CIO: BUILDING A CYBERSECURITY CULTURE

At this 11.15.22 Roundtable 55, *NOREX Members discussed current pain points around cybersecurity; layering cybersecurity education; partners used for immutable backups; offering cybersecurity education when onboarding new employees; MFA methods in use to safeguard users and for audits; cybersecurity policies for users to read and sign; cyber Cloud insurance; frequency to audit security practices; reporting Key Risk Indicators; IT department structure for manufacturing organization; and vendors for implementation of a machine learning approach.*

EXECUTIVE SUMMARY

On the topic of offering cybersecurity education and training when onboarding new employees, a Director of Information Security confessed to needing to mature the process they have in place. Currently, they conduct a 15-20 minute training session after which each individual has to renew and sign off on an acceptable use policy. A CIO / CTO shared that their environment operates the same way. During onboarding IS typically gets a 30-minute slot to discuss their systems, environment, security policy, protecting PII, and what an individual can and cannot do. He does want to be more purposeful in the future as it relates to making sure that security is up front in peoples' minds. A CIO is using Barracuda to perform training every two weeks for employees with email accounts, but he felt the content could be improved. He questioned if there was pre-produced content out there that you could buy and use. A few organizations are using KnowBe4 for phishing simulations and just-in-time security awareness. For annual training, Inspired eLearning is in use by one organization because of the affordability, and the staff likes the content of the 10-15 minute training course they provide. Finally, a Senior VP of Technology / CIO stated that his organization uses Arctic Wolf for their SOC. Subscriptions are available for the training content – 2-3 minute video clips – that they send out every two weeks. The videos are the perfect length to motivate staff to view and train. It has been very effective for them to keep security front and center on people's minds.

Discussing multi-factor authentication methods in use and whether these strategies are actually implemented to safeguard users or simply in place for audits, an organization shared that they have utilized a multi-layer approach from the get-go. Strategically, they are doing it to safeguard their end users, but also to supply security they are confident in. It is not just for auditors. The issue they are having now is that people still do not have smartphones or do not want to use them. A CIO / CTO experienced this as well when they rolled out MFA during the first year of COVID when many people were remote. They simply said if an individual did not want to install the app and use their cell, they could come back to the office and have the phone ring on their desk. This got people to install the app. A Duo shop organization took a different approach. They were able to tack third-party applications onto Duo due to its wide open API and add that integration for those people without a cell phone. They also tied in YubiKey in conjunction with Duo. This allowed them to layer two different approaches to solve the issues for users without a cell phone. Another organization is using Microsoft MFA solution. When they first rolled it out, they had a problem with MFA fatigue. People were getting hammered with calls, texts, and app notifications. They switched it to conditional access where they did a lot of other checks before they would MFA. People actually started paying attention to it more.

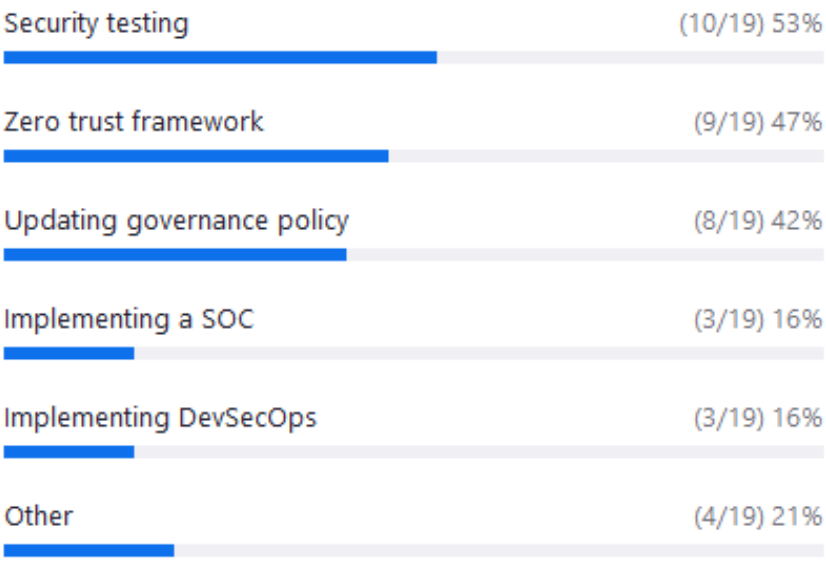
Additional headline topics:

- **Cybersecurity insurance** for Cloud.
- **Key metrics** reported around enterprise risk management.

