Zebra Your Edge Podcast

Host:

- **Chuck Bolen (Chief Software Architect) , Erv Comer (Fellow Of Engineering) , Adam Arruda (Project Manager – Mobile Computing Organization)**

Guest:

Transcript for Industrial Automation Insider “When Sustainability And Security Align” Episode

Chuck Bolen

00:00:00,790 --> 00:01:50,142

Today's topic is security and sustainability, which are both really relevant and hot topics that lots of people are talking about.At first glance, you may think they're somewhat conflicting.On one hand, security professionals will want you to update devices every year or two to ensure that you're fully protected.

On the other hand, we build devices that could last six to 10 years. And both from a sustainability standpoint - less devices going into a landfill and of course less budget to buy new devices - you might want to try to keep your devices for a longer period of time. So are the two really conflicting goals?

It kind of goes back to something I blogged about a few months ago.Just because the device may still be functional, doesn't mean it's without risk or the right thing for you to do to keep using that device for a longer period of time.

Joining me today are two experts in this area.Erv Comer who's a fellow in our engineering team with over 40 years of experience in security. And Adam Arruda, a senior product manager in our mobile computing organization.

Part of Adam's job is to balance features, life cycle and security. While not always a really easy task, Adam does a great job of creating that balance there.

So I'll put Erv and Adam on the hot seat today to help answer some of those questions on the topic.I wanted to start with something you said a few months back.Somebody else at Zebra had commented, she's starting to see security and sustainability aligning in our space.

You know, I know it's not as simple as just, you know, taking one device and replacing with another device. There's a lot involved for our customers to move to new devices. But you also, as I recall, you had said, you can absolutely have a long life span with devices as long as the software is updated.

The inflection point, as I recall, you saying, really had to do with what the customer's risk acceptance.Can you expand on that in terms of what you meant there?

Erv Comer

00:01:50,492 --> 00:03:01,911

Sure, sure.Chuck our devices are multipurpose in a bunch of different operating environments, serving a bunch of different use cases. From a security perspective, you actually want to provision these devices to meet the principle of least privilege, put them on a mission critical path.

So these devices that get locked down if you will to mission critical only, and that's the only thing they do, they can be kind of you will get a little big wall around them. If you will, in some senses.

You'd like to think of this. I always use an analogy of washing a pair of jeans. Right. When you first put your jeans on, they're brand new, they're stiff, they protect you from everything.There's no holes.A few years later, a few 1.000 or so washes later, you use them ... now you're starting to see the knees are wearing out. You're getting a few holes in places, maybe holes you wouldn't want. Same thing with devices, you know, after a few years, you're gonna start to see holes in these devices where you probably don't want to be seeing holes and there's some sensitive information that could be leaking out or you don't want people to see that sensitive information.

So that's part of what we've got to do with the security side of this is from: make sure it's ready for the future as well.

Chuck Bolen

00:03:02,992 --> 00:03:09,405

Cool. So that's an interesting analogy. I've never heard anybody compare our devices to worn jeans,but definitely applies.

Erv Comer

00:03:09,406 --> 00:03:11,255
Well, we got to know where our holes are at.

Chuck Bolen

00:03:12,215 --> 00:03:18,685
Well very apropos Adam, I know we add a lot of features to our devices to help control this. Can you expand on some of those?

Adam Arruda

00:03:19,676 --> 00:03:58,280
Yeah.So it's not just what Zebra does, it's who Zebra partners with.

So, on the Zebra side, we make sure customers have APIs and tools in place to help manage access on the device.

So if we wanna be able to maybe restrict access to settings, stop users from getting unwanted notifications, be able to do things that they shouldn't be doing on that device ...by doing that, they're more efficient and we have less support and security holes.

And on the other side, we partner with vendors like our E-MM providers who provide additional tools to help lock down the device and provide a much more tailored experience as Erv described.

Chuck Bolen

00:03:59,335 --> 00:04:04,384
Cool.So I can see how that could really help our, our customers really control that balance.

Erv Comer

00:04:04,736 --> 00:05:44,879
It's interesting to me now what we're talking about - risk -because if we see anyone buy what I'll call a low cost device these days for business use, I mean, I know there's some normalization around risk and security in that sense. It's going to be small business owners who may think, "No one really cares about me.They're not going to target me. I'm small potatoes in this game." So they let their guard down, they utilize their products, if you will, a little bit too long.

Bad actors then have the ability...I saw something that said something like 60% of small and medium businesses go out of business within six months of experiencing in a hack or a cybersecurity incident.

Hm.

Well, you would think that only buying devices would have top notch security, like a Zebra device, everything would be automatic and over the air updates.

Yet it seems more business owners and leaders are saying I just need the bare bones minimums in my device and nothing more for my front- line worker to access my systems.

Show me the cheapest option again, Dollars kind of rule sometimes. I'm not too worried about security but have some specific sustainability goals.

If I have to replace that phone in a year because they break, I'll do that. But if I suffer a data breach, I'll deal with it when it happens.

But I don't think I have to worry about that. All, the while, they're probably in the sights of a bad actors making themselves vulnerable, and they're creating all this liability for their business.

So, at the end of the day, it comes down to: why do we wanna go to that level? Price and sustainability even with large budgets, no one wants to overpay for security.But security is a baseline inside of the product.

