Cloud Computing – The new approach to securing Personal Information and addressing new EU regulation

Special research prepared by Rubos, Inc. team:

Mikhail Utin, PhD, CISSP and Daniil Utin, MS

(We do independent research on security matters in various domains)

Prepared for DeepSec 2012

Presented by Mikhail Utin

(Questions will be answered after the presentation. Please, submit them to the speaker in writing)

WHY?

EU General data Protection Regulation will be enacted sooner or later ...

Then it will go into Implementation Phase, and the question is How To Do That?

1. Introduction (1)

1. Five centuries old question “To Be or Not To Be?” or “Share PI or Not to Share?” has been resolved to “Share” over public network – Internet. Then how to share? Three problems:
2. Problem#1: Whether comprehensive PI protection law exists?
- None in the US
- Almost, but not clear when in EU
3. Problem #2: PI sharing environment
- Centralized – easy to secure but impossible to utilize, for instance – EU or US with numerous states
- Decentralized – Internet, which was not expected of public sharing non-public information on public resources, i.e. IT and security technologies
4. Problem #3: Implementation of sharing in Internet according to laws (i.e. compliance with) and within business resources limits

Is a sort of “PI Bermuda Triangle” – Laws and Regulations, IT and Security Technologies, and Real Life Implementation

1. Introduction (2) – regulations, technologies, compliance and real life problems – our past research – small businesses and Information security

Past experience:

-Small and Mid-size Businesses (SMB) are reluctant to do anything beyond even very basic InfoSec controls, mostly because the lack of knowledge and experience , and resources as well

-Millions of businesses should be officially complain to various regulations: MA 201 CMR – 700,000, US HIPAA – 4 millions, EU GDPR – 100 millions?

- Compliance requirements deliberately ignored - from 90 to 99%

1. First presentation – DeepSec 2011 – We discussed various laws protecting PI in the US, and how required compliance could affect small and mid-size businesses (SMBs). Implementation of compliance with Health Insurance Portability and Accountability Act (HIPAA) Security Rule [2] can easy cost tens of thousands dollars in consulting and implementation fees. However, the highest SMB business risk is associated with US government non-compliance penalties, with could be as high as $1,500,000. ***Audit is coming*** …

1. Introduction (3) – our past research – industry Cloud Computing (CC) syndrome:

-Intensive advertizing that CC solves all IT and InfoSec issues including SMB

-Falsely claiming compliance to InfoSec regulations

- Misunderstanding InfoSec concepts and legal requirements beyond standard security services

2. Second presentation – OWASP AppSec DC 2012 [3] considered the implementation of compliance to HIPAA Security Rule within CC Services (CCS) technology:

- CCS do not provide easy to use concept and security model. We identified that CCS is nothing more than an extension of well-known Hosting Services, *which we named Dynamic Hosting Service (DHS)*

-We introduced the *implementation of HIPAA Security Rule Standards utilizing DHS*.

- *Addressing high level law requirements and following implementation is very difficult both organizationally and technically for SMB*

Some of our conclusions are important for this research and this presentation, and will be discussed further below.

1. Introduction (4) - Next step – implementation of PI protecting laws

Is it possible to implement comprehensive PI protecting regulations utilizing means like Cloud Computing? Our research milestones:

- *Analysis of comprehensive PI protecting law* concerning major privacy security requirements: proposed EU General Data Protection Regulation (GDPR)
- *Analysis and comparison of privacy and security controls* as they are proposed in new US NIST 800-53 Rev.4 Draft [5] with GDPR and old HIPAA [6] Security rule,
- Based on our research [3], we proposed *new 9-Layer DHS security model*, which includes new Privacy Control layer and two additional sub-layers as Data Protection and Data Management- *Simple 9-Layer DHS security model makes it possible to identify controls for securing PI*
- *Develop a framework* as technical background for future real life implementation of GDPR and similar regulations.

2. PI protecting regulations

Laws protecting PI do exist on both sides of the Atlantic Ocean. They are:
- Directive 95/46/EC of the European Parliament and of the Council and new EU proposal on GDPR [4]; will be repealed by GDPR
- US HIPAA with Subpart E “Privacy of Individually Identifiable Health Information” [6]
- New NIST 800-53 Rev.4 Draft [5]

2.1. Overview of regulations that protect PI (1)

2.1.1. EU experience, future and details of GDPR

- Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data, October 23, 1995; the first law considering protection of personal information in "free movement of data"
- The above Directive has been complemented by Council Framework Decision 2008/977/JHA of November 27, 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters
- On January 25 2012 new legal framework consisting of Directive and Regulation of the European Parliament and Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Quote: "This initiative is the result of the current legal framework for the protection of personal data, which lasted for more than two years and included a high level conference in May 2009 and two phases of public consultation".

The discussion in the EU member states still continues ...

2.1. Overview of regulations that protect PI (2)

2.1.2. US legislative experience in protecting PI

- Despite numerous attempts to secure PI by one blanket federal law*, there is still no such law as proposed in the EU*. For better or worse, all of the attempts either already stalled in various discussions, or are expectedto stall
- The most common opinion is, as expected, that such law will involve *additional compliance expenses, and that it will affect businesses* while in recession time

There are two laws in the US currently in effect

- Federal regulation “Health Insurance Portability and Accountability Act (HIPAA)” requiring protecting personal health related information in its Security Rule and Privacy Rule; current is 2006 year revision
- State of Massachusetts so name “201 CMR 17.00 Standards for the Protection of Personal Information of the Residents of the Commonwealth”
- NIST 800-53 R.4 standard. It is not a law, it is mandatory security standard for US Government agencies and organizations. May be used as an advisory or “best practice” standard

2.2. Comparison of privacy protection requirements (1)

EU GDPR, and two US – NIST 800-53 R4 and HIPAA Privacy Rule .
The criterion is if a requirement relates to the data movement and operations with data in distributed computing environment like Cloud Computing services.

2.2.1. GDPR privacy controls

EU proposed regulation is definitely complex and covers great deal of legal details of Data Subject (a person or an individual), Controller (data owner) and third parties: 119 pages, 92 Articles:

1. Article 6: Lawfulness of processing:

(a) The data subject has given consent to the processing of their personal data for one or more specific purposes;

2. Article 7: conditions for consent:

(3) The data subject shall have the right to withdraw his or her consent at any time.

... *We finally identified GDPR list of 15 provisions related to implementing of data movement.*

NIST 800-53 R.4 privacy protection controls:

Seriously changed standard to address new technologies (CCS) and concerns (PI protection).
New release includes Appedix J with “Privacy Controls Catalog”. There are 25 controls in 8 categories:

AP – Authority and Purpose

AR - Accountability, Audit and Risk Management

DI – Data Quality and Integrity

DM – Data Minimization and Retention

IP – Individual Participation and Redress

SE – Security

TR – Transparency

UL – Use Limitation

NIST provides NO guidance which controls could be related to CCS.

We did our best and picked up 13 controls.

