DREW & NAPIER

DREWTECH SERIES

CHAPTER 15

Looking at the Man in the Middle (in a cyber breach) – allocation of risk

5 March 2025

LEGAL UPDATE

In this Update

While cyberattacks relying on technological advances become increasingly common, the weakest point of any system often remains the well-intentioned but occasionally unintentionally bumbling human actors. This article looks at a venerable attack in any threat actor's toolkit – the man-in-the-middle attack – and the legal implications arising therefrom.

INTRODUCTION

Cyberattacks utilising sophisticated technological tools have become increasingly common with developments such as ransomware-as-a-service and the general proliferation of advanced penetration tools. However, it remains a fact that the humans in the system remain a particularly vulnerable attack surface – unsurprising given that for as long as there have been honest men doing honest business, there have been unscrupulous individuals trying to profit at their expense (and pass off poor copper as good). Recent reports suggest that as many as 83% of all cyberattacks start as a phishing attack, where the attacker pretends to be someone they are not to obtain some kind of benefit for themself.

One attack of considerable vintage which is often used to great effect by attackers is the man-in-the-middle attack. The effectiveness of the attack lies in its simplicity. The attacker covertly intercepts and relays communication between two parties who believe they are interacting directly. By inserting themselves between the victim and the intended recipient, the attacker can eavesdrop, steal sensitive data or alter transmitted messages. The repercussions can be severe, ranging from identity theft and financial fraud to unauthorized access to confidential systems.

A classic implementation is as follows:

(a) Two parties Alice and Bob are in a commercial relationship with Alice regularly providing services to Bob and regularly receiving monies from Bob. Alice is in the habit of using an email address alice[at]alice.com to communicate with Bob.

(b) An attacker Chuck becomes aware of this relationship, and sends an email from alice[at]alice.com (did you notice the “l” was replaced by an uppercase “i”?) to Bob with an invoice asking for payment. The invoice provides details of a bank account controlled by Chuck. Bob, none the wiser, pays on the invoice to Chuck.

(c) Some time later, the real Alice, who has not been paid, angrily asks Bob for money for services rendered. Bob, confused and disoriented, says that he has already paid. Befuddlement abounds. Chuck has long fled.

LEGAL ALLOCATION OF RISK

In the scenario above, Alice and Bob are left with a foul taste in their mouths, both being victims. However, they must still allocate the loss between them.

The UK courts have had the opportunity to consider these very issues (proof indeed that this scenario is far from academic). In summary, Bob would typically be the party left holding the baby.

In *J Brazil Road Contractors v Belectric Solar Ltd* [2018] WL01 993147, the customer had paid on invoices which it thought had been sent by the vendor. However, IT investigations suggested that an attacker had gotten control over the email address used by the vendor. The vendor therefore never received payment, and sued. The court decided the attacker communicating through the compromised email address was not the vendor nor the vendor's agent. It was *"well known that emails are not secure; they can be hacked and even if you are a contender for the US Presidency"*. The vendor had not represented that its emails would be secure. The customer was therefore still liable to the vendor for payment.

A similar situation arose in *Sell Your Car With Us Ltd v Sareen* [2019] EWHC 2332. In that case:

(a) Sell Your Car With Us Limited ("***SYCWU***") agreed to sell Mr. Sareen's *"Maserati Levante"* vehicle for a fixed fee. After selling the vehicle, SYCWU was obliged to pay Mr. Sareen £51,800.

(b) Mr. Sareen originally communicated with SYCWU using an email address ending with *"1[at]gmail.com"*. The contract between SYCWU and Mr. Sareen provided that Mr. Sareen consented to receive all documents *"exclusively through electronic means"* and that any change of Mr. Sareen's email address had to follow a prescribed procedure.

(c) It transpired that during the course of the transaction, an email was sent from an email address ending with *"01[at]gmail.com"* to SYCWU, purporting to be from Mr. Sareen. The email signature was almost the same save that the words *"Sent from my wireless device from an unknown location in our Solar System"* appeared on just two lines, whereas it was usually spread closer to the left-hand margin and across three lines. Crucially, the banking details in the email had been changed.

(d) SYCWU noticed that the bank details were not the same as those previously provided, and sought clarification. Unfortunately, SYCWU continued corresponding over email with

what in retrospect was the attacker. Eventually, SYCWU paid out monies to the changed banking details.

(e) Mr. Sareen, not having been paid, sought to wind up SYCWU. SYCWU argued that Mr. Sareen should have been obliged to exercise reasonable care over the security of his email account, or had represented that he would do so.

(f) The Court disagreed with SYCWU. In the absence of an express contractual clause, there was no duty that Mr. Sareen should have been obliged to exercise reasonable care over the security of his email account. Mr. Sareen had also not represented that he would exercise reasonable care over the security of his email account. In fact, SYCWU had its own security procedures which had not been complied with. SYCWU was *"alone responsible for sending money to an unauthorised account on instructions received from an unknown third party"*.

ACTIONABLE STEPS AND CONCLUDING THOUGHTS

The foregoing cases appear to cast a pallor over the use of email communications, an alarming idea given the ubiquity of email as a means of communication. However, it is nigh impossible to give up the convenience of email. What then can organisations do to protect themselves?

There are obviously technical workarounds to this problem, but these may increase cost or not be commercially appropriate. Instead, one option is to instead contractually allocate the risk between parties.

In this case, parties could pre-agree that a certain form of communication is conclusive and binding, and any instructions provided or messages delivered through that form of communication are binding on the party controlling their end of the communication framework. Parties will require each other to represent that they will keep secure their ends of the communication framework, and that the other party is entitled to rely on any message thereby received.

This however may not address the situation where there is no email compromise, but rather interception of email communications between the parties (as in the case of Alice, Bob, and Chuck). In this case, another option is for parties to also pre-agree that certain instructions may not be conveyed via a potentially insecure communication protocol. For instance, parties can agree that any change in banking details will never be communicated over email, but only via a video-call which will be followed up by a written letter delivered by registered mail (but see recent developments where

attackers have begun using AI-generated fake videos to pretend to be the management of a company for phishing attacks).

Internally, staff need to be trained to spot attempts by attackers to infiltrate the conversation. Policies need to be developed, and equally importantly, complied with. Protocols and processes should be established to deal with matters of importance such payments and procurement (such as doing callbacks or using other non-electronic means to ensure and verify that payment details which have been provided are accurate), with unauthorised commitments and other off-the-books transactions treated severely to ensure that the organisation is protected.
Given the very real and present risk of a man-in-the-middle attack, organisations would be well minded to consider carefully their operations to mitigate the risk arising therefrom. While technological solutions may offer some reassurance, there remains strong arguments for traditional approaches such as legal risk allocation and training, which should ultimately remain as solutions in the overall toolkit to deal with attackers.

UPDATES IN DREWTECH SERIES

1. Chapter 1: The Importance of an Exit Strategy in Technology Contracts <6 March 2019>
2. Chapter 2: Employees, Technology and A Legal Hangover – Bring Your Own Problems? <4 June 2019>
3. Chapter 3: I host, you post, I get sued? <24 September 2019>
4. Chapter 4: Diabolus ex machina <18 February 2020>
5. Chapter 5: Bringing hygiene online – the MAS notice on cyber hygiene <28 April 2020>
6. Chapter 6: Signing without signing – contactless contracts <16 July 2020>
7. Chapter 7: My Kingdom for a Horse – When your Systems are Held to Ransom <22 January 2021>
8. Chapter 8: New risks in new skins – Updates to the Guidelines on Risk Management Practices – Technology Risk <3 March 2021>
9. Chapter 9: Of blockchains and stumbling blocks <21 July 2021>
10. Chapter 10: Service by airdrop – no parachutes required <7 July 2022>
11. Chapter 11: Large Language Models and Larger Legal Minefields <4 April 2023>
12. Chapter 12: Beset on all sides – liability for data breaches <19 July 2023>
13. Chapter 13: Pitfalls of user-generated content <18 October 2023>

14. Chapter 14: Red queen races – vulnerability disclosure programs <1 August 2024>
15. Chapter 15: Looking at the Man in the Middle (in a cyber breach) – allocation of risk <5 March 2025>

If you have any questions or comments on this article, please contact:

Rakesh Kirpalani
Director, Dispute Resolution & Information Technology
Chief Technology Officer
T: +65 6531 2521
E: rakesh.kirpalani@drewnapier.com

DREW & NAPIER

Drew & Napier LLC
10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T : +65 6535 0733
T : +65 9726 0573 (After Hours)
F : +65 6535 4906