APPENDIX A

Lessons from the Masters

The following insights are from companies that perform security awareness training in various forms. These companies are on the leading edge of security awareness training, and they are defining the state of the art in effective approaches, techniques, and tools. These companies generously consented to interviews where they were asked questions about how they approach security awareness training and what tips they could pass on to you.

Wombat Security Technologies

www.WombatSecurity.com

Jordan Schroeder: Who is Wombat Security Technologies?

Joe Ferrara, CEO: Wombat Security Technologies provides information security awareness and training software to help organizations teach their employees secure behavior. Our SaaS-based cyber-security education solution includes a platform of integrated broad assessments, as well as a library of simulated attacks and interactive microlearning training modules. Wombat Security Technologies' solutions help organizations reduce successful phishing attacks and malware infections by up to 90 percent. For two years in a row, we have been recognized as a leader in the Gartner Magic Quadrant for Security Awareness Computer-Based Training Vendors, and we are helping Fortune 1000 and Global 2000 customers in industry segments such as finance and banking, energy, technology, higher education, retail, and consumer packaged goods to strengthen their cyber-security defenses.

J. Schroeder, *Advanced Persistent Training*, DOI 10.1007/978-1-4842-2835-7

JS: What would you say is your unique approach or philosophy in security awareness training?

JF: At Wombat, we have developed a unique continuous training methodology based on established learning science principles. Our platform blends interactivity, storytelling, immediate feedback, and other proven educational techniques that are critical to knowledge retention and long-term behavior change.

We take a 360-degree view of awareness and training, and our approach integrates assessments (via topic-focused questionnaires and simulated social engineering attacks), education (via interactive and game-based modules), reinforcement techniques (via licensed posters, newsletters, and giveaways), and measurement (via data collection from assessments, education, and user input).

We encourage all our customers to think beyond programs that only use simulated phishing attacks and/or infrequent and nonengaging training sessions via methods such as presentations and videos. This is because the *and* in "security awareness and training" can be the differentiator between a successful program and lackluster results. Making users aware that a problem such as phishing exists is not the same as teaching them how to apply best practices in their day-to-day routines and how to make the right decisions in risky situations.

JS: How do you implement "gamification" in your training program?

JF: Several of the training modules we offer would be considered "game-based training" in the traditional sense, in that they utilize lives, scores, and time. But the rest of our modules also feature what we feel is the most important aspect of gamification in training: interactivity.

All of our training modules actively engage users and allow them to practice what they've learned. Key interactivity features include drag-and-drop sorting, password practice, scenario-based decision-making, and "day-in-the-life" progressions. With noninteractive presentations, users can easily tune out or shift focus to other activities while videos run. Interactivity enables engagement, and an engaged participant is far more likely to remember what they're taught. And as we all know, knowledge retention is the key to any successful education program.

JS: What challenges have you faced when integrating into an organization's culture?

JF: One (somewhat surprising) cultural challenge we faced in our organization's early days was related to simulated phishing attacks. We learned that many organizations were not comfortable sending mock attacks to their employees. This also meant, however, that they were missing the key benefit that simulated attacks provide: the capability to measure the vulnerability of the users within their organizations.

Because we understand the importance of assessing knowledge levels and establishing a baseline measurement of susceptibility, we accepted the challenge of developing a tool that would allow organizations to evaluate their employees' recognition of phishing threats. But we took it a step further by enabling assessments of other security-related issues in all threat areas, including safe use of mobile devices, physical security safeguards, and proper use of passwords.

Out of this challenge came our CyberStrength Knowledge Assessment product, which offers administrators a library of questions about a number of cyber-security topics, including compliance matters. We also allow administrators to craft their own questions so they can get a sense of how well their employees understand organizational policies and known issues. This portfolio is tightly integrated with our training modules, which means we can effectively educate users about the concepts they have the most trouble grasping.

By eliminating this cultural barrier, we made it possible for all our customers to effectively assess their employee base prior to, and during, an awareness and training program, a step that is essential to measuring progress and gauging results.

JS: What noteworthy reasons have you heard about why users resist awareness training?

JF: If we're honest, we don't believe there are any "noteworthy" reasons for resisting training. Education is critical to the advancement of people and ideas in virtually every space; why not cyber-security? That said, we certainly do come across people who question whether awareness training is "worth it," even though these same people have benefited extensively from training in order to be more effective at their jobs. Generally, these are also the same people who tend to regard "perfection" as the only adequate result for security awareness and training. Technical safeguards fail all the time; we would never suggest they be eliminated from an organization's security posture. Why take away an opportunity to make your users more savvy about cyber-hygiene and make them part of your defense against attack?

