By Tara Cho (Chair of Womble Bond Dickinson (transatlantic law firm) US Privacy and Cybersecurity) and David Clarke (CTO of The TrustBridge)

edited by Penny Heyes

The Wisp, the Written Information Security Program has been more relevant in the US until recently, but now it's becoming more and more known and adopted in the UK. In this article we ask:

- What is the importance of a WISP?
- What exactly is required?
- Is it really necessary?
- What are the advantages of having one?

What is the importance of a WISP?

It is a legal requirement in most US states now to have a WISP but as yet there is no federal regulation**.** In fact, the US approach at the federal level is still quite sectoral. This can be illustrated when we look at HIPAA (The Health Insurance Portability and Accountability Act controlling the lawful use and disclosure of protected health information in the United States) which is one of the prime examples of a more structured security law at the federal level, but it would only apply to certain entities in the healthcare sector.

However, as yet there is no one, one size single stop federal standard for the WISP.
The key thing for organisations to remember is that the requirement for a WISP is not just for entities that are registered with their head offices in the states where it is a legal requirement that have to have one, but also organisations that operate or have **any** business in **any** of these states, regardless of where the head office is registered.

If an organisation is operating in those states and is collecting data of any residents of those states, most of the US laws apply. The situation is the same for data breach implications and privacy and the legal rights of citizens. It is pretty hard to escape the need for a WISP, for instance, if you have an online business that could touch everybody across the internet in all jurisdictions.

It would be hard to have a single standard at a federal level because the cyber situation and the threats evolve so rapidly. However, the requirements for a WISP address universal needs, whereas the actual security implementation can ebb and flow.

Governments, especially the US and the UK governments, are giving absolute specific guidance. There are 15 to 20 high level components that both governments would expect organisations to be aware of and be doing. And of course, most of those need managing.

So, how do you manage them? You need a policy and the WISP effectively could be seen as a high level policy that states that the organisation is undertaking the required procedures, and has the relevant policies in place and is keeping them up to date.

What exactly is a WISP?

In simple terms, a WISP is a positioning statement that explains what a specific organisation will do / does to protect personal data: what security obligations they fulfil, some detail of how they do

them, who is responsible, point of contacts, how the organisation manages risk, how it manages security technology.
A WISP can be quite detailed, although no organisation should be releasing information about their security protocols, or making intellectual property and specifics for the organisation public. There is a fine line between giving too much detail which can be taken advantage of by malicious actors, and by stating that you have a risk governance committee in place.

Stating that you have serious security change control, you keep up to date with patching etc is sensible but the information should be generally kept very generalized.

Clearly, an organisation should have all its data protection and cyber security policies and processes in place, before they can even start writing a WISP. Frankly, the WISP is just the tip of the iceberg…a commitment made make publicly and which needs to be backed up with real activity. An organisation needs policies and procedures, backed up with an evidential trail that supports those policies and procedures, which is regularly reviewed and updated.

What is required?

Having a SOC2 certification or an ISO 27001 certification does not negate the need to prepare a WISP but if these are in place, an organisation will have all the information already to write a very simplified WISP.

SOC2 can be quite detailed, but the principles could be extracted and put into a WISP.

A WISP should be a well documented and detailed part of an organization's governance. Its preparation and publication often allows the senior management to see and understand what policies and procedures are in place, who is responsible and accountable, and the level of risk the organization is prepared to accept. It will identify gaps but will ensure that the organization is prepared and resilient.

Under various data protection regulations, there is a requirement for evidence and audit trails, and with a WISP, it is necessary to evidence certain things so that if an organisation's WISP is challenged it can prove that it is really following the policies and procedures it has declared.
Also, the organisation needs to make sure that the WISP is maintained.

Especially, as people change roles and staff changes, so in order to make sure that a level of knowledge and understanding of the security and data protection policies and procedures is being maintained, all personnel should have security training. And this must also be evidenced, via a learning system and the audit trail.

Is it really necessary?

