Security Awareness Training Evolution

Version 1.5

Released: October 30, 2013

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

Licensed by PhishMe

PhishMe provides organizations the ability to improve their employees' resilience towards spear phishing, malware, and drive-by attacks. PhishMe's methodology entails periodically immersing employees in simulated phishing scenarios and presenting bite-sized, engaging training, instantly to those found susceptible. The solution provides clear and accurate reporting with metrics on user behavior, allowing customers to successfully manage their employees' security behavior. With over 4 million individuals trained in 160 countries, PhishMe has been proven to reduce the threat of employees falling victim to advanced cyber-attacks by up to 80 percent. PhishMe works with Fortune 1000 companies and organizations across industries such as government, financial services, energy, healthcare, higher education and defense. For additional information, please visit: www.phishme.com.

Copyright

Security Awareness Training Evolution
Table of Contents

Why Bother Training Users?

Security luminaries largely pan awareness training as an ineffective waste of time and money. Are they wrong?

Everyone seems to have an opinion about security awareness training, and most of them are negative. Security luminaries largely pan awareness training as an ineffective waste of time and money. They use weird analogies, claiming we cannot train folks not to eat fast food, so no training ever works. Are they wrong? We have all sat through endless PowerPoint slides telling us what we can and cannot do on the Internet. They threaten us with termination unless we follow the rules specified in the 15-page Acceptable Use Policy, without any context for why those rules matter. It's not much different than parents saying you cannot do something "because we said so!"

But regardless of the specific situation, security awareness training occurs for a few reasons, some more productive (and strategic) than others:

1. **Limit Corporate Liability:** If an organization doesn't make very clear to employees what they can and cannot do using corporate technology, they cannot terminate employees for doing the wrong thing. Too much of today's awareness training is built as a warning to justify termination. This kind of training is designed by lawyers expressly to enable them to prosecute employees if needed. That gives you a warm and fuzzy feeling, doesn't it?

2. **Compliance Mandate:** This use case is in play at many government organizations, who are expected to follow NIST 800-50 to comply with FISMA and build a security training program. We applaud the mandate — we all know security training wouldn't happen otherwise. But compliance requirements rarely create sufficient urgency to excel or address the original goals *behind* the regulation.

3. **Protect Information:** Before our cynicism gets the best of us, some organizations perform security awareness training to actually train employees about security. Imagine that. In this case employees need to know what not to click and why. They need to learn who to call when they think something is wrong, and how to protect their mobile devices, which increasingly contain sensitive data and access. This content is typically built by the security team or under their watch.

Adversaries have gotten better so you need to prepare employees more effectively to be the first line of defense.

If your current security awareness program is controlled by Human Resources with a heavy influence from your General Counsel, you have some work to do. If you are in charge of an awareness training program at least you can roll out some content to achieve *your* objectives. That doesn't mean you understand the latest and greatest training techniques. Nor does it mean you actually have the time to build effective training materials. But at least you can make some decisions about the training program, and that's a start.

This paper will discuss how security awareness training needs to evolve — fast. Adversaries have gotten better so you need to prepare employees more effectively to be the first line of defense. Obviously they are an imperfect line of defense, but a human control is better than no control at all.

Pragmatic Security Training

It's not like a focus on security awareness training is the flavor of the day for us. We have been talking about the importance of training users for years, as unpopular as it remains. The main argument against security training is that it doesn't work. That's just not true. But it doesn't work for everyone. Like security in general, there is no 100%. Some employees will never get it — mostly because they just don't care — but they do bring enough value to the organization that no matter what they do (short of a felony) they are sticking around. You need to accept that those folks will do what they want, and you will clean it up. You also need to realize that some of your employees will be targeted by advanced attackers. No amount of security training will protect these employees if they are targeted by an advanced adversary. To clean up you will need high end forensics, and if that's in play you probably should consult our CISO's Guide to Advanced Attackers.

