Philip Stringfield (00:00:00):

Good morning. Thank you for joining us for part two of our Business Intelligence webinar series, the journey to becoming a data driven organization. My name is Phillip Stringfield, specialist of health center operations training here at NACHC. NACHC mission of promoting efficient high quality comprehensive healthcare that is accessible culturally and linguistically competent, community directed and patient center for all would not be possible without the service that you provide to your community day in and day out. Today's webinar is titled aligning your data strategy and strategic plan. I am joined by two of the panelists who will guide us through some of the final steps to becoming a data driven organization. Joban Singh, director of business intelligence and strategy at Johnson Health Center in Lynchburg, Virginia.

Philip Stringfield (00:00:46):

And O'Shea Bowens, founder and CEO of Null Hat Security in Boston, Massachusetts, who did a great job last week setting the theme for what's to come today. But before we get started I want to remind everyone of a couple of housekeeping items. The webinar series is being recorded and the slides will be sent to you at the conclusion of the call. So, for those who aren't able to attend last week's webinar no worries. We'll make sure to send out both webinars recorded, and we'll make sure to send the link to where they can be accessed within two weeks of today's date. If you have any questions during today's presentation, please go ahead and use the Q and A section. And in addition to Q and A, we're also going to be using the last 10 to 15 minutes of the webinar for open discussion and peer exchange.

Philip Stringfield (00:01:36):

So, really taking any feedback that you have during today's presentation if you have any insight from how nuggets from today can improve internal operations or as you navigate through COVID-19, looking at really what your health center needs around business intelligence, data strategy and looking at how you can protect your organization. And then just a couple of last reminders for that open discussion we have our race hand feature. So, once we get to that part of the discussion if you have more direct insight you would like to provide to us just go ahead and raise your hand and just make sure your audio is connected and we'll unmute you so you can have direct engagement with everyone. Last but not least we have all of the additional resources for COVID-19. If you have any questions around that or once you get insight or access our archived webinars are going to be all on our website at nachc.org\coronavirus, so that's where everything will be accessed.

Philip Stringfield (00:02:42):

You can access all of your COVID-19 resources there. So, without further ado, I'm going to go ahead and hand it off to Joe Bornstein to get us started with today's presentation. So, I'm going to go ahead and pass the ball now, and Joban you can take it away.

Joban Singh (00:03:04):

Great. Thank you Phillip. Can everybody see my screen?

Philip Stringfield (00:03:09):

Sure can.

Joban Singh (00:03:10):

All right. Well, thanks to NACHC for allowing me to present all this. We're going to be presenting on a light on your data strategy and your strategic plan, how you leverage your data and how it goes hand in hand with finding out the next 12 months to three years of your organization and how they really work together. My name is Joban Singh. I serve as the director of business intelligence and strategy for Johnson Health Center. I joined the community health center space six years ago. I've been in love with it since of what community health centers do for communities all across the country. I lead the business intelligence department. We report on different things such as quality metrics, risk management, and even expansion opportunities. A little bit of what we'll be going in today. And I've served on numerous boards whether on a state level, national level or even local committees as well. Definitely something I enjoy doing.

Joban Singh (00:04:27):

So, the topic areas that we're going to be going over today or what is business forecasting, business intelligence and strategy, utilizing business intelligence in the pharmacy landscape. Specialty services in continuity of care. Going over a few helpful tips that I've learned over my several years of being in business intelligence and strategy. And we're going to be touching base on COVID-19, some of the things my organization doing to prepare for things like televisits and different triage processes that we put into place to make sure the organization contains say operational. So, what is business forecasting? The business forecasting is the model to predict the future where the feature narrowly defined by economic conditions. It combined information gathered from past circumstances. It's an accurate picture of what presents economically to predict future conditions for business.

Joban Singh (00:05:48):

So, it's a combination of what we talked about in the glass webinar last week about taking presumptive analytics and predictive analytics, and combine those together to really see what the future stores and how to really navigate through that landscape. So, business intelligence and strategy. So, how are these two things really interconnected? It's basically decision making and planning. Utilizing the data to help align your strategic plan. The data show the organization's plan is achievable. You know, within your strategic plan you could put all sorts of goals and initiatives into it, but does the data show it's possible to achieve. Building models that predict and optimize the outcomes? Looking at how you could forecast things in different ways or see if things are going to work or if they're not going to work.

Joban Singh (00:06:58):

And how can you bring in other things to it to help achieve your strategic plans. Transforming your organization's decision making. For the organization I work at any major decision is ran through assessment, looking at the analytics. Seeing if that making this decision is right for us from a financial operational standpoint, or whether it may pose a risk to us. So, every decision we make goes through a projection model, utilizing qualitative information to understand the needs and use the data to confirm. So, how did would Johnson Health Center utilize business intelligence for a pharmacy? So, Johnson Health Centers has nine sites and we're varied all around central Virginia. We got a lot of qualitative information from staff, patients that a pharmacy at our Bedford location, which is about close to 38 miles away from our other pharmacy. We had only one pharmacy within the organization, in-house pharmacy.

Joban Singh (00:08:35):

And we got a lot of feedback from individuals saying a pharmacy would do great out there. Pharmacy will thrive. You'll need to open a pharmacy. So, we're going to go through the journey of the things that we looked at to make sure a pharmacy would be successful in align your organization strategy. So first thing we did is we assessed the need. We did a needs assessment of community. Our Bedford Community Health Center is in a rural area in central Virginia. The county has a population of almost 78,000 people. Their area has only two retail pharmacies. And Bedford is 38 minutes away from our original pharmacy and patients that are on the slide may not be able to get their prescriptions at retail pharmacies due to cost, and would have to travel a great distance to our downtown pharmacy, our original pharmacy to pick up their prescriptions.

Joban Singh (00:09:49):

When we looked at the data, about 33% of our slide patients that were utilizing our pharmacy services were coming from Bedford. So, they were traveling significant means to pick up their prescriptions. Then we went into analyzing the data. We looked up the number of scripts from 2017 to 2018 had practically doubled that were read and at our Bedford location. Our Bedford location at that time was a newer location. Overall, 95% of the scripts were filled outside of JFC. The health center capped at 31% of the patients under the 100% federal poverty level within that area. So, we would penetrate aiding a good amount of patients withing Bedford itself, which is on par with the rest of our location. So when we looked at our prescriptions written by JFC providers and filled as a JMC pharmacy 95% of them were walking out the doors to retail pharmacies or other local pharmacies.

