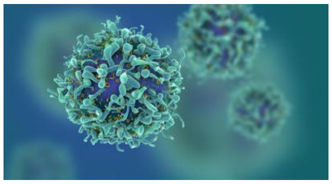

Going Molecular To Solve A Big Problem

by Steve Brown

In a great news story, scientific researchers at London's Royal Marsden Hospital have reportedly been able to dramatically shrink tumors related to ovarian cancer. A reported 70% of patients with a specific molecular target responded positively to the drug. Scientists are calling this the biggest breakthrough in ovarian cancer in a decade and that is good news indeed.

In banking, technology experts have been seeking good news when it comes to defending against security breaches. According to Identity Theft Research Center, last year saw a 40% increase in reported data breaches, including the largest in history affecting a billion Yahoo accounts. This year is not looking much rosier. As banks increase their IT budgets to account for the growing importance of cybersecurity, a new issue needs to be considered - the false positive.

One of the big issues in cybersecurity right now is this phenomenon known as false positive. This is when systems detect a threat where none exists. While a false positive alert results in no damage, it still requires investigation. The cost of the cyber alert system and its follow-up inquiries may seem reasonable at first glance. But add in a high level of false positives, and cybersecurity costs are on the rise quickly.

How prevalent are these false positives? Apparently, they happen all the time. A Ponemon Institute survey of more than 500 IT professionals in the US looked at the state of malware detection and prevention. Of the thousands of malware alerts coming out of cybersecurity systems, about 29% were investigated as real potential threats. However, 40% of those investigated incidents were deemed false positives. That's a lot of time spent chasing ghosts.

The amount of wasted time can be particularly taxing for community banks who have limited staff. Also, regulators expect high compliance standards for fraud and cybersecurity. Banks could end up spending so much time responding to false positives that they have little time left to improve detection and response.

In the Ponemon survey, 68% said they were spending a significant amount of time chasing false positives, but only 32% said they were spending a significant amount of time prioritizing alerts that need to be investigated.

In this same survey, 36% of participants said that C-suite executives were given information related to cyber episodes only on a "need to know" basis, while 34% of participants never informed the C-suite of cyber incidents at all. Although the IT team may be even busier these days, communication is a critical component of your cyber prevention plan. It may be a good time to ensure regular updates are built into your plan and practices.

Getting a handle on false positives is no simple matter, of course. Detection programs work on algorithms and their rigid rules invariably spit out false positives. A new class of algorithms that take a less restrictive approach may offer some relief, however. These algorithm programs are touted as better at separating real threats from false positives.

If these new algorithms live up to their billing, they might help bankers improve cybersecurity detection while reducing the cost and time to follow up on false positives. This would indeed be good news. That said, we shouldn't be lulled into a sense of false security. In the world of fraud and cybercrime, today's security solution is often just another wall to scale for cybercriminals.

BANK NEWS

Vendor Understanding

A Deloitte survey of senior corporate leaders worldwide finds that while 55% say they have a reasonable to excellent understanding of third parties they use, just under 14% say they have forward looking vigilance capabilities to identify imminent risks and performance issues of those vendors.

Compliance/Ethics

The Wall Street Journal reports that a survey by business ethics advocacy organization Ethisphere Institute and compliance services firm Convercent of senior level executives involved in compliance, ethics or anti-corruption programs finds 49% say they are almost always or regularly involved in strategic decisions (vs. 39% in 2015).

Governance Framework

Regulators indicate a good corporate governance framework will include: setting the bank's strategy, objectives, and risk appetite; establishing the bank's risk governance framework; identifying, measuring, monitoring, and controlling risks; supervising and managing the bank's business; protecting the interests of depositors and shareholders; aligning corporate culture, activities, and behaviors with the expectation that the bank will operate in a safe and sound manner, with integrity, and comply with applicable laws and regulations.

Personal Risk

A DLA Piper survey of compliance executives, in-house counsel and directors finds 67% of chief compliance officers say they are at least somewhat concerned about their personal liability.

Retirement Saving

Research by the Fed finds the primary ways people save for retirement are as follows: 401k (50%), outside savings (46%), IRA (31%), none (28%), and a defined benefit pension (25%).

SHARED NATIONAL CREDIT WEBINARS: JULY 13 AND JULY 20

In this 2-part webinar series, PCBB's C&I experts will offer a deeper understanding of Shared National Credits (SNC). You'll also, learn how PCBB manages its own SNC and how your bank can benefit. Register today by visiting our website.

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.