Addressing Malware WITH Cybersecurity Awareness

By Carlos Valiente, Jr. – ISSA member, Tampa Bay Chapter

People are your biggest asset and weakest link. Investing in cybersecurity awareness training is the most cost-effective and efficient method to deter malware in organizations today.

Your company has invested in the most sophisticated firewalls, intrusion detection systems, and physical security alarms and guards. Technologies are built, operated, and maintained by one of your company's biggest assets—people—yet people are the most prone to mistakes and accidents. You do everything you can to protect your assets, but without security awareness and training those efforts are wasted.

Of all methods and techniques that can be applied to prevent malware in organizations today, building a culture of cyber compliance and awareness is one of the most cost-effective ways of deterring malware. Changing your biggest assets' behaviors remains a people problem, where hovering over a link can start a malware infection. Converting the human weakest link into a human firewall will yield the most positive return on investment.

This article will look at the cost of human data breaches in a study sponsored by IBM and independently conducted by the Ponemon Institute LLC[1] in June 2016 titled, "2016 Cost of Data Breach Study: Global Analysis."[2] We will then focus on known industry best practices for developing a strong security awareness program from the ground up utilizing US National Institute of Standards and Technology (NIST) special publications.

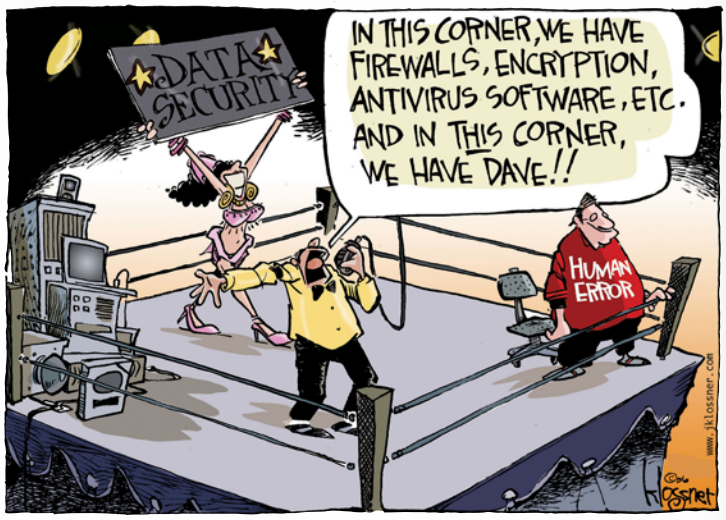

Figure 1 – Computerworld cartoon by John Klossner [Copyright 2006 John Klossner, www.jklossner.com]

The biggest assets is your weakest link

Remember the phrase "To Err is Human"?[3] It is not entirely accurate to assume that all malware and data breaches are caused by outsider threats. There are plenty of insider threats along with conditioned bad habits that help make malware the overwhelming success it is in today's organizations.

1 Ponemon Institute – https://www.ponemon.org/.

2 Larry Ponemon, "2016 Ponemon Institute Cost of a Data Breach Study," Security Intelligence (June 15, 2016) – https://securityintelligence.com/media/2016-cost-data-breach-study/

3 Part of a longer phrase ""to err is human; to forgive, divine" in English from Alexander Pope poem, "An Essay on Criticism" – http://wwweighteenthcenturypoetry.org/works/o3675-w0010.shtml.

Nobody puts it better than cartoonist John Klossner,[4] where no matter how much money we spend on firewalls, encryption, and antivirus in the fight for data security, we will always have the human—Dave. His cartoon shows a boxing ring with assorted security hardware and software technology in the one corner. In the other is Dave wearing a shirt labeled "Human Error." This is clearly an illustration that Dave, representing us users, can sometimes cause a lot of havoc when not properly trained, and organizations spend millions in technology only to be defeated by their humans.

The human cost of data breaches

The Ponemon Institute study looked at 383 companies operating in 12 countries with an average $4 million total data breach cost. A 29 percent increase in cost has been realized since 2013, and $158 dollars was the average cost per compromised record.[5] Over the years the Ponemon Institute has been studying the data breach experience of 2,013 organizations in every industry, the research has revealed seven megatrends. Of those trends, which can be referenced in the section of the study titled, "Seven Global Megatrends in the Cost of Data Breach Research."[6] This article will focus on number six: "Employee training and awareness programs…continue to result in cost savings."

