Emerging security risks for banks: Trouble begins at home in most cases

ET CONTRIBUTORS | Feb 27, 2018, 11.18 PM IST

Malicious insiders need to be considered just as much as any external threat. The cybersecurity threat is serious, concerted, sophisticated and it constantly evolves.

Kiran Shetty, CEO, Swift India

Networked technology is introducing huge benefits – making hitherto unthinkable advances. The inroads and advances that have been made in India and introduced here are outstanding – just consider how much mobile banking is being done here.

But the risks the networked world brings can't be ignored: security is key to ensuring that we reap the advantages of these advances. The financial sector has invested hugely in security – and, logically, it is among the most advanced when it comes to IT security. But clearly, there is more to be done. Malicious insiders need to be considered just as much as any external threat. The cybersecurity threat is serious, concerted, sophisticated and it constantly evolves. Our security behaviours have to evolve with it.

At SWIFT, more than 11,000 customers in more than 200 jurisdictions around the world rely on us for their messaging making security our priority. While all customers are responsible for protecting their own environments, we have established a customer security programme (CSP) to assist customers in protecting and securing their local environments; in preventing and detecting frauds in their commercial relationships; and in sharing and utilising fraudrelated information to defend against cyber threats.

We are engaged with our customers both in developing and in rolling out this programme; running workshops; roadshows; webinars; roundtables; training sessions and more, raising awareness and ensuring the programme and its tools are properly understood and adopted. Over the last 18 months in India alone, we have run multiple events, including six security boot camps, a CISO and CTO Forum, and a regional conference almost wholly focused on security. There were roadshows in collaboration and coordination with the Indian Banks' Association and the Reserve Bank of India.

A particular focus now is on our new customer security controls framework, a detailed description of customer security controls. These controls provide a security baseline for the community, clearly describing which mandatory and advisory security controls customers should implement both on their local SWIFT infrastructure, and on the full endto-end transaction ecosystem within their firms.

All SWIFT customers had to attest to their level of compliance with the mandatory controls by December 31, 2017 and 89% of customers, representing 99% of SWIFT traffic met the deadline. This was an overwhelmingly positive response from the community, but that is just a first step. All customers should now be working both to absorb this information from their counterparts and build it into their risk assessments, and to address any gaps in their own compliance with the mandatory controls.

All customers will also have to re-attest by the end of this year, confirming their compliance with all mandatory controls. We will work closely with customers in India, as we will right across the world, to help ensure their preparedness. Cyber preparedness cannot come soon enough; a security mindset is pivotal, wherever the threat may be coming from, inside or outside organisations.

Since the incident in Bangladesh in early 2016, we have worked with customers who have experienced incidents, both to assist them, and so that we can share anonymised insights back with the wider community. In every case, we have seen the same basic patterns. Firstly, the customer's local environment is compromised, and second, valid operator credentials are obtained and used. In protecting against these critical first two steps, customers must consider both insider as well as outsider threats – the attacks will not necessarily be perpetrated by remote outsiders, malicious insiders present just as much risk.

Cyber risk is not limited to technology risk – it is also a people risk. The mandatory controls set out in the framework are designed to help customers structure their approaches to these risks: a lack of user privilege segregation; missing transaction business controls; poor password policies; inadequate logical access controls; or shortcomings in personnel vetting. These controls should apply throughout organisations, ensuring that no access permissions or privileges are unintentionally granted.

Once the attackers have obtained valid credentials, attackers (or insiders) can then submit fraudulent messages and subsequently attempt to hide the evidence. Here, users need to implement measures for prevention and detection. This includes monitoring

transactions, managing business relationships and reconciling activity – SWIFT provides capabilities for all these; as well as ensuring the rigorous implementation of business flow security measures. The financial sector has to operate with an assume breach mentality.