NIST 800-53 R4 privacy controls table (1)

DO- Data Owner, SP – Service Provider

ID	Privacy Control	Description	Relates to
AR-1	Governance and Privacy Impact	Governance and Privacy Program (PP): required a PP document and appointed official as Privacy Officer	DO & SP
AR-2	Privacy Impact and Risk Assessment	Requires a document of risk assessment, including risks caused by DHS/CCS to DO	DO & SP
AR-3	Privacy Requirements for Contractors and Service providers	Requires identifying roles and responsibilities of service providers; it goes beyond current service agreements adding privacy to security controls;	DO & SP
AR-8	Accounting of Disclosures	Accounting of disclosures and retaining records for 5 years or lifetime; while data owner should provide such information to the person, the information itself exists in DHS/CCS, should be retained and made available if requested	DO & SP
DI-2	Data Integrity (DI) and DI Board	The data owner should guarantee the data integrity; however, for the data on DHS/CCS premises, the service provider should guarantee that	DO & SP

NIST 800-53 R4 privacy controls table (2)

ID	Privacy Control	Description	Relates to
DM-2	Data Retention and Disposal	PI retention time is identified by DO, but retention procedures for all time spectrum and according to a schedule are implemented by SP, and the same applies to the disposal procedures	DO & SP
IP-1	Consent	It is a legal record, which authorizes operations operations with PI, and should reside within SP services together with PI	DO & SP
IP-2	Individual Access	This is a right of a person, which is to be implemented via DO access to the person's PI or directly to SP resources handling PI to view, change, delete, etc., which is the "redress" control below	DO & SP
IP-3	Redress	Based on IA control as above, it includes all "redress" procedures as view, change, delete, etc., plus the dissemination of changes done to PI via SP resources to all users of the individual's PI either in the same DHS/CCS or others; such record of users should be kept together with PI on SP resource	DO & SP
SE-1	Inventory of Personal Identifiable	DO should establish, maintain and update an inventory of programs and systems using PI, thus the same applies to the SP,	DO & DP

NIST 800-53 R4 privacy controls table (3)

ID	Privacy Control	Description	Relates to
SE-2	Privacy Incident Response	Required are Privacy Incident Response Plan and, and according to it, Response Team; both organizational requirements are applicable to both DO and SP; however PI incidents should be investigated by SP, reported to DO, and DO should take care of reporting to persons and organizations according to applicable regulations	DO & SP
TR-3	Dissemination of Privacy Program Information	It is applicable to both DO and SP privacy programs which required by AR-1 control; programs should be made available to all individuals and organizations associated with both DO and SP operations	DO & SP
UL-2	Information Sharing	DO shares information as follows: - entering in agreements with SPs describing covered PI and purposes PI may be used - monitoring, audit and train staff on authorized use of PI - evaluates new instances of sharing PI with SPs Monitoring and audit pertains to various security controls as log management, audit trail records, etc. usually performed by Security Information and Event Management System, which should perform such operations on SP premises	DO & SP

NIST privacy controls conclusion:

1. It was *finally possible to identify the group of 13 privacy controls*, which can be used in DHS implementation.
2. Looking through the list above, we can see that *some controls are related to “legal” or “compliance” group and others are “data”, or say “technical” controls*. We will discuss that in our privacy protection model below.
3. We see that *each of 13 controls involves both Data Owner and Service Provider reflecting the fact that security is shared responsibility*, and that “outsourcing” to DHS does not mean outsourcing the responsibility and participation in all processes. Outsourcing implementation requires having on both sides highly interconnected documents and processes.

HIPAA 45 CFR 164 Subpart E – Privacy of Individually Identifiable Health Information

This is a set of 15 standards, which has been written around 2006 with focus on a legal side of the procedures and documents reflecting US healthcare system, and completely independent of the technology.

We identified just three standards that could be related to electronic PI processing.
Next to each standard is a reference to the associated control in NIST 800-53 R4 standards from the table above:
- 164.524 - Access to individuals to protected health information (IP-2)
- 164.526 – Amendment of protected health information (IP-3)
- 164.528 - Accounting of disclosures of protected health information (AR-8)

Conclusion: New NIST set of privacy protection controls supersedes old HIPAA standards. We will discuss GDPR and NIST standards further.

Correlation of EU GDPR and NIST privacy protection controls (1)

The table below represents a correlation matrix between NIST 800-35 R.4 privacy controls and EU GDPR.

NIST ID	NIST Privacy Control	GDPR Article	GDPR Control
AR-1	Governance and Privacy Impact	11(1) 30(1) 35	The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks Designation of the data protection officer
AR-2	Privacy Impact and Risk Assessment	30(2)	The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data
AR-3	Privacy Requirements for Contractors and Service providers	26(1)	Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organizational measures and

Correlation of EU GDPR and NIST privacy protection controls (2)

NIST ID	NIST Privacy Control	GDPR Article	GDPR Control
AR-8	Accounting of Disclosures	14	Information to the data subject
DI-2	Data Integrity (DI) and DI Board	30(2)	The controller and the processor shall … protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorized disclosure, dissemination or access, or alteration of personal data
DM-2	Data Retention and Disposal	14(c) 15(1d)	The period for which the personal data will be stored The period for which the personal data will be stored
IP-1	Consent	6(a), 7(3)	The data subject has given consent to the processing The data subject shall have the right to withdraw his or her consent
IP-2	Individual Access	14(d)	The existence of the right to request from the controller access to
IP-3	Redress	14(d) 16	rectification or erasure of the personal data concerning the data subject

Correlation of EU GDPR and NIST privacy protection controls (3)

NIST ID	NIST Privacy Control	GDPR Article	GDPR Control
SE-1	Inventory of Personal Identifiable Information	23 33	Data protection by design and by default Data processing impact assessment
SE-2	Privacy Incident Response	31 32	Notification of a personal data breach to the supervisory authority Communication of a personal data breach to the data subject
TR-3	Dissemination of Privacy Program Information	11	Transparent information and communication
UL-2	Information Sharing	14(b) 15(1a) 15(1c) 26(2d) 26(3) 40 - 45	The purposes of the processing for which the personal data are intended, including the contract terms and general conditions The purpose of the processing The recipients or categories of recipients Enlist another processor only with the prior permission of the controller The controller and the processor shall document in writing the controller's instructions and the processor's obligations Transfer of personal data to third countries or interbational organizations

2.3. Conclusion to comparison of regulations

1. We see here that *NIST list very well correlates with GDPR requirements*, while in some cases we've seen multiple instances of EU regulation requirements corresponding to one NIST control. That, of course, was expected and relates to general nature of GDPR, its legal structure, and the purpose of the document.
2. We considered three regulations as providing a background for the identification of privacy protection controls in DHS distributed computing environment. *Each document has its own purpose, and is not aligned with our goal. However, our analysis has shown that there is a very strong correlation between privacy controls*. In fact, NIST standards supersede old HIPAA, and represent more concrete outcome of EU GDPR. Thus, in the following consideration of the implementation of privacy controls in DHS environment, we will refer to NIST set as a basis for PI protection controls.

