Making an Impact with Security Awareness Training

Version 1.3
Released: October 15, 2018

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.

This report is licensed by Mimecast.

mimecast®

Awareness Training

Mimecast (NASDAQ: MIME) makes business email and data safer for thousands of customers and their millions of employees worldwide. Founded in 2003, the company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.

www.mimecast.com

Copyright

Making an Impact with Security Awareness Training

Table of Contents

Structuring the Program

We have long been fans of security awareness training. As explained in our 2013 paper Security Awareness Training Evolution, employees remain the last line of defense, and in all too many cases those defenses fail. We pointed out many challenges facing security awareness programs, and have since seen modest improvement in some of those areas. But few organizations rave about their security awareness training, which means we still have work to do.

In the paper, Making an Impact with Security Awareness Training, we will put the changes of the last few years into proper context, and lay out our thoughts on how security awareness training needs to evolve to provide sustainable risk reduction.

> Employees remain the last line of defense, and in all too many cases those defenses fail. Despite the modest improvement of security awareness programs, few organizations rave about their training, which means we still have work to do.

Revisiting Security Awareness Training Evolution

Before we get going on making an impact, we need to revisit where we're coming from. Back in 2013 we identified the challenges of security awareness training as:

- **Engaging students:** 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 be stuck in the education dark ages, and don't take advantage of these insights. So the first and most important issue is that training materials aren't very good. For all training, content is king.
- **Unclear objectives:** 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 an overly broad curriculum. Focus on specific real threats which are likely in your environment.
- **Incentives:** Employees typically don't have any reason to retain information past the completion of training, or to use it on a daily basis. If they click the wrong thing IT will come to clean up the mess, right? Without either positive or negative incentives, employees forget courses as soon as they finish.

- **Organizational headwinds:** Political or organizational headwinds can sabotage the training efforts. There are countless reasons other groups within your 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.

The industry has made minor progress in these areas, mostly in the area of engaging content. The short and entertaining content emerging from many awareness training companies does a better job of engaging employees. Compelling characters and a liberal sprinkling of humor help make their videos more impactful and less reminiscent of root canal.

But we can't say a lot of the softer aspects, such as incentives and the politics of who controls training, have improved much. We believe improving attitudes toward security awareness training requires first defining success and getting buy-in for the program early and often. Most organizations haven't done a great job selling their programs — instead defaulting to the typical reasons for security awareness training, such as a compliance mandate or a nebulous desire to having fewer employees click malicious links. Being clear about what success means as you design the program (or update an existing program) will pay significant dividends down the road.

Success by Design

If you want your organization to take security awareness training seriously, you need to plan for that. If you don't know what success looks like you are unlikely to get there. To define success you need a firm understanding of why the organization needs it. Not just because it's the right thing to do, or because your buddy found a cool vendor with hilarious content. We are talking about communicating business justification for security awareness training, and more importantly what results you expect from your organization's investment of time and resources.

If you want your organization to take security awareness training seriously, you need to plan for that. If you don't know what success looks like you are unlikely to get there.

As mentioned above, many training programs are created to address a compliance requirement or a desire to control risk more effectively. Those reasons make sense, even to business people. But quantifying the desired outcomes presents challenges. We advise organizations to gather a baseline of issues to be addressed by training. How many employees click on phishing messages each week when you start? How many DLP alerts do you get indicating potential data leakage? These numbers enable you to define targets and work towards them.

We recommend caution — you need to manage expectations, avoiding assumptions of perfection. That means understanding which risks training can alleviate and which it cannot. If the attack involves clicking a link, training can help. If it's preventing a drive-by download delivered by a compromised ad network, there's not much employees can do.

Once you have managed expectations it is time to figure out how to measure employee engagement. You might send out a survey to gain feedback on the content. Maybe you will set up a game where different business units can compete. Games and competition can provide effective incentives for participation. You don't need to offer expensive prizes. Some groups put in herculean effort to win a trophy and bragging rights.

To be clear, employees might need to participate in the training to keep their jobs. Continued employment offers a powerful incentive to participate, but not necessarily to retain the material or have it impact day-to-day actions. So we need a better way to connect training to corporate results.

