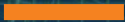


Whatworks



WhatWorks in Reducing Time to Detect Through Security Awareness Training and Testing

Introduction

The financial impact of ransomware attacks has increased the need for security operations to reduce time to detect, mitigate and restore. Financial pressures as the world emerges from the pandemic are driving efforts that can quickly show positive return on investment without increasing staffing requirements or capital expenditures. Raising the level of security awareness and preparedness of users and applications developers has proven to be the critical first step to meeting both demands.

During this SANS WhatWorks, SANS Director of Emerging Security Trends John Pescatore interviews Nick Adams, Senior Information Security Analyst from Guidewire Software to gain his insight on what he went through in the business justification details and deployment SANS Security Awareness Training offerings. Guidewire Software is a global provider of financial application used in the insurance industry. The awareness training and testing resulted in behavior changes by users and reduced vulnerabilities in application code that supported both decreased time to detect attacks and decreased business impact from incidents.

About the End User

Nick Adams is an Information Security Analyst specializing in Cybersecurity Training and Awareness at Guidewire Software, the leading developer and provider of software for major property and casualty insurance companies around the world. Specifically, we offer a suite of solutions for billing, claims, and policy portals. In his role with Guidewire, Nick focuses on building and maintaining the Security Awareness training program and educating employees in best practices. He also has a passion for data governance and data privacy standards, regulations, and controls, such as CCPA and GDPR. Having been in cybersecurity for six years, Nick graduated with a BA from Auburn University and a Juris Doctorate from Birmingham School of Law. About the Interviewer

About the Interviewer

John Pescatore joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and “the occasional ballistic armor installation.” John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Question

Nicholas, to start out, tell us about yourself and your position at Guidewire and what Guidewire does.

Answer

My name is Nicholas Adams, and I am at Guidewire Software. We're a software and SaaS provider of the platforms that property and casualty insurance companies use around the country to run their business, such as billing, policy, claims, and other products that help P&C insurers and insureds conduct the necessary business of P&C insurance. I work in the information security program as a leader in the Governance Risk, and Compliance (GRC) team, specifically handling the cybersecurity/information security awareness program, phishing simulations, role-based training, and all security-relevant training for the company. Guidewire is a global company with offices in 26 countries and over 2,500 employees. We meet the demand for all security awareness training and developer security training for the company globally.

Question

Do you report up to the CISO or is the GRC team under the chief legal counsel?

Answer

I report to our GRC team lead, who reports up to the CISO.

Question

In many companies, any type of training either goes through the human relations department or HR plays some kind of role in funding or selecting training. How does your program relate to HR?

Answer

Human resources is an important relationship to have for this sort of thing because you can get the cooperation and buy-in for many elements of the training program from them even before you need it from internal stakeholders. It helps grease the wheels

for the program. We work closely with each other. They know all data for the employees around the organization. They also know all distinctions between general employees and contractors, which is an especially important part to get down because the distinction between which contract employees need our training versus which contract employees get their training from a third-party source they actually report to is an important line of delineation to figure out so that we can make sure we're training exactly how we need to be training.

Question

In order to get started in procuring security awareness training, how did you define the business problem that you were trying to address?

Answer

It was really defined around minimum standards of compliance, becoming compliant with standards like PCI DSS, ISO, and SOC 1 and SOC 2 standards we have to comply with. So, we were starting from the ground up from "Let's get people compliant with these requirements." Then we began chipping away at the cultural aspect. What is the security culture in the organization and how do we continually improve it? That takes a lot of working with folks internally, the important relationships I have with information technology, within information security, including our security operations team. They really helped me understand and focus in on the risks in the organization as far as what type of phishing threats and other malicious threats can get through our secure email gateways.

The data privacy and legal teams are really important relationships that I've made to understand what has to be done with data privacy governance. Do we have a good handle on where our sensitive confidential information is in the organization so that we can begin to lock that down? Another important relationship is with the identity access management team, which controls privileged access management and least privilege type of data availability. Understanding who has access to what types of data in our organization was critical.