Cloud Computing Services as they are and new security and privacy protection model for Dynamic Hosting Service

Laws, which we considered above and guaranteeing free PI movement and protecting it as well, are written technology independent, but with new information technologies in mind. *What did we get during last thirty years?* There are: LAN, WAN, Internet, WLAN/WiFi, datacenter, hosting, and finally Cloud Computing. Latter is considered as universal distributed computing environment, which basically replaces whatever we had before. By the opinion of CCS providers and numerous institutions, including US government, *CC services are the only one possible technology concept for free data movement and sharing*. We need to return to our analysis of such assumption, which we did for OWASP Appsec DC 2012.

4.1. Cloud Computing misconceptions (1)

Terminology:

We know *Analog Computing, which was the beginning of computing, next - Digital, Multiprocessor, Mainframe, etc., and each identifies which computation method is used*. So far, a “cloud” cannot compute, it neither a means or a method of computation.

The essence of *CC: it is a service delivering data to a computational point* and back to the user *in dynamic manner*, i.e. ***moving computation point between various resources like datacenters***.

The history of CC Services (CCS) goes back to Internet Bubble, which required a lot of datacenters hosting multiplying web sites. After the Bubble has burst, such datacenters became useless, or used just for a percent of their power. But *what is the difference between hosting http protocol application, or any other*? Thus, new marketing *label “Cloud Computing” has been designed to sell old hosting service to customers* uder new marketing label.

Cloud Computing as pure marketing term has been used in the same way as Intranet. Old product is on sale under completely new and sophisticated label.

4.1. Cloud Computing misconceptions (2)

Models:

Marketing campaign works well if there is some sort of a science behind. And CCS got two well-known models: Deployment Model and Service Model. There are three NIST-800 (144. 145 and 146) publications [12, 13, 14] considering such models.

CC Service Model:

1. “Infrastructure as Service” (IaaS) – quote: “providers offer computers, as physical or more often as virtual machines, and other resources”, and concerning provided services, it is *well-known to us as Hosting Service*, nothing more, nothing less
2. “Platform as a Service – PaaS” is actually *Application Programming Interface* (API) *hosting service*, which may include runtime environment, databases, development tools, etc.
3. “Software as a Service – SaaS” *is application environment hosting various applications* – email, office productivity, games, etc., so hosting service as well

4.1. Cloud Computing misconceptions (3)

Models:

CC Deployment Model:

Service Model has been discussed, and helped us to confirm again that CC is a service – it is about **data** freely moving across organizational boarders. Then, why do we need “Deployment Model” (DM), which is about **computing resources** and provides no explanation of how **data** moves inside or the exact meaning of service to the customer.

1. “Public Cloud” – quote: “*…It is owned and operated by a cloud provider delivering cloud service to customers*”. Do we really need a new model of “Public Cloud” to explain what *we know since year 2000 as “Hosting Service”?*
2. “Private Cloud” – quote: “… *is operated exclusively for a single organization. It may be managed by the organization or by a third party, and may be hosted within the organization’s data center or outside of it.”*

So, again we can *easy explain new “Private Cloud” in old and easily understood terms – LAN, WAN, or Outsourced Infrastructure* (LAN, WAN, etc.) and such well established terms are much easier to comprehend and to use than “Private Cloud”

4.1. Cloud Computing misconceptions (4)

CC Deployment Model (continued):
3. “Community Cloud” – quote: “… *the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security, and regulatory considerations, rather than a single organization.*” . A “community” is not a legal entity and cannot sign an agreement, unless organizations within form such entity legally. In this case, we again see one-to-one relationship, and “public cloud” – Hosting Service. So far, since Roman time, there was no legal practice of signing service agreement by a vaguely defined “community” with a service provider.
4. “Hybrid Cloud” – it is a composition: “*… more complex than the other deployment models, since they involve a composition of two or more clouds (private, community, or public). Each member remains a unique entity, but is bound to the others through standardized or proprietary technology that enables application and data portability among them.*” .” As far as services are concerned, this model is a composition of LAN/WAN (private cloud), and a hosting service (public cloud). “Community”, as we discussed above, is either a hosting service or cannot legally exist.

4.1. Cloud Computing misconceptions (5)

The following tables show what CCS really are:

CC SM	As Hosting Service	As Dynamic Hosting Service
IaaS	Hosting Service	Dynamic Hosting Service (DHS)
PaaS	API Hosting Service	Dynamic API Hosting Service (DAPIHS)
SaaS	Application Hosting Service	Dynamic Application Hosting Service (DAHS)

CC DM	What is it concerning services?
Public Cloud	Hosting Service
Private Cloud	LAN, or WAN, or Outsourced Infrastructure (LAN, WAN, etc.)
Community Cloud	Legal Nonsense
Hybrid Cloud	Interconnected LAN, WAN, and Hosting Service

4.2. CC models' consideration conclusion (1)

The goal of our consideration of CCS was to identify if there is any value in this concept, and if its models would help us in implementation of privacy controls.

Vague and complex models with no real technical value cannot help is our case. Laws are complex, implementation is complex, and any extra complexity will make the implementation unmanageable.

