Johner Institute

Interplay between risk management and IT security

With Christian Rosenzweig, Prof. Dr. Christian Johner

Transcript

00:00:05 Speaker 1

Medical Device Insights, a podcast by the Johner Institute for medical device manufacturers, authorities and notified bodies.

00:00:20 Speaker 2

You may also have heard about the recent incident where a medical practice manufacturer accidentally failed to properly protect millions of patient data, and that's obviously a

00:00:32 Speaker 2

Problem with the confidentiality of the data, with data protection.

00:00:36 Speaker 2

But now we are also here at the institute.

00:00:39 Speaker 2

Let's support many manufacturers who manufacture medical devices and have such problems with the I.T.

00:00:45 Speaker 2

Safety, and often also have a direct impact on patient safety.

00:00:48 Speaker 2

And it's not just about data protection.

00:00:51 Speaker 2

And so today I wanted to illuminate with Christian Rosenzweig how I.T.

00:00:56 Speaker 2

security, how risk management interacts, what regulations we have, but also perhaps a few

00:01:02 Speaker 2

Best practices, which in turn will help you not to make the same mistakes.

00:01:07 Speaker 2

Yes, and as already announced, Christian Rosenzweig is with me today, who best says a few words about himself.

00:01:13 Speaker 2

Then you can also assess it a little better if you don't know it yet.

00:01:17 Speaker 3

Yes, hello, my name is Christian Rosenzweig.

00:01:19 Speaker 3

I am 50 years old, have 3 wonderful children, learned nursing in the 90s.

00:01:25 Speaker 3

He then studied medical technology and worked in industry for many years as a development engineer for medical devices.

00:01:32 Speaker 3

I then switched to quality management, was also a quality management officer and finally came to the Jona Institute three and a half years ago as a consultant for medical devices, where I am responsible for the focus areas of risk management and I.T.

00:01:45 Speaker 3

Security.

00:01:46 Speaker 2

Yes, we are all happy, very happy, on the one hand that you are there and on the other hand that you are also taking care of these focal points and, among other things, also offering the seminar on both topics.

00:01:58 Speaker 2

Yes, let's take a look.

00:02:00 Speaker 2

So, what are

00:02:01 Speaker 2

Typical difficulties that manufacturers are now facing in the area of risk management, I.T.

00:02:07 Speaker 2

security again and again.

00:02:08 Speaker 2

What are also things that the notified bodies, the authorities regularly criticize in them?

00:02:14 Speaker 2

You could just say, yes, what kind of problems are there in this context?

00:02:18 Speaker 3

Yes, there are quite a few.

00:02:19 Speaker 3

First of all, you have to start with the question, what are the regulatory requirements that I have to meet as a manufacturer?

00:02:25 Speaker 3

And that's where manufacturers sometimes have a hard time.

00:02:27 Speaker 3

When it comes to risk management, it is still relatively simple, as the harmonized standard ISO 14971 has been the gold standard for many years.

00:02:34 Speaker 3

The situation is a bit different when it comes to IT security, because there is not yet this gold standard for medical devices.

00:02:41 Speaker 3

The manufacturer is then usually confronted with a mass of regulatory requirements that are more or less binding.

00:02:48 Speaker 3

There are a lot of guidance documents,

00:02:51 Speaker 3

Frameworks, norms and in this mass he has to navigate and find his way around somehow and actually there is always the feeling for him that he has left something out of consideration and then fails at the implementation because it is simply too much.

00:03:04 Speaker 3

The next problem is that these regulatory requirements must of course also be implemented.

00:03:10 Speaker 3

That means you have to interpret them and understand how to transfer them into your own practice, into your own company.

00:03:15 Speaker 3

With the 14971 it is the case that the now very concise

00:03:19 Speaker 3

The individual requirements are formulated, but it still offers room for interpretation and manufacturers find it difficult to implement them accordingly.

00:03:28 Speaker 3

It always helps to have experienced colleagues at your side who have a bit of best-practice experience.

00:03:34 Speaker 2

Well, I've heard 2 points now.

00:03:36 Speaker 2

The first type of difficulty is that you don't even know what is required by regulation and the second, if you do, you don't know how to implement it.

00:03:42 Speaker 2

Exactly, maybe let's take a look at both topics again.