The True Measure: Risk Reduction

The most valuable outcome is to reduce risk, which gives security awareness training its impact on corporate results. It's reasonable to expect awareness training to result in fewer successful attacks and less loss: risk reduction. Every other security control and investment needs to reduce risk, so why hasn't security awareness training been held to the same standard? We don't know either, but the time has come to start thinking about it.

What does risk reduction mean in the context of security awareness training? It's giving employees the necessary training, while understanding they won't retain everything. Not the first time anyway. Learning requires repetition, but why repeat the same training for someone who already gets it? That's a waste of time. So to follow up and focus on retention, you want to deliver appropriate content to employee when they need it. That means refreshing employees about phishing — not after an arbitrary or random time, but after they clicked a phishing message.

It's reasonable to expect awareness training to result in fewer successful attacks and less loss: risk reduction. Every other security control and investment needs to reduce risk, so why hasn't security awareness training been held to the same standard?

Contextual training requires integration with applicable security controls. For example you need a trigger from the email security gateway when an employee clicks a dangerous link in an email. You can also get triggers when an employee navigates to a malicious site via DNS and web security gateways which track where they browse. Finally, integration with DLP offers opportunities to revisit training on protected content after making a mistake.

Content Remains Key

We can slice and dice it many different ways, but we can't get around it. Without the right content any security awareness training program will fail. Here are five keys for engaging and effective awareness training content.

1. **Behavioral modification:** The training content needs to work. You should be managing to outcomes, and your desired result 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, that's an indication of ineffective content.

2. **Current:** Security remains a dynamic environment; your security training curriculum must keep pace. Yes, you still need to tell employees about vintage 2015 attacks because they will still see them. But you also need to train them to defend against new attack vectors like ransomware which they are likely to see in the short term. That will require ongoing training on these new attacks.

3. **Comprehensive:** Employees need to be prepared for the most likely situations. It is neither realistic nor feasible for security awareness training to turn regular employees into security professionals. But they can understand the major attack vectors and develop some sensitivity, to help them detect attacks in progress.

4. **Compelling:** Most employees don't know what's at stake, so they don't take training seriously. Don't try to scare employees or play Chicken Little, but they need to understand the consequences of attacks. It gets back to helping them understand the organizational risk of screwing up. You do this by integrating a few stories and anecdotes into the training materials, making attacks and losses real and tangible; and humanize attacks, so they feel personally relevant.

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 no retention.

6. **Short:** Also keep in mind the attention span of your typical employee is getting shorter every year. They won't sit still and pay attention to a 45 minute training session. We recommend you keep the training content short and sweet. Deliver in targeted 3 to 5 minute chunks and repeat frequently to ensure maximum retention.

Of course content is also subjective. What you like might not interest the rest of the organization. So we always recommend a broad testing/PoC process to ensure the content works for your organization. We'll get into procurement later in this paper.

Buy-In

Clearly you want employees to have fun and find the training entertaining, otherwise they tune out. But that's not the only thing you need for a successful security awareness training program. You need senior management to understand the importance of security awareness training and buy into your vision of success, as well as how you plan to quantify risk reduction and measure the impact of your program.

Many security professionals don't have a lot of experience in getting this kind of buy-in, so let's map out a few steps:

1. **Get face time:** As with any program you need to sell the benefits, which means getting off your butt and talking to business leaders.
2. **Sell the business value:** As mentioned above, you need to communicate value and clearly define success.
3. **Identify risks:** Make sure they also comprehend the risks of not training successfully. They may involve system downtime, data loss or breaches, or compliance fines. It's not about mindless fear — you need a realistic and pragmatic assessment of the downside.
4. **What do they have to do:** Finally, internal leaders need to understand the requirements on them and their teams. Are you asking for money from their budget? How much time will employees need to devote to the program?

Once you help the leadership team understand what's in it for them, the risk, and what they need to do, you should be positioned to enlist their support. You don't need senior management to push the program, especially if it's required for compliance. But it certainly helps, so spend time to line up support before you launch.

Continuous Contextual Content

Organizations need to architect training programs around a clear definition of success, both to determine the most appropriate content to deliver, and also to manage the expectations of management. The definition of success for any security initiative is measurable risk reduction, and that applies just as much to security awareness training.

To overcome limitations in security awareness training, we introduced the concept of *Continuous, Contextual Content (3C)* as the cornerstone of the kind of training program which can achieve security initiatives.