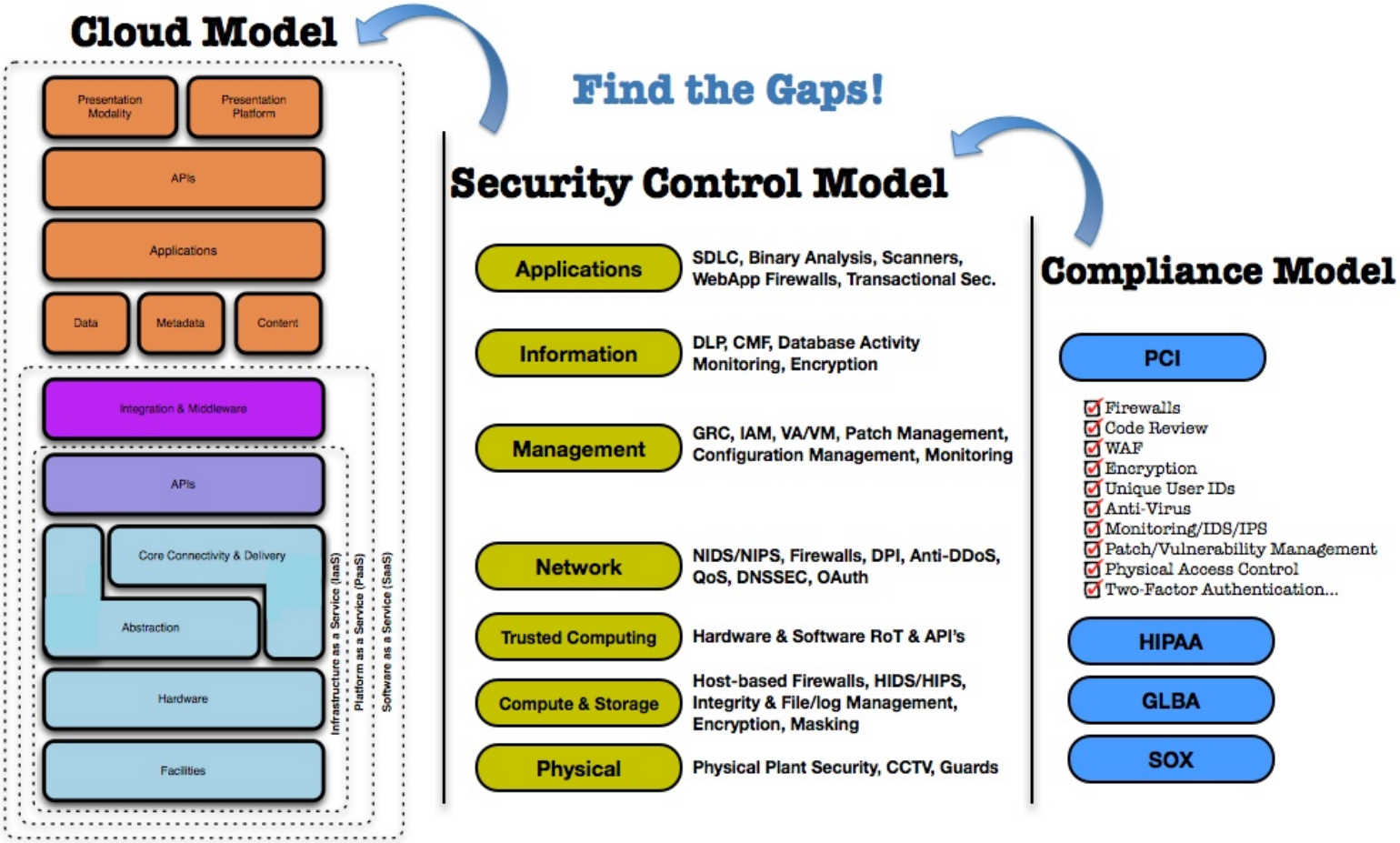
1. Cloud Computing Service Model utilizing IaaS, PaaS and SaaS models is *over sophisticated presentation of a hosting service*; our concept of Dynamic Hosting Service and its extensions (DHS->DAPIHS->DAHS) is based on traditional hosting service model; it is simple and explains interconnection relationship in Internet computing environment as connection between various hosting services and processes transmitting PI.
2. Cloud Computing *Deployment model is irrelevant to the consideration of interconnecting and utilizing PI processes;* in fact new DHS model represent higher abstraction layer, thus infrastructure level can be easy explained in old terms of LAN, WAN, outsources LAN/WAN, and hosting service.

4.2. CC models' consideration conclusion (1)

Numerous CCS security models do not include what is our core concern – protection of PI in a form of privacy controls. In most cases they are a *derivation of 7-layers OSI model*, and, as in one of the most complex cases below (see picture below), *include cloud model, various security controls (Security Model), references to regulations (Compliance Model), but completely missing what is related to PI protection*. As we see on the picture below, Cloud Model (on the left) does not help at all to understand what is missing concerning privacy protection.

When we talk about DHS, we completely understand that this service should be protected as well, not just infrastructure, nodes, etc. The following paragraph explains our PI protection model.

4.2. Typical CC security model

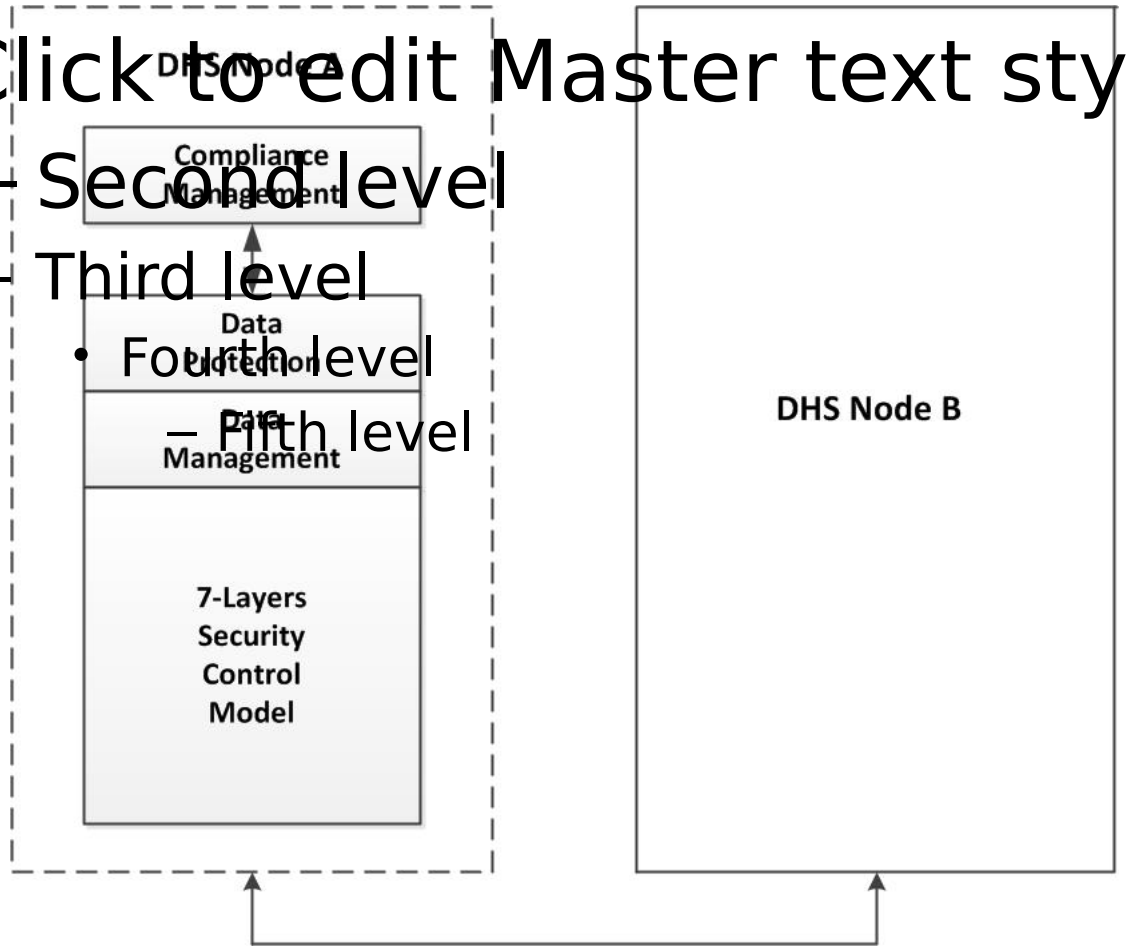


4.3. PI Protection 9-layer Security and Compliance Model (PIP9 Model) (1)

There are *two privacy protection processes running in between infrastructure nodes providing DHS. They are Data Protection (DP) and Data Management (DM)*. First process - DP - is concerned of various controls providing confidentiality, integrity and availability of PI. The second – DM - *provides necessary controls for manipulation and movement of PI*. Various control information data structures participate in such processes, which identify the status and the location of PI in distributed environment, and we include them in DM as well. Our model also includes Compliance Management (CM) layer, which we place above 9-layer structure with our proposed DP and DM layers. *CM is universal and controls compliance with all involved regulations and internal policies.*
Next table explains the relationship between NIST 800-53 PI controls and layers of our model.