TABLE OF CONTENTS

Moderator: Good morning, everybody. I'll be your moderator this morning for our discussion around building a cybersecurity culture, one of our special CIO Roundtables. Thank you for joining us this morning. I think we're going to have a great discussion. The security ones are always very, very good. We are going to kick this off today with just a broad view into the top topics keeping you awake at night. I have a poll I am going to launch right now. You can choose as many of these as you like. What are the things that are top security priorities in your world? Folks who marked “other”, do you mind either raising your hand or unmuting yourself, and telling me what is not on this list that you are interested in, in addressing in your own environments? What's one of your priorities that falls into the “other” space? Frank, go ahead.

POLL & TOPIC: Top Security Priorities



Frank C.: Identity and access management.

Parag P.: I would say more on education, on how critical cybersecurity is. Because our weakest link is our humans.

Nathen F.: I would second identity and access management. But then also one of those challenges that I have is partnership with the other parts of IT. Security is a team sport, and not every other part of IT believes that they're on the same team.

Moderator: Interesting. Can you tell us what parts don't seem to play nice as well?

Nathen F.: I wouldn't say they don't play nice. I would say that they have their own priorities and security isn't always that priority. It's just trying to, when you're talking about things like vulnerability management and patching, it's trying to get the partnership with the end user teams and the infrastructure teams to make sure that they're prioritizing the things that you need addressed from a security perspective over in some cases other requests. Everybody likes to chase the next shiny new

fun thing to work on. Patching is one of those things that we, as an industry, believe that we have figured out. But we usually don't.

Terra C.: Enterprise risk management and just risk management as a whole. How do we make sure we are balancing between quantitative and qualitative risk management? Considering I personally don't think that there's a good way to do either, because there's a lot of feelings when you talk to people around risk because risks are scary. A lot of companies don't have great ways in actually assigning dollar values to things. You just hear it's expensive, and so how do you balance hearing it's scary and it's expensive to actually effectively communicate this is a risk because of XYZ. This is how we should handle it. ABC, so on and so forth.

Matthew W.: Keeping track of all the new regulations coming out from states is a pain point. We are in 15 states or something now employee wise and probably 30 + EU for clients.

TOPIC: Immutable Backups

Moderator: Awesome thanks. We're going to move on to our next topic. Skip, tell us if you are using immutable backups or not? Have you selected a partner already?

Skip H.: We haven't yet. We've been doing more traditional. I'd just like to listen and see the options out there. Are they really saving, have you had an effective restore from immutable backups that you maybe used a traditional method in the past.

Austin M.: We use Veeam for our immutable backups, and I have to say it works.

Matthew W.: Yeah, we used Veeam too. They have a ransomware resistant Linux repository feature, in the newer versions of Veeam. We have that enabled. And then when we send them off site we send them to a partner. They actually copy them to a separate storage array that's completely different from the one that you're main copying to. And even if I call and say delete that, it has seven days before they get those purged out. We do that too.

Lindsay A.: Good morning. We've been looking at Rubrik, doing a POC between Iland, Rubrik, and Cohesity. Rubrik does a really good job of a demonstration the immutable piece. You might look into them or their team on getting a hands-on demo of how that works exactly. But so far it's been pretty good. We have not implemented more of the POC process but hopefully we'll have some good news and go that direction.

TOPIC: Cybersecurity training for current and new employees

Moderator: Thank you for sharing. I would like to talk about onboarding new employees. How do you get them up to speed on your environment and the importance of cybersecurity in your environment? Do you guys just let your new employees go willy-nilly, go crazy?

Nathen F.: We do a new employee onboarding with cybersecurity. We have about a 15-20 minute training that they go through. And then we also have the acceptable use policy that each one has to renew and sign off on. Beyond that it's largely tribal knowledge is how we do the different security processes. There's obviously some maturing that needs to occur in that space. But I think that's across the board.

Michael P.: I will jump in and let Nathen know that he's not alone as it relates to an environment that operates that way. Onboarding usually is the one time we can grab people, and you need to sign up

for open enrollment and benefits. And okay, IS has got a thirty minute slot to talk about not only the systems, our environment, what you can and can't do. We also have an acceptable use policy that everyone signs. They get either 20 minutes with the IS Manager or myself to talk about security, PII, protecting information, some of the things that may pop up. Sometimes we will pull examples of things that are live, happening around the time a person comes on board and say okay, here's when an executive got spoofed as a related to an email. Here is an issue where someone got something that looked like it was from a parent. Should you click these things? It is honestly that one time where we kind of get it. We know that it is something that we want to be more purposeful in the future, and more regular about as it relates to making sure that this stays up in front in peoples' minds as they use our systems, or our environments or applications.

