CISO Track - BSidesLV 2019

Following are the anonymized proceedings of the CISO track that was held during BSides Las Vegas on Tuesday, August 6th, 2019.

Attendees: The track facilitated 48 (out of a maximum of 50) full-time CISO/CSO role holders from various industries. Participants represented Fortune 500 companies, as well as healthcare, startups, education and government organizations.The participants list has been redacted to allow for the proceedings to be published without attribution, and allow the discussion to be conducted in an open and honest manner.

Opening

The original goal of the BSides Las Vegas CISO event is to provide our participants with a closed-door environment where sharing information and practices around a select number of topics is done properly. This isn't about some vendor pitch, nor was it about sitting and having someone talk at you for 45 minutes. It was about a discussion between peers, curated by peers, around topics presented briefly by a vetted industry vendor. What's a vetted industry vendor? They're speakers who had agreed not to pitch or sell products, and their presentation has been reviewed and pre-approved by the program committee.

The day started out with a plain spoken message of not being a sales pitch in any way shape or form. The session was broken out into seven distinct sections. There were presentations given by vetted vendors who spoke on the subjects of Board Communications, Zero Trust, Supply Chain Security, AppSec/SDLC/DevSecOps and Crisis Communications & Brand Monitoring and the “unconference".

Board Communications

On the topic of board communications the conversation opened with a discussion on how we were trying to think about someone who could give a perspective from both sides. A lot of CISOs get burned after their second tour.

The first attendee to offer up a perspective opened with "I love security.” They talked about how for their first board presentation they were absolutely terrified. The problem being that they were not well prepared by their colleagues. The point of view offered was that, "a board is one big con game. Everyone tries to seem important to demonstrate their authority. Your boss will be at the meeting as they will be sweating bullets as the board is their bosses boss.”

"If you are reporting to the board that everything is good that's no help for anyone. If you are asking the board for resources is a failure of management not to provide that. If you are a CISO that reports to the CIO this will be a test of the relationship. CISO needs to report risk." This attendee requested $30 million and got it, but didn't realize that the money would come from other IT budgets.

It was proffered that if you present to the board and end up looking foolish you need an ally to help understand the message. An ally on the board to help sway other board members is extremely beneficial. The problem being that no one really cares about security in startup land. Start-ups are just trying to survive. The focal point of the board meetings in these instances is to help the company be successful.

There were hard lessons learned about boards. They like to see continuity. A lot of board members have come up through finance. This is their sense of knowledge. They will review previous board reports and seek out that continuity.

An issue that was broached was that when a board makes a statement such as, "So we've given you money, how have you moved the needle?" When you look at a CMM model it's easy to point at where we are on the scale initially. Then trying to demonstrate the incremental change is difficult.

Discussion then turned to the amount of time spent in preparation for board level meetings. One attendees said that their first presentation was much different from the second presentation to the board. Having someone with experience presenting to boards is key to preparing to help anticipate the questions. While another said that they had an aligned assurance council. Head of global risk, internal audit, corp sec, privacy to help have a unified message. Making sure that the message is aligned across the organization. The point that having interactions with legal can help a great deal with preparation. While they are most likely not technically savvy they do understand and appreciate risk. It's all about understanding the role of the board and making sure all of the stakeholders are aware and not caught off guard. Making sure that the CEO is clear on the messaging.

All of the preparation can be for naught in the case of a "news of the day" that overtakes day to day operational focus. The risk appetite can pivot quickly. It was pointed out that one should "Never waste a good crisis" but this is dependent on how open and honest you can be with your board. Put it into the larger context of the discussion and don't be reactive but, definitely speak to the issue.

A lot of these stories that were shared were ones that you can find commonalities with your own organization. A small deep dive as to how this will affect your own organization and understanding the lessons learned. It's sometimes easy to shift the blame. Sometimes it is necessary to take ownership without making other people look bad. The CISO is one of the most technical officers reporting to the board and there can be a tendency to talk down to board members as a result. The board members are there because they have an insight into how businesses are run. It is necessary to have humility when speaking to the board and be sympathetic to their perspectives. You don't want an adversarial relationship with the board as this will be self defeating.

When discussing risk it is important to understand the board's definition of risk as opposed to that of the CISO. Unquantifiable risks are the tough one. What risks are presented are not normally internal risks but, pointed to external risks. It goes back to the relationships and how we are aligning ourselves and teams with the board and putting ourselves as business leaders. Need to address risks as they pertain to the mission of the company. It's a game of trust.

A few additional questions that a CISO should ask themselves in this context were raised, such as: What is the board's interest in security. Why are they inviting you to speak to the board? What they want to see is that you are on top of things and know what you're doing? Measuring against something that is known. NIST, etc. What are the top five risks and what are you doing about it. Tracking those 5 risks over time from meeting to meeting.

