SANS

WHAT WORKS™

What Works in Supply Chain and Partner Security: Using BitSight to Assess and Monitor Third-Party Cybersecurity

SPONSORED BY

BITSIGHT

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. Got a story of your own? A product you'd like to know about? Let us know.

www.sans.org/whatworks

SUMMARY

Many recent breaches have exploited security weaknesses in third party vendors and suppliers to attack business and government agencies. During this SANS What Works webinar, the CISO at Fannie Mae will detail his experience using BitSight's service to assess the cybersecurity level of third party business partners and vendors, as well as using BitSight for ongoing monitoring of externally visible signs of lapses in security levels.

ABOUT FANNIE MAE

As the leading source of residential mortgage credit in the U.S. secondary market, Fannie Mae is supporting today's economic recovery and helping to build a sustainable housing finance system. They exist to provide reliable, large-scale access to affordable mortgage credit in all communities across the country at all times so people can buy, refinance, or rent homes. Fannie Mae is working to establish and implement industry standards, develop better tools to price and manage credit risk, build new infrastructure to ensure a liquid and efficient market, and facilitate the collection and reporting of data for accurate financial reporting and improved risk management.

ABOUT THE USER

Christopher Porter, Deputy CISO, Fannie Mae.
In this role, Mr. Porter helps to communicate the importance of information security across the enterprise and to mature and innovate Fannie Mae's defense and response capabilities. Mr. Porter has over 15 years of experience in IT and security industries. His background includes work as an economist, network and system administration, information security consultant and researcher. In his previous role at Verizon, Mr. Porter was a lead analyst and author of Verizon's Data Breach Investigations Report series. He was also the co-creator of the VERIS Framework (Vocabulary for Event Recording and Incident Sharing) which allows organizations to collect and report security incident metrics in a standard and repeatable manner. Mr. Porter has a bachelor's degree in Economics and Psychology from the University of Virginia. He also earned his master's degree in Management of Information Technology from the University of Virginia's McIntire School of Commerce. He is a member of the McIntire School of Commerce M.S. in MIT Advisory Board at the University of Virginia.

ABOUT THE INTERVIEWER

John Pescatore, SANS Director of Emerging Security Trends
Mr. Pescatore joined SANS in January 2013 with 35 years' experience in computer, network and information security. He was Gartner's lead security analyst for 13 years, working with global 5,000 corporations and major technology and service providers. Prior to joining Gartner Inc. in 1999, Mr. Pescatore was Senior Consultant for Entrust Technologies and Trusted Information Systems, where he started, grew and managed security consulting groups focusing on firewalls, network security, encryption and Public Key Infrastructures. Prior to that, Mr. Pescatore spent 11 years with GTE developing secure computing and telecommunications systems. Mr. Pescatore began his career at the National Security Agency, where he designed secure voice systems, and the United States Secret Service, where he developed secure communications and surveillance systems. He holds a Bachelor's degree in Electrical Engineering from the University of Connecticut and is an NSA-Certified Cryptologic Engineer. He is an Extra class amateur radio operator – callsign K3TN.

Q Can you tell us a little bit about yourself and your role at Fannie Mae?

A My name is Christopher Porter. I am the Deputy Chief Information Security Officer at Fannie Mae. I am responsible for cyber incident management, which is focused on communication and coordination of incidences across the organization. I'm also responsible for the third party due diligence process for our vendors as well as any general Fannie Mae third party business for which I've been focused on developing a new vision. I was previously at Verizon working on the Verizon Data Breach Report.

Q As it relates to third party security side of things, were there issues or problems why Fannie Mae wanted to change the way it had been doing third party security?

