Fighting Cybercrime: Old Tools for New Threats

By Thomas Stapleton,
People's United Bank

People's United Bank®

What know-how can do®

Fighting Cybercrime: Old Tools for New Threats

By Thomas Stapleton, People's United Bank

Digital communications and transactions have vastly increased the speed and convenience of business. But this digitization has also paved the way for whole new types of threats and risks that many companies struggle to contain. In particular, middle market companies that use wire transfers to buy and sell goods directly with overseas customers and suppliers are being targeted by hackers at an alarming rate, and many are incurring serious financial losses.

Whether called "man-in-the-middle" attacks, or "man-in-the-email" attacks or simply "business email compromise" (BEC), the tactic is essentially the same. A criminal manages to hack into a company's email, monitors its correspondence with buyers and sellers, and when a payment is due will send a "spoof" email—designed to look like it's come from the actual counterparty—telling the company to redirect its payment into some account the criminal controls. These spoof emails look so genuine they are all too often successful.

According to the FBI internet crime complaint center, total BEC losses in the U.S. have grown from $1.2 billion in 2015 to an estimated $7.2 billion in 2018, with the average loss rising from $147,000 to $187,000. And it's not just large companies that are targeted, 43% of cyberattacks are aimed at smaller businesses. Overall, one in every 131 emails contains malware. According the FBI "BEC is a sophisticated scam targeting businesses that often work with foreign suppliers and/or businesses and regularly perform wire transfer payment."

Interestingly, there are some time-tested bank tools that once seemed on the edge of obsolescence that could be instrumental in protecting companies against cyberattack fraud and losses: Letters of Credit (LOCs) and Documentary Collection.

A LOC is a letter from a bank guaranteeing that a buyer's payment to a seller will be received on time and for the correct amount. In the event that the buyer is unable to make payment on the purchase, the bank covers the purchase. Due to the nature of international dealings, including factors such as distance, differing laws in each country, and difficulty in knowing each party personally, LOCs have been used for literally hundreds of years.

Documentary Collection is a trade transaction in which the exporter puts its bank in charge of collecting payment for goods supplied. The bank sends the shipping documents to the importer's bank together with payment instructions. Documentary Collections do not provide the same level of security as LOCs. As a result, the costs are lower. But companies can purchases either LOCs or Documentary Collections for as little as a few hundred dollars.

Despite these low costs, many middle market companies have gravitated to the near zero cost of direct wire transfers in what is known as an "open account" environment. The bank no longer has a role except as a conduit for the transfer of funds through SWIFT. However, if a hacker successfully spoofs the company there is no bank guarantee. The money is rarely recovered, and the buyer typically has to make good in whole to the seller—essentially buying the products twice. Moreover, if the funds have gone to a red-flagged jurisdiction overseas, the Federal authorities may get involved.

Given this environment, middle market companies should consider LOCs or Documentary Collections even with counterparties they know well. A few hundred dollars is cheap insurance to protect against a BEC loss. While both of these bank products do take more coordination and paperwork than a simple wire transfer, the payment itself is actually rarely delayed. That's because the paperwork for these transactions is sent to the bank ahead of delivery, so the bank is ready to facilitate the payment as soon as the goods arrive.

While LOCs and Documentary Collections are starting to come back into fashion, these should not replace other forms of risk transfer such as cyber insurance. Many company executives assume that their traditional commercial general liability policies cover cyber, but most do not. Insurers have developed other policies to bridge the cyber gaps. Typical cyber-related coverages can include:

Data breach response and liability. Covers the expenses and legal liability that arise from a data breach.

Computer attack. Covers damage to data and systems caused by a computer attack, such as a virus or other malware attack or denial-of-service attack.

Network security liability. Provides defense and liability coverage for third-party lawsuits alleging damage due to the insured inadequately securing its computer system.

Cyber extortion. Covers the "settlement" of an extortion threat against a company's network, as well as the cost of hiring a security firm to track down and negotiate with blackmailers.

These new types of cyber insurance coverage, when combined with time-honored bank products such as Documentary Collections and LOCs, can help middle market companies supplement existing risk mitigation strategies as they continue to expand their business relationships overseas while keeping their fraud and loss risks under control.

Tom Stapleton is Senior Vice President of International Banking at People's United Bank, responsible for Trade Finance and Foreign Exchange. For further information contact Mr. Stapleton at thomas.stapleton@ peoples.com.