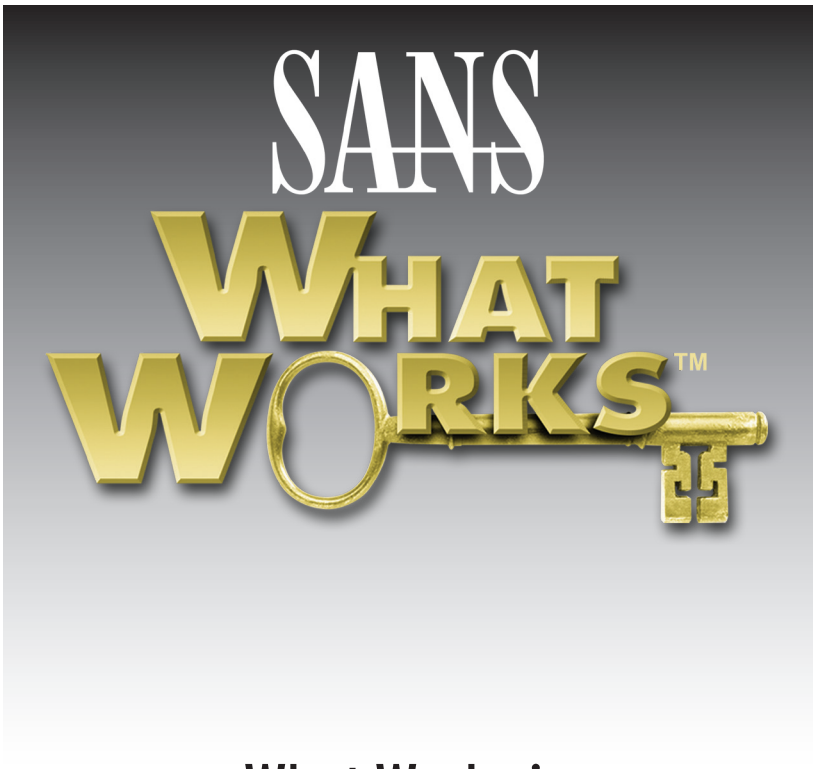

What Works in Third-Party Risk Assessment: Using BitSight for Continuous Monitoring

SPONSORED BY

BITSIGHT®
The Standard in SECURITY RATINGS

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

ABOUT KPMG

KPMG is one of the world's leading professional services firms and the fastest growing Big Four accounting firm in the United States.

ABOUT THE USER

Armando Rodriguez is an Information Security Practitioner who manages the third party risk assessment for KPMG. He has held positions at both ADP and Citi, and received his MIS from Stevens Institute of Technology.

ABOUT THE INTERVIEWER

John Pescatore, Director of Emerging Security Trends, SANS Institute

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 5000 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 a NSA Certified Cryptologic Engineer. He is an Extra class amateur radio operator, callsign K3TN.

SUMMARY

The Third-Party Risk Assessment Program Manager at KPMG US uses BitSight Security Ratings as a key input in assuring that KPMG's third-party suppliers and partners that will handle sensitive information are secure enough to keep that information protected. BitSight Security Ratings are monitored against thresholds that trigger potential investigation or re-certification of suppliers. The use of the BitSight services increases the depth of KPMG's risk assessment and decreases the time spent approving and recertifying key suppliers.

Q I Tell us a little bit about your background and your role at KPMG.

A I've been at KPMG for about eleven months. I was previously with ADP, and prior to that, I was with Citi for 17 years. My role at KPMG is to manage the third-party risk assessment process, to make sure that vendors meet the security requirements of KPMG in protecting sensitive and confidential information that they have access to. I report to the Associate Director of IT Risk Assessment.

Q What type of problems drove you to look at products and services like BitSight offers?

A The risk assessment process can become a "check the box" type exercise as questionnaires are used to assess the security posture of third parties. The questionnaires may be effective if aligned to well-known frameworks. For instance, ours is aligned to ISO 27001. But, as the environment changes, we decided that we needed to find new approaches to manage risk and have additional insight as to how our vendors are really protecting our data. BitSight was one of several vendors out there that provide services that allow you to better gauge - or take the temperature - of the security posture of the vendors that have your data, so you have assurance that the data's being protected.

We were focusing on who offered the most value, and we found BitSight specifically focused on information security. BitSight fits the mold because that's their expertise and their area of focus.

