Cyber: the threat to financial institutions turns real

With regulators paying increasingly close attention to risk mitigation strategies and considerable media attention focused on the rising frequency and extent of the threat, financial institutions are on high alert regarding their potential exposures to cyber attacks.

Unprecedented scale of attacks: the Carbanak example

The recent Carbanak cyber attack is described by Kaspersky, the firm that uncovered the attack, as an Ocean's Eleven-style sting. The attack targeted 100 international banks, including institutions in Russia, Germany, France, Spain, Great Britain and several other European countries.

As Giorgio Aprile, Financial Institutions Director for Aon explains, despite investments in IT security, business continuity and disaster recovery, the cyber threat facing financial institutions is fast evolving from a perceived risk to a substantial sequence of very real economic losses. According to some estimates, up to USD 1 billion may have been lost by banks in the co-ordinated Carbanak cyber attacks.

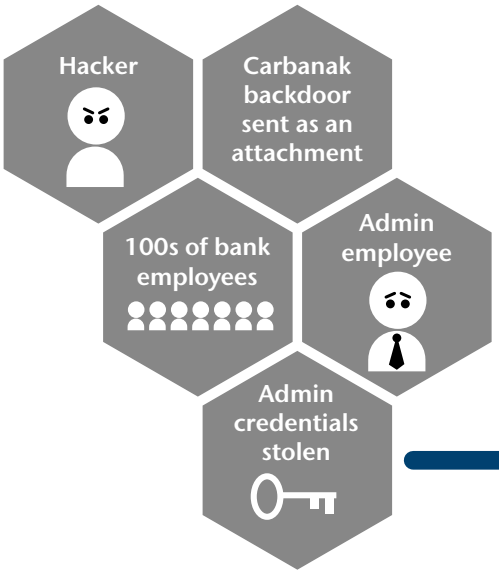
The Carbanak attack is very different to previous incidents.

In the past, cyber attack stories that made headlines entailed data breaches, reputational damage, quickly recovered losses or near misses. This attack resulted in the loss of significant amounts, with cash being extracted from remotely controlled ATMs, SWIFT transfer or e-payment.

Aprile argues that the Carbanak attacks raise the prospect of systemic cyber risk within the banking sector. "Many banks are relying on very similar IT infrastructure. General ledgers, trading systems, data warehousing, branch applications and IT connectivity are all provided by a limited number of players. The same is also true of standard operating systems."

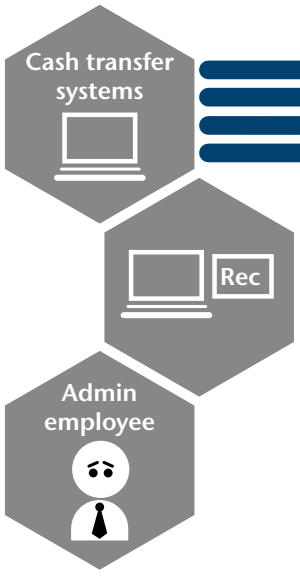
The Carbanak attack – patient and problematic

Infection



The messages sent to employees included a link that, once clicked, triggered the download of malware. The attackers used malicious code to find the employees who were in charge of cash transfer systems or ATMs.

Harvesting intelligence



The hackers installed a Remote Access Tool (RAT) on the machines of those admin employees. The attackers collected snapshots of victims' screens and studied their daily activities in the bank.

Mimicking the staff

Online banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the USA

Inflating account balances
The extra funds were pocketed by a fraudulent transaction

Controlling ATMs
Orders to dispense cash at a pre-determined time

The hackers were then able to remotely control the ATMs to dispense money or transfer money to fake accounts.

AON
Empower Results®

Systemic concerns trouble regulators

From an IT infrastructure perspective, financial institutions have many similarities from one to another, and the vulnerabilities exploited by the hackers at one bank could be replicated right across the global banking system with the potential for a multiplication effect.

In the UK, the Financial Conduct Authority (FCA) has been warned of a previously unidentified vulnerability in the two-step bank verification process widely used by banks, whereby customers receive changing codes by mobile phone to use alongside their regular passwords.

Stay ahead of the threat

The cyber threat continues to evolve, with attacks such as Carbanak raising the prospect of further sophisticated stings in the future.

Aon recommends that risk managers discuss with their Chief Information Officer, IT Security experts and Legal departments to coordinate developing appropriate attack mitigation policies and procedures, in conjunction with the company's Human Resources division.

This vulnerability has the potential to provide hackers with unrestricted access to customer accounts and highlights the kinds of vulnerabilities that new technology may create and hackers look to exploit.

Commenting in the Financial Times in March, an FCA spokesperson stated that the FCA "is widely engaged with a large number of stakeholders on the cyber issue, and has established a large network of engagements and contacts to leverage a wide range of skills".

Aon has been working with financial institutions internationally to help assess and diagnose the extent of their cyber risk exposures. We have also been reviewing financial institutions' current insurance protections (typically Bankers Blanket Bond /Crime, Professional Indemnity, Cyber Liability) to assess applicability as well as potential coverage gaps that are unprotected.

For further details from the Aon team contact:

Stephen Trickey
Financial Specialties
t: 02 9253 7577
m: 0410 452 415
stephen.trickey@aon.com

Empower Results®