FINANCIAL TIMES
MONDAY 18 JANUARY 2016

FT.COM

Securities and Exchange Commission gets tough on cyber security

US regulator signals that prevention is the centrepiece of its strategy, says **Craig Newman**

As 2015 drew to a close, the Securities and Exchange Commission talked tough on cyber security.

On top of the ever-growing drumbeat of business and headline risk and a series of bold public statements warning that lax cyber security would not be tolerated, The US regulator censured a small regional investment company, RT Jones Capital Equities, after a cyber attack from China exposed information on 100,000 brokerage clients.

For years, the SEC has offered more bark than bite on cyber security, pairing a tough public stance with a lighter regulatory touch. But last year the divide between the SEC's words and action narrowed. The hardline approach to RT Jones signalled a newfound willingness to step up enforcement efforts to police the data security of investment companies.

It also sent a clear message about the agency's expectations for 2016: investment advisers and broker-dealers must get their cyber defences in order before the hackers strike.

By emphasising the need to have planning in place, the SEC is signalling that prevention is the centrepiece of its cyber-security enforcement agenda this year.

In the case of RT Jones, the SEC charged the St Louis-based company with not having data security policies and procedures in place before the attack. RT Jones stored its client's personal information including social security numbers, on a third-party web server, which the hackers compromised.

After the attack was discovered, RT Jones did all the right things. It brought in a cyber forensics company and notified each client whose information was exposed. To date, none of RT Jones's clients has reported any financial loss or identity theft as a result of the attack.

But tidying up after the fact was not the point. The SEC expected RT Jones to have its cyber defences up and running before its firewalls were breached and used a 15-year-old rule to enforce that expectation. RT Jones was charged under Regulation S-P (the safeguards rule), adopted in 2000. It requires broker-dealers and investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards".

The SEC's list of grievances against RT Jones went beyond failure to implement sound defences and included not conducting periodic risk assessments, not encrypting sensitive data, and not having a breach response plan ready if there were a cyber attack.

The case was accompanied by a series of public statements promising to hold investment companies and their leadership accountable if data security standards were not up to par. In a speech in October, Mary Jo White, chairwoman of the SEC, said it was "incumbent" on financial companies to develop "robust, state of the art" plans against cyber attacks.

Andrew Donohue, the SEC chief of staff, later warned that the agency would bring enforcement actions against companies' chief compliance officers for looking the other way when it came to addressing important compliance issues.

And barely a week before bringing the RT Jones case, the SEC announced a new cyber-security examination initiative for US-registered investment advisers and broker-dealers. The initiative is not just filled with "check box" compliance measures but includes a series of significant and detailed steps towards creating a broad platform of cyber-security safeguards that touch on important areas of an investment business's operations.

There is ample reason for the SEC to finally clamp down. Cyber attacks on big financial institutions, broker-dealers and hedge funds make headlines regularly. The pervasiveness of such attacks is alarming. The SEC's own cyber-security sweep conducted in 2013-14 revealed that, of the more than 100 companies examined, 88 per cent of the broker-dealers and 74 per cent of the investment advisers had experienced a cyber attack.

Not surprisingly, the SEC is betting that preventive measures are the best way to minimise the crippling impact of cyber attacks in the financial service industry. Companies that fail to implement them in 2016 should fear not just hackers, but an SEC that is resolved to take action on cyber security.

Craig Newman is a partner at Patterson Belknap Webb & Tyler, the law firm, and chairman of its privacy and data security practice group.