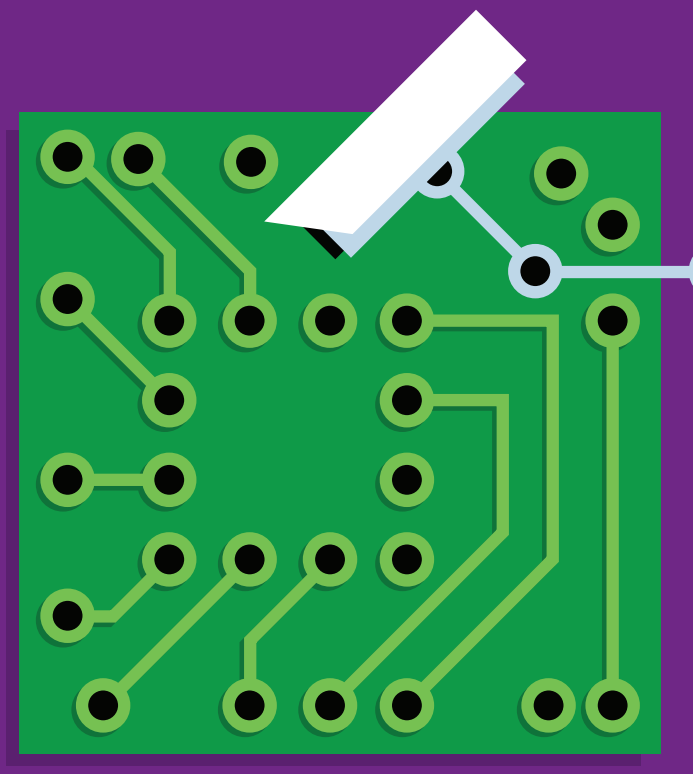
KPMG

Closing the gap

Cyber Security and the asset management sector



January 2018

kpmg.com/uk/closingthegap

The changing threat

As much as new technology has provided a platform for business innovation and growth, it has also brought new risks. One of these, that is never far from the headlines, is cyber security. The attacks seem to keep on coming. The WannaCry ransomware attack in May 2017, for example, impacted more than 200,000 systems worldwide.[1] This was swiftly followed a month later by the Petya (and variants) ransomware attack that had its epicentre in the Ukraine and caused widespread disruption.

Globally, cybercrime is now estimated to cost $400bn a year, meaning cyber risks are among the top issues that businesses have to consider when it comes to their resilience and continuity planning.[2]

What makes cyber risks so challenging to deal with is the rapid pace of change in the digital space. Because new cyber threats are emerging all the time, businesses have to monitor developments constantly and ensure their security systems are up to date to protect themselves more effectively from cyber-attacks.

But what of the asset management sector specifically? How are asset managers faring in the cyber battle, and what should their priorities for action be?

A rising priority for asset managers

Because most asset managers don't have public-facing infrastructures, they have perhaps been somewhat insulated from the cyber threat compared to their banking and insurance counterparts.

The result has been that cyber security has not received the same level of focus amongst the fund management industry. But the signs are that this is changing – as it needs to. The realisation is growing that no sector is immune to the danger, and that cyber criminals will relentlessly hunt out any weak links. With banks and insurers steadily strengthening their defences, the asset management industry will inevitably come more into view as hackers look for an easier target.

Commoditised attacks

- Attackers: Organised crime groups operating internationally. Smaller-scale criminals. Hacktivists.
- Victims: Wide range of individuals and businesses, often via their customers.
- Victim numbers: Hundreds of millions.
- Financial cost: $300-$10,000.
- Overall impact: High. Although returns may be relatively low, these economy-of-scale attackers monetise millions of victims and damage many more.
- Method of attack: "Spray and pray" techniques, using spam emails, malicious website "watering holes" that target a group of people from a certain organisation or geography, and criminal infrastructure to leverage vulnerabilities in often out-of-date software.
- Common tactics: Financial Trojans, commodity ransomware, denial-of-service attacks, SQL injection

