**EMCS2430: Human Factors: People and Software**

Assignment: Reflection on Hypothetical Attacks

Brian Russel Davis, brd@brown.edu

*Pay special attention to Chapter 15 of the book [“Information Security Awareness and Training”].*

*Which of these do you think you already do well? Which ones do you find most difficult to do?  
  
Which of these do you think your organization already does well? Which ones do you think your organization would find most difficult to do? Which recommendations do you disagree with and why?*

My current organization ( I have been working there for 2 weeks ) doesn’t do anything in the way of training for cybersecurity. They rely on single sign-on and MFA for the security of user accounts. Also, there is no phone system so many of the social attacks that involve calling people would not work. No one’s phone number is listed in any directory, even internally. It seems pretty inapplicable to evaluate my current organization based on any of the training because we are a young start-up with no cybersecurity at all.

When I worked at NASA there was a very lengthy training program. The entire program is about 40 hours of training. It took me one week to complete the entire thing and it did include most of the thing the author spoke of. There are no “employee numbers” but everyone is issued a smart card. If you lose that smart card or forget the pin you can’t restore access without going into a NASA security office and presenting ID and being fingerprinted. However, NASA does have a phone system and I imagine there are printed directories, though I have never seen them.

With NASA I am pretty sure many of the social attacks would work but an attacker would get blocked in many ways by the smart card system. There is no way to authenticate as another user without the smartcard and the pin. It is not possible to authenticate FOR another person or to use a “spare” smartcard to authenticate remotely ( like the author demonstrated with the snow storm and the attacker calling in asking to use the spare MFA key ). Once a user loses their smartcard all work for the employee literally stops. The smartcard is used to login to the computer, the network, email, and every single application. When a user at NASA gets a new computer they can’t even unlock the computer without the smartcard. This means that any theft if IP or Data has to be done by a contractor.

In terms of things the organization can do better … I do see one vulnerability, the conference call system. After people leave, the PIN numbers for conference lines do not change. It would be quite possible for me to call up any of the conference calls that I used to participate in an listen with no issues. This is a training issue that could be addressed pretty easily, but I think NASA employees and contractors have no awareness that an attacker could be listening to calls where NASA IP and secret plans are being discussed. This doesn’t mean the attacker has access to the systems that hold the data, but they surely have access to all the conversations talking about NASA systems, plans, and strategy.

For the most part, the author outlines a list of common sense approaches that I agree with 100%.

1. Spending 40% of CyberSecurity on training **very** smart. Having the best tools but not knowing how to properly use them is like having a Rolls Royce Wraith and no Driver License.
2. Reminders of the risk ( with stickers on phones, messages on the computer, email tips, etc ) are perfect. Little fun reminders are exactly what people need to unlearn the naive trust they tend to have when dealing with attackers.
3. Having one person who is trained to handle the distribution of sensitive data is also very smart. When it is one person’s job to guard the crown jewels this person is more likely to take that responsibility more seriously and deal with situations “by the book” rather than succumbing to the persuasion of a slick talking social engineer.

The book is a little \*outdated\* with all the case studies about faxing and phone directories, but I am sure for each of those systems I think may be outdated, attackers have found another vector. For the most part, many of the fax and phone attacks are replaced with email spear phishing and social media attacks. I am continually surprised by the number of people that fall for these emails, but I must admit they are pretty good sometimes. I found myself reading through some pretty carefully before deleting them. So, maybe a revision of the book needs to replace all the phone and fax attacks with email phishing case studies.