Chuck Bolen

00:05:45,350 --> 00:06:18,372

So Erv, I think what you're saying, Erv, it's not just the cost of a lower cost regional device but what's the the value of the customer's proprietary data? What's the value of their customer's data that they're protecting and their reputation, right? So that all factors into their costs. So it's really not just about, you know, for these people who are not considering security in their devices. You know, they're risking a lot of, a lot of costs in addition to the cost of the device, Adam, what do you think? How does the trend towards low we cost devices impact security and manageability of our devices?

Adam Arruda

00:06:19,232 --> 00:07:31,030
Yeah, it's a great question, Chuck.

It's something that we keep in mind and keep an eye on quite frequently when we look at a lot of our competitors in this space, the one area that we see a gap is really in the consistency and their commitment to security patches and OS updates.

Whereas Zebra commits to a monthly security patch as well as additional patches for features and bug fixes. We see a very intermittent release cycle from our competitors, some maybe once a quarter, others once every six months and even within the same competitor, their products may vary.

So different models may get a different update at a different time and there's just no consistency there.

Now, why is it important? You know, there's been studies done by folks like ServiceNow and others that show somewhere in the range of 60% of all breaches could have been prevented because the patch was already available.

So that just shows the importance of two things: One, are we getting patches and security patch fixes out to our customers in a timely manner? and then, two, do we make it easy for them to get those patches onto the device?

And for Zebra, we can say yes to those things.

Erv Comer

174
00:07:34,430 --> 00:08:16,809
History, Adam, if you look back in time, we've actually beat Microsoft. Wanna-Cry was a ransomware that came out a few years ago.Microsoft released patches, people didn't install those patches and then actually look what happened with Wanna-Cry.

We don't want to see that happen inside of Android and that's why we make sure that as you said, even the back porting of our patches for the critical helps delay and avoid all of these critical vulnerabilities that people are experiencing.

The true cost is the cost of your data.

How valuable is the data and what's the value in that sense? What's the value of your job, your company and the data that really runs it? So it all comes down to data and protecting that data and understanding the security and the value of it.

Chuck Bolen and Adam Arruda
00:08:17,481 --> 00:08:19,685
Great example, great example.

Chuck Bolen

00:08:19,686 --> 00:09:04,539
Thanks Adam and Erv. So, you know, we talked about the trade off between life cycle and security, right?

Some of the challenges about, you know, manufacturers who don't consider security. It kind of brings us back to, the risk tolerance and kind of that inflection point of how much risk somebody is willing to take and how often they should be, updating their software and / or hardware.You know, one thing to keep in mind is, you know, some things are out of our control wtih Google and support for aparticular Android OS right?It may not be possible for us to to do as many updates as we would like.But we've actually worked really hard.We have a dedicated team to continue that support and to extend the life cycle and security, as long as possible.

Adam, can you give us some more details about, how we do that?

Adam Arruda

00:09:05,235 --> 00:10:06,900
Yeah, no problem. So you're right. There is a point in time, roughly three years after an OS launches, where Google does end support for that OS and the expectation kind of from the consumer world is you continue to move forward, whether you're with Windows, Apple,Android. That's kind of the motto in the consumer world, but it's not always the same in the enterprise.

And because of the longevity of our devices, we do go out of our way that even when Google support ends, that we continue to provide critical security patches for those devices.

So that's something that we offer well beyond that three year period, in some cases, it could go 3, 4, 5 years depending on the type of device that you've bought, where we continue to offer quarterly critical patches for anything that Google highlights, and we'll take a look at what they've found, we'll validate: does it impact any of the devices that we may have released in the OS that they're residing on? And then we will make sure that we offer those patches to our customers.

Erv Comer

233
00:10:07,951 --> 00:10:24,649
So, Adam, good security wisdom here says to always keep your device updated, especially a high profile device. Those should be updated and sometimes, the look beyond this again, the importance of the data and sensitivity of the data that you're dealing with on your devices comes into play.

Adam Arruda

00:10:25,970 --> 00:10:28,969

Yeah, and that's that risk profile that you were talking about.

Erv Comer
00:10:29,530 --> 00:10:39,951
Yes.

What's your overall risk acceptance? How much data are you actually willing to leak out and allow it to go public if something were to go wrong because you didn't keep your device updated?

Chuck Bolen

00:10:41,241 --> 00:11:02,809

So, you know, I think the moral of the story here and what you're both saying is you can't compromise on security, right? You might be able to decide how much risk you're willing to take. But if your device has any business-related data on it, any customer data or drives your business, right? Its Enterprise grade security is really nonnegotiable when deciding on a mobile device.

Erv Comer

00:11:04,480 --> 00:11:07,690
Absolutely, security is fundamental.Yeah.

Chuck Bolen

00:11:08,271 --> 00:11:45,036
So, I think that's a great summary here, right? You know, just kind of wrapping up, you know, we talked a lot about sustainability. You know, sustainability, we do a lot obviously in extending the life of our devices so people can have them, use them, for a longer period of time and avoid them having to be going to landfills.

But there's other things that we're doing and how we manufacture, how we ship devices and things like that, you know, beyond kind of the tradeoff between life cycle and security.

So I appreciate Adam and Erv joining us today, a great conversation.I appreciate everybody for listening in.
Thank you.

Adam Arruda
00:11:45,328 --> 00:11:45,916
Thank you.

Erv Comer
00:11:46,337 --> 00:11:46,906
Thank you.

NA and Corporate Headquarters
+1 800 423 0442
inquiry4@zebra.com

Asia-Pacific Headquarters
+65 6858 0722
contact.apac@zebra.com

EMEA Headquarters
zebra.com/locations
contact.emea@zebra.com

Latin America Headquarters
zebra.com/locations
la.contactme@zebra.com