REDLEAF CONSULTANCY
A SECURITY PRACTICE

With a Rise in Cyber Threats and a Fall In Bank Robberies is There a Future for Bank Physical Security?

Cyber Threats Are On The Rise And Bank Robberies Have Bottomed Out – Where Does Banking Physical Security Sit Now?

The 21st Century Change

If there is one industry that is transforming in the digital age its banking. Gone are the days of employers paying their workforce by cash, contactless cards are used for transactions and online banking is pervasive. Bank branches are being closed, seemingly on a daily basis as technology takes hold, tighter cost control on operations imposed and staff numbers reduced.

Daily the spectre of Cybercrime is in the news; attacks from nation states, organised criminal gangs and teenagers in bedrooms is where the 21st Century threat lies. The ability to sit remotely and untraceably, to steal money with ease, disrupt systems with a keystroke and to damage a banks reputation, without setting foot inside the door is clean, neat and a threat to a banks very existence.

With crime seemingly moving online and studies suggesting that overall crime in the West is falling, it is perhaps little wonder that the number of bank robberies has dropped. The British Bankers Association has reported that the number of bank robberies in the United Kingdom fell from 847 in 1992 to 66 in 2011. A significant fall and with the attention of governments and the industry on cybercrime, what is the role of physical security in banking, no robberies, no raison d'être?

Security Risk is one part of a banks overall Enterprise Risk Management programme. It does not sit outside but is an integral part of risk based decisions made in light of the facts

Security Risk

The world of Risk Management is moving on, as risk becomes imbedded within business lines, it is they who deal with risk issues as part of normal business. Risk Management, including Security, is there to set strategy, maintain a monitoring regime and report within the Enterprise Risk Management Assessment Framework. In addition, it is there to provide specialist advice, not only to ensure consistency and project evaluation but where specific skills are lacking within business lines.

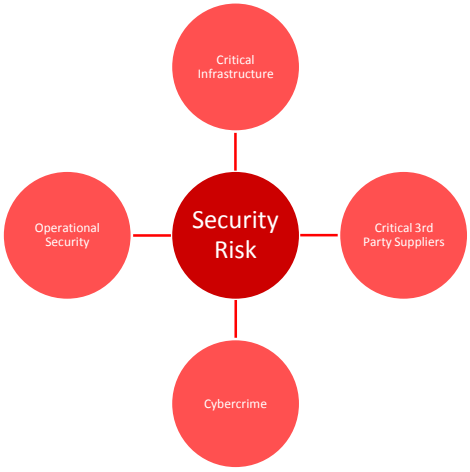
Physical security is not about bricks and mortar, electronic security devices or guards, it is about evaluation of the Security Risk. It requires a deep understanding of the threat, the vulnerabilities that there may be to any threats, the impact those threats would make if realised and how those threats could be treated to mitigate the risk. It is from this analysis that those senior executives and members of the board, who are tasked with managing and governing a bank can decide on what actions to take.

Security Risk is set within the same framework as all other risks within a bank, whether that is Liquidity, Credit, Regulatory or Legal. They could in effect, if not managed properly, seriously affect a bank's ability to operate, result in serious fines and reputational damage. Bank robberies remain a risk and have to be managed but they are not (and never were) a risk to any bank. Robberies had to be managed to ensure staff and customer safety not because of the losses incurred. The damage caused to banks through the recent recession, product miss-selling and the severe fines imposed by regulators are examples of the clear stresses that banks can be put under and survive, even with reputations and balance sheets diminished.

Where Is the Risk?

Physical security is often taken as protecting assets, which it is, but what is actually being protected is a banks ability to operate. Operations, whether they are Retail or Wholesale banking activities, cheque clearing or electronic payments rely on key support elements; its critical infrastructure and 3rd party suppliers. Added to this there are the daily issues posed through Cybercrime and Operational Security.

Although there will be Business Continuity Plans in place to allow for unforeseen outages, BCP is a fall back and to some degree reactive position, whereas security is proactive in identifying potential risks to operations. It is through proactively establishing the risk posed to a bank, by these 4 key elements and bringing them within Enterprise Risk Management, that the risk of not being able to operate can be recognised.



All businesses have dependencies and some, including suppliers and infrastructure are key in banking operations, with their loss or compromise providing a serious risk issue

Critical Infrastructure

While Critical Infrastructure is often cited in relation to countries, it is equally applicable to banks and describes the assets that are essential to their operations. Typically those assets are taken to be Head Office buildings, where there is a concentration of staff undertaking business critical functions, as well as Communication Hubs, Data Centres and Cash Centres.

As banks reduce the number of head office buildings they occupy and generally demand more from their property portfolio, the criticality of these buildings is increasing. In a sense the inbuilt resilience that there was with a number of head office locations is being lost, with staff and the functions they perform being concentrated into fewer sites. While the overall threat itself may not increase, the impact that it would have, if realised, would probably be substantially more than previously allowed for.

Tackling the risk posed by critical infrastructure is one of the key building blocks in developing resilience within organisations. Through systematic security review of the operations within the buildings, the level of security provided, when taken against the threat, ensures a high degree of understanding the risk.

Critical 3rd Party Suppliers

It is probably the case that as business processes were outsourced or new services bought in that the reliance on 3rd Party Suppliers increased. From cleaning to computing and from cash to clearing, there is a dependency on suppliers to deliver in line with Service Level Agreements. However some suppliers, either because of the services they provide or the unique products they offer are deemed as being critical.

The loss of a critical supplier or even just their disruption could have a catastrophic effect on business operations. It is normal that contracts are managed by a relationship manager, Procurement Department and overviewed by Internal Audit. In addition, it is highly likely that there is a Business Continuity Plan in place for any service outage.

It is also undoubtedly true that if these services were in house that they would come under the Security Risk structure. The threats would be known about, probably because they are part of the overall threat to the business, the vulnerabilities explored, impacts analysed, risk mitigants proposed and be part of regular Security Risk reporting. Leaving critical 3rd Party Suppliers outside this process is, to a large degree, blindsiding the Risk Programme.

Cybercrime

The interconnectivity of the world seems to be unstoppable and it is without doubt a critical function for businesses and individuals. If reports are to be believed and there is no reason not to, some businesses are attacked thousands of times per day. Whether those attacks emanate from nation states, organised criminal gangs or teenagers, without ongoing preventative measures, industries centred around digital technology may fail and the promised increase in business revenues lost.

Countering aspects of cybercrime clearly falls to those individuals who have a depth of technical knowledge, enhanced by qualitative experience, in dealing with head on threats. This goes beyond simply knowing how malware functions but how its effects can be managed and mitigated.

Assessing the degree of risk that cybercrime actually poses to banks is difficult to quantify, as published information is scant. However, what is known is that this form of crime can, in some cases, rely on insider assistance. If the goal of cyber criminals is that great and they cannot overcome the cyber defence mechanisms, it is highly probable that they will exploit other weaknesses.

Those weaknesses are likely to centre around people, procedures and facilities. Unlike cyber threats, these forms of threats are not new. The issue of insider threats did not come about with the digital age, the effects of terrorism were felt long before Al Qaeda and hostile nation states were always after information from targeted companies.

Establishing the risk posed by cybercrime is not only a case of monitoring the number of attacks that take place, it is also about understanding within the physical security world what may allow those attacks to succeed. It's about generating uncertainty in the mind of any attacker, it's about the proactivity of all security measures and it's about the maintenance of an effective monitoring regime. What is being generated is a strong security culture and it is this that provides the qualitative aspect to Security Risk reporting. Cyber security is not a standalone risk, it has dependencies.

Operational Security

Operational security is the day to day running of security within an organisation. It is about ensuring the analysis required to track threats including robbery, kidnapping, terrorism and protest groups is in place and used to generate intelligence. That together with a monitoring plan is employed to systematically collect, collate and evaluate information relating to protective measures. Through its maintenance, direction is provided on which areas need reinforcing. It is also about ensuring protective measures are promulgated and those responsible for incident response are well versed in dealing with, what may be, life threatening incidents.

Cybercrime is a major threat with high frequency attacks and is a source of serious concern. It is however only one security risk that a bank faces and without evaluation of those risks a bank may be blindsided. Physical security always had a raison d'être beyond robberies with quantification of the risk proving that

Does Physical Security Have A Raison D'être?

While it might be the case that Cybercrime is the intensive focus of business and government, it is far from the only risk that banks face. Cyber attacks are high frequency, while those affecting critical infrastructure and critical 3rd party suppliers are much less so, but their effects could be catastrophic for the bank concerned.

Threats are changing, bank robberies are infrequent but the way in which modern day business is undertaken has meant that threats are posed in a different way. Enterprise Risk Management provides an opportunity for physical security risks to be set beside and evaluated with the range of other risks that a bank faces. It is through this that it can be seen that bank robberies were not the only raison d'être for physical security. Physical security is essential for protecting operations and ensuring banks can deliver their objectives.

RedLeaf Consultancy

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

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