) covertly gain unauthorized access to the victim's computer to avoid the bank's security features that are activated when it does not recognize the login "fingerprint," (This is referred to as a "Man in the Middle" attack) and (3) transfer the victim's bank funds to an account the cybercriminal controls.

Electronic Banking

In the first step, credentials are usually compromised by using a malicious program distributed as an e-mail attachment, unintended web browsing download, or file transfer of a seemingly legitimate/innocent file. The user inadvertently allows this malicious program (for example, a “Trojan horse”) to be downloaded and executed.

Electronic Banking

The attacker then can use the program's keystroke-capturing functionality to capture the organization's bank account information, banking credentials, and online activities (for example, EFT transactions). The user of the compromised computer is usually unaware that anything malicious has occurred. These Trojans can be more advanced than even the latest up-to-date antivirus software from the most popular providers.

Electronic Banking

Bank security systems use a technique that can be described as a “fingerprint” to authenticate customers for online banking. It is basically a snapshot of one or more computer/IT features such as an IP address, cards attached internally to the computer, and other technical aspects of the system that are accessible from the computer’s memory. Those are read by the bank’s system to create a relatively unique set of technology features. The fingerprint is saved when the customer registers with the bank.

Electronic Banking

At any login, the bank's authentication system takes a snapshot of the computer logging in to the system, matches that fingerprint against the one on file, and if it is substantially the same, the system assumes the user is authentic. If it does not match, the bank's authentication system adds a layer of authentication by asking a security question or using an alternative authentication procedure (for example, a personal identification number (PIN) sent to a previously arranged cell phone or e-mail account)—which again was established by the customer during the account setup process.

Electronic Banking

In the second step, the cybercriminal hijacks the victim's computer system to use it as a trusted source to avoid the security of the fingerprint, and to allow the fraudster to conduct a fraudulent EFT. The criminal uses a hacker tool (software) to hijack the system.

Electronic Banking

If the criminal simply stole the credentials and tried to log in from his or her own computer, that would lead to another layer of authentication (that is, fingerprints do not match) that the criminal would likely be unable to compromise. But the bank's system recognizes the login from the victim computer's fingerprint, does not sense a need for further security measures, and mistakenly allows the unauthorized user to access the account.

Electronic Banking

Once logged in and authenticated by the bank's security system, the criminal proceeds to the last step. He transfers out most, if not all, of the funds in the victim's bank account, usually via wire transfers, and typically sends the funds to individuals known as "money mules." Mules are often recruited through common online help-wanted job sites, and, in most cases, are unaware that the activity they are performing is related to a crime, usually under the impression that they are working for some legitimate business, such as a marketing company.

Electronic Banking

The criminal wires the mule amounts just under $10,000, to avoid Bank Secrecy Act requirements to file a Currency Transaction Report (CTR) for deposits of $10,000 or more and thus avoid potential immediate detection. The mule is instructed to keep a small amount (usually $500 or less) as compensation, and then to transfer the remainder to an account specified by the criminal.

Electronic Banking

That account is typically an offshore account in a safe harbor for the crook (for example, the funds may be transferred to a foreign country uncooperative with the FDIC and U.S. banks, such as Latvia or Ukraine), usually preventing recourse by the bank to recover the funds.

Electronic Banking

The primary hope of recovery is that the bank will be able to reverse the wire transfer. The Uniform Commercial Code (UCC) requires banks to make a best effort to recover the funds. But there is a catch: Section 202 of Article 4A of the UCC says that "a payment order received by the bank is effective as the order of the customer, *whether or not authorized*, if … the bank proves that *it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer* …" (emphasis added).

Electronic Banking

If the fraud can be traced to a security breach in the victim's computer (for example, malware or hijacking program), the bank may be able to avoid responsibility for the recovery of the lost funds. The bank also may find that the customer is not in compliance with its security authentication procedures, which also impairs the victim's ability to recover lost funds.

