Security versus virtual working

Tim Nyland-Jones, Information Security Manager at Northgate Vehicle Hire, investigates why IoT software and interoperability are still a long way from being standardised.

The 'make it work, make it right, make it fast' mantra is an oft-quoted one in the world of software development:

- Make it work: do the minimum necessary to create a product that meets functional requirements
- Make it right: do the important work to make sure that the main risks are addressed around legality, compliance, etc., that it passes all tests, and conforms to our best practices
- Make it fast: now that the product does all the things we need it to, and does them properly, the code needs to be made as lean and efficient as it can possibly be.

Business need drives software development; that's why concepts like agile and extreme programming have become so popular; they allow development effort to be targeted towards what will really deliver business benefit.

And that's great if you're working on powerful servers, with mature platforms, using frameworks that have been developed and refined over years - you know that the security is already there from all that prior experience, even if the product is only at the 'make it work' stage.

But when we're looking at IoT devices, with their small processing footprint, and myriad operating systems, there's not always a lot of room for security, and the development focus tends to go on what customers pay for - functionality. At the moment, it's enough that you can switch the light on with your phone.

The software running on many IoT devices right now certainly 'works', but is it 'right'? What if others can switch your light on with their phones? As enterprise IT professionals implementing new technologies, these are the kinds of questions we're more interested in. What risks are introduced by installing these devices in our infrastructure? And how do we handle those risks?

There are many different technologies in use in the world of IoT right now and in some cases IT departments may find they are simply not involved in an IoT implementation in their business. Hence, we need to arm ourselves with a practical, constructive approach to deal with common risk factors.

Are there standards we can make use of?

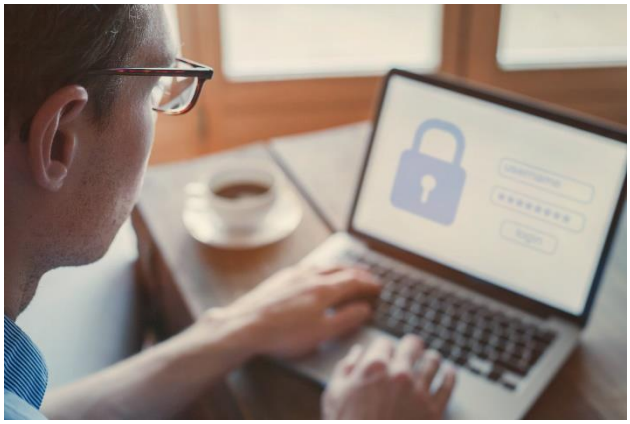
While international standards for an organisational approach to information security such as ISO27001 have been around for a good number of years now, a similar software-level standard has been more difficult to get in place. ISO 27034 (application security) may go some way to meeting this need but is currently incomplete.

Looking specifically at IoT devices, there are numerous frameworks and platforms to assist with interoperability - Apple's HomeKit is probably the most well-known but this is targeted at the consumer market rather than business; all the usual players like Amazon, Google, IBM and Microsoft provide IoT integration frameworks; there are also many open source options.

In short, the complexity of software development and the immaturity of the IoT sector together mean that IoT software and interoperability are still a long way from being standardised.

So how can we be responsible users?

In the meantime, some common-sense questions based on the UK Government's Cyber Essentials programme may begin to provide a practical framework for using IoT devices in the enterprise. These are:



- Usernames and passwords - Many recent problems with IoT devices have come about because of default credentials either being unable to be changed, or with credentials being entirely embedded in the software code. To provide assurance, all accounts should be documented and there should be a mechanism for changing them.
- Encryption - All user data on any IoT device must be encrypted, and responsible users would expect to see documentation of what algorithms are used. IT departments need to know vendors aren't rolling their own encryption. So, we should ask what encryption is used – the only reason vendors would have to keep the encryption algorithm secret is if
  (a) it's no longer regarded as secure (MD5, SHA-1) or
  (b) there isn't actually any encryption...
  Patching - Nothing we ever install is fully secure; this is even more true in the cast of IoT devices. If we're managing devices on our network, we expect that they will be patched regularly. Therefore, we should ask how often, and for how long, we can expect to get security updates for it. Because once our device is end-of-life, we'll need to replace it. Also, we'll need to know where the updates will come from; it would be great if they came as automatic notifications, but if not, a web page to visit regularly would work too.
- Vulnerabilities - How do they get reported? Hopefully not by Sky News or the BBC! All users of the device should have a method of reporting any vulnerabilities back to the vendor; that way we all find out about problems and get them fixed quicker. Of course, we need to be sure that the vendor acts on them, too.
- Testing - Can you provide evidence you've tested the device already for vulnerabilities? What was found? Have you put an action plan in place, or is there a roadmap for further developments and fixes?

What else?

Maybe we didn't get the chance to ask all the questions we wanted to before the devices arrived. However, there are still plenty of things we can do to mitigate - on the basis that the devices will be inherently insecure:

- Segregate - Any IoT devices should be kept well away from the main corporate network. You probably already have mature patching and security management practices for your main network - don't compromise them by allowing devices with the potential for basic security holes in there.

- Test - If the vendor can't provide their own testing results for the devices, and you don't have the skills within your own IT department to test the devices, there are plenty of companies out there who will be happy to test them for you and report back.
- Patch often - Once IoT devices are in, it's easy to forget they need patching - but if the vendor's not able to provide an easy way to flag when patching is required, it's up to us to remember. A once-a-week check is appropriate. And more often if the headlines dictate!

One final point to note: the IoT devices on your network may not actually be under your control - they may be managed separately by a third party. CCTV is a common one for this; the facilities department manage the contract with the CCTV provider, who install the kit and provide access to staff, and no-one really regards it as needing any IT involvement.

Then there's an incident: a CCTV box was hacked - if we are lucky, it just became part of the latest botnet; if we're not so lucky, our CCTV was taken down so our premises could be broken into. Either way it's now IT's problem.
Who's responsible for patching? No-one really knows. It is tempting to start playing a blame game at this point, but at times like this the business is looking to IT to solve the problem, so it's very important that we approach a situation like this constructively.

Managing the risks

Many of us in IT will not come near to the internal workings of IoT devices. But we have all got a duty to ensure we manage the risks facing our businesses, and make sure we, the manufacturers and vendors, don't just 'make it work', we all 'make it secure'.

Further reading

- ISO27034 discussed in detail
- Two articles on standardisation options: Standardising IoT Standards and Groups and IoT Cloud Platform Landscape
- The full Cyber Essentials questionnaire
- More on Security courses from TSG Training