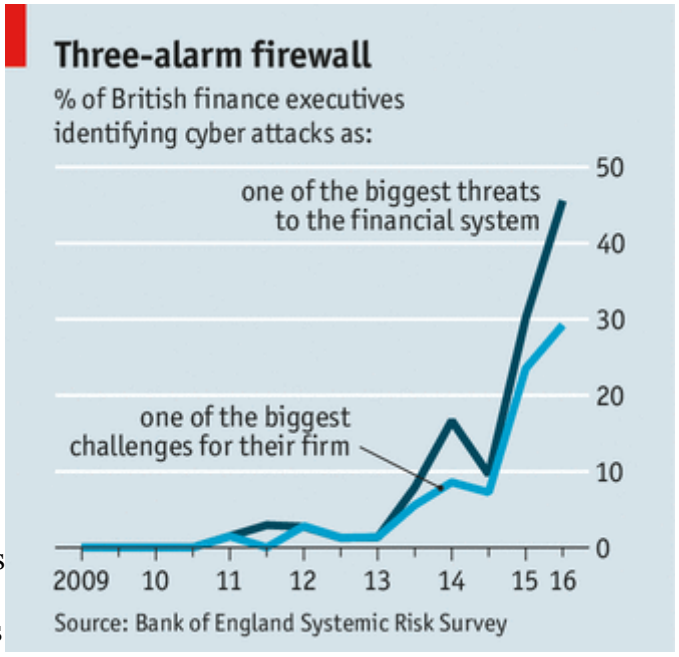
Cyberattacks on banks: Heist finance

May 28th 2016 | World | Banking | Multiple companies

Recent hacks highlight the vulnerability of the cross-border payments system.



BARELY an eyebrow is raised these days when the credit-card details of retailers' customers are stolen en masse; such crimes are attempted or committed daily. But when banks' own funds are pinched, it is time to pay attention--especially when the theft involves hijacking banks' connections to the global payments system. This week the Society for Worldwide Interbank Financial Telecommunications (SWIFT), a network that thousands of banks around the world use to move money, described a recent spate of cyber-heists, which netted $90m. Gottfried Leibbrandt, SWIFT's boss, described them as a "watershed moment". The threat now, he said, is not just to banks' reputations, but to the very existence of those that fail to protect themselves.

Investigators are still trying to piece together how thieves pulled off a spectacular hack that siphoned $81m out of Bangladesh's central bank in February, let alone who was behind it. This was one of the biggest-ever bank robberies, but it could have been worse: $850m of the bogus transfer requests were blocked. The stolen money went to a bank in the Philippines, then on to casinos. Where most of it went from there is unclear. Some ended up with a Chinese operator of junkets for gamblers (who denies knowing it was stolen).

The scam sent banks and SWIFT scrambling to check for other infiltrations. Their probes have turned up at least one similar, albeit smaller, case: hackers tried unsuccessfully to nab $1m from Tien Phong Bank, in Vietnam, in December. Another case has come to light through court filings: Ecuador's Banco del Austro is suing Wells Fargo for waving through fake transfers of $12m ($3m of which was later recovered) to accounts in Hong Kong. The American bank is fighting the action.

Experts say there are likely to be dozens of other actual or attempted breaches of this kind that have yet to be detected. Cyber-criminals have become very good at covering their tracks. In the Bangladesh break-in, for instance, they wrote malware to interfere with a machine whose printouts the bank relied on to check transactions. Jens Monrad of FireEye, a cybersecurity firm that is conducting an audit of the theft, says the median time it takes for targeted companies to realise their systems have been compromised is 146 days.

Banks' coffers being raided by cybercrooks is bad enough. Worse, the thefts expose weaknesses in a vital bit of financial plumbing: banks' connections to the SWIFT network. In each of the cases that have come to light, the thieves hacked into the bank's system, used malware to log on to the SWIFT network using the bank's unique code, and re-routed transactions to new beneficiaries.

SWIFT, a co-operative owned and used by 11,000 financial firms, processes 25m messages a day, covering half of all big cross-border transfers. Were it to be compromised, trust in the global payments system could evaporate. SWIFT insists its network and core messaging services were not breached; the security problems were at the banks themselves, it says. Officials at SWIFT express frustration that targeted banks can be slow to share information with it about hacks, meaning other banks don't get intelligence they could act on.

Nevertheless, calls have grown for SWIFT to do more (with some geeks even suggesting it be replaced by blockchain technology). Mr Leibbrandt responded on May 24th by announcing a "customer security" plan,

aimed at encouraging better network security, information-sharing and fraud detection. He also called for a new wave of innovation in cyber-security--covering "pattern recognition, monitoring, anomaly detection, authentication, biometrics"--to meet the growing threat from "hoodies hunkering over keyboards".

But SWIFT has no power over banks. That is down to regulators, whose performance in this area varies greatly. Among the most switched-on is the Bank of England, which runs a widely respected resilience-testing programme for big banks that includes mock attacks. British banks that fail to beef up their defences may even be forced to hold extra capital.

Standards in some emerging markets are much lower. Security at Bangladesh's central bank was outdated and inadequate. One investigation found evidence of infiltration by three different groups. It is unlikely to be a coincidence that the hackers have targeted banks in relatively undeveloped markets rather than bigger (but much better protected) prizes in countries like Britain and America.

Not that banks in bastions of high finance can rest on their laurels. Even if their cyber-defences are strong, there is always the risk from accomplices on the inside (help from whom has not been ruled out in Bangladesh). Several big banks, including JPMorgan Chase, have begun to whittle down the number of employees with access to the SWIFT gateway. As experts never tire of saying, cyber-security is about people as much as it is about technology.

Source: The Economist