Electronic Banking

The bank must explicitly agree in advance to be liable for damages from EFT fraud before recovery is generally possible. Even if the bank makes a best effort to recover the funds, it may be impossible for the bank to recover anything, leaving the victim to suffer the loss. Therefore, the bank seldom gets stuck with a loss from this EFT fraud. Even lawsuits by victims against banks are difficult because of the UCC rules, the fact one cannot sue the overseas bank involved, and the resistance likely to be encountered by the bank's attorneys.

Electronic Banking

I could provide a laundry list of companies that have recently been affected by fraudulent EFT transactions, some with losses in the millions of dollars, but often folks still think that it couldn't or won't happen to them.

Well, it does! In the last year we have had several of our clients affected by fraudulent EFT transactions and are aware of several other SMBs that have been hit.

Electronic Banking

In the fraudulent EFT hits that we are aware of, the cyber criminals had an intimate knowledge of the banks controls and notification features to the extent that they modified existing payees instead of adding new ones which would have prompted a notification.

Electronic Banking

The users that had their access credentials compromised were intelligent, savvy users that had knowledge of typical phishing schemes.

They were running up to date anti-virus software from one of the more popular companies behind the latest and greatest firewall.

Electronic Banking

They were not using a key fob at the time, however it is important to note that using a key fob is not as effective as you would think.

Electronic Banking

Genlabs Corp., a California chemical manufacturing firm, lost nearly $437,000 after cyber thieves broke into its bank account and sent transfers to roughly 50 different money mules.

The attackers succeeded despite the fact that the company's bank requires the user to enter their password in addition to the output from a key fob that generates a new six digit number every 60 seconds.

Electronic Banking

“Okay, you finally have us scared.

What should we be doing to prevent and detect EFT Fraud?”

Electronic Banking

Dedicate a computer or system for online banking, especially EFT (ACH transactions and wire transfers).

Some even suggest running that computer on an operating system other than Windows to allow an even larger layer of protection against viruses that are typically geared toward Windows operating systems.

Electronic Banking

Use a “run as needed” bootable CD (such as the Linix operating system) that cannot be contaminated by a virus or malware for the computer accessing online EFT. This is an FDIC recommendation.

Electronic Banking

The dedicated computer should also not be used for e-mail, web browsing, or other high-risk online activities associated with contracting malware infections, but only for online banking.

In addition, all critical activity around this system should be logged and monitored.

Electronic Banking

Use multifactor authentication with independent mechanism (for example, require login credentials and a temporary PIN sent to a pre-determined cell phone or pager device; login credentials plus swipe card; etc.).

As mentioned earlier, this isn't a failsafe, but it is an additional layer of protection.

Electronic Banking

Segregate EFT controls. For example, one person performs online EFT function (ACH transactions and wire transfers), and a second person approves the transfer or verifies/reconciles that transaction.

One user should not be able to initiate and authorize a transaction no matter what.

Electronic Banking

Dedicate clearing accounts using “just-in-time” deposits. For example, set up a separate bank account for EFT transfers (ACH transactions and wire transfers), and make deposits (or online transfers from a different computer) into that account just before a wire transfer occurs. The risk is limited to a very brief time frame when money is available in the clearing account.

Electronic Banking

Make sure ACH origination is not allowed on the other accounts.

If possible, work with your bank to allow an outside verification of any transfers between accounts, specifically transfers into an account with ACH payment capabilities setup. An “out of band” method is preferred.

Phone call or fax would be best.

Electronic Banking

Log and monitor key computers or systems.

Reconcile EFT transactions daily.

Review all banking activity for anything suspicious. (very small deposits under $1 can mean someone is verifying the account for future withdrawals)

Electronic Banking

Most people tend to setup a process and then forget about it. Most business have been direct depositing payroll checks for decades and still have the same procedures in place that they did when they first set it up.

Hopefully your bank will have implemented numerous security features since then that you should be able to begin using.

Electronic Banking

Review all notification features and use them. Most banks will allow notification to be sent for adding new payees, a new IP logging on, incorrect passwords being guessed, etc.

