Ronald Kelson
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

Benjamin Gittins
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

Synaptic Laboratories Ltd.
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Wednesday, 27 January 2010

PART 4 OF SYNAPTIC LABORATORIES LIMITED INPUT TO THINK-TRUST's CONSULTATION ON THEIR DRAFT "D3.1B RECOMMENDATIONS REPORT" TO THE EUROPEAN COMMISSION

The need for the EC to fund the development of an electronic requirements management process and deliverables to support existing standards, existing policy guidelines and existing laws of several nations simultaneously in a unified model that also supports national and regional variations.

Such a process could also include new standards requirements and best practice recommendations as they become available.

The process and deliverables would reduce costs and duplication of effort across European organisations and remove the existing discriminatory barrier that all micro and SME face when attempting to create innovative solutions that satisfy legislative, standards and best practice for the European and global markets.

1. The importance of codifying standards, laws and policy requirements electronically

The US National Institute of Standards and Technologies Computer security Division has 17 active Federal Information Processing Standards[1] (FIPS), and over a 100 active Special Publications[2] that all Federal Information Processing systems must comply with. These standards and special publications relate to information assurance risk management processes, identity management, cryptographic security standards, configuration of security hardware, business survivability, achieving high availability, auditing, physical access controls and other important subjects relating to information processing.

The NIST FIPS and SP documents are freely available to the public and can be used as a basis for creating IT processing systems by non US Federal organisations. This body of work represents many "best-practices" that could be adapted for use internationally and if adopted, would result in a more secure global IT infrastructure. Corresponding documents are known to exist for the UK and Europe.

The Payment Card Industry Data Security Standard[3] is an example of an industry standard that must be met by organizations that process card payments.

In addition to these information processing standards, there are a large number of national and international laws that a company is required to comply with. For example some international companies might have to simultaneously consider, the European Data Privacy Directive[4], the American Health Insurance Portability and Accountability Act (HIPAA) of 1996, US Communications Assistance for Law Enforcement Act, US Electronic Communications Privacy Act, the German Informational self-determination law, the Canadian Personal Information Protection and Electronic Documents Act and so on.

It is exceedingly difficult for a new software project (such as an e-commerce web-site) to know that it has met these requirements. This difficulty is compounded because the requirements are not readily defined in an exploitable format. There is currently no mechanism available for a new project to import all the legislative requirements and best practice recommendations on data privacy into a requirements management tool. Each project must individually identify, and read the relevant laws, manually extract the requirements (imperfectly), so that they can then begin to show traceability of requirements satisfaction down to the executable, test suite and business processes. These requirements will need to represented in open standards based formats so they can be imported by most of the project management and requirement management tools. For example the process should generate deliverables that can be imported by tools like Borland CalibreRM and IBM Rational DOORS and their open source equivalents.

We note that many of the Think-Trust ideas implicitly require this type of deliverable but D3.1B does not explicitly propose it.

For example section 4.4 of Deliverable 3.1B states: "Accountability is a research priority, as it creates the means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress." Section 4.2 of Deliverable 3.1B recommends "verification of conformance requirements". Section 4.3 of Deliverable 3.1B raises the question of supporting different legal domains that have different priorities stating that "Technology is needed to support this 'dynamic switch of security controls' based on legal and best practice policies".

Clearly this can only be cost effectively achieved if the laws and legal policies requirements are electronically specified and can be traced through to the source code.

If every large organisation must build a requirements document for themselves already, so they can be sure they satisfy their obligations under law, then it makes sense that this be done in an authoritative and comprehensive manner so that the singular effort can facilitate the creation of law abiding, secure IT systems by even the smallest micro innovative design company. This lack of co-ordination and unification within at least one set of design tools **discriminates heavily against smaller corporations and constitutes a serious barrier to the creation and dissemination of new solutions.**

---

[1] http://csrc.nist.gov/publications/PubsFIPS.html

[2] http://csrc.nist.gov/publications/PubsSPs.html

[3] http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

[4] http://en.wikipedia.org/wiki/Data_Protection_Directive

2. An example of how capturing the security requirements of other countries could help Think-Trust meet one of its identified objectives

We quote the following requirement stated in section 4.10 of T-T D3.1b:

> *"There should be constant engineering vigilance about economic viability. Is it more cost-effective to prevent a data breach or just address the consequent damage when one occurs?"*

In National Security Systems and US Federal IT Systems this subject is comprehensively addressed under what the US call an "Information Assurance Risk Management Framework". The principal goal of the US National Security Community Information Assurance (IA) risk management approach is to enhance the mission assurance posture of the US National Security Community by protecting its information assets. An IA Risk Management Program enables a US Federal Department, Agency, Bureau or Office to successfully assess IA risks arising from information systems, prioritize those risks, implement security controls to mitigate the risks and meet their information assurance priorities, assess the operational performance and effectiveness of those controls, and maintain the appropriate level of trust that enables the sharing of national security information with other enterprises. *For more information on the comprehensive American risk frameworks, see CNSS Policy No. 22, FIPS 199, FIPS 200, FIPS SP 800-53, CNSSI-1253 and FIPS SP 800-60 as starting points.*

