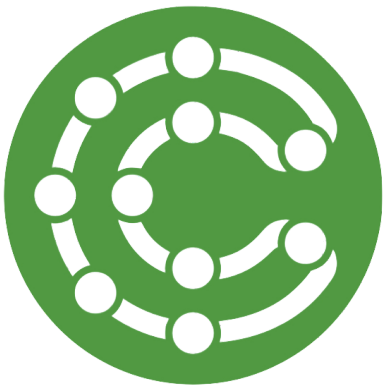

CISO TRACK

RSA 2020 Event

Session 3: Supply Chain Risk Management

Problem Domain SME: Alex Yamploskiy

(Sponsored by SecurityScorecard)

Date: February 25th, 2020
Staff: Iftach Ian Amit and Chris Nickerson
Transcribed and Prepared by: Scott Lyons, MS.

CISO TRACK

Executive Session Summary

Any third party with access to a company's data, network, systems, facilities, or other assets can potentially compromise that company's information security efforts, even if the nature of the relationship feels like they couldn't pose that much of a risk. To illustrate how "in 42% of cases when a data breach occurs, a data breach involved some type of an infiltration of a third party," Alex gave the example of an small air conditioning company, Fazio, which had a lapse in security that allowed hackers to penetrate Fazio and then jump to compromise the target. Using his personal experience as a Chief Information Security Officer (CISO), Alex gave another example where the company he was working for was,

> "When you are in hyper-growth mode like we were. We were doing hundreds and hundreds of millions of dollars in revenue when you sell luxury merchandise online, That attracts credit card fraud; people want to steal information from you. In terms of my own cyber security posture, I felt pretty good; I knew where the skeletons were buried,I had threat intelligence feeds, I had log aggregators, and I had a team that was doing pen testing, I was, at that time, PCI DSS compliant. I felt pretty good that I knew where the risks are, and that I was taking a methodical prioritized approach to mitigating those risks."

What Alex's team was doing internally wasn't the problem. But the Chief Financial Officer wanted to roll out an e-commerce fraud prevention system, which would involve sharing all of their company's customer data with the vendor, so Alex kicked off a rigorous due diligence process. He met with the vendor's representatives and they sounded very credible; they gave him a copy of a stellar report from one of the top penetration testing companies out there, and their responses and diagrams when he asked for information about their security architecture and the controls they had in place all looked great…

HOWEVER, when Alex's team started integrating that solution with their Quality Assurance environment, one of his guys was able to discover unencrypted credit card data belonging to other companies. Even though he employed proper due diligence practices before engaging with this third party, that vendor's lapse in security would have posed a major risk to his customers.

Process

For this reason, companies' risk management efforts should account for the security controls that are implemented by their vendors, suppliers, data recipients, business partners, consultants, subcontractors, and other affiliated third parties. But because you

really only have control over your company's internal practices, there are a lot of issues with third-party risk management efforts, and the overall process has "pain points" at every step:

Step 1: Inventory all third parties, including a business justification for the relationship and a "critical"/"non-critical" classification…

BUT you may have incomplete inventories, and there may not be clear justifications for specific third-party relationships;

Step 2: Conduct due diligence reviews to ensure third parties' security controls are sufficient…

BUT you may have outdated or inaccurate contact details for a particular third party, or your point of contact may be slow or unresponsive.

Step 3: Assess the risks to your company's information security posture based on gaps in those third parties' security controls and the risks you would inherit…

BUT you don't really know whether the information you received is accurate and up-to-date; it may have just been pulled from an external auditor's point-in-time assessment. AND your department might not have the authority to terminate a third-party relationship regardless of what you find.

Step 4: Assign remediation (or otherwise convince the third party to implement compensating controls) in order to mitigate the assessed risks…

BUT you may not have any mechanism to enforce this or verify follow-up actions.

Step 5: Implementing a continuous third-party monitoring solution to ensure third-party risk management is an ongoing effort and any risks can be identified and mitigated in a timely manner…

BUT you're likely already feeling overwhelmed just trying to catch up with point-in-time assessments, and it may feel like a pointless Sisyphean task already.

Solutions

Some people have found really interesting solutions. One of the participants at this event described how a CISO they spoke to would leverage gaps found in a vendor risk management questionnaire to negotiate a deal:

> "The CISO accepted that some of their vendors aren't going to have what he wants, So he doesn't send them a questionnaire. Instead, he says, 'These are the 10 kinds of things I want in place: yes or no (like MFA)? And if they come back and say, *We don't have MFA*, he's like, *Okay, here's what I want: You're going to give me X percent discount on the subscription for the next year and a half. I'm going to pay for your MFA, and I'm going to*

> *give you 10 hours of my engineers' time to implement MFA in your organization. And then, contractually, you're going to indemnify me - like, I'm not guaranteeing you don't get breached.* He's actually, up-leveling the security of his vendors and having them pay for it."

Roadmap and Risk Debt

Another participant talked about how business units will identify a product/service of interest based on what their competitors are using, not the vendor or their security posture, so his team involves the Procurement, Legal, and Compliance departments in the vendor due diligence and onboarding processes so that they can renegotiate the vendor's agreement to write in compensating controls as contractual obligations or, if there are too many issues to enforce mitigation efforts in that way, they will go back to the business units and ask them to find alternatives.

