THE one BRIEF
AON EXPLORES THE WORLD'S MOST PRESSING BUSINESS ISSUES

RISK & INNOVATION

The Bangladesh Bank Heist: Lessons In Cyber Vulnerability

OVERVIEW

How do you steal a billion dollars?

It takes time, planning, manpower – and capitalizing on your target's vulnerabilities.

Over the weekend of 5th February 2016, a group of still-unidentified hackers attempted to steal $951 million from the Bangladesh Central Bank (BCB) in Dhaka. Much of this was eventually recovered, but the thieves still managed to get away with $81 million. The attempt is considered one of the biggest bank heists of all time.

The thieves were organized, well networked, and well funded. But their success was, more than anything else, down to weaknesses in the institutions they robbed.

Understanding exactly what went wrong in the BCB hack – which has been suggested by some to be linked to the WannaCry ransomware attack of May 2017 – can provide businesses with invaluable lessons in how to improve their security strategies.

IN DEPTH

The Hack

The hack was highly complex, and took place over several lines of attack:

- The theft involved manipulating the SWIFT system – a digital messaging platform that manages many of the world's interbank financial transfers – to fool the New York branch of the U.S. Federal Reserve (which holds many international banking assets) into transferring funds to accounts owned by the thieves.
- Pretending to be the BCB, the thieves sent fake instructions over SWIFT to the New York Fed, asking for some funds to be transferred to bank accounts in Southeast Asia.
- SWIFT usually notifies banks of transfers by sending the order to a bank's printers. But in this case, the attackers disabled the BCB's printers with a piece of malware. This meant the bank's employees in Bangladesh were not aware that the heist was going on.
- By the time the BCB reactivated its printer and received the notifications of the transfers – and requests from the New York Fed for clarification — it was already too late and the money had been sent.
- While a series of spelling and formatting errors in the thieves' SWIFT instructions halted the vast majority of the transactions, a total of $81 million was transferred to banks in Southeast Asia and quickly laundered through, among other places, the Manila casino system.

It was one of the most audacious and successful bank robberies in history. But what can organizations learn from it?

Beware Of Human Error

You can have the most sophisticated state-of-the-art security systems in the world, but if people are cutting corners or failing to follow instructions, then criminals can exploit that. And human error played a great part in the BCB attack, at several points during which the theft could have been stopped:

- In Manila, Philippines, workers at the Riza Commercial Banking Corporation allowed the attackers to open accounts using fake driving licenses; these accounts were then used to receive and traffic stolen funds.
- There is evidence that the workers who installed the SWIFT system in BCB did not follow official guidelines and that could have opened up security vulnerabilities.
- There is also evidence of slack procedure in New York: There were numerous inconsistencies in the fraudulent SWIFT orders which should have been spotted.

As Dennis Distler, Director, Cyber Resilience at Stroz Friedberg, an Aon company, puts it: "Humans are the weakest link in any security program." And much of this human error can result from relatively innocent mistakes – the malware that sabotaged the BCB's printers could have entered the system via a spear phishing campaign targeted at specific BCB employees, or via an infected USB drive.

However, some investigators, including the FBI, have speculated about the possibility of an inside job. Security cameras were switched off during the attack, and it's still unclear how the SWIFT credentials were acquired. And if a USB drive was used, it would have to be introduced into the office by someone who was at least partly aware of the plan.

Ed Stroz, Co-Founder of Stroz Friedberg, sees people — and the risks they pose — as a central part of any cyber-protection strategy: "The root cause of many cyber breaches is human behavior. As technologies evolve to become more secure at a technical level, the employee becomes the soft target, and the weak link in security. An employee might pose a risk unconsciously, through carelessness. They could be tricked into clicking on a link or attachment through a spear-phishing campaign. Or they could pose a more active risk, because of anger or disgruntlement at work. If you don't address the human element in cyber vulnerability, you are not going to be able to deploy an effective strategy. It's dangerous to be overly focused on technology."