A I think it was less about Fannie Mae wanting to change it as it was me wanting to change it when I came over, since I had experience doing assessments. Prior to my work on the Verizon Data Breach Report, I did security consulting which involved going onsite to perform third party assessments; going through checklists, making sure there are locks on the doors, walking into the data center and making sure that it's cold and things of that nature. I realized when you're doing these types of assessments, you're not actually determining whether you're reducing or increasing risk by doing business with this third party. There are some very general compliance-type issues that you're inquiring about, but it doesn't get at the heart of what I'm primarily concerned about which is whether or not the vendor that you're doing business with or the third party that you have a relationship with has a security program in place. Do they have the capabilities in place today and the governance in place to maintain that program over time? That is one of the reasons that I've changed our program to where it's not just a checkbox mentality of going through questions, but also, a more mature model of each of these questions, adding some continuous monitoring pieces. There's an inside and outside approach for evaluating our third parties. The inside-out is talking about the traditional way of doing things, then doing a little bit more with the maturity model. The other piece is the outside-in approach: How can I look at an organization and understand, based on the information that's out there, if this organization is practicing good security. BitSight does a good job of evaluating that based on the information they have accessible to them. I like the model they have in place where they're evaluating companies both on events or compromises as well as some of the due diligence information on some of the practices that these organizations have in place.

Q When you decided you wanted to add this sort of continuous external assessment piece, what sort of alternatives did you look at, and what sort of evaluation criteria did you have?

A The whole idea of a credit score or scoring an organization based on external information is fairly new. This is a cutting edge space. I always thought that you could tell a lot about an organization by various cyber intelligence feeds, for instance. So, what happens when there's a compromise? Usually, the bad guys are compromising some sort of other infrastructure using that as a hot point and then using that to attack their intended victim. So, by virtue of that hot point, that means that there's another victim out there, whether it's a home user or some other type of organization, something has gotten compromised that the attackers are then using to launch further attacks against their intended victim. I've always thought "that gives me some good information potentially about this middle organization - maybe they don't have a very good view into their security posture." We had to make up what the evaluation criteria was for this kind of approach. One of the things that I think is most important from evaluation criteria is the management team. I had a very good relationship with the BitSight organization and the management team that they had in place. I had some familiarity with them because I had worked with them previously. They were a partner with the Verizon Data Breach Report, so that was certainly a component. Veracity of information is also important and having the confidence that the information that is being utilized to create these scores is accurate. The last thing you want to do is use a evaluation criteria on a company and get a security score and then go to this company and say, "hey, I saw today that your score dropped by 50 points, why did that happen?" only to find out that the reason it happened was this information wasn't valid, it wasn't accurate. I was very confident that BitSight had the processes in place to validate the information in their system that they were then creating these security scores for. And lastly, I like the methodology and how BitSight, in particular, is utilizing their criteria and the algorithm that they're using for scoring. What they've got is two separate pieces: There's the event risk vectors and the diligence-based risk vectors. The diligence--or the event based ones are really looking at that kind of open sourced and closed sourced information and identifying whether or not there's been some sort of infection or compromise within that particular organization's infrastructure. I believe that the kinds of incidents you have are really a reflection of your security program. And so, this is a much greater component of their score. Also, with BitSight, I think their acquisition in the last

I was very confident that BitSight had the processes in place to validate the information in their system that they were then creating these security scores for.

year of Anubis Networks was also one of the defining factors for us in selecting this technology because they have that very tightly coupled threat intelligence component with sinkhole information that allowed us to be confident in the information they had. The second factor I mentioned was diligence risk vectors. So, these are looking at very specific practices that are either implemented or not implemented in place: Do you have DMARC set up? Do you practice good methodologies with your SSL and TLS certificates? Do you have DNSSEC in place? What sort of open ports are up and available, and also some various application security. What is utilized to create a score? We were very confident in BitSight's ability to deliver accurate information to us and have that accuracy over time.

Q Let's talk about how you got started and how this works. So, you select BitSight. Fannie Mae obviously had some existing set of vendors and third party partners. You now had access to these risk ratings from BitSight. What did you do from there?

