Risk Management

Jacob Koshy, chief finance officer at global change and transformation consultancy CubeMatch

Accounting for risks is no easy task

BY JASON WALSH

Banks have been at the forefront of risk even before cyber threats, notably lending risk. Arguably, this has provided insights that can today be applied to other areas, including cyber security.

Indeed, lending risk itself has been around for as long as finance has existed, said Jacob Koshy, chief finance officer at global change and transformation consultancy CubeMatch.

"The first document on risk is 3,700 years old, from Babylon. It's a stone pillar, and part of it is things like risks on loans," he said.

"Similarly, if you go to the Bible, in II Kings, Elijah shows the importance of debt and repaying debt. Lending has been around for a long time," he said.

More recently, modern banking, more or less founded in the 18th century as government enterprises expanded risk exposure, and with it, reward.

"Back in the 1930s they were fairly stable organisations and had the 3-6-3 rule: borrow at 3 per cent, lend at 6 per cent, and get onto the golf course at 3pm, but banks started moving into new areas with the business market exploding in the 1980s," he said.

By then, operational risk had become a major issue, with the collapse of Barings Bank being a fine example. Today, even greater risks exist, including fraud, money laundering and funding of terrorism, all of which have driven expansions in know-your-customer regulations.

The 2008 financial crisis, however, demonstrated that risk exists on books and yet can sometimes go unseen.

"Banks have gone through a lot: a whole shift from financial to non-financial risk, including fraud and operational risk, and today we have technology risk, cyber, Covid, and we're all doing remote banking. There's also the whole outsourcing side of things," said Koshy.

Cyber risk typically falls under the rubric of fraud, and recent events from the hacking of the Health Service Executive to oil and gas pipelines have demonstrated it is a real problem.

Banks, however, are more aware of it than most, Koshy said, as they have been under threat from day one.

"It's a different kind of ransoming and kidnapping, but it's what banks always had to go through, except now it is done electrically."

Working with banking and financial services clients, CubeMatch runs the gamut of risk exposure, helping to develop analyses and responses that manage and make sense of it.

"Most of our work has been, in the past, things like credit risk and a lot of drivers have been regulatory. But banks have to go beyond that. Regulatory standards are the minimum that you have to do. Typically, banks have to decide on their own risk models, looking at things like capital and liquidity."

The 2008 financial crisis, however, demonstrated that risk exists on books and yet can sometimes go unseen. This can mean making complex projections.

"If you have a lot of money in the oil industry, for instance, and the price of oil drops dramatically, what does that mean for you? You can't ignore geopolitics either: what happens if you have money in a country and things change," Koshy said.

Indeed, this is something we have seen in recent years, with the Brexit process creating new forms of risk.

CubeMatch brings its understanding of risk to board level, presenting real figures and possible scenarios in order to define acceptable risk exposure.

"They come to us because we've read the book, seen the movie, bought the T-shirt. We constantly skill ourselves up in this area," said Koshy.

Today, risk is so wide that it is no longer possible to have a single risk officer who looks at everything from liquidity to the locks on the safe. Instead, specialists, including external consultants such as CubeMatch, look at areas such as credit risk, market risk, operational risk and more, reporting back to the chief risk officer.

"Cyber crime is technically under operational risk: you need to be able to run the bank and the threat of being defrauded electronically is certainly there. How you calculate that risk requires real granularity," said Koshy.

> **If you understand risk, that then allows you to logically decide if you want to take the risk**

Understanding risk can mean unlocking rewards, however. There is nothing wrong with a bank saying "We're going to go into this market because it's the best thing for shareholders", but the chief risk officer must be well informed enough to demonstrate where the risks lie.

"If you understand risk, that then allows you to logically decide if you want to take the risk, because the way of looking at risk is traditionally in terms of risk and return," said Koshy.

Driving home the data hardware risk

Data leakage from outdated IT equipment creates a unique risk vector, but a range of solutions is available

BY JASON WALSH

Philip McMichael, chief executive officer, Vyta

While many fret about the technical side of IT security, it is worth remembering that physical security matters too. This may mean physical access policies and secure door locks, but it also means understanding that data is not just bits, it also consists of atoms with a tangible presence in the material world.

IT lifecycle solutions specialist Vyta understands this, and offers a range of solutions for destroying data when hardware reaches the end of its life.

What was once a relatively uncommon process, secure data destruction is now on the corporate agenda.

"I think it just depends, from customer to customer. Some people will see it as a big issue, and to a certain degree the GDPR has put it to the front of people's minds," said Philip McMichael, chief executive, Vyta.

"It also depends from industry to industry and I think a bit of education needs to be done, as people do need to think about old data on equipment.

"Any organisation has a certain amount of data held, whether that be from providing services to the general public and so holding data on people, there's risk around that, but even smaller businesses will have data about their employees and so on. Then there's the commercial risk."

All of us who have lost precious data, this writer included, could be forgiven for thinking all those ones and zeros on hard drives and solid-state devices were fragile. In fact, they are anything but.

Standard operating systems may offer few tools to recover deleted data, but the open secret is that supposedly "deleted" data is not gone at all: instead, the sectors on the drive are simply marked for future use and are overwritten by the system when needed. This is even true of formatting disks.

"People think reformatting the hard drive is adequate, and it's certainly not," said McMichael.

This then poses a question: what to do with devices if the data can be scooped off them by anyone with minimal technical knowledge?

Vyta has more than one approach to data destruction, and while both are final, one is rather more dramatic than the other.

"The two services we provide are overwriting the data using a fully certified piece of software, certified by the UK government, the Japanese government, the US government. The other method is shredding, which we do on-site," said McMichael.

While shredding hard drives and SSDs sounds like something an intelligence agency would do, McMichael said that for some businesses it was simply a matter of policy.

"It's not necessarily the data that drives that choice, sometimes it's the organisation. In fact, nowadays a laptop shouldn't really contain a lot of data; as it's all held in the cloud."

While Vyta has 100 per cent confidence in the erasure process, some businesses simply want to see the destruction.

In both cases, Vyta also records crucial information to help with compliance, such as where an item came from, what it was, what was done to it and where it went. "We can show that data the whole way through and we have the certificate," said McMichael.

Given this, Vyta is very clear where it fits into the business landscape – and it is not low tech. "Yes, we do the waste, recycling and so on, but we're an IT security company," he said.

Indeed, the security-first approach is just what businesses need when it comes to disposing of devices.

Certainly, recycling and sustainability come into the picture, but only once data has thoroughly been dealt with.

"The whole sustainability agenda is much more at the forefront than it ever was before. It's not just going to charities and education, which it does, but small businesses often buy three- or four-year old laptops from us. They're perfectly suitable for most people's uses," McMichael said.

According to him, the message of data destruction has got through, particularly where data is central to business activities.