Dan A.: We do similar things with onboarding. We have policies they sign as well. The one thing I think that would be different is we also force monthly testing, and we force through our learning management system a monthly training on everyone. They pretty much have to do it. If they go too long without they get a talking to by me, then their coach or their manager, and then eventually HR. And they've signed that policy off. Every month we run them through something. It's usually not long, but something related to security awareness of some kind.

Austin M.: This is more of a question. We have like the onboarding, but our training is really not that great. It goes over a lot of our policies and stuff like that. Is there any like canned content you can buy or present, or does everybody just make their own content? And then also in relation to that a couple of questions ago, it was about the annual training and a similar question there, is there somebody out there that makes the canned training for annual stuff? We typically do some sort of training every two weeks to all employees that have email accounts. We use Barracuda. I forget what they call their training program. But we try to keep it 2-6 minutes, because if it's longer than that, people just don't do it. That's my concern about doing a long annual training, and just curious of some thoughts on all of that.

Parag P.: I would say KnowBe4 is something we use, and I would recommend it.

Ricardo A.: Microsoft has their attack simulation training. We also use Vector training.

Austin M.: Our every two week training is required. We use Barracuda's Security Awareness Training.

Michael P.: Good morning, everybody. We currently have sort of a single layer approach, and we try to do the best job at the onboarding as it relates to policies and processes and giving them that one-on-one time with the IS manager and the team, as it relates to the different pieces of security. But other than that, we have not been particularly consistent as it relates to coming back and reevaluating things. If we see a spike in some thing, whether it's a tax on 365 accounts or compromises with other things we may call something out to say hey, be aware of this. But we have not had I won't say really good luck, I would say we just haven't been really purposeful about meaning to maintaining that throughout the employee experience.

Nathen F.: We've actually taken a multi-pronged approach. At new employee onboarding we do security awareness training. We do monthly phishing simulations with just-in-time training. We do annual required security awareness training, and then we also take over October we follow CISA, Cybersecurity Awareness Month program. For the entire month of October we post quizzes, trivia content, we make in-house videos using the security team for different security topics and then gamification is huge. We hand out prizes throughout the entire year, especially during October.

Moderator: Awesome. What prizes are you using?

Nathen F.: Internally we use this program called Snappy. It's very similar to the corporate gifts platforms. This year we handed out 27 prizes, a total of a $1000 during October.

Moderator: Wow! That's amazing. At the International Roundtable it was interesting to hear that a lot of people were using more stick than carrot. And I think it's interesting to hear people talking more about the carrot to help people be better at this. Terra, go ahead.

Terra C.: I'm a cybersecurity manager. In the spirit of transparency, I'm on like week three. But I can still talk about what I've done in other parts of my life. One of the things that we're doing at least there at the moment is, we have our annual security training as most folks do as well, as well as like monthly, very short videos that are more geared towards real life stuff that happens. For instance, election season, as we all know, has come and is still just hanging around. But the monthly video this past month was around phishing, especially in text messages, considering there's an influx of text messages saying hey, look at this person. Look at that person. How much of this is real, though? Known, unknown. And then we also sent out like a follow-up email just saying here's how you can actually report spammy text messages via your phone to a different service that is hoping that'll span like worldwide.

I think the most important part of cybersecurity education that I've started to do throughout my last couple of jobs is just showing that security team is not a black box and is like available for you to talk to and to ask questions to. We're not like these weird people that sit in corners that you should never ever approach, or that we are going to constantly chastise you or bad mouth you. It actually calls in a good way, like a lot of really positive conversations for folks, both from what you should be doing in your day-to-day job to keep stuff secure, but also how you should be having good cybersecurity practices in your everyday life and at home. I think that actually goes a lot longer as far as teaching folks how to just be good cybersecurity practitioners, even though that is not your everyday job, and it is not your expectation for it to be your everyday job. But if you do even really small things at home, it actually sits more in the forefront of when you come to work and when you're just hanging out in life.

Matthew W.: We get rando texts every 15 minutes or so to users impersonating me or the CFO/CEO. We do monthly 5 minute NINJIO videos, we do in person trainings twice at all hands meetings, we do monthly phishing trainings. You also get a very in-depth training when you're hired.
WEB JAIL. We were one of the ones at the Intl Roundtable that does web jail for cybersecurity offenders.