Joban Singh (00:11:02):

But we were continuing to grow in the number of scripts we're writing year over year. So, we utilize existing data. We collected the total number of visits at our JFC facility, so our downtown facility. And we looked at all of that. 65% of prescriptions written at that facility were filled at that facility. So, that's a very good number. And then we were looking at only 5% for our Bedford location. We calculated the average cost of the script and projected the average profit of filling each script. So, we ran the projections on it. We did our needs assessment or due diligence. In 2017 we saw we have 1.4 FTE providers at that location. 2018 we have 3.2 FTE providers, full-time providers. Each provider we saw was writing about 10,000 scripts per year. JFC was projecting to capture only 5,500 scripts annually. This projection also included a nine month ramp up period.

Joban Singh (00:12:26):

At our downtown pharmacy we were capturing about 40,000 scripts a year with the staffing we had. We projected that expenses were way too great to be able to support a full-time pharmacist, the full-time tech when comparing salary. And the project was just great to … There was too much risk for us to go in and open up a pharmacy knowing that we were only going to be capturing 6,500 scripts. And it just did not financially make sense for us. But then going and how do we make adjustments to see if we could continue to achieve the goal that individuals within that community wanted and also support the organizational strategic plan and still be financially responsible. And what we had done was we had looked at the number of prescriptions written across the organization. And in 2018 we had 1,000 … 850,000 scripts written across the organization, across nine sites.

Joban Singh (00:13:50):

Currently, we were only capturing 21% from our downtown pharmacies. So, the solution was how about we create a home delivery option for patients that may have difficulty accessing the pharmacy. This

would allow the organization to open up a home delivery part of their pharmacy business and do it out of our Bedford location, the same location where we're only projecting to fill 6,500 scripts annually. This was allow us to be able to support that function out of that pharmacy, and also bring a service to the community that greatly need it. So, with the nine month ramp up period we were looking to see how we would do. And this next slide shows we opened in August, month over month we've almost doubled the amount of prescriptions going right along with what we projected for our first time months, and even surpassing some months of what we were projecting to do.

Joban Singh (00:15:02):

And a nine month period, we would start off at 25% and then work up every three months to 50%, 75%, and then being fully operational at 100%. Sort of passing what we expected to do. We do these types of analysis with anytime we're doing an expansion project. Now in new community health center, we'll do a full deep dive of what are our penetration rates, how is the health center going to look when it's fully up and running and build our staffing models along with that, and the type of facilities that we're going to need in the past several years, especially in 2018 we opened up three new sites with a span of a year. And they're all running successfully and have been going along what we projected for them to do, and really honing into the data and making sure those decisions make sense for you and your organization.

Joban Singh (00:16:16):

Now I'm going to look at expanding access to specialty services and continuity of care. Just a little bit of background on this. Our health center was only known to refer out to offices. We never really had official process of referring into us by other primary care providers for services like OB or dentistry or behavioral health. So, before we open up this referral process to the community, what we also did was create an internal referrals process. In the past, patients were just told to go schedule appointment at the front with one of the specialties when leaving their appointment. What we had come to find out was compliance percentages were low on patients when scheduled and showing up for their appointment. Patients would either not mention anything to the person at the front and they weren't scheduled for that appointment or that they just didn't show up for their appointments.

Joban Singh (00:17:28):

We actually saw once we put this process in place, increase in compliance with pregnant women with a dental visit. We were in the stable digits and compliance when we had our old method in place of go make an appointment with the front when you're checking out. When we put a process in place we saw a very significant increase of having 30 to 40% supplier with those patients receiving dental services, at least one throughout the pregnancy. So, as you see this process, we have more and more internal referrals between our providers that we're able to have a staff member reach out to the patient, schedule with the patient, get the patient in for their appointment. If a patient shows or has any social determinants, they're able to walk them through any of those things that may be coming up.

Joban Singh (00:18:35):

So this is the ladder overall compliance for referrals in between providers to go up within the organization. Next, we created a process forward incoming referrals. In the past we had no way of tracking who was referring to us, which primary care providers referring to us for specialty services, or were patients just being scheduled through our call center. We created a process to track and contact patients scheduled for services. We developed relationships with community providers. If we saw one of the groups were not referring to us for let's say behavioral health, reaching out to them, letting them

know that we offer these services. We were very surprised at how many community providers did not know that we offered certain services beyond just primary medicine.

Joban Singh (00:19:35):

And this allowed us to continue to build those workflows and allow the organization to continue to expand access to some of these specialty services like behavioral health. The projected result increase the number of patients seen by a Johnson Health Center. We really started this process in 2018. And we saw almost a double …. We're seeing double the amount of incoming referrals in 2019 that we did in 2018. And for 2020 we're projected to continue to increase this number of incoming referrals by other community providers. And this process works the same way with a staff member, outreaching the patient, getting them set up for their specialty appointment, and really coordinating that with the rest of the care team being one integrated care team. So, just some helpful tips as I've learned through my career with business intelligence and strategy.

Joban Singh (00:20:53):

View service area information on UDS Mapper. I heavily utilized UDS Mapper. UDS Mapper compiles all the information that you submit to HRSA when doing UDS, and actually maps it out. You're able to see different penetration rates of health centers, number of patients that you were seeing. Number of patients that may live in certain zip codes or certain counties. It's been very helpful to utilize when looking and making decisions as an organization. Based or projections on existing information or other health center data that may be similar to your organization, when we looked at creating a mail-out program, we looked at a health center that's been doing it for many years. And we are realistic with the numbers that they were doing and how long it took for them to be able to continue to build their home delivery program, and what we would need to do and build our projections off of that.