We described 3C as:

> *"It's giving employees the necessary training, understanding they won't retain everything. Not the first time anyway. Learning requires repetition, but why repeat training to someone that already gets it? That's a waste of time. Thus to follow up and focus on retention, you want to deliver appropriate content to the employee when they need it. That means refreshing the employee about phishing, not at a random time, but after they've clicked on a phishing message."*

Now we can dig in to understand how to move the training program toward 3C.

Start with Users

Any focus on risk reduction requires first identifying employees who present the most risk to the organization. Don't overcomplicate your categorization process, or you won't be able to keep it current. We suggest 4-6 groups categorized by their access to critical information.

1. **Senior Management:** These individuals have the proverbial keys to the kingdom, so they tend to be targeted by whaling and other adversary campaigns. They also tend to resist extensive training given their other responsibilities. That said, if you cannot get senior management to lead by example and receive extensive training, you have a low likelihood of success with the program overall.

2. **Finance:** This team has almost the same risk profile as senior management. They access financial reporting systems and the flow of money. Stealing money is the objective of many campaigns, so these folks need a bit more love to prepare for the inevitable attacks.

3. **HR and Customer Service:** Attackers target Human Resources and Customer Service frequently as well, mostly because they provide the easiest path into the organization; attackers then continue toward their ultimate goal. Interacting with the outside world makes up a significant part these groups' job functions, so they need to be well-versed in email attacks and safe web browsing.

4. **Everyone else:** We could define another dozen categories, but that would quickly pass the point of diminishing returns. The key for this group is to ensure that everyone has a baseline understanding of security, which they can apply when they see attacks.

Once you have defined your categories you design a curriculum for each group. There will be a base level of knowledge for the *everyone else* group. Then you extend the more advanced curricula to address the most significant risks to each specific group, by building a quick threat model and focusing training to address it. For example senior management needs a deep understanding of whaling tactics they are likely to face.

There will be a base level of knowledge, for the everyone else group. Then you extend the more advanced curricula to address the most significant risks to each specific group, by building a quick threat model and focusing training to address it.

Keep in mind that the frequency of formal training varies by group. If the program calls for intensive training during on-boarding and monthly refreshers, you'll want even more frequent training for HR and Customer Service since they are frequently targeted. Given how quickly attack tactics change, updating training all the time for those groups will keep them current.

Continuous

Just as we finish saying you need to define the *frequency* for your different user groups, the first "C" is *continuous*. What gives? A security training program encompasses both formal training and ad-hoc lessons as needed. Attackers don't seem to take days off, and the threat landscape changes almost daily. Your program needs to reflect the dynamic nature of security and implement triggers to initiate additional training.

You stay current by analyzing threat intelligence looking for significant new attacks that warrant additional training. Ransomware provides a timely example of this need. A few years ago when the first ransomware attack hit, most employees were not prepared to defend against the attack and they certainly didn't know what to do once the ransomware locked their devices. For these new attack vectors, you may need to put together a quick video explaining the attack and what to do in the event the employee sees it. To be clear, speed matters here so don't worry about the training video being perfect, just get something out there to prepare your employees for an imminent attack. Soon enough your security training vendor will update existing training and will introduce new material based on emerging attacks, so make sure you pay attention to available updates within the training platform.

Continuous training also involves evaluating not just potential attacks identified via threat intel but also changes in the risk profile of an employee. Keep on top of the employee's risk profile, integrate with other security tools, including email security gateways, web security proxies and services, web/DNS security tools, DLP, and other content inspection technologies, security analytics including user behavior analytics (UBA), etc. These integrations set the stage for *contextual training*.

Contextual

If any of the integrated security monitors or controls detects an attack on a specific user, or determines a user did something which violates policy, it provides an opportunity to deliver *ad hoc* training on that particular attack. The best time to train an employee and have the knowledge stick remains when they are conscious of its relevance.

People have different learning styles, and their receptivity varies, but they should be much more receptive right after making a mistake. Then their fresh experience which puts the training in context.

The best time to train an employee and have the knowledge stick remains when they are conscious of its relevance. People have different learning styles, and their receptivity varies, but they should be much more receptive right after making a mistake.