Then there is everyone else. Maybe it's 50% of your folks, or perhaps 90%. Regardless of the number of employees who can be influenced by better security training content, wouldn't it make your life easier if you didn't have to clean up after them? We have seen training reduce the amount of time spent cleaning up easily avoidable mistakes.

Yet far too many organizations lose interest when they don't see immediate results. Like any program, security awareness training requires patience and persistence. This is covered in Mike's Pragmatic CSO book. Here is an excerpt:

> *The easiest thing to do regarding security awareness is to give up. Most organizations (and CSOs) are impatient. It's hard to make a consistent effort when it is not clear that progress is being made. There really is a "tipping point" in security awareness, and until you get there, it's hard to justify the time and investment required by the program.*
>
> *Thus the most critical success factor for security awareness is CONSISTENCY and PERSEVERANCE. It takes months and years of consistent effort to make security awareness second nature. Your employees have to overcome years of bad habits, like opening attachments and clicking links in emails.*

What's Broken?

How hard could it be to teach folks what not to do? You know — don't click that link. Don't open that email. Duh. If your machine doesn't work well and seems slow, call the help desk. Easy, right? Not exactly. Building effective training content is hard. You have to engage students and provide practical information and examples to keep them participating. Researchers have spent a lot of time discovering the most effective ways to structure content to teach information with the best retention. But most security awareness training materials seem to still be in the education dark ages, and don't take advantage of these insights. So the first (and most important) issue is that training materials just aren't very good. For any training content is king.

Building effective training content is hard. You have to engage students and provide practical information and examples to keep them participating.

Another problem is unclear objectives. Is the training's purpose to check a box and get an auditor off your back? Are you trying expressly to get employees not to click things? Perhaps you don't want them to plug in USB sticks found in the parking lot? Are you trying to make them understand the physical threats from an intruder gaining access to your facilities? When training materials attempt to cover every possible attack vector they get diluted, and students retain very little of the material. Don't try to boil the security ocean with overly broad materials. Focus on specific real threats that are likely in your environment.

What about incentives? Clearly employees need to complete the training. Maybe they need to pass a test to get corporate-issued computing devices, but what then? As a rule employees don't have any reason to retain information past course completion, or to use it on a daily basis. If they click the wrong thing IT will come clean up the mess, right? Without either positive or negative incentives, employees forget the course as soon as they finish.

Finally, political or organizational headwinds may sabotage your training efforts. If you approach HR to improve training materials, they may not cooperate because they don't want to disrupt their carefully scripted first-day orientation schedule. Or business users may not want to take employees out of their jobs for some crappy security training that doesn't help them make their numbers. There are countless reasons other groups within the organization might resist awareness training, but many of them come back to a lack of incentive — mostly because they don't understand how important it is. And failure to make your case is your problem.

New Training for a New Day

There are many problems with existing security awareness training approaches. But pointing out problems is much less useful than offering solutions. Let's list some ideas to improve the training:

1. **Proper Outcomes:** The objective of any security awareness training program must be to improve the security of the organization. Focus on that outcome — not on checking a box for compliance or any other justification. You need to develop metrics and incentives in the context of the business problem of protecting information, rather than for anything else.

2. **Better Content:** Security awareness training content clearly needs to be better, so we need modern training methods. Education has changed, and your training materials need to be current. It is also a good idea to integrate video as appropriate — especially because some modern tactics need to be seen to be believed. Simulated attacks on employees have proven effective, particularly phishing because it is one of the most common vectors for gaining presence on your network.

3. **Reinforcement:** If your training program starts and ends with a class your chances for success are limited. It usually takes 4-5 impressions to really absorb any lesson, so make sure the training program includes ongoing reinforcement.

4. **Gamification:** We talked about the lack of incentives above, and one effective type of incentive is a game or contest that focuses on results: a reduction in successful attacks. This engages the competitive instincts of business leaders who hate to lose — even if it is just a security contest.

5. **Organizational Buy-in:** The rest of the business takes its lead from the executive suite. So you need to sell security awareness training in a language senior executives understand: dollars and cents. You might position training as a way to improve the effectiveness of security controls you are already paying for.

