PCBB

BID® Daily Newsletter

Dec 18, 2017

Delivery Of Cybercrime Pushing Bank Limits

cyber security risk management artificial intelligence

Summary: In 1H 2016, 554mm records were compromised and the cyber thieves are getting more sophisticated. Some banks are turning to AI for help.

Holiday deliveries are already falling behind, so you may want to plan ahead. UPS expects to process 750mm packages this season - up 5% YOY, while FedEx expects to deliver 400mm. Despite strategic investments by the big delivery companies, surging retails sales and much more online purchasing will likely push delivery companies to their limits. Food for thought if your gift gets "lost in the mail".

Banks are also being pushed to their limits when it comes to cybercrime and keeping up with more sophisticated attacks. Cyber-criminals are better at perpetrating card/new account fraud, account hijacking, and other theft.

As the criminals have become more sophisticated, so too have banks. More are embracing the use of enhanced technology efforts utilizing machine learning (ML) and artificial intelligence (AI) to weed out potential threats with greater accuracy and speed than previously possible. Indeed, MIT researchers have demonstrated that a virtual AI security analyst trained by human experts can accurately identify 85% of attacks. This beats previous benchmarks 300% and reduces false positives 500%.

Certainly, it is tough for even the largest global banks to stop nation state or organized crime bad actors. This is even more difficult as hackers improve their technology tools and play a more sophisticated game over time that requires an ever-evolving response from all banks.

With that in mind, it is little surprise that Forrester Research forecasts 300% growth in AI investment this year. Several large banks are already trying to bring AI into their operations, particularly in IT security where it can better detect anomalies. Perhaps even more surprising, community banks are also getting into the AI game. Digital Banking Report research finds 15% of banks w/assets $100mm to $1B has at least one AI solution implemented or that they plan to implement in the next 12 months.

One of the publicized benefits of ML and more advanced AI is that it is purportedly able to reduce the number of potential threat alerts. This allows banks to avoid so-called "security fatigue" that human teams must deal with when receiving a flood of undifferentiated potential security issues.

If your bank is thinking about ways to better leverage AI or ML to keep the bad actors at bay, consider the following tips.

Understand your risks: Using more AI/ML technology may pose new risks in third-party reliance, audit and interconnectedness, so know this as you protect your bank.

Keep up with regulation: The rapidly changing landscape of regulation adds complexity to any new technology adoption. Community banks must keep track of this as it evolves to ensure any changes to your cybersecurity do not lead to unintended consequences for your teams.

Look then leap: Cybersecurity gaps often result when banks do not thoroughly understand or test new technology. The rise of cloud computing, internet of things (IoT) and dependence on third-party vendors adds even more layers of complexity. Consider the full scope of new technology before implementing it.

Stay ahead of the threat: The big issue in security right now is that IT security professionals are always chasing yesterday's attack to predict and prevent tomorrow's attack. Using AI/ML is different, because these technologies can dynamically recommend actions to take, even if the attack being seen has never been seen before.

As with anything, be sure to bring in prudent experts to help and give your team time to get up to speed on the latest things before anyone delivers anything to your doorstep.

OUTSOURCED PROFITABILITY SOLUTIONS FOR YOU

ProfitIntel is an outsourced relationship profitability solution that combines a powerful pricing model with full-time consulting support. Contact us today for more information.