Through these relationships I began to highlight which areas of risk were most important to the company and grouped a few together into related areas. Identifying and avoiding phishing emails and malware was a risk area that quickly rose to the top of the list. Secure use of cloud services is another big one these days. This allowed me to focus on awareness training on the most important business drivers and came about from building those relationships internally.

Question

When you grouped those things together and started looking for training awareness and program-type offerings, what were some of your key criteria for how you're going to judge which ones are better than others?

Answer

Like many other companies, we started by looking at reports from analyst firms like Gartner, mainly to validate our perceptions of the capabilities and brand reputations of the vendors. SANS has been a huge brand and successful for so many years in educating security teams around the world, not just in operations but in what we are trying to achieve in security culture and behavioral change.

We believed it was important not to focus on the technical solutions and tools at the expense of ignoring the human aspect and the human gaps. SANS was the first that I remember identifying the importance of all that and really bringing that into focus for the end user. So that was important. Developer training was another area that was also really important and we were looking at getting solid training around. SANS has long played a leadership role in the identification and selection of the top developer vulnerabilities and what became the OWASP Top 10 and the OWASP Top 25.

We felt that the game changer would be cultural changes around this within organizations, that as technology advanced, we couldn't take security lightly. SANS was the mover and shaker early on in the market recognizing this.

We believed it was important not to focus on the technical solutions and tools at the expense of ignoring the human aspect and the human gaps. SANS was the first that I remember identifying the importance of all that and really bringing that into focus for the end user.

The most important element was identifying which offerings would enable us to change the security culture and organization, to really advance people's understanding of what it means to be a front-line defender and securing the systems and information on a daily basis with what they do in their jobs. It was clear SANS was the one who could best help us with all of that from the very beginning. And so we've been in a relationship with SANS for over five years now, and we've continued to renew because we've continued to see how we've grown year over year over year, and also how SANS listens to us for feedback that allows them to improve the product, which helps us as well.

Question

Employee security awareness training phishing simulation/testing are often tightly coupled. Are you doing both?

Answer

We use SANS for the awareness training and another vendor for phishing simulations. It's good to marry those two elements because the phishing simulations have become a big part of the core of what is a security awareness program now, but we don't feel both need to come from the same vendor—though in many instances, it can be helpful to bundle security awareness training and phishing simulation products. The end-user security awareness program is the most important core component that we build out from.

In fact, what we've been able to do lately is really make the SANS end-user security awareness training be the proficiency testing layer of our program to really tell us if people are getting what we're educating them on year-round. Then we test people twice during the year, in the spring and in the fall, with SANS' security awareness pre-knowledge check, and use the test-out option. If people understand the concepts that we're training them on throughout the year, they'll be able to test out of watching the related video modules. It gives us an interesting gauge twice a year when we roll the SANS training out because we've made it into a model of proficiency testing. We're not wasting users' time on modules that they don't need to see.

The SANS program consists of a lot more than just the videos. They have the standard videos. Now we can package those into a pre-knowledge check, but we also have the micro-videos that we can find interesting times during the year to roll out. We also have infographics. We have animation-type things. We have a lot of different material that SANS gives us throughout the year that really supplements the program and allows us to build campaigns month to month and quarter to quarter to focus on and highlight certain topics.

Question

Do you have some metric you've been able to collect to tie what you're doing to business benefit?

Answer

We run the phishing simulations once a month. Because, throughout the year, we're training on core security topics that we need to be training on, we can see if that causes better performance in the phishing simulations. We can also see if there are increases in how many people successfully test out via the SANS pre-knowledge check videos as part of the proficiency testing we are doing.

So, how many people can score perfectly on... I think it's three questions per subject, per training module. So, if you have password security lumped with malware lumped with encryption lumped with mobile devices, each of those subjects will have three questions assigned within that subject component. And if you can answer correctly each series of three questions for each

topic, then the person can test out. This is a growing trend, and xAPI data will only make this more possible in the future where we can gain more metrics around the actual training of the videos, what would be the end-user awareness, than we've ever had before. A lot of that data will go to the training experience itself and how confident people were in answering and selecting the answer choices that they ultimately ended up selecting.

