Get Cyber Serious With Vendors

by Steve Brown

Ok, we don't want to freak you out, but we came across an interesting story about researchers at MIT who have created a robot controlled by human thoughts. That's right - this robot responds to commands triggered by thinking alone and does not need electronic or voice commands. Given all the weird stuff people think about during the day, we wonder how these robots will someday respond.

While not as cool as think-moving a robot perhaps, almost all community bankers we know are worried these days about how best to respond to the risk of cybersecurity. If you are leaving this issue to vendors to solve, note that as we said recently, the regulators aren't messing around here and scrutiny is at an extreme level. In short, this is a national security issue, so your team should be taking extra steps now to ensure compliance.

In particular, regulators are warning banks that outsource core operations and/or security administration to make sure vendor management programs are designed to manage and mitigate cyber threats. Understand that national security issues raise the bar to the highest level possible, as that definition means the government is working to protect our secrets and citizens from enemies domestic and abroad.

Cyber risks affect bank activities at many levels. These include technological, regulatory, operational, strategic and even customer trust. Not only that, cyber threats that community banks face can be at least as difficult to mitigate or root out as they are for much larger banks and entities.

Unfortunately for community banks with limited resources, it is often necessary to rely on networks of outside vendors for operational cost effectiveness, stability, and innovation. Yet, those very same relationships may open you up to added risk as they increase potential hacker access points. As such, it is important to set cyber security expectations up front with your vendors - even if it seems like a basic thing to do.

Another thing to do here is to ensure ongoing monitoring of services provided by your vendors. It may even be helpful to have your own team of specialized professionals make it a point to stay informed through cyber industry events and communications. Sharing information within the industry is becoming more critical to stay ahead of the culprits.

At a recent conference, Comptroller of the OCC Curry opined that vendor relationships can pose "significant" risks to banks. While he did not discourage the use of vendors, he underscored the need for careful monitoring in these relationships and with other connected suppliers downstream.

To do so, community banks may also want to consider contractually obligating their outside vendors and contractors that interact with sensitive data. Here, you want to be sure these players have their

own cybersecurity measures and make sure that the bank is notified quickly in the event of any kind of breach.

According to PwC research, the contract is the strongest form of security assurance between any company and a third party vendor. They indicate the contract should be used to spell out all cyber security conditions and obligations.

Additionally, once you have things in writing, be sure to assign someone in the bank to be in charge of monitoring and reporting to management and the board around third party activity. Doing so will ensure your bank is communicating regularly with your third-party vendors as to your security expectations, especially as regulations become more vigorous.

Finally, don't forget to be aware of and think about the scope of access to your data. Limit information access to a "need to know" basis to protect yourself and your customers. Maybe someday you can just think about cybersecurity and it will be taken care of, but until then be careful with your data and have strong controls around third party vendors.

BANK NEWS

Social Usage

Pew research finds 69% of Americans use some type of social media. By age category, this breaks down as: age 18 to 29Ys (86%), 30 to 49Ys (80%), 50 to 64Ys (64%) and 65Ys+ (34%).

Security Constraints

Cisco cybersecurity research finds the primary constraints to adopting advanced security products and solutions are budget (cited by 35% of respondents), product compatibility (28%), certification (25%) and talent (25%).

Digital Push

Accenture Strategy research finds 92% of business leaders surveyed say it is critical or important that they take actions now to transition their workforce to succeed in the digital economy.

Branches

Bank of America research finds 50% of deposits now occur at an ATM (vs. 35% 5Ys ago), 30% are done through tellers (vs. 65% 5Ys ago) and 20% occur through mobile (no comparative here was indicated).

Purchasing Influence

Deloitte research finds the primary places people age 26 to 32Ys old say influence their buying decisions are recommendations from within their social media circle (74%), online reviews by virtual strangers (64%), TV ads (63%) and social media ads (56%).