Do You Have Cyber Alert Fatigue?

cyber security risk management

Summary: There are many security tools that can identify potential threats to your financial institution, but there are also many false positives too. We give you tips to help.

Warren Buffett, also known as the Oracle of Omaha, and one of the best investors in the world has some advice for you. He says the difference between successful people and really successful people is that really successful people say no to almost everything. His point -- constant focus drives success.

To be successful when it comes to cybersecurity, you have to focus too. After all, there are many security tools that can identify potential threats to your financial institution (FI), but there are also many false positives too. This massive ongoing flow often overwhelms information security professionals. This issue can lead to mistakes, as frequent alerts are often unimportant -- to the point where valid threats might be missed.

Case in point: MasterCard's security executives recently reported that the card company sees as many as 460k intrusion attempts a day. That is 70% more than 1Y ago and a huge problem. In like fashion, UK-based research firm Ovum found in 2017 that 40% of banks were getting as many as 160k duplicate, irrelevant or incorrect cyber-alerts every day.

A typical community financial institution (CFI) may see only a fraction as many alerts, but the challenge is similar. Using the CFI's security staff and tools to weed through too many alerts to try and separate genuine risks from false ones, can be an exhausting and time-consuming process. Hence, we have three key tips to help.

Try using security analytics to winnow down potential alerts. Ovum reports that 37% of banks (including mega-banks) see as many as 200k security alerts daily. It just isn't possible for humans alone to review that many potential threats. Roughly 80% of security teams feel overwhelmed by alerts, according to a survey by SC Media. By using security analytics you can more easily rank potential threats, so security professionals know where to focus their efforts.

Consider using machine learning. Machine learning (ML) and artificial intelligence technologies are both becoming a mainstay as cyber security tools. They can deliver more refined and actionable information to information security professionals. According to at least one study, 90% of FIs cut their false-positive security alerts by using such ML tools.

Simplify. Many companies, including CFIs, invest in security information and event management (SIEM) tools. These are now making alert review more complicated. Ovum discovered that 36% of FIs use from 51 to 100 different IT security tools. Look for a solution that integrates your basic SIEM with security analytics for a streamlined solution.

<B>WHITEPAPER:</B> CECL AND PREPAYMENTS

CECL creates many new challenges for bankers. One of them is prepayments, especially with a diversified portfolio. To learn more about the effects of prepayments on your CECL reserve, download our white paper, "CECL Challenges: Prepayments and Diversification" now.