The UK Cyber Essentials Requirements for IT Infrastructure provides a window into GDPR expectations for data security requirements

12 September 2018

The EU's General Data Protection Regulation (GDPR), which went into effect in May 2018, requires companies to implement appropriate security measures when handling personal data. But, although it lists a number of types of security measures that may be appropriate, the GDPR is not always precise or direct about the specific measures to be implemented, says Nathan Salminen, a senior associate at Hogan Lovells in Washington, D.C. He noted that data security teams often struggle to translate the GDPR's requirements into specific policies and procedures. And there's another complication: because the GDPR is new, there is no precedent as to how the regulators will apply its requirements in practice.

Fortunately, the Information Commissioner's Office (ICO) in the UK has issued additional guidance, which relies heavily on an existing standard called the Cyber Essentials Requirements for IT Infrastructure. In this hoganlovells.com interview, Salminen details several guidelines in Cyber Essentials, including five basic data security topics: firewalls, secure configuration, access control, malware protection, and patches.

Can you give us an overview of the Cyber Essentials guideline and its relationship to the GDPR?

Nathan Salminen: The GDPR has a number of security requirements, but those security requirements are sometimes vague. They're really high level and general, and use language like, you need to implement "appropriate measures." A lot of tech security people are struggling with trying to figure out what that really means.

There are a handful of different sources of clues. One of them is that the UK's regulator — the ICO — published their own guidance about security under the GDPR. That guidance refers frequently to a standard they released earlier, called Cyber Essentials. Cyber Essentials, unlike the GDPR, is a pretty detailed playbook, with a list of specific measures in each area. We don't know that outside the UK they'll necessarily defer to this list, but within the UK, they likely will, and outside the UK it's at least a clue as to what they're looking for.

Can you walk us through the main areas in the Cyber Essentials document that clients should be aware of, starting with mobile

devices?

Salminen: A number of the requirements in the Cyber Essentials are predictable sorts of things that everybody expects to be required of them, but there are areas where it deviates from normal expectations, and those are the areas that I'll highlight.

Regarding mobile devices, there are a couple of things. One is that they expect that any device that connects to the network is in scope of the company's security responsibility, and that would include personal devices. So companies that have "bring-your-own-device" (BYOD) policies may have a greater responsibility with regard to those devices than they might under other schemes.

Another expectation is that — and this is sort of an odd one — phones are required to have some sort of malware protection. Malware protection as we think of it is not common on phones. You don't usually have virus protection software on a phone. But luckily, the Cyber Essentials defines malware protection broadly, so that it includes sandboxing and application whitelisting, which are technologies to limit what apps can be installed or to run apps in a secure way, such that they can at least contain the harm done by malware.

You've also mentioned another area that Cyber Essentials covers, which addresses service providers.

Salminen: With service providers, this is always a tricky line to draw: where does the company's responsibility end and its vendor's responsibility start? And that's something that we struggle with in a lot of different contexts.

The Cyber Essentials took a pretty clear stance on it, so that's interesting. They said that, with regard to software-as-a-service (SaaS), and platform-as-a-service (PaaS) offerings, those are essentially within the vendor's universe of control. So you have to enter into an agreement with the vendor where the vendor agrees to protect the data, but you don't yourself have direct responsibility for configuring the security.

But, for infrastructure-as-a-service (IaaS) offerings — like Amazon web services, places where you're configuring everything, where they're putting up a type of a box and your applications run on and configure the operating system, the security, and all of that — then those are considered more your responsibility rather than your vendor's. Essentially what they're saying is that the party that's in the position to control security is responsible for controlling security. Which makes sense.

The next topic — and this is common to security standards, but it is probably more expansive in the Cyber Essentials guidance than it is in the GDPR itself — is that they talk about a number of areas where you need to document the decisions that you make. So you should be documenting any sort of big security decision you make, and any decision not to implement an important type of security control or to make an exception from a security rule.

A couple of ones that they specifically noted: if you set up a rule to allow inbound traffic through the firewall, and that's something that you should document. Also, if you want to give a user permission to access websites that are potentially malicious, you want to document that.

What are the best practices when it comes to documentation?

Salminen: It isn't really clarified in Cyber Essentials. You just want to maintain some sort of record that you could point to. Essentially, the scenario that would come up is that a regulator comes to you and says, why did you do this thing that resulted in a data breach? It looks like maybe a bad decision in their eyes. You want to be able to go back and say, we did it because of *this*. You're trying to prove to them: I'm not just making up that rationale now, this actually is what we were thinking in 2016 or whenever we made that decision.

So as far as a best practice, you want to keep it somewhere centralized, not just having it stored in peoples' e-mail boxes. You want to make sure it's a record that will survive. It's not a bad idea to have it in the files of the chief information security officer or someone like that, who will have a responsibility to pass those things along if they move on. But there isn't a particular format that is required. Other legal requirements may have more specific requirements for documentation, and those should be kept in mind as well.

What does Cyber Essentials say about systems and patches?

Salminen: For systems and devices, they have a couple of requirements that I think have been seen as sort of a best practice for a long time, but have not really been seen as a baseline requirement. They're kind of elevating them up to a baseline requirement. One is to remove any unnecessary user accounts. So, for example, a standard Windows installation comes with a number of pre-installed accounts that you may not actually need, like guest accounts.

You're also obligated to remove any auto-run feature. So, you know how on Windows, you can set it up so every time I login, it should open my e-mail or something like that? That capability is frequently exploited, so Cyber Essentials requires disabling it.

The next topic is patching. Applying patches in general is a requirement and pretty much an everyday security standard, and has been a standard practice for a long time. But they add one specific detail that I think is important, and that's for patches to vulnerabilities that are identified as critical or high risk. They require you to deploy the patch within 14 days of the patch being released, which is not necessarily easy or consistent with the practices of a lot of companies. A lot of companies typically roll out patches once a month, or maybe they roll out operating system patches frequently but patches for applications that are less widely used less frequently. Cyber Essentials puts a 14-day clock on all of those, which is pretty aggressive.

I understand that IT professionals are looking for clarity, and that the GDPR is broadly written and will probably evolve over time. So

how do we help our clients navigate the vagueness in the GDPR now?

Salminen: We frequently help companies with these questions and advise a lot of them on how to comply with the security requirements of the GDPR. We have done a number of GDPR security assessments. Sometimes we bring in a consultant to work with us while we've led them. The particular measures that make sense and satisfy the requirements vary significantly from one context to another, and are sometimes judgment calls, so we try to rely on whatever guidance we can find when advising clients in this area, including the Cyber Essentials.

What's involved in a GDPR security assessment?

Salminen: There's a wide range of definitions of what a security assessment could mean. Companies that come to realize they are required to comply with these security requirements go through some sort of process to determine whether they meet those requirements and what they need to improve. That process can range from just looking for the very biggest risks to the most important data, up to a much more exhaustive review. A company can make a risk-based decision to conduct a review with a limited scope, or it can say, many of our systems have personal data, maybe we're a high-profile company, so we want to do a really thorough, extensive assessment.

So security assessments range from a few days' work to multiple years' work, depending on the size of the company, the sort of data they have, the nexus they have with Europe, and how risk averse they are.

EU companies were supposed to be GDPR compliant by 25 May 2018. Do some companies still have work to do in terms of being compliant?

Salminen: Yes, the compliance date has already passed. Very few companies were 100 percent compliant on May 25. And regulators are just sort of firing up the enforcement engines. They may be currently focusing on some of the very biggest, most high-profile companies. And they have maybe not yet worked their way down to most of the other companies, but they're coming. And were a regulator to come, you would ideally like to point all the way back to the May 25th deadline and say, we were already compliant then. Many companies can't do that.

So it's a question of, how bad will it look to the regulator. The more ducks you have in a row earlier, the better that will look to regulators. In any case, we advise that you reduce your potential risk and liability by moving towards compliance as quickly as you are able.

About Nathan Salminen:

Nathan Salminen counsels clients regarding transactional, privacy, and cybersecurity matters. He

focuses on helping his clients secure favorable terms in agreements that involve sensitive or valuable data, evaluating the privacy and data security risks associated with mergers and acquisitions, assessing data breaches, and assisting clients in complying with privacy laws. He advises leading companies regarding the privacy and data security terms in service and licensing agreements, with a focus on agreements that involve personally identifiable or other regulated or sensitive data. Before becoming a lawyer, Salminen worked as a software engineer for 13 years, and has broad knowledge of software development and network security.

Contacts

Nathan Salminen
Senior Associate
Washington, D.C.

> Read the full article online