4.3. PI Protection 9-layer Security and Compliance Model (PIP9 Model) (2)

- Click to edit Master text styles
  - Second level
  - Third level
    - Fourth level
      - Fifth level



4.3. PI Protection 9-layer Security and Compliance Model (PIP9 Model) (3)

ID	NIST Privacy Control	PI Protection Model
AR-1	Governance and Privacy Impact	CM
AR-2	Privacy Impact and Risk Assessment	CM
AR-3	Privacy Requirements for Contractors and Service providers	CM
AR-8	Accounting of Disclosures	DM
DI-2	Data Integrity (DI) and DI Board	DP
DM-2	Data Retention and Disposal	DM
IP-1	Consent	DM
IP-2	Individual Access	DP
IP-3	Redress	DM
SE-1	Inventory of Personal Identifiable Information	DM
SE-2	Privacy Incident Response	DP
TR-3	Dissemination of Privacy Program Information	CM
UL-2	Information Sharing	CM

4.4. PIP9 Model conclusion

1. We considered CCS as they are well-known through various sources, including three official US Government NIST standards. *Unfortunately, market driven approach affected the most of associated industries and security professionals,* and NISTs usually balanced position as well. *We cannot use vague models and recommendations if we want to address such challenge as EU GDPR*. We *proposed our simple to understand and getting right to the point Dynamic Hosting Services Model*, which includes two extensions for API and application implementation.
2. *Our high level presentation of processes in Internet computing environment as DHS running on interconnected nodes permitted us to introduce new 9-layer PI protection and Compliance Model*. Such logical and common sense approach *is confirmed by easy fitting of NIST 800-53 privacy controls in our model.*
3. *Our DHS and corresponding PIP9 models give us a change to consider a framework of PI protection implementation* in Internet computing environment

5. PI Protection Implementation framework

Our limits of the implementation are DHS model, PIP9 model, and 13 PI protecting controls from NIST 800-53. We need to stress here that these NIST controls, which we picked up from the original set, address very common EU security community written or verbal concerns over Access, Accounting, Retention, Integrity, Consent, and Redress of PI. Additionally, our list includes Inventory and Incident Response controls.

In our proposed framework we will consider the implementation of three groups of privacy controls, which we identified above, and which correspond to our model layers: Compliance Management, Data Protection and Data Management.

We would like to mention here one *fundamental security principal*, which very often forgotten while always clear in any security regulation:

Outsourcing of security controls and privacy protection functions from Data Owner to a Service Provider does not mean outsourcing responsibility to control security and privacy. It means that Data Owner should be aware of what and where happens, ability and readiness to act, and being responsible for what happened as we see in NIST Privacy Control table.

5.1. Compliance Management (CM)

Compliance Management layer represents the legal part of PI protection implementation, which, according to our PIP9 model, has universal character and is above our DP and DM layers and general security controls (7-layers in our model), and is required by various US regulations like HIPAA Security Rule, SOX, PCI DSS, and others.
There are 5 control at this layer:
1. Governance and Privacy Impact
2. Privacy Impact and Risk Assessment
3. Privacy requirements for contractors and service providers
In this control we introduced Delegation of Trust concept (DoT), which regulates the process of guarantees' exchange and provides unified level of trust.
4. Dissemination of Privacy Program Information
5. Information Sharing

In this presentation we skip descriptions of controls' implementation to simplify fhs discussion. All descriptions provided in the presentation text.

Compliance Management conclusion

1. Having internal and service provider's privacy program, security program, and risk assessment *is the responsibility of PI data owner*.
2, In a case of distributed network of DHS providers, Delegation of Trust should be implemented by having either guarantees from ***all*** service providers, or *independent certification of providers is implemented*.
3, Risk assessment should include DO internal risk assessment, service provider's assessment, and in the provider assessment it *also should be an assessment of risks invoked by the provider's services* to the data owner.
4. Our experience shows that service providers deeply unaware of the meaning of compliance and what are privacy and security requirements, including legal part as above.
5. Each new kind or instance of PI sharing involves complete assessment of privacy controls and may be security controls as well.
6. Such controls of sharing as monitoring and audit of PI usage involves implementation of complex and costly SIEM-class system at each service provider's premises.
7. Privacy Officer should be appointed to supervise activities as above and monitor security status.

5.2. Data Protection (DP)

Per NIST opinion, and we share that, PI data protection is to be implemented mostly by utilizing security controls (which we identified as 7-layer security control model). However, both Data Owner and Service Provider should be aware how to use security controls to protect PI, and what to do in a case of privacy violation.

There are three controls:
1. Data Integrity (DI) and DI Board
2. Individual Access (IA)
3. Privacy Incident Response

Data Protection controls conclusion

1. *Data Protection controls are implemented utilizing associated security controls*. The management of both DO and SP involved in resolution of PI compromises, should be aware of regulatory requirement how to handle such incidents, including reporting to authorities and affected individuals.
2. EU GDPR considers various and complex aspects of sharing and access to PI data, and such requirements should be reflected in Individual Access implementation. In a case of PI data is moving over Internet between DHS processes, access information (like ACL) should move together with data, and is updated according to changing access requests and permissions.

5.3. Data Management (DM) – some ideas of the implementation

1.This group represents controls responsible for support of free movement of data between distributed DHS processes. Whether a transfer of data it dictated by internal status of the infrastructure (failure or overload of a node, etc.) or by a requests for data, *the transfer functions is implemented by a communication connection oriented protocol. Such protocol provides assurance that DM operation has been finished and the status of PI in distributed nodes infrastructure is always known*

2. DM group of controls guarantee that PI free movement does not mean uncontrolled release of information. Thus, DM control(s) should permit accounting of PI movement and thus knowing where a PI record is now, where there are copies of, and what is the status (active, deleted, etc.)

3. *Conceptual character of GDPR requires that the access to PI should be implemented on per individual record bases and the transfer of records across multiple nodes* rather than collecting all PI records in one central repository. The latter seems impossible to implement considering EU principals of cooperation as well.

4. *Each PI record should have supporting data structures, which we name "descriptors". Such descriptors save and release necessary privacy control information*. We already discussed one of descriptors – ACL – while discussing the access to PI record.

