The People Factor in Security

Assuming that the physical environment, data and network have been secured, the weakest link in most security plans is the people who are involved in the business processes. In our industry, we spend large amounts of time and money to verify that the reported data is for the correct applicant or consumer. How much effort is taken to ensure that only the right people can access this information? If there is a breakdown in validating the identity of the people who provide, review, deliver, or receive the information, then the rest of the security measures were wasted.

For this reason, all system security begins with authentication, the process of determining whether the person is who they claim to be. The key to authentication is balancing the level of certainty that we need about the person's claimed identity with the level of inconvenience that they are willing to accept. In other words, the more onerous the requirements are to prove their identity, the harder the system will be for them to use it and the less likely they will be to continue using it.

Multi-factor authentication (MFA) is an approach that depends on more than one factor to validate a user's claim of identity. MFA uses a combination of something a user knows, like a password or PIN, with something the user has, like a smart card or ATM card, and/or something the user is, like a fingerprint or biometric characteristic. By authenticating the username (claim to identity) with a strong password (something they know) and a rotating security code from a smart card (something they have), the system can recognize the user with a higher level of certainty than a username and password combination alone would provide. The more factors that are required, the greater the certainty will be while the usability of the system will decrease. The key is finding the sweet spot in each implementation that will ensure the user's identity while remaining easy to use.

The increasing numbers of people who bring their personal smart phones and tablets to work and reach out to colleagues using social networks like LinkedIn and Facebook is driving the consumerization of information technology in the workplace. The challenges that it presents are not going away and will continue to make it increasingly difficult to authenticate the users of systems that hold personal background information. At some point, on some level, each of us is the applicant. The additional steps that we take to ensure that the people who access personal information about us, our family, and our friends are who they claim to be will only server to strengthen our industry and increase the confidence we all have about how our records are being used.