Minimizing Risk and Liability from Man-in-the-Middle Attacks (or, How to Keep Your Company's Wire Transfers from Going Awry)

Written by Christopher Escobedo Hart, Colin J. Zick, Nicholas C. Theodorou

May 2, 2019

Imagine this scenario: you've had a productive and mutually advantageous ongoing contractual relationship of several years with another party. You have built up quite a bit of trust over the years, and communicate regularly over email. Your email communications include you receiving invoices and then confirming payment; your email messages might include a note about an upcoming shipment or provision of services, or even a note wishing the family well.

One day, you receive a request: "Can you please change the wiring instructions? We just switched bank accounts – the new instructions are attached. Thanks." Thinking nothing of it, you do so.

Sometime later, you get another email: "When can we expect payment? We should have received the wire a week ago." You could have sworn the payment went out, and so you double-check; sure enough, the payment was sent the same day of the month it always is. You respond with a PDF of the wire confirmation. And then you receive this response: "That's not our bank account. You still owe a payment.

What Happened?

Scenarios like this one are increasingly common. Often referred to as a man-in-the-middle attack, or a payment fraud hack, it can prove difficult to minimize the loss after the attack occurs. Here at Foley Hoag, a man-in-the-middle attack has crossed my desk half a dozen times over the past twelve months. In this essay I hope to give you an understanding of what these attacks are and why they happen; how to minimize the risk that you suffer such an attack; and what steps you can take to navigate the fallout should such an attack occur.

Anatomy of a Man-in-the-Middle Attack

A man-in-the-middle attack is what is sounds like: a third party (often part of a larger criminal enterprise) inserts himself in the middle of the communications between counterparties, poses as one of the parties, and successfully diverts one or more payments to a beneficiary bank never identified in the original transaction. Once payments are successfully diverted, the same third party empties the account, and disappears. The counterparties are often unaware of the fraud until days, weeks, or even months later, depending on the attack's sophistication.

How does the man-in-the-middle actually get in the middle? Often through a simple spear-phishing attack. "Spear-phishing" is a targeted form of phishing – that is, an attempt to send malware to a specific party, often by posing as someone you know through the use of email spoofing. The perpetrator of a spear-phishing attack will usually use a spoofed account and asking you to open an attachment, in order to gain credentials or access to a system. The spoofed account might look something like Johm.Doe@google.com, replacing the "n" in "John" with an "m," a change one would normally never spot in the ordinary course of email communications.

In other words, man-in-the-middle attacks prey on trust and on the shortcuts that the human mind may take on a regular basis. It is a kind of "social engineering" attack: attackers assume that the people engaging in transactions over email trust each other, and that the counterparties won't check email addresses in the "From" line carefully. That assumption is often correct.

Once the malware is installed through a successful spear-phishing attack, the attacker can access the victim's email account, allowing the attacker to read through emails to understand the course of the relationship. The attacker uses this knowledge to plan the payment fraud attack, eventually inserting himself in the middle of the relationship by impersonating the parties. He will send information about a new

beneficiary bank to the payor, and will simultaneously distract the payee by sending messages that (for example) the payment is late, or some other diversionary tactic to keep the payee from investigating or asking the payor direct questions. Payment will be sent to the third party account, the attacker will continue to distract the parties while the account is drained, and then eventually the parties will figure out what happened, with the damage already done.

Mitigating the Risk

Man-in-the-middle attacks are possible because of trust, and because parties are not necessarily trained to spot "red flags": a phishing attack, an odd-looking email, even odd and out-of-character grammar and syntax in an email. There are some ways you can mitigate risk:

- **Verification.**Orally verify any change in the transaction process. If your counterparty, who has been using a Bank of America account based in New York for years, suddenly asks you to switch your payments to ABC Bank in Hong Kong, pick up the phone and verify the change. That should often be enough to thwart the attack. (Although not always – some very sophisticated hackers have been able to get in the middle of phone calls, too.) It is even better to make this kind of oral communication a regular habit, and to find ways to minimize email traffic concerning payment.
- **Vigilance.**Be vigilant about phishing attacks and take steps to verify email accounts. This should be a matter of good day-to-day cyber-hygiene.
- **Training.**If you have an accounting and finance department, make sure these employees are appropriately trained to both spot such attacks and to be skeptical of requests to change the ordinary course of a transaction.