That said, we know that some organizations are resistant to training. Often, we hear concerns about taking time and attention away from employees' "day jobs." We certainly recognize that organizations are spread thin from a resources perspective. This is a prime reason we advocate for "bitesize" training assignments served at regular intervals (10 minutes here, 15 minutes there) that employees can work into their schedules as they have time. This is far more efficient than half-day or daylong training sessions that can cause disruptions department- or organization-wide for days at a time. In addition, educated employees are less likely to suffer from malware infections and other equipment downtime, which, in turn, means that IT resources are less consumed with fire drills and device cleanup.

JS: Do you think that a reward system works in security awareness training?

JF: We definitely believe in positive reinforcement techniques; in fact, they are a foundational element of our "assess, educate, reinforce, measure" continuous training methodology. Employees are far more receptive to training when they feel they are being empowered rather than shamed. When rewards are incorporated into a program, it seems to invigorate employees and make them more attentive and engaged.

We encourage, and help, our customers to recognize departments and individuals who are making positive strides and serving as good examples to others. Our PhishAlarm e-mail reporting button makes employees an active part

of an organization's cyber-security defense system, and anyone who reports a suspected phishing message is immediately recognized with a pop-up display or e-mail thanking them for their efforts and encouraging them to continue to monitor their inboxes for suspicious messages. In addition, our security awareness materials, another part of our reinforcement product offering, include options for small gifts and giveaways that our customers can use to reward good behaviors.

PhishLine

www.PhishLine.com

Jordan Schroeder: Who is PhishLine?

Mark Chapman, CEO: PhishLine performs millions of security awareness training exercises worldwide each year, including traditional computer-based training, mock social engineering tests, and risk-based surveys using our proven "plan, train, test, measure, and take action" methodology. Since 2011, millions of people have engaged with PhishLine's unique risk-based platform.

JS: What would you say is your unique approach or philosophy in security awareness training?

MC: As part of a risk-based continuous improvement process, the results of an effective information security awareness program should provide actionable observations to improve the people, processes, and technology layers of security controls.

We do not believe in a one-size-fits-all approach to training. We also do not believe that training is the only or best solution in all cases. While training can be effective, the level of effectiveness is dynamic. Training methods must be objectively measured and adjusted over time to ensure success. An effective training program must be synchronized with changes to the technical and process control environment to enable the most powerful and efficient combination to mitigate certain threats.

A big component that makes our approach unique is the emphasis on hypothesis-based testing. Rather than depending solely on external studies and benchmarks, our customers leverage specific tests to improve the security posture of their organization.

A simple example is the hypothesis that "users are more likely to click e-mails in their native language than in English." Before designing a test to validate the hypothesis, it is imperative to identify what actions will be taken if the test results support the hypothesis, negate the hypothesis, or are inconclusive.

If you cannot identify meaningful actions, there is little justification for performing the test. Risk-based methods should be used to identify more actionable tests.

We strongly feel that hypothesis-based testing is a critical component to any security awareness program. It provides context, ensures relevance, and enables appropriate remediation actions based on the resulting metrics.

JS: If you use "gamification" in your training program, how have you implemented it?

MC: Gamification can be applied to several levels of an information security awareness training program.

A basic approach is to integrate gaming elements directly into security awareness training materials with the hope of adding excitement to traditional computer-based training. Sometimes these things are engaging and fun. Other times, they are viewed as trivial or childish and can quickly reduce the credibility of your overall program. The corporate culture, geographic location, and age groups involved make a huge difference in how this style of content is perceived. We provide many styles of training directly through our Content Center Marketplace and through our content partners. Gamification may or may not be the best way to increase engagement rates and effectiveness.

Another way that we use gamification is through a customer-defined risk-based scoring system. Customers can set point values for positive and negative actions. They can then compare risk-based scores to internal and external benchmarks and measure improvements over time.

