HCLTech Trends and Insights Podcast

00:00:07:07 - 00:00:34:01

Hello everyone, and thank you for tuning into the HCLTech Trends and Insights weekly podcast where we'll be discussing the latest key technology stories and events that are impacting on disrupting business and society. I'm Nick Ismail, the Head of Brand Journalism at HCLTech. I'm happy to be joined by Prabhat Kumar, a seasoned Global Cybersecurity Leader and Senior Director at HCLTech.

00:00:34:02 - 00:01:05:06

Prabhat, how are you? Hi, I'm doing fine. And how are you? I'm all good. Thank you so much for joining us today. Well, we're going to be discussing the main cyber security trends in the life sciences and health care industry, which is an increasingly popular target for hackers. So just to kick off, what is the current state of the cybersecurity landscape in the life sciences and health care industry?

00:01:05:06 - 00:01:36:04

What's unique about this industry compared to others when it comes to cybersecurity? I think that's a very interesting question, Nicholas, but I think when we are talking about life sciences industry, I think we have to start looking at them into three let's a kind of a silos in which all the organizations in which they're working, I think the life sciences and health industry, basically you will have a Research and Development Board offered.

00:01:36:06 - 00:01:58:05

Then you will have to look at manufacturing and supply chain part of the organization, and then you have to look at the commercial organization. Now you will have life sciences organizations, which might be just in research and development, or they might be in research and development and manufacturing and supply chain, or you might be having Albany issue which are on the commercial organization side of things.

00:01:58:07 - 00:02:28:02

Now when I then I talk about life sciences and what is happening across that trend of well, there are a lot of new digital and EEA adoption and data driven adoption which is let's say happening in the life sciences organizations. And, you know, you talk about, let's say within the research and development, we are talking about genetic data training, we're talking about microbots, we're talking about real world data like clinical trials.

00:02:28:02 - 00:02:51:04

You're talking about using AI or the big data discovery, right? We have been seeing that how IaaS are being used to develop or this, you know, identify the antibiotics for the one for the different diseases as an example. Then on the manufacturing and supply chain, we are talking about industry 5.0 or continuous manufacturing on mobile manufacturing as well.

00:02:51:05 - 00:03:17:14

I don't know about these are the new trends, you know, but we are talking about and mobile manufacturing for the organizations of other countries specifically where you can set up big plants. And the most interesting part of the whole immature organization in the lifecycle of industrial, if you have an Apple Watch or if you have a, you know, Garmin, not if you have any other, you know, wearable tech devices which are collecting your health data.

00:03:17:15 - 00:03:44:09

I think again, that is something which is an important part. You know, you have people who are having diabetes. Type two were having those, you know, diabetic monitors within. They're going to be adding within their body implanted or effectively monitor, you know, having bands to monitor their levels of insulin through the different apps and everything else. So when we use the term Life Sciences organization, we have to look at that.

00:03:44:09 - 00:04:18:09

How different parts of the these organizations are operating and how different cybersecurity threats which can be there for different parts of the business but in this with this larger scale of organization. Now, if you ask me that, how is the trend looking like? Of course, since, let's say, over pandemic, that the last couple of years all the organizations have been hit by, let's say, malware attacks or an increase in the cybersecurity attacks.

00:04:18:11 - 00:04:48:09

And Life Sciences organization is not afraid of what we are seeing is that there are top eight brains, you know, which are actually increasing in the life sciences organizations in the cybersecurity perspective. One of them is like life sciences organization, whether in the research or development or in the commercial and modeling law in the manufacturing, they are adopting a lot of public cloud and the usage of public cloud.

00:04:48:09 - 00:05:16:08

So the whole cloud security becomes a very important part of it. Then, since they have access to a lot of customer data, especially in the wearable tech space or creating the medicines which are specific for your genetic condition, like data privacy, identity, access management, and of course the whole zero trust kind of a trend in the cybersecurity becomes a very important area.

00:05:16:08 - 00:05:43:04

And my sites in the industry then security automation is a very important area because the amount of data in which the life sciences organizations be made and the reach of that data is beyond the boundaries and would a good example of clinical trial, it's that happening. So you have a lot of data which is related to the patients and if that gets leaked out, then that becomes a big challenge for any organization.

00:05:43:05 - 00:06:06:13

So I mean, that becomes a very important part that how do you automate the security within the organization and with that culture, the whole point of privacy rights, monitoring, privacy and the other area, which is very interesting to talk about, is the resilience about how organizations typically have a how about thinking that I want a business continuity plan?