Data Management conclusion

1. We considered an implementation of all NIST Data Management privacy controls in our distributed DHS environment. We suggested using high level connection oriented protocol to transfer PI and control information between nodes.
2. *We concluded that both the nature of GDPR and EU states' cooperation principals require decentralized storing of PI and associated with it information,* and that can be done utilizing DHS nodes infrastructure.
2. *Decentralized PI and control information should reside in each DHS node, which thus is considered as "parent" node for PI originated in it and all PI control information.* The latter resides in an information depository named "Parent Status Descriptor".
3. *Depository of all control information is an inventory keeping information about DHS distributed infrastructure, and information about all operations with PI and where is has been released. Parent Status Descriptor information is changed upon conclusion of each DM operation.*
4. It was possible to design implementation framework utilizing proposed solution for all NIST Data Management group control, thus proving that all standard operations with PI is possible to implement within our models and the framework.

6. The Presentation Conclusion

1. *We proved that our approach of replacing Cloud Computing services by Dynamic Hosting Service model works*. Instead of using sophisticated combination of useless models, we concentrate on one, which is high level, simple and easy to use.
2. We analyzed three major regulations concerned of PI protection – EU General Data Protection Regulation, and US NIST 800-53 Privacy Control standards and HIPAA Privacy Rule. *We identified that complex and thorough GDBR requirements can be mapped to NIST controls*, and which provide a ground for privacy controls implementation framework.
3. *We proposed new 9-Layer PI Protection Security Model (PIP9), which include considered as standard 7-layer Security Control Model and two additional of data protection and Data Management representing PI protection. The model also includes Compliance Management layer*.
4. *We divided 13 NIST Privacy Controls is three groups corresponding to our PIP9 model, and considered implementation of controls utilizing proposed models and principals*. It was possible to develop the implementation framework, which covers our list NIST privacy controls and required operations with PI, thus implementing in our framework high level GDPR requirements.

7. References (1)

1. Mikhail A. Utin, Daniil Utin. US Experience: Laws, Compliance, and Real Life – When everything seems right but simply does not work; DeepSec 2011, Vienna, November, 2011.
2. 45 CFR Subtitle A, Subchapter C, Part 164, Subpart C – Security Standards for the Protection of Electronic Protected health Information
3. Mikhail A. Utin, Daniil Utin. Private Information Protection in Cloud Computing – Laws, Compliance and Cloud Security Misconceptions, OWASP AppSec DC 2011, April, 2012.
4. Proposal for a regulation of the European parliament and of the Council on the protection of individuals with regards to the protection of personal data and on the free movement of such data (General Data Protection Regulation); COM(2012) 11 final, Brussels, 25.1.2012
5. National Institute of Standards and Technology (NIST), US Department of Commerce, NIST Special Publication 800-53 Revision 4: Security and Privacy Controls in Federal Information Systems and Organizations, February, 2012.
6. 45 CFR Subtitle A, Subchapter C, Part 164, Subpart E – Privacy of Individually Identifiable Health Information.

7. References (2)

7. Review: National Concerns over the proposed EU Data Protection regulation, Infosecurity magazine, August 6, 2012; http://www.infosecurity-magazine.com/view/27399/national-concern
8. GovTrack.us: S3333 - Data Security and Breach Notification Law http://www.govtrack.us/congress/bills/112/s3333/text
9. Code of Massachusetts Regulations: 201 CMR 17.00: Standards for protection of Personal Information of Residents of the Commonwealth - http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf
10. MGL Chapter 93H – Security Breaches - http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapt
11. Public Law 111-5, February 17, 2009 - http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.p
12. Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, December 2011.

7. References (3)

13. The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September, 2011.
14. Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146, May 2012.
15. Wikipedia: Cloud computing - http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Service_m
16. Wikipedia: Cloud computing security model - http://www.google.com/search?q=cloud+computing+security+mod
17. Computer Incident Handlinh Guide, NIST Special Publication 800-61 R1, March, 2008.

Thank you!

All questions will be answered:

- mikhailutin@hotmail.com

or

- mutin@rubos.com

Rubos, Inc. (presentations, texts, articles, etc.)

- www.201cmr17.00ma.com
- This presentation will be available on DeepSec site or on our site above

Cloud Computing – The new approach to securing Personal Information and addressing new EU regulation

Special research prepared by Rubos, Inc. team:
Mikhail Utin, PhD, CISSP and Daniil Utin, MS
(We do independent research on security matters in various domains)

Prepared for DeepSec 2012
Presented by Mikhail Utin

(Questions will be answered after the presentation. Please, submit them to the speaker in writing)

WHY?

EU General data Protection Regulation will be enacted sooner or later …

Then it will go into Implementation Phase, and the question is How To Do That?

1. Introduction (1)

1. Five centuries old question “To Be or Not To Be?” or “Share PI or Not to Share?” has been resolved to “Share” over public network – Internet. Then how to share? Three problems:
2. Problem#1: Whether comprehensive PI protection law exists?
- None in the US
- Almost, but not clear when in EU
3. Problem #2: PI sharing environment
- Centralized – easy to secure but impossible to utilize, for instance – EU or US with numerous states
- Decentralized – Internet, which was not expected of public sharing non-public information on public resources, i.e. IT and security technologies
4. Problem #3: Implementation of sharing in Internet according to laws (i.e. compliance with) and within business resources limits

Is a sort of “PI Bermuda Triangle” – Laws and Regulations, IT and Security Technologies, and Real Life Implementation

1. Introduction (2) – regulations, technologies, compliance and real life problems – our past research – small businesses and Information security

Past experience:

-Small and Mid-size Businesses (SMB) are reluctant to do anything beyond even very basic InfoSec controls, mostly because the lack of knowledge and experience , and resources as well

-Millions of businesses should be officially complain to various regulations: MA 201 CMR – 700,000, US HIPAA – 4 millions, EU GDPR – 100 millions?

- Compliance requirements deliberately ignored - from 90 to 99%

1. First presentation – DeepSec 2011 – We discussed various laws protecting PI in the US, and how required compliance could affect small and mid-size businesses (SMBs). Implementation of compliance with Health Insurance Portability and Accountability Act (HIPAA) Security Rule [2] can easy cost tens of thousands dollars in consulting and implementation fees. However, the highest SMB business risk is associated with US government non-compliance penalties, with could be as high as $1,500,000. ***Audit is coming*** …

1. Introduction (3) – our past research – industry Cloud Computing (CC) syndrome:

-Intensive advertizing that CC solves all IT and InfoSec issues including SMB

-Falsely claiming compliance to InfoSec regulations

- Misunderstanding InfoSec concepts and legal requirements beyond standard security services

2. Second presentation – OWASP AppSec DC 2012 [3] considered the implementation of compliance to HIPAA Security Rule within CC Services (CCS) technology:

- CCS do not provide easy to use concept and security model. We identified that CCS is nothing more than an extension of well-known Hosting Services, *which we named Dynamic Hosting Service (DHS)*

-We introduced the *implementation of HIPAA Security Rule Standards utilizing DHS*.

- *Addressing high level law requirements and following implementation is very difficult both organizationally and technically for SMB*

Some of our conclusions are important for this research and this presentation, and will be discussed further below.