Generally, customers assign negative points to unsafe actions such as the following:

- Clicked a link or filled in a web form
- Replied to an e-mail or text message or disclosed too much information in automated out-of-office replies
- Called an unknown phone number in an e-mail or plugged an unapproved portable media device into a business computer

In a similar manner, customers assign positive points to positive actions such as the following:

- Completed training
- Reported a suspicious e-mail using the correct channels
- Hung up on a phone call before disclosing sensitive information

Customers use these metrics to look at the results of individual campaigns and to analyze trends. The scores can be arbitrarily grouped to enable custom dashboards to drive a competitive spirit that fits the specific culture and goals of the organization.

JS: What challenges have you faced when integrating into an organization's culture?

MC: At the basic level, everyone initially struggles with selecting appropriate themes for the mock social engineering exercises. The frequency of tests, the sophistication of tests, the pre-announcement of tests, the number of people to test, what level of results to share, and other common issues need to be addressed.

Beyond the basics, the biggest cultural challenges we face are misguided metrics and too much focus on a small number of solution choke points.

Many information security awareness programs become obsessed with one and only one metric: the click-through rate. This easy-to-understand metric represents the percent of people who clicked a link in a particular campaign e-mail. To be fair, much of the marketing in this industry historically focused on reducing click-through rates.

This myopic view ignores the fact that not all clicks are created equal from a risk perspective. If a user clicks a link, then submits a login and password, and then uploads a budget spreadsheet, is that the same risk than if they just clicked a link and closed a landing page? Are there other risky actions a user can take other than clicking? Many attackers are using attachments and other techniques to perform social engineering. You can learn a lot by performing a mock phishing campaign that has no links whatsoever. The call to action can be to solicit an e-mail reply or to direct the user to a different vector, such as calling a phone number.

One of our customers made the analogy that measuring the success of a security awareness program by looking only at raw click-through rates is just like measuring the success of a patch management program by looking at the number of new vulnerabilities found each month.

Metrics must be contextual, relevant, and actionable. For a vulnerability management solution, the raw number of patches is much less interesting than the average time to patch. For a phishing program, putting raw click-through rates in the context of hypothesis-based testing and risk-based observations will allow much better, more actionable metrics. "We learned this, we validated that, we discovered this, and we adjusted that."

The second biggest challenge is the tendency to put too much focus on a small number of solution choke points. Early on, programs tend to exclusively focus on the "teachable moment."

While there is good supporting evidence that the teachable moment can be the most effective single approach, there are many easily identifiable scenarios where alternative approaches may be more effective.

- The "five-second rule" is where users quickly close their browsers in the hopes that they were quick enough that the click did not count and they do not need to take the in-the-moment training. How can you identify those users and apply a different approach?
- Although it may be the teachable moment, some users are not exactly in a "teachable mood" right after you tell them that they have just been duped. How can you change your approach to provide an opportunity for positive behavior modification for those users?
- Finally, you need to be careful you are not training your employees to be excellent "mock phishing detectors." By performing tests that do not have a teachable moment, you may find additional insights into user behavior in a broader variety of real-world scenarios.

There is more to life than click-through rate. The same thing goes for incident response reporting rates or other single-focused raw metrics. These are all important components to an effective program. The raw metrics just have limited value on a stand-alone basis.

Ultimately, your information security awareness program should be measured based on the answer to the question, "How many risk-based observations have led to measurable remediation of controls at the people, process, and technology layers?"

JS: What noteworthy reasons have you heard about why users resist awareness training?

MC: Training is too boring, technical, childish, cartoonish, ominous, or any number of other subjective measures.

Training is incomplete, inconsistent, or contradictory. Training users to mouse over a link is of limited use to mobile device users who need to use the click-hold method. Remember when it was standard advice to instruct users to always unsubscribe from spam e-mails? More recent examples of contradictory training happens when the URL-rewrite capabilities of various spam filtering solutions no longer allow users to see the actual URL in an e-mail before clicking.

Training does not work on a device or in a work environment. A lack of speakers or the ability to use them in an office without disturbing co-workers is a valid consideration. Bandwidth requirements for multimedia training or lack of plug-in support for tablets and mobile devices can be a real problem, with similar issues for obsolete desktop hardware. The solution is to plan ahead, test, and provide multiple versions of training to accommodate various technical limitations.

Poorly translated multimedia materials can be frustrating, especially for languages with strongly divergent regional dialects. Be sure to have users in each region review the materials before deploying. The subtle nature of many security awareness training concepts can easily get lost in translation. From a scheduling perspective, be aware of local holidays before sending out campaigns and realize that current events at the local level can introduce unexpected, even offensive, interpretations of proven training content. Establish a clear feedback loop to quickly adjust content.

Finally, some people fundamentally believe training does not work. They eagerly cite examples like, "If training worked, then there would be no car accidents because we all passed driver's education." Of course, training is not a 100 percent solution, but can you imagine if all those other drivers had never taken driver's education? In the information security awareness context, you can and must objectively measure the effectiveness of specific training content on specific subsets of your target audience. Expect the results to change over time.

There are solutions to all of these problems, which should be addressed during the formal planning process with comprehensive checklists and feedback channels to guide the continuous improvement process.

JS: Do you think that a reward system works in security awareness training?

MC: At the individual employee level, what works or does not greatly depends on the culture of the organization and the age, background, and job role of the various groups of employees.

The most interesting pattern for success we see is when organizations align the security awareness training reward system with the most effective incentive systems engrained in the business.

Is your organization metrics-driven? We have seen great success where managers at every level of an organization include a security awareness scorecard every month as part of their overall metrics scorecards. Of course, the managers need to see how this helps them be more effective rather than it being punitive. Work with them to find out what they are most afraid of happening in the business. If that is susceptible to happening because of a social or cyber-attack, they are more likely to embrace your program as a solution to their problem rather than a distraction.

Is your organization audit-driven? We have seen great success where results of the awareness program were put in terms of formal observations or risk-based audit findings with observation descriptions, potential business impact statements, recommendations, and the whole audit-committee-style management response mechanisms.

Is your organization profit-driven? Quality-driven? Figure out how things actually get done and model the reward system for information security after the most effective reward system at the company.

Is there a similar program that has been effective? We have seen companies emulate effective safety programs as the model for a security awareness program. This does not mean they are merged. It simply means that if your

organization values safety, talk to the safety director to see how success is measured, communicated, and rewarded.

Ultimately, the most consistent path to success is to tightly integrate the reward at all levels with the rest of the business reward structure to take advantage of the tone at the top and to align the existing management structure to support the program because it provides real business value.

JS: What is an example of a situation where your training ended up being a much bigger success than you expected?

MC: The security awareness team at a large organization decided to leverage the "tone at the top" to encourage people to be more aware. They produced a professional video of the CEO talking through what phishing is, why it is a threat to the organization, and what he expected people to do about it. He specifically stated that mock phishing tests would be performed by PhishLine, and while he could not expect perfection, he made it clear that users would not want to get on the repeat offender list.

The "before" and "after" picture was a dramatic improvement on a sustainable basis because of a clear, consistent, strong tone at the top. Security is critically important to this organization and to the CEO. This one simple video had a bigger measurable impact than all the prior announcements, threats, rewards, and prizes.

Rapid7

www.Rapid7.com

Jordan Schroeder: Who is Rapid7?

Todd Lefkowitz, vice president of professional services: Rapid7 is engineering better security with simple, innovative solutions for IT security's most critical challenges. The company's security data and analytics solutions collect, contextualize, correlate, and analyze the security data its customers need to dramatically reduce threat exposure and detect compromise in real time. Rapid7's security awareness curricula combines learning theory and subject-matter expertise to deliver an online course that is informative and compelling. These highly interactive scenario-based modules equip employees to recognize the value of different types of information; to understand the scope, nature, and origin of the diverse risks to such information; and to behave proactively to protect this information in their everyday work.

JS: What would you say is your unique approach or philosophy in security awareness training?

TL: Our approach is to promote modularization, topic relevancy, and interactivity. Additionally, we provide supplemental and customizable content such as articles, tip sheets, infographics, and templates that can be leveraged by our customers to drive adoption and/or create specialized corporate-wide campaigns. We also offer a more flexible consumption model that allows customers to run on their own or through a hosted/cloud solution.

JS: How do you implement "gamification" in your training program?

TL: First, we use modularized, interactive "learning moments" that are little exercises that reinforce the behaviors learned in earlier training modules. Instead of being presented as assessments, they are mini-games that capture the user's attention to focus on specific topics. We find this method much more approachable and more engaging than videos and a better way to gauge a user's understanding than a multiple-choice test, which tends to be too easy and not a great test of retention.

Of course, in addition to the security awareness program modules and learning moments, we recommend that organizations use Metasploit Pro to launch simulated phishing attacks on the users of the organization as a true test of its susceptibility to attacks.