However, not every company is set up to incorporate information security requirements into the procurement process and third-party contracts. One problem that came up several times in discussion was that there often isn't sufficient support and buy-in from management to change third-party relationships when major cyber risks are identified. If the operational impact of a product/service is perceived to be more valuable than the potential risks the company will inherit by incorporating that third party into their data ecosystem, the security team's risk assessments might not actually change anything.

Vendor Behavior

The vendors themselves may use the questions that their customers ask in vendor management questionnaires to go to *their* management and say something like, "Look, these are the things that our clients care about; it might be worthwhile for us to expend the resources to implement these security controls." That proactive, customer-first security attitude might not be widespread though. One vendor expressed concerns about the number of vendor risk assessments she's asked to fill out every year, stating:

> "I'm a vendor, I answered 356 security questionnaires. And I will tell you it's - all metrics, it's bullshit; you don't get any view of my risk profile by sending me these questionnaires, because you want to know who's filling them out now? My interns. You want to know why? Because security people are freaking expensive and I need them working on security,
>
> So I've got interns who…just look at the prior questionnaires, and they mark, 'Yes, yes, yes,' all the way down, really fast, Then you want me to provide comments to 350 questions on your one questionnaire, and they're just, you know, copy-and-pasting from policies, right? You're not

> getting a risk profile when you're doing security questionnaires; they're shit. And, I gotta tell you, we're spending entirely too much time filling out questionnaires, and I'm spending [a] million dollars a year to have a compliance audit firm come in and test 600 controls. And I'm spending that money to give *you* assurances around our security program. That's my personal opinion on this matter. I would love to see these questionnaires go away because they're just a nightmare for us…
>
> We've created compliance packages. But what I find is the people that are handing these security questionnaires are just trying to check a box, right? There are very few companies that are actually diving into our answers and asking more questions - good questions - so I know it's not a security person reading my answers, right? So, I'll hand [them] the compliance package, and sometimes it works and sometimes it doesn't. Obviously it didn't work a lot because we did 350 of them last year, but we're getting to the point that I'm ready to say, 'No,' but the business, of course, you know, like, 'Oh, but we need to sell,' you know…
>
> So, we're getting ready to say, 'In order to do this…we're going to charge you…300, 500, $1,000 per questionnaire, depending on how long it is…
> Yeah, I mean I'll pay a college kid just to fill these things out. Like, it's all theatrics… there's nothing *real* about that, about my answers, and you're actually not digesting them well. Because, if you were, you would know that was all theatrics. Like, a good CISO reading that knows I didn't even answer that right, right? But you're…people are checking boxes."

Conclusions

How do companies address vendors? Their security, the various risk streams, and what the CISO's do not like about vendors.

If there was a way to get vendors to stop sending 300 question questionnaires, yeah… that would be great! Unfortunately most risk assessment questionnaires are filled out by interns and other people that are not in or directly tied to security. The CISO's in attendence felt that they had enough to worry about, without trying to fill out useless questionnaires.

Alex talked about risk, what you do about risk, vendors, etc. Almost immediately, when Alex completed his opening, the session was hijacked with "Stop sending me damn

questionnaires!" But, Alex pushed through with the will that he wanted to address 3 main things.

- How do we manage risk
- How do people manage risk on us [as CISO's].
- How many times do we fill out forms all day long versus hit a button and give the thumbs up or thumbs down.

How to provide accurate data to CISOs? Mainly, through questionnaires. Unfortunately, our tactics and methods are antiquated. Checkbox mentality is an old and useless mentality.

If someone can check a box, you're done!! Right?
Except any decent CISO can look at a filled-out questionnaire and tell if you're full of crud.

9 times out of 10, interns fill out questionnaires. People without the requisite security experience, or already done, premade questionnaires. They're not actually ANSWERING the questions.

So the real question of, "what do you measure for a scorecard" was proposed and where and how do you get REAL ANSWERS????

It feels that this ongoing issue is part of a bigger problem as a whole. However one way to tackle the answer to the issue, is to break up the main stalwart behind compliance. Policies, procedures, and control implementation, and grade accordingly. The bigger issue is, how do we as practitioners, delete the checkbox mentality from business in general. As in, get the auditors to stop looking for "just the checkbox" for example.

Takeaways

In the BsidesLV concept of CISOTrack, there was a sense of drift that was elucidated on, with regards to supply chain risk management (SCRM). In that session, tools were thrown around that are major players in the SCRM space and there was not enough time to complete the discussion. Therefore Alex Yamploskiy from SecurityScorecard was asked to come in to not only stoke the fire of discussion but to drive the interaction around defending the fortress from supply chain risks.

To be more specific, Alex was asked to address the following:

- Understanding of really where are those products going
- What problems, are they seeing that, you know, get solved for their clients
- How are we seeing those things materialize themselves in our day to day practice

This was intended to lend to the discussion of:

- How do we manage risk
- How do people manage risk on us [as CISO's].
- How many times do we fill out forms all day long versus hit a button and give the thumbs up or thumbs down.

The actual discussion focused on:

- Questionnaires and the reduction needed in that realm
- Vendor Behavior
- How to deal with Supply Chain Risk