Risk management for cybersecurity in Islamic banks

A cybersecurity strategy is primarily a risk management and risk mitigation approach used to ensure policies, procedures and tools are in place and regularly updated to reduce the risk of a cyberattack on the organization. The prolonged and severe pandemic has brought many risks for banks but one of the biggest is the increase in cyberattacks. From February to April 2020, there was a 238% increase in cyberattacks on the financial sector globally, according to Carbon Black. The biggest impact of a cyberattack is productivity loss resulting in direct financial loss and damage to the brand. SHARJIL AHMED writes.

Sharjil Ahmed is the co-founder and CEO of Cykube. He can be contacted at sharjil.ahmed@cykube.com.

Why have these attacks increased? The work-from-home concept practiced by employees during the coronavirus pandemic has caused a sudden multifold increase in cyberattacks. Organizations now have a much wider area to ensure protection so that no loopholes are left open that will allow cybercriminals to enter an organization's network. As an example, there was a 667% increase in spear-phishing email attacks since the end of February alone. Why?

Spear-phishing is simply a mechanism used by cybercriminals to disguise as a trustworthy entity in an electronic communication to steal sensitive data such as usernames, passwords and credit card details for malicious purposes. In the financial services industry, these attacks are especially targeted at bank executives, particularly in private banks, acting as high-net-worth prospective customers.

Working from home, as well as the inability to meet face to face, just makes it easier for the executives to fall into this trap. By clicking the links sent by the cybercriminals, it could end up targeting the individual or even compromising the bank's entire infrastructure with ransomware. This is just one of the many scenarios.

Cybersecurity is one of the biggest risks institutions are facing globally and Islamic banks are not immune from this either. The CIBAFI Islamic Global Bankers Survey 2019 ranked cyber risk as the number one risk facing Islamic banks. The World Economic Forum cites a global value of US$5.2 trillion that will be at risk from cyberattacks in the 2019–23 period.

What can Islamic banks do to minimize the risk of cyberattacks?

One of the fundamental steps is to have in place a clearly defined cybersecurity strategy with a cyber risk management policy. Many banks have not focused on this matter, and either do not have any strategy at all or the strategy is flawed. According to some Islamic bank senior executives whom I have personally met, their response to my question about a cybersecurity policy/strategy was, interestingly: "We are too small for cybercriminals to attack us." This is the biggest misconception. It is not a matter of 'if' anymore but 'when'. It will happen to every financial institution — it is just a matter of time.

Cyberattacks do not only cause a loss of customers' data or capital but also cause a bigger risk for banks such as reputational risk, which has a domino effect on the bank's credibility and reflects the operational failure of the bank's risk management policies. If a bank's reputation is at risk and customers risk losing their money and sensitive information, this could have a systemic impact on the financial institution. Hence, it is no longer a chief information officer or chief information security officer who will take care of the situation but the CEO, CFO and board equally need to ensure compliance with security policies.

How can Islamic banks introduce a well-defined risk management policy for protection from the imminent threat of cyberattacks?

First and foremost, banks need to define their risk appetite which needs to be set and approved by the board members. The next fundamental step is to determine what procedures and risk mitigation policies banks have in place in case of a real cyberattack leading to the temporary disruption of the bank's digital services and the compromise of clients' data.

Institutions can manage their risks effectively if there is support from senior management and defined risk management processes and policies are in place. A risk-aware culture and regular assessments of defined risks against the objectives of the organization are also key.

The primary objectives of the risk management process are to identify the key threats and issues, assess the

Continued

impact, communicate with the key stakeholders within the organization and address the consequences. It can only be effective once these risk management activities are embedded within the business process such as responding to incidents, product development and design, and sales and social media campaigns.

Awareness of cyberattacks and the associated risks should be communicated regularly across the organization. There should be dedicated training hours allocated for cybersecurity for all members of the organization which should be made mandatory. This keeps them abreast of all the latest developments and threats to be aware of as cyber risks are constantly changing.

Ideally, banks should have a separate budget allocation for cybersecurity with a clear key performance indicator of what level of risks would be mitigated using this budget. This goes back to the first question of risk appetite. This budget can only be set once banks have performed a full risk analysis along with commercial exposure in case of an attack materializing. It allows a bank to explore the degree to which its assets require protection and how this can be managed effectively.

Generally, in most organizations there is a serious disconnect between the business executives and board members. To bridge this gap, it is important to have a clear understanding and support among the board members and the executive committee, which will allow them to have a unified cyber risk management and mitigation policy across the organization. It is equally, or even more, important for an Islamic bank's management and executive board to ensure a high level of security since they are appointed as the custodians of clients' funds and data and it is their moral and ethical responsibility to have a well-defined and executed cybersecurity strategy to protect them.

In conclusion, it is an ongoing process and to be able to thwart cyberattacks on your organization, you continuously need to be at par with or one step ahead of the latest tricks and tactics of cybercriminals.