
Stone Soup And Cyber Crime

by [Steve Brown](#)

You might remember the story of Stone Soup from your childhood, but if not, here's a short synopsis to jog your memory. Some hungry strangers come upon a town carrying nothing but an empty cooking pot. Local villagers are unwilling to share their rations, so the clever strangers fill their pot with water and place it over a fire. Curious townspeople ask what they are doing, to which the strangers reply they are making "stone soup." Soon, all the stingy townspeople want some of the enticing soup and begin to donate previously withheld items like carrots, potatoes and onions. More and more villages contribute to the soup and in the end a hearty and delicious pot of soup is shared by all.

The story clearly highlights the power of collaboration--a lesson that is extremely apropos when it comes to fighting cyber crime. Online crime has become all too prevalent in recent years, with more and more retailers falling prey to crooks' costly schemes. Many banks are frustrated, and understandably so, as the clean-up costs associated with the growing list of high-profile data breaches continue to mount. But rather than placing blame for cyber crime, we urge you to heed the lesson from Stone Soup: there's more to gain by working together toward a shared solution.

When the system fails, everyone loses. If the data breaches keep happening--regardless of who is at fault--customers will be less likely to adopt new technologies that are coming to market. It won't bode well for mobile banking or mobile payments or other innovative ideas that are yet to come.

Of course, it almost goes without saying that on an individual basis, companies need a well-defined strategy for fighting cyber crime. They need to make sure that they have adequate security measures in place, employees are well-trained in online crime prevention and business partners are held accountable.

It's also become obvious that a large number of companies are going to have to spend significantly more money on prevention and detection. A June study by PricewaterhouseCoopers LLP showed a significant connection between the level of spending on cyber security and the number of events detected. Yet the same survey found that retailers--which have been getting slammed with data breaches left and right--are outlaying significantly less on cyber security measures than other industries. Retailers spend only about \$400 per employee, while banking and finance companies spend roughly \$2,500 per employee, according to PwC.

Still, no company can realistically expect to fight the massive online criminal world alone. It will take a united team of business leaders from multiple industries, security professionals, and utilities and regulators, to make any real progress. There are some signs of this happening already, but even greater collaboration is called for. According to the PwC study, only 25% of respondents participate in Information Sharing and Analysis Centers (ISACs) and only 15% work with public law enforcement agencies. Sensitive data is only as strong as the weakest link in the chain, and there's way more work to be done.

The criminals aren't going away, but the US will have a better chance of keeping them at bay if everyone works collectively toward a common goal. The reward for doing so will be even more

satisfying than a piping hot bowl of vegetable soup.

BANK NEWS

Bank Closed

(15 YTD): Regulators closed: NBRF Financial (\$188mm, MD) and sold it to Howard Bank (\$533mm, MD) under a P&A agreement. The agreement calls for Howard to get 5 branches, all deposits and most of the assets.

M&A

First Southern National Bank (\$668mm, KY) will acquire First National Bank of Muhlenberg County (\$149mm, KY) for an undisclosed sum.

M&A

Starion Financial (\$1.1B, ND) will acquire WPS Community Bank, FSB (\$98mm, WI) for an undisclosed sum.

M&A

Pinnacle Bank (\$3.9B, NE) will acquire Home State Bank (\$83mm, NE) for an undisclosed sum.

M&A

Harbor Community Bank (\$695mm, FL) will acquire First America Bank (\$266mm, FL) for an undisclosed sum.

Branch Closures

First Niagara Bank (\$38B, NY) said it will close 17 branches as it adjusts to a customer shift toward more digital banking and a resulting decline in branch traffic.

Apple Pay

Apple announced it has signed up 500 more banks in addition to the 6 largest US banks it announced during the launch of its Apple Pay service, which is now available today.

EMV Launch

A report by the Payments Security Task Force projects almost half (47%) of merchant payment card terminals in the US will be able to process EMV chip cards by the end of next year. Meanwhile, the 9 largest US card issuers project they will distribute 575mm EMV cards by that time.

Cyber Spending

JPMorgan said it plans to double the amount it spends on cyber security over the next 5Ys or about \$500mm.

Lower Profitability

FDIC data shows service charges as a percentage of noninterest income for the banking industry have fallen to the lowest level in 70Ys. Experts point to a sharp increase in regulation and increased customer use of alternative financial products as likely drivers for the trend.

Shadow Banking

The Fed is reportedly preparing to move forward with rules that would impact the so-called shadow banking system to reduce risks in short term funding markets during periods of volatility. The rules are expected to tighten up margin requirements for hedge funds, private equity funds, money market funds and others deemed to be shadow banks.

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.