This comprehensive framework attempts to ensure that the security controls applied to a particular information system are commensurate with the potential adverse impact on organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

It would seem desirable to electronically encode the national requirements for the US, identify and electronically encode all equivalent efforts in the EU, and then create a unified model security model that draws out the common international requirements and create regional appendixes for localization efforts. This common framework would provide an excellent platform for enabling the global community to increase assurance of our common service and software infrastructures, while also reducing the cost of regional certification efforts when desired/required. **This could be a joint undertaking by the US and the EU.**

If we side step out of information assurance and consider the European Data Privacy Directive, this is an example of where Europe could "export" its enhanced social norms to be facilitate their adoption by US organisations seeking to improve their data privacy operations internally within the US and to ensure they are providing appropriate protection of the data they manage on European citizens and organisations.

3. Synaptic's recommendations to Think-Trust

We argue that D3.1B should strongly point to the need for the codification of EU standards, policies, and laws in an electronic format that can be exploited by requirements management and reporting tools including:

- Parallel deployment of laws, policies and security standards as electronically importable requirements that permit their ready adoption, integration and verifiable traceable compliance in existing and future systems. In this context, Systems includes business, software and hardware processes,

- Establishing a large scale project to identify the common themes and requirements of international laws, various national laws, policies and standards, and unifying those requirements in a single suite of electronic requirement documents, and then building annexes that outline the variations and additional requirements that must be met to satisfy any given jurisdiction or law. Priorities of requirements should be advised by Governments as part of a safe-harbour arrangement to protect organisations so long as they can show strong evidence of their progress towards obtaining full compliance of their systems in independent audits,

- Ensuring that the system of requirements is maintained real time, and safe-harbour provided to organisations who have shown compliance with electronic requirements if there is a gap between the occurrence of law on paper and the subsequent rendering of that law in electronic form,

to enable organisations/corporations of all sizes (Micro, SME, large enterprise) to adopt and show compliance to regional and international norms and thereby provide appropriate confidentiality, integrity and availability of software systems for all stake holders. END

About Think Trust

Think-Trust (T-T) (www.think-trust.eu/) is an F5 Coordination Action under Framework Program 7 (FP7) Challenge 1, Objective ICT-2007.1.4 – Secure, Dependable and Trusted Infrastructures. T-T has been allocated the task of helping to coordinate the response to the needs of a trustworthy ICT future in Europe, through working groups, surveys and consultations resulting in Reports with recommendations and priorities about what needs to be done. Its target audience is the European Commission and policy-makers responsible for future direction, strategies, and priorities for European ICT. T-T deliverables complement the RISEPTIS (Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society [5]) work by providing feedback on priorities based upon input from their various activities and input from the perspective of participants in the European ICT Framework Programme. T-T has completed and published a Report entitled "Recommendations Report" D3.1a [6] and has provided to Synaptic Laboratories Limited a draft of D3.1b for our input prior to its publication. This document forms Part 1 of Synaptic Laboratories Limited input to D3.1b.

About Synaptic Laboratories Limited

Synaptic Laboratories Limited is developing the next generation of secure communications products and protocols to protect global communication networks. Synaptic is guided by a vision of "Long term, high-assurance global data security for all stake-holders".

Synaptic drives data security through the development of innovative security technologies founded on well studied cryptographic techniques. Synaptic can be found on the Web at http://synaptic-labs.com

The Synaptic CTO has been the guest speaker on post quantum security **without the use of quantum cryptography** for three consecutive years at the World Smartcard and Electronic Identification Congress CARTES held each year in Paris, FRANCE.

Synaptic responded with three submissions to the public calls for new 'leap ahead' cybersecurity proposals issued by the US Government's Networking and Information Technology Research and Development Program (NITRD).

Consequently Synaptic Laboratories CTO was formally invited to attend their 'closed' by invitation only' National Cyber Leap Year Summit. The Summit brought together government, industry and academia including the USA's leading innovators to identify requirements and proposals for next generation cyber security solutions. Several Synaptic proposals were taken forward at the Summit. At this Summit Synaptic also actively promoted SecureIST and ThinkTrust deliverables, and consequently Think-Trust is referenced by name along with Synaptic authored proposals in the Summit Participants Idea Report. This Report has been fed as input into the US Administration's cybersecurity planning. More on the Synaptic participation in the US Cybersecurity Initiatives can be found here[7].

Through its participation in US cybersecurity initiatives Synaptic Laboratories Ltd. acts as a bridge to promote European ICT research and planning projects, such as Think-Trust, to an extensive and influential audience in the USA. At the same time we seek to promote the US cybersecurity initiatives and their outcomes in Europe at every opportunity, for example in our presentations at the CARTES World Congress. Our objective is to encourage and accelerate international collaboration in cybersecuriy initiatives with a focus upon globally scalable identity management and cryptographic key management that offers long term assurance (without requiring the use of quantum cryptography) even into the quantum future.

---

[5] http://www.think-trust.eu/riseptis.html

[6] http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html

[7] http://media.synaptic-labs.com/downloads/pub/publications/NCLY/20091115-NCLY-Summit2009-Participants_Ideas_Report-Extracts.pdf