Similar to teaching a child not to touch a hot stove after they've burnt their hand, showing an employee how to detect a phishing message is more impactful *right after* they clicked on a phishing message. We'll dig in with a detailed example later in the paper.

To wrap up our earlier frequency discussion, you have a few different options for training delivery:

- **Scheduled:** As described above, you provide materials during on-boarding and as part of the ongoing training program. Monthly refreshers and updated training on new attacks are likely the bare minimum to meet your compliance requirements. Remember, repetition enhances retention and having an ongoing cadence to deliver training as frequently as practical will make a bid difference in your success.
- **Preemptive:** In this model you deliver training when triggered by threat intel or a change in risk profile, as determined by security analytics/UBA. The emergence of a new ransomware variant is an example of a likely trigger for preemptive training.
- **Reactive:** This model triggers delivery of training when an employee makes a mistake. For example, train on how to protect customer data after the DLP system blocks an outgoing email with a customer's social security number in the body.

Metrics

Assuming risk reduction is the overall objective of your security awareness training program, you need a way to assess its effectiveness. How can you measure your security training program? It starts by defining a baseline of security effectiveness. We all understand that assessing security goes well beyond training, but you need to understand your current security posture *before* starting a new training program.

That means tracking attacks against the organization, particularly the types of attacks most impacted by security training — including phishing, drive-by downloads, customer data leakage, etc. Obtain this information via integration with your email and web security tools and your SIEM or UBA system. If you cannot establish a baseline before the program starts, we recommend you initiate data collection immediately. It's decidedly suboptimal, but you can trend improvement over time from the start of your program.

As far as metrics to track, you can use these buckets to get started:

- **Micro:** Here you monitor employee-specific risk, such as how many times an employee clicks on a phishing simulation and how many times you've had to clean up the employee's device after malware outbreaks.
- **Macro:** These indicators include benchmark data from organizations of similar size and sector. You'll want to know how many successful attacks hit your peers. Your training vendor likely has benchmark data you can use, and we increasingly see this kind of information in training dashboards and reports to provide insight into effectiveness.
- **Organizational:** Based on micro and the macro data, how does your organization stack up? Here you'll want to make an overall assessment of the organization, based on results from tests and other risk metrics/analytics.
- **Qualitative:** You'll also want to understand what employees think of your training program. We recommend organizations perform 360° evaluations via employee surveys to gauge the effectiveness of training content, and for a sense of their general understanding of security.

For each of these metrics/assessments, you should be able to access the data quickly and easily via both a dashboard and results. The dashboard should clearly reflect both the micro and macro effectiveness of your efforts. Which employees need additional training because they make the same mistake over and over again? Which employees can't seem to find the time to complete scheduled training? Are the number of bad clicks during phishing simulations trending in the right direction?

The documentation from the program will substantiate (or not) the training efforts, which will make the difference between expanding the program or sending it to the dustbin.

Quick Wins

The 3C concepts accepts that users won't get it, at least not initially. That means you need to reiterate your lessons over and over (and probably over) again. But when should you do that? Clearly you want to have a monthly cadence to ensure they are used to hearing about security risks frequently. But also you want to train them when receptivity is high — when they just made a mistake.

To reiterate the contextual aspect of the approach, you start by determining the relative risk of users, and watching for specific actions or alerts. When you see such behavior, deliver the training within the *context* of what they see then. But that is not enough. You want to track the effectiveness of the training (and your security program) to get a sense of what works and what doesn't. If you can't close the loop on effectiveness, you have no idea whether your efforts are working, or how to continue improving your program.

If you can't close the loop on effectiveness, you have no idea whether your efforts are working, or how to continue improving your program.

To solidify the concepts, let's go through a scenario which works through the process step by step. Let's say you work for a large enterprise in the financial industry. Senior management increasingly worries about ransomware and data leakage. A recent penetration test showed that your general security controls are effective, but in a phishing simulation over half your employees clicked a fairly obvious phish. And it's a good thing your CIO has a good sense of humor, because the pen tester gained full access to his machine via a well crafted drive-by attack which would have worked against the entire senior team.

So your mission, should you choose to accept it, is to implement security awareness training for the company. Let's go!

