Johner Institute

Competitive advantages thanks to IT security

With Gerd Dautel, 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.

00:00:17 Speaker 1

The topic I.T.

00:00:19 Speaker 1

We probably won't be able to get rid of security for a long time.

00:00:22 Speaker 1

New data scandals, intrusions and attacks keep busy

00:00:29 Speaker 1

IT companies, but also all other industries, including healthcare.

00:00:33 Speaker 1

A sad example was also the recent attack on the University Hospital Düsseldorf, in which a patient may even have died as a result of this attack.

00:00:45 Speaker 1

This means that we medical device manufacturers must do our part to develop safe products.

00:00:53 Speaker 1

And today in the conversation I have someone with me who

00:00:56 Speaker 1

a medical device manufacturer works and takes care of such products.

00:01:01 Speaker 1

This is Mr. Daudel.

00:01:03 Speaker 1

Mr. Daudel, could you perhaps introduce yourself as a person or your role and the products you make?

00:01:10 Speaker 1

I think that will give us a good context for what we are talking about today.

00:01:14 Speaker 2

Yes, hello, first of all, thank you very much for the invitation.

00:01:17 Speaker 2

I'm Gerd Daudel, from the background I'm a medical computer scientist

00:01:24 Speaker 2

and I work for the Streiter company and there as head of quality management and approval and have been for quite some time.

00:01:33 Speaker 2

And I've been dealing with cybersecurity for about 4 years now.

00:01:39 Speaker 2

In the Group, our goal was to raise cybersecurity measures at Group level, so to speak, to Group-wide standards, i.e. out of the projects and into the corporate quality management system.

00:01:53 Speaker 2

and to harmonize and integrate them in such a way that we are also equipped for our digital future, so to speak.

00:02:01 Speaker 2

Striker is a pure medical device entrepreneur, a pure medical device company.

00:02:06 Speaker 2

We make from implants to networked products, we have a very wide spectrum.

00:02:12 Speaker 2

If you talk about connected products, maybe you can mention our navigation systems, which are connected, but we also do things like defibrillators,

00:02:22 Speaker 2

that are network-capable or hospital beds that are networked and much more.

00:02:30 Speaker 1

This means that on the one hand you have networked products and on the other hand products that are particularly relevant to safety.

00:02:38 Speaker 1

You have just talked about navigation systems and defibrillators.

00:02:42 Speaker 1

I think it's obvious what meaning a good I.

00:02:45 Speaker 1

T.

00:02:46 Speaker 1

Security hat.

00:02:47 Speaker 1

What are you doing in your company to improve cybersecurity

00:02:51 Speaker 1

and who is involved, i.e. which roles carry out which activities?

00:02:58 Speaker 2

Yes, I just mentioned it, on the one hand, we have implemented a wide variety of procedures at the level of the quality management system, the Tryker quality management system, especially in the Design for Security, so how do I have to implement security in the development process.

00:03:19 Speaker 2

Another big question was how I can harmonize security risk management with risk management on 14,971, i.e. health protection, if you will.

00:03:31 Speaker 2

And another big topic was post-market management.

00:03:35 Speaker 2

What does cybersecurity mean when the products are on the market, how do I do the monitoring, which channels do I have to look at and all that.

00:03:44 Speaker 2

To get all this done, we have

00:03:48 Speaker 2

we were organizationally active, if you will.

00:03:51 Speaker 2

We have set up a central core team, which is in constant contact with the management of our divisions, for example, to discuss plans on a monthly basis on how to proceed.

00:04:09 Speaker 2

But we have also set up specialists or focus groups that take care of the 3 topics I just mentioned, Design and Privacy for Security, Risk Management for Security and Post Market Management.

00:04:24 Speaker 1

Could you give us a few examples of what you do in the field of design?

00:04:29 Speaker 1

So I don't have any secrets, but general considerations, so to speak, that you make there and

00:04:35 Speaker 1

very roughly, perhaps, measures they take.

00:04:37 Speaker 2

Yes, one of the first considerations was years ago when I started with it.

00:04:43 Speaker 2

Are there any catalogs that can be used to understand user needs in this case security needs and how can they be underpinned and how can they be boosted to the software development process, which we have of course established for a long time.