3rd party Due Diligence

The concept of the WISP has been created and adopted by many European and UK based organisations for the purpose of managing due diligence, especially in the third party supply chain. As described, most organisations have received questionnaires from potential clients, partners, alliances. These questionnaires ask for information about data security protocols, which can help the third party gain a level of reassurance that such policies and procedures are in place.

Many organisations, especially in the vendor sector, are inundated with these questionnaires, which require regular updates. Although it can be possible to limit, contractually, how many times an organisation has to complete them in one year and there are some efforts in the US to standardize this evaluation for third party vendors so that they are obliged to complete it once in a given year. Some of them are quite intrusive and do present potential security risks in themselves.

A well-documented WISP is a good alternative for the questionnaires and can be used across their customers more consistently. Some vendors will seek SOC2 certification or other qualifying certifications or assessments to try to shortcut this process.

Outside the USA, the need for a WISP is not mandatory, however, in our opinion it is a great idea: having a prepared public statement about the security and data privacy protocols that are practised by your organisation is best practice, as well as economically sensible.

Liability

Further to the evidence considerations, there are few US states where having certain components of a WISP well documented can be a safe harbour to data breach liability. For example, in Ohio, a WISP could be used to escape some litigation and other impacts in the event of a data breach when talking to the regulatory authorities. However, in those instances, it is not good enough to have a superficial document with no real substance to it. A proper WISP shows that the organisation has taken it seriously and actually undertaken and has the ability to demonstrate that it is operational. In a similar way to the SOC2, it needs evidence of continuous audit.

Throughout the pandemic we saw such a surge in cyber attacks, especially as everyone pivoted into remote working. Since then cyber insurers have enhanced the level of questioning and evidence of the measures organisations are taking. Some require regular penetration testing too. If an organisation manages certain types of regulated data or more sensitive data, any insurance policy questionnaire will be even more onerous, as is the level of evidence that has to be provided. Recently we have seen big data breaches with no insurance payout because the organisation didn't adhere to the required (and stated) procedures.

If any regulator scrutinizes a WISP and it were found to have been created but not followed, an organisation would be considered to be non-compliant with its own standards, its own policy. The WISP should not be just a check box exercise.

Of course, all relevant documents sets, policies and procedures have to be in place before the WISP can actually be written.

Who is responsible?

Senior management within an organization is responsible for the WISP – it is a governance issue. So board members should approve it, provide the direction although not necessarily operate it. As with all the data protection regulations, the WISP needs to be taken seriously at a senior level.

In the US there is some agency guidance, which might not always be construed as legally binding. The implication under recent departmental guidance suggests a fiduciary duty, and this will of course create a ripple effect into contracts that may well state that the organisation needs to have a Written Information Security Program.

What are the advantages of a WISP?

There are obvious advantages for an organisation to have a WISP. A consequence of preparing one, is that personnel focus on how they potentially need to react when then, when there is a cyber incident because they have possibly haven't thought about certain things, and the WISP is actually making them focus.

For example: what is the incident management plan? Does anyone know what to do, who to alert if they suspect an incident has occurred ? And how does the senior management know, unless they've encouraged staff, suppliers, anybody who deals with your company to review the plan?

All data protection and cyber is fundamentally based on risk and it's how you manage that risk that is key. The WISP provides a tool to give guidance on where to focus, a means to mitigate trouble with regulators as it demonstrates management and control.

Many of the US privacy laws have requirements around documented risk assessments, particularly for sensitive personal information. These are similar to the requirements under the EU GDPR and UK GDPR for a privacy impact assessment.

By having a WISP, the organisation can manage those specific legal components that are required, obviously making it easier and more effective to operate those prescribed components under state laws, which will then help with the insurance exposure and breach liability where an organisation must maintain reasonable and appropriate security.