So there's a lot of data that we're going to be able to gain. There's already more data than we've ever had before. It used to be just pass or fail. They either completed their training or they didn't. Now we're evolving into a whole other layer where we're able to, again, take the assessment of individuals' training experience as they sat down and they watched a video, or if they test it out completely. Maybe that'll reflect in the data. And then we can say, "Okay, well, these people get it, and they understand. These people had a little trouble."

But also, I think, like you alluded to, whether we're using the SANS content and training around the end-user experience effectively throughout the year will ultimately show up in the phishing data and how well people are understanding the need to report phishing when they see it and whether they're identifying those red flags in an email that relate to it being a phishing email or not, whether it's just a spam email or whether it's a phishing email. So, it should all funnel into the data relating to a lot of that user experience with the proficiency testing and the phishing simulations.

Question

Okay. I think you were an early adopter of the behavioral risk assessment capabilities. How does that fit into the mix?

Answer

That's a really important layer that we've decided is important to add. And I've promoted that internally to sell that as an option. It becomes a branch between data privacy, that data governance aspect I mentioned, and information security governance, and it's a real bridge between those two areas of our department within our company. The reason for that is because through my relationships with the legal teams and the

data privacy managers and the data privacy custodians at the organization, it became really important to understand the need to identify where the sensitive confidential data is in the organization. We can't just have it pop up by accident sometimes. We talk to this person, or this person comes and asks us a question. And then through that conversation, we find out, "Oh, you've been storing sensitive data in a repository that's actually externally facing and open to our customers," type of situation.

That's the type of information you find out before it becomes a problem. So, for instance, I look at the phishing data. I see the phishing data all the time. If I see in the phishing data that we have a certain problem with folks being susceptible to certain types of phish, and especially now that ransomware is huge in the news again, and at the same time if I see that we don't have an overall acceptable grasp of, or understanding of, where our sensitive confidential data is stored in the organization—because it could be stored in so many places, and it could be open to anybody in the organization—then there could be very broad access available instead of role-based access and privileged

access. So, that could be a huge, huge problem, both realizing you have a threat from social engineering and phishing- and ransomware-type things all the time, and you don't know where all the data is being stored that's most sensitive and confidential. When we bridge those two areas of risk together, you can begin to sense the anxiety that that could cause, that you're really sitting on quite a big threat there.

And so something like the behavioral risk assessment allows us to deploy that. And voluntarily, people are giving us information about what data they're handling, where they're handling it in, which repositories they're using to store it, if it's at rest, if it's in transit, how they're transmitting the data, or how they're storing the data. So then it's going to assign risk-based metrics and scores around departments and even individuals, depending on how granular you want to get with that. That's going to give us a lot of insight we didn't have before. And to be honest, it seems like an even more prudent first step to take before a company may go out and hire someone externally to come in and help an organization get a hold of their data governance program. Identifying where it is first becomes an important step.



Figure 1. An example of Guidewire Software's Behavioral Risk Assessment results illustrates the highest priority risks, such as IP, PII, and authentication data, that should be addressed and identified.

And so something like the behavioral risk assessment allows us to deploy that. And voluntarily, people are giving us information about what data they're handling, where they're handling it in, which repositories they're using to store it, if it's at rest, if it's in transit, how they're transmitting the data, or how they're storing the data. So then it's going to assign risk-based metrics and scores around departments and even individuals, depending on how granular you want to get with that. That's going to give us a lot of insight we didn't have before.

Question

Were you using that before the pandemic and after the pandemic? I mean, a lot of people saw the way personal or sensitive data was being handled just to keep things going. It had to be done pretty riskily as people switched to work at home. Were you having that data before and through the transition?

Answer

I would say that mindset changed during the pandemic because of that situation, like you mentioned. Far more people, the physical spaces moved remote, all remote for companies like ours. And so we really understood that what was the physical security aspect of what we did before was less concerned about what people were doing with sensitive data that they may live on a copy machine versus how they're sending data in transit all the time, or storing data on their hard drives, or storing data in the cloud, or whatever the case might be. Understanding that, and certainly the pandemic and forcing everybody remote only highlighted the need to have to move this direction even quicker.

