Morgan Stanley breach leads to $35 million lesson in IT asset management

Published 06-Oct-2022 by
Robert Baugh, Keepabl

The U.S. Securities and Exchange Commission (SEC) last month charged Morgan Stanley Smith Barney LLC (MSSB) $35 million for failures in privacy and security practices under the SEC rules.

The failures were "astonishing" and the firm "fell woefully short" in protecting the personal information of its customers, said Gurbir Grewal, director of the SEC's enforcement division.

"Today's action sends a clear message to financial institutions that they must take seriously their obligation to safeguard such data," Grewal said.

The case concerned the management and retirement of IT assets, and while the rules here may be those of the SEC, the same behaviour would lead to similar sanctions under the Financial Conduct Authority (FCA) rules in the UK, as well as under privacy and data protection laws such as the UK General Data Protection Regulation (GDPR) and EU GDPR.

What financial institutions can learn from MSSB

The October senior team and board meetings at MSSB are unlikely to have been happy events, particularly for the risk committee. Thankfully there are easy fixes firms can implement, and the SEC Order provides numerous lessons for financial institutions in four main areas: a sset management; v endor selection; v endor management; and u se of available technological measures.

First, a review of the risk that eventuated for MSSB, due to its own actions and inaction.

Risk from poor asset management

All staff use IT equipment — or assets — to get their job done: typically mobiles, tablets and laptops. Organisations may still have their own on-premise servers and databases. Financial institutions in particular have large estates of desktop devices, for example, for trading rooms.

These devices are regularly retired and financial institutions, more than most, have an interest in maintaining state-of-the-art IT estates, shortening the lifespan of their IT kit.

This SEC Order relates to pre-COVID-19 times but remains just as salient today. Flexible working conditions mean financial institutions have reduced the need for extensive office space and equipment and are likely to be looking at retiring a larger number of these devices than in previous cycles.

MSSB's asset management failures

Separate but fundamental to the vendor-related failures examined below, the SEC Order states that MSSB failed properly to manage its IT assets in accordance with its own policies and procedures. For example, in 2019, MSSB had decommissioned approximately 500 devices from local offices and branches, "as part of a broader hardware refresh program".

When MSSB tried to reconcile its records to confirm destruction of these decommissioned devices, it was unable to locate 42 of them (or slightly more than 8% of the devices). The missing devices potentially contained "unencrypted customer PII and consumer report information".

(PII is personally identifiable information, the term commonly used in U.S. federal and state privacy laws. UK and EU laws use the term "personal data". For this article, it can be assumed they are the same.)

As well as being necessary to enable compliance with SEC rules, maintaining an asset register is an important part of security good practice. For those looking for certification to the relevant security standard ISO 27001, the accompanying code of practice, ISO 27002, sets out guidance on how to meet 27001's requirements. In control 8.1.1, the 2017 version of 27002 states: "The process of compiling an inventory of assets is an important prerequisite of risk management."

It continues: "An organisation should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion and destruction."

In control 8.1.2, it refers to asset owners who have management responsibility for the asset and that asset's lifecycle, stating: "The asset owner should … ensure proper handling when the asset is deleted or destroyed."

LESSON 1: *create and maintain an asset register with identified asset owners, making sure it is managed according to the firm's policies and procedures.*

MSSB's vendor selection errors

The facts, according to the SEC Order, are pretty damning. In 2014, MSSB contracted with a moving and storage company ("Moving Company") to remove thousands of electronic devices from the data centres and to "remove, destroy, or delete" any data contained on such devices.

It is important to note that Moving Company "had no experience with, or expertise in, providing such data destruction services". It really was a moving and storage company.

The contract stated that Moving Company "would work with an e-waste management company ("IT Corp A") to wipe or destroy any data present on the decommissioned devices", but the SEC Order confirms that:

- MSSB did no due diligence on IT Corp A, despite Moving Company literally being a moving company with no relevant expertise, and so clearly not an appropriate vendor on its own;
- the use of IT Corp A was not validated under MSSB's procurement procedures, Moving Company was qualified as a sole contractor unable to sub-contract, and MSSB had no procedures for looking at such sub-contractors; and
- as there had been no due diligence on IT Corp A, MSSB had no recorded proof that it had chosen a supplier that had been certified to any relevant standard for these activities.