We have found that it takes a minimum of three training sessions for the material to sink in. If you plan for the need for repetition, you can optimize how, and what, you repeat. For example, some organizations assess their users first with a simulated phishing attack, follow up with training, and then assess again. By doing it this way, they gain an "extra" repetition of the training by starting with the assessment before the user is trained.

JS: What challenges have you faced when integrating into an organization's culture?

TL: Integrating awareness training into the organization's culture is all about getting the users engaged and integrating training and testing as a normal business process. When people are thinking about awareness training as a typical business activity, then training interleaves with the culture pretty naturally.

Cultural issues aren't confined to organizational culture. When we prepared translations for training materials for international customers in the past, we ran into situations where the accents of the voice actors were an issue in one country and where the color schemes had an unintended cultural significance in another. If you are preparing training materials for a company with offices in other countries, take these potential issues into account and run your materials past knowledgeable people in those areas as early in the development process as possible.

JS: What noteworthy reasons have you heard about why users resist awareness training?

TL: We really don't see users actively resisting awareness training. If you look at industry statistics, such as the annual Verizon Data Breach report, you will see that the leading attack vectors are phishing, user credentials, and social

engineering. Security awareness training is designed specifically to close those gaps and to safeguard against human compromise. Our customers realize that educating the human custodians of their data and assets is crucial to the security of their organizations. For the most part, the companies we speak with realize there are some amazing security solutions on the market; however, if you don't have competent people managing those solutions and the right supporting processes in place, it doesn't really matter how good your technology is. In the end, it's not really a question of whether companies will adopt security awareness but whether they build or buy. Threat landscape conditions demand it.

JS: Do you think that a reward system works in security awareness training?

TL: Scores can be an effective reward system. When people are confronted with competition or if they are rated against their peers, they instinctively behave differently. No one wants to see themselves slipping down a Top Users list, and people want to try to get on one. If you do post Top Users lists, don't post the Bottom Users lists or post a list of where every user ranks in the organization. Be careful not to publicly shame users because it will backfire.

Some organizations can get very creative with their rewards and punishments with success. One organization I know posted bounties for noncompliant behaviors, such as not securing laptops. Employees were rewarded $25 for taking and turning in laptops that were not physically locked. The mild shame a user felt of having to go to the security department to retrieve their laptop was more than enough to make sure it didn't happen again, and the bounty made all employees extra aware of everyone else's secure behaviors.

Recognition and rewards programs can also work, and many mature organizations have programs like this already in place. What you have to watch out for is that the existing programs do not get overloaded with the flood of work that is required to make recognition and rewards worthwhile to include in awareness training. If you do have a recognition and rewards program like this in place, don't pass off all the metrics and reporting to that team. Only the awareness administrator can fully understand the meaning of certain metrics.

Curricula

www.GetCurricula.com

Jordan Schroeder: Who is Curricula?

Nick Santora, CEO: Curricula is a new organization that takes traditional concepts from brand awareness and applies it to security awareness. Our team has a diverse background in advertising, marketing, cyber-security, compliance, audit, and education. We use a simple approach to convert learners through automated campaigns to deliver a unique experience that engages learners.

JS: What would you say is your unique approach or philosophy in security awareness training?

NS: Curricula uses story-based learning to engage learners through our campaigns. Our goal in aware campaigns is designed to connect with our learners on a personal level first. As you travel through an aware experience, you are presented with interactive experiences that engage you on the story being told and not just about security content. Each story uses characters, animations, and a detailed storyline that describes the scenario being discussed. We learn at a young age through storytelling, so we take the same approach and deliver an educational experience like no other.

The production quality behind our campaigns is very high. Our team puts so much effort not only into the content but into building the storyline, the characters, the colors, music, and everything else that plays a role in the user experience. It is that quality and expertise of delivery that is unique to Curricula.

JS: What challenges have you faced when integrating into an organization's culture?

NS: Most organizations have a linear approach when it comes to training or security awareness. Training usually consists of dumping videos or slides onto their users at the end of the year, along with HR paperwork and a few other "check the box" activities. Security awareness training shouldn't be one of them. Our approach is to educate our clients first on the purpose of security awareness, its goals, and the ROI that quality education places on the organization.

This is typically a difficult discussion because most organizations do not provide enough funding, resources, or support for cyber-security education programs. Most budget money is spent on the latest and greatest firewalls, security appliances, and other technology, hoping that users do not need to be relied on. This is a fundamentally flawed approach because setting a strong foundation of cyber-security education can be the difference between a successful attack and a prevented incident. Empowering your users with education will never cease to have an impact, and it continues to be the best ROI for preventing cyber-attacks.

