Time to Focus on Mobile Security

We may have improved information security in the office but are we secure on the road?

Mobile devices are often able to access the most crucial company data, but does that mobility put our data at greater risk? Despite drums sounding on mobile security for years, Verizon's *Mobile Security Index 2019* shows that mobile devices continue to be ignored or dismissed when it comes to security protections.

Verizon surveyed 700 professionals involved in buying, managing and securing mobile devices for their organizations. Some 67 percent acknowledged they were less confident about the security of mobile devices than other devices. Not surprising, then, that more companies admitted they'd suffered a compromise that involved a mobile device—33 percent in the 2019 survey compared to 27 percent in 2018.

The vast majority, 83 percent of survey respondents, though, say the risk from mobile threats remains high, and a similar number (85 percent) say they need to take mobile device security more seriously.

When companies were asked what they're doing to improve mobile security, more than two-thirds—69 percent—said they would be spending more next year on mobile protections. At the same time, 77 percent thought that the biggest barrier to protecting data on mobile devices was a lack of user awareness.

Be it money or education, the directive is clear, according to Thomas T.J. Fox, SVP, Wireless Business Group at Verizon: "It's time to close the chasm between levels of protection."

To read the survey in full, go to https://enterprise.verizon.com/resources/reports/mobile-security-index/#report.

Look, Don't Leap: What to Know Before Diving into Machine Learning

Excerpted from the April (ISC)² Insights e-newsletter

Paulo Shakarian

IDC ANTICIPATES a $57.6 billion worldwide investment in cognitive and artificial intelligence (AI) by 2021, which means there's a good chance your company is considering, if not already buying or building, AI and machine learning (ML) solutions for both business processes and security operations.

Paulo Shakarian, CEO and co-founder of CYR3CON, which uses AI to predict cyberattacks, offers some words of advice—and a few warnings—to make sure AI and ML implementations and ongoing usages work as intended and do not lead to data leakage and other potential cybersecurity threats.

Beware of the hype.

Do your homework before you spend a dime (or thousands of dimes), cautions Shakarian. "The hype is mainly coming from vendors. … The CISOs then feel pressure from the executive suite."

What to do before you buy.

Shakarian recommends doing adequate due diligence before an AI/ML purchase.

Engage the board.

"Board members often come across innovations. It's up to the CISO," Shakarian says, "to coach board members on the pros and cons."

Know your business needs.

Not every solution requires AI, Shakarian counsels. "If you're looking to predict something; if you're looking to find something that is abnormal and that would normally require human interaction; if you're looking to optimize the decision-making process in an automated way—I see those as the holy trinity of AI, probably 90 percent of what you need AI and machine learning for."

Challenge the vendor.

When listening to a pitch from a vendor, Shakarian advises information security professionals get answers in some crucial areas.

Peer review.

The first question to ask, Shakarian says, is whether the underlying technology in the product has undergone peer review. "If it's not, that should be a big alarm bell if they're vetting their own stuff."

Relevant data.

Does the data fed to algorithms make sense? Shakarian posed that question in a blog post on this subject. "Regardless of how fancy an algorithm or piece of software is, it's making the prediction based on some piece of data—and you should ask the vendor what that is and ask him or her why it makes sense."

Data security and reliability.

Unless your company is large enough to afford a data scientist or data science department, you're going to outsource to an AI/ML provider. This raises the scrutiny required to ensure these providers keep your data safe and available at all times.

"Transparent" algorithms.

In order to monitor accuracy, you need transparency, Shakarian warns. If the algorithm is a "black box, you can't tell the difference between failure and your normal error rate. Whereas, if there's some level of transparency of how it's producing the results, the user can check up on it."

Updates to the machine learning model.

"…expect that the model is being updated on a regular basis by the vendors. If it's not, that, I think, is a major red flag because there's a high chance that the product might not work as advertised."

Before succumbing to the siren song of machine learning as the business solution, Shakarian believes you should ask if such a solution is needed at all. "Does the business need/require AI or machine learning to address it in an impactful, sustainable way?" If the answer is yes, then you have a roadmap here to follow. ■