Targeted attacks

- Attackers: Organised crime groups operating internationally.
- Victims: High-net-worth individuals and businesses, often targeted through their supply chains and customers.
- Victim numbers: Tens of thousands.
- Financial cost: $10,000-$1 million.
- Overall impact: High.
- Attack methods: Demonstrate an understanding of the industry they are attacking, including its systems and communications, and often causing significant business disruption by tailoring the attack to the victim, thus ensuring greater impact and financial rewards.
- Common tactics: Repurposed banking Trojans, business email compromise fraud / CEO fraud, targeted ransomware

High end attacks

- Attackers: Often smaller-scale, highly covert, organised crime groups operating internationally.
- Victims: Financial systems and infrastructure, through inside and specialist knowledge.
- Victim numbers: Dozens.
- Financial cost: $1 million-$100 million.
- Overall impact: Extreme – the damage to reputation and financial costs will permanently affect a business.
- Attack methods: Conceived from a specialist viewpoint with insider knowledge and understanding. These attackers develop their own custom toolkits to target software vulnerabilities. While their attacks can sometimes be easily recognised as the work of a particular group, in many cases the true motivation remains unknown.
- Common tactics: Breaking into banks and financial systems, disrupting critical infrastructure

1 https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23
2 Net Losses - Estimating the Global Impact of Cyber Crime, Center for Strategic and International Studies, June 2014

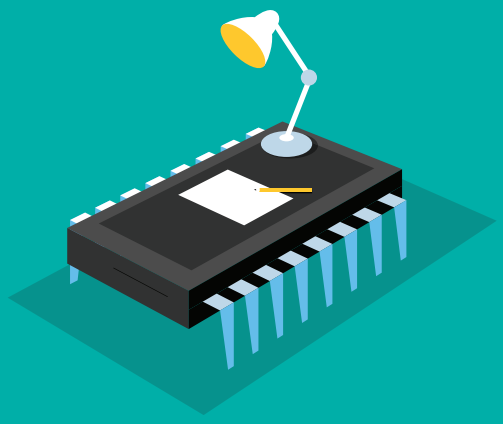
The urgency of the situation is illustrated by KPMG's recent CEO Outlook Survey, in which less than four in ten of the asset management CEOs surveyed (39%) said that their organisation is fully prepared for a cyber event.[3] This was several percentage points lower than the cross-industry average, and, in an industry dealing daily with huge financial transactions, it shows a worryingly low level of confidence.

The changing threat

The threat landscape continues to evolve. Criminals are looking to repurpose attacks used against banks to target new institutions such as insurers, e-retailers, healthcare and, potentially, the asset management sector. Industrialisation of cybercrime continues, with criminals scaling their operations, and looking to automate the targeting and exploitation of asset managers. At the same time, nation states continue to invest in cyber-espionage and military cyber-attack capabilities. Geopolitics will drive the use of these cyber weapons.

Eyes on asset managers

Asset managers may not directly interface with the public at large, but they can still be a tempting target to attackers for several reasons. Firstly, they hold a wealth of customer financial data. Secondly, they possess highly valuable intellectual property around investment strategies and mechanisms (such as algorithms and 'quants'). Information they hold could also be used, if obtained, to front-run trades with huge profits potentially achievable. This means that there is a high potential risk of data theft by insiders as much as by external parties. In addition, many asset managers rely on internet connectivity for their trading services which could become the target of a denial of service attack, with a ransom extorted before the ability to trade is reinstated.



3 https://home.kpmg.com/uk/en/home/insights/2017/06/2017-ceo-outlook.html

Financial services

Banks are locked in a battle with cyber criminals to secure digital banking channels and counter fraud.

The roll out of two-factor authentication has reduced online fraud levels. Chip-and-pin has limited the ability to exploit stolen card data, but card-not-present frauds are increasing. Criminals are becoming more financially savvy, and have started to target bank systems and financial infrastructure.

Information technology

Cloud-service providers can find themselves targeted for distributed denial-of-service attacks aimed at hosted services, which cause collateral damage and disruption to other clients.

Professional services

Lawyers and accountants are being increasingly targeted as the trusted route into major firms. They often hold sensitive client data, and criminals have used their email systems to send highly targeted phishing emails to clients as part of business email compromise fraud. This sector also encounters ransomware frequently.

