People: The Cyber Wild Card in Terms of Security, Attacks

Christopher M. Brubaker, The Legal Intelligencer

June 15, 2016

As details continue to emerge concerning the $81 million cyberheist of funds from the Bangladesh Central Bank by way of hacked wire-transfer requests sent to the Federal Reserve Bank of New York (NY Fed), a lingering question remains regarding the role people played in approving the transfer requests. It has recently been reported that shortly before the fraudulent transfers were approved, they had been denied before being resubmitted. The Bangladesh cyberattack consisted of a total of 35 fraudulent transfer requests totaling over $1 billion in transactions. The first time the 35 requests were submitted, all 35 were rejected because they did not contain all of the information required to process a transfer request.

Later that same day the hackers resubmitted all 35 requests and this time five were approved and 30 were flagged for additional review. Of the five requests that were - approved, one was later denied because of a typo in the name of the recipient. However, four of the fraudulent transfers made it through the system resulting in a loss of $81 million. In light of the news of the initial denial of all 35 fraudulent requests, the question becomes, was a person involved in screening the resubmitted transfer requests? And if not, why not?

Before we look further at what happened at the NY Fed as these transfer requests were processed, it's useful to step back and look at the bigger picture regarding the role of people in the realm of cybersecurity.

People, from entry-level workers to senior management and the board of directors, are a conundrum because they are simultaneously one of the biggest threats to cybersecurity, but also the best chance of thwarting many cyberattacks. The internet is replete with articles and reports discussing the threat posed by both malicious and negligent employees. The - malicious employee, whether motivated by money, hatred or both, is one of the most difficult challenges faced by cybersecurity professionals. How do you guard against someone intent on causing harm who has authorized access to your systems? That is a problem that may never be fully solved, but there are ways to minimize potential harm, such as limiting access to discrete systems necessary for their job, monitoring activity, looking for unusual or suspicious activity (3 a.m. login for example), locking former employees out of systems immediately on termination, and requiring dual access to key systems.

The negligent or careless employee is another concern altogether. They come in many forms and at all levels of the organization. Remember, "C-Suite" executives are employees too, and need to follow the same protocols and guidelines as all other employees. As top-level managers are increasingly the target of cyberattacks given the potential payoff, if anything they need to observe even higher standards than rank-and-file employees. Allowing "exceptions" for top-level employees is also a potential double-edge sword in

allowing a breach to take place in the first place and then in potential liability from a shareholder suit afterwards.

Lax password security (allowing simple passwords or writing them down in accessible locations), failure to secure devices (cellphones, tablets, and laptops), insistence on using personal devices, and connecting to secure systems from public internet are some of the more common examples of careless behavior that can compromise an otherwise sound system. Sometimes all it takes is one careless click on a bad link and the damage is done. Spear phishing (socially engineered targeted fake emails) is a highly successful method used by hackers to gain entry to systems or perpetrate fraud. These attacks take advantage of an otherwise honest employee's interest in doing their job. But data suggests that employee training is a highly effective method for combating this type of cyberattack.

Indeed, employee training and awareness is increasingly being discussed as a key element of a comprehensive cybersecurity program. This ranges from training all employees how to recognize bogus emails (for example, looking for typos and formatting issues and hovering over links to see what the address is) and requiring verbal confirmation (either face to face or by phone) of payment instructions, to educating board members not only on what is being done internally regarding cybersecurity but also on what is happening elsewhere, to training employees what to do in the event of an attack or when they have that "oh no" moment after clicking on a link.

Board involvement is becoming an increasingly important aspect of cybersecurity with respect to controlling post-event consequences with incidents of post-breach shareholder derivative suits on the rise.

But whether your organization is a large publicly traded one or a small- to medium-size, family-controlled entity, the premise is the same: there needs to be awareness and training at all levels of the organization. This helps to foster an open environment where employees feel comfortable in speaking up when they notice suspect or unusual activity. It is important not to criticize or chastise employees who report what turn out to be false alarms. False alarms can also be used to help improve training.

It is generally accepted that all systems will have cyberincidents; attempts to gain unauthorized access to or control over your systems. A well trained and aware workforce can help keep cyberincidents from becoming breaches. Remember Target? It was widely reported shortly after the breach that Target's headquarters in Minnesota received four different warnings of suspicious activity on their network before any data actually left their systems. The warnings were not heeded. Sound familiar? The NY Fed disallows 35 transactions involving the Bangladesh Central Bank totaling over $1 billion. All 35 are resubmitted. Thirty are flagged for additional follow-up related to economic sanctions review, but not initially for potential fraud. Five are approved. One of the five is stopped due to a typo, but four transfers go through totaling $81 million.

Now consider the reports that the NY Fed was aware of and had considered the possibility of just this type of scenario: foreign central bank is hacked and used to send false transfer requests through the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system and chose not to focus on this as a security priority taking comfort in the fact that the SWIFT system had never been cracked. It is quite understandable and frankly impractical to think that a human would be reviewing all transaction requests received by

the NY Fed. However, it is harder to imagine how in this day and age the denial of 35 transfer requests from Bangladesh totaling over $1 billion on one day did not trigger an automatic review by a person of all 35 requests when they were resubmitted hours later. Particularly if it is true that some of the same payees were on both the blocked requests and the approved requests.

Another reported anomaly with the requests is that many of the payments were directed to individuals. If someone was involved in reviewing the resubmitted requests, shame on them. If not, shame on management for not having someone in position to prevent the transfers.

This same scenario plays out in the private sector all of the time in situations where third-party business associates have access to computer systems. Remember the Target breach was initiated through Target's HVAC contractor who had access to Target's network. Consider this scenario: you are aware of the potential risk associated with a third party's access to your systems but take comfort in the level of security employed by the third party and knowledge that they have never been successfully breached before.

You view them as a low-level threat and as such you do not take any specific steps to monitor activity coming through that third party but instead focus your security efforts on direct attacks. Your company suffers a massive data breach after the third party is breached and used to compromise your systems. Prior to the information leaving your system there is both a change in the pattern of activity coming from the third party and a dramatic increase in activity. A review by someone in the IT (or finance/accounting etc.) department when the change in activity began would have readily revealed that unauthorized activity was occurring and could have prevented data from leaving your system. Don't let this happen to your company.

We are all familiar with the expression "our employees are our greatest asset. "While this is true to an extent for everyone, it is equally true that they can only be a company's greatest asset if they are empowered to be that. A well trained, aware, and engaged workforce can be a company's greatest cybersecurity asset turning a potential liability into the difference - between a cyberincident and an all-out cyber disaster.

Christopher M. Brubaker of Clark Hill concentrates his practice in complex commercial litigation and insurance matters. He regularly provides advice to companies on insurance and cyberrisk issues related to transactions and risk management and also advised companies on regulatory matters involving insurance and environmental laws, rules and regulations. He frequently speaks and writes on cybersecurity matters for legal and professional groups.