On Educating People to Pay Attention as a Key Defense Against Data Security Incidents and Breaches

W. David Salisbury

University of Dayton

Subject Area: Information Systems
Article Type: Viewpoint

To spend much time reading the popular press these days, one may understandably decide that we are all doomed when it comes to protecting organizational information resources. Scarcely a day passes without headlines that describe millions of records that have been exposed to hackers, with resultant threats to individuals' privacy, finances or medical records[1]. With the advent of the so-called Internet of Things[2], still greater opportunity exists for data to be exposed and eventually breached.

True, these things collectively pose a challenge, but there are some fairly simple things (at least in concept) that can be done to mitigate at least some of the concern. As part of the preparation for a class I teach, I read more than a few reports on data breaches and the resulting bad things that happen. More and more, however, researchers are identifying that the problems aren't necessarily technical, but managerial and educational. Regardless of the sophistication of the boxes or software theft we install in our organizations that are designed to protect against malware and data theft, the major problem seems to be people.

Evidence of this problem is found in this year's Data Breach Investigations Report (the 2016 version is most current, which focuses on data from 2015), published by Verizon3. What Verizon does in this report is gather security incident and data breach information from a variety of sources, format it so they can talk about apples and apples (rather than oranges and apples), then identify some patterns. Other organizations have similar reports that are very good, but Verizon's, in addition to being free, is written in a fairly light and breezy style, and if I'm going to read roughly 80 pages of reporting about a depressing topic (e.g., how much data gets stolen in a given year) I prefer a few Yogi Berra quotes along the way.

One major finding in this report pertains to the impact and success of so-called "phishing" attacks. For some of the readers here that might not be familiar, a definition and an explanation might be in order. Dictionary.com defines "phishing" as an attempt "…to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one."

To decompose this a bit, somebody (let's call them a hacker or a cybercriminal) sends an email to a target that attempts to either get the target to provide information that can lead to a data breach, or perhaps encourages the target to click on some link. This can result in malware, for example a keystroke logger, being installed, or perhaps it's a link to a website that looks legitimate that asks for information that can be used for identity theft. What happens at this point could be any of a variety of bad outcomes, for example an individual's corporate network credentials and/or personal information being stolen, which lets the hacker/cybercriminal make some money, and usually results in the target losing something of value (beyond their personal

information) and/or their employer having its network security compromised. Clearly these are things to avoid if possible.

To address this problem, the organization can put in a wide range of security controls, for example malware blockers, anti-virus packages, email filters, complex passwords, perimeter firewalls, and so forth. These are effective tools and definitely should be part of a layered defensive strategy. However, the target in the present example isn't any of those; it's the user. Humans tend to get distracted and do a lot of things without paying much attention, and this what this sort of attack depends on for success.

To get a feel for the problem, the reader is invited to play an online game devised by OpenDNS[4]. In this game, various websites that either are or are not legitimate are provided, and it's up to the player to decide which sites are legitimate and which are phishing sites. Play the game and be honest with yourself. How did you do? Even if you do well, before you feel too proud, keep in mind, you've been primed by reading this to look for "phishy" emails and websites, and you were focused on the task at hand. While doing their day-to-day jobs, your users (and indeed you outside this little exercise) are likely not this focused on spotting "phish".

The challenge, then, is to work on our "weakest link" in the security chain – the user – and help her/him to pay attention and be more thoughtful, so as not to get "phished". Users aren't necessarily bad or careless, but they generally have a lot going on and sometimes react to the malicious email (in something less than two minutes according to Verizon's data) rather than thinking matters all the way through. Further, organizations can make policies (e.g., password complexity) engage in various technical controls (firewalls), or procedural controls (e.g., "…our organization will never ask you for sensitive information via email…") but these alone don't prepare the user for ongoing and novel situations where s/he is called upon to assess an email link or website for possible malicious content.

The focus to now has been on training and rule following; there is, however, a growing realization that what we need education; to focus on developing users' reasoning and judgement as pertains to cybersecurity. As described by IT researcher Matthew. Jensen and his colleagues[5], Traditional training in security practices doesn't necessarily help, because it tends to focus on concrete scenarios for which specific programmed responses are useful. To be useful this training requires recognition of the situation (i.e. situational awareness) to be called upon, which requires the ability to think abstractly and engage in some reflection about the particular circumstances in which one finds oneself. To prepare individuals for this sort of thing requires education, which by its nature involves reasoning and judgement rather than reaction to a given stimuli.