The conversation then shifted to cyber insurance. It was pointed out that it is very difficult to get insurance to pay out on policies. A lot of policies have "act of war" exclusions. The framing of the discussion is key for discussing risk for the board. No longer based on finance, but on customer risk. Will the customer be negatively impacted? With the example of Sony one attendee posited, 'what if this happened to us?'. What was mentioned that was missing from the conversation was the downstream risk exposure. We are too focused on ourselves and not spending time on others.

Zero Trust

The next section started into the subject matter of Zero Trust. The premise was that the discussion was going to figure out what people like about zero trust and what they hate about it. The point being made that we are where we were with cloud 10 years ago.

It was positioned that with zero trust It sounds like you're going to make things harder for users. It's really hard to sell a restrictive policy. Classification is really hard. GDPR and other drivers are really helping to drive zero trust as an example. The perimeter is anywhere an access decision is being made. The opinions on zero trust were wide ranging. One perspective was that zero trust was all about risk appetite. Zero trust was seen by some as analogous to defense in depth in some measure. There is a need to make security as approachable as possible. Otherwise it's an impact to the business. One attendee stated that their users think zero trust is any device any time. How do we transition to a zero trust environment?

As an example, the hardest part in any red team engagement is getting the initial foothold. "I would almost see the perimeter as a vulnerability in of itself." It was suggested that this is a

political battle. How can you let me use my devices my way on the work network. It is a fundamental culture shift.
As to the question of how to get started with zero trust one person offered that setting the secure baseline is key. MFA everywhere and then have an incremental approach. Additionally, it has been recommended to complete foundational work first (e.g., know your assets).

The assumption should be made that everything is facing the Internet. An attendee offered they had gotten sales teams to never use VPN again. This was the idea that you can start with the use cases that you can accomplish. The approach being offered that one chops pieces off via threat modeling and then tackled them to get towards a zero trust frame.

So how does one initiate that culture shift? The rest of the world will not understand what is “zero trust” as this could introduce friction. It may often be perceived as a negative term. Unpacking and making it something that makes sense. An attendee shared that they use 'horse trading'. They would get their users to utilize something like MFA in exchange they would reduce complexity requirements for passwords. A novel approach. "The way we have gone about it is WIIFM (what’s in it for me) reduce requirements in other places. Give them something a little easier in exchange for other controls.”

The key point made that trust is neither binary or permanent. That zero trust as a concept has been abused. Even with zero trust you must trust something. We should talk about context based authentication since the network can be a data point used in the authentication policy to enable a better user experience.

The problem with adoption is that one attendee found that they had to roll back to single sign on and MFA as they found that not all of the technology partners are ready for this concept. Additionally to that basic concept, participants voiced that many of them had issues with storing device certs in Firefox, and ended up falling back to glorified SSO with MFA.

Supply Chain Security

The section on supply chain kicked off with a discussion of mapping suppliers, classifying relationships et cetera. When it comes to supply chain interaction they find out about it one way or the other. It has been a training process for people to understand the risks involved.

The question was asked, "How many of you are following up with vendors and are revisiting risk assessments?” It was pointed out that you have to treat your third party risk assessments like any other program. There needs to be a maturity that is often found to be lacking. It was put forward by another attendee that the contractual language would cover off security issues.

The question was posed that, regardless of the technology, how do you ensure that at answer a supplier provides is accurate? The response for many was that the right to audit needs to be baked into the contract. When dealing with vendors one attendee shared that it was important to front load design decisions at the beginning of the conversation. Security needs to be included from the outset of any project.

A problem that was highlighted was that scaling is a problem as it pertains to supply chain security. The issue being that most of this is handled via manual processes and that simply doesn't scale.

When dealing with potential security issues that may arise as a result of working with a supply chain vendor one of the attendees stated that if the vendor doesn't have a bug bounty they would pay for them to have one.

An attendee shared that they were audited multiple times per year. Only one audit produced a finding with anything of substance. Most auditors ask questions in a way that makes it a game. Are companies doing the right thing from a security perspective? For instance the question was posed as to how many supply chain companies were removed for failing security reviews. While the numbers were not large one person did share that they had removed roughly a dozen vendors as a result of security reviews.

So, who can accept the risk in the organization? If a risk is identified then a risk acceptance must be signed off on either via acceptance or to see it mitigated. How high in the organization does this go? For example one CISO has a process of signing an acceptance letter with the business owner which makes it a partnership. Further to this end another ties the conversation of risk acceptance to revenue discussions. We change from risk appetite to acceptable loss. An attendee offered that they think that for our profession to grow we need to not only be seen as risk managers. It's a trap to only look at risk. We're leaders of companies and we're also adding to the direction of an org.

Participants raised issues with dealing with 4th party risk (e.g., a subcontractor or service provider of a 3rd party). Aside from contractually requiring your 3rd party to manage the security risk for their downstream vendors, there is no practical solutions to the issue. The debate around the value of third party risk management vendors is still on. Some still saw value as one metric of many going into a larger formula, although the general sentiment was that it was not of value due to misalignment of incentives.

It was noted that the CEO has a very lonely job. Everyone has a bias that communicates with the CEO. AS a result the CEO can't trust anyone due to the aforementioned bias. You hear conflicting advice regarding risk. Are the decisions acceptable to the business? You cannot eliminate the risk, but you can manage it. We have things that are exposed due to the nature of our interconnects. Third party risk is what keeps most up at night. We are still trying to get to a place where data is secure.

AppSec/SDLC/DevSecOps

Right off the bat the question was posed, is there a non-linear way to discuss appsec? Then the term DevSecOps was brought up and the room broke into a round of chuckles. Has DevSecOps lost its meaning? One attendee answered with I never use the term DevSecOps. I use DevOps. “Dev should be doing ops”. There was some discussion as to how the term transitioned from DevOps to DevSecOps and the CISOs in the room arrived at the idea that there was probably an analyst at some firm that coined the term DevSecOps.

The problem as seen by the attendees was that the problem with this term is that it's a marketing term which ends up losing it’s value. Another attendee offered the following. We need to make it feel secure. An example is SDLC. We’re looking at a cultural shift. It was suggested that people should read the agile manifesto to really understand it. Security leaders have to be present and approachable. DevOps is hard like crypto. What is your application security risk model? We as security have to be part of the DevOps team. The universal agreement was that there is a need to stop using the DevSecOps term.

To build on this idea of security in DevOps it was positioned that a security champion should not fix the code. They should not be the ones to implement the fix. Another attendee offered that security leaders need to stop treating bugs as security issues. You want a consistent cadence. The sky is not always falling. You need to effectively align with deployment. Security champions are a way point.

At the point one person said, I want to walk out of this room with what people are doing in their environments. How they did it in their environments. The responses that followed were, one said they have appsec teams that are embedded with programmers. Dynamic and static analysis. They had not figured out scale. They were throwing people at the problem.

Another offered that their appsec team was not big. They seek to build controls (paved road) that eliminate entire classes of bugs. We want to get things automated. See which teams are opted into controls that mitigate risk. You can try to throw people at the issue you have to… We want to take problems away from developers. Was software security a thing 15 years ago? No. It was garbage. We can’t tie ourselves to what we think should be the case.

This caused one to ask, are you saying the ownership of security should be decentralized? They answered that they definitely recommend, but not enforce. We’re generally not going to give advice if it’s not easy to adopt. You can verify things programmatically. Building those things that help engineers move faster. Accelerating the development problem. Another weighed in, our biggest risk is competition. Do you really want your programmers worrying about security?

Crisis Communications & Brand Monitoring

What constitutes a crisis? Who is responsible for declaring who is in a crisis. You want to have a process in place with an understanding of who is going to be involved. How do we declare when a crisis is over? When does an issue become a crisis? It depends on what your risk model is. What is your tolerance? Decisions are made be legal.

An attendee added, We have a crisis management team to handle and declare incidents. Out business could fail if we don't comply with regulations. While another said, thorough investigation, controlling the freaking out, engaging legal, communication and external parties. We practice incident table tops.

Talk turns to managing the external communications. How do you tackle external social media such as people talking badly about a brand? The response, CISO will get calls for physical or social media because people think security is "magic". Another attendee said, we monitor breach announcements from other companies and proactively address if that issue affects us. What I have noticed is that our team knew about breaches before anyone asks us about it. It is important to get ahead of the narrative. We expect to have an awful day at some point. We have a data-breach toolkit. Not on network. You need to own the narrative or it will own you. Reputation of the company is a huge factor for preparing to deal with security leaders and press on a security breach issue. We underestimate the effect we can have on the security message. We don't give ourselves enough credit.

Lessons learned is important. If we were able to do a full RCA (Root Cause Analysis) we would hugely benefit the community if we can share with the wider audience. This brought the question, do you have more confidence in an external RCA on a breach or something provided by the affected the brand?

How do you handle external security researchers? An attendee said they were working with a researcher who was working with a press person who was looking to make a name for themselves. How can we set a message as to what is acceptable behavior? Maybe as a group comment on these issues as opposed to voicing as individuals.

Responsible disclosure is a two way street.