00:06:06:13 - 00:06:32:13

Eduardo Disaster recovery. But this whole avenue about thinking that in case you are headed by a rather some better forum out of that, how resilient are you that how securely you can bring back the data that's not about how soon you can make your data available back, how securely you can bring back the data, the right data, know the right integrity you something what is important.

00:06:32:14 - 00:07:01:04

And as the trends move towards expanding boundaries of health organizations or the sad about implanted security chips microbots you know speed of self-delivering medications through let's say their insulin provider in your body and you know you know it can go ahead and provided insulin dosage at the right time control to the app the boundaries all the life sciences organizations have now started increasing.

00:07:01:05 - 00:07:24:09

So it becomes very important that, oh, all these security devices are monitored, managed and, you know, secured in case you have a security flaw in the design that you had done. Maybe they knew as I walk because I was you know, that when you are developing something for life sciences organizations, sometimes the research and development may happen for, you know, five years plus, right?

00:07:24:10 - 00:07:57:10

So that that's the nature of the life sciences industry. You know, what we talk about and Brant Nicholas, thank you. And I want to pick up on a couple of things that you mentioned. And just to start, okay, so we're talking about an increasing amount of patient or clinical trial data. Obviously, there's a distinction between life sciences organizations and health care organizations, but there's more data being generated, valuable data being generated across those two, and that's particularly attractive.

00:07:57:11 - 00:08:38:03

Or hackers, edge devices, remote health care devices without security built in by design are vulnerable on staff of frequently accessing data remotely. In addition, things like cybersecurity initiatives or skills training in the life sciences and health care industry often fall flat. So that's why it's increasingly vulnerable. But just to pick up on a topic you were mentioning, which is the rise of remote health, remote devices and patient care, what pressures is that specifically creating from a cybersecurity perspective?

00:08:38:04 - 00:09:01:05

You know, interestingly, you know, we all see in the science fiction movies, all the spy movies, right, that, you know, somebody gets hold of somebody, you know, a digital device monitor gets help and you're able to manipulate the data. It's all about the long delays going on to the system and the wrong dosage of the emergency medicine is being delivered to the to the person.

00:09:01:06 - 00:09:47:05

But these are no longer, you know, fictional stories. You know, you talk about. So health data have the nanny. Right. Is one of the key areas which becomes challenging of one of the key challenges, which is therefore the let's say I.T devices or let's say remote wearable devices, you know what you're talking about. So therefore, behold identity management, access management, who's having access to what the entire user lifecycle management of its monitoring and how do you verify that that item that is having the you know, the access to that particular health data, it can be clinical data, it can be your data that you're getting from your remote device, right?

00:09:47:06 - 00:10:14:07

How do you handle that? So, these are the areas which become very important of digital rights monitoring, consumer identity, access management, the whole lifecycle period. Then the most important part becomes the data governance and privacy. Now this is the fundamental for any particular organization which is going ahead and trying to drive out any new devices which might be collecting the end user or the consumer data.

00:10:14:08 - 00:10:39:04

And also, own data governance and privacy management system needs to be implemented. But again, this is not just has to be limited to the notification processes, right? Or that, you know, in case of a breach has happened, you know, you are being notified, but effectively you need to have a proper privacy risk assessment for that kind of data.

00:10:39:04 - 00:11:02:10

And what data you are collecting for, you know, from users. And that is what you hear from big companies like Apple or Samsung. Right. Which are collecting a lot of health data now from the organizations, from the individuals. I'm sorry that how concerned about the privacy. But still having said that, they collect a lot of lot of data, you know, because they're in the organization.

00:11:02:10 - 00:11:22:08

So I think in a nutshell, if I have to look at the top three, you should be looking at data governance and privacy, digital rights management and the whole consumer identity access management. When you're talking about the whole remote, you know, health data collection from debatable text or any other text which are that in B but in the you know and use it.

00:11:22:09 - 00:12:00:08

Nicholas, so those are the three main strategies that you would deploy to protect remote data in that life sciences and health care industry. How important is improving the user experience when it comes to identity access management or data governance? Because, you know, having something like a 30 carries a password that needs to be updated every 15 or 30 to 60 days might not be the best way to engage consumers seeking to access healthcare services from their personal devices.

00:12:00:08 - 00:12:23:06

So how important is user experience and what more can be done to improve it in the security space? I think, Nicholas, we have come a long way from the 15 not that would be, you know, user password kind of a story, but you are absolutely right. We do have the legacy systems or the old archaic system which are still using those 15 to 30, you know, passwords.

00:12:23:07 - 00:12:44:14

But if you now look at the new systems, right, the data collection systems, you know, they are getting validated, authenticated by biometrics. I mean, take your own iPhone or around you have a smartphone, which you have. You have the whole biometrics which are stored locally on the device and not actually stored on the on the system, any of that.

00:12:44:15 - 00:13:16:08

Both kind of biometrics are now being used for authentication, passwordless authentication, still multiple mechanisms. Some things, you know, which are actually improving the user experience. So while you know, you do have, you know, certain legacy systems or certain legacy thing which are, you know, still working on that 15 party password thing. But I think when you're talking about the new future trends, we are definitely looking at the trends where the biometric data, all the user value is being utilized to verify the user.

00:13:16:09 - 00:13:47:01

And of course, that data is actually not being shared with the organization, which is using that that particular, you know, well let's say data which is getting collected. It is just that all biometric information is stored within the device itself. Now, since we're talking about the device and the user experience, one or the other thing which comes to the mind with the kind of the apps which you see, so you have you know, you have different devices like Fitbit and all those things which are collecting a lot of information.

00:13:47:01 - 00:14:11:05

And you can see all that data within the apps to also not, you know, shared with the, with the providers of other important things while the user experience becomes a critical part is the whole how the whole apps are getting you know well developed these days. You know you have the whole DevOps kind of a method that, you know, you have the whole development and the production cycle being very, very fast.

00:14:11:06 - 00:14:30:11

So while we are talking about the whole data security, the I think be from the end user perspective, the organization should also need to look at the whole secure software development part and bring that security in the whole DevOps also that so that while the release cycle is very fast and they are also they are not securing, you know, compromising on the security as well.

00:14:30:12 - 00:14:54:07

So biometric data is stored on the local device not being transmitted to the end user that that can help improve your user experience. Secure apps again can help improve the security. You know, consumer experience does also give them a trust that yes, you are actually keeping their data secure and, you know, help you and your business has met.

00:14:54:08 - 00:15:34:01

Thank you. And crucially, health care or life sciences organizations aren't experts in cybersecurity. They do need to partner on. It's something that HCLTech offers. They have cybersecurity and governance risk and compliance services. So, can you just explain how companies like HCLTech all helping protect the life science and health industry? And can you provide any examples of where HCLTech has helped an organization improve its cybersecurity posture when it comes to it's here and the life sciences customers, right?

00:15:34:03 - 00:16:15:10

We ensure that cybersecurity is being managed in all the phases that is from prevention to test to detection, to response and recovery. You know in the in case that is an event which has taken place now on top of it, we incorporate security and privacy. You know, during the whole complete data lifecycle. So effectively, you know, specifically, you know, in terms of health and health enterprises that they're talking about data privacy and that of course, embedding that as a part of the any and all initiative that becomes a very important part of how easy, you know, interacts or supports life sciences organizations in this cybersecurity.

00:16:15:11 - 00:16:46:11

Now, we do have several very, very large fortune, let's say, part intelligence for 50 life sciences customers, because all of us are being sold on Switzerland and how we are helping those organizations and in one such Swiss organization, which is a global one of the largest global organizations, we are helping them secure that entire security operations. That is, you start from identity and access.

00:16:46:11 - 00:17:34:01

But in bringing you start from infrastructure and cloud security, we are working with them on data privacy, securing their application, that is on the application security, on the manufacturing and the plant and IP security. We are doing also working with them on the whole security orchestration, security monitoring, portal things, identity and access management, privileged access management. So effectively in this particular organization, we are not just our security supplier, but we are happy to be working with the business organization and helping them helping understand what are their business strategy and helping them realize their business strategy by securing that entire organization from doing so effectively.

00:17:34:05 - 00:18:04:08

They are now very much happy with what day to day providing to them. So this is provided to them and we are always helping them improve that Business processes, increase their footprint in the market. So again, as we said, we help our life sciences customers from end to end. That is prevention to detection, response and recovery and of course helping them how can improve their business processes as well.

00:18:04:09 - 00:18:32:10

That's great and obviously absolutely crucial. Prabhat Thank you so much for your time, Stan, for your excellent insights. Thanks. Also, Nicholas, as well, the pleasure of figs. And just as we round off today's podcast, I'd like to finish with the event round up the last month of summer will see the return of major conferences. The HCLTech Trends and Insights team will be attending Google next in San Francisco on August 29th.

00:18:32:12 - 00:18:48:00

And we'll be bringing you all the latest from the world of cloud on the growing impacts of technologies like generative AI and its impacts on sectors like retail. Thank you for your great insights once again and to the audience for tuning in. Goodbye.