Joban Singh (00:22:00):

Be conservative projections using nine month ramp up period for all new projects. When presenting information to your executive team or either board of directors you want to be conservative with the numbers that you're projecting and continue to succeed month over month what we had projected than to be put in a situation where your numbers may not be matching up with your projections. Pull information and cross analyze data from different reporting systems. When doing this needs assessment on our pharmacy we pull information from our pharmacy software, we pulled information from our electronic health record and even other areas and we cross combine it to see what this would really look like and thinking outside the box on it. Just wanted to touch base on COVID-19 and what my organization has been doing to prep for COVID-19 among many of the other community health centers around the nation.

Joban Singh (00:23:13):

One of the things that we really do we have talked about for many years is telemedicine. Some senators ahead of other centers, some centers it's a completely new concept. Within the last three weeks we have heavily utilized telemedicine getting it launched and implemented and what that would look like for our own innovation. Utilizing telemedicine for virtual visits. One, if you don't have a telehealth program finding the right one for you and your organization. For us, we were fortunate enough to have a part of our EHR, have a telehealth module, and we were able to enable that overnight and start working through the workloads of it. Educating staff and patients on the telehealth tool. Once you get

this tool enabled how did you utilize the tool? How can patients access the tool and use it? Create a workload to map out your telehealth process from start to end.

Joban Singh (00:24:27):

So there's no confusion on who's supposed to be doing what in times like this, when job duties may change around from day to day based on your organization's needs. You try on your process and be prepared to make tweaks as you go. I'm looking at this next slide. This is our roadmap to what our telehealth program is for primary care. And just looking at this now and what this was this morning this has continued to change on who's responsible for what area it is. Going through this when patients calling in are they qualified to have certain types of appointments, or do they need to be seen in person? What visit types do we need to utilize for our telehealth visits having set up fast to reach out to the patient to get them set up for the telehealth program. What are the nursing staff responsible for when they're on the phone with the patient?

Joban Singh (00:25:38):

Having the nursing staff call the patient ahead of time about 15 minutes before, and what information they need to collect whether it's chief complaint or surgical history or allergies. And then at that point, what needs to happen next? They have a health visit and I thought what does the tarps they changed? Or if the patient can't get enabled onto the telehealth module, what do we do at that point? Whether we turn the visit itself into a chronic care management visit, and do they qualify for chronic care management visit, or does it need to be a virtual communication with the patient? And then lastly, what the provider needs to do to be able to code the visit itself and making sure that we're capturing things like consent. Then the HPI location if it's a telemedicine visit versus if it's a non-transit medicine visit. Any questions?

Philip Stringfield (00:26:51):

Thank you, Joban. So anyone who did have a question in relation to today's presentation around our data strategies, business intelligence feel free to ask your questions now or you can save them. Towards the end of our presentation we do have another segment coming in from O'Shea. I do have a couple of questions that came in we can address now. One specifically was around your patient population demographics. Will you be able to give a little bit more insight into the demographics.

Joban Singh (00:27:24):

So, what type of demographics in general are we-

Philip Stringfield (00:27:28):

Just a general patient population. Sorry.

Joban Singh (00:27:34):

So with our health center we have about 24,000 patients. We have a pretty diversified payer mix. We're heavily Medicaid pretty even on commercial and uninsured for commercial and Medicare. And our uninsured population right now it's about 10% with adults and pediatrics where I would say we're about 60% pediatrics, 40% adult.

Philip Stringfield (00:28:10):

Thank you. And I have another question in relation to just giving a little bit more detail in the resources that you use. It says, what resources beside UDS Mapper do you use to collect operational data for your organization?

Joban Singh (00:28:26):

So, with operational data, a lot of it does come from our electronic health record. When pulling different information we're able to access almost any operational data out of our electronic health record and extract that and really make decisions based off that data.

Philip Stringfield (00:28:50):

Awesome. And just speaking to data and extracting, do you have any tips or insight on how organizations could go about storing that data to insure that it's all kind of like locales?

Joban Singh (00:29:06):

So, with data storage we actually have our homes data server that we store the information on. It's a standalone server that we log into. We utilize bridge IT to capture the data from our server itself. It comes in as a mare image of what's kept on the server and replicated over onto a data warehouse.

Philip Stringfield (00:29:39):

Thank you. And then just one last for tool for insight. So, what insight would you give for those who are maybe just starting a BI program or really looking to get it off the ground, looking at some of the examples you showed with utilizing BI for for pharmacy, what insight would you give for those who are looking to kind of get that staff support around ensuring that data is collected and ensuring that it's accurate so that predictions can be made?

Joban Singh (00:30:15):

Great question. That goes back actually to our webinar last week. The biggest thing about having data that you can make decisions on what information you're capturing, that information being captured appropriately. Looking at whether if it's structured or if it's unstructured we installed a new pharmacy system in 2019 at the beginning of 2019. And one of the things that I played a key role and bond that system is, what information is fast to like? What information do they need to select other fields where it's free texts, or it needs to be structured and just having … Looking over your systems to make sure that your systems are set up appropriately to be able to capture information.

Philip Stringfield (00:31:10):

Awesome. Thank you so much. So, with that, we'll go ahead and hand everything over to O'Shea Bowens with Null Hat Security, really looking at how we can take some of what Joban has given us now and really elevate it into how we can use those measures to protect our data. And as we use these for predictions and as we use this to ultimately operationalize what we're doing. So O'Shea, you should have the floor, and I'm unmuting you know.

O'Shea Bowens (00:31:44):

Cool. Can you hear me okay?

Philip Stringfield (00:31:47):

Yup. Sounds good.

O'Shea Bowens (00:31:48):

Awesome. Cool. So, thank you Joban for that. So, what we'll do is dive into the second part of the series from last week and then I'll be focusing more on the cybersecurity aspect, BI and data strategies. What to expect. Today we'll walk through a data strategy approach embedding information security practices into data strategies, and key components of an efficient security program. A bit about myself. Here's the long drawn out part of it of, my name's O'Shea Bowens, currently living in Boston. I'm the founder and CEO of a company here called Null Hat. Actually, I'll just go to this one. Of a company called Null Hat, where we focus on security operations and cyber defense operations. So, primarily incident response, security analytics, threat hunting.

O'Shea Bowens (00:32:47):

And we also provide training to small, medium and large organizations that may look for outside help to either build out security programming or a cybersecurity team, or actually just train transitioning individuals from an IT position into a cybersecurity team. Money is tight nowadays. Data strategy approach. So I will say my presentation may differ a bit because keep in mind I'm focusing more on the security aspect. So, just kind of keep that in mind. I think there were some questions I received last time around the security aspect and how it relates to business intelligence. So, the objective for me is to try to find areas of correlation and share those in regards to building out your data strategy as you move towards incorporating business intelligence into your organization, and really how you incorporate security.

O'Shea Bowens (00:33:37):

But from a data tech strategy perspective, typically what you'll find is this consists of managing, overseeing, and analyzing or developing organizational data to further the firm's strategy. I always try to simplify things. So, from my world than what I've seen with many of the customers that I consult with, not only healthcare but business, but specifically on the healthcare side. This is typically that data strategy is broken down into two different buckets. And that's defensive and offensive. The defensive side is really a goal to minimize downside. You're looking to meet compliance or regulatory regulations and really optimize data extraction, standardization, storage and access. So, if you think about it from a defensive side, it's really what can you prevent actions that you would be interested in understanding how to prevent, let's say data theft or IP theft or patent or formulas that may be of interest to your organization for the upcoming quarters.

O'Shea Bowens (00:34:40):

Really, how do you understand how to build a strategy around protecting those and really creating a defensive posture. From an offensive perspective, that's the goal of gaining customers, increasing sales, improving customer services of. So, this leads back to the first discussion we had around business intelligence. So, if I had to give an awaiting system, I would say it's typically 60, 40 from an offensive perspective. So, the idea of building or incorporating the data strategy with the final objective building out business intelligence is really to really how do we look to obtain more customers? How do we optimize our data that currently exists within our environment? How can we create modeling and visualization to understand where we can become more offensive? Not offensive of more efficient at either raising capital, increase in sales or possible expansion of a company.

O'Shea Bowens (00:35:36):

And then cyber security controls are key mostly in the defensive the sense of data strategies. So, data resources. People versus technology. So, whenever or whatever your primary mission is regarding building out the data strategy, I built an out a data strategy plan to move towards BI or business intelligence. This can be broken down from a people and technology perspective, but also understanding that the people side is really who can you leverage to help you reach these goals, whether that's primarily data scientists, consultants, but moving yourself into a mental position. Something I always like to say in a related to like cyber security is that it's not only the technology that plays a biggest part and how successful you are and your mission is the people. So, when I say people versus technology is really understanding that, that people come up with the primary objectives and goals and you're leveraging technology to implement that and leverage technology to obtain a final result on that.

O'Shea Bowens (00:36:41):

From a structured data perspective, the data that you're looking to ingest or leverage, it's either in two formats as either structured data or unstructured data. Structured data would be something along the lines patient information, billing data. Unstructured data would be inherit instructors around letters, discharge summaries, sometimes even medical trial information. If you were to move more towards raw logs, which we will discuss a bit further down the line that's really data generated from like sensors also that you may leverage from a medical device perspective. So, if you think about like pacemakers that are leveraging Bluetooth to communicate with a central console center console within your hospital that the information that they are beaconing or extending to that console is typically some type of data that's in a raw format in regards to the logging.

O'Shea Bowens (00:37:45):

A central source data versus a multiple sources. So this is moving back to the data that you're ingesting. Is it coming from a single source or is it coming from a stage where it's a bit conflicted as there's multiple sources of multiple sources from maybe a console or maybe a server that is sending data to a central repository. One of the things you would like that you should potentially look into is this, your end data resources are positioned in a way that they can be used, shared, shifted and efficient are kind of three marks that you would like to hit. The shared aspect is really the use of data and analytics to infill these scaled and operationalize with applications to two thousands of small decisions.

O'Shea Bowens (00:38:26):

So, think about it from, I had data from … Going back to our example, I have data from this pacemaker in regards to this pacemakers uptime, in regards to when this pacemaker may receive instructions from a console or from a doctor or from a nurse, or when this remote pacemaker may need to update its current operating system. All of these smaller, smaller pieces of data needs to be digestible to someone maybe IT staff, or maybe even a nurse, just to get readings from it. But all these smallest uses of data would allow this individual to make a decision that would allow the best patient care. So you're taking the smallest small data and you'd populate in that data into another resource. Whether that's a BI tool, like a Tableau or some big data analytics tool. The idea idea is I'll try to normalize this data that's coming from multiple places and also in different forms.

O'Shea Bowens (00:39:29):

You want to ensure that you can shift easy with this data. So you want to ensure that and when it's time to make that point, to find that single pane of glass or find that or move towards a centralized repository of data, you should be in a position where you can essentially point to a new resource or a new repository and send that data without having to create too many smaller projects to either clean that data up or reformat that data. You want to be sure that this is efficient, the business impact contributed by data and analytics is continued to be measured through sets of KPIs. So, if you can't measure this or if you can't really understand where you need to improve or where deficiencies are, the data is likely not as valuable as it requires more time to clean up and centralize than it would in another form where it's easily readable to a secondary data system.

O'Shea Bowens (00:40:27):

The types of data you're going to be looking for, from a healthcare organization perspective you're looking at medical supplies, potentially treatments, patient illnesses, PII, patents, these data sources, the data sources that you would likely leverage there or in the EHR arena or electronic healthcare records arena. And again, this data is unstructured or potentially structured or not well defined at all. And once you actually have this data of what are you doing with it, you're moving into, this goes back to part one, but you're moving back to … You're moving towards a position where you can ingest this data or forward this data, or place as a central repository to feed into a BI tool, whether that's Oracle or SAP. What I try to convey to customers or individuals in conversations that are other technologists is finding the individuals to do this it's very scarce. Finding individuals with PhDs in statistics or mathematics or computer science that can become a very scarce. Scarcity.

O'Shea Bowens (00:41:31):

So you may have to look to consultants. If I had another slide to speak about this, what I would say is you want to ensure that you have that focal point on the structuring of your data. Because if you are in a position where you have identified a tool from a BI perspective, but your data is instructed or unstructured and you don't have that resource, it's going to become a lot more expensive to bring in a consultant to help you reach this goal if certain items haven't are even checked off via their structured or unstructured data perspective. And once you actually have these different pieces in place, you understand what your central repository would look like. You understand what type of data you're pulling over, you understand what business intelligence tool you're going to leverage try to focus on an MVP. If you're unfamiliar with that term, minimum valuable product.

O'Shea Bowens (00:42:27):

A good example that I like to provide is like myself working at a startup currently, and also working in previous startups when we're building out applications that we would like to either take the market or raise funds for. It's not that we need like 80% of the functionality that we envisioned for that application before we can actually take it to market. It's really, do we have 20 to 30%? What are the easy wins that we can knock down to prove value and to showcase our full capabilities? The same type of mentality can be applied towards the data strategy for a healthcare organization. So, going back to what I stated earlier in regards to the data structure, the tools, the overall goals, looked for those easy wins.

O'Shea Bowens (00:43:11):

Maybe you're not currently at that time period in the position where you can fill it out, 50 to 60% of your use cases, but you can do 20 to 30% of those and then actually showcase those as success cases and provide value. Embedding information security practices into data strategies. So, the healthcare

field is … It's a pretty unfortunately targeted sector, especially within the US, but this is worldwide. But it's a fairly popular and targeted sector for cyber criminals as it stands now. Healthcare organizations are simply prime targets for hackers, often due to the incorporation and the use of older technologies. When I say older technologies it's not necessarily from a BI perspective, move towards the technology that's in place that helps your organization actually run, whether that's older Windows servers or older Linux servers.

O'Shea Bowens (00:44:14):

These systems are likely out of date, out of patch. Then there's vulnerabilities that exist in which cyber criminals identify and take advantage of. The Pullman Institute did a cost of data breach study from 2018 and found that in most breaches from a healthcare organizational perspective costs up to about $400 per record loss. The 2019 numbers, I think it's about 520 per record loss. And this is really due to a simple fact that healthcare records are a bit more valuable when it comes to selling these … Selling healthcare records is much more valuable than selling stolen credit cards. Stolen credit cards can be called in by the user or by the customer to let's say MasterCard and you call and say, "Hey, by the way, I lost my car and I was on vacation in Paris. I can't find it. I see some weird unknown activity.

O'Shea Bowens (00:45:06):

I didn't buy $5,000 worth of Louis Vuitton shoes," or whatever it may be. And once the credit card company actually counsels that card it's no use to any other hackers or individuals that have purchased your credit card information. PII or healthcare or personally identifiable information on the other hand, it's much more valuable because the shelf life is much longer. It's harder to change your social security number. It's harder to change your address. It's harder to change your name. And when you couple, all three of those together it is ripe with opportunity for identity theft and other nefarious behavior by criminal organizations. Healthcare organizations typically face threats in a few different areas, primarily phishing, hacking of ransomware. Out of the list I have provided here typically fishing is one of the top ways that cybersecurity criminals into the organization and via a specialty crafted email that looks very normal.

O'Shea Bowens (00:46:05):

If you're a salesman or you're in sales, it looks like something where you could potentially perform your job and make a bit of money because someone's may be interested in a product that you may have. But in reality, the email is either embedded with malware or they're pushing you towards a website that they'd like you to click on that takes you to a malicious website where there is malware baked into the website. So, if they can't target you from the email side and hope you click and download the document, they're hoping to target you by pushing you to circumvent your own security controls and navigate to a website that is malicious. And they're really kind of … The take back there, what I did, the primary take away from this and leading into the remainder of the of the presentation is thinking about budgeting and thinking about how much it costs to build out security programs.

O'Shea Bowens (00:46:57):

Typically on average the average security cyber security program budget for a medium size business is upwards of 400 to 600,000. Naturally this goes higher the bigger your organization is, the more money you have. But from a healthcare perspective, look at that 400 to like $600,000 marker. And then really kind of ask yourself, from what I know right now within my organization, is that amount of money something that's attainable to build out security of it is great. If it's not we can dive into that in a

moment. Due to the types of attacks that the healthcare industry is acceptable to the repercussions range from mildly annoying, whether your website goes down, but it comes back up in about 24 hours to dangerous from a life loss expectancy be about your whole hospital system is down and now you can't actually care for the customers within your building or within your hospital, within your clinic.

O'Shea Bowens (00:48:06):

The worst cases that we're seeing right now currently are typically ransomware events that are targeting hospitals and healthcare. If you think back to see there was stigma that was breached, which is a Chinese or Singapore, a healthcare company and they suffered a pretty bad breach from a ransomware perspective and lost data and had to shut down temporarily. There was also the case in Beverly Hills in 2009, 2010 timeframe where attackers hit the hospital with ransomware and completely shut down services within the hospital. So the hospital couldn't rely on anything electronic at that time and period. They had to totally shift back to paper records and paper forms to complete their day to day tasks. Like I said before, it can shift from that mildly annoyance to, "Okay, I think something's up on our website."

O'Shea Bowens (00:48:56):

To, "Oh my goodness, what did we do now? All of our systems are inoperable and we can't use them. What's our next step?" But the silver lining is when you're moving down the path to when you're creating your data strategy program with the ultimate goal of incorporating business intelligence into your healthcare organization, you have this chance to kind of step back and take a 5,000 foot overview of not only your goal from a security perspective, but also what's the goal from the BI perspective? Why are we looking to move towards that? We've already mentioned a couple of different reasons why you looking to move towards incorporate in business intelligence. But now it'd be that time if you have an individual that is in charge of security for your healthcare organization or the chief information security officer, or a CSO.

O'Shea Bowens (00:49:44):

Or if you just have a manager that's in charge of it or an it manager who may not focus a 100% on security, but maybe 10 to 20% of their role is security base. Now's the time to take a step back and really start to ask yourself these questions like, "What is my current security posture? Do I understand the entirety of my environment? Who's responsible for specific areas of our IT infrastructure and operations? Do we have a disaster recovery plan? What type of protected healthcare data do we have in regards to PII on medical records? And how are we truly, truly protecting these types of systems?" And the objective here isn't necessarily to paint a negative picture of your capabilities is to approve upon them.

O'Shea Bowens (00:50:30):

The advantage you would have in this position when you're planning out the data strategy and BI side is you can potentially stretch those funds from BI perspective to a cybersecurity or information security arena and tackle the same task as you're incorporating different types of logs and different type of data. You're just adding different data sources that may be more valuable from a cyber security perspective. I'll dive into that in a second or two. But think about what happens when you come to either a board or a CEO with a budget from cyber security. Typically you're told it's too expensive. We don't have the budget, we don't have the people, we don't have the time, frankly. Another option which I help customers walk through this is, let's think about a major project that's underway. How can we attach or attach the security purposes to that particular budget?

O'Shea Bowens (00:51:31):

Maybe we don't get 90% of what we need from a security perspective, but we get 20% and 20% homeless protect us. We'll dive a bit more into that aspect. A key data component. So, three different areas of focus, especially from a data perspective when you're trying to pitch security can be again levied or leveraged or piggyback on top of the specific data components goals that you're looking to express from a data storage perspective. So you think about data storage and accessing those centralized sources, facilitate efficient access for both structured and unstructured data. Okay, great. When you have data flow lineage that's optimizing path over which the data flows from an organizational to minimize redundancy in an unauthorized use when you're thinking about your data standards in regards to the life cycle of your data, the format of your data.

O'Shea Bowens (00:52:28):

These are the questions that you're already asking in your data strategy planning that you've likely pitched to your C level or your founders or your board of directors. You've already asked these questions. Now, flip it and begin to ask these questions from an it security perspective in regards to cyber controls. All right, so going back to data storage and access what type of user access management system is common from an IT perspective? In the security apparatus understanding who has access to what is that's job number one. At the very minimum when you're attempting to build out a cybersecurity program or information security program you need to understand who has access to what data. But I think this is one of the most important points to drive home when you were actually moving towards constructing your data strategy plan.

O'Shea Bowens (00:53:19):

Because when you identify valuable assets or valuable pieces of data that are important to feed into your BI tools, most likely if it's valuable to you it's valuable to someone else. So it's asking that question around who has access to what could save you a headache down the line if your organization, like we just saw from the statistics perspective becomes a target for hackers, which we previously discussed that healthcare organizations are a prime target for hackers. Thinking about the data flow. So, in regards to where that data is on your network or within your systems, how does that flow from network to network, from server to user machine, how is that data stored in regards to presenting it from a front end perspective?

O'Shea Bowens (00:54:08):

So when the user clicks on a link from an internal application to view this critical information, it would end at BI tools, thinking about how that is presented from a server, from raw data to server to use your presentation on the front end via like a web gooey. All you're doing really now is applying it from a security perspective. So, not only are you worried about how the data trend this is across the environment. You want to understand within your environment how could you potentially segment certain aspects of your network or certain parts of your network from a security controls perspective. And data standards. So, that's really understanding how the data is served up and how the data is queryable whether that's with Java or whether that's Python is your data in Excel or PDF. Whenever form or whatever standard they may exist in you would like to understand how you can bake in security controls around that.

O'Shea Bowens (00:55:05):

One of the areas where I see more organizations and customers that I've worked with start to move towards is really having some type of data like is essentially a system or repository of data that's stored in natural raw format of an object blobs or files. And in simple terms a data like is basically a massive platform, a platform where you store massive amounts of data that you've targeted and that you can feed into either other analytical tools that are searchable, that is queryable or that you have. A specific project we moved to look into leverage that, going back to offensive and defensive data types and data structures of your look into determine where I can make a bit more money or how can I help more customers for a smaller amount of resources, specifically around what's happening now. And what you're hearing with ventilators.

O'Shea Bowens (00:55:58):

I imagine there are many healthcare organizations that are running some type of analytics to understand the life cycle of a ventilator if the output is beyond the normal capacity. So, let's say a ventilator is only meant run 18 hours out of the day. What happens when you need to run them at 24 hours out of the day, and you need to add more than one person. Those types of analytics could be performed, but then a data leg up and then pushed to some type of a business intelligence tool. But at the same time, so we're always thinking transition, transition. "How can I attach myself to the budgetary aspect from a business intelligence and data strategy perspective?" Instead of thinking about the data that you would ingest from medical records, PII side, you're thinking about data that's currently exists within your your current IT organization.

O'Shea Bowens (00:56:52):

So, you're looking at access logs, user authentication, networking logs, SIM or a security event information management system logs. And it's not necessary to state. You need to grab all items that are listed here. But again, you're putting on that hat of, "What is the quickest win that I can get to?" "How do I win quickly?" "How can I actually pull down data that my it operations can provide to us?" Pushed into our data lake, run reports and get bat and then begin to understand, "Hey, it's something fishy kind of going on in regards to who was accessing the sense of the data that we've targeted that is being forwarded into our business intelligence. Who's accessing our formulas? Who's accessing our patient names?" "That's not a nurse. Why is Michael from HR looking to understand what medications that we're currently ordering for each month? Or who our suppliers of that medication are?"

O'Shea Bowens (00:57:47):

So you begin to create these use cases that are fast wins that you can knock down and have provability with. And when you actually have these type of logging in place, or I'm sorry. The data in place that you can forward to a data Lake and leverage that for a security purpose, you begin to find the fishy things that go on inside of your network. Majority of my jobs that I work with from a consultancy perspective are clients that I work with it's either comes in proactive or reactive security. So, when I say proactive security, I'm coming in and helping them stand up security controls, build out a security framework, processes our procedures, and bring in security tools. Another half of it is more than the incident response side, which is okay, there's already been some type of record or some type of log that indicates there's a bad guy in our system. Or the customer knows they've been hacked and they're looking to clean it up.

O'Shea Bowens (00:58:49):

And what you typically find I'd say about 40 to 50% of the time with a customer has already been hacked and they're looking to clean it up. I would come in and I ask, "Okay, well, do you have a central repository of logs that you're leveraging for monitoring and alerting that in place so I can take a look at?" And the answers more often than not, no. So, it puts me in a position of, "Okay, now we have to go dig back in time, dig through artifacts on your disk or on your servers to try to understand where that specific attacker, where he or she entered the environment and how they got in. But if you take the data like example, when you're able to shift what you're thinking, again, shifting the type of data that you're incorporated into the data lake, if you can begin to run those reports to look for like spell logins.

O'Shea Bowens (00:59:34):

You're looking for individuals that access incident data. You're looking for data leaving your environment. Data leaving your environment is one of the clear cut, canary in the coal mine methods of, "Hey, I think something has definitely happened because we're seeing our formulas, we're seeing patient information leave our environment and these aren't going to third parties that we have business relationships with. It's going to some weird websites that our IT these guys were saying is in Pakistan or Russia," or wherever it may be. But if you don't have the ability to understand where your data is going from a networking perspective, if you're not in a position where you can understand when data leaves your environment, you're losing the battle essentially.

O'Shea Bowens (01:00:19):

Because that's something where attackers will take advantage of any moment they choose, pretty much majority of the time, always think or something I try to push to customers is whatever may happen from a cybersecurity perspective, the objective of the bad guys is it gets something outside. So, naturally they need to get inside in order to obtain data, but they have to move outside of your environment. They have to move the data outside so they can sell it or repurpose it however they see fit. And you start asking yourself these questions around, "How do I know when data leaves our environment? How can I identify that and how can we place controls in place to stop it?" If there's anything I'd leave you with, I would say asking those questions of your IT staff around exfiltration would likely be a job number. Actually job number two. Job number one would be understanding what access controls are in place since your sensitive data.

O'Shea Bowens (01:01:13):

Job number two, understanding how data leaves your environment and is it possible to identify that? Mapping out viable security controls? Excuse me. So when you are … Again, going back to the time and the money side of things when you're looking to incorporate a data strategy to recess to reach those business intelligence goals, that's also a good time for you to piggyback on understanding what type of frameworks from a security perspective can we bring into our environment. If you already have an environment where you're leveraging this and NIST, National Institute of Standards and Technology or ISO to actually build security controls around you're a healthcare organization, that's great. If you're not really start to ask those questions when you undertake bigger projects, specifically bigger projects like bringing in BI where you need to incorporate some type of data strategy, what type of frameworks we have around security.

O'Shea Bowens (01:02:04):

Again, going back to if the data is valuable for me it's likely valuable for someone else. And then understanding from the security components effective, "How can I bake in some of the easy wins? How

can I pull in firewalls? How can I build that out? How can I build out of antivirus software?" And I know a lot of times when I speak about these things to people that don't necessarily concentrate in the cyber security perspective, the first thing that goes off is money, which is as it should. But some of these components are also open source and free. It just requires a bit of human equity and use sweat equity to actually incorporate them. So again, if you don't have a security team maybe you can sit down with your it staff and really begin to understand how they can help you build out these tools and capabilities.

O'Shea Bowens (01:02:52):

So, really help you stay safe, but also ensure that that investment that you're spending to incorporate business intelligence, doesn't go out the window if an attack were to happen. And putting this together from a data lake perspective, again, you're looking to understand firewall logs. You're looking to understand active directory logs. You want to ensure that the data is structured in a way that it is digestible and usable to individuals that are outside of maybe the data scientist roles. Again, thinking about what departments are going to touch these reports, or what departments are going to run reports from the BI tool, understanding what type of timestamps are available so you can go back in time and understand who's touched what. And then you are essentially pumping what you have on the data lake perspective into more of a monitoring or security mining fashion.

O'Shea Bowens (01:03:38):

And when you start to like incorporate security monitor you're thinking about, how can we pull in those active directory logs? So identify multiple failed logins to this particular system that has this sensitive data. Why is O'Shea looking to access again our formulas or maybe our medical supply chain information? That's not something that he has access to, nor should he wants to do that. That could be an indicator that something has gone wrong. If you're monitoring anything around intellectual property and you're also monitoring how often your data structures may shift. So when you receive logs that are out of a better unstructured, that are a bit out of the norms this could be indicated that someone has touched something and made a mistake and reformatted your data. I like to always try to say that yeah, hackers are great.

O'Shea Bowens (01:04:27):

There are some really, really talented individuals out there. But there's also just normal people that make mistakes on the keyboard like anyone else. And some of those mistakes could lead to visibility of you understanding what's actually going on inside of the environment. Then once you have the monitoring in place, you're looking for security alerting, you're creating an alert levels of service level agreements amongst other departments within your environment. Then from those service level agreements you want to ensure that like, hey, if we have an alert that happens from our firewall our IT staff will communicate with at least one individual in management. One individual and management will begin to communicate with our C level and so on and so forth down the chain. So, until the investigation is totally completed.

O'Shea Bowens (01:05:16):

So you have service level agreements that range from 28 hours to 72 hours of responding to those types of alerts. And you also want to incorporate severity levels into into your security alerting. So understanding, hey, if we see something that's a severity one versus a severity three what type of response and what SLA are we operating under for those different severity levels? In conclusion, your data strategy plan kind of dictates a strength and the value of your business intelligence. So, if you don't

have a strong data strategy plan it becomes a bit more convoluted and difficult to move towards incorporating business intelligence tooling as the data is, as you need certain pieces of data that are essential. But going back to structured and unstructured, but you cause more hiccups out a data strategy plan. Look for immediate wins, quick wins, going back to that 20 to 30, 40% rule versus 80, 100% rule.

O'Shea Bowens (01:06:20):

You're looking for ways that you can prove value quickly as an executive or management member, thinking about where you can incorporate security into your data strategy. So this goes back to understanding when bigger projects are in play of when maybe money is a bit tighter. How can you hit your wagon alongside whichever department is responsible or has pitched the idea for incorporating some type of new tooling or business intelligence tooling that requires a bit more man hour. How can I piggyback my causes onto that to build out more security controls? And going back to the data lake example. No matter what central repository of what system you're leveraging to capture all your data a log is a log as a log. So it doesn't matter if it's a patient record log or if it's a log for your networking activity.

O'Shea Bowens (01:07:15):

There's always a way to structure it. There's always a way to clean it up. And there's a way to incorporate that into your overall monitoring capabilities. And security is, it's difficult and it can be expensive, especially with the amount of tools that are out there currently. Some tools can brains in to a couple thousand to 100,000 for full implementation. But it's necessary in today's world. So, taking the mindset of how can I protect my team and organization is coming from a guy that practice in cybersecurity for much his whole life. I would say that's essentially mandatory and our current landscape. Any questions?

Philip Stringfield (01:08:00):

Thanks so much, O'Shea. I say I really appreciate your presentation. And really being able to bring out a lot a lot of practical strategies and kind of concepts that healthcare organizations, organizations alike and can really start on now. We do you have a couple of questions coming in? So feel free if you have any questions related to any part of today's presentation. You can go ahead and send them in now. I'll be sure to get them for you. So it says, first question coming in, what statistical methodologies are centers using for predictive analytics procedures? So this could be for O'Shea and Joban up here. I'll unmute you as well. So that if you have any insight you can provide that as well. So we should be all unmuted. So the question was, which statistical methodologies are centers using for predictive analytic procedure?

Joban Singh (01:08:52):

So, what are the methodology that we use right now for projecting those accounts and what things are going to look like is standard deviation. I know a month over month things can fluctuate. But having a solid projection of where things are going to be able to go, and changing the format of your formula right now all these accounts have been affected. So our center deviation would be off.

Philip Stringfield (01:09:25):

Awesome. Thank you. And then a question for O'Shea as well. And Angela Bonzo term it just kind of currently your organization is doing. But I just had a question around currently with COVID-19 and

organizations really switching to working from home and then also switching to telehealth. What type of practical safe parks can they really look at the staff kind of accessing from remote areas? And then also doing the same from their own organization, kind of doing that same outreach to patients.

O'Shea Bowens (01:10:10):

From a security perspective of this is a conversation in which I think a lot of companies are forced to have. But understanding how individuals can... Their day to day jobs. So understanding how they can leverage their VPN, which is a virtual private network in order to authenticate on their healthcare organization or just an organization in general. Using a VPN to authenticate to those systems. One of the things I'm seeing now the customers when they start asking these questions around COVID is really understanding how can they tighten up their email filtering. One of the unfortunate results of COVID-19 outbreak has been cyber criminals are taking full advantage of the opportunity to leverage more efficient attacks. So what you're seeing is emails claiming there's, 'Here is a cure for COVID-19 that you can make in your home. There's home remedy. Click on this link.'

O'Shea Bowens (01:11:08):

And cyber criminals or hackers attempt to leverage more phishing campaigns organizations have to constantly keep up with, "Well, how tight are our email filters? Do we have the ability to act if one of these emails slips through the cracks? The odds are at least one or two are going to reach a user. Do we have the ability to zero down on that specific user's machine to understand what has happened from a malicious activity perspective?" But what I recommend a company to do, ensure that you have a VPN, ensure that you're updating your users' passwords are somewhat complex, longer passwords with alphanumeric combinations, but also ensuring that you understand where your users are. If you have a VPN and your company operates in the US, should you really see someone from Iran trying to access your network via the VPN?

O'Shea Bowens (01:12:02):

That should be a big indicator that something is wrong. So doing the simple things first. Locking down access controls, locking down the VPN, and then more password complexity.

Philip Stringfield (01:12:15):

Awesome. Thank you for that insight. Joban, did you have anything to add, just kind of what's currently going on at your center?

Joban Singh (01:12:23):

Yeah. Definitely 100% support O'Shea on the statement of having a VPN. Our health center, our employees when they're working remotely having access to the EHR need to go through our VPN to be able to get access to that patient data. Also with the features that you may be using to provide telehealth services, making sure that they're encrypted, HIPAA protected, making sure that you're not using a third party app that you may not necessarily have a business agreement with.

Philip Stringfield (01:13:00):

Awesome. Thank you for that as well. And then just kind of piggybacking off of that, I'm just kind of from my insight, I want us to know, as some health centers with their EHR as they moved to the cloud, do you

think like times like these are good to have your information in the cloud, or is there anything that organizations could look for if they do kind of utilize those systems?

O'Shea Bowens (01:13:26):

I think having it in the cloud allows you to expand quicker. So, we have message span. So let's think about leveraging like some type of business intelligence tool. If you need to copy more data, or shift more data to feed into those intelligence tools. Many of the cloud providers, AWS, Azure, Google Cloud provider, they have internal tools that help you scale out. And also the offer internal security capabilities too. So, in general I think it's kind of a good time to go to cloud, but systemically now if you're going to have more remote workers, maybe the people that physically you can't go to a data center be having things in cloud available is a great resource.

Philip Stringfield (01:14:12):

Awesome. Thank you again. I'm just going to check to make sure we don't have any other questions coming in from the field. But we definitely want to use this time just to share any information or resources that we have right now around COVID-19, or even just taking today's presentation and kind of what you're currently doing in your organization or how we can elevate what we're working on now. So if there's any insight anyone would like to provide definitely feel free to go ahead and put that into the chat box. Or like I said, if your audio is connected feel free to raise your hand and I'll make sure to unmute mic so that way you can have direct engagement. So, I will give it some time for those who might have additional questions for today's presenters or would like to provide some discussion throughout today.

Philip Stringfield (01:15:02):

But if not, I'm not going to take too much more of your time me give you a little bit more time back to your day. So, I will leave it open for a few minutes and then we'll see where it goes from there. And then of course, if there's any additional insight you O'Shea or Joban would like to add feel free to jump right on it. All right, everyone, well, thank you for joining today's webinar. Again, we'll make sure to send out the recording within two weeks as we get off this call you will note that we have a survey, so if you could please just complete that. If you don't see it on this screen, it will be in your inbox shortly. So once again, just feel free to fill that out. Let us know how we did today. If you have any direct questions feel free to reach out to me directly, and I will get your questions answered.

Philip Stringfield (01:16:04):

In addition, like I said before, if you have any questions around COVID-19, if you like to access some of our resources we have archive webinars all of this at your fingertips, just visit nachc.org\coronavirus. Looks like we have a question, or was that just an answer? Oh, Nope. So, that's where you can access our coronavirus resources. And then, like I said, if you have any direct questions, feel free to reach out to me. I'll be sure to send out the presentations from today. And everyone enjoy your evening. Take care.