00:03:45 Speaker 2

So, it drives 271 for risk management, you have already mentioned it and I think that the IVDR and MDR also require a risk management system.

00:03:54 Speaker 2

I think that already appeared in Article 10.

00:03:56 Speaker 2

I think this is well known.

00:03:57 Speaker 2

If we now perhaps go back into the area of IT security, what do we have in it

00:04:02 Speaker 2

Specifications, what standards should be on a manufacturer's list?

00:04:07 Speaker 3

Yes, it starts with the demand in the M.

00:04:10 Speaker 3

D.

00:04:10 Speaker 3

R.

00:04:10 Speaker 3

himself or I.

00:04:11 Speaker 3

V.

00:04:11 Speaker 3

D.

00:04:11 Speaker 3

R.

00:04:12 Speaker 3

It is now stated in Annex 1 under the essential safety and performance requirements that Topic I.

00:04:16 Speaker 3

T.

00:04:16 Speaker 3

safety must also be taken into account.

00:04:19 Speaker 3

Period.

00:04:19 Speaker 3

And for many manufacturers, this is now an entry point, a trigger point, but of course that doesn't give much substance.

00:04:26 Speaker 3

The next level is the M.D.C.G.

00:04:29 Speaker 3

Guidance document 2019 deleted 16 revision 1.

00:04:34 Speaker 3

That describes a bit more specifically what is meant by I.T.

00:04:39 Speaker 3

Security, but to be honest, it remains very unspecific and very superficial, but it does have preferences for different standards or other guidance documents, which you can then use to dig deeper and deeper into the topic.

00:04:50 Speaker 3

And last year, a brand new standard came onto the market, the IEC 81001 deleted 5 stroke 1.

00:04:57 Speaker 3

This is now also on the E.U. list of proposals.

00:05:00 Speaker 3

Commission on harmonization and this will hopefully establish itself as the gold standard in the medical device world.

00:05:06 Speaker 2

Could you briefly name a few points that this new standard now addresses, i.e. that you just have a feeling for what is being demanded?

00:05:14 Speaker 3

Yes, the beauty of it

00:05:15 Speaker 3

What is important about this standard is that it follows 62304, the software life cycle, a bit.

00:05:21 Speaker 3

This means that it adopts the same basic concept of the development process and latches on to it with its activities.

00:05:27 Speaker 3

And it says, for example, that if you do requirements management, then please also take into account the requirements for IT security and also the IT security environment in which your product is integrated and juggle a bit with the requirements that you set for the product itself or that you direct to the operator.

00:05:44 Speaker 3

And

00:05:45 Speaker 3

Together, this security concept or I.T.

00:05:48 Speaker 3

Security Capabilities of the product and then it goes on to the architecture, where I then also use certain I.T.

00:05:55 Speaker 3

security-relevant aspects such as this Defense In Depth model.

00:06:01 Speaker 3

From the implementation to the tests and the tests, there is now also a bouquet of new tests that were previously unknown or were not common.

00:06:11 Speaker 3

Penetration Test, Vulnerability Scanning.

00:06:14 Speaker 3

Are there or almost testing, they are just new to it.

00:06:17 Speaker 2

So, new in the sense that it is required by regulatory medical device-specific requirements, because it is not so new in the IT security cell now.

00:06:25 Speaker 2

Exactly, but new, just that it is now, that one becomes so concrete.

00:06:30 Speaker 2

So, what you can hear now, what you have already reported, is that IT security is not something that you check in, but that it is over the entire development or, you even have to say, product life cycle.

00:06:43 Speaker 2

must be lived.

00:06:44 Speaker 2

In other words, that we have activities in all phases, perhaps a little advertising on our own behalf.

00:06:48 Speaker 2

That's why we also designed the I.T.

00:06:50 Speaker 2

Security Guide, which we wrote together and which the notified bodies now also use for themselves, sorted exactly according to these phases, in order to perhaps become a step more granular or verifiable as far as these lifecycle activities are concerned.

00:07:06 Speaker 2

Well, I think that's really important for manufacturers

00:07:09 Speaker 2

Insight, what you just said, or an important thing to keep in mind: IT security begins with the beginning or before the start of development and not only when the product has been built and you then look, yes, is it even safe?

00:07:21 Speaker 2

Now we were already very much involved in the topic of IT security.