Start with Urgency

As mentioned, your company has a well-established security program, and you can hit the ground running using the existing baseline security data. Next, you identify the most significant risks and triage immediate action to start addressing them. Acting with urgency serves two purposes. It can give you a *quick win*, and we all know how important it is to show value immediately. As a secondary benefit you can start to work on training employees on a critical issue right away.

Your pen test showed that phishing poses the worst problems for your organization, so that's where you should focus initial efforts. Given the high-level support for the program, you cajole your CEO into recording a video discussing the results of the phishing test and the importance of fixing the issue. A message like this helps everyone understand the urgency of addressing the problem and that the CEO will be watching.

> Acting with urgency serves two purposes. It can give you a quick win, and we all know how important it is to show value immediately. As a secondary benefit you can start to work on training employees on a critical issue right away.

Following that, every employee completes a series of five 3-5 minute training videos walking them through the basics of email security, with a required test at the end. Of course it's hard to get 100% participation in anything, so you've already established consequences for those who choose not to complete the requirement. And the security team is available to help people who have a hard time passing.

It's a balance between being overly heavy-handed against the importance of training users to defend themselves. You need to ensure employees know about the ongoing testing program, and that they'll be testing periodically. That's the continuous part of the approach — it's not a one-time thing.

Integrate Contextual Training

As you execute on your initial phishing training effort, you also start to integrate your security awareness training platform with existing email, web, and DNS security services. This integration involves receiving an alert when an employee clicks a phishing message, automatically signing them up for training, and delivering a short (2-3 minute) refresher on email security. Of course contextual training requires flexibility, because an employee might be in the middle of a critical task. But you can establish an expectation that a vulnerable employee needs to complete training that day.

Similarly, if an employee navigates to a known malicious site, the web security service sends a trigger, and the web security refresher runs for that employee. The key is to make sure the interruption is both contextual and quick. The employee did this, so they need training immediately. Even a short delay will reduce the training's effectiveness.

Additionally, you'll be running ongoing training and simulations with employees. You'll perform some analysis to pinpoint the employees who can't seem to stop clicking things. These employees can get more intensive training, and escalation if they continue to violate corporate policies and put data at risk.

Overhaul On-boarding

After initial triage and integration with your security controls, you'll work with HR to overhaul the training delivered during the on-boarding process. You are now training employees continuously, so you don't need to spend 3 hours teaching them about phishing and the hazards of clicking links.

Then on-boarding can shift, to focus on establishing a culture of security *from Day 1*. This entails educating new employees on online and technology policies, and acceptable use expectations. You also have an opportunity to set expectations for security awareness training. Make clear that employees will receive training at least monthly, but it small chunks as to not disrupt their work day. Inform them of the ongoing testing requirement, and who sees the results (their managers, etc.), along with the consequences of violating acceptable use policies.

Again, a fine line exists between being draconian and setting clear expectations. If the consequences have teeth (as they should), employees must know, and sign off that they understand. We also recommend you test each new employee within a month of their start date (preferably with the delivery of the monthly training content) to ensure they comprehend security expectations and retained their initial lessons.

Start a Competition

Once your program settles in over six months or so, it is time to shake things up again. You can set up a competition, inviting the company to compete for the Chairperson's Security Prize. Yes, you need to get the Chairperson on board for this, but that's usually pretty easy because it helps the company. The prize needs to be impactful, and more than bragging rights. Maybe you can offer the winning department an extra day of holiday for the year. And don't forget the **huge** trophy. Teams love to compete for trophies they can display prominently in their area.

Once your program settles in over six months or so, it is time to shake things up again. You can set up a competition, inviting the company to compete for the Chairperson's Security Prize.

You'll set the ground rules, including an internal red team and hunting team attacking each group. You'll be tracking how many employees fall for the attacks and how many report the issues. Your teams can try physically breaching the facilities as well. You want the attacks to dovetail with ongoing security training and testing initiatives to reinforce security culture.

Run Another Simulation

You'll also want to stage a widespread simulation a few months after the initial foray. Yes, you'll be continuously testing employees as part of your *continuous* program. But getting a sense of company-wide results is also helpful. You should compare results from the initial test with the new results. Are fewer employees falling for the ruse? Are more reporting spammy and phishing emails to the central group? Ensuring the trend lines are moving in the right direction boosts the program and helps justify ongoing investment. You feed the results into the team scoring of the competition.