1. Introduction (4) - Next step – implementation of PI protecting laws

Is it possible to implement comprehensive PI protecting regulations utilizing means like Cloud Computing? Our research milestones:

- *Analysis of comprehensive PI protecting law* concerning major privacy security requirements: proposed EU General Data Protection Regulation (GDPR)
- *Analysis and comparison of privacy and security controls* as they are proposed in new US NIST 800-53 Rev.4 Draft [5] with GDPR and old HIPAA [6] Security rule,
- Based on our research [3], we proposed *new 9-Layer DHS security model*, which includes new Privacy Control layer and two additional sub-layers as Data Protection and Data Management- *Simple 9-Layer DHS security model makes it possible to identify controls for securing PI*
- *Develop a framework* as technical background for future real life implementation of GDPR and similar regulations.

2. PI protecting regulations

Laws protecting PI do exist on both sides of the Atlantic Ocean. They are:
- Directive 95/46/EC of the European Parliament and of the Council and new EU proposal on GDPR [4]; will be repealed by GDPR
- US HIPAA with Subpart E “Privacy of Individually Identifiable Health Information” [6]
- New NIST 800-53 Rev.4 Draft [5]

2.1. Overview of regulations that protect PI (1)

2.1.1. EU experience, future and details of GDPR

- Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data, October 23, 1995; the first law considering protection of personal information in “free movement of data”
- The above Directive has been complemented by Council Framework Decision 2008/977/JHA of November 27, 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters
- On January 25 2012 new legal framework consisting of Directive and Regulation of the European Parliament and Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Quote: “This initiative is the result of the current legal framework for the protection of personal data, which lasted for more than two years and included a high level conference in May 2009 and two phases of public consultation”.

The discussion in the EU member states still continues …

2.1. Overview of regulations that protect PI (2)

2.1.2. US legislative experience in protecting PI
- Despite numerous attempts to secure PI by one blanket federal law, *there is still no such law as proposed in the EU*. For better or worse, all of the attempts either already stalled in various discussions, or are expectedto stall
- The most common opinion is, as expected, that such law will involve *additional compliance expenses, and that it will affect businesses* while in recession time

There are two laws in the US currently in effect
- Federal regulation “Health Insurance Portability and Accountability Act (HIPAA)” requiring protecting personal health related information in its Security Rule and Privacy Rule; current is 2006 year revision
- State of Massachusetts so name “201 CMR 17.00 Standards for the Protection of Personal Information of the Residents of the Commonwealth”
- NIST 800-53 R.4 standard. It is not a law, it is mandatory security standard for US Government agencies and organizations. May be used as an advisory or “best practice” standard

2.2. Comparison of privacy protection requirements (1)

EU GDPR, and two US – NIST 800-53 R4 and HIPAA Privacy Rule .
The criterion is if a requirement relates to the data movement and operations with data in distributed computing environment like Cloud Computing services.

2.2.1. GDPR privacy controls

EU proposed regulation is definitely complex and covers great deal of legal details of Data Subject (a person or an individual), Controller (data owner) and third parties: 119 pages, 92 Articles:

1. Article 6: Lawfulness of processing:

(a) The data subject has given consent to the processing of their personal data for one or more specific purposes;

2. Article 7: conditions for consent:

(3) The data subject shall have the right to withdraw his or her consent at any time.

... *We finally identified GDPR list of 15 provisions related to implementing of data movement.*

NIST 800-53 R.4 privacy protection controls:

Seriously changed standard to address new technologies (CCS) and concerns (PI protection).
New release includes Appedix J with “Privacy Controls Catalog”. There are 25 controls in 8 categories:

AP – Authority and Purpose

AR - Accountability, Audit and Risk Management

DI – Data Quality and Integrity

DM – Data Minimization and Retention

IP – Individual Participation and Redress

SE – Security

TR – Transparency

UL – Use Limitation

NIST provides NO guidance which controls could be related to CCS.

We did our best and picked up 13 controls.

NIST 800-53 R4 privacy controls table (1)

DO- Data Owner, SP – Service Provider

ID	Privacy Control	Description	Relates to
AR-1	Governance and Privacy Impact	Governance and Privacy Program (PP): required a PP document and appointed official as Privacy Officer	DO & SP
AR-2	Privacy Impact and Risk Assessment	Requires a document of risk assessment, including risks caused by DHS/CCS to DO	DO & SP
AR-3	Privacy Requirements for Contractors and Service providers	Requires identifying roles and responsibilities of service providers; it goes beyond current service agreements adding privacy to security controls;	DO & SP
AR-8	Accounting of Disclosures	Accounting of disclosures and retaining records for 5 years or lifetime; while data owner should provide such information to the person, the information itself exists in DHS/CCS, should be retained and made available if requested	DO & SP
DI-2	Data Integrity (DI) and DI Board	The data owner should guarantee the data integrity; however, for the data on DHS/CCS premises, the service provider should guarantee that	DO & SP

NIST 800-53 R4 privacy controls table (2)

ID	Privacy Control	Description	Relates to
DM-2	Data Retention and Disposal	PI retention time is identified by DO, but retention procedures for all time spectrum and according to a schedule are implemented by SP, and the same applies to the disposal procedures	DO & SP
IP-1	Consent	It is a legal record, which authorizes operations operations with PI, and should reside within SP services together with PI	DO & SP
IP-2	Individual Access	This is a right of a person, which is to be implemented via DO access to the person's PI or directly to SP resources handling PI to view, change, delete, etc., which is the "redress" control below	DO & SP
IP-3	Redress	Based on IA control as above, it includes all "redress" procedures as view, change, delete, etc., plus the dissemination of changes done to PI via SP resources to all users of the individual's PI either in the same DHS/CCS or others; such record of users should be kept together with PI on SP resource	DO & SP
SE-1	Inventory of Personal Identifiable	DO should establish, maintain and update an inventory of programs and systems using PI, thus the same applies to the SP,	DO & DP

NIST 800-53 R4 privacy controls table (3)

ID	Privacy Control	Description	Relates to
SE-2	Privacy Incident Response	Required are Privacy Incident Response Plan and, and according to it, Response Team; both organizational requirements are applicable to both DO and SP; however PI incidents should be investigated by SP, reported to DO, and DO should take care of reporting to persons and organizations according to applicable regulations	DO & SP
TR-3	Dissemination of Privacy Program Information	It is applicable to both DO and SP privacy programs which required by AR-1 control; programs should be made available to all individuals and organizations associated with both DO and SP operations	DO & SP
UL-2	Information Sharing	DO shares information as follows: - entering in agreements with SPs describing covered PI and purposes PI may be used - monitoring, audit and train staff on authorized use of PI - evaluates new instances of sharing PI with SPs Monitoring and audit pertains to various security controls as log management, audit trail records, etc. usually performed by Security Information and Event Management System, which should perform such operations on SP premises	DO & SP

NIST privacy controls conclusion:

1. It was *finally possible to identify the group of 13 privacy controls*, which can be used in DHS implementation.
2. Looking through the list above, we can see that *some controls are related to “legal” or “compliance” group and others are “data”, or say “technical” controls*. We will discuss that in our privacy protection model below.
3. We see that *each of 13 controls involves both Data Owner and Service Provider reflecting the fact that security is shared responsibility*, and that “outsourcing” to DHS does not mean outsourcing the responsibility and participation in all processes. Outsourcing implementation requires having on both sides highly interconnected documents and processes.

