Michael Stango

Michael Stango is the Information Technology Supervisor for A.I.M. Mutual Insurance Companies. He has a background in database programming, information systems analysis, and project management, and leads A.I.M. Mutual's Cyber Awareness Training program. He is also the current chair of the company's Massachusetts Data Security Committee.

DATA SECURITY:

Protecting the Home Front

AS information about cyber security becomes more and more available, the business community of the twenty-first century may be misplacing resources in the fight against cyber crime. It seems industry experts, research firms, and the media alike emphasize protection against "malicious attacks," but network security infrastructure and software can be extremely expensive. Perhaps there is a more cost effective way for businesses, especially small ones, to shield themselves from a data security breach.

It's abundantly clear why the experts give extra attention to malicious attacks that may involve hackers, viruses, or internal cyber criminals. According to Ponemon Institute's *2016 Cost of Data Breach Study,* 50 percent of reported breaches by US organizations in the study were the result of malicious or criminal attacks. The cost of these types of attacks was approximately $236 per record breached. However, system glitches accounted for another 27 percent and human error accounted for another 23 percent, costing the surveyed companies $213 and $197, respectively, per record breached. [1]

Though malicious attacks were the most costly for the surveyed companies, they are also expensive to defend against. Network security infrastructure can cost companies thousands, and once purchased, an expert must undertake the grueling task of configuring the gear. Network security software can also be costly, but may provide an easier solution for smaller businesses, as most of this software is easy to install and configure. Overall, the best protection against malicious attacks is a combination of security infrastructure and software. Of course, that is, if your business can afford it.

Mitigating the risk of malicious attacks can be expensive, but protecting your company from system glitches and negligent employees may be more cost effective if budgets are tight. In fact, most operating systems will proactively attempt to fix system glitches; they simply require your blessing as an end user. Take Adobe Reader, for example. The average user has likely been asked by this software to allow "required updates." Admittedly, between Adobe, Java, and Microsoft, the update requests can be fairly annoying. Still, these updates tend to contain key security patches that will keep your network and data safe from loopholes that have been exploited by hackers and cyber criminals. It is strongly recommended that all software is kept up-to-date to help reduce the risk of system glitches.

As for negligent employees, a

Figure 1
Root Cause of Data Breaches

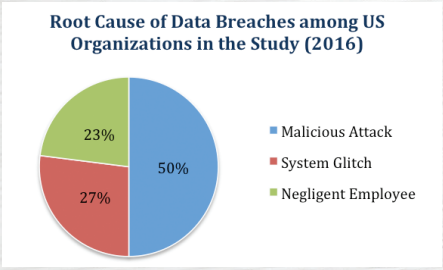
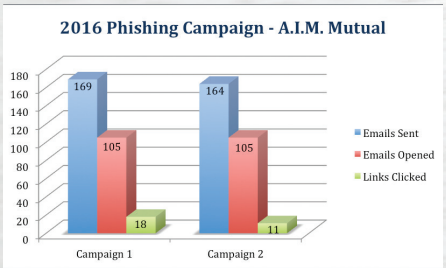


Figure 2
2016 Phishing Campaign



great course of action is to address carelessness and lack of knowledge with what A.I.M. Mutual Insurance Companies likes to call "Cyber Awareness Training." This training should not only inform employees on how a data security breach could impact the company but also explain how employees could be impacted on a personal level. At A.I.M. Mutual, we like to focus on topics such as password best practices, identifying phishing emails, and recognizing suspicious behavior at the workplace. We use a more focused approach when training employees who work off-property, as there tends to be more exposure associated with carrying around a company cell phone or laptop.

One primary area of focus for A.I.M. Mutual's 2016 Cyber Awareness Training was identifying and reporting phishing emails sent to company email addresses. According to Verizon's *2015 Data Breach Investigations Report*, up to 70 percent of cyber attacks in 2015 targeted a secondary victim after compromising a primary victim.[2] Employees should be considered a primary conduit between the company network and the increasingly dangerous World Wide Web, and it's important to train them accordingly. We discovered that a combination of training and real-life testing was the most effective way to teach employees how to identify scam emails.

In order to test an employee's likelihood of clicking on malicious email links and attachments, we initiated a quarterly "phishing campaign" with the help of an industry-known security organization. We sent quarterly emails to all employees containing phony links and attachments. The phishing software logged all emails sent, emails opened, and links clicked. In Figure 2, compare the results of our first and second phishing campaigns, which helped us gauge how "phish prone" our employees were at the time.

Though the percentage of emails opened increased slightly from 62.1 percent to 64 percent, the percentage of links clicked dropped considerably from 10.7 percent to 6.7 percent. Fortunately, the initial campaign provided the information needed to focus the Cyber Awareness Training on certain areas of the company, likely resulting in improved results after the second campaign. Considering the 12 percent click rate reported by Verizon's *2016 Data Breach Investigations Report*, [3] the phishing campaigns were deemed to be so effective that we intend to continue them for the foreseeable future.

Overall, A.I.M. Mutual has taken a holistic approach to cyber security. Between robust network infrastructure, security software, patch schedules, and end-user training, we believe we have considered all the angles necessary to protect ourselves from a data security breach. What's most important is to identify the exposure that your business may have and build a budget based on the potential cost associated with a breach of all sensitive records. Regardless of industry, this is an area that every business owner should be willing to cut a check for. I can assure you of this: It will be less expensive to take the appropriate preemptive measures than to recover from a large-scale data security breach.

1. Ponemon Institute, LLC, 2016 Cost of Data Breach Student: Global Analysis, sponsored by IBM, retrieved from https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094wwen/SEL03094WWEN.pdf
2. Verizon, 2015 Data Breach Investigations Report, retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf
3. Verizon, 2016 Data Breach Investigations Report, retrieved from http://www.verizonenterprise.com/Verizon-insights-lab/dbir/2016/