JS: What noteworthy reasons have you heard about why users resist awareness training?

NS: It's a behavior that has been around for so long. As soon as the word *training* is mentioned, an unconscious behavior is made to immediately ignore the material that is about to be presented. This is from past experiences and an understanding that this will be similar to a past experience. Training is treated as punishment, and it is sad to see that approach by many companies we have

spoken with. By changing the experience, you can change interest, and by changing interest, you can change behavior.

JS: Do you think that a reward system works in security awareness training?

NS: I spoke to one organization that did phishing against their own company. They said that if a user is a contractor and clicks a link in their mock attack, the contractor is immediately fired. Subsequently, if a staff member clicks a link, they are suspended for a day. I have even talked to companies that reward a learner by offering $200 or more if they do not get phished by the mock attempt. What happened? In both scenarios, the results were more than 50 percent of the staff were *still* caught in phishing attacks. So, there is no silver bullet in implementing rewards or penalties that replaces education. The goal should be to focus on connecting with your users and delivering quality content that will help improve their behaviors.

How to Implement Third-Party Training

I asked each of these security awareness companies what advice they would give a security awareness trainer who was interested in implementing a third-party training provider into their organization. The following is what they had to say.

Wombat Security Technologies' Joe Ferrara

"We feel there are enormous benefits to utilizing third-party training over internal training. Many organizations simply don't have the resources or expertise in house to develop tools that are research-driven, fully integrated, and updated frequently to reflect the ever-evolving threat landscape. As well, relying on an internal vision can be limiting; it's often difficult to step out of the immediacy of day-to-day issues and get a sense of the bigger picture that is employee-based cyber-security risk. Coming at the problem with an internal, tunnel-like focus can cause organizations to miss out on key opportunities to change behaviors and reduce risk.

"We really encourage our customers to think beyond single-tool programs. If they're only doing simulated phishing attacks, they're missing out on the opportunity to truly educate their employees. Similarly, if they're only using training messages, they're missing out on the chance to assess and evaluate how employees respond in situations that mirror real-world attacks. A combination of assessments, education, reinforcement techniques, and measurement give organizations the variety they need to keep a program fresh and effective over the long term.

"There has been an overreliance on videos and instructional presentations in the training space, particularly with compliance-related topics. We get it; these tools feel like "the path of least resistance," and they seem to offer a quick, easy way to check the box on compliance training. But videos and presentations, though good informational tools, are not effective educational tools. Studies have

shown that users tune out during noninteractive training situations. If users are not paying attention, they have no hope of learning anything, and organizations have no hope of seeing measurable results from their training. Without interactivity, users are far less likely to be engaged and far less likely to retain knowledge. So, it's easy to see why video- and presentation-based programs have a bad rap for being ineffective. Change that approach by utilizing third-party training, like Wombat's, that puts users in the driver seat, allowing them to set the pace, make decisions, and engage with the content. This is key to driving results."

PhishLine's Mark Chapman

"Leveraging third-party security awareness programs is a great way to shorten the learning curve, quickly establish credibility, and hasten the return on investment. Dedicated vendors can provide a broad set of experience, innovative tools, and robust data that can help programs be more successful today and into the future. To maximize success, you must select the right vendor in the context of a dynamic, objectives-based program.

"The following are important factors to consider when selecting a vendor.

"Are you looking for an education-only platform, or would you like the ability to combine both threat simulation and training? If all you need is an education platform, there are many more vendors that can service those limited needs. Integrated platforms simplify the follow-up process, validate the effectiveness of campaign content, streamline reporting, and future-proof the investment.

"Is your vision to test e-mail phishing only, or would you like to be able to conduct voice, SMS, and mobile media attack simulations? While all vendors have some of these components, each will have their particular strength. The ultimate goal is to choose a fully integrated platform that includes completely automated social engineering vectors with robust educational content.

"What particular security, privacy, and/or regulatory considerations need to be met by the prospective partner? There is a lot of variation when it comes to security, with options ranging from software that is hosted on shared public cloud infrastructure to highly secure dedicated hosting facilities. Some vendors provide options for on-premise deployment.

"Do you want the vendor to provide hosting of your own training content? Vendors who can host SCORM-compliant content can provide flexibility that can allow you to focus on the content and let the vendor handle the hosting. There are also options where you can host vendor training content on your existing learning management system.