Focus on Great Content

How much time and effort to spend on security awareness training is a company-specific decision which depends on the sophistication of your employee base, the kinds of adversaries you face, and your organizational culture. Regardless of how much you invest and which techniques you use, if your security awareness training *content* is poor it will be wasted. Now let's tackle the issues around developing (or buying) great content — as we said before "Content is king."

> Regardless of how much you invest and which techniques you use, if your security awareness training content is poor it will be wasted.

We begin by defining great content. Here are some key requirements:

1. **Behavioral modification:** The training content needs to work. You should be managing to outcomes, and your desired outcome for security training is that employees learn what not to do (and subsequently don't do it), so if behavior doesn't change for a reasonable percentage of employees, the content is ineffective.

2. **Current:** Security is a dynamic environment so a security training curriculum needs to be kept up to date. Yes, you still need to tell employees about vintage 2009 attacks because you will still see those at times. But you also need to train them to defend against the latest and greatest attacks, which they are *more* likely to see in the short term.

3. **Comprehensive:** Captain Cliche reminds us that security is only as strong as the weakest link. Employees need to be prepared for most everything that will be thrown at them. It is neither realistic nor feasible to turn normal employees into security professionals, but they can understand the major attack vectors and develop a 'Spidey-Sense' so they are aware of attacks as they happen. They won't be able to defend against attacks you don't train them on.

4. **Compelling:** Most employees don't really know what's at stake so they don't take the training seriously. We are not fans of trying to scare employees or playing Chicken Little, but they need to understand the consequences of data breaches. This is a matter of integrating a few stories and anecdotes into the training materials to make the situation a bit more real, humanizing attacks, and taking them from theory to reality.

5. **Fun:** Boring content is boring. If employees don't enjoy the training materials they will shut down and do just enough to pass whatever meaningless test you put them through. They will forget what they learned as soon as they leave the room. As corny as it sounds, no fun generally means little or no learning.

Most folks have short attention spans. Optimize your content in small chunks, typically 3-5 minutes for some kind of lecture, or an exercise that can be completed in that timeframe. The gluttons for punishment may want to blast through 5-10 chunks at a time, but give folks the option to get through a lesson during a quick break. That way they don't have to totally disrupt the flow of their day for training.

Weigh the effectiveness of video against a presentation deck with a talking head. Stories are more effectively told through video, and training materials need to tell a story about the importance of security and how to defend against attacks.

Gamification

Two key requirements for better content are that it should be *compelling* and *fun*, so the shiny new concept of 'gamification' comes into play. It's not actually new — many of your younger employees were probably taught to type by Mavis Beacon. Now academia is catching on, and a number of studies show that competition and gaming dramatically increase learning and retention.

One organization we have worked with pits business units against each other for the fewest infections per quarter. The BU with the lowest number each quarter gets possession of a $100 trophy, and the company takes the contest very seriously. It turns out business leaders want to win, whatever the game is. That isn't really an educational 'game,' but it is competition to achieve the right outcome for the organization, minimizing infections along the way. And nothing gets everyone on board faster than senior management making it clear they want to win.

In terms of structuring content within the context of a game, here are a couple ideas to ponder:

1. **Levels:** Humans love to achieve things and feel that sense of accomplishment. If your training involves multiple levels of content within the materials, and employees need to qualify to proceed to more advanced lessons, they will be pushed to advance their skills to attain the next level.

2. **Points:** Depending on the nature of the training you can award points for better or faster results or performance. Again, human nature is to collect things for a sense of accomplishment.

3. **Scoreboard:** If you award points for proper outcomes, you might as well highlight the best performers to recognize employees doing exceptionally well, and to drive others to compete.

4. **Penalties:** No one likes to lose what they have gained, so you could take points away from an employee if they don't complete the next level (or at least go through the next lesson) within a certain amount of time. Knowledge erodes over time so you want employees to complete materials as quickly as possible, and reinforce the material soon after.

And that's just the tip of the iceberg. You could design (or license) a curriculum using an offensive mindset. Perhaps a simple capture the flag scenario where employees try different tactics to compromise devices, move laterally, obtain the targeted content, and exfiltrate. By understanding the methods and processes attackers use, employees prepare to defend themselves. And it's fun. Just ask any pen tester. The possibilities are endless, but it has become clear that gamification will become a key part of security awareness training.

Keep in mind that without incentives and/or penalties, even compelling games can fall by the wayside. Employees are busy and under job pressure. If they need to choose between your fun security game and getting something to their boss on time you know what they will choose — and if they don't it is your fault. So organizational buy-in and a mandate from senior management about the importance of training are critical. We will talk about getting that buy-in later in this paper.

Hack Thyself?

Above we discussed how training content depends at least partially on organizational culture. The same goes for attacking your own employees with social engineering tactics. When hacking your employees you risk offending some who fall for an internal phishing simulation or insert a found USB stick into their computer. Folks don't like to be called out on their mistakes — especially in a public forum. But that doesn't mean you shouldn't be testing them. The folks who are pissed off are likely to be your best students. They are very unlikely to make the same mistakes again. Just understand that you might need a flack jacket to handle their ire.

> Folks don't like to be called out on their mistakes — especially in a public forum. But that doesn't mean you shouldn't be testing them.

There is a simple reason using social engineering against your employees (usually via simulation) is critical to security awareness training: *adversaries use social engineering*. Adversaries gain presence on your networks by sending phishing email to unsuspecting employees. They call your help desk to reset passwords and use a variety of tactics for reconnaissance and to stage attacks.

Your only defense against these tactics is to show employees how they work, and you cannot do that effectively with static training content. You cannot get enough feel for how well employees get the message from whether they fell asleep during the lesson or not. Social engineering attacks lend themselves particularly well to simulation — if you actually stage a phishing (or other social engineering) simulation in your environment you will see very quickly how effective your training efforts have been.

> Use mistakes as a catalyst to deliver impactful training to educate employees about what they did wrong and should do differently next time.

Be sure to handle employees duped by the simulation with grace. There is no need to publicly embarrass employees or call out their mistakes during a company all-hands meeting. Use mistakes as a catalyst to deliver impactful training to educate employees about what they did wrong and should do differently next time.

Also be sure to get your General Counsel and Human Resources into the loop before the test. This isn't a question of asking for permission, but make sure they are aware, and hopefully they can suggest how to handle the inevitable friction.

If you are going to social engineer employees, here are a couple requirements to keep in mind:

1. **Deliverability:** Step 3 of the Kill Chain, which describes how advanced attacks work, is all about deliverability. The best exploit in the world isn't effective if the targets don't have an opportunity to execute it. So whether you are dropping USB thumb drives or sending phishing messages, you need to make sure your simulated attack gets through.
2. **Flexibility:** Today's attackers don't use just one tactic. So your simulation needs to be able to launch a variety of attacks at employees, not limited to email delivery, but covering other web-based and application-centric attacks. Attackers use whatever means are necessary to break in, so you need to simulate their tactics.
3. **Metrics and tracking:** First make sure to grab a baseline to figure out how your employees do with little or no training. That way tracking the success of employees in detecting attacks over time enables you to identify trends and isolate weak links: employees. These metrics also provide a way to justify your ongoing investment in awareness training — assuming the results are positive.
4. **Integration with existing training platforms:** If your organization already has a corporate training platform it makes sense to leverage that. Anything you build should use the existing platform, and security awareness training content you buy should be integrated with the existing training system — typically via a standard like SCORM.

Buy or Build

We don't want to make snap judgements about your capabilities but you probably aren't a world-class video director, game designer, or phishing attack simulator. So developing this kind of content on your own may be beyond your skills and interest. You should probably look for commercial training content. How can you find and buy these kinds of services?

It is a fast-moving market so you can start with a quick web search. Take a look at 5-10 providers of security awareness training content listed in your web search and check out their sites. Remember that this content is generally delivered online. Watch their demo videos, play their demo games, and get a feel for how their system works. Much of this decision is subjective. Do you like it? Is it entertaining and current? Would your employees like it, and therefore be much more likely to participate?

> Many of these training services are now delivered via a subscription-based SaaS-type offering, so apply the same discipline as when buying any service.

Once you have a short list of potential providers you will want to run a test group through the training or simulation and do a focus group of sorts to gauge effectiveness and cultural fit. Many of these training services are now delivered via a subscription-based SaaS-type offering, so apply the same discipline as when buying any service. You need to negotiate service levels, understand the provider's data security (your employee data will be in their system), and ensure you can get out of the agreement if the curriculum isn't kept up to date.

Quick Wins

As you move your security awareness training program from theory to reality, don't forget the unassailable truth that the success of any security initiative is based on building momentum and making demonstrable progress early in the deployment cycle. This is not only for projects that involve implementing shiny boxes to block things. With a program as visible as security awareness training, where success is not necessarily directly attributable to training, the need for a Quick Win is more acute. Especially given the likely pushback from employees duped by attack simulations. But let's not put the cart before the horse.

> Don't forget the unassailable truth that the success of any security initiative is based on building momentum and making demonstrable progress early in the deployment cycle.

Buy in

You cannot roll out new and updated content without getting the organization to buy into the need to revamp any security awareness training initiatives. Selling the training program internally involves making a case that the investment in training curriculum, services, and employee time will be recouped in security outcomes.

The best way we have found to make this case involves leveraging attack and breach data, which fortunately is reasonably plentiful. Start with data on the types of attacks that result in compromised devices (available in the myriad breach reports hitting the wires each week), and position the value of training around the fact that most delivery methods for weaponized exploits involve social engineering. From there you can look at the potential economic impact of those attacks — in terms of lost data, compliance fines, direct incident response, and disclosure costs. Compare to the costs of improving training, and the case for investment should come clear.

Don't stop justifying with direct cost savings from reducing successful attacks — point to operational benefits as well. These include improved malware detection and accelerated incident response from having employees versed in security and attack vernacular. Security-savvy employees can tell you what they clicked on, which websites they visited, and why they believe they have been compromised — facilitating triage and root cause analysis.

And don't be bashful about using information from your own organization. If any of your employees have been compromised due to tactics directly taught in the awareness training (such as phishing messages), you have good evidence that the impact of attacks (including clean-up costs) could potentially be reduced by more effectively training employees.

Baseline

Once the organization is on board you should be able to demonstrate the program's ongoing value. You need to figure out where you are right now. Run a representative sample of employees through the qualification tests and/or simulations to gauge where they are before training starts. This will provide a baseline to compare future results and metrics against.

Of course there is always the happy chance that your sample of employees could perform exceptionally well in the baseline tests, reducing the urgency of security awareness training. This would be a lovely problem to have. We have been doing this a long time, and we cannot pinpoint many (or any) examples of being pleasantly surprised by employee security knowledge, but there is always a first time, right?

More likely you will see the seriousness of your situation and gain a renewed appreciation for the importance of moving the training program forward decisively and quickly.

Low Hanging Fruit

The good news is that starting without a formal or effective security awareness training program, initial improvement is likely to be obvious and significant. You can pretty much count on employees starting with very little security knowledge, so a little training typically makes a big difference. Getting the quick win is about making sure you take a baseline and improve on it right away. That is not a particularly high bar, but the momentum gives you leeway to expand the program and try new techniques.

Be careful not to squander any momentum you build or leave ongoing improvement up to chance. You know the old adage: failing to plan means planning to fail. You should think about a broader and more strategic program to deliver on your security awareness training program.

> Be careful not to squander any momentum you build or leave ongoing improvement up to chance.

