REDLEAF CONSULTANCY
A SECURITY PRACTICE

Bank Branch Designs Are Changing – What Are The Security Risks

The Nature of Retail Banking Operations is Changing and Poses a Challenge for Physical Security

Changing Nature of the Retail Bank Branch

The nature of retail banking operations is changing, driven by the advance of technology, the closure of branches and the need to reduce costs. The process, which started some years ago has accelerated, with it seems all banks chasing a branch design that will attract customers in and allow them to experience the products that are on offer.

Future branch design is ultimately about ensuring that a bank can deliver the products and services that its customers need. It is not just about tinkering on the edges and slightly modifying a design that largely hasn't changed for years and which was dominated by a counter, with staff on one side and customers on the other.

New branch designs are bright and open plan, allowing customers a high degree of interaction with staff and technology, in what banks see as the "Apple" store experience. Unfortunately bank branches aren't Apple stores, the risks are not the same but security designs must develop as the business changes.

The modern bank branch

> The nature of bank retail operations is changing, driven by the digital age, branch closures and cost controls. New open plan and highly interactive branch designs generate a change in the security risk

Security Risk

Providing mitigation on the attendant risks in the traditional bank branch is well known, with preventative measures having been built in over a number of years. These were captured both through threat evaluation and as a result of incidents. Traditional branches lent themselves to a solid security regime, with good staffing levels, strongrooms and a counter that provided an effective boundary, which could be enhanced with bandit screens and other devices.

The majority of staff, spent most of their time behind the protected counter and while they did interact with customers, in meeting rooms to the front of the branch they were not there all the time.

The branches themselves presented an image of security that was robust and difficult to overcome. It was probably this type of branch design, coupled with tight cash controls that has resulted in the UK currently having a bank robbery rate at just over 1 per week, as opposed to a previous figure of 16 robberies per week.

The move towards highly open plan and interactive branches, with the majority of staff sitting forward of the counter, does increase the risk. In light of either assumptions made by design teams or in a drive to boost sales it can be difficult to quantify the risk, after all, who robs banks these days?

But bank robbery is only one risk, overseeing and overhearing present a threat to the security of information, and PCs and other devices not under the watchful eye of staff can be compromised.

Where Is the Risk?

Cash

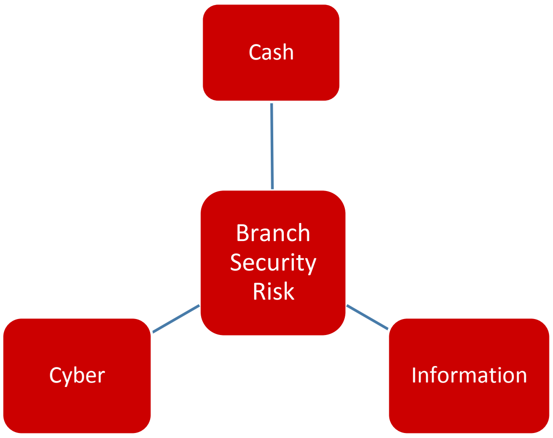
Despite the belief that the use of cash is decreasing, this is not borne out by the cash circulation figures produced by the Bank of England, where the value of notes increased between 2009 and 2014 by 29%. In addition to this, according to statistics from Link, the number of ATMs within the UK doubled between the years 2000 and 2014, to a position where there are now 64,000 machines – that's nearly 1 ATM per 1000 head of population.

The majority of cash based transactions are small and to that end a range of electronic solutions have been introduced, including PayM, contactless cards and Apple Pay. Whether any of these systems can dent the pervasive nature of cash is difficult to know; they might, but they might equally just resemble the construction of a new motorway or town bypass, designed to reduce congestion, which they initially do but in the long term only increase traffic volumes.

Within branches ATMs for purely dispensing money, together with cashiers, who deal with more complex transactions might be superseded. ATMs will become more advanced and will be able to give credit for deposits, process cheques, as well as dispense notes. This is perhaps a significant gain but someone has to replenish the ATMs, prepare cash for transportation and undertake periodic balancing. This can be outsourced to a cash in transit company and in some cases already is, but it is not a low cost solution, particularly if a branch experiences a high footfall and has a requirement for daily servicing.

Although in the much longer term the use of physical cash might well diminish, it remains highly probable, certainly in the short term and very likely in the medium term that cash will remain a core branch function. Its use by both personal and business customers is likely to continue and as a result so will the threats to it. Not all crime requires the sophistication of cyberspace as hard cash is readily obtainable, exchangeable and largely untraceable.

> Cash volumes continue to rise, weaknesses in IT systems are being exploited and the protection of information remains key in assessing the security risk to bank branches



Three Security Risks in the New Branch Design

Cybercrime

Cybercrime is not just restricted to those criminals who remotely try and exploit weaknesses in firewalls and other protective measures on IT platforms. It can be about exploiting legitimate hardware, patching that into equipment and taking advantage of loopholes that exist.

Within the new branch designs it is quite common for PCs, linked to a banks network to be in public areas and while they are password protected they are not secure. In two separate banks in London, criminals exploited weaknesses in technology and human behaviour to fit a keyboard, video, mouse (KVM) to branch PCs. The KVMs, which have a legitimate use, were fitted with mobile phones and used to remotely capture passwords and other data that staff were entering. The criminals then used that information to remotely gain access back into the PCs and to transfer customer funds out.

It can be difficult for anyone to gain access behind a branch counter, but as staff are moved out from behind it and take their PCs with them, the risk increases. If the use of KVMs was thought about before these particular incidents, it wasn't taken into account and in all likelihood nor will the next piece of legitimate equipment exploited for criminal purposes.

Information Security

The protection of customer information is of vital importance. Customers rely on it to keep their personal dealings confidential and regulators insist upon it. It may not only be the open plan nature of bank branches that generate an issue but the unintended actions of international banks, setting Group designs without due or in fact any regard for local sensitivities.

Although some of these issues already arise, if more staff are pushed forward into a space that is shared with customers, the problems will increase. Sound reinforcement is already used to increase the ambient noise level, but that is of limited use. Staff need to talk to their colleagues, head office and others about customer issues.

Computer screens tend to face away from customers, reducing the possibility of overseeing and in a traditional branch this is relatively easy to achieve. The same cannot be said in open plan offices, if customers are circulating around a branch. How are screens to be protected and the documents that will be lying on desks secured?

Designed for security but little customer interaction

RedLeaf Consultancy is a Security Practice with a depth of understanding in securing banking activities from bank branches to critical 3rd party suppliers.

For more information visit our website:
www.redleafconsultancy.co.uk

Or to discuss your needs email:
info@redleafconsultancy.co.uk

New branch designs represent a long term investment and similarly requires a long term risk assessment to ensure that in built vulnerabilities can be recognised

Lifecycle Risk

In what may appear to be a low risk environment, especially in one where a business strategy demands cost reductions and increased revenues, security can be seen as a drag on modern day banking. But new branch designs will have a long lifecycle and over that period of time the threat picture will change as criminals exploit weaknesses.

If those weaknesses are built in, they can present a serious problem as taking retrospective action to negate their effects can be costly. While projecting what may happen in the future is difficult and requires a more analytical approach than short term threats, there is no reason why it cannot be reasonably undertaken. This and the well documented vulnerabilities that can be exploited, will lead to the impacts being realised and the risk picture projected.