Question

So I think everybody's familiar with the new employee comes on board, they get the training, or yearly, there's training. You mentioned campaigns. Could you give us an example of some typical campaigns you might've done, might do, on special topics during the year that you've done recently?

Answer

Yeah. A good example is actually with the recent ransomware situation. One of my favorite things to do—and it's usually brought about from a situation like the Colonial Pipeline ransomware attack or the JBS, some of the critical infrastructure type attacks that we've seen—is to begin to package content around that and to roll that out companywide. So it could be something that I just... I usually end up going to SANS first and foremost, and saying, "Do you have any content that we can package around this topic?" And then I do some open source intelligence and some open source research to add on to that. And then it becomes about creating and packaging that content digitally, these days especially, even more important to do it digitally. But packaging that and putting it into a sort of sub-site through our SharePoint or GNET. That's something we can communicate internally. And then creating a special message to the organization and then communicating that message, running that message up and getting checks from people within information security to make sure we're hitting all the right points.

But, ultimately, guiding people to a source of information that includes all different types of training methods based on whether people are auditory, visual learners, combination learners. Do people like engaging training content? Just packaging a bunch of different type of content, that's videos, that's some podcasts even that address the subject, and finding a lot of that information, packaging it together to highlight the importance of doing whatever we need to do to mitigate the risk of that becoming an issue at Guidewire.

So certainly, the Colonial Pipeline issue recently with ransomware attacks on our critical infrastructure brought about a need to really hone in and focus on phishing email attacks that bring ransomware and could install malware on individual systems. I always look forward to October as cybersecurity awareness month. That allows me to do a specialized program like that each week in October, each full week. So, each week in October. There will be four packages of content exactly like I just described to you for the ransomware situation. I get to do that four times in the month of October around different topics. It could be insider threat, which also, by the way, has its own month that I learned recently, in September—insider threat awareness month. So using events that come out on the calendar like that. The cybersecurity community has really gotten together and decided that there are special times throughout the year that they want to highlight certain things, password security, data privacy. And then you can build content packaging around those things for those specific times and use the events as they come up on the calendar.

Question

You mentioned earlier, cloud security is becoming important. Is that a sort of “tell them the same things,” and it’s just now that the servers are in the cloud? Is it specific to Guidewire’s use of specific cloud-type applications and systems? Or how are you addressing cloud security on the awareness side?

Answer

We’re focusing on private use of a private cloud account versus their public use. So, they might have certain cloud accounts and Dropbox or such that they use within their private lives, and then not co-mingling those with work accounts and kind of what is shared back and forth. We’ve really locked down the ability for content to be shared internally in that way unless it’s an official, approved repository or mechanism, cloud security account. We have all sorts of data governance tools that we’re using now. And that’s really helping control some of the situation of potential for data loss prevention. So, preventing some of that data loss potential for insider threat is obviously always a big deal, and we want to make sure that we can clamp down on that. So, the use

of those private accounts versus as in, I guess, what would be their public private accounts—the ones they use in their personal time, those personal accounts versus the work accounts that they use through the cloud—and making sure that they really understand the importance of, if they store data, it goes into this account and not that account.

But also understanding the need for securing cloud accounts through configuration and such, putting the right security around a cloud account to make sure that if there were a compromise on their system, that at least if they had sensitive data stored in such a cloud account, whether it be work or personal, that it be locked down and locked off and you couldn’t get to that information. There’s a lot of focus around issues like that. And it’s become an increasingly more important topic the farther we go down this road where physical data centers are being used less and less, and everything is moving to the cloud.

Question

Okay. One last question on the awareness side, then few questions on the developer training side, and we’ll close out. So how many years have you been doing this in your position in charge of this?

Answer

Six years total.

Question

All right, you’ve got a lot of experience. If someone’s coming along and they’re you six years ago—they just got a job to take over an awareness program that’s probably doing things in the minimalist way or the old-fashioned way—what are some things you know now that you’d go back and tell yourself when you first started, some lessons learned you could pass on?

