Swimming With The Online Sharks

by Steve Brown

Even in California with all the surfing going on, people get scared by sharks. There are 470 known species of sharks in the world and an estimated 1B+ roaming the oceans. As if that weren't enough to think about, scientists have now determined that some species of sharks live 2x as long as previously thought.

As you chew on that, consider that community banks have plenty of sharks swimming around them in the online world too. Attacks come in the form of online breaches, phishing, malware and cyber-scams. As such, banks are trying something new.

For years, technology and software firms and larger companies have sponsored "bug bounty" programs. These programs offer ethical hackers (or so-called "white hat hackers") a reward for locating and notifying the firm of vulnerabilities or flaws in their systems or their technology products.

As the risk of online vulnerabilities has grown, more banks are taking a page from companies in the tech space and launching their own bug bounty programs to discover their own weaknesses.

Many banks already embrace penetration testing, or "pen testing" as it is often called. This is where a security solutions company brings in a group of ethical hackers to prod and pry at your systems to find potential flaws that cybercriminals might exploit. That is old news.

Newer news is that by creating a bug bounty program with such companies, banks can broaden the base of would-be testers. Rewards can be offered to both amateur and professional hackers alike. Whichever one successfully uncovers and reports flaws to the bank gets a bounty for their efforts.

For community banks who have long relied on close ties with vendors and the secrecy of their code and their systems to stay safe, the idea of opening the flood gates and encouraging thousands or tens of thousands of "hackers" to wheedle their way in may seem counterintuitive at best, and insane at worst.

Then again, other industries that have long depended on secrecy have embraced this tactic. Witness the Department of Defense's "Hack the Pentagon" program, launched in March 2016. In this case, within the first few months hackers discovered more than 100 vulnerabilities in DoD systems. For its part, online payments Goliath PayPal has paid out more than $2mm in bug bounties over the past 5Ys alone.

According to industry experts in this area, bug bounty programs that are poorly managed can be harmful however. This is especially true those for small-or-midsize businesses that lack the ability to fix vulnerabilities. But, community banks should at least consider the option of instituting a bug bounty program.

Here are a few best practices:

Have the proper internal resources in place. While bug bounty programs rely on reaching out to the broader data security community, banks must also consider what personnel and budget they have to review and repair vulnerabilities as they are reported.

Consider how to suitably value bounties. A bank will not want to throw money at hackers, but there is value in uncovering flaws in the system before the bad guys do. To attract talented insight, value your bounties fairly and be prepared to pay out more for sizable flaws.

Choose a bounty approach that works for you. Some bug bounty programs throw open the doors and encourage all ethical hackers to find flaws. Other programs take a more select approach and work more like a penetration testing exercise. For these, a select group of hacker-researchers are encouraged to poke holes in the system to find weak spots.

There are plenty of cyber sharks swimming around your systems waiting to take a bite, so running programs like these might help patch up holes in your boat to avoid sinking.

BANK NEWS

More Focused

PwC's Digital Banking Survey finds about 33% of customers use all of a bank's platforms vs. about 50% who did so just 5Ys ago.

Account Success

A Deloitte survey finds 73% of bank customers think the account opening process could be improved. By age category the findings were: <35Ys (42%), 35Y to 50Y (35%), 51Y to 64Y (18%) and >65Y (7%). This is important because the same research finds customers seeking improvement are 5x more likely to take their business to another bank when they don't get it.

SIFI Change

Congress is working on a bill that would lift the threshold of when a bank becomes a systemically important financial institution (SIFI) from $50B to $200B. SIFIs are subject to greater regulatory supervision under Dodd Frank.

Branch Shift

Umpqua Bank ($25B, OR) said it will close 33% of its 310 branches by 2020, as it seeks to improve returns, invest more in digital and modernize the bank.

Disaster Construction

It is estimated 10,000 homes and other structures have been destroyed by recent natural disasters in the US. Unfortunately, the positive impact of a building boom that usually follows such things may be slower to come, as the construction industry deals with a labor shortage, labor costs are rising and raw materials costs are high.

ON DEMAND HELP FOR COMMUNITY BANKERS

Community bankers face many difficult challenges every year, but you are not alone. Our experts stand ready to help you address a variety of issues. Go here to view options and opportunities.