LESSON 2: *perform appropriate due diligence on vendors, make sure the contract reflects the reality, and do appropriate checks and audits along the way.*

MSSB's failure to manage its vendors

Quite soon after the contract was signed, things started to go wrong, but MSSB appears to have had no idea, because:

- no one at MSSB monitored the database provided by IT Corp A even though they had access; and
- no one at MSSB "had any direct contact with IT Corp A during the decommissioning process to ensure that the devices were properly handled".

Under the contract, IT Corp A would wipe devices and resell them, with 60% to 70% of the resale amount going to MSSB, which would "receive an asset report and a disposition report (in essence, inventories of the devices collected and whether they were returned to MSSB, resold or destroyed), as well as certificates of destruction (CODs) documenting the destruction of relevant devices".

As well as these reports and certificates, IT Corp A maintained a database with inventories of devices it had wiped and sold or destroyed, and MSSB had direct access to that database.

As the SEC Order notes, with all these mechanisms, MSSB "could have monitored the entire process independently, if it chose to do so".

It is of particular concern if a firm has the ability to monitor and fails to do so. As a sign of this lack of oversight, the SEC even noted that "it does not appear that MSSB ever requested or received the remainder of the resale amount from Moving Company, as contemplated in the contract".

Unauthorised sub-contractor change

Another clear indication of this lack of vendor management came early in the life of the contract, when Moving Company swapped out its specialist sub-contractor, IT Corp A, with another company, IT Corp B, without notifying MSSB.

Even though MSSB had not been notified of the change by Moving Company, the SEC stated that MSSB should have realised the specialist sub-contractor had changed, because:

- IT Corp A's inventory tracking database was no longer used; and
- IT Corp A stopped providing, and MSSB stopped receiving, CODs for any devices.

MSSB was relying on, and paying, Moving Company to wipe and destroy devices, but this was no longer happening. IT Corp B was able to do this, but Moving Company "never asked IT Corp B to perform those services and IT Corp B understood that the devices had already been wiped".

This led to another oversight failure by MSSB: IT Corp B provided certificates of indemnification (COIs) on possession of the devices. These were not destruction certificates, but "simply represented that IT Corp B assumed possession of the devices and risk of loss".

The COIs were on IT Corp B's letterhead and the SEC Order notes: "MSSB, however, did not review the COIs. If MSSB had reviewed the COIs, it would have been clear that Moving Company was using a sub-vendor that had not been vetted by MSSB and that the hard drives were not being wiped of data, including potential customer PII and consumer report information".

LESSON 3: *managing vendors and complying with policies and procedures is a continual process during which a firm needs to be alive to "risk flags" and act accordingly.*

MSSB's very late reaction

In 2017, a year after the contract ended, an IT consultant notified MSSB that they had purchased hard drives with MSSB customer data and chastised MSSB for not having processes on retiring hardware.

Various activity followed and it was in 2020 that MSSB notified roughly 15 million customers that "certain devices believed to have been wiped of all information still contained some unencrypted data", including, potentially, their PII.

Such a slow reaction would not go down well with GDPR regulators.

LESSON 4: *a firm must react quickly when it becomes aware of a breach, considering its obligations to customers, regulators (financial, data protection and other), insurers and other stakeholders.*

Poor use of available solutions

The 42 missing "local devices" mentioned at the start of this article were, it transpired, equipped with encryption capability, but MSSB had failed to use it until 2018. Moreover, because the encryption software only encrypted newly-created data, some data from before 2018 remained unencrypted.

LESSON 5: *financial institutions must ensure they are making full use of solutions available to them, often included within their technology purchases for no further charge.*

Robert Baugh *is the founder and CEO of Keepabl, privacy management SaaS based in London. Prior to Keepabl, Robert was general counsel of technology growth companies for more than a decade.*

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 06-Oct-2022