A We're still rolling this out across the organization, but this is essentially what happens. You put your vendors in a list and send it over to BitSight, and they begin populating your portfolio of vendors or third parties that you're doing business with. So, what does that mean? It means that I can log into the BitSight portal and I can see a list of all of the third parties as part of our portfolio. I can click on each of these vendors and see their security scores and whether or not they're basic, intermediate or advanced with their score. All of that information is available for each of these vendors. The only thing you don't see is some very specific information on events where the IP addresses of your vendor are masked. BitSight makes sure that sensitive forensics information related to a vendor is maintained only for the vendor's visibility. Therefore, BitSight provides customers with the ability to give vendors fourteen days of free access to the platform, allowing vendors to remediate their own major network security issues. One of the things that we're doing—and this is very customized to our organization—is we're taking all of the vendors and we're sorting them and bucketing them in something called folders, which is a feature of their tool, but it's done by the VPs within our organization. Ultimately, what I'm trying to do is give some awareness to our executive management around the risk of each of the vendors/third parties that they are doing business with. I want them to understand whom has good security and whom has improvements to make. That gives them better visibility into their vendor management program.

We were very confident in BitSight's ability to deliver accurate information to us and have that accuracy over time.

Q So, if a score changes dramatically, let's say gets worse for a vendor, something changed. How is that handled, and how does that information flow?

A One of the nicest features around the tool set is, each week, BitSight sends an email that shows when your vendor's score deviates by 5 percent, whether it's positive or negative. If I have a vendor that may have had some sort of compromise or some type of incident – malware is showing up in a cyber intelligence threat feed list – then their score may drop. Every Monday, I get an email that states which vendors' scores have dropped or have gone up by X percentage. At that point, we can begin our process of trying to identify what the specific issue was that caused the score to go down. Once we've identified what that is, we can then reach out to the third party and let them know that there may have been a potential incident, and give them some information, see if they need any help and start a conversation. What I want to be able to do with our vendors is have that security conversation, making sure that they know that they're part of our ecosystem and we can help them along in whatever way we can.

Q Do those VPs of the business units you mentioned get this email directly, or do you forward it to them at some point to let them know there's something they may need to be aware of? How does that work?

A We plan to report that information on a quarterly basis when we do our regular briefings for each of the different executives. The BitSight scores and the third party scores are a component of that slate of metrics.

Q How long have you been up and running?

A Since July, 2015.

Q Will you be including this type of scoring in the evaluation process when you are evaluating third party vendors using RFPs in the future?

A We're looking into that today. We haven't gotten that far into our implementation yet. But, ultimately, the goal we want to put in place is to have this be a component of our procurement system where they can reach out via API (potentially), grab the score of that particular vendor and pull it back in – and that be a field that is available as part of the decision support tree of vendor selection.

Q **You mentioned accuracy was a very important evaluation of criteria. It does seem like it would be a negative thing if there were false positives or false negatives constantly feeding in. What's your experience been so far?**

A We haven't seen many false positives, but I think what happens is service providers typically have lower scores because of the breadth of information that they have. I don't want to use specific vendors here or third parties. But a cloud security provider has an enormous amount of IP address space that they own, but each of those little places are divided into the organizations that they're selling to. So, what I've found so far is that service providers typically have lower scores because it's part of an overall component of their organization, even though they may not have responsibility for the cleanliness or the hygiene of their specific vendors. At the same time, I think that is important to understand. If you're working with a particular service provider and they have a pretty low score, maybe it's because they don't have a good abuse process in place, or maybe the SLAs or the contractual requirements that they have with the organizations that they're doing business with aren't strong enough or not practicing good security. You can have the most secure customer, but if they happen to be using infrastructure that's owned by a service provider, some of their scores are a little bit off in some ways.

Q **You worked outside the financial industry, and you're now in the financial industry. The ratings you get from BitSight and the internal acceptance of that sort of methodology, do you think it was easier because you're in financial and they're used to credit ratings, since they are a very similar methodology? Or do you think it can translate easily into other verticals, as well?**

A It was easier since the financial industry, in general, does understand this information a little better. However, I believe everyone understands credit scores. So, I don't think that the financial services industry is at an advantage in understanding this technology. I do think other industries can adopt this type of technology and data as well, and it shouldn't be difficult to sell to those within their organization.