One result of this sort of thinking is to identify organizations that routinely operate in environments where carelessness or ignorance can lead to very bad outcomes, then adopt their processes. An example of this, cited by Weick and his colleagues[6], is the U.S. Navy Nuclear program. One might imagine that mixing submarines, aircraft carriers and nuclear reactors and young men and women under a lot of pressure may create opportunity for bad things to occur. Despite this, the Navy has enjoyed an exemplary record, having tallied the equivalent of nearly 5,400 *reactor years* of operation without adverse impact on the thousands of personnel that have worked in close proximity with nuclear reactors[7].

How do they do this? The Navy Nuclear program is an example of Weick and his colleagues term a "High Reliability Organization". These are organizations that feature a high sensitivity to the situation, and emphasize alertness to deviations from normal expectations. Such

organizations, realizing that the nature of their work is inherently complex and non-routine, focus on dealing rapidly with the non-routine. Likewise, Maitland Bryson, and Van de Ven[8] have done research that suggests command and control hierarchies (much like training for tasks) don't do well for complex situations. They suggest that an organizational form of the "clan", characterized by shared values and norms is best to deal with greater complexity.

These sorts of things have utility as it comes to educate a user that the organization hopes to help understand when somebody is attempting to social engineer (i.e. "phish") them and react accordingly. They first must be educated in identifying when something is non-routine. In some cases, this is fairly easy. For example, if one receives an email from an African prince that offers to deposit a few million dollars in their bank account if they only click the link and enter their bank information so the prince can withdraw the $200 transfer fee then deposit the millions, most people are sufficiently dubious of this. However, when it comes to "your email account has been disabled pending a password change; please click this link to fix it" in an email with your organization's email, logo and standard typeface, it becomes more problematic. This requires first establishing with the user what is routine (helping them to be intimate with password reset procedures) and thereby identifying what is not routine, and therefore deserving of a greater degree of skepticism. It also requires helping users to see that they are part of a "clan" that shares responsibility for data security, and that their individual actions have impact beyond themselves.

I am aware of at least two examples of training and education initiatives extant that have begun to move the focus away from a more training-focused model and toward an education and awareness-based model. The first is actually offered by the U.S. Department of Homeland Security[9]. Called the "STOP.THINK.CONNECT." program, it is a public awareness campaign aimed at improving the understanding of cyber threats and providing tools, approaches and strategies for individuals to use to enhance their safety online. A key feature of the program is the emphasis on understanding the situation when online and thereby make more informed decisions about using the Internet.

The second is one that was developed by our IT group here at the University of Dayton[10]. Here at UD, our institution is engaged in a year-long "Year of Safe Computing" education initiative, which has monthly training topics and focuses on the notion of "cyber-mindfulness", drawing upon Weick and his colleagues' notion of "high reliability organizations". The point is not to train people with specific responses to specific stimuli, but to encourage them to be more aware of the issues, to be more engaged in the protection of data (both the University's and their own), and thereby be less susceptible to social engineering attacks such as phishing.

At the end, your security is only as good as your weakest link. Educate your people to be skeptical of the non-routine and to pay attention, and you will have done a lot to shore up your security.

---

[1] Information is Beautiful (2016). World's biggest data breaches. Online: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (September 16, 2016).

[2] Morgan, J. (2014). A simple explanation of the "Internet of Things". Forbes, May 13. Online: http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#1293845d6828 (September 16, 2016).

[3] Verizon (2016). Data Breach Investigations Report. Online: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/ (September 16, 2016).

[4] OpenDNS (2016). Phishing quiz: Think you can outsmart Internet scammers? Online: https://www.opendns.com/phishing-quiz/ (September 16, 2016).

[5] Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J.B. (2013) Training to Mitigate Threats from Customized Phishing Attacks, in Briggs, Robert O. and Nunamaker, Jay F., Jr. (Eds.) *Report of the Hawaii International Conference on System Sciences, Symposium on Credibility Assessment and Information Quality in Government and Business*, Maui, HI, Jan 6-10.

[6] Weick, K. E., Sutcliffe, K. M., and Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. In Sutton, R. S. and Staw, B.M. (eds), Research in Organizational Behavior, Volume 21. Stamford, CT: Jal Press: 81-123.

[7] Conca, J. (2014). America's Navy: The unsung heroes of nuclear energy. Forbes.com, October 28. Online: http://www.forbes.com/sites/jamesconca/2014/10/28/americas-navy-the-unsung-heroes-of-nuclear-energy/#4adf325f651f. (September 19, 2016).

[8] Maitland, I., Bryson, J., and Van de Ven, A. H. (1985). Sociologists, Economists, and Opportunism. Academy of Management Review, 10(1): 59-65.

[9] United States Department of Homeland Security (2016). Stop. Think. Connect. Online: https://www.dhs.gov/stopthinkconnect (September 16, 2016).

[10] University of Dayton Information Technology (2016). 2016: A year of safe computing. Online: https://www.udayton.edu/udit/safe-computing/yosc/index.php (September 16, 2016).