Lather, Rinse, Repeat

At some point, when another high-profile issue presents itself, you should take a similar approach. Let's say your organization does a lot of business in Europe, so GDPR presents significant risk. You'll want to train employees on how you define customer data and how to handle it.

Next you determine whether to undertake *special* training for this issue, or whether you can integrate it into the monthly training cadence for all employees.

At some point the competition will end and you'll crown the winner. We suggest making a big deal of the winning team. You want to make sure all employees understand security is essential and visible at the highest echelons of your organization.

Once that round of training completes, you will roll out new tests to highlight how customer data could be lost or stolen. Factor the new tests into your next competition as well, to keep focus on the changing nature of security and the ongoing contest. This ongoing process both solidifies the training employees have received already, as well as continuing to extend their knowledge of current attacks.

To wrap up the scenario, at some point the competition will end and you'll crown the winner. We suggest making a big deal of the winning team. Maybe you can record the award ceremony with the chairperson and memorialize their victory in the company newsletter. You want to make sure all employees understand security is essential and visible at the highest echelons of your organization.

Sustaining Impact

We'll close the paper by highlighting what's required to sustain the impact of security awareness training over time. If the focus remains only training during the on-boarding process or just every six months, and employees don't have incentives to protect corporate date — shockingly enough, they won't. Thus, we suggest you delivery targeted training every month. Large topics can (and should) be broken up into a series of training sessions delivered each month. As part of addressing this new topic, you'll integrate with the relevant controls to enable ongoing contextual training and perform an initial test (to establish a baseline), and then track improvement over time.

You'll also want a more comprehensive set of reports to track the effectiveness of your awareness training relative to the success criteria you established at the beginning of the process. Then seek an opportunity to deliver this information to senior management, and perhaps the audit committee. Maybe each quarter you'll report on how much contextual training employees received, and how much or little they repeated mistakes after training. You'll also want to report on the overall number of successful attacks, alongside trends of which attacks worked and which got blocked. Being able to map those results back to training topics makes an excellent case for ongoing investment.

You'll want a comprehensive set of reports to track the effectiveness of your awareness training. Being able to map those results back to training topics makes an excellent case for ongoing investment.

It's a journey, not a destination, so ensure consistency in your program. Add new focus topics to extend your employee knowledge, keep your content current and interesting, and hold your employees to a high standard — make sure they understand expectations and the consequences of violating corporate policies. Building a security culture requires patience, persistence, and accountability. Anchoring your security awareness training program with continuous, contextual content will go a long way to establishing such a security culture.

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.

About the Analyst

Mike Rothman, Analyst and 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:

- **Primary research publishing**: We publish the vast majority of our research for free through our blog, and package the research as papers that can be licensed for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements, and follow our Totally Transparent Research policy.
- **Cloud Security Project Accelerators**: Securosis Project Accelerators (SPA) are packaged consulting offerings to bring our applied research and battle-tested field experiences to your cloud deployments. These in-depth programs combine assessment, tailored workshops, and ongoing support to ensure you can secure your cloud projects better and faster. They are designed to cut months or years off your projects while integrating leading-edge cloud security practices into your existing operations.
- **Cloud Security Training:** We are the team that built the Cloud Security Alliance CCSK training class and our own Advanced Cloud Security and Applied SecDevOps program. Attend one of our public classes or bring us in for a private, customized experience.
- **Advisory services for vendors**: We offer a number of advisory services to help our vendor clients bring the right product/service to market in the right way to hit on critical market requirements. Securosis is known for telling our clients what they NEED to hear, not what they want to hear. Clients typically start with a strategy day engagement, and then can engage with us on a retainer basis for ongoing support. Services available as part of our advisory services include market and product analysis and strategy, technology roadmap guidance, competitive strategies, etc. Though keep in mind, we maintain our strict objectivity and confidentiality requirements on all engagements.
- **Custom Research, Speaking and Advisory**: Need a custom research report on a new technology or security issue? A highly rated speaker for an internal or public security event? An outside expert for a merger or acquisition due diligence? An expert to evaluate your security strategy, identify gaps, and build a roadmap forward? These defined projects bridge the gap when you need more than a strategy day but less than a long-term consulting engagement.

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. For more information about Securosis, visit our website: <http://securosis.com/>.