Nathen F.: Cyber Security "Motto" I have been using that seems to resonate with my user base - "Security is a team sport and our bench is deeper with you on it". Feel free to use that.

John S.: I had a peer run a NIST focused Slack "roleplaying" event, pitting different departments to make decisions day to day and for each group they'd get an update of their choices from the day before. And the one who made the most NIST sort of choices and got the best outcome won the event. Apparently, people were very engaged. Looking for the whitepaper they wrote on it to share. But a fun idea that people seemed to really enjoy.

Parag P.: I think you hit one point that I want to bring up about using more carrot than stick. We are changing that approach. I started here less than a year ago, and were using a lot of stick versus carrot. We are changing that approach on top of it. The other thing is, instead of a yearly or onboarding training, we are trying to move towards more on more frequent training, in a fun way. Like another gentlemen mentioned gamification. We are using that approach too.

Mike L.: We use KnowBe4 and our CISO loves it.

Matthew H.: We use KnowBe4 also. Fantastic solution.

Alberta O.: We use KnowBe4 too. It's great.

Dan A.: Same. KnowBe4 a security awareness company. Because we do it monthly, so it's a split between that canned content and then annually we'll refresh on different policies and things as well on separate months.

Wade J.: Yeah, we use Arctic Wolf for our SOC, and you can subscribe to training content from Arctic Wolf and they do an excellent job with it. They're short. I think it's every two weeks we send out a little video clip, or 2-3 minute video clips, and then every now and then they throw in a little quiz. It's been very effective for us on the training, keeping it front and center on people's minds, I think, is one of the key pieces of it.

Terra C.: I'll be a deviant and say we use Wizer, and in a previous company used a company called Curricula. I like both of them actually, they're also very short. They have gamification aspects to them. Curricula I know has like a free instance that actually gives you a decent amount of licenses. I'm not sure how many folks are in your program. But free is always nice, and if you can make it work, that's even better. And then Wizer, I don't know if they have a free one, but I do like both of those and the amount of content that they have available.

Nathen F.: We use KnowBe4 for our phishing simulations and just-in-time security awareness. But for our annual training, we get content from a company called Inspired eLearning. It's super cheap, and everyone seems to like the content. It's about a 10-15 minute training course is what they provide.

William N.: We actually utilize KnowBe4 and Wizer and for various reasons. But Wizer is our new onboarding tool for when people come on. It's quick hit, it's fast, and then we gradually go to KnowBe4.

TOPIC: Multi-factor Authentication

Moderator: What multi-factor authentication methods do people use? And are you implementing them to actually safeguard your users, or just to check the box that says hey, we do this? Tell us more in terms of your security environment, what you feel comfortable sharing, and how you guys approach this.

William N.: Sure. We utilize from the get-go multi layer approach. Everybody has layers on their onions, right? Not just for audits, but over the past few years we had audits ask us if you MFA this or MFA that. The issue is what do you really want to put multifactor authentication into? Do you want to use it for your office application? You want to use it for your Citrix applications? Things like that. Strategically we're doing it to make it simple for the end users, but also to supply security so we feel comfortable with it. Not just the auditors. We're doing it to safeguard our users. The issue that comes in now is some people still don't have smartphones. How do you do that effectively with those? And some people don't like putting in numbers. Some people just like to push. That's where it gets tricky, and we're still trying to figure that all out.

Michael P.: William, just to add, we had a similar situation I guess the first year in COVID, when we rolled out MFA for some of our things because so many people were remote. And one thing that we

were able to do was to say if you did not want to install the app and use your cell, guess what? You can come back to the office and have it ring on your desk. That would take care of it that way. And suddenly people got real willing to install the app on their devices when they were faced with the alternative. Not that I would recommend that because that had a bunch of cultural ripples that came with it. But it was one of those things that we said if you are this hard on that line, this is the other option.

William N.: That's great. Thank you.

Lindsay A.: William, to combat those users without a cell phone, we needed a combination – we're a Duo shop, so to answer the first question, might have been security or cybersecurity, cyber insurance mandated to start. But then we found the importance of how many third-party applications we had in our organization that we could tack on Duo to. It's got a very wide open API so we're able to add that integration for those people without a cell phone, which we did have a small percentage, we tied in a YubiKey, we got them a physical device where they were able to prove that they were at the device. And then we did that in conjunction with Duo. We're able to layer two different approaches to solve that problem with users who didn't have a cell phone.

Nathen F.: Yeah, we actually took a slightly different approach and this is going to sound a little cliche and a little buzzwordish, but we actually took the identity as the perimeter approach. We implemented identity and access management controls, multi-factor authentication, user risk detections, all that stuff before we hardened a lot of our firewalls. And the reason we did that is because with the COVID pandemic and everybody wanted to work remote, we wanted to make sure that were protecting that user rather than our corporate environment. It seems a little backwards, but it actually worked out with our cyber insurance and everything else. We have the same challenge William, that you just referenced. And that is we have a lot of retail workers and a lot of distribution center workers that in some cases they have old flip phones and so they can't even install the app. But they can receive text messages. We took that approach of if you have a smartphone you can handle the app, then that's the requirement. If you don't, then text message. Right, wrong, or indifferent, our Chief People Officer at the time decided that if you didn't want to participate in MFA you didn't need to work for this company either. We saw a little bit of attrition with that statement, but.

Matthew W.: Okta on 40+ Apps and Networking Gear, DUO On Servers, SMS on everything else that supports only text.

William N.: Maybe it's worth it.

Dan A.: We had a similar thing. We did use Microsoft MFA solution. When we first rolled it out one big problem we had actually, we didn't roll it out for audit, but we rolled that out because of the tax against some specific things and trying to stop that. When we first rolled it out we just rolled it out with like a three day sat on it, and we started getting MFA fatigue from people where they just get hammered over and over with calls, texts, the app. We actually had some people just let it go through based on that. Once we switched it, which was expensive to make the bump, to conditional access to where we did a lot of other checks before we would MFA, people actually started paying attention to it more. That really helped us quite a bit.

Skip H.: I didn't do anything here at [organization]. It was already implemented when I got here. But at my last organization I was with a company who did this. Surprisingly enough, we did lunch-and-learn / mandatory about 35-40 minutes of telling you why, letting you know why it's important to do that, and I think that really helped us get more engagement to the rest of the company.

Prasanna P.: Regarding this topic, MFA, we did implement it. We did implement it when we were doing the Azure migration for all our portfolios. I've migrated two of my portfolios to Azure. We do a handshake between Azure authentication and Active Directory authentication on-premise to talk to each other by creating a UPM where user privileges are checked against AD first, and then go on to Azure application the person is from who is actually connecting to [org] applications on Microsoft platform in Azure. It was a big journey for the security. We've implemented multiple layers within that. We use _____ as well as open-based. We do see some good benefits with that application. Only issue what we see now is basically the time mode of the authentication, because it's going back and forth to compromise Azure networks. That's where we are working with Microsoft directly, and it's going well, I would say. But there are some challenges.

TOPIC: Cybersecurity policy user tracking

Moderator: All right. William, next topic is yours. Do you have a firm cybersecurity policy that users read and sign? It sounded like many people did. How do you track them?

William N.: This is probably the first year we've been doing this, but we actually use KnowBe4 now. They have a pretty good tracking policy area. We've been using KnowBe4 since 2017. Been using it for a long time, but it's like let's do something we should have done a long time ago and do that. So we use KnowBe4 to track that. And it seems to be working well. We get over a 60% hit rate. We should help well over 90, but right now we'll use that to track it.

Moderator: Sounds good. It sounds like Skip's doing the same thing.

Nathen F.: We actually have a similar approach, not KnowBe4, but our learning management system the information security policy yearly acknowledgment is the last question of the training. You go through the training and then before you can actually complete it, you have to acknowledge the information security policy.

Austin M.: We are going to implement something through our learning management system. But years ago, through Active Directory group policy. To first log on to the system you hit control-alt-delete. There's a box that pops up that basically talks about our policy and then links to our internal internet of that policy. That way people acknowledge it every time they log into the computer, although I would probably say 99.9% of the people don't realize that's what they're doing. But at least from a legal standpoint we cover ourselves that way.

Skip H.: We use KnowBe4 to track signing our IS Policy.

Terra C.: Google Forms.

Matthew W.: We have some of the cyber policies on the splash as well.

Mike L.: ADP as part of annual policy acknowledgement / agreement, working with HR.

Michael P.: We utilize splash on our machines, and for any domain admins regardless of where they log on.

TOPIC: Cybersecurity Insurance for Cloud

Moderator: Awesome, thanks. Let's move on. How about cybersecurity insurance? Big discussion about this at the IRT.

William N.: We have cyber insurance for other things, but not necessarily Cloud yet. I think this is newer in the industry, things like if Microsoft goes down for an hour, ten hours, how does that impact your firm? You've got to get those numbers down, because especially our friends in accounting utilize Excel and the Office suite a lot. It doesn't necessarily mean if the Cloud's out - Excel still works, but parts of that where they keep in their OneDrive and stuff. Does anybody utilize cyber Cloud insurance, and for what services? We also have our tax applications in the Cloud and stuff like that too. Just curious to see if anybody else is doing that.

Nathen F.: I'd have to say I have to plead ignorance on this one, William. I know that we do cyber insurance every year, and I go through the lengthy forms. But I'm not sure if our policy covers Cloud.

William N.: Yeah, I believe it's a separate policy. It's newer out there that I'm aware of. Not many companies have it, but there are a few that do. I was just curious. If your 365 is down or our tax application's down on April 14 and tax is due April 15, that hits us hard. And that happened a couple of years ago, where you had two days of outages right before tax season. We have to understand the impact of that and then see if our insurance covers it.

Michael P.: We also have cybersecurity, and we listed some of our environments within our rider, and we had to specify how much data is there and what percentage we felt was PII related. They did sort of this last year of renewal, take sort of like a finer screen as related to some of the policies that we had on-prem versus the stuff that's sitting out in Azure. We have a couple of tenants out in Azure for our services, and they took a look at it. I would imagine if anything happened or there was a hit on anything in the Cloud, most insurance companies are going to try to make sure we go out of it as quick as possible so they don't have to actually pay out. But there's nothing about it that says specifically this is Cloud or this is for your current on-prem stuff. They just incorporate all of it into our cyber insurance policy.

Dan A.: I just had a curiosity question about this myself. Because I would consider most of my computer systems to be included in third party networks. Right? That I'm contracted with so that if my data processing was messed up it would be covered under that cyber insurance policy. The Cloud computing one to me sounds like if you're doing Cloud services to consumers and you're using one of the majors for that and now you've got a risk to a revenue stream disappearing, which probably doesn't fit me as a manufacturer.

William N.: Makes sense.

Dan A.: Okay, cool. That's what I thought. I just wasn't sure.

William N.: Exactly. Perfect statement. That's very clear.

Matthew W.: We have claimed the SLA from Microsoft before and gotten account credit. Same with Okta and Mimecast when we had them.

Skip H.: I think this is also based on the actual insurance company. Now they're starting to delineate between Cloud and on-premise, because I've been involved with this for about five years, and actually longer than that with [org]. But they're trying to get out of it, but they're trying to delineate

because of the differences in the system. I think it's by insurance company. Ours doesn't currently say Cloud, it says if we have a breach, if we have an outage due to a breach, then we'd be a part of that about that policy if that makes sense.

Moderator: Yeah, That was my question too. When you talk about Cloud, you talk about someone else's responsibility. It feels like the responsibility's out of your hands. There's only so much you can do for that. Matthew, I know you guys work in the same space as William does. Is that something that you guys use? William was mentioning that one of the issues with them is their revenue source. That's one of the reasons that they're considering.

Matthew W.: No, we don't have anything Cloud-facing really that's customer... we have some SaaS products, but if those go down. We're an accounting firm. Those are the widely used accounting firm services, so if we're down, [the other firms] are having problems too. It's not like it's a huge issue.

TOPIC: Auditing Security Practices & Penetration testing

Moderator: All right. Let's move ahead. Skip, you have our next topic. How are organizations auditing? How often are you auditing your security practice?

Skip H.: I've only been with [organization] about a year and a half, and they did one right before I got here. What I've typically been doing is doing it every other year just so I can get a roadmap together to address some of the issues or findings that I have. I was just curious if others are doing it more often with more of a third party, I guess, audit than just doing it internally. Or if you do it internally you probably have a team that can be able to do that for you.

Austin M.: We're starting to see more and more with especially cybersecurity applications and things like that where they're all wanting us to have a third party audit every year, internal and external. We've just put it in our budget now to do it every year. We used to do it every other year. I mean we would always do internal and external vulnerability scanning. We do that all the time, but as far as like a formal audit, we're just seeing more and more organizations require it every year.

Moderator: Who does it? Who does a third party audit?

Austin M.: There's a local company that we use. It's called Quadrant. But we've done them through like Dixon Hughes accounting firms, and we've done a bunch of different things just to make sure we're not sticking with one vendor, and don't have the fox guarding the henhouse approach. But there's tons of companies out there that do it.

Michael P.: Annual controls assessment with 3rd party vendor.

William N.: Currently, we do this quarterly.

Matthew W.: We periodically use focal point data risk for that (they are now part of CDW).

Michael P.: We use RedZone Technologies. Dell SecureWorks previously. Hey everyone, great sharing, got to hop off to deal with a fire that has popped up.

Dan A.: We do a NIST CSF external review every 18 months.

Chris L.: Do you use different PEN testing vendors annually and who would you recommend?

Matthew W.: Yes.

Terra C.: I like Doyensec for penetration testing. Abira Security is also great.

Matthew W.: We just used Rapid7, otherwise I usually use Mandiant, Red Siege or Black Hills Information Security.

Terra C.: Consilium Labs is good for audits (SOC + ISO).

Matthew W.: We rotate them yearly and I ad-hoc pen tests if we spin something new up.

Terra C.: Vonahi also for pen tests.

Nathen F.: Yeah, we just completed our first external, NIST CSF alignment assessment. But we don't do like your traditional audit. We have plans to continue doing those yearly, but after next year we'll see if that slips to every other year. It's not a cheap assessment.

Moderator: Do you do internals more frequently?

Nathen F.: We have a really weird scenario. We have no internal audit department. We have a third party that acts as our internal audit, so we technically do internal audits for regulatory compliance, but not specific to our security program.

Terra C.: I realize most companies don't have an internal audit function just because of size and cost prohibits. Internal audit is also funky because they have to maintain the aspect of independence, and that gets very weird when you work for the company and that company cuts your paychecks, and then you make friends with the one person that you need to be auditing. I'm a previous auditor, and auditing is actually what I love tremendously. I realize a lot of companies don't have internal audit, and also a lot of the frameworks that call out like you need to have internal audit are actually, I don't want to say wrong, but what they're trying to mostly have people make sure that they assess that there is some sort of non-biased party coming in and assessing the security controls. Because while self assessments are great and obviously beneficial, we all do still have our own biases when we're looking at our controls, and we don't necessarily want to look at our own baby and say our baby is ugly.

TOPIC: Key metrics for ERM

Moderator: Good way to put it. Thanks Terra. Aaron, let's move on to your topic. Key metrics being reported as part of the report around enterprise risk management. Aaron, what do you guys currently report? It sounds like you don't love what you guys currently do.

Aaron E.: We have these key risk indicators that we track and monitor and report up through our Enterprise Risk Management Committee, and they're not very meaningful currently. We use the KnowBe4 platform, so we'll do phishing campaigns, and we'll report how many of our employees clicked on something they shouldn't have and failed the test, so to speak. We report that as a percentage, and we report the results of pen tests. We do those twice annually. But we're really struggling with other meaningful, more regular KRIs that we can report. We've got a SEIM solution in place and we're looking at extracting information out of that to report. We utilize a tool called ARMUS, gives us a lot of rich information, but how to assimilate that in a way that's meaningful and report it up through the Risk Management Committee is something we're really struggling with. If there's anyone out there with experience, I would love to hear more.

Moderator: Yeah. Folks, share with us if you will what you report back. What kinds of metrics are you using to report your success? I know at the IRT there was a little conversation around attempts at getting into the system that people are reporting. Terra go ahead.

Terra C.: A big one that I did in a previous role was vulnerability. We were just talking about pen tests and things. Pen tests are pointless if you're not - and vulnerability scanning in general is pointless if you're not doing something with that content. We did like a month-over-month assessment of how many vulns were actually closed out when we reached back out to those teams and who was involved, how much time it took, etc. We also did that from an incident response standpoint, doing that same month-over-month saying how many SOC 1 did we have for a month, how much time did it take for us to actually close out these, what teams were involved? And the reason why I keep honing on what teams were involved is because that did actually help us understand if we're noticing that we're having these behaviors in this particular team, what's the root cause analysis? Is it a lack of education? Is it because we have actual gaping holes in the code? Is it some combination thereof? That was very beneficial for our product security team. We did threat modeling, we also reported how many threat models were happening for teams as they were pushing out new features and things of that nature. Because again, we were trying to be more proactive than reactive once we got to the vuln scan side of the house from a compliance standpoint, because were SOC 1 and SOC 2 audited we reported on the different remediations that were happening. Or if you're more in the Federal space or plan of actions and milestones, those are just like some of them. I do recommend if you are doing vuln scans and having incidents and have that program built out, those metrics are very beneficial for your company because it also lets your management know if we're having 4 scans a month around availability. But you have no redundancy in place. Maybe this is your time to be like. Look at me. I need that money for redundancy that I've been asking about for months. And now we actually are having problems.