Controlling the Fallout

If you discover you have been the victim of a man-in-the-middle attack, on either end, there are four things you should be immediately concerned about:

- **System compromise.** A successful man-in-the-middle attack likely means that a third party was able to gain credentials or infiltrate an email system with access to other sensitive information. You should immediately investigate to what extent your system or systems have been compromised in order to understand the scope of any breach and to remediate the compromise. An investigation should also reveal whether the compromise likely happened on the side of your counterparty, providing you with potential legal arguments and defenses.
- **Insider fraud.** While man-in-the-middle attacks normally implicate third party criminals, you cannot rule out the possibility that a disgruntled or dishonest employee has been involved in company theft. You should take steps to rule this out, through an internal investigation if necessary.
- **Law enforcement.** Whether the criminal is an insider or an outsider, alerting law enforcement (usually the FBI) can often be critical, for a few reasons. The first is that law enforcement often has tools at its disposal to kill the transaction if it is caught early enough (usually within 72 hours). The second is that law enforcement can often tell you whether the attack affecting you is linked to some other specific criminal activity, and can connect the attack that happened to you to other attacks, potentially to your benefit. The third is that, depending on the circumstances, contacting law enforcement quickly can demonstrate your efforts at mitigating any loss should there be ensuing litigation.
- **Notification.** You will want to notify your bank and the beneficiary bank immediately regarding the fraud. Public companies as well have separate SEC reporting obligations, as do companies in certain states (such as New York). A broader compromise might also trigger additional notification obligations.

Managing Liability

The liability issues that stem from payment fraud hacks can be tricky, and the legal questions are still novel. This is an evolving area with limited case law.

The legal issues involved normally sound in contract. To be the payor in such an incident means that you are in danger of paying double the amount (one to the cyber-criminal, and one to the counterparty). Case law is not favorable to the payor in such circumstances: some courts have said that even though the payor has provided payment in good faith, the payor is still in breach. While this is good news for the payee, to be the payor means you must think creatively about how to avoid being on the hook for a double payment.

A contract-based defense might be located in a force majeure clause that covers the acts of a criminal third party (something you should consider at the contracting stage). Contracts can also specify payment terms (such as what accounts must be used) that can shift risk and liability. There are also analogies one might draw to the UCC, which can allow for avoidance of a payment under the so-called "imposter rule" (making the party last or most able to avoid the fraud the one liable for bearing it).

Tort-based defenses such as negligence on the part of the payee might also be available. Here, the facts of the fraud matter greatly. The payor might be able to demonstrate that the payee, and not the payor, caused the harm, especially where a spear-phishing attack affected the payee (and not the payor) and the payee did not have adequate controls to spot or prevent the attack.

Finally, while you should check your insurance policy, you should know that insurance policies as currently written often do not allow for recovery under this kind of circumstance. Policies often require the direct manipulation of a transaction by an employee or an agent for purposes of recovery (as opposed to a third party directing a fraudulent transaction, normally not a basis for recovery). Case law is also not helpful for companies trying to recover, often finding for the insurer when disputes arise under these circumstances. Before such an attack happens, review your policies to understand the potential scope of coverage, and investigate whether additional coverage is needed or can be obtained.

Conclusion

While the law is slow to react to new realities, attackers have already quickly discovered the potential goldmine opportunities that can come from a successful man-in-the-middle attack. Think about how you manage your transactions, be skeptical and vigilant, and if you are a victim, act quickly to minimize your losses.

RELATED INDUSTRIES

- Healthcare
- Life Sciences
- Energy & Cleantech
- Technology
- Investment Advisers & Private Funds

RELATED PRACTICES

- Cybersecurity Incident Response
- Privacy & Data Security
- Healthcare
- Business Counseling
- Litigation
- White Collar Crime & Government Investigations
- State Attorney General Investigations