Q You mentioned data a number of times. How widely are you using this? Is it just for third parties that are handling KPMG or client data, or does it extend to all suppliers?

A Our focus is only on any vendor that has access to KPMG confidential information or client information. There are different levels of criticality, and we classify our vendors by tier: tier one, two, and three – with tier three being the most critical. Those are the ones that we want to touch, not those that offer services that do not access KPMG information. For instance, Cisco or HP or Dell; we buy gear from them, but they do not have access to KPMG data. Therefore, they don't come under our process.

Q How does this work if, say, there's a partner or another group or project that wants to use a certain service that would be handling this type of confidential data? Do they come to you, or is the BitSight output widely available? How are you using it?

A The way it works is that the businesses that want to engage a third party or a vendor must come through procurement. If there's confidential data being accessed, then they get moved over to our assessment process. Once that's done, we do an initial security review, which is an in-depth review to make sure that they have policies, procedures and controls to manage the information. After that process, in subsequent years, there's revalidations or recertification. My area deals specifically with revalidations, meaning we do the recertifications of vendors at different periods of time, specifically if it's a critical vendor annually or biannually or every three years.

Currently we only manage vendors that are the highest criticality with BitSight. We are looking to expand it to our tier two vendors, which are the next range. As part of the revalidation process, we look at BitSight to get additional risk information and see things that we may not be aware of that provide additional insight. We can then bring this information to the vendor and make them aware of these additional risks that are in their environment that not only impact us but also them if there was a breach or some incident because of those vulnerabilities. In many cases, we provide vendor access to BitSight so that they themselves can see their rating, and get further insight into their own vulnerabilities and infections.

Q So, as part of the recertification effort, you're using the information that comes back from BitSight. Do you use the ratings at all? Do you have some sort of threshold for the BitSight rating?

A We do. We have taken BitSight's recommendation. So, anything over 740 is considered healthy, if you will, in terms of security. Anything 400 and below is suspect. So, we need to dig in a little deeper.

Q You mentioned you're using BitSight currently for your tier three endors. Roughly, how many is that?

A We have about 54 of these vendors that are the most critical. Those are the ones that we monitor continuously. We look at the reports. We have it set up to get alerts so that I see things changing. There's been one case where there's been a data breach at a vendor reported where the rating dropped drastically, and when we looked at BitSight it had details on the data breach. So, we used that report and that information because it provides factual and actionable information that we can use. Then we invite the vendor to also log onto the platform and see it for themselves and also engage BitSight to help them understand what's going on. We can offload that to BitSight to kind of collaborate and help us do a deep dive with the vendor. That's a plus.

Q Who gets those alerts? Those come to you, and then you notify the particular business areas within KPMG?

A Yes, there's a few alerts set up and used, and we notify the business owners for those vendors that trigger alerts, because they need to be aware of what's going on. If there's a drastic change, we ask the business to submit the BitSight report to the vendor. The reason we do that is because, having the business owner go to the vendor has more weight than me going directly to them, since they won't necessarily know who I am. We engage the vendor through the business as the relationship owner for more effectiveness.

Q You mentioned, there are competitors to BitSight. Did you do a competitive analysis and chose BitSight over another? How did you select BitSight?

A We did because we were focusing on who offered the most value, and we found BitSight specifically focused on information security. Others had other things that we didn't really care for. There was another vendor who had things like bankruptcies and legal aspects that we're not concerned with. We have procurement doing those types of things, so, we want to focus purely on information security risk. BitSight fits the mold because that's their expertise and their area of focus.

BitSight is easy to use and has actionable information that allows us to proactively manage our vendors and is recognized as a source of vendor risk management.

Q Obviously, every product and services cost money. How did you convince management to get funding to add this capability?

A BitSight provides insight that we didn't have. So, there was a business case for having an additional tool in your tool kit to manage and monitor with vendor risk. BitSight is easy to use and has actionable information that allows us to proactively manage our vendors and is recognized as a source of vendor risk management.

Q It sounds like your management was already on-board with the idea of using some type of risk rating service.

A Yes, management decided they wanted to engage an external source for threat intelligence and when I got involved, BitSight was one of the finalists after a POC (proof of concept) was performed. BitSight had good features, an intuitive user interface, and offered a good price range. One other selling point was that we could start small with the idea that we would increase the licenses in the future once we learned the tool.

Q I've talked to others who use BitSight for some of their other services. One thing a lot of people seem to do is they also look at their own rating and present this to their own CISO and executives. Are you doing this?