Answer

Yeah. I’d really say this is a job where people can and should wear a lot of hats. They likely need to wear a marketing hat, a public relations hat, a communications hat. Certainly, data privacy. And security. It helps to talk

regularly with the security operations team about threats to gain a good knowledge and understanding of the existing threat landscape. Human risk continues to be a big issue, like I've brought up several times here. You have to wear a lot of different hats, and learning how to most effectively communicate to the organization is critical in building trust. But what's great about this job is the creativity that you get to demonstrate in the role. And so if you're in a more conservative type of organization and it's at a compliance focus level when you come into it and you want to build from that, then all it'll take is you beginning to meet with peers who do this in other organizations to figure out, "Wow, there are some great advancements. There are some great things happening in this industry and space around mitigating human risk that are outside the box approaches and really advanced from the perspective of behavioral sciences, psychology, and the user experience. There are ways that people are gamifying their training experience to get more engagement from everybody."

There are things like we began doing at Guidewire, where we're focusing on a full, 12-month calendar of all of these events being scheduled, including bringing in CISO experts who work for the government, FBI experts who work in our law enforcement communities who understand and work in cyber. And they understand the cyber threats and giving a presentation twice a year, which is something we also do.

So I would say the things that I slowly grew into it. And it was when I began attending the SANS Summits that I began talking to my peers, and that opened the door to understanding all of these other things that can be done in a training program that are so far above just mere compliance. So the networking aspect will give you a thousand ideas you want to implement right away. And then it becomes really important to just plan and prioritize the few things that you can do each year to continue to advance your security awareness program to really move the needle and to really move from mere compliance to complete cultural change.

And then eventually with what we've been able to do at Guidewire, which is when you're really at a top level with this and you've been doing this a while, you're hopefully producing enough metrics that you let the metrics determine the training program, not the training

program to get the metrics. So getting to where you're producing so many metrics and you're able to use those metrics to then guide the direction of the program is huge. It doesn't happen overnight, though. It's incremental evolution. But a ton of that happens from just talking to peers and networking through this community. There's a lot of people in this space now, and six years ago, there weren't as many.

Question

Okay. Just a couple of quick questions on the developer training side. So the compliance pulls a little different there. I mean, Guidewire as a software company was... How did the developer, or the CIO side or the head of app dev, or somebody say, "I'm tired of this. All these bugs in our product cost us a lot of money. Let's do something." How did you get started on the developer training side?

Answer

It came about kind of the same reason and user came about, which is there's a security control in PCI DSS that says you'll train your people in OWASP Top 10 secure coding best practices. And so we began doing that very manually the first year before we found SANS. And then we began using the SANS program for developer training. That's been evolving to where it's become something where we want to get the developers a lot more engaged, and not just a knowledge transfer of understanding. These are the vulnerabilities in development that we don't want to fall prey to, and we can answer quiz questions on that, to actually putting that into practical use. Developers love games. They love things that are gamified of sorts, and there's a lot of gamers in that space.

...let the metrics determine the training program, not the training program to get the metrics. So getting to where you're producing so many metrics and you're able to use those metrics to then guide the direction of the program is huge.

So all of a sudden, we can actually use their practical knowledge of developing in a product to apply that to finding flawed lines of code. And so it's a product that is really awesome right now the way SANS is developing that out to become such a practical use for developers like ours. But it's going to even continue to get better, and it allows us to actually grow the program like the end-user program we've just grown into more of a 12-month. We're going to find ways to engage developers even outside of typical training windows. But obviously the need comes about there from maybe a compliance standard at first, or maybe if you're in our case as well, you realize, "Hey, we've got a very robust risk management framework and risk management program. And we want to make sure that we're not seeing risk be logged in our risk management program that associates with OWASP Top 10 secure coding issues.