These aren't going to necessarily prevent a fraudulent EFT transaction from occuring, but it should help you detect it as soon as possible.

Electronic Banking

Controls designed to combat the prevalent distribution of malware should also be considered. All systems, especially the computer used to conduct online banking, should be protected by a firewall and monitored with updated antivirus and malware protection.

Electronic Banking

A key to prevention is to have adequate protection against a malicious keylogger being planted on a computer. Company management should make sure that security software is updated. Firewalls must be able to detect viruses, spyware and other malware. Trojan horse programs used to perpetrate these crimes are often difficult to detect and remove.

Electronic Banking

There is also targeted malware which is very effective in certain key verticals.

Being small does not make a business less of a target – in the game of spreading botnet infections, size doesn't matter – the criminals just want in.

Electronic Banking

End-users lacking education on cybercrime risks can undo all the security protection in place with a single click.

It’s very important to raise all employee awareness of basic security and should probably come up with a formal policy to distribute to all employees.

Electronic Banking

Often thefts are timed to allay suspicion. Cyber criminals begin stealing during the window of time SMBs are not using the account and may not notice any activity for a while.

Late afternoons, transfers to banks in earlier time zones, etc.

Electronic Banking

A few last minute thoughts to help convince you that you need to implement procedures to strengthen your electronic banking controls.

Electronic Banking

$100 billion, a “low estimate” of what cybercriminals earn worldwide per year, is able to finance the most brilliant hackers and social engineers.

This is Organized crime, many cyber criminal syndicates are spending millions of dollars on research and development.

Electronic Banking

Once a workable malware or middleware software is developed, the criminals will sell the software to other criminals to recover development costs.

Many new cybercrime tactics are entirely automated so return-on-investment is irrelevant.

Electronic Banking

Shawn Henry, who left the FBI after more than two decades with the Bureau, said in an interview that the current public and private approach to fending off hackers is "unsustainable." Computer criminals are simply too talented and defensive measures are too weak to stop them, he said.

From Wall Street Journal Online

http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html

Electronic Banking

Mr. Henry said companies need to make major changes in the way they use computer networks to avoid further damage to national security and the economy. Too many companies, from major multinationals to small start-ups, fail to recognize the financial and legal risks they are taking—or the costs they may have already suffered unknowingly—by operating vulnerable networks, he said.

Electronic Banking

Mr. Henry said FBI agents are increasingly coming across data stolen from companies whose executives had no idea their systems had been accessed.

"We have found their data in the middle of other investigations," he said. "They are shocked and, in many cases, they've been breached for many months, in some cases years, which means that an adversary had full visibility into everything occurring on that network, potentially."

Electronic Banking

The FBI's Mr. Henry said there are some things companies need to change to create more secure computer networks. He said their most valuable data should be kept off the network altogether. He cited the recent case of a hack on an unidentified company in which he said 10 years worth of research and development, valued at more than $1 billion, was stolen by hackers.

Electronic Banking

He added that companies need to do more than just react to intrusions. "In many cases, the skills of the adversaries are so substantial that they just leap right over the fence, and you don't ever hear an alarm go off," he said. Companies "need to be hunting inside the perimeter of their network," he added.

Electronic Banking

Companies also need to get their entire leadership, from the chief executive to the general counsel to the chief financial officer, involved in developing a cyber security strategy, Mr. Henry said. "If leadership doesn't say, 'This is important, let's sit down and come up with a plan right now in our organization; let's have a strategy,' then it's never going to happen, and that is a frustrating thing for me," he said.

Electronic Banking

The advantages to electronic banking are clear and they are here to stay.

By strengthening your procedures relating to your electronic banking you can minimize the risk and still enjoy that convenience.

If you haven't been hacked, be very thankful, but odds are that it is going to happen. Please do what you can to limit your risk of loss.

ANMTA

2015 Spring Conference

May 14, 2015, Albuquerque, New Mexico

Electronic Banking

Presented by: Nathan Paden, C.P.A.

Bolinger, Segars, Gilbert & Moss, L.L.P.