"Will you require significant customization of the training content? Customization capabilities and costs widely vary between vendors. Many allow you to incorporate your own branding, logos, and styles. The ability to customize the actual curriculum with your specific message is another important consideration.

"Does the vendor provide third-party content from other security awareness providers to broaden the training catalog? Training content needs to be fresh and objective. A one-stop shop can provide depth without introducing new vendor relationships.

"Is malware analysis and centralized phishing reporting a requirement? Do you require a plug-in for your e-mail client? If so, what e-mail clients require support? Many vendors provide options. The lines are starting to blur between awareness vendors and incident response solutions. Be sure to consider if a best-of-breed or an all-in-one approach is the most appropriate for your environment.

"Do you have specific reporting requirements? It seems every vendor allows reporting data to be exported to Excel. Are you required to perform extensive gymnastics in Excel to get the data you need? Look for a vendor that allows for custom reporting and analysis in a format that is ready for you to use.

"Are there other systems or data sources that you would like to integrate with the testing and training platform? Risk-based solutions tend to work better with more data. Vendors provide several approaches, which may help take your program to the next level by extending the teachable moments to the teachable moments that matter. API options can help you leverage the data and capabilities otherwise trapped in a vendor solution.

"While this list is not exhaustive, it will help you narrow down your search to a few providers and will help you focus on the key capabilities you require to make *your* program successful.

"The best advice is to recognize that a successful program is dynamic and must have clear goals and objectives. Leverage the vendors that most deeply align with your current and future objectives."

Rapid7's Todd Lefkowitz

"Generally speaking, it's cheaper to buy security awareness training than to build. Enlisting a third party, whose job it is to focus intently on security awareness, will not only be diligent in innovation to stay ahead of competitors but also be active in ensuring content is kept fresh and relevant.

"Third parties also have greater access and economies of scale when it comes to rollout and localization on a global scale. Translation can be exceptionally expensive, and third-party vendors can significantly lessen the financial burden to their customers with the inclusion of language packages within their solutions. If a vendor you like doesn't have a language you require, they may be willing to make the investment without an up-charge to translate, knowing that it will be a reusable commodity after your purchase.

"A lot of companies are migrating to the cloud, and security awareness vendors are certainly among them. Some vendors allow their learning modules to be run through a learning management system. Picking a vendor that allows for this will streamline onboarding and use of the solution; it negates having to

learn an entirely new system. Furthermore, if you're already accustomed to a learning management system, you will be familiar with the reporting formats, reducing costs, since they reduce hosting fees.

"A solid phishing simulation tool is a must as well. It's a great way to really assess the efficacy of training and how well your employees adopt the content through their training experience. If the third party does not have a phishing simulation tool, then a product like Rapid7's Metasploit Pro can be leveraged to generate phishing campaigns pre- and post-training."

Curricula's Nick Santora

"There are a lot of great tools and services out there. With cloud services becoming a popular option, it is easy to find expert third-party organizations that can perform a function for your business at fractions of the time, cost, and effort. Take accounting software, for example. There are plenty of companies out there that can handle your books, transactions, integrations, and management, all with a few simple clicks.

"Likewise, third-party security awareness teams are an excellent option for businesses to leverage the resources and development of a focused service. At Curricula, all we do is cyber-security awareness training. We don't do consulting work, we don't sell widgets, we simply focus on teaching people cyber security. In today's world, taking advantage of your core competencies can mean the difference between staying in business and floundering. Getting flooded with wasted resources, stressed-out staff, and an unclear plan on how to deliver security awareness training can be easily avoided by engaging a third-party security awareness team who is ready to execute a proven plan."

References

Aaron Dignan. Game Frame. Free Press, New York, NY, 2011.

Abraham Maslow. Toward a Psychology of Being. Wiley and Sons, New York, NY, 3rd edition, 1998.

Charles Coonradt. The Game of Work. Gibbs Smith, United States, 2012.

Dave Aitel. Why you shouldn't train employees for security awareness. CSO Online, July 2012. http://www.csoonline.com/article/2131941/security-awareness/why-you-shouldn-t-train-employees-for-security-awareness.html.

Jaikumar Vijayan. Phishing emerges as major corporate security threat. Network World, April 2011. http://www.networkworld.com/article/2202359/security/phishing-emerges-as-major-corporate-security-threat.html.