And so you realize, "Okay, let's actually find a way to track that and then minimize the risk associated with the OWASP Top 10 so that our developers aren't falling into those traps during development of the product." And certainly, that can eliminate bugs. It can really mitigate the risk of security bugs being an inside gateway to our more sensitive information and even our entire network should a product be created, should a platform that our developers are creating be created in such a way that it includes one of those OWASP Top 10 secure coding issues. Then it creates a backdoor into our entire network and front end and architectural framework, and then becomes a much bigger problem. So being able to tell leadership that we have a solid year-round program for developer training to help mitigate and prevent those types of risks from surfacing is a big deal. And that gives you a lot of credibility in the way of leadership.

Question

So have you been able to show those type of metrics that there's a decline in security bugs per thousand source lines of code or at least the OWASP side as time's gone by as you've been doing this training?

Answer

Yeah. You can actually begin showing how there are far fewer risks being logged. There are much, much fewer. In fact, so few that they don't really register as high

issues. But you can begin by cataloging and staying in tune with what the risk management program is producing in the way of risk. You can really begin seeing how that falls off the more you begin to engage developers with those issues.

And there's a trust relationship there between developers and the security team that's very, very important in the process of all of this. And they know the difference when you're just pushing them training that's for compliance versus you actually want them to gain practical use, practical knowledge from what you're giving them in the way of training. So it's an important relationship that the security team has with the developers right there.

...being able to tell leadership that we have a solid year-round program for developer training to help mitigate and prevent those types of risks from surfacing is a big deal. And that gives you a lot of credibility in the way of leadership.

Question

Okay. Final question. Standard one I always ask. Obviously it's a rapidly changing area. Quite often you need a lot of support from the vendor to update the product or do things, get improvements in. What support do you use from SANS, and then have you rated it on the support?

Answer

Yeah, I do. I use the customer service wing. I have a person who is dedicated to supplying us and touching base with us regularly. At least it's been monthly for as long as I've used SANS, but even lately, it's been even more frequently because the needs have increased. So SANS has a whole customer support team that when folks like me who run a program like this and they use SANS' suite of solutions, and we use the video modules and we use all of that. And any content that I feel like there is a gap in, I can easily go to the person who handles customer service for us, our customer rep, and that person is always really quick to find out how they can fill the need and meet that demand from us.

Sometimes it's something that comes about in an internal meeting that I'm having with my team, and I realize we really need to get some content around whatever issue may be out there. And then I have to pop on and shoot an email across that day. And a lot of times I get it within the day. So it's a very important relationship. In fact, I vocalized this more recently. It's probably the greatest value that I get of anything SANS provides us, that partnership and relationship. It's become a pure win-win from our standpoint, and also with SANS because SANS always does a good job making sure they understand the customers, which is us on this end, that we have feedback to provide. And the door can either be shut for that feedback and then it prevents growth, or you can be welcome with that feedback. And then there's a lot of growth potential out of that.

And so SANS has always welcomed the feedback from folks like me along the lines of the products and just the whole presentation of the training modules even, improving the training modules, making the presentation of the training more engaging. Always been extremely open and welcome with the feedback that I've had to provide for that. And so it's been a really, really great relationship from that standpoint. That's the value the SANS brand brings, in my opinion.

Question

Okay. Just before we close out, anything I didn't ask that you'd like to bring up before we close?

Answer

I don't think so. I think that hits all the nice bells and whistles. There's certainly a lot. The more we do this, the more layers of the program we add on. But those are the core elements right there. End-user security training, developer training, phishing simulations. And since supplementing that and really being able to identify where a culture in an organization needs to change—by using the assessments, using the behavioral risk assessment, using a cultural assessment—that SANS has to identify what behavior is riskier at, at a place like Guidewire and using an assessment to gain that information. So I'm a big believer in the assessments helping to add intelligence that'll be able to help us grow our program.

SANS Security Awareness

SANS Security Awareness provides organizations with a complete and comprehensive security awareness solution, enabling them to easily and effectively manage their human cybersecurity risk. SANS Security Awareness has worked with over 1,300 organizations and trained over 6.5 million people around the world. The SANS Security Awareness program offers globally relevant, expert authored tools and training to enable individuals to shield their organization from attacks and a fleet of savvy guides and resources to work with you every step of the way. To learn more, visit www.sans.org/security-awareness-training

About SANS WhatWorks

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned.