SECURITY INITIATIVES FOR 2023

At this 01.17.23 Roundtable 55, *NOREX Members discussed quantifying cyber risk to justify investment or avoid spend; implementing a Zero Trust framework and with what vendors; changes to security environment to accommodate clients / customers sending questionnaires about security posture; MDR service and pen testing with a 3rd party; EDR vendors; GRC tools to manage change and improvement of cybersecurity controls; open source security software; and email security vendors.*

EXECUTIVE SUMMARY

Regarding a Zero Trust framework and vendors used to implement, a Director of Infrastructure and Support believes Zero Trust means different things to different people, depending on what you are doing. His organization is using the Microsoft ecosystem to accomplish close to a Zero Trust system. Through their identity access management platform, they use conditional access policies to allow access based on if your device is a company-managed and compliant device. Is the user account compliant and registered for MFA, and is the application using SSO? They have a very specific SharePoint site that has closely guarded access. They use that framework inside the Microsoft ecosystem to help them control it all. A GISO / Head of IT Operations shared he has found that Zero Trust is more of a marketing buzzword that means a layered security approach to your enterprise and your infrastructure. Zero Trust should be unique to your organization. You need to talk to your stakeholders, security teams, IT teams, developers, and DevOps teams and really drill down to what needs to be most protected. Then, determine how you set up that access control for the various data and controls that you have in your system. As far as vendors, Microsoft does have some tools, but you need to complement them with other vendors. BlackBerry is also big in the Zero Trust space.

When discussing EDR vendors, a Senior IT Security Analyst said that they are now using Artic Wolf. The choice was difficult, as most vendors claim to have the same sort of tooling. A VP of Information Technology shared they switched to Cisco's AMP replacing Malwarebytes. They did this because they use Cisco Umbrella for their web filtering. Their new security interface allows you to get to that one pane of glass where you can manage all the components from the same place. A Senior Director of IT is using CrowdStrike Complete, which handles everything end-to-end. If you are a smaller organization like theirs, it makes sense because it is one of those set it and forget it type models. A full Microsoft shop uses the entire Defender stack of software. They have E5 securities add-ons to their E3 licenses, and Azure P2 as well. They have heard from their pen testers and red teamers that they are very impressed with the performance of the Defender stack – Defender for Endpoint; Defender for Identity; and Defender for Cloud apps. It really does provide comprehensive protection of all of your endpoints. Plus, it feeds directly into the Sentinel CM Solution so you can put everything in a single pane of glass.

Additional headline topics:

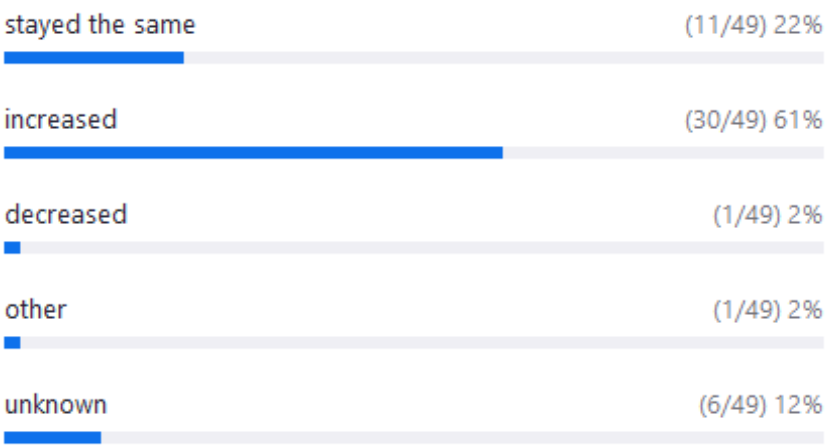
- **GRC tools** to manage, change and improve the controls.
- **Security** – making the case.

TABLE OF CONTENTS

NOREX Roundtable 55 Transcript
Security Initiatives for 2023
January 17, 2023

Moderator: Good morning, everybody. I'm so grateful that you joined us this morning around a discussion for your Security Initiatives for 2023. Let's go ahead and get started. We've got a couple of polls that we're going to do to find out where people are today.

POLL: For 2023, our security budget:



POLL: What are your top security initiatives for 2023?

TOPIC: 2023 Top Initiatives

Moderator: Who wants to kick us off today and talk about “other” as an option for things that you're focusing on this year. What did I miss? Go ahead and jump in and tell us top priorities. Maybe the top 3 would be helpful. Go ahead, Joel.

Joel N.: One of the things we're going to look at this year is Zero Trust. In addition to a couple of things, we’re starting to explore that. It means a bunch of different things to a bunch of different people, so I need to figure out what exactly it means to us and looking for a vendor to help us implement that.

James R.: Some of the top three that we're looking at is number one I would say would be EDR. We just recently implemented a solution for EDR / XDR. Second on that list is Zero Trust as well, in the form of remote access and a hybrid workplace. And then I’d say number three, which I also checked off was secure backups. We do have a secure backup solution but I guess looking for something a little bit more isolated and more air gapped than what we have today.

Brent H.: I have my top priorities on a little piece of paper. Vulnerability management, that's number one. We've got definitely secure backups. We're looking at security awareness training which we already had on there, and then the SIM. We also implemented XDR in 2022 and we're looking to get our SIM implemented this year as well.

Chris H.: Some of our year-one objectives this year are just around identifying and detection. We are diving into the SIM and SOC approach as well as auditing our XDR, but also looking at our SaaS detection. Looking at different automation pieces in there to see what's shared externally, or on the Shadow IT side is who registered for what with their email accounts.

Alex T.: CMMC

Matthew W.: Micro Segmentation of network (other).

TOPIC: Zero Trust Framework

Moderator: Thanks, Chris. Let's go ahead and move on. Joel, let's go ahead and jump into a Zero Trust framework. Tell us about where you're at and how the members can be helpful.

Joel N.: We are at zero. I haven't really done anything with it yet, just starting to. We have our trusted MSP that I work with on a lot of things. I just started having some conversations with them around it. Just wanted to hear what other companies are doing and have been doing it. It was Zero Trust. I don't know what I don't know, and I’m just fine in saying I don't know enough about this to confidently speak to it, but I know that I need to get there.

Nick S.: I wouldn't say we're technically Zero Trust. But you had said earlier, Zero Trust means different things to different people, depending on what you're doing. We're using the Microsoft ecosystem to accomplish close to a Zero Trust type system. Through a combination of their identity access management platform we use conditional access policies to allow access based on if your device is compliant. Is it a company-managed device? Is your user account compliant? Are you registered for MFA? Is the application using SSO? We use a combination of all of those things. Then we have varying levels within that. For instance, we have a very specific SharePoint site that has closely-guarded access. You actually have to have your device ID added to a conditional access policy because you're only allowed to access it from that specific device. You can't just go to some

other company-managed device and hop on. We're using that framework inside the Microsoft ecosystem to help us control all that and it seems to be working quite well. We're slowly just ramping up. We've been working on it for almost the past year now and it's becoming much easier, especially when you have that single pane of glass. We're fully integrated with Defender. We are E5 licensed. That does make things a lot easier because all of that stuff comes right out of the box available to you. I think we're P2 E5, so it makes it really easy. But we're liking it. Again, as you said, we have a trusted partner as well that works with us on that. Where we have gaps, they kind of help us close those gaps or assess what those problems are. It's been very minimal disruption to our users as well, which is quite handy.

Moderator: Nick, are there any lessons learned that you could share? Things that you would say you started down this path and don't do that.

Nick S.: I guess the biggest thing I would say is if you're implementing policies, always use the report-only mode first, especially if you're an M365. It's not available with every policy. But what I really do like about it is it tells you specifically who and what will be impacted and how. Sometimes it's not necessary for the report-only because it's pretty cut and dried, but there is some stuff that is a little bit ambiguous. Having that report-only mode will tell you how it would have implemented a certain policy based on how someone was accessing something.

Moderator: Thanks, Nick. Some folks have jumped into the chat. Feel free to open up your mic and share some of your lessons learned, or a partner you particularly care for that you feel your experience has been really good with.

Matt S.: Somebody mentioned in the comments that Zero Trust seems to be more of a marketing term those days, and in my research that's what I found out. Zero Trust in itself is more of a marketing buzzword that means a layered security approach to your enterprise and your infrastructure, whatever you're managing. What does zero mean? What's the measurement? It should be unique to your organization. You need to talk to your stakeholders, security teams, IT teams, developers, and DevOps teams and really drill down to what needs to be most protected and how you need to go ahead and set up that access control for the various data and controls that you have in your system. What I would suggest is to do some research. There's some really good frameworks, but frameworks can get 50 / 50 sometimes. That's really what it should be. As far as what vendors we're using, there's a lot of vendors out there. I know BlackBerry is big in the Zero Trust space. Microsoft does have some tools, but you need to complement them with other vendors. That's just something to keep in mind when you're thinking about Zero Trust.

Matthew W.: We are about to purchase Illumio for Zero Trust Network Micro Segmentation.

James R.: Did you evaluate any other vendors as well? We recently ran a POC with Barracuda Zero Trust.

Brian B.: We implemented the Dell Avamar / Data Domain Backup Solution PROD / DR and their cybersecurity vault. It has worked well for us.

Chris H.: Where are you starting with Zero Trust? We are working with IT first, then branching out from there. Its a mindset and a long road. We use Rubrik for our secure backup with Zero Trust.

Brent H.: Looking, and have been speaking to Rubrik as well for backups.

Chadd B.: We've been Rubrik for 4+ years now. Very happy with their solution. If you have any questions or want to chat, NOREX can connect us.

Brent H.: Thanks Chadd! I will do that.

Matthew W.: Zero Trust to me is minimizing what can talk to each other on the network / devices / apps and verifying it's really them before they are allowed to do anything with each other.

Chris H.: We are building towards least privileged access first.

Jeffery R.: We just moved over to Rubrik for secure backups. Previously had Cohesity, but there were limitations on a multi-tenant environment.

Matthew W.: Zero Trust was a marketing term invented by Forrester, just like XDR was a term invented by Palo Alto.

James R.: I've seen Zero Trust used a lot for marketing with backup vendors as well. Agreed in level setting on the context of Zero Trust (network segmentation / privileged access vs backup segregation).

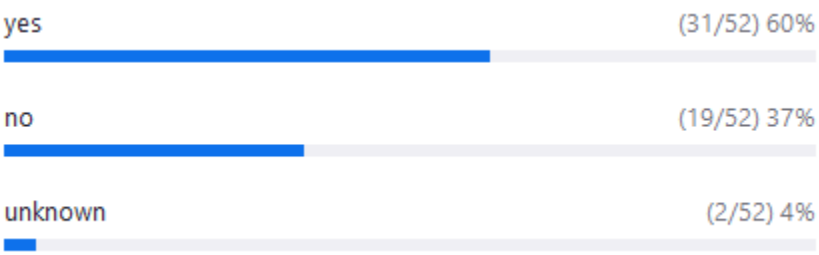
TOPIC: Security questionnaires from customers

Moderator: Yeah, I appreciate that insight, Matt. Let's move forward. It looks like Rob isn't with us today. Does anyone want to cover this topic? Questionnaires that you get from clients around your security. Go ahead, Matthew.

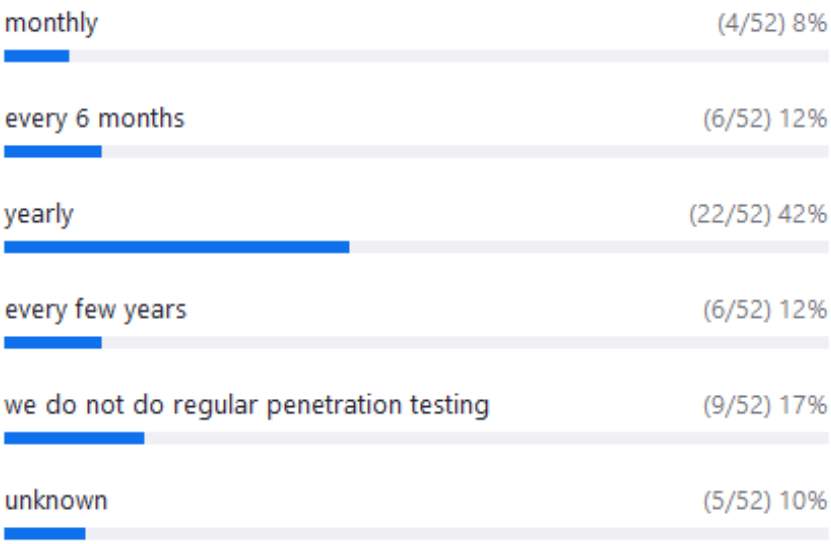
Matthew W.: I believe that's from an accounting firm. We're also an accounting firm. We just basically have a cheat sheet for all the main questionnaires. We get this all the time. We have a main one-page or cheat sheet of everything that's basically asked in most of those questionnaires. Usually the typical questionnaire that's used is the SIG Lite. What we're usually seeing, we actually send the SIG Lite out to our own vendors. Just fill the SIG Lite out yourself to see if you have all the questions answerable. As I said earlier, most of this stuff the security products we're having to put in are being required. Cybersecurity insurance vendors are saying you have to do EDR, DLP, this, that. And that's what's driving a lot of the changes and stuff like that. But yeah, one-pager. Fill out the SIG Lite yourself just so you know what the answers of the possible questionnaire might be. And look at your cybersecurity insurance.

Moderator: Thank you, Matthew. Next topic: do you have an MDR? Are you still doing penetration testing? I have actually a poll for this one as well. Do you have an MDR service? If so, how often are you penetration testing? Go ahead.

POLL: Part one - Do you have an MDR service:



POLL: Part two - If so, how often do you pen test:



Matthew W.: We use MDR service. We happen to use Rapid 7. They also do pen testing services because they on Metasploit. They do recommend that you don't use them entirely for their own pen tests. They want you to go out. We've used them before for pen tests, but they've explicitly told us go get a bunch of different vendors every year. We don't know everything, so you don't necessarily want to use your MDR vendor as your pen test vendor.

Randy B.: I was just interested in this because we've been using the same vendor for a while now, and we changed our MDR service. I was just wondering what other folks were doing and what their view on that was. I appreciate those comments.

Robert N.: We are just implementing Rapid7 IDR as well as their vulnerability management because we're just rolling them out. We're also going to use them for our penetration test this year. There are two completely separate arms of the company, but I understand what the other gentleman was saying about not using the same - the fox guarding the henhouse, so to speak. But we have had good success using different vendors each year, just to keep them all honest. Next year I will not use Rapid7, but do recommend switching it up every year.

Joel N.: We use Arctic Wolf for our MDR service. I'll use them for managed risk and managed security awareness. I thought I saw that on the agenda as well for awareness training. I haven't done a pen test, but since we've implemented them we will be using a third party or a different vendor than Arctic Wolf to validate those changes.

Kyle D.: We also use Arctic Wolf, and I believe they have some sort of monthly penetration test. But we are using another vendor for a yearly penetration test.

Brent H.: We use End Game through Elk Analytics for our XDR with 24/7 SOC. SIEM will be through them as well.

Matt S.: All of these.

Matthew W.: We rotate between Rapid7, Mandiant, Black Hills Information Security and Red Siege and TrustedSec for pen tests.

Chris H.: Anyone use Artic Wolf for MDR/ SIEM?

Peter G.: Used Arctic Wolf at my previous company.

Brent H.: Vulnerability management - Tanium anyone?

Oku O.: Anyone using VMWare Carbon Black?

John L.: MDR monthly via Arctic Wolf.

Will S.: We use Carbon Black.

Peter G.: Have used Carbon Black previously.

Matthew W.: We are entirely a Rapid7 shop: InsightIDR, InsightVM (Nexpose vulnerability manager), and Rapid7 MDR.

Janet A.: We use Arctic Wolf for MDR/SIEM as well.

Alex T.: Sophos MDR.

James R.: We use Qualys for VM and patch management. We have used Rapid7 in the past for a VM scan and pen test.

Joel N.: AW does do the monthly external vulnerability scans. I'm not entirely sure it's as thorough as a true pen test.

Oku O.: Also, I was recently recommended to look into the free DHS pen testing service. Anyone heard of them or used them? Link here: https://www.cisa.gov/cyber-hygiene-services

TOPIC: Governance, Risk and Compliance management tools

Moderator: Anyone else? Let's move ahead. Are people having success with GRC tools, specifically using them to manage, change, and improve the controls? Are you guys using a tool today, Randy?

Randy B.: We have a homegrown tool we built in a Smartsheet to help us keep track of things. We're a small shop so we don't have access to a lot of the bigger tools. I was just wondering what folks were doing there.

Maria H.: I am the CIO. We don't have a lot going on in this space, unfortunately. I really wanted to hear from some others what they were using. Hopefully, I can go off and do some research on some things. We're not quite ready to take on a big footprint yet in some of our cybersecurity controls. I'm hugely interested. But we're working on some foundational stuff right now. DLP control access, conditional access groups, getting our MFA a little bit more clean. It's going to be the next phase for me. Tell me more, you guys. What do you think?

Robert W.: We use a product called Netwrix. It's a cost-effective software to use, and it has a lot of really good features. I've used it across multiple organizations in the past 10 years and always find that it gives me what I need. They have built-in templates for meeting the requirements and good notification. And like I said, it's cost-effective. It's not real expensive at all.

Moderator: Robert, how big is your organization?

Robert W.: We're a group of retirement communities with about 1,200 employees.

Moderator: Thanks much. Okay folks. Help Maria and Randy out. Who are you using and what do you like?

Robert N.: We use ManageEngine's ADAudit Plus and Netwrix. I've used Netwrix in the past. It's excellent. I would say ManageEngine gets a little bit more granular and it's a little bit more challenging in the setup. But the tools within it are very good, as long as you keep your Active Directory clean and put all the connectors in place. It takes a little maintenance to get it to a happy place. But once you do, you can get great automated reports. An example would be right now I have a weekly report that goes out to IT and HR that shows all of the active employees and non-employees in the company. Because they're always asking how many contractors we currently have. It just goes out automatically now. We're going to build upon that in the coming months.

Moderator: Thanks, Bobby. Buzz, you had your hand up briefly. Is that also your comment?

Buzz W.: For a GRC tool, we're using Archer right now. We moved away from OpenPages. It was very, very difficult to work with. Both are not cheap, but Archer has made it easier to align projects and initiatives with audit controls to make sure we're keeping everything in sync. The automated processes that Archer has are pretty impressive once you get them set up.

Chadd B.: Just echoing what couple of people said about Netwrix. We've used it for 3 or 4 years now, and it works really well. We have quite a few alerts set up for different activity. We also use Rapid7, and a couple other tools that look for suspicious behavior, file moves, or things like that. But Netwrix seems to every once in a while pick something out that Rapid7 or one of our other tools doesn't pick up. It's been something that we've kept around, and if anybody is looking at it, I definitely would recommend it. We have their monitoring tool for all of our infrastructure. They sell it in different pieces for file servers or AD or Exchange, and we have all their components. It works really well.

Matthew W.: KnowBe4 GRC. We used to use OneTrust until they tripled the cost without telling us until the renewal. We exported everything out and imported it into KB4.

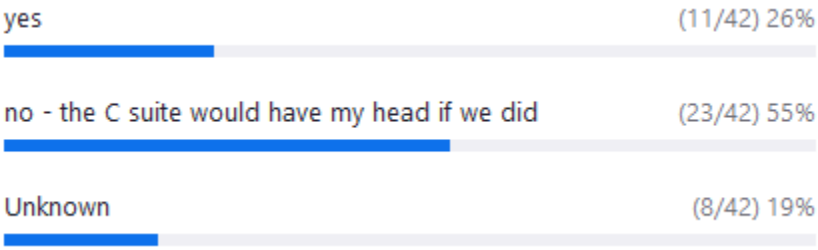
Andrew H.: I've loved using StandardFusion for GRC. https://www.standardfusion.com/

Matthew W.: We have Sysmon on every Windows box, but only because Rapid7's MDR agent installs it.

TOPIC: Open source security tools

Moderator: Thanks for sharing that. All right, let's move ahead. I have a poll here. I'm always curious about the concept of open source and security together. Are you using open source tools for security? Maybe you're not in a position to really know the source of the tools.

POLL: Do you use open source security tools:



Kyle D.: I know we have as part of Arctic Wolf we have Sysmon being installed on the computers. I know we've been having issues deploying that onto all of our endpoints with Intune right now, and I don't know if anyone else has had to deal with that before. But we've been having an issue. We had one version of it. It was outdated, and they need the latest one and trying to use Intune for that.

Joel N.: Yeah, we're going through the exact same thing right now. Like if there's a vulnerability or something identified, and the Sysmon version so trying to update that through Intune. We're actually working with Arctic Wolf on that now to figure that out. I could just check the status of that and see if we come up with anything on it.

Moderator: Yeah, for sure. That'd be good for you guys to chat.

Kyle D.: We've just been uninstalling Sysmon entirely and then having to reinstall on every single computer. And that's definitely not ideal. We have a hybrid AD environment with some people not connecting to the corporate network potentially ever. It takes a while for those things to get deployed or removed.

Joel N.: Yup.

TOPIC: EDR Vendors

Moderator: Anyone else? All right. Let's move on. EDR vendors. Go ahead, Kyle.

Kyle D.: We ended up with picking Arctic Wolf this year. We started last year, but I know the search for them was very difficult, because a lot of them claim to have the same sort of tooling and stuff. It's very hard sometimes to go and pick between multiple different vendors, and there's so many of them out there. It'd be really difficult.

Robert W.: We just switched to Cisco's AMP replacing Malwarebytes. The reason we did it is we already use Cisco Umbrella for our web filtering and their new security interface allows you to get to that one pane of glass where you can manage all the components from the same place. In the past 45 days we got it completely switched over to that to AMP.

Buzz W.: We use CrowdStrike primarily. We're continuing to grow that within the environment. We've used some other one-off types of vendors, different pieces from Microsoft. But the majority of our work comes through CrowdStrike. That's our primary one.

Robert N.: Like Buzz, we use CrowdStrike Complete, which means they handle everything end-to-end. If you're a smaller company like we are, it makes a little bit more sense because it's really one of

those set it and forget it type models. The only downfall is that the reporting is challenging to say the least. But they do a great job, and it's given me a lot of peace of mind.

Jeff S.: We're a CrowdStrike customer as well and very happy with the things that CrowdStrike has done for us, but we've also been able to integrate it into our SOC as well. They're seeing all the work come in and help them to manage that from that standpoint. I've been a big fan of CrowdStrike at this point.

Matt S.: We're a full Microsoft shop. We use the entire Defender stack of software. We have E5 securities add-ons to our E3 licenses, and Azure P2 as well. But we are using the complete Defender stack, and from what I've heard from my pen testers and the red teamers that we've had work with us over the years, they're actually very impressed with the performance of the Defender stack, the entire Defender stack. Defender for Endpoint, Defender for Identity, Defender for Cloud apps. It's all pretty much part and parcel of the E5 suite when you get it. But they actually do a really great job, especially if you're a Windows native shop. If you have Linux machines, they do also have a sensor for Linux servers as well as Android and iOS and the whole Mac universe. It really does provide you a comprehensive protection of all of your endpoints. Plus, it feeds directly into the Sentinel CM Solution. You can put everything in a single pane of glass. One thing to note, though, especially with the Azure side of things, watch your Azure spending, because you will see those virtual machine prices and those I/O costs creep up very quickly the more you connect into the Sentinel universe. The Defender has a pretty good pane of glass, but it's not comprehensive as with Sentinel, so just keep your costs in mind, because your server costs will go up.

Kyle D.: I know for us we have Defender in a passive mode right now, and we have Sophos as our current active EDR. I'm just wondering how that goes. I know some people have it for MDR as well, and I was wondering how that plays with it. I know from my experience using it with the EDR we've gotten so many false positives with Sophos over the years. This year we've had some pretty big false positives from them, and when we ask them for additional feedback, they have not really been giving us useful information. Because we have Defender in passive mode, they seem like they've had a few conflicts over time, even though it's not in active mode. I don't know if anyone else has had any issues with it.

Gary C.: We switched to the full MDR in Sophos a few months ago, and we had Intercept X and their solution there for years before that, and we never had the problems that people are showing here at the CPU usage and some of the false positives. We've only had MDR for a little while, but so far it's been great. They contact us when they see something out of the ordinary. We reach out to them, or they reach out to us, we get a result. It's been pretty smooth so far.

Moderator: Thanks for jumping in Gary. Any other Sophos shops want to jump in with a good experience or seeing what Kyle has seen?

Kyle D.: I'd like to add sort of another question too. Anyone who used to be Sophos and switched to Defender, has anyone done that over here? Because we are potentially looking at that. And Sophos has done some good at eliminating, like it's been good. But the false positives have definitely been an issue that we've seen, and just the lack of visibility into the endpoints. Like with Defender, we have timelines, and I haven't been able to really find that same view with Sophos. I don't know if anybody has seen that sort of side of it.

Matt S.: We're a Microsoft shop so our EDR is Defender for Endpoint.

Chadd B.: +1 CrowdStrike.

Gary C.: Sophos MDR.

James R.: +1 CrowdStrike. Just implemented last month. Seems great so far!

Brent H.: Are CrowdStrike costs reasonable?

James R.: Seemed reasonable. Took advantage of an end-of-year deal. Happy to connect afterwards and discuss further details.

Brent H.: Would love to, James. Thanks.

Chadd B.: If I remember right, it was reasonable for us. We came off Cylance. I didn't handle the purchase directly but wasn't that much more than Cylance.

Kyle D.: I see a few people with Sophos. How do you like it so far? We were looking in to them earlier.

Alex T.: It just became a full MDR, before that it was only a EDR. Otherwise, they have been fine. No issues so far.

Matthew W.: We used to have CrowdStrike. It was almost 2x the cost of SentinelOne, and SentinelOne beats CrowdStrike in the MITRE tests, if you believe those.

Brent H.: The full Defender stack is not bad at all. We have E5s as well.

Matt S.: 👍

Jacob K.: We use Carbon Black Cloud on our systems.

Matthew W.: Sophos Intercept X. We looked at it years ago but the CPU usage was insane.

TOPIC: Top Security Tools

Moderator: Let’s move on. Email security. Tell us about what you guys use today. Are you looking to change?

Joel N.: We’re a Microsoft Shop. We have the canned Microsoft email security right now. I did get in with Darktrace at the end of ‘22. We have not implemented yet, but we do have that sitting in the background waiting to go in. It's in passive mode right now. Some interesting finds in there. Seems like it’s going to be a little bit tighter than the Microsoft product. We were getting a lot of leakage, I guess, through their phishing, scoping, especially for the C Suite. We need something a little better to tighten that down for us.

Moderator: Looks like lots of people using Barracuda. Folks who have a tool that you feel works well, go ahead and jump in and tell us about it and why you're using it.

Jeff S.: We were Mimecast prior, and then last year we switched to Proofpoint and really saw the decrease in spam happen through that transition as well as with their security awareness built into it. You can help educate the users as to why this is spam or this was a phishing email. It's all built in. It just helps reinforce the cybersecurity throughout the organization at the same time.

Moderator: And, Jeff, I'm sorry. Tell me again. You went from who to who?

Jeff S.: Oh, sorry! We went from Mimecast previously to Proofpoint.

Buzz W.: We use a lot of what everybody else has been talking about. One of the ones we use though, that's different and really helped us a lot is a company called Area 1. What they do with email, and especially I really like their pricing model, because the way they price out is if they don't stop something, they don't get paid. It's their advantage to try and find the instances to do it, and they're very successful at what they do. That's one besides Cisco AMP and all the other ones people talked about. I don't think there's any one single answer out there that can catch everything. They all do different pieces, but Area 1 was a great add to us. We've been with them now for a couple of years.

Kyle D.: We have Proofpoint over here, and it does pretty well.

Chadd B.: We use Mimecast right now for email security.

Kyle D.: Proofpoint primary as well as MS for internal.

Gary C.: We use Sophos Email Gateway.

Will S.: Cisco Email Security.

James R.: Barracuda Total Email Security.

Leslie N.: We use Mimecast for email security.

Alex T.: Mimecast.

Steven B.: Barracuda. Looking at Avanan.

Jim J.: We use Barracuda EGD.

Matthew W.: I haven't had a legitimate phishing email hit a single user in over 8 months.

Ashley S.: Mimecast.

Matthew W.: How do you spell that?

Justin M.: We use Area 1 as well and am happy with this filtering capabilities.

Matthew W.: Area1, like Cloudflare's email security?

Chadd B.: Doesn't Cloudflare own Area 1 now?

Justin M.: Chadd, yes.

Chadd B.: 👍

Buzz W.: 👍

Chadd B.: We use Cloudflare and I thought I noticed that show up in our console recently.

TOPIC: Making the Case for Security

Moderator: Another thumbs-up for Proofpoint. Lots of thumbs-up in the chat. Anyone else? Maria, you weren't quite on right at the beginning when we started the conversation, and so we jumped over that very first question around making your case for security. Do you want to jump in now and have that conversation now?

Maria H.: Sure. Let me give you all a little background. About nine months into my current company, and I've walked into a bit of a mess, but have certainly been in other companies for longer periods of time where putting forth that cybersecurity improvement and additional layers that you want to put in and asking for that budget and fighting for it. Compared to other business initiatives it makes money. It's a hard sell sometimes, so I always like to ask other folks in IT leadership positions how are you defending that? Certainly through a lot of lessons learned and things happening in the world around us it makes it a little bit easier, because we all know it's not *if,* it's *when.* It can come down to how much is too much and how you defend that conversation when you're looking for that budget. That's what I always love to hear what other people have to say.

Will S.: We're a specialty clinic, so I have the sometimes unfortunate oversight of HIPAA. But in this instance I am able to leverage HIPAA, and I say here's this issue. I was able to leverage cybersecurity insurance to be able to push through MFA. But otherwise, if we have some aging servers or just some aging hardware, I can point to HIPAA violations. I say well here's how much it would cost for us to replace it. And here's how much it would cost if the OCR comes in and says we have this many HIPAA violations. When you do the comparisons it's usually cheaper to just replace the object. That's an easier way for us, but just pointing to the cost of not doing it I think usually helps when I go to pitch my cause, I guess.

Moderator: Thanks for sharing. I know at the very beginning Matthew, you talked about the insurance checklist, right? That it's just required. Do you want to jump in?

Matthew W.: Yeah, our cybersecurity insurance has an eight-page cybersecurity questionnaire that's gotten progressively longer over the years. Every single time they add an item, we basically buy it, because otherwise the premium doubles.

Robert W.: Building off of Will and talking about using cyber insurance and using HIPAA. Four weeks after I came on we had a ransomware attack. That gave me a whole lot of political capital in the beginning. That was three years ago. But since then, it has been the cybersecurity insurance and HIPAA to the point that we had an incident. We were investigated by OCR because of an email account breach. Their findings came back that they said we're just going to close the case because you're doing all of this stuff so we know that this wasn't systemic. This was an outlier, and so we didn't have to pay a fine or anything. That was a big win for me personally, because the C Suite was very happy not to have to spend any extra money.

Brent H.: We went through one of those as well. We went through an OCR investigation as well. About a year and a half ago we had a breach. Got through it, checked all the boxes like you're saying. But even though we got through it clean, there's still a lot to implement. We check the boxes, but we need to flush everything out. But yes, we did. We were able to do it, and unfortunately, we had hardly anything, so they gave me a lot of political capital power to implement some things, but that also made it really difficult to understand where to start. This stuff really helps a lot. Thank you for that.

Buzz W.: We were fortunate and unfortunate at the same time. Back in 2011 we had a breach,

and that was before the target and everything that started getting everybody's attention about cybersecurity. Because of that breach, very small, nothing lost, nothing ever found, it still took over 5 years to settle because of all the AGs. While the fine was only about $5.1 million, the amount that it cost over that 5 years to defend it far exceeded that number. But what it did was it got the Board of Directors' attention. Kind of like what Brett was saying there, because everybody assumes when they hear a word they think they have it. Oh, you have DLP? Okay, so that means it does all these things, right? No, not necessarily. You're filtering everything that goes out to a box, so that means nothing gets out there. No, not necessarily. I mean it's really that whole mindset that this helped us do besides looking at all the right things to do to increase our infrastructure and our ability to detect. It also helped us realize things like solidifying a really solid event management process, really being clear and definitive when it came to this is what it will do, this is what it won't do. Or this is where the costs are to make it perfect versus good enough. It's a world where nobody can afford perfect. Plus, perfect changes every day. I like the comment that someone said it's an if not a when. I mean that's just the world we live in today. For everybody else, ransomware and all these attacks have really helped. It's helped us, in a way, to get people to remember. Sometimes you do so good, and you get all this big chunk of money, you do these things, you're stopping, and we talk about it. Well, why do I want to spend this more money? Where are we doing all this? Well, because it's a never-ending project. It always continues. And so, these little pop-ups that happen help solidify that, help keep it fresh and front-of-mind. I think those are the advantages to looking at how do you always make sure that you're getting the funding to do the right thing. Definitely the financial regulatory controls that we face being a financial and insurance company and all that. The New York DFS and all that good stuff, that helps you too. We can't do this, or if they come and check this, we might not be so favorable in our outcomes. My biggest thing, too, is I'm so thankful that we're not an international company and I don't have to deal with all that mess. But I think those are the items that help you motivate. It's the stories of others. How do you build on the stories and the experiences of others to help sell your case?

Patrick H.: Piggybacking off of what was just said, is that in addition to being very fortunate and looking around for some wood to knock on, we've not experienced a breach living in the HIPAA PHI world to the degree that others have. But what he just said is, I make sure that those stories get across the Executive Board every time it happens so that they're reminded every day of the investments we make and why we make those investments that we do make. We're fortunate to say that previously we only had been held to the HIPAA standards, but more recently now we're required by the state to achieve the SOC 2 Type II and also align ourselves with the State Department of Information Technology standard, which is NIST. I'm actually very pleased about that because that allows me now to implement some things that I have previously not been able to implement.

Matt S.: Everybody's saying great stuff. But there's two things that I found actually very effective to get the investment and the C Suite and executive buy-in to our whole security platform that we implemented in 2019. One was the cost-benefit analysis. We are in the healthcare sector and we are international. Not only do we have HIPAA and PCI, but we have GDPR, PIPEDA, and a couple of other international privacy laws that have some pretty stiff fines. And some examples of companies our size, I did a real quick one-page comparative analysis. Here's a healthcare companies that are our size that are doing similar things to what we're doing (selling medical devices) and here's what happened when they got breached. Here's the fines that they got hit with. Here's the consequences for our international executives to travel the world there. I'm like, you could get visas revoked, you could get residencies revoked because you're no longer working here. The sheer cost involved in there. And then I got questioned by one of our C Suites, where I said well, what's the actual risk for my stuff being taken? So I hacked his phone. In a few short hours I was able to share some private messages with him and some contact information for the partners that were in our network as well as for some customer data that he had stored on his phone. I sent it to him, private message, of course

this was all on the up-and-up. He knew what I was going to try. But yeah, when I started showing him his data, he's like oh, and what do you want to do to stop this from happening? I said absolutely. Let me get a trial. Let me show you a proof of concept. I got a trial for the Defender stack, upgraded a couple of licenses so I could go through a 45-day trial, installed the controls on his device, and proved while he's sitting right next to me that I was unable to get into his phone because now we had a security solution in place. I also showed that I wasn't able to get into his laptop, his computer, any of his accounts, because our security platform alerts and the alarms were blaring, as they say. A five-alarm fire kind of thing, literally detecting every step that I tried to take through the network and stopping it. Every step I tried to take through his device and stopping it. And I said because we would have this solution in place for everybody we would avoid this many millions of dollars, or tens of millions of dollars in potential fines. I just went over the laws with him, gave him examples, and opened his eyes to the fact that the risk could happen, even though he's like who am I? We're just one company of millions on the planet, and I'm one of eight billion people so why am I special? And I showed him why he was special, and he signed off right then and there and did not put a limit on what I needed to spend. It became a spend what's necessary moment for him without having to actually go through having a breach, actually having a problem, having to deal with legal issues and lawyers and governments. Because it gets nasty. You can get real nasty, real fast.

Brent H.: Making it an investment instead of a cost, right? You've got to change the cost center into an investment center.

Mark B.: Good info. I don't think I'll be able to top what Matt just shared. But one tool we had implemented about a year ago is Black Kite, a cyber-risk platform. A couple of things I really like about that is it provides three different indexes. A ransomware susceptibility index, data breach index, and then they also do some work related to the fair framework to try to quantify the financial impact. I think what's nice about that is it gives you at least a gauge in terms of where you're at from an organization. Then also you can put other competitors in there, other vendors, etc. It at least allows you to get basically information that any hacker can get visibility to for the justification in terms of why, maybe some of the control, some things that you're doing actually makes sense. And then you could show how it improves it. Just a nice tool.

Janet A.: Metrics showing everything you are detecting & blocking is great data to provide to leadership.

Matt S.: Exactly. Show them what their investment is doing for the company to protect revenue generation and enhance profitability.

Brent H.: Alex, we have about 1000 employees and 3 people on our security team. More hiring coming, but that is what we have, which is no where close to enough.

Chris H.: My org size is 1000 and my security team is a half a person. Currently dual role and hope to split soon.

Brent H.: We did something similar to show our passwords are weak across the organization. I called it the "White Hat Hacker Challenge" and we were able to crack the majority of our user's passwords within a half hour.

Matt S.: I did this, lol. Used a rainbow table with 10M most popular passwords, cracked 2/3 of my user's passwords. Changed the PW policy 8 hours later, lol.

Brent H.: We are increasing our passwords to 16 characters now, lol.

Buzz W.: We moved to 12 characters a couple years ago and 16 characters for sec IDs.

Aaron W.: Brent, what tools did you use to crack the users' passwords?

Brent H.: Aaron, connect with me through NOREX. Happy to discuss with you.

Matthew W.: You can crack passwords with Hashcat.

Moderator: Thanks, Mark, for sharing that. The tools are always appreciated. All right, folks. We are at time. A huge thank-you today to everybody who jumped in. It is your participation that makes these work. That's what we're here to do. We'll look forward to seeing you on an upcoming Roundtable 55. Take care, everybody.

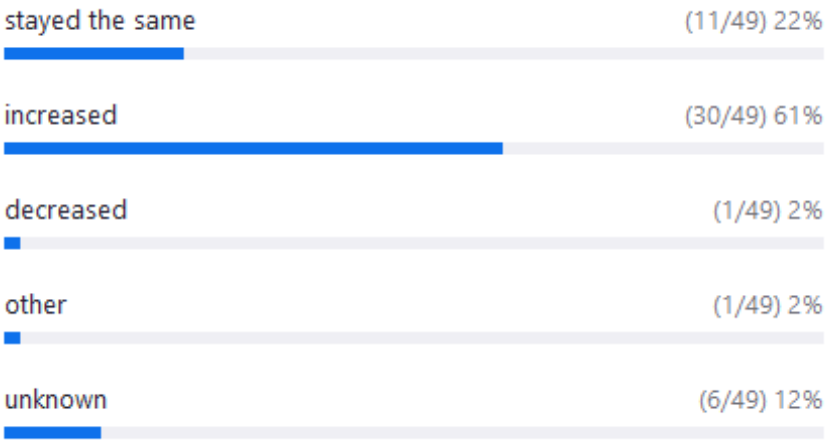
End of discussion

Products / Vendors / Technologies shared in this Roundtable 55:

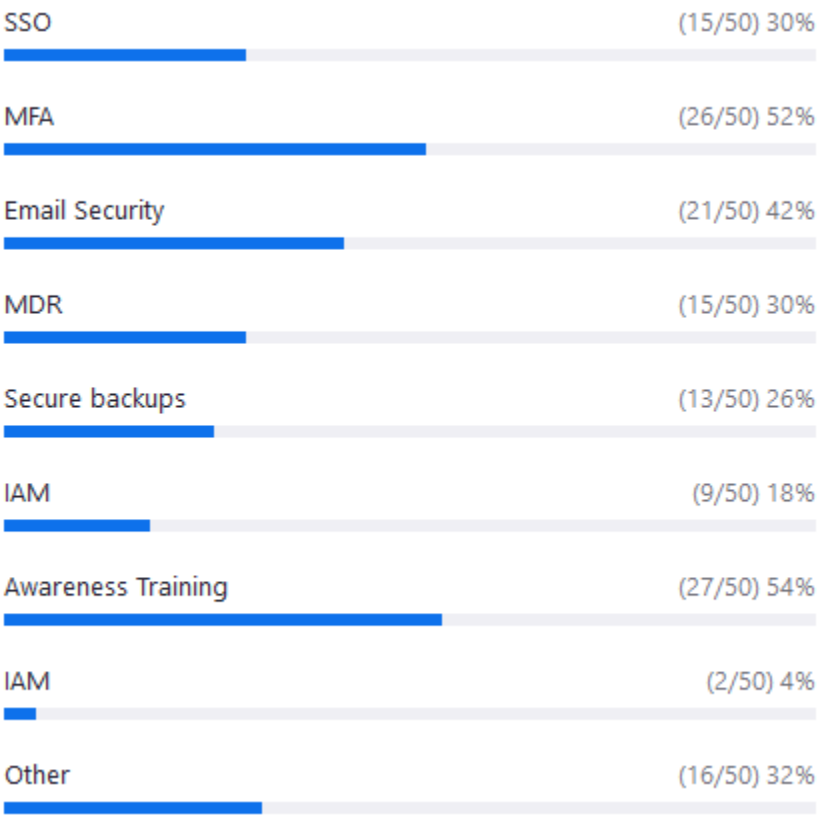
ADAudit Plus
Artic Wolf
Avanan
Barracuda Zero Trust
Black Hills Info Sec
Black Kite
Carbon Black
Cisco AMP
Cisco EM Security
Cloudflare
Cohesity
Crowd Strike
Dell Avamer
End Game
End Point
Hashcat
Illumio
Insight IDR
Insight VM
Mandiant
Mimecast
Netwrix
Nexpose
Proofpoint
Qualys
Rapid 7
Reid Siege
Rubrik
Sophos
Sophos EM Security
Sysmon
Tanium
Trusted Sec

Appendix A: All Poll Results

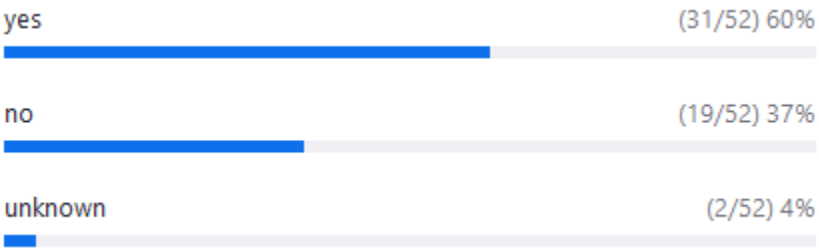
For 2023, our security budget:



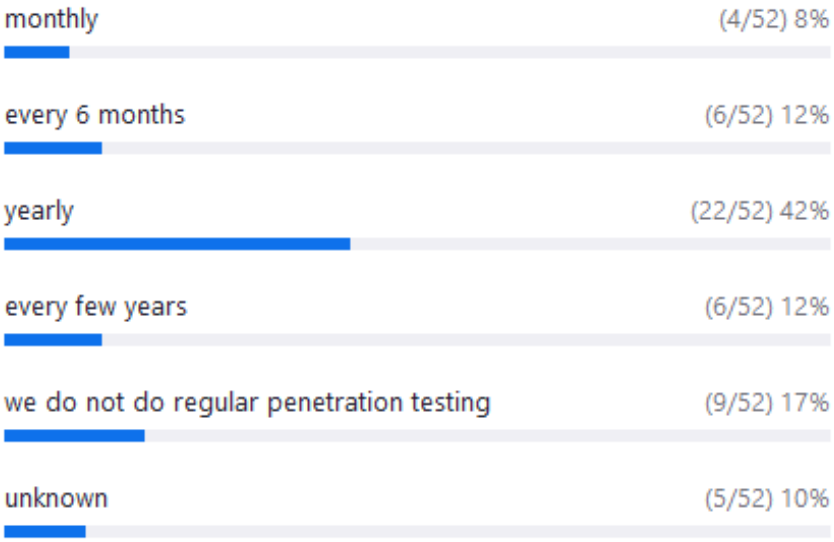
What are your top security initiatives for 2023:



Part one - Do you have an MDR service:



Part two - If so, how often do you pen test:



Do you use open source security tools: