Why are social engineering attacks targeting law firms?

In March of 2010, a Houston-based lawyer fell victim to a scam asking the individual to represent a Hong Kong corporation to pursue debtors in the US that owed the company over USD 4 million[1]. Engagement letters were signed, but before the law firm took any action, cashier's checks drawn on US banks started to arrive. The lawyer deposited the checks and remitted the balance – less their fees – to the client in Hong Kong. The cashier's checks were fraudulent, and the law firm was left with a loss of USD 185,000[1]. The firm contacted the FBI who stated that they were investigating similar cases totaling USD 23 million[1].

In January of 2013, a Nigerian national pleaded guilty in connection with a multi-national scheme that stole USD 70 million[2] from law firms in the US and Canada.

Social engineering theft is not a new phenomenon.

Law firms are frequently targeted because:

- They are perceived as wealthy
- Law firms receive, control and process large sums of money through trust accounts/escrow/client accounts
- Clients often have law firms act for them in managing financial transactions & instructing escrow agents etc.

This form of theft can take many forms, from the relatively unsophisticated "bad debt collection" scams, to highly complex fraud that can involve hackers compromising email systems of clients and vendors, fraudsters impersonating corporate officers on telephone calls (vishing) and copy invoices being stolen and amended and then sent from "spoofed" email addresses.

How do social engineering scams operate?

Criminals invest considerable time, effort and resources into perpetrating these scams and they do so for very good reason; the payoff can be enormous.

A group known as Cosmic Lynx, known to have been operating since April 2019, puts a great deal of research into their M&A scams; they research their targets, craft their email campaign meticulously and set up a secondary email chain that appears to be from a major law firm who are 'facilitating' the deal. The average transfer request made in one of these attacks is USD 1.27 million[3], with the highest being nearly USD 3 million[3].

---

1 **https://www.khou.com/article/news/houston-lawyer-loses-big-in-internet-scam/285-342174533**

2 www.justice.gov/usao/pam/news/2013/Ekhator_01_18_2013.htm

3 Barth, B. 2020. BEC scams grow in complexity as Russian actors launch Cosmic Lynx operation. SC Media.

Law firms appear to be particularly vulnerable to invoice scams and the frequency of hacking attacks that appear to be collecting invoice information is increasing. During these attacks, the hackers acquire copy invoices, alter them to change the banking information and then send them to the client for payment noting that the bank deposit information has changed. Law firm clients have reported losses in excess of USD 1 million as a result of these attacks and law firms will often be asked to share the loss even if their systems were untouched and it was pure impersonation.

How can these threats be insured?

The FBI includes what they term 'BEC' (Business Email Compromise) within their statistics for cyber-crime and many assume that the use of spoofed email addresses and other electronic communications techniques means that a **cyber insurance** policy should cover any losses arising, while others assume that Commercial Crime policies will provide coverage.

The reality is not so clear. It has taken some time for the insurance market to understand and act on this new form of crime.

Crime policies:

- Historically had an exclusion for "voluntary parting" (i.e. the money was not stolen against the will of the insured but was actively and willingly sent to the criminals by the insured in the mistaken belief that it was for a genuine purpose or transaction)
- The "Computer Fraud" extension to a crime policy is typically only triggered if the criminals hack into the insured's systems and transfer money themselves, without any participation by an employee

Cyber policies:

- Typically have an exclusion for loss or damage to "property" (assets of the insured, which includes money and many policies have a specific exclusion for loss of money)
- Also have very specific triggers for coverage and these are typically predicated on a breach of the insured's systems or theft of confidential information – receipt of an email does not typically fall into either category

Commercial crime insurers are now offering "Social Engineering" extensions to cover this sort of loss, although it is usually subject to a low sublimit within the policy and subject to onerous terms and conditions. Some insurers require that the insured proves that they followed specific anti-fraud protocols before a loss will be paid. The loss experience for this coverage is so severe that some insurers have recently decreased the amount of coverage they are prepared to offer and have been underwriting the risk more aggressively.

Some cyber insurers are also offering extensions for "electronic crime". The terms and conditions of the offerings are variable and great care should be taken to ensure that the coverage both provides what is expected and dovetails/does not conflict with the commercial crime policy. Cyber insurers too are carefully managing how much limit they will offer. Insureds should also bear in mind that payments made for such losses erode the aggregate limit of the policy, leaving less limit available to respond to other covered losses.

How can law firms defend against social engineering scams?

Social engineering scams are highly sophisticated and targeted, and can be very difficult to detect, particularly if the email system of a trusted party has been compromised and is being used by the criminals.

“Out of band checking” – in which parties validate instructions with one another using another form of verified communication outside the communication chain of the transaction – has been shown to be very effective in most cases. When used in conjunction with other protocols and procedures, it is possible to reduce the opportunity for loss very significantly.

Nonetheless, investing in both Crime and **Cyber insurance** and discussing how best to leverage and structure of the policy in order to maximize available coverage, is an important measure when building a robust risk management strategy.

To discuss any of the topics raised in this article, please contact **Tom Ricketts**.