4 John Klossner. John Klossner's cartoons and illustrations have appeared in a wide variety of print and electronic publications, including The New Yorker, Barron's, Computerworld, Federal Computer Week, and The Wall Street Journal. Mr. Kloosner is an Adjunct Professor New Hampshire Institute of Art – http://www.jklossner.com/; http://www.jklossner.com/computerworld/security.html.

5 The terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report. Per capita cost is defined as the total cost of the data breach divided by the size of the data breach (i.e., the number of lost or stolen records).

6 2016 Cost of Data Breach Study: Global Analysis

Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC June 2016. https://www.ibm.com/security/data-breach/. To download a copy: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN.

Below is a summary of the seven cost of data breach megatrends:

1. The cost of a data breach has not fluctuated significantly.
2. The biggest financial consequence to organizations that experienced a data breach is lost business.
3. Most data breaches continue to be caused by criminal and malicious attacks.
4. Organizations recognize that the longer it takes to detect and contain a data breach, the costlier it becomes to resolve.
5. Regulated industries, such as health care and financial services, have the costliest data breaches because of fines and the higher than average rate of lost business and customers.
6. Improvements in data governance programs will reduce the cost of data breach. Incident response plans, appointment of a CISO, **employee training and awareness programs** and a business continuity management strategy **continue to result in cost savings**.
7. Investments in certain data loss prevention controls and activities such as encryption and endpoint security solutions are important for preventing data breaches. [7]

Root cause of data breach

While nearly half of data breaches were caused by malicious or criminal attacks, system glitches that include both IT and business process failures, and human error comprised the remaining half, with human error at 25 percent:

7 Page 2 and 3 of the Ponemon study listed the megatrends and other factors noted about human error and training.

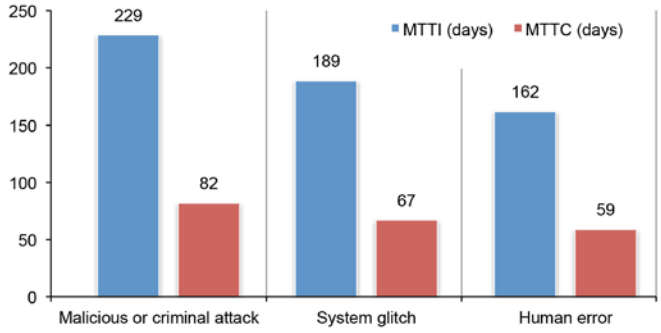

Figure 2 – Mean time to identify and contain data breach incidents

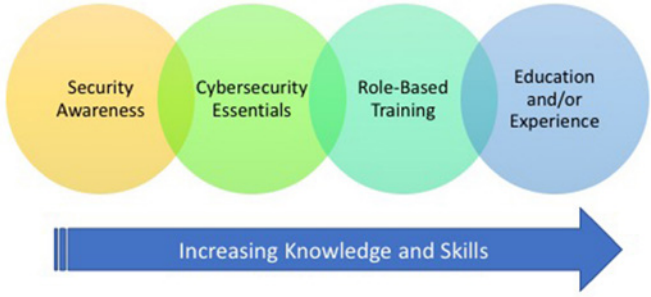

Figure 3 – The learning continuum

- Malicious or criminal attack: 48 percent and $170 per breach
- System glitch: 27 percent and $138 per breach
- Human error: 25 percent and $133 per breach

Of the factors that determine data breach costs, an incident response team, extensive use of encryption, employee training,[8] participation in threat sharing, and business continuity management contributed to decreasing the cost of data breaches. Employee training and business continuity management involve the "human factor" and continue to play an important part in reducing cost.

The human factor consists of negligent insiders who caused a data breach because of their carelessness and criminal insiders, which include employees, contractors, and other third parties. The most common types of malicious or criminal attacks by malware infections include criminal insiders, phishing, and social engineering—the human factor.

Of the 12 countries sampled by root cause—malicious or criminal attacks, system glitches, and human error—human error played a significant role, ranging between 16 percent and 37 percent, with the US at 23 percent. The per capita costs for human error ranged between $54 to $197, with the US topping the chart at $197.

The study looked at *mean time to identify* (MTTI) and *mean time to contain* (MTTC) metrics. Both are used to determine the effectiveness of an organization's incident response time skills. MTTI is the time it takes to detect an incident, and MTTC is the time it takes to resolve a situation and ultimately put things back in service or order. While lower for human error, organizations are taking on the average 162 days to detect the incident and 59 days to correct it (figure 2).

While each metric places malicious/criminal attacks in the highest category of impact, human error consistently presents a significant cost to an organization, one that can be affected by security awareness and education.

Identifying a security awareness program

Why reinvent the wheel? A few trusted source documents for building a human firewall security awareness program are available for free, thanks to US tax payers:

- NIST Publication 800-50 "Building an Information Technology Security Awareness and Training Program"[9]
- NIST Publication 800-16 "A Role-Based Model for Federal Information Technology/Cyber Security Training"[10]

Both documents work together: 800-50 is a high-level discussion on how to build an awareness program, while 800-16 is more tactical, focusing on role-based training.

Before proceeding, first ask yourself these questions:

1. Does your organization take security seriously?
2. Does your staff know how to fend off social engineering attacks via phone and email?
3. Are your organization's portable devices such as smartphone, laptops, and tablets encrypted?
4. Does your organization require staff to certify as part of the onboarding hiring process? Do they complete an annual awareness training course?
5. Do you know what a rainbow table is?[11]
6. When you walk around your organization, do you see awareness posters displayed and rotated quarterly?
7. Are you responsible for information security in your organization?

As "Rome wasn't built in a day," an adage attesting to the need for time to create great things, it'll take time and commitment to develop a solid program. Everyone in your organization is responsible for information security—protecting your assets—and everyone can become an effective human firewall.

Building a security awareness and training program

Both NIST publications 800-50 and 800-16 discuss what is known as a learning continuum (figure 3) or continuous improvement life cycle, a process that starts with awareness, followed by training and education. Learning is a role-based

8 Page 11 of the study

9 NIST, "Building an Information Technology Security Awareness and Training Program – http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf.

10 NIST, "A Role-Based Model for Federal Information Technology / Cyber Security Training (03/14/2014) – http://csrc.nist.gov/publications/drafts/800-16-rev1/draft_sp800_16_rev1_2nd-draft.pdf.

11 A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes – https://en.wikipedia.org/wiki/Rainbow_table; https://lasec.epfl.ch/~oechslin/projects/ophcrack/.

continuum; it starts with awareness, builds to training, and evolves into education.

This continuum demonstrates that roles and responsibilities within an organization are determined by type and level of awareness, training, and education required, possibly based on job function. For example, security awareness is provided to all users in the organization, while a more focused cybersecurity essentials training is provided to members of the IT department. The appropriate level of cybersecurity awareness, training, and education is determined by the role within an organization.

As an example, the model illustrates the following organizational concepts:

1. **Security awareness** – required for all employees of the organization
2. **Cybersecurity essentials** – this includes employees and contractors involved with IT systems
3. **Role-based security training** – focused within the organization and based on function
4. **Education** – includes on-the-job training, certifications, and advanced education

NIST 800-50 identifies four key steps in the life cycle of an IT security awareness and training program: **Designing, development, implementation, and post-implementation** (see figure 4).

Figure 4 – Security awareness and training program life cycle

Step 1: Designing

Assessment is conducted and a training strategy is developed and approved.

Depending on the size of your organization and available resources, consider one of the three models for managing the

training program: 1) centralized, 2) partially decentralized, and 3) fully decentralized, with courses focusing on beginner, intermediate, and advanced users. The type of model considered should be based on an understanding and assessment of budget and other resource allocations, organization size, consistency of mission, and geographic dispersion of the organization.

Consider the *how to* as you follow sections 3.1 through 3.6 of 800-50:

- Structure the awareness and training activity (section 3.1)
- Conduct a needs assessment and why (section 3.2)
- Develop an awareness and training plan (section 3.3)
- Establish priorities (section 3.4)
- Determine the level of complexity of the subject (section 3.5)
- Fund the program (section 3.6)

Step 2: Development

Focus on available training sources, scope, content, and development of training material.

When the design is completed, it's time for the supporting material to be developed. When developing the materials, keep in mind the "behavior" you want to reinforce and the "skills" that you would like your audience to learn. You might ask yourself, what is the difference between training and awareness? Awareness focuses on security practices—the message is short and simple. Training is focused on a specific audience and includes everything related to security that attendees need to know in order to do their jobs. Training materials are usually far more in-depth than materials used in an awareness session or campaign.

Consider the *how to* as you follow sections 4.1 and 4.2 of Pub 800-50:

- Develop awareness materials (section 4.1);
- Provide examples of awareness topics (section 4.1.1)
- Develop training materials (section 4.2).
- Provide examples of sources of awareness materials (section 4.1.2)

Step 3: Implementation

Effective communication and roll out of the awareness and training program.

Implementation should occur only after a needs assessment has been conducted, strategy devised, and a plan for implementing the strategy and all training materials is developed. It is important that the program's implementation phase is clearly communicated to the organization to obtain support and commitment for necessary resources. The techniques for delivering awareness and training materials include many different formats; examples of these techniques are included in section 5.2 and 5.3 (e.g., newsletters, posters, streaming videos, web-base training, etc.)

Consider the *how to* as you follow sections 5.1, 5.2 and 5.2 of Pub 800-50:

- Communicating the plan (section 5.1)
- Techniques for delivering awareness material (section 5.2)
- Techniques for delivering training material (section 5.3)

Step 4: Post-implementation

Lessons learned, guidance on keeping the program current, and monitoring its effectiveness.

An organization's cybersecurity awareness and training programs can become stale and obsolete if sufficient attention is not paid to technology advancements, IT infrastructure and organizational changes, and shifts in organizational mission and priorities. Continuous improvement (or lessons learned) should be the most important part of the cycle. As Pub 800-50 puts it, "you can never do enough."[12]

Consider the *how to* as you follow sections 6.1, 6.2, 6.3, 6.4 and 6.5 of PUB 800-50:

12 This concept is borrowed from William E. Deming and Walter Shewart's continuous improvement process "Plan, Do, Check, Act" – https://en.wikipedia.org/wiki/W._Edwards_Deming; https://en.wikipedia.org/wiki/Walter_A._Shewhart; https://en.wikipedia.org/wiki/PDCA.

- Monitoring compliance (section 6.1)
- Evaluating and feedback (section 6.2)
- Managing change (section 6.3)
- Ongoing improvement (section 6.4)
- Program success indicators (section 6.5)

Other examples in Pub 800-50 (e.g., Appendices A through D) include the following:[13]

- **Needs assessment interview and questionnaire**: A needs assessment is a process for determining and addressing needs or "gaps" between current awareness or training needs vs. desired conditions. The discrepancy between the current condition and desired condition must be measured to appropriately identify the need and target the appropriate training.
- **Sample awareness and training metric questionnaire:** Training metrics give you the ability to track and measure the impact of your security awareness program. This can be used to improve your training, demonstrate return on investment, or compare the human risk.
- **Sample awareness and training program plan template:** This provides an example of a plan that includes goals, objectives, roles/responsibilities, the education planned, and the target audience/resources requirements (including costs, etc.) etc.
- **Sample awareness poster materials:** Traditional posters, emails, images, articles, and other types of communication materials are designed to reinforce your awareness/training education initiatives. These types of ongoing communications are probably the most fundamental tools needed to keep your staff, contractors, and vendors aware of current threats and vulnerabilities related to cyber and physical security.

Summary

Nobody puts it better than cryptographer and security professional Bruce Schneier who once said, "Only amateurs attack machines; professionals target people."[14] People are the most important asset an organization has, while at the same time they are also the weakest link. Organizations give more importance and spend the most amount of money on technology instead of people who are the most critical factors in ensuring information systems security.

One way of achieving the protection of information systems is by continuous awareness and training. This article applies the concepts in NIST Pubs 800-50 and 800-16, discussing a

13 Appendices A, B, C, and D of NIST Publication 800-50 provide these examples – http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf.

14 Bruce Schnier, "Phishing Has Gotten Very Good," Schneier on Security (March 1, 2013) – https://www.schneier.com/blog/archives/2013/03/phishing_has_go.html.

four-step process or continuum for how to design, develop, implement, and follow up an awareness and training program.

Of the three major costs of data breaches determined today, your biggest bang, most cost-effective and efficient method for your money to deter malware in organizations is educating your employees who are both your most valued asset and weakest link. A strong security awareness and training program will help build your organization's human firewall.

About the Author

Carlos Valiente Jr., CISSP, CISA, CISM, CGEIT, 27001-LA, is a results-driven cybersecurity specialist and compliance audit professional with 25+ years experience leading and managing global IT, information security, compliance, and risk management programs in Big 4, Fortune 500 and 1000 companies. For more information, comments, or questions, email vtechno@gmail.com.

This announcement does not necessarily reflect the opinions of the ISSA Journal or the ISSA.

— Equifax Breach Public Service Announcement —

Data Breach Alert: 143 million Equifax Records Hacked!

Equifax, one of four credit reporting firms in the US, is the latest company to reveal a major data breach! Discovered on July 29 and disclosed to the public on September 8, Equifax revealed the stolen data contained Social Security numbers, birth dates, home addresses, and in some cases driver's license numbers. Using this data, hackers can open lines of credit or file fraudulent tax returns!

Is the Equifax breach a big deal?

Equifax said 143 million American's financial records, 209,000 credit cards records, and 182,000 individual's personally identifiable information were stolen when hackers breached their website. Based upon previous breaches of this kind, it is expected that these numbers will go up over time. Anthem, for instance, initially said 43 million records were breached but later confirmed almost 79 million records!

Like the Anthem breach this is a big deal because unlike a credit card, which is easily replaced when lost or stolen and charges can be contested with relative ease, your Social Security number, once stolen and in hacker databases, can be used and reused for malicious purposes until the US government finds a replacement scheme for this outdated, misused, and largely insecure number.

Okay, now what should you do?

Freeze your credit at all four credit reporting agencies

Yes, there are four credit reporting agencies. Hackers know this, but very few consumers are aware of the little known fourth player in this market: Innovis. Cybersecurity experts advise consumers to put a credit freeze on your account at each credit reporting agency. Here are the links:

- Transunion Credit Freeze: https://www.transunion.com/credit-freeze/place-credit-freeze2
- Equifax Trusted ID Premier: https://www.equifaxsecurity2017.com/trustedid-premier
- Experion Freeze Center: https://www.experian.com/freeze/center.html
- Innovis Credit Freeze: https://www.innovis.com/personal/securityFreeze

Experion charged a $10 fee to do this. Do it anyways.

Additionally, some of the credit monitoring agencies such as Transunion offer additional notification services such as texting you whenever your credit is pinged. Enable text alerts if possible to keep track of anyone actively touching your credit data.

A credit freezes is in place; am I all set?

In a word: No

Following the Anthem breach hackers allegedly submitted hundreds of thousands of fraudulent tax returns before legitimate tax payers could do so. Consumers lost time and money regaining access to their own tax accounts. Unfortunately, this could happen all over again with this Equifax breach because hackers likely have the data they need to submit fraudulent tax returns from this breach.

Furthermore, the IRS, while acknowledging this identity theft problem, has failed to come up with any safeguards like a credit freeze on your tax account. They do have "Identity Protection: Prevention, Detection and Victim Assistance" [1].

Get your tax documents in order and submit your taxes as early as possible to preempt any belated hacker attempt to submit a false return in your name!

Summary

Anytime static data that cannot be recreated is breached, there are long-term consequences, which is the case with the Equifax breach of Social Security numbers, birth dates, home addresses, and driver's license numbers. Putting a credit freeze on your account will protect you largely from hackers taking credit out in your name, but doesn't prevent them from submitting fraudulent tax returns in your name. Get your tax documents in order and submit as early as possible.

[1] IRS – https://www.irs.gov/identity-theft-fraud-scams/identity-protection.

About the Author

Craig Taylor is the Chief Security Officer for Neoscope Technology Solutions. He can be reached at CTaylor@neoscopeit.com.