Sphinx Logon Vendor Viewpoint:

What's really holding customers back from implementing multi-factor authentication?

Customers know that multi-factor authentication is recommended by security-conscious government entities. Many customers are in verticals that require proof of stronger authentication by their auditing agencies. So why does multi-factor authentication go on the back burner of many corporate security plans?

What we hear repeatedly from our customers is that the multi-factor marketplace is a confusing and complicated space. They know they need to implement something, but one vendor suggests an invasive solution that requires reconfiguring their current systems, another wants to send in a consultant to analyze their needs. Then there are the cloud solutions that mean giving away control of your most valuable data, which make many IT managers uncomfortable.

When it comes to protecting access to corporate networks and logon locations, we believe that getting back to basics is best. Sphinx Logon's simple approach is two-fold: add the recommended additional layer (or layers) of security by requiring an authentication factor for logons (card or token), and have admins manage employee passwords to ensure that they're complex.

As we all know, complex passwords are the other security necessity that government entities have been championing for years, and complex passwords continue to provide strong protection for network and app logons. The important challenge here is to solve the quintessential "password problem" - by taking the responsibility out of the hands of employees. With Sphinx Logon, centrally-managed complex passwords are automatically generated and updated to each user's account, so the process is essentially hands-free. Employees don't even know their passwords so they can't give them away, forget them, or lose them. To logon, employees must present their card or token and enter their PIN. Then Sphinx takes over and performs the secure logon. Repeated wrong PINs will lock the card, thwarting this type of attack.

Again, two critical things to point out here. First, Sphinx works with Windows in a non-invasive way and requires no change to the existing Windows network setup - no need for confusing and potentially risky reconfiguring, no need for consultants to analyze anything. Secondly and an important factor that differentiates Sphinx Logon in the marketplace, the customer remains in control of their data. Customers store their logon data on their own onsite secure server.

Another important concern is user experience, and this can't be overlooked when considering a new solution. Instead of increasing the user's complexity and responsibility, if a multi-factor authentication solution can take over that responsibility, users are delighted. This has won the Sphinx Logon software many fans on the front lines.

While we're talking about users, let's call attention to Sphinx' role-based user groups, which make it easy for admins to provide access to different levels of information. Also important in terms of audit readiness, user card logon activity can be traced throughout the day.

So you may ask, what does this mean in today's world, with many employees also working from home - don't we need a cloud for that? Nope. Employees can still logon to the corporate network from home using their card and PIN. And when you logon to a network from home it's actually even more important to use Sphinx, since Sphinx transfers the employee's strongly encrypted Windows password under the hood, protecting it from attackers.

To get back to the all important authentication factor, it's interesting to note that ID cards are still used to control access to most buildings. So most of our customers already have one of the authentication factors when they come to us. And if that ID card has a more advanced technology such as Mifare/Desfire featuring on-card encryption, that's even more secure. Looking to the future, as more places are allowing smartphones to be used as access devices, likewise smartphones can also already be used as a logon authentication factor - you just need to have the corresponding card reader.

So now we've looked at complexity, and if you're willing to trust a vendor with your private data, and user experience. How about the cost question, is this an important factor as well? Certainly cost is important if vendors are requiring you to revamp your systems. Also worth noting is that many vendors charge by module, so even though their initial quote for you to get started sounds reasonable, costs may add up alarmingly as you realize you're not getting the features you need in the starter module. Consulting and installation charges may also add up.

Again we revert to our mantra: why over-improve in confusing ways when you can easily handle the root of the problem, the password. So there's no need to pay for and struggle to install complex solutions. Sphinx Logon has one license fee based on the number of users. With that fee customers get a sophisticated software that was originally purpose-built for an exacting Fortune 500 electronics company, which has been continually enhanced over the years based on customer needs. Customers get a hardened software with all the features they need already build in. And although the software itself is complex, it is simple to use. Referring back to the security-conscious government entities mentioned at the beginning, Sphinx' fastidious customers include government entities from numerous countries around the world.

To wrap up, complexity, data ownership, user experience, and cost appear to be the major factors influencing a buy decision for multi-factor authentication. Customers need to weigh these considerations against the tragic potential a major breach could cause.