WISEGATE ANSWERS

REAL PRACTICES

# Security Awareness Programs:
## CISOs Share Practical, Simple Strategies

2014 Edition

# Introduction

To maintain an effective security awareness program, it's helpful to learn what other CISOs are doing and have done, and to replicate their successes and avoid their pitfalls. Wisegate recently completed in-depth research with expert CISO's, spanning multiple industries. In this report you will hear them talk about the challenges of promoting security awareness and share strategies that improve user adoption of data protection controls.

In the Wisegate report titled, "Preparing for the Top IT Security Threats of 2013," Wisegate CISO Members shared their viewpoints on the top anticipated threats—and how to prepare for them. The general consensus among Members was that specific threats—like the latest virus in the wild or DDoS attacks from hacktivist groups like Anonymous—are not the most urgent security concerns to address. Rather it's broader areas such as mobile computing, BYOD (bring your own device), cloud computing, and data protection that need their heightened attention.

Across all of these most worrying threats, Wisegate Members recognized *the user* as the most commonly exploited security vulnerability. It is little wonder, then, that improving user security awareness ranks high on the list of CISOs' current priorities.

Research from Wisegate focused on the following areas:

- **Data classification: keep it simple.** At issue is whether staff either understand or abide by different data labels and how to develop labels that can be understood and followed.
- **Education of staff: keep it going, use the experts.** Awareness training and aware staff do not necessarily go hand in hand. Effective security awareness only follows from a continuous & imaginative approach. You'd do well to engage your company's marketing & communication experts to help drive effective campaigns.
- **Education: It's for work *and* home.** Security awareness isn't just for the office anymore. As more people work at home—or bring their work home—it becomes important to think in terms of educating employees to be aware of security both in their work and home settings.
- **Third-party training & vendors that shine.** In the area of third-party training, several vendors emerged with high marks.
- **How to know if your security awareness is working.** You many not always like the answers; however, there are surefire ways to assess how it's going.
- **You are not alone.** Keep the faith. Many (if not most) organizations are still relatively new at this.

## Membership
### HAS ITS ADVANTAGES

Wisegate is a new kind of advisory service built on the collective expertise of IT leaders. We provide unbiased feedback, experienced insight, and actionable information to our members through an anytime, always-on website, concierge service and mobile app.

Wisegate upholds a high bar for its members because it is through these members that we gather our curated information in the forms of polls, Q&A, product reviews, document sharing, roundtables and working groups. 100% of Wisegate members are senior level, and 89% of them have more than 16+ years experience in IT. There are no vendors, analysts, or inexperienced IT professionals in the Wisegate network.

## Data Classification: Keep it Simple

A common problem felt by CISOs is that users often fail to understand the company's data taxonomy. They lack understanding of what data is sensitive and what data is not, and don't necessarily know how to treat the different categories. As a result, sensitive data can be passed around and treated in an insecure manner.

### No accepted standards, so keep it simple

Confusion may arise because no cross-industry standard taxonomy exists: different companies have different classifications. Instead of assuming that staff—already busy doing their non-security jobs—will learn a complex taxonomy, focus on how to make it easier for staff to figure out what they need to do. Assume people on your staff are smart (they are) and work to make it easier for them to know what's needed.

> Our company effectively has only two labels: *'highly sensitive'* and *'not highly sensitive.'* The highly sensitive data is a *'no-brainer'*—people get that. This gives a good starting point that all staff can understand."
>
> — *"Steve," CISO, Insurance Industry*

### Other departments need to be involved in data taxonomies

The involvement of other departments in data classification is a fact of life, and an additional complication. The legal department is *'on the hook'* because of the pressure of

compliance. Compliance, the requirement to fulfill legal (such as HIPAA) or organizational (such as PCI DSS) regulatory obligations often defines the highest data security classification. But compliance is not usually owned by security—there is often a separate compliance officer under a separate legal or risk management department.

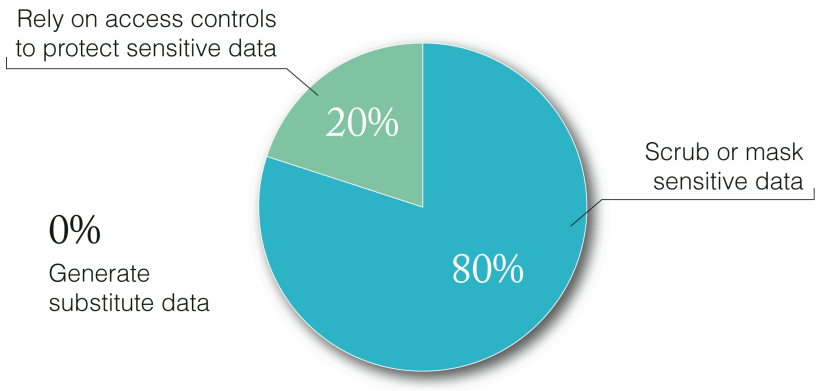
Mark, a CISO with a company in the financial sector, said, *"I am spending most of my time on the non-credit card data since I don't own compliance."* He wants to raise the bar on everything else, but believes that too many labels just confuse the user.

> We are just focusing on 'protected' or 'unprotected.' We feel that having three or four levels of different control sets based on the confidentiality or criticality is going to be too much for people to manage. So we're really just going to do red light (protected) or green light (unprotected)."
>
> —*"Mark," CISO, Financial Industry*

## Data classification in engineering organizations

One group that commonly has special access to sensitive data is engineering. This is particularly relevant with the growing use of cloud computing to handle peak development periods, and outsourcing development to third-party developers and consultants. The problem is that development often breaks the least privilege principle—developers might need access to data for system testing that they would not normally have rights to access.

Figure 1. Wisegate Member Poll: *"How do you handle sensitive data in development environments?"*




Source: Wisegate

Wisegate recently polled its Members on techniques used to protect data during the development phase. The vast majority (80%) actually scrub or mask this data. The rest (20%) allow sensitive data to be used, but rely on access controls to protect it. Noticeably, none of the companies choose to generate substitute data to be used in place of real data.

On one thing, the panel of experts agreed: it is very difficult to get users to understand what data belongs in which category.

> We found that people were erring on the side of caution—putting things in too sensitive a category. People were being careless when they shouldn't have been or they were really being too strict when they didn't need to be—just because they didn't know any better."
>
> *—"Isaac," Director of Security Operations, Health Care Organization*

## Education of Staff: Keep it Going, Use the Experts

Security training and awareness campaigns are used to help users understand such data classification taxonomies—and indeed every other aspect of the corporate security policy.

### Let Marketing & Training do what they do best

Just as some companies go to the legal department for a definition of what needs to be *'highly sensitive,'* many go to the Marketing and Training departments to develop or deliver user awareness campaigns. *"We didn't do that in the beginning,"* admitted James, CISO at an energy company, *"and a lot of what we thought that people were going to want was rejected."*

> We all sat in the room as security people and said *'oh, this would be really catchy, this would be really cool, people are going to love this'*—and a lot of it was rejected; and a lot of people actually hated some of the things that we thought were really cool and clever. But working more with the people who have experience with actually training people and presenting things was a really smart move."
>
> *—"James," CISO, Energy Company*

## Keep it going and consider all they ways people learn

What emerged from the experts was an agreement that there is no one-size-fits-all answer to awareness training—and that CISOs need imagination and perseverance to get their message across. Keep in mind the different ways in which people learn (visually, verbally, logically, socially, etc.)

> One of the things I always try to keep in mind is that everybody learns differently. So in our awareness program, we always try to use every medium we can think of: from calendars on the walls, to posters, to *'standard of the week'* reminders; from coffee talks to webinars—even if it doesn't engage the whole company at once. Maybe a newsletter with the security crossword puzzle will get 10%, and the poster will catch another 10%."
>
> *—"Steve," CSO, Consumer Products Company*

One CISO even did a video on how to be more secure at home, realizing that people would be interested in this personally and much of it would translate to work.

## Using security champions to break down barriers

The use of security champions or liaison officers in different departments and offices throughout the company is strongly advocated. These should be drawn from the staff themselves, rather than imposed from outside. Unfortunately, security staff intimidates many employees:

> People seem to be hesitant to bring things up. Maybe they think we are just going to say *'no,'* or they're going to get in trouble. No matter how many times I feel like we try and prove the opposite of that, people are still afraid to bring things to us."
>
> *—"Megan," CISO, Financial Institution*

Liaisons and champions can also help break down these barriers. *"We call them 'security leads',"* said Megan, a CISO at a financial institution. *"They are people within a department,"* she explained, *"who have an interest in information security, or are looking to expand their leadership role within the company."* These liaison officers are frequently more

approachable, and users often bring things up with them quasi-anonymously. The security leads can help relate security goals with the users' business constraints; and help the security team find acceptable solutions.

In fact, this particular program was so successful that the security leads began to organize their own informal security campaigns within their departments.

> One of our groups had trouble about not labeling documents. The leads organized their own internal campaigns to get people more educated about it and make it more real for them, and to relate the security policy to what their business unit does on a regular basis. I saw that as a sign of success."
>
> *—"Megan," CISO, Financial Institution*

One CISO, who didn't have such liaison officers, saw the potential and decided on the spot to introduce them. *"We're going to do some data discovery*," he said. *"Not just the DLP type technology but more of a focus group working session where we sit down with the different organizations and do a data business impact analysis. I can see we actually need someone in the products and sales and marketing and ops functions to help us carry that deeper into their teams. I definitely think that's a good idea."*

## Keep it informal

Beyond implementing liaisons, CISOs should adopt an informal approach to help break down barriers to user reluctance in coming forward. One expert noted his informal approach after a recent employee meeting:

> I did an afternoon coffee talk session—to target some of our materials to the people who are more out in the field —and then I just sat in the office afterwards. What I found interesting was that people started coming by bringing up complaints or concerns on things that they probably hadn't mentioned to anybody in a year and a half of worrying about it and thinking about it."
>
> *—"Steve," CSO, Consumer Products Company*

Steve regularly sits and works in the company's cafeteria simply so he is accessible to employees who walk by and have a question. Much like the old Peanuts cartoon where Lucy hung up the sign *"The doctor is in"* our CISO experts recommend hanging up the shingle, *"The CISO is in."* Hang up your shingle—make yourself accessible—and this will help get the conversation going and the barriers down.

Even if you don't have a common area, be easy to identify and locate, says another CSO:

> I wear a Hawaiian shirt every day. I don't care if it's 9 degrees below zero; I always wear a Hawaiian shirt. That way, everybody knows who I am. I have 1,000 plus employees in my building, and while I don't know everybody, I guarantee everybody knows who the security guy is."
>
> *—"Steve," CSO, Consumer Products Company*

### Make it required

Wisegate CISO experts agree that making security training part of new employee orientation is a must. Following that up with a required annual refresher quiz helps formalize the ongoing communication to staff.

The training needs to have teeth, too—not just be an optional, suggested video that nobody ends up watching.

> If staff don't complete the training, then they don't get a raise for that year. That gives them an incentive, and it's worked pretty well."
>
> *—"James," CISO, Energy Company*

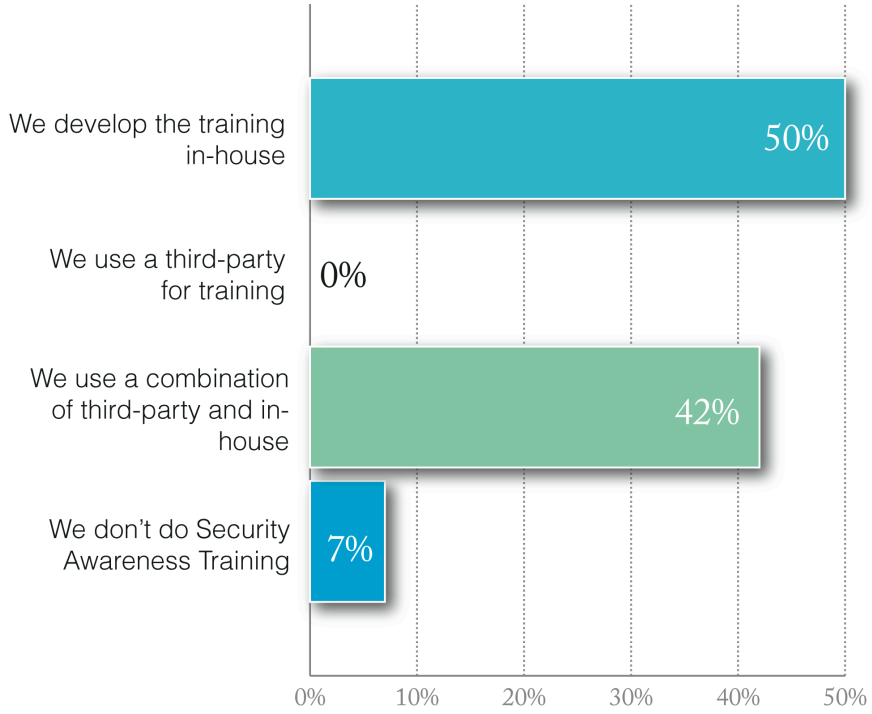
## Third-Party Training & Vendors that Shine

Awareness campaigns are one thing; formal training is another. And while most security professionals see high value in face-to-face training in *theory*, in practice, company size and multiple locations make in-person training difficult to achieve.

> I like the idea of face-to-face, but it's just impractical. It's too expensive, which is why we went to online training."
>
> —*"Martin," Director of Information Security, Government Agency*

There are numerous specialist third-party companies that offer awareness training courses and materials. Wisegate asked its Members how they put together their company's overall awareness programs.

Figure 2. Wisegate Member Poll: *"Is your training conducted in-house, by a third party, or by a combination of the two?"*




Source: Wisegate

Fifty percent of Members put together the entire program in-house. Slightly fewer Wisegate Members, at 42%, use a combination of third-party training and in-house training. Surprisingly, none relied solely on third-party specialist awareness training. But the biggest surprise of all is that as many as 7% of Members said they do no awareness training at all.

The reason for the relatively low use of specialist training probably goes back to one of the takeaways from the expert CISO's at the core of this research—there is no simple training schedule that will suit all members of staff. So even where a third-party product is attractive,

it either has to be customized for the customer, or incorporated with additional and alternative in-house material.

### Customizable third-party training preferred

One CISO described his involvement with the SANS training options. *"We selected various modules for different audiences in our organization,"* he explained, *"and packaged it that way. We are very happy with that. We have other channels and content that we used but that's really the primary one we are using. It's a good set of content and also my staff has been working directly with the SANS folks to package it, get it into our system and do some custom content, and it's been a very successful relationship."*

This seems to be key for third-party suppliers—the degree to which they are willing and able to customize their content for different parts of different companies.

### Vendors who shine

A few third-party training vendors emerged as well-regarded. SANS with their www.securingthehuman.org programs came out well because of their solid off-the-shelf content as well as their customizable modules. Members also recommended using as much off-the-shelf as possible to keep the cost down and mentioned they would like to see more standard content on HIPAA training.

Safelight came out as a strong vendor for their third-party training for developers, and other panelists reported satisfaction in using PhishMe, a company that delivers user training on the recognition and avoidance of phishing attacks.

## How to Know if Your Program is Working

The research revealed several ways of measuring whether current programs are working. See what people are actually doing by walking around or by having your liaison officers walk around and report back. There is no better way than to observe the natives being native—to see what is really sticking. Once you get liaisons in place, watch for them to really take ownership by running their own programs without the security team's involvement (this is a good thing).

Keep track of what kinds of questions you are getting. If you are still getting the same basic questions the vast majority of the time after 6-12 months of a focused awareness program, take a hard look at the program; questions should be getting more advanced.

Implement annual refresher quizzes, and keep track of how the scores are faring. This kind of feedback on scores, most missed questions, etc. can help the security team know where

to focus new programs. Tracking key DLP metrics is another way to see how awareness programs are faring. If the messages and training are taking hold, the metrics should improve over time.

Results may not always be what you think they should be, but it's important to keep them in perspective and know where you are so you can improve on it. For example, one CISO in the research found that the PhishMe tests resulted in a 25% click rate on phishing emails, and remarked, *"That's pretty good."* Another CISO saw the same results and said, however, if a 25% click rate on phishing emails was good, *"We're all screwed."*

Keeping these results in perspective, separate figures from PhishMe suggest that almost 60% of users who receive a phishing email will be tricked by it. A separate study from Trend Micro suggests that 91% of successful APT attacks start from phishing. Since such emails do penetrate companies' technological defenses, then real defense against APTs has to start with the user.

## In Closing...

Security awareness will always be challenging, but doesn't have to be impossible. In the view of these expert security Members of Wisegate, there are many innovative and practical ways to improve your security awareness efforts, and better protect your corporate data.

Some of the key takeaways from this Wisegate research are:

- **When classifying your data, keep it simple** so it's easy for employees to use. Start with labels that are easy to understand like "protected" and "unprotected."
- **Establish security leads** or liaison officers within and from the different departments to help bridge the credibility gap between the security team and end users.
- **The old adage of *"manage by walking around"* is true when it comes to security awareness.** Make yourself accessible to staff and regularly observe what staff is actually doing as one key way to see how things are progressing.
- **Keep it going, you're never done.** Use a variety of ways to get the message out that accommodates different learning styles. Get creative and tap your in-house experts in Marketing & Training to help the program be successful.
- **Know if your efforts are fruitful by actually observing employees**, by tracking the questions they ask, and by tracking key metrics from training and DLP tools. Use that information to improve your next awareness program.

- **You are not alone in trying to figure it out.** Even the veteran CISOs from this research are still learning and trying new things. Leverage others inside and outside your company for help, and tap into peer-based resources like Wisegate. Your peers are an amazing source of creative ideas.

More discussions on security awareness training challenges and success strategies continue online at www.wisegateit.com.

## About This Report

Complete access to Member discussions on Security Awareness and other related topics are available to Wisegate Members.

**Would you like to join us?** Go to http://www.wisegateit.com/request-invite to learn more and to submit your request for membership.

EMAIL info@wisegateit.com

**www.wisegateit.com**