00:04:58 Speaker 2

What does it mean for architecture and design, how we can further refine it?

00:05:04 Speaker 2

and how does it relate to cybersecurity risk management.

00:05:10 Speaker 2

We now understand this as an iterative process, so what we have done there, I'll start again at the beginning with the cybersecurity needs and the cybersecurity specifications, if you will.

00:05:22 Speaker 2

There are catalogs that can be found in various standards, which are called capabilities, for example.

00:05:29 Speaker 2

they are categories on cybersecurity that you can pay attention to in this context, which are further broken down into so-called controls.

00:05:38 Speaker 2

These are more specific requirements.

00:05:40 Speaker 2

This has been implemented in our general design input framework.

00:05:44 Speaker 2

So I talk a bit American, because I'm always an American company.

00:05:48 Speaker 2

I hope that it will still be understood.

00:05:51 Speaker 1

Absolutely.

00:05:52 Speaker 1

If you could give us an example of a need and a control, then we would be even safer,

00:05:58 Speaker 1

That all listeners have the same mental model, so to speak.

00:06:02 Speaker 2

Yes, you don't want that if a computer is located somewhere in a practice, for example, or on a ward in the clinic, that if the person who has just dealt with it, when he gets up and leaves, that everyone else can do it.

00:06:19 Speaker 2

So, such a capability or something, do you need an Outlook of.

00:06:22 Speaker 2

a controlware, which functions have to be switched on, so to speak, to ensure this auto-lock-off after a certain time, for example, that it switches off after a minute, after 2 minutes or whatever.

00:06:37 Speaker 2

Another example would be if someone else takes it, yes what does it look like now, that if he tries to penetrate there 345 times, that you can just prevent it?

00:06:48 Speaker 1

Mhm.

00:06:49 Speaker 1

and then implement the control again, the measure that recognizes this and then reacts accordingly.

00:06:55 Speaker 1

You have already made it quite clear, and I think this is very important, that this topic I.

00:07:01 Speaker 1

T.

00:07:01 Speaker 1

Security is actually a complete lifecycle topic, i.e. it encompasses all phases of development, but also afterwards, and in this context you already have

00:07:11 Speaker 1

the term post-market surveillance or post-market activities is also mentioned.

00:07:17 Speaker 1

What do you do in this area, i.e. after the products have been placed on the market, in order to make the I.

00:07:23 Speaker 1

T.

00:07:23 Speaker 1

ensure the long-term safety of your products.

00:07:26 Speaker 2

Yes, you first have to understand from which channels, sources of information, so to speak, vulnerabilities again in the American, i.e. potential weaknesses that affect your products, your network-enabled products,

00:07:40 Speaker 2

from which channels should such information be able to come?

00:07:45 Speaker 2

Typically, as a medical device manufacturer, you know complaint handling or you know a non-conformity kappa system and all that kind of thing.

00:07:53 Speaker 2

Yes, but in this case the public, the media for example, also plays such a big role.

00:07:58 Speaker 2

Man denke da an WannaCry.

00:08:01 Speaker 2

Maybe you know this, WannaCry was a ransomware attack,

00:08:05 Speaker 2

which has paralyzed large parts of the English health care system.

00:08:09 Speaker 2

That was about two and a half years ago, if I remember correctly.

00:08:12 Speaker 2

Yes, you have to monitor for something like that and then there are now also databases that are publicly accessible, which, for example, regularly update which weaknesses, which weaknesses apply to Windows 10, for example, which patches have to be installed and something like that also needs to be monitored.

00:08:30 Speaker 2

All in all, this is a relatively complex event.

00:08:34 Speaker 2

and that's why you can and probably have to think about whether you use the tools to help you.

00:08:39 Speaker 2

There are tools such as Black Duck that monitor such databases, so to speak, if they know which components are integrated into their software.

00:08:49 Speaker 1

Yes, this is probably also spelling at the NIST database, which may overwhelm some with several 1000

messages per month.

00:09:00 Speaker 1

and tools like the Black Duck, which you just mentioned, or our post-market radars help to monitor exactly that, just the whole range of information sources you have just described.