Telecommunications

As the heart of our networked world, telecom firms attract criminal attention as a route to compromise mobile devices. They also find themselves a target for state espionage and, occasionally, infrastructure attacks.

Utilities

A less frequently targeted sector by organised crime, although occasionally the subject of denial-of-service attacks. Concerns over attacks by nation states and political activists, linked to increasing dependency on industrial control systems, have led to growing government pressure to improve security.

The true cost of cyber crime

The costs of a cyber incident typically occur in two distinct phases – immediate and slow burn (see diagram below). The extent of these costs can vary considerably by sector, and can be affected by a range of factors. These include the type of company targeted, the data the company handles, and the regulatory and legal implications of any incident. This means that cyber- attacks with similar impacts can have vastly different costs.

Research undertaken by BT and KPMG in the UK suggests businesses also have very different concerns regarding breach costs depending on which sector they are in, with litigation and regulatory enforcement concerns dominating in the financial services sectors.[4]

Financial-loss concerns dominate in the retail sector, while tech firms are the most concerned about reputational impacts.

Immediate costs

These are the largely unavoidable costs that include the immediate business and media impact, plus the cost of restoring the confidentiality, integrity and availability of data and systems. Immediate costs include:

– Forensic investigation costs
– Legal costs
– Customer notification costs
– Credit monitoring for customers
– Potential business interruption costs
– Public relations expenses
– Fraud costs
– Extortion costs
– Physical damage costs
– IT/business remediation costs

Slow-burn costs

These vary according to the type and severity of the event, and how it is handled, but typically include the long-term business impact and costs incurred by reimbursing victims, as well as reparation and the payment of penalties for failure to meet obligations. Slow-burn costs include:

– Third-party litigation expenses
– Customer churn from reputational damage
– Regulatory fines and penalties
– Share price impact
– Loss of management focus
– Loss of competitive advantage
– Loss of revenue

4 https://home.kpmg.com/uk/en/home/insights/2016/07/taking-the-offensive-working-together-to-disrupt-digital-crime.html

Where from here?

KPMG suggests that asset managers should focus on five key areas to address cyber risks.

Ownership: Cyber security needs to be owned by someone senior in the business. But many asset managers still do not have a Chief Information Security Officer (CISO), with cyber managed by an asset manager instead. More asset managers need to look seriously at appointing a CISO – who should report directly to the COO, creating a clear line of sight between the business and the risk.

Capabilities: New and improved cyber security capabilities are likely to be required. But asset managers will also want to assess their current 'pockets' of cyber security excellence and ensure those best practices are shared across the enterprise. Leading organisations are starting by ensuring that their existing capabilities are being properly utilised.

Awareness: Improved awareness from the C-level down is key. In particular, asset managers need to focus on improving their understanding of their ecosystem of third party suppliers – fund administrators, custodians, platform providers – to manage their risk in a consistent manner.

Organisation: CEOs will need to work with their business leaders to understand the right balance of centralised and decentralised services to most appropriately meet the cyber risks in each market. Creating the right structure for robust and consistent cyber security is key to fielding a responsible (and defendable) response.

Preparedness: Successfully activating a response and recovery programme takes practice, commitment and clear lines of responsibility. Many asset managers have found 'red teaming' exercises that simulate a cyber incident to be a wake-up call and prompt asset managers to urgently strengthen their ability to detect and respond to attacks.

"The cyber-attacks that frequently dominate the headlines can distort how businesses perceive the risks associated with cyber. There is a natural tendency to focus on the unusual or memorable, but this doesn't always reflect the reality of the cyber risks facing companies every day."

Contact us

Matthew Martindale
Partner, Cyber Security
KPMG in the UK
T: +44 79 1755 2588
E: matthew.martindale@kpmg.co.uk

David Ferbrache
Technical Director
KPMG in the UK
T: +44 7780 225463
E: david.ferbrache@kpmg.co.uk

kpmg.com/uk/closingthegap

CREATE | CRT089283 | January 2018