



Scaling Up Your Security Efforts

🔒 cyber security security

There are a lot of doozies in the world of strange but true crimes and this one recently caught our eye. It's the case of a Florida man facing assault charges after Fish and Wildlife officials said he tossed a 3.5-foot live alligator into the drive-thru window of a Wendy's. He claims it was only a joke, but local officials aren't taking it so lightly. A judge has reportedly ordered him to stay out of all Wendy's restaurants, keep away from animals other than his mom's dog, undergo a mental health evaluation and remain weapons-free. Of course, none of this is unexpected given the nature of the alleged crime.

Banks always have to be prepared to expect the unexpected or risk getting bitten--particularly when it comes to cybercrime. According to the Identity Theft Resource Center (ITRC), there have been 5,754 data breaches between Nov 2005 and Nov 2015, exposing some 856mm records. Further, IBM research estimates that the average breach costs \$3.8mm.

As you build protections against cybercrime, you have to be careful not to derail your own efforts. Some banks, for instance, may believe that encrypting data is enough to keep hackers out. While it's true that strong encryption is a critical defense mechanism, it's not a panacea. After all, even good algorithms can be susceptible if thieves are persistent enough. Look no further than the Logjam vulnerability uncovered last year. It allowed attackers to intercept and decrypt secured communications between users and thousands of websites and mail services worldwide. There's no doubt that banks need strong encryption, but beyond that, it is critical to utilize sophisticated tools such as advanced detection analytics to help identify emerging threats in real time.

Another area bankers should stay on top of is making sure to have an effective patch management program. Just doing this can significantly decrease the number of security breaches because hackers buy old tools on the Web and repurpose them frequently. They also try to tunnel into weaker systems, so having the latest updates communicates a simple "go somewhere else" message to them.

An effective patch management program should include written policies and procedures to identify, prioritize, test and apply patches in a timely manner, the FDIC notes. Such a program should also utilize vulnerability information culled from threat intelligence sources. Bank boards and senior management need to be held accountable for requiring regular reports on the status of the patch management program and for creating strategies to deal with systems or products that are at end-of-life or close to it.

Next, given more employees are using their own devices for work purposes, banks are asking for trouble if they don't make extra efforts to encourage staff to regularly update their personal computing systems. Just recently, Oracle warned Java home users to beware of a flaw that attackers could exploit in older versions of the application. Oracle urged users to delete any previous installations and replace them with patched versions.

Banks have ample resources to help boost proper defenses. The FDIC, for example, has developed Cyber Challenge exercises, which are a series of videos and simulations that are available free on its website. The

FDIC also has a cybersecurity awareness training program, so send your teams and get the training. In addition, the FFIEC has its new cybersecurity assessment tool, which helps banks assess their risk and better determine cybersecurity preparedness.

Cybercriminals will continue to bare their teeth and try to attack, so be careful when swimming on the Internet. It's up to banks to make sure to have the proper defenses that make thieves feel as unwelcome as finding an alligator in your lunch box.

Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.