



## Binging On Behavioral Analytics

by [Steve Brown](#)

Lately, it seems everyone is binge watching something. Whether you are churning through Game of Thrones, Breaking Bad, or something else it can be fun. In fact, according to Deloitte, 73% of people have binge watched and the average time they spend doing so is five hours at a clip. The bad news - other studies have found the more you binge watch, the lower quality of sleep, greater symptoms of insomnia and higher fatigue. The way people behave is interesting and perhaps that is one reason behavior analytics are being used more in banking and the broader corporate world.

Many information security experts point out that one of the biggest security vulnerabilities is the human employee. Hence, behavior analytics are becoming the life blood of information security and especially within banking.

Understanding where risks are surfacing in the technology layers of your bank typically requires a vast amount of data. Crunching all of this as you include a focus on users can help prevent malicious or more innocent insider threats. By determining whether employee activities are consistent with normal behavior, your teams can more readily correct issues before they get too large.

[Research firm IDC predicts that in 2017](#), behavioral analytics across compliance, fraud, cyber detection and prevention will be installed at 15% of banks. This will help banks avoid losses, regulatory fines and sanctions. In fact, banks have already made a big start in the fraud space, with FICO having introduced behavioral analytics in the early 1990s. It now is used to analyze 67% of the world's payment card transactions for fraud.

Behavioral analytics has also become a prominent area for cybersecurity defense, with many vendors emerging in this space. Behavior analytics in cybersecurity is defined as using software tools to detect patterns of data transmissions in a network that are out of the norm. The theory is that the analytics tool would detect the anomaly and alert managers, who would stop the unusual behavior or breach.

While the market for user behavior analytics is still relatively nascent, it is quickly gaining steam according to 451 Research. Adding artificial intelligence (AI) and machine learning technologies eventually will help banks take a more proactive approach to corporate defense.

It's no secret that community banks are spending more for cybersecurity, but CIOs will continue to struggle to balance cyber investments against managing risks to the core business.

Behavioral analytics is also increasing as phishing scams become more convincing and connect with their intended targets more. Behavioral analytics relies upon anomaly detection to identify patterns that do not conform to those statistically expected. In the context of security, such anomalies might represent a variety of threats. These include intrusions to networks by an impostor, unwarranted escalation of privileges, and transmission of sensitive corporate information across irregular channels.

Perhaps it is time to start exploring the benefits of behavioral analytics. It could be yet another step to help keep your bank safe without breaking your IT budget.

## BANK NEWS

### Over Their Heads

A CareerBuilder survey finds 56% of workers say they were "in over their heads" in debt and the same percentage claimed they save \$100 or less each month.

### Initiative End

The Department of Justice has confirmed it has ended the controversial Operation Choke Point initiative, which sought to curtail legal but politically disfavored businesses.

### Fewer Employees

FDIC data finds that from Q2 2016 to Q2 2017 total employees for financial institutions with assets <\$1B declined from 146,727 to 139,456 or about 5%.

### Consequences of Unwinding

Stocks and corporate bonds may be the surprise big losers once the Fed starts reducing its \$4.5T balance sheet, according to a JPMorgan Asset Management strategist.

### Office Space

International Facility Management Association research finds 70% of US office spaces are open concept layouts.

### Tech Growth

Forrester Research finds CIOs at US public and private organizations expect to increase technology spending 4.85% this year and 5.2% next year, as the focus on cloud technology increases.

### Municipal Stress

A National League of Cities' survey finds only 69% of cities say they are capable of covering their financial obligations. This is the lowest level in 5Ys and most claim this is due to needed infrastructure repairs and increasing employee wages and benefits.

### Payments Challenges

An ABA Payments Strategy Survey finds the largest challenge with payment technology reported by banks is data security, followed by technology integration. Other challenges noted were changing customer preferences (52%) and finding the appropriate partners (48%).

### Engaged Clients

Schwab finds their robo advisor clients are more likely to open weekly emails (50%) and 2-3xs more likely to click links within the email. These clients favor technological channels which drives this high email engagement.

### Cyber Crime

The Department of Homeland Security reports that the primary motives for cybercrime are financial gain, espionage and activism.

## INTERNATIONAL SERVICES FOR COMMUNITY BANKS

Our [international services](#) are designed for community banks to help you capture more customers and fees. Contact us today for more information.

*Copyright 2018 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.*