The Virtuous Cycle of Training Success

Your program needs to acknowledge and address the fact that most students (of anything) rarely understand and retain key concepts during initial training. Don't assume that security awareness will be any different. So let's consider a logical process which provides a number of opportunities to expose employees to the material, in order to increase their likelihood of retention.

1. **Initial Training:** As described above you need to deliver great content that will be current, compelling, comprehensive, and fun, while providing a catalyst for behavior modification.

2. **Competition:** A good way to get the most value out of the initial training and ongoing efforts is to establish contests and other means to get employees' competitive juices flowing. Award prizes, use incentives to reward employees for doing the right thing and competing effectively, and motivate them to practice their new security skills and awareness.

3. **Reinforcement:** Whether it is a matter of additional training based on the results of periodic simulations or tests, mandatory re-qualification to force re-engagement with the content, a monthly newsletter, or all of the above, you want security to be top-of-mind (or at least not out-of-mind) — which requires a number of opportunities to reinforce the training content with employees.

4. **Updates:** The dynamic nature of security, with its constantly changing attack vectors, isn't normally viewed as a positive, but when looking for opportunities to reinforce the messages of security training that dynamism provides an important opportunity. You need to retrain employees on new attack vectors as they develop. This provides an opportunity to go back to the fundamentals and hammer security basics again.

5. **Lather, rinse, repeat:** The only way to fail at security awareness training is to give up. Build a process to stay in front of employees, reward them for good outcomes, and reinforce training materials on an ongoing basis — together these techniques position your program for continuous improvement.

Trending and Ongoing Success

You have a baseline and a repeatable process to ensure employees get the most value from your security awareness training program. What next? Go operational: track the success of your program over time, and adapt to what's working and what isn't. Remember — there is no place for ego when trying to get employees to do the right thing. If an aspect of the training program isn't measuring up, either tune it or jettison it. If your employees reach a plateau of success and improvement levels out, you might need to look at more individual training options to work directly with the ones making the same mistakes over and over again. Whatever it takes to keep trending in the right direction.

Remember — there is no place for ego when trying to get employees to do the right thing.

As with every other security control, you should be constantly evaluating effectiveness and tuning the program to optimize its value. By taking a baseline and showing quick improvement you buy some time, but sustainable success for awareness training requires consistent improvement to justify continued effort and funding, so you need to be open to evolving the program as needed.

Summary

We explained why for liability, compliance, and even security reasons you need to train your users in security. The question is how much time and effort to put behind the effort. We see that consistent efforts driven by great content, particularly coupled with modern tactics such as gamification to engage employees, can quantitatively help people defend themselves against common attacks. But you need to be realistic — nothing is perfectly effective in a security context. That means you cannot reach every employee, and employees do stupid things. But you can reach some or even most, and they will minimize the number of issues you need to clean up.

> Security-aware employees protect your data more effectively, it's as simple as that, regardless of what you hear from naysayers.

To give yourself a fighting chance you need senior management support, so ensure you have organizational buy-in from the get-go. Once the training program goes operational it is about delivering the training, keeping it fun, and reinforcing the lessons on an ongoing and consistent basis. It's not brain surgery but it takes commitment and persistence.

As we have said throughout this paper, employees are clearly the weakest link in your security defenses, so without a plan to actively prepare them for battle you have a low chance of success. It is not about making every employee a security ninja — instead focus on preventing most of them from falling for simplistic attacks. You will still be exploited, but make it harder for attackers so you suffer less frequent compromise. Security-aware employees protect your data more effectively, it's as simple as that, regardless of what you hear from naysayers.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com or ask via the Securosis Nexus <http://nexus.securosis.com/>.

About the Analyst

Mike Rothman, Analyst/President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **The Securosis Nexus**: The Securosis Nexus is an online environment to help you get your job done better and faster. It provides pragmatic research on security topics that tells you exactly what you need to know, backed with industry-leading expert advice to answer your questions. The Nexus was designed to be fast and easy to use, and to get you the information you need as quickly as possible. Access it at <https://nexus.securosis.com/>.

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and/or speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <http://securosis.com/>.