A Yes, we are doing that. In fact, our CISO is very concerned that our rating is not as high as it should be. There were IP addresses attributed to KPMG U.S. that don't belong to us, they belong to KPMG international member firms that are being associated to our rating. What we did initially, as a result, is we isolated KPMG U.S. and removed anything that we could tell was not ours. For instance, there was a bunch of Canadian IP addresses for KPMG Canada. We were able to isolate and remove those IP addresses, but there are some others from KPMG international member firms that required more work. We have communicated this to BitSight, and they are helping us put together a report that lays out where the IP addresses belong and how some of them are registered. But, the main point is that we, too, care about others looking at our rating and seeing if it is low. There is concern at the CISO level that we have our house in order and have a rating that reflects the environment correctly.

Q One last question about your usage of BitSight. You mentioned that for a brand-new vendor or a third party, you have a formal on-boarding process, and then BitSight also comes into play in the recertification. Is that all you're doing for recertification - using BitSight - or are there still other things other than the BitSight information and ratings used for recertification?

A Depending on the criticality, regardless of the tier, in addition to BitSight, we also require that they complete our questionnaire, provide information security policies, evidence and pen test reports performed by third-party independent testers. So, these are additional things we require aside from BitSight.

Q How long have you been using BitSight?

A I've been using it for about six to nine months.

Q So, based on what you know, are there things you know now that that would cause you to do anything differently when you started using it?

A Yes, absolutely. In fact, this morning, I had a monthly meeting with BitSight to review how we are using it and learn from them what some of their other customers are doing that we can also leverage. That is a work in progress but using the

actual BitSight rating, gives me a better idea quickly as to whether there is risk or not that I need to be aware of and dig in and investigate.

Q You said you have a monthly meeting with them. Is that part of standard support or are you paying for extra support from BitSight?

A No, it's not extra and it's part of the agreement. BitSight provides several levels of support. If we need additional information on a particular aspect of a vendor rating, we have access to support. The same goes for vendors – BitSight is available to our vendors that may need to better understand their rating and its detail. However, a monthly meeting is in place for us to collaborate and improve the process and service. BitSight offers ideas as well as seeks our ideas to improve the partnership.

BitSight offers ideas as well as seeks our ideas to improve the partnership.

Q Just so I understand the scope. This is for KPMG U.S.?

A Yes, only U.S. Our licenses are KPMG U.S. only, and the reason is because each KPMG member firm is independent. We don't share anything with KPMG UK or KPMG Canada. KPMG International is made up of several member firms. We really don't talk to them. If KPMG International wanted to use BitSight, we can't share anything with them since our agreement is limited to the U.S. firm.

The beauty of BitSight is that it not only detects some of the threats that are out there, but it also has specific actions for remediation...

Q Since you're the primary user, for other people considering using BitSight, what sort of expertise would a person need to be able to use BitSight? Is it security expertise, financial expertise or procurement expertise? What do you think a good background and a good set of skills is for somebody to make use of BitSight?

A Definitely information security--an information security background is needed, because you need to be able to understand what the vulnerabilities are, what they mean. The beauty of BitSight is that it not only detects some of the threats that are out there, but it also has specific actions for remediation and specific things that can be done to remediate a vulnerability or something that is going on in the environment. This type of information makes it easier for me to be able to go to the vendors and say, "Look, I see this." And if the vendor is not convinced, there's actual factual information that can be made available that they can then take action on.

Q How do you primarily use it? Do you go to a website and view things, or do you get alerts via e-mail or other ways?

A We use it primarily as a part of the risk assessment process. We look at it to see what's out there. What additional information we need to bring to the vendor - that's one way. The other one is through the alerts. When I get the alerts, I look and see what's going on. Again, if it's severe enough, then we need to kind of dig deeper and communicate with the business and the vendor because it may be a security incident. I know that vendors are coming through the pipeline. I also encourage the security managers that are involved to use BitSight.

Q Anything you'd like to mention that I didn't bring up?

A I think the relationship with BitSight is good in the sense that they are very open to hearing our ideas and concerns and addressing them.

Bottom Line:

Assessing and monitoring the security of third-party vendors and business partners has become even more important as threat actors focus on and exploit those connections. The Third-Party Risk Assessment Program Manager at KPMG found that using BitSight Security Ratings enabled him to continuously monitor the security posture of critical vendors, and facilitate more effective collaboration on risk reduction based on BitSight's proposed remediation plans.