While the idea of "an inside job" might seem like the plot of a Hollywood blockbuster, there are plenty of reasons for organizations to worry about the risk posed by their staff. "It's unpleasant to admit, but people can just be out for themselves. Or they could have an axe to grind with the company. And what if they're being blackmailed from someone outside the company?" asks Stroz. "An employee with any of these motivations can pose a serious risk to the integrity of an organization's defenses."

Educating staff about the many ways a computer system can be compromised is critical if a company is to have the strongest cyber defense possible. It's also important to learn how to spot the early warning signs of employees who might pose a security risk, whether through malice or error. Companies should assess which employees are accessing what type of information and take the appropriate steps to restrict their access to that information if that person is deemed to pose a risk.

The Problems With Protocols: People and Organizations

The potential for people to fail to do what they're supposed to is why organizations have security protocols and guidelines. But these are worthless if they're not followed or enforced. Organizations need to ensure their staff are properly educated and trained in what to do, how to do it, and educated in the consequences of failing to follow proper processes.

However, the risks don't end there. It's easy to think that by issuing protocols, you've solved the problem. But what if you've got the wrong set in the first place? In the BCB hack, the New York Fed did not have a real-time fraud detection system. Instead, requests were reviewed and any suspicious transactions addressed periodically. This gave the thieves a window of opportunity to launder the money before fraudulent activity was identified. According to its rules, the Fed did nothing wrong. The problem was that those rules were not up to the task at hand.

Or what about if you've forgotten to put in a key piece of the protocol in the first place? There were very few ways the BCB and New York Fed could communicate with one another, other than the printouts. This meant that, in the hours and days following the malware attack on the BCB, the cyber thieves got all the time they needed to launder their stolen funds while the printer was out of commission.

Protocols must be continually tested and reviewed and, where needed, altered to make sure they can confront the threats posed by an ever-changing risk landscape. Or they need to be built in a way that captures even the most extreme eventualities. The BCB robbery teaches us that in an age of continually evolving cyber threats, there's no such thing as invulnerability.

What the BCB Heist Can Teach Us

The investigations into the BCB attack are still ongoing and, no doubt, more revelations will emerge. All the while, cyber-attacks will continue to grow in scale and severity as the world becomes more and more connected.

The cyber thieves were skilled, but their real success was in exploiting vulnerabilities in the organizations they targeted – vulnerabilities which may have been invisible beforehand.

By looking at what happened, identifying the key weak points – in understanding vulnerabilities, in maintaining security procedures, in training employees, and in testing processes – companies can work to mitigate similar weaknesses in their own organizations.

The Bangladesh attack was not the first cyber attack to lead to serious losses, nor will it be the last. Only by approaching every such event with fresh eyes will organizations learn to respond to – or prevent – these threats.

TALKING POINTS

"As more financial services are delivered over the Internet, there will be growing security and privacy concerns from cyber threats. And maybe even systemic concerns. It is not inconceivable that the next financial crisis is triggered by a cyber-attack." – Ravi Menon, Managing Director, Monetary Authority of Singapore

"In my previous risk management experience, cyber was something for the IT department. More and more, for CROs, cyber is what makes you lose sleep at night. On our own and as part of a larger White House effort, we have spent a great deal of time and effort reviewing and updating our systems." – Ken Phelan, CRO, U.S. Treasury

"Each business has to assess the risks posed to it based on its profile and make these policy determinations. Businesses should learn from the mistakes of others and consider implementing some of the directives imposed by regulators in enforcement actions against other companies. There should be training, and it should inform people as to how to use their devices more appropriately, including how to write emails. There are always changes in what is permissible, and those updates should be a part of this ongoing training." – John Carlin, Partner at Morrison & Foerster, former Assistant Attorney General, U.S. Department of Justice

FURTHER READING

- Evaluating Cyber Risk From The Board Of Director's Seat – CIO, May 18, 2017
- The Best Cybersecurity Investment You Can Make Is Better Training – Harvard Business Review, May 16, 2017
- How WannaCry Went From A Windows Bug To An International Incident – Forbes, May 16, 2017
- Cyber Risk Hangs Over Western Elections – Reuters, May 10, 2017
- Mitigating And Managing Cyber Risk: Ten Issues to Consider – Aon