00:07:25 Speaker 2

Do you have a few more for us?

00:07:27 Speaker 2

Tips on how we can manage this interaction between IT security and risk management.

00:07:33 Speaker 2

So, you've now nicely shown how IT security and the software lifecycle process interact.

00:07:38 Speaker 2

Yes, if you look at the requirements or the architecture, so to speak, for example, who applies threat modeling and then the tests, then you have the special tests such as penetration tests, but how?

00:07:47 Speaker 2

does this IT security process and the risk management process interact now?

00:07:52 Speaker 2

Could you give a few more tips?

00:07:54 Speaker 3

Yes, this is a very important topic, where many manufacturers also fall flat on their faces, I don't want

to say, but at least have their problems, because IT security is always about the protection goals of data integrity, data availability and data confidentiality, and risk management according to 14971 is actually about the protection goal of preventing patient harm or harm to humans.

00:08:13 Speaker 3

And it is difficult to put the two issues on top of each other now.

00:08:16 Speaker 3

At least with the evaluation catalogs, I have difficulty saying the classic damage to the human evaluation catalog, I now bring in the data protection issue and that's why it makes sense to separate the two areas and say, I have a standalone risk management process for IT security and on the other hand I have the 14971 construct with its own risk table.

00:08:38 Speaker 3

And now I'm just creating a risk table on the IT security side, either on the basis of the thread modeling that you have already mentioned.

00:08:46 Speaker 3

or via other methods, such as this more FMEA-based threat risk analysis model and the risks that I find in the process, I just transfer them to the list of IT security risks, make another evaluation catalog, such as a CVSS score, and then also define measures and risk acceptance in the area.

00:09:06 Speaker 3

And when I am done with it, then I transfer the findings from this table, if they are relevant, into the

00:09:14 Speaker 3

Risk table according to 14 971, because then I can go on to the harm to humans and then I have also recorded and evaluated these risks there and provided them with measures, if they go beyond what I described in the I.

00:09:28 Speaker 3

T.

00:09:29 Speaker 3

Security as measures.

00:09:31 Speaker 2

Ah, OK, so maybe that's a thought and a very short summary of me, so to speak, whether I understood everything correctly.

00:09:37 Speaker 2

So the first thing you said is, watch out, we have different goals or we can

00:09:42 Speaker 2

may have different goals in IT security and risk management, perhaps even an example of this.

00:09:48 Speaker 2

It may be that we compromise safety by increasing IT security.

00:09:54 Speaker 2

We had even had such a case before, where they reduced access rights to patient data for nursing staff and thus increased confidentiality as an aspect of IT security.

00:10:06 Speaker 2

The result was, the nurses were no longer

00:10:10 Speaker 2

Able to find errors in medication prescriptions and it really happened.

00:10:14 Speaker 2

Patient Safety went down.

00:10:15 Speaker 2

This means that they can even be contradictory in extreme cases.

00:10:19 Speaker 2

And in one standard, I think that's UL 2900 dash 2 stroke 1, there is even such a concept in it and the FDA has it too.

00:10:25 Speaker 2

Breaking the Glass, so to speak, like a kind of fire alarm, where you can say, I'm going to overwrite everything now, forget about confidentiality here.

00:10:33 Speaker 2

We now have to take care of patient safety here.

00:10:35 Speaker 2

So, I think that's an important aspect.

00:10:37 Speaker 2

then the second thing you said was actually how the two of them play together.

00:10:42 Speaker 2

And if I understood you correctly, on the one hand we have this I.T.

00:10:45 Speaker 2

Security process with the aim of I.T.

00:10:48 Speaker 2

Identify security risks and these in turn are then incorporated into the risk management process.

00:10:55 Speaker 2

And then you look at what would be such a risk or a compromise, what would the significance of the I.T.

00:11:00 Speaker 2

Safety for patient safety, can you say that?

00:11:03 Speaker 3

Exactly, and it even goes one step further.

00:11:06 Speaker 3

If you look at the M.D.C.G.

00:11:07 Speaker 3

document, then you can see on the very last page that the two processes are juxtaposed, the I.T.

00:11:14 Speaker 3

Security risk management process and the 14 971 risk process and then there are arrows painted in between and these are these references that you have there.

00:11:21 Speaker 3

I'm just looking, has a risk from the I.T.