John Leyden. Half of phish marks respond to scams within one 'golden hour'. The Register, December 2010. http://www.theregister.co.uk/2010/12/03/phishing_response_survey/.

Karen Pryor. Don't Shoot the Dog! Bantam, San Francisco, USA, 1999.

Karen Pryor. Hidden aversives: Are you punishing unconsciously? KPCT, January 2005. http://www.clickertraining.com/node/101.

Karen Pryor. The shape of shaping: Some historical notes. KPCT, April 2007. http://www.clickertraining.com/node/1135.

Karen Pryor. The eight ways of changing behavior. KPCT, September 2012. http://www.clickertraining.com/node/290.

Karla Jo Helms. Cybercrime statistics expose five industries most susceptible to phishing attacks. PR Newswire, May 2011. http://www.prnewswire.com/news-releases/cybercrime-statistics-expose-five-industries-most-susceptible-to-phishing-attacks-122436438.html.

Melanie Greenberg. Nine essential qualities of mindfulness. Psychology Today, February 2012. https://www.psychologytoday.com/blog/the-mindful-self-express/201202/nine-essential-qualities-mindfulness.

J. Schroeder, *Advanced Persistent Training*, DOI 10.1007/978-1-4842-2835-7

Nancy Toppel; Allen Smith. Use of spear phishing exercises to increase security awareness. Proceedings of the 14th Colloquium for Information Systems Security Education, June 2010. http://cisse.info/resources/archives/category/14-papers?download=165:1716-2010.

NRC. The problem of changing food habits. Bulletin of the National Research Council, (108):35–65, October 1943.

Oliver Rochford. Security awareness training: It's the psychology, stupid! SecurityWeek,September2012.http://www.securityweek.com/security-awareness-training-its-psychology-stupid.

Ponemon. The state of information security awareness: Trends and developments. Technical report, Ponemon Institute, 2014. https://www.securityinnovation.com/uploads/pci-ponemon-whitepaper.pdf.

Ponnurangam Kumaraguru; Justin Cranshaw; Alessandro Acquisti; Lorrie Cranor; Jason Hong; Mary Ann Blair; Theodore Pham. School of phish: A real-world evaluation of anti-phishing training. Carnegie Mellon University, June 2009. http://cups.cs.cmu.edu/soups/2009/proceedings/a3-kumaraguru.pdf.

Ponnurangam Kumaraguru; Yong Rhee; Steve Sheng; Sharique Hasan; Alessandro Acquisti; Lorrie Cranor; Jason Hong. Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. Technical report, Carnegie Mellon University, 2007.

Richard Fry. This year, millennials will overtake baby boomers. Pew Research Center, January 2015. http://www.pewresearch.org/fact-tank/2015/01/16/this-year-millennials-will-overtake-baby-boomers/.

SANS. 2015 security awareness report. Technical report, SANS Securing The Human, 2015. http://www.securingthehuman.org/media/resources/STH-SecurityAwarenessReport-2015.pdf.

Samantha Manke; Ira Winkler. The habits of highly successful security awareness programs: A cross-company comparison. Technical report, Secure Mentem, 2012. http://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf.

Sean Gallagher. DHS infosec chief: We should pull clearance of feds who fail phish test. Ars Technica, September 2015a. http://arstechnica.com/security/2015/09/dhs-infosec-chief-we-should-pull-clearance-of-feds-who-fail-phish-test/.

Steve Corbett. Targeting different generations. Encyclopedia of Educational Technology, 2008. http://www.stevecorbett.net/edtecportfolio/generations/start.htm.

Taylor Armerding. Millennials becoming known as Generation Leaky. CSO Online, February 2015. http://www.csoonline.com/article/2884638/security-awareness/millennials-becoming-known-as-generation-leaky.html.

Thanuja Vasudevan. Cyber goons phish beyond financial transactions. Financial Chronicle, August 2010.

Tim Greene. Phishing scams dupe the most active online users. Network World, April 2011. http://www.networkworld.com/article/2201901/malware-cybercrime/phishing-scams-dupe-the-most-active-online-users.html.

William Jackson. To defeat phishing, energy learns to phish. GCN, June 2011. https://gcn.com/articles/2011/06/13/doe-phishing-test.aspx.

Index

J. Schroeder, *Advanced Persistent Training*, DOI 10.1007/978-1-4842-2835-7

N

O

P, Q

R

S

T, U

V

W, X, Y, Z