Q **Can you give us an idea of the scale you're doing? Is it with a dozen vendors, 100, 1,000?**

A Right now, we've got around 400 to 500 specific vendors. We'll be ramping up to around 1,000 to 2,000 by the end of 2015 to mid-2016.

Q **Who are the primary users? You mentioned you get the email. Are you the primary user? Are there more people that see the information, use the information or directly interact with the service?**

A Right now, the primary users are the third party due diligence team that's underneath me. This is a team that is doing the actual inside-out and outside-in approach for assessing our third parties. In addition, we're working with other organizations within Fannie Mae to present this information to them, as we're doing new assessments coming on board and then reassessing third parties that we've already had relationships with.

Q **Was there a need for an additional FTE on the third party due diligence team to manage BitSight? Or is this now just an additional tool they use?**

A No need to hire additional FTE for this specifically. This is a new tool that we're incorporating into our program as we're changing it to this new approach.

We want to have a better continuous monitoring of our third parties in place. Before BitSight, we didn't have that.

Q **As you wanted to change the approach, you obviously had to justify going out to procure a tool or a service like BitSight. How did you convince management to fund it?**

A Any time you're trying to purchase new technology or some sort of business initiative, you have to identify what the business value to the organization is for that – not just security ROI. We need to show how are we protecting Fannie Mae better, how are we getting more information to our decision makers within the organization, and how can we use this information over time to make sure that we're protecting Fannie Mae not just today but going forward. We want to have better continuous monitoring of our third parties in place. Before BitSight, we didn't have that. We want to have that visibility into our third parties over a period of time. Are they showing that their security programs are still in place, because ultimately, if we're seeing events via BitSight and showing a score drop, we also should see remediation because that information will then disappear off the list and their score will go back up. I think what's important for us is we're not just doing that point in time assessment of a security program, but we're checking it over time, and therefore, we have more confidence that we're reducing risk over time.

Q Now that you've been going for a few months, are there any lessons learned or anything you know that you would have done differently?

A Not yet. One component that is also interesting that I'll mention is that you can evaluate your own organization with this as well. This wasn't something that we discussed early on. Looking at my own score, I can learn a lot about my own organization. A component of this is that it's almost doing a bit of a digital footprint of your organization, since BitSight, because of their information, is immediately populating all these network ranges that they see to be associated with your organization in some way. Therefore, we're now able to take that information and check with our network engineering team to see if there is anything on this list that we're not aware of. Having that ability to look at your own score is important. We've been able to track our own information over time and see improvement as we begin implementing some of the diligence practices and seeing the scores go up. To me, that's a good return, because now I can say, "hey, by the way, we implemented such-and-such practice this week, and our score went up 30, 40 points based on this one change that we did." I think it's important for our organizations to be able to show that third party perspective – this is a third party from the outside that's making this evaluation of your company.

We've been able to track our own information over time and see improvement as we begin implementing some of the diligence practices and seeing the scores go up.

Q Are there any things you've asked BitSight to add or features/requirements you'd like to see?

A There was one item that I requested that was delivered which was the ability to bucket each vendor or third party into specific groupings that I can then evaluate. The next piece that we've talked with them about adding is graphics on the portal that allow us to visualize the data for more descriptive statistics information.

Q How do you rate BitSight's support so far?

A So far, it's been great. They've been very responsive. Within, a day, I usually have a response back on the information that I'm submitting.

BOTTOM LINE

Assessing and monitoring the security of third party vendors and business partners has become even more important as threat actors focus on those connections. The Deputy CISO at Fannie Mae found that using BitSight's service enabled him to add an "outside in" cyber-risk rating capability to the usual compliance-oriented "inside out" self-assessments in use.