00:11:24 Speaker 3

Security also has a reference to the damage to humans, then I will convict it.

00:11:27 Speaker 3

But it may also be that a measure in the area of I.T.

00:11:30 Speaker 3

Security is now a

00:11:32 Speaker 3

is for 14,971 and, conversely, a measure in the 14,971 area can also be classified as an I.

00:11:40 Speaker 3

T.

00:11:40 Speaker 3

Security risk.

00:11:41 Speaker 3

If, for example, I say I have the problem that my medication data can also disappear because the hard drive crashes, for example, then I just make a backup in the cloud so that I no longer have this problem on 14,971 pages.

00:11:55 Speaker 3

but of course this has now torn a hole again in the area of data confidentiality, because my patient data is now in the cloud and then I have to handle it there again and these, these constant circular references or these constant iteration steps, I have to take them into account in the development process.

00:12:11 Speaker 2

Mhm, do you have any other tips that could help us with this complex handling, so to speak, I know, in the direction of automation, tools, process models?

00:12:21 Speaker 3

Yes, the most important thing is, I have

00:12:23 Speaker 3

an interface in the responsibilities.

00:12:27 Speaker 3

I usually have a team that takes care of the 1479 risks, the classic risk manager is named as a role and on the other hand I have this team of IT security experts and they have to somehow either sit down at a table or communicate with each other and also have to have the appropriate tools and what has just been established there is, that they keep their separate tables, but then always exchange them and that can of course be done tool-supported

00:12:52 Speaker 3

although I have not yet come across a tool that I could really recommend without any problems.

00:12:57 Speaker 2

What would you recommend to people who want to go deeper?

00:13:02 Speaker 2

Well, I would probably give away your contact details there.

00:13:06 Speaker 2

What else can they do, if they may also have product-specific questions or go even deeper into this topic, yes, interface risk management, I.

00:13:15 Speaker 2

T.

00:13:15 Speaker 2

Security, if they want to go even deeper.

00:13:17 Speaker 3

Yes,

00:13:18 Speaker 3

a very good start is always the seminar for both risk management and I.

00:13:23 Speaker 3

T.

00:13:23 Speaker 3

Security, because you can find out all the topics about this concept or the procedure in 2 days and many manufacturers have an aha experience, because they say, I've always implemented this in a certain way for myself until now, but now I've got a full view of the topic again and that has now brought me even further.

00:13:44 Speaker 3

In addition to these seminars, we can also offer workshops as a format.

00:13:48 Speaker 3

You can interactively go through your files together with the manufacturer, discuss his procedures, answer questions or establish completely new procedures and processes or create files that can then also be used in accordance with the approval.

00:14:05 Speaker 2

Auch F.D.L.

00:14:05 Speaker 3

Yes, exactly.

00:14:07 Speaker 3

we also work internationally with our corresponding teams, which are also established in other markets, and at ID Security we have a brand new addition to our program on the topic of penetration tests, which means that we then also offer operational support in the implementation, i.e. the execution on behalf of the manufacturer of penetration tests or vulnerability scanning as well as risk analysis for its product and this is now a supplement to our services in the way that we are now full

00:14:37 Speaker 3

offer comprehensive service around I.

00:14:39 Speaker 3

T.

00:14:39 Speaker 2

Security.

00:14:40 Speaker 2

Yes, and I think that has always done the manufacturers who were there pretty good, because we have never found anything.

00:14:44 Speaker 2

So some of them were even catastrophic mistakes and don't have to have someone else on the Tagesschau, although we would have returned to the beginning of the podcast.

00:14:54 Speaker 2

I think that's exactly how we started with this one practice manufacturer.

00:14:57 Speaker 2

So that would definitely be a very good measure to knock out these holes.

00:15:02 Speaker 2

Yes, so I would say I just link that, so then both

00:15:06 Speaker 2

your two seminars Risk Management I.

00:15:08 Speaker 2

T.

00:15:08 Speaker 2

Security and also the information about our penetration testers.

00:15:13 Speaker 2

I think this is an extensive, a good offer.

00:15:15 Speaker 2

Yes, you, all that remains for me to do is to thank you very, very much.

00:15:18 Speaker 2

It was super fun.

00:15:20 Speaker 2

I hope to see you again soon.

00:15:21 Speaker 3

Thank you too, Christian.