00:09:15 Speaker 1

It sounds as if some resources are needed for this, not only in terms of quantity, but also in terms of competences.

00:09:25 Speaker 1

Now Stryker is a very large manufacturer,

00:09:28 Speaker 1

What would you recommend to other manufacturers and when do you think it would be necessary for them to also seek external help?

00:09:36 Speaker 2

Yes, I can perhaps speak of myself when I started about 4 years ago and was asked if I could help establish the Corporate-Wide, i.e. cybersecurity management and integrate it into our, into our Corporate Quality Management,

00:09:53 Speaker 2

I had an idea like about 10 years ago, when I did something similar for the 14 971 14 971, i.e. health risk management, if you can distinguish it from cyber security risk management.

00:10:07 Speaker 2

What I have experienced is a wealth of standards, of guidance.

00:10:12 Speaker 2

So yesterday I did a quick calculation, I have

00:10:15 Speaker 2

now well over 100 standards in guidance, which I have read more or less thoroughly.

00:10:20 Speaker 2

What I'm trying to say is a pretty challenging field and a relatively complex area.

00:10:26 Speaker 2

So, where someone can help, is to give orientation at all when getting started, where do I have to go there, where do I have to reach there, what do I read through, what is relevant for me, what does integration mean for my specific context, i.e. what kind of medical device do I do and

00:10:45 Speaker 2

What does this mean for my cybersecurity quality management system?

00:10:49 Speaker 2

By the way, what is also being added in Europe is the General Data Protection Regulation.

00:10:55 Speaker 2

So, what you should do at the same time, in my opinion, are general data protection regulations, requirements are also considered, because cybersecurity is a necessary prerequisite for data protection for me, but not a sufficient one.

00:11:07 Speaker 2

That's why I have to think about it, in my opinion.

00:11:09 Speaker 1

You have already said that you would recommend help in order to get into the topic at all, to get an overview of what best practices, standards, norms and so on.

00:11:21 Speaker 1

exist and which of them are also worth studying more closely.

00:11:25 Speaker 1

If we go a little further down the technology, for example coding standards, penetration testing, fast testing, would you also give such activities to the outside world or is it something you say, no, that belongs in the company.

00:11:40 Speaker 2

It depends, it takes a lot, a lot of competence and knowledge.

00:11:48 Speaker 2

if you have to set it up yourself, again, I really think it's a complex topic, then you need a while to get up to speed.

00:11:56 Speaker 2

So it makes sense to give this to the outside world, to give an example from your own organization, to show it, we are currently in the process of establishing a worldwide central test laboratory for exactly this type of test.

00:12:08 Speaker 2

Precisely because we want to prevent people from reinventing the wheel again and again and thus also creating the inconsistent approach, so to speak.

00:12:17 Speaker 1

And I think it also becomes clear that you need a certain size to make it pay off, to build up an infrastructure, a staff base that is not only able to familiarize itself with these topics, but is also able to keep up with the state of the art.

00:12:35 Speaker 1

Yes, now you have already talked about norms, about standards, about best practices.

00:12:40 Speaker 1

They said that they are

00:12:42 Speaker 1

some 100, What are the most important ones that they use as a guide or think you should not only know, but perhaps also have read?

00:12:52 Speaker 2

Yes, there are 2 essential ones from the F.D.A. that have been published for several years, namely the one that there are 2 guidance from the F.D.A., one on design controls, i.e. what documents on cybersecurity are expected for the approval of medical devices in the U.S.A.

00:13:10 Speaker 2

That would be one thing

00:13:11 Speaker 2

and the other guidance relates to post-market, post-market surveillance and risk management for products that are already on the market, and this is also associated with reporting obligations in the U.

00:13:22 Speaker 2

S.

00:13:22 Speaker 2

A.

00:13:23 Speaker 2

by the way, also a very interesting aspect.

00:13:25 Speaker 2

If you go back to the development process itself, then we have oriented ourselves on a few I's.

00:13:31 Speaker 2

E.

00:13:32 Speaker 2

C.

00:13:32 Speaker 2

and NIST standards.

00:13:33 Speaker 2

I've already talked about the capabilities or the cybersecurity user needs,

00:13:39 Speaker 2

a standard like the I.E.C. helps

00:13:41 Speaker 2

800001 dashed 2 dashed 2 the Listed Capabilities or these categories of cybersecurity.

00:13:49 Speaker 2

And if they then look into the NIST Standard 800 dash 53, then you get all the controls that they want to establish in order to fill these capabilities with life, so to speak, if you will.

00:14:06 Speaker 2

In risk management

00:14:09 Speaker 2

Would it be important to deal with this with an AMI guidance that the T.I.R.

00:14:16 Speaker 2

57, which describes Principles for Medical Device Security and where it does a pretty good job, in my opinion, is basically the explanation of how cybersecurity, risk management and safety-o-health-risk management, how they can be brought into harmony.

00:14:34 Speaker 1

Yes, I think that is a very, very important addition that you are making here, because many of these guidelines have the I.

00:14:42 Speaker 1

T.

00:14:42 Speaker 1

security, i.e. the ability to protect information and information technology and to protect their confidentiality, integrity and confidentiality.

00:14:55 Speaker 1

To ensure the availability of information, information technology.

00:14:59 Speaker 1

But for us medical device manufacturers, this is not the end point or not the only one.

00:15:03 Speaker 1

We always have the safety that we ultimately have to keep in mind.

00:15:07 Speaker 1

Yes, but you have already reduced this endless list for us.

00:15:12 Speaker 1

I think that will be very helpful.

00:15:14 Speaker 1

We have in the accompanying materials, we also have a

00:15:18 Speaker 1

Articles are listed, where you get an overview of all these norms and standards and there are also the

ones just mentioned, commented on and I think they are quite important, which you have just mentioned here.

00:15:33 Speaker 1

We have just talked about the topic of outsourcing certain I.

00:15:38 Speaker 1

T.

00:15:39 Speaker 1

Security activities.

00:15:41 Speaker 1

I would like to come back to outsourcing, but this time a bit from a different perspective.

00:15:46 Speaker 1

Many manufacturers

00:15:47 Speaker 1

do not necessarily develop the software themselves, but use development service providers themselves.

00:15:55 Speaker 1

What would you recommend what a manufacturer, i.e. a distributor, should do to ensure that the I.

00:16:01 Speaker 1

T.

00:16:01 Speaker 1

To ensure the security of its products even if this software is manufactured by the third party?

00:16:09 Speaker 1

So to speak, which

00:16:11 Speaker 1

You recommend controlling these processes.

00:16:13 Speaker 2

Yes, you have to look a bit in the books, I think.

00:16:15 Speaker 2

In other words, how well equipped is the manufacturer to actually design cybersecurity into the products.

00:16:23 Speaker 2

And that‘s when I came across her guide for I.

00:16:27 Speaker 2

T.

00:16:27 Speaker 2

Security some time ago and I'm actually using it at the moment.

00:16:31 Speaker 2

Exactly in such a relationship with the supplier of software, which we like to call O.

00:16:35 Speaker 2

E.

00:16:36 Speaker 2

M.

00:16:36 Speaker 2

product.

00:16:38 Speaker 2

and it is really, really, really helpful and useful in this context, because it harmonizes the most diverse aspects and brings them together in a checklist that you can simply work through.

00:16:52 Speaker 2

What I also like is the maturity model, which they have designed in there, i.e. these levels from 0 to 2, what do I need at least, where am I already quite good and what would be best in class, so to speak.

00:17:05 Speaker 2

By the way, there is something similar, a little longer on the market.

00:17:10 Speaker 2

There is this Medical Device and Health I.T.

00:17:13 Speaker 2

Joint Security Plan.

00:17:14 Speaker 2

I don't know if you know it.

00:17:16 Speaker 2

It was published in early 2019 by the Healthcare and Public Health Sector Organization in U.S.A.

00:17:26 Speaker 2

This is a conglomerate of F.D.A.

00:17:30 Speaker 2

Medical devices, industry and and and consulting firms.

00:17:36 Speaker 2

In the one in this guidance, they describe a very nice, I think, holistic picture of cybersecurity and medical devices and, by the way, also Health I.

00:17:46 Speaker 2

T., which I find interesting in this context.

00:17:49 Speaker 2

It not only focuses on medical devices, but also takes Health I.

00:17:53 Speaker 2

T.

00:17:53 Speaker 2

into the scope, which I think is important, because you can cut something like that off quickly.

00:17:57 Speaker 2

And there is also a kind of assessment procedure, which is based on C.M.M.I.s.

00:18:04 Speaker 2

so this maturity model, which comes from Carnegie Meln University, is a little bit shorter.

00:18:09 Speaker 2

So if you want it to be shorter and faster, for example for yourself, where do I stand today with my cybersecurity quality management system, what it says can be quite helpful.

00:18:20 Speaker 1

Absolutely, and I think we're going to get into both documents, the one from the, so this maturity model and the I.

00:18:27 Speaker 1

T.

00:18:27 Speaker 1

Security Guide We

00:18:29 Speaker 1

which have developed at the Jona Institute and, by the way, have also continued the notified bodies, we will link to both.

00:18:36 Speaker 1

So far, we have looked at cybersecurity more from one point of view.

00:18:41 Speaker 1

Yes, we have to build the products safely and there is a bit of resonance there, in and of itself you can only lose on this topic.

00:18:48 Speaker 1

So in the best case you just don't have an I.

00:18:51 Speaker 1

T.

00:18:51 Speaker 1

Security problem and in the other case you have 1, but you can't really win with this topic.

00:18:56 Speaker 1

Or do you have an idea how to

00:18:59 Speaker 1

on topic I.

00:19:00 Speaker 1

T.

00:19:00 Speaker 1

Security may even be able to gain a market advantage.

00:19:03 Speaker 2

Yes, we can actually see that in U.

00:19:06 Speaker 2

S.

00:19:06 Speaker 2

A.

00:19:07 Speaker 2

Well, it started years ago when I got into the topic that more and more customers, i.e. hospitals or purchasing companies, demanded explanations for cybersecurity.

00:19:20 Speaker 2

Not to mention, I'm talking about an American market form again, the Department of Defense, which together with the already mentioned Carnegie Mellon University

00:19:29 Speaker 2

i.e. really demands very high standards when it comes to cybersecurity.

00:19:34 Speaker 2

We, we were already faced with the situation that we were really fighting for contracts, because the presentation was not immediately there, if you will, as far as cybersecurity is concerned.

00:19:49 Speaker 2

The

00:19:50 Speaker 2

So and and I mentioned it earlier, we are, we are of course also involved with purchasing companies, large purchasing companies for medical products in U.

00:20:01 Speaker 2

S.

00:20:01 Speaker 2

A.

00:20:02 Speaker 2

in contact.

00:20:02 Speaker 2

They not only demand the presentation of cybersecurity as far as concrete products are concerned, for example with the help of an M.

00:20:09 Speaker 2

D.

00:20:09 Speaker 2

S.

00:20:10 Speaker 2

Square shape or M.

00:20:11 Speaker 2

D.

00:20:11 Speaker 2

S.

00:20:11 Speaker 2

2 form, which is a kind of questionnaire in a structured way

00:20:16 Speaker 2

where they can answer with yes-no which elements are relevant for this, i.e. for the specific product, but the formulated cybersecurity requirements into the contracts, into the basic contracts.

00:20:31 Speaker 1

I think they made it very clear to me that cybersecurity is not only a regulatory requirement, but also a market requirement.

00:20:39 Speaker 1

This means that the manufacturers ultimately get pressure from 2 sides.

00:20:43 Speaker 1

Yes, thank you very much, Mr. Daudel,

00:20:45 Speaker 1

that they have given us these insights, that they have shown us, yes, what activities are carried out at their premises, that they have named important documents for us, that they have not only drawn our attention to the pre-market side, so to speak, but also to the post-market activities.

00:21:06 Speaker 1

and the guidelines that we can use to meet these regulatory and market requirements as elegantly as possible.

00:21:14 Speaker 1

Thank you very much, Mr. Daudel, for being there.

00:21:16 Speaker 2

Yes, thank you.

00:21:17 Speaker 2

Have a nice day.

00:21:18 Speaker 2

Thank you very much.