Having a WISP will definitely help further protect an organisation by actually implementing those controls in a less superficial way. For example, some organizations like to draft their privacy policy first because they know that it is a privacy law requirement. In order to do that, it necessitates a data inventory, understanding what data they are collecting, where it's going, how it is being protected, how data subjects' legal rights are effected. The WISP is like that: if you want to have an effective WISP, you have to know the policies and procedures you have in place to how protecting the information, how users/ employees are trained, or how access to data restricted. All these things are necessary; it's good for insurance protections, it is good for legal risk.

In addition, the work associated with answering 3rd party questionnaires, as discussed above, will be reduced. Your response will be quicker and easier.

Key Message

The key message here is that having a WISP is a very wise thing; it is a really good idea to have one of these, even if it's not necessarily a legal requirement in some countries at the moment. It is a way to manage your data assets really well, to manage your data protection and your cyber protocols well, and focus the mind.

The WISP is really meant to serve a purpose; it forces senior management to think about those cross-functional activities and take ownership, which will again impact the cyber liability coverage, the legal risk, and the business reputation.

As with all data protection and cyber policies and procedures, the WISP must be looked after and managed, monitored and maintained.

A webinar discussing this issue is available here:
https://www.youtube.com/@adpfromthetrustbridge5808

For more information please contact

Penny@thetrustbridge.co

www.thetrustbridge.co

tel +44 (0) 7768 962 480

Authors:

Tara Cho is a Partner at Womble Bond Dickinson (US) LLP and is Chair of Privacy and Cybersecurity practice at this AmLaw100, transatlantic law firm.
Tara is a board-certified specialist in Privacy and Information Security Law, assisting clients with data security design and assessments, contracting, breach response, and other privacy and data security compliance needs across industry sectors, such as retail, finance, technology/software development, healthcare / health tech and life sciences. Tara also counsels clients in commercial transactions involving data assets, use rights and international data transfers and data privacy matters throughout the data life cycle. Tara became certified as a legal specialist in Privacy and Information Security Law by the North Carolina State Bar Board of Legal Specialization in 2018 as part of the inaugural class of specialists in this field. She is also recognized by the IAPP as a certified information privacy professional for both the U.S. (CIPP/US) and Europe (CIPP/E).

Tara provides guidance on matters related to the US individual state data privacy laws such as CCPA, CPRA, HIPAA, COPPA, CAN-SPAM, and other state and federal privacy, security and data breach laws in the U.S. She also advises clients on the EU and UK GDPR and related requirements of European data protection laws.

David Clarke FBCS, Chief Technology Officer, The Trust Bridge
Dave is a highly experienced Chief Information Security Officer/Cyber Security and GDPR Management and Consultant with a deep knowledge of Global project delivery and operational leadership. He operates across FTSE (Financial Times Stock Exchange) 100 index companies, SME and start-ups within Financial Services, FinTech, Telecoms, Technology and Utilities sectors developing strong coherent cyber security, GDPR data protection and privacy strategies.

When working for BT, Dave created a Global Infrastructure for the World's Largest private trading Network, Trading $ 3 Trillion a day, and has managed Multiple Global Security Operations Centres for Reuters and British Telecom.

He is the founder of GDPR Technology Forum with over 23,000 members https://www.linkedin.com/groups/1201767

David has been recognised as one of the top 10 most influetiual thought-leaders by Thompson Reuter in risk management, compliance and regtech in the UK and features in top 50 list of Global Experts list by Kingston Technology

More recently he has been working with companies to help them achieve their ISO 27001 accreditations. He is a speaker in much demand

Editor: Penny Heyes

Penny is a co-founder of The Trust Bridge and the Chief Commercial Officer. A highly experienced international sales, marketing and business development professional, she has worked in multiple product & service sectors, globally, and has been instrumental in the growth of several start-ups, early-stage companies, as well as multinational established businesses who wish to diversify into new areas or new initiatives.

More recently she has been advising clients in their Innovation in Business strategies, examining how technology is changing how businesses run, engage with their customers, employees and suppliers by creating an effective strategy and finding the right solution or solution partner to implement.
She also launched ADPP – the peer to peer community for Data Protection and Cyner professionals
www.digitalarena.co