Dan A.: I'm probably a smaller organization privately held. It's a little different for us. I guess we do the reporting on obviously things like phishing, and it gets reported back up to our MIS steering team, and those help us make changes to what we want to do organizationally. But when I get above our MIS steering team and we start talking about the different business process leaders or the board, things like that, I don't talk any of those types of metrics. Really, all I do at that level is review our NIST audit externally, what we want to do over the next eighteen months, and how that ties back to their business. I use that to try and get money to keep the program rolling. Trying to roll metrics to that top level has been very difficult for me and hasn't added much value. I guess it's the level you're reporting at is what I'm trying to get at. That depends on what you're going to do.

TOPIC: Best practices around IT structure in a manufacturing environment

Moderator: Other comments about things that you have found to be successful in the reporting space? All right, Aaron. Let's go ahead and move on to your next topic. Organizational structure for a manufacturing organization. I think this relates maybe back to the IT covering the OT space. Is that where you're going with this Aaron?

Aaron E.: Yeah, there's kind of three elements to this that I'm struggling with. One is the IT-OT bifurcation for sure, and those two teams. Another is the concept of build versus run within the department, and then the third is just the simple bifurcation of the applications team from the infrastructure team. Nowadays there's so much overlap between infrastructure and applications between IT and OT, between building and running that I'm struggling with the right organizational structure for the team. Of course talent influences this as well. But I'm trying to ignore the talent and the people that I have and come up with the ideal and then try to work towards the ideal rather than

try to make the pieces I have fit something that maybe isn't ideal. Hopefully I articulated that well enough to draw some discussion.

Parag P.: It all depends on what your strategy is. If your strategy is to move to 100% SaaS, I would say more towards integration. Have one group and not segregate the infrastructure and applications. If your intention is to have in-house on-prem development, it depends on how stable your environment is. If it's unstable, I would say run versus build. And if it's fairly stable, I would move towards Agile. And automation I would say move it more towards DevSecOps. Have multiple small groups. Hope that helps.

TOPIC: Vendors for Machine Learning

Moderator: Thanks Parag. Aaron, let's take our last question for today. What are some good vendors for the implementation of machine learning? Do you mean specifically around cybersecurity? We talked about that earlier. Or just in general?

Aaron E.: Oh, this is more in general. We're a manufacturing environment, and we're very data rich. We've got lots of sensors and information being provided by the machines that we utilize to manufacture. But we don't have the tools, the processes for using that data to help us make better decisions. We have some very simplistic things in place like heat sensors and vibration monitoring, but that's not cutting edge at all. We'd like to go on a journey towards more of an AI or a machine learning, advanced data analytics sort of approach. I need to work with a vendor to get there. I don't have the skills in house to really explore that the way I want to, and I was just wondering if anyone had some experience out there with some good vendors.

Moderator: Yeah, that is such a good question. Matthew, go ahead.

Matthew W.: We're an accounting firm. We don't do AI consulting but basically large amount of the accounting and advisory firms. I just put BDO's link in there. But they pretty much all can do AI and data analytics and stuff like that. You might want to take a look at that. A bunch of the bigger ones. https://www.bdodigital.com/services/data-analytics-ai/artificial-intelligence which we are an affiliate of.

William N.: Thank you!

Dan A.: We don't do as much AI as RPA in manufacturing. UIPath as an example.

Moderator: Thanks so much, Matthew. Other thoughts? Thanks so much for sharing your thoughts and experiences. It is what makes these work as a conversation. What a great group we had today. Really appreciate the variety of thinking and the number of people willing to share their experiences. We will look forward to seeing you very soon another Roundtable 55. Take care.

End of discussion

Products / Vendors / Technologies shared in this Roundtable 55

Abira Security
Arctic Wolf
Barracuda
Black Hills
Cohesity
Consilium Labs
Curricula
Dell SecureWorks
Doyensec
DUO
Focal Point Data Risk
KnowBe4
Mandiant
Okta
Rapid7
Red Siege
RedZone Technologies
Rubrik
Splash
Vector
Veeam
Vonahi
Wizer

Appendix A: All Poll Results

Top Security Priorities: