GENETEC PERSPECTIVE

The challenges of securing banks in the new normal

Evgenia Ostrovskaya
Genetec

Evgenia Ostrovskaya, Business Development Director, Genetec

The emergence of new fintechs had already disrupted the competitive landscape of retail banking, prompting traditional banks to adapt the way they conducted business well before COVID-19. The arrival of the pandemic, however, brought a chain of events that changed everything.

Banks had to recalibrate their business models and make the unprecedented transition to remote working overnight. Branches were forced to close and customers had to shift to online banking, something which has now become widely adopted. As a result, branch numbers have greatly declined, with KPMG reporting that 25% of branches globally have shut down and the remaining 75% are operating at reduced hours. But these stories of relentless decline often conceal a more complicated reality – many financial institutions are in fact investing in branches and modernising their existing ones to appeal to the new age customer. There is still a lot to be gained from in-person banking, particularly as it offers consumers something that digital players cannot – and that is empathy.

Many financial institutions are in fact investing in branches and modernising their existing ones to appeal to the new age customer

Recently I was fortunate enough to participate in an online workshop with Morten Jorgensen, head of consulting at RBR, to discuss the impact of COVID-19 on security operations, as well as the challenges facing organisations as they navigate through the new normal. Outlined below are a few takeaways from the discussion.

Where cyber meets physical

Cyber attacks on financial institutions are growing in frequency and are becoming more diverse, ranging from simple phishing attacks to complex attempts to access credit cards and bank accounts. The results are extremely damaging to both revenue and reputation; in 2020 alone US banks lost $4.2 billion to cyber criminals. That financial institutions should be targeted is far from shocking as the very nature of what they handle makes them an attractive target. However, what is troubling is the plethora of ways in which cyber and physical security threats are converging.

IP security cameras and other security devices are connected to the internet, as it is how authorised administrators access them remotely to check in on their businesses. But this feature can also be their Achilles' heel. If not properly secured, any camera or access control device in the so-called Internet of Things (IoT) can be used remotely by just about anyone, not just those with whom you want to share access. IP cameras, for example, made up a large portion of the Mirai botnet that was used to take town Dyn in a major DDoS attack in 2016. Protecting these devices through effective cyber security now goes hand-in-hand with physical security. Teams need to enhance their cyber posture by investing in technologies and cyber talent on both the offensive and defensive sides to better understand the risks that physical security devices can present to an organisation's corporate network.

Workshop participants highlighted the value of working hand-in-hand with systems integrators and third-party technology vendors when deploying and maintaining physical security systems. Physical security leaders are getting more involved in this process and creating a framework of best practice for partners and colleagues to follow and adhere to across multiple sites.

Indeed, all too often, people are the weakest link when it comes to cyber security breaches. This is either because they lack the requisite knowledge and training to practice good cyber security hygiene or because they are not being properly supported with the tools needed to do the heavy lifting of deploying and maintaining secure systems. For example, the failure to ensure default passwords are changed before a device is connected to the network is a common mistake which offers cyber

criminals an opportunity to gain access. Given a physical security system can comprise tens, hundreds or even thousands of individual sensors, it is sensible to leverage technology to automate this activity instead of relying on fallible manual processes.

Most physical security solutions are a work in progress with new devices being added to expand the system or to replace outdated or broken products. The process of adding new equipment – perhaps from a different manufacturer with less secure standards – is another opening through which a vulnerability can enter the system. One of the most important ways to combat such cyber threats is with a plan. Companies must therefore continue to educate their workforce and support them with technology to ensure company policies are adhered to.

Increased collaboration

Another major concern voiced by workshop participants was the siloed relationship that still exists between information security and physical security professionals. A siloed approach simply cannot keep up with the evolving threat landscape that banks are dealing with today. Digital logs need to be processed, stored and shared with the correct people in the organisation. And most importantly, all IoT devices need to be configured and secured. It is therefore imperative that physical security teams break down these siloes, develop internal relationships with stakeholders in information security and enterprise architecture, and tap into their expertise to minimise risk. This is particularly essential when undertaking complex projects, such as moving from software-as-a-service to platform-as-a-service and developing multi-cloud set-ups.

Security teams are also under more pressure to reduce costs as traditional institutions embrace digital banking to compete for market share. To secure the necessary budgets, physical security professionals should therefore carefully consider how their system of choice can deliver business value beyond the protection of people and premises.

Implementing a modern security system is a considerable investment, but when configured correctly, it can be transformational for all manner of business operations. Streamlining operations, simplifying compliance and gaining a better understanding of how branches are being used are just some of the possibilities. Working with colleagues at the outset to pool resources and define the requirements is vital in sourcing a truly unified system with capabilities beyond what any one department could hope to deploy on their own. ■

Implementing a modern security system is a considerable investment, but when configured correctly, it can be transformational for all manner of business operations