HIPAA 45 CFR 164 Subpart E – Privacy of Individually Identifiable Health Information

This is a set of 15 standards, which has been written around 2006 with focus on a legal side of the procedures and documents reflecting US healthcare system, and completely independent of the technology.

We identified just three standards that could be related to electronic PI processing.
Next to each standard is a reference to the associated control in NIST 800-53 R4 standards from the table above:
- 164.524 - Access to individuals to protected health information (IP-2)
- 164.526 – Amendment of protected health information (IP-3)
- 164.528 - Accounting of disclosures of protected health information (AR-8)

Conclusion: New NIST set of privacy protection controls supersedes old HIPAA standards. We will discuss GDPR and NIST standards further.

Correlation of EU GDPR and NIST privacy protection controls (1)

The table below represents a correlation matrix between NIST 800-35 R.4 privacy controls and EU GDPR.

NIST ID	NIST Privacy Control	GDPR Article	GDPR Control
AR-1	Governance and Privacy Impact	11(1) 30(1) 35	The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks Designation of the data protection officer
AR-2	Privacy Impact and Risk Assessment	30(2)	The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data
AR-3	Privacy Requirements for Contractors and Service providers	26(1)	Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organizational measures and

Correlation of EU GDPR and NIST privacy protection controls (2)

NIST ID	NIST Privacy Control	GDPR Article	GDPR Control
AR-8	Accounting of Disclosures	14	Information to the data subject
DI-2	Data Integrity (DI) and DI Board	30(2)	The controller and the processor shall … protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorized disclosure, dissemination or access, or alteration of personal data
DM-2	Data Retention and Disposal	14(c) 15(1d)	The period for which the personal data will be stored The period for which the personal data will be stored
IP-1	Consent	6(a), 7(3)	The data subject has given consent to the processing The data subject shall have the right to withdraw his or her consent
IP-2	Individual Access	14(d)	The existence of the right to request from the controller access to
IP-3	Redress	14(d) 16	rectification or erasure of the personal data concerning the data subject

Correlation of EU GDPR and NIST privacy protection controls (3)

NIST ID	NIST Privacy Control	GDPR Article	GDPR Control
SE-1	Inventory of Personal Identifiable Information	23 33	Data protection by design and by default Data processing impact assessment
SE-2	Privacy Incident Response	31 32	Notification of a personal data breach to the supervisory authority Communication of a personal data breach to the data subject
TR-3	Dissemination of Privacy Program Information	11	Transparent information and communication
UL-2	Information Sharing	14(b) 15(1a) 15(1c) 26(2d) 26(3) 40 - 45	The purposes of the processing for which the personal data are intended, including the contract terms and general conditions The purpose of the processing The recipients or categories of recipients Enlist another processor only with the prior permission of the controller The controller and the processor shall document in writing the controller's instructions and the processor's obligations Transfer of personal data to third countries or international organizations

2.3. Conclusion to comparison of regulations

1. We see here that *NIST list very well correlates with GDPR requirements*, while in some cases we've seen multiple instances of EU regulation requirements corresponding to one NIST control. That, of course, was expected and relates to general nature of GDPR, its legal structure, and the purpose of the document.
2. We considered three regulations as providing a background for the identification of privacy protection controls in DHS distributed computing environment. *Each document has its own purpose, and is not aligned with our goal. However, our analysis has shown that there is a very strong correlation between privacy controls*. In fact, NIST standards supersede old HIPAA, and represent more concrete outcome of EU GDPR. Thus, in the following consideration of the implementation of privacy controls in DHS environment, we will refer to NIST set as a basis for PI protection controls.

Cloud Computing Services as they are and new security and privacy protection model for Dynamic Hosting Service

Laws, which we considered above and guaranteeing free PI movement and protecting it as well, are written technology independent, but with new information technologies in mind. *What did we get during last thirty years?* There are: LAN, WAN, Internet, WLAN/WiFi, datacenter, hosting, and finally Cloud Computing. Latter is considered as universal distributed computing environment, which basically replaces whatever we had before. By the opinion of CCS providers and numerous institutions, including US government, *CC services are the only one possible technology concept for free data movement and sharing*. We need to return to our analysis of such assumption, which we did for OWASP Appsec DC 2012.

4.1. Cloud Computing misconceptions (1)

Terminology:

We know *Analog Computing, which was the beginning of computing, next - Digital, Multiprocessor, Mainframe, etc., and each identifies which computation method is used*. So far, a “cloud” cannot compute, it neither a means or a method of computation.

The essence of *CC: it is a service delivering data to a computational point* and back to the user *in dynamic manner*, i.e. ***moving computation point between various resources like datacenters***.

The history of CC Services (CCS) goes back to Internet Bubble, which required a lot of datacenters hosting multiplying web sites. After the Bubble has burst, such datacenters became useless, or used just for a percent of their power. But *what is the difference between hosting http protocol application, or any other*? Thus, new marketing *label “Cloud Computing” has been designed to sell old hosting service to customers* uder new marketing label.

Cloud Computing as pure marketing term has been used in the same way as Intranet. Old product is on sale under completely new and sophisticated label.

4.1. Cloud Computing misconceptions (2)

Models:

Marketing campaign works well if there is some sort of a science behind. And CCS got two well-known models: Deployment Model and Service Model. There are three NIST-800 (144. 145 and 146) publications [12, 13, 14] considering such models.

CC Service Model:

1. “Infrastructure as Service” (IaaS) – quote: “providers offer computers, as physical or more often as virtual machines, and other resources”, and concerning provided services, it is *well-known to us as Hosting Service*, nothing more, nothing less
2. “Platform as a Service – PaaS” is actually *Application Programming Interface* (API) *hosting service*, which may include runtime environment, databases, development tools, etc.
3. “Software as a Service – SaaS” *is application environment hosting various applications* – email, office productivity, games, etc., so hosting service as well

4.1. Cloud Computing misconceptions (3)

Models:

CC Deployment Model:

Service Model has been discussed, and helped us to confirm again that CC is a service – it is about **data** freely moving across organizational boarders. Then, why do we need “Deployment Model” (DM), which is about **computing resources** and provides no explanation of how **data** moves inside or the exact meaning of service to the customer.

1. “Public Cloud” – quote: “*…It is owned and operated by a cloud provider delivering cloud service to customers*”. Do we really need a new model of “Public Cloud” to explain what *we know since year 2000 as “Hosting Service”?*
2. “Private Cloud” – quote: “… *is operated exclusively for a single organization. It may be managed by the organization or by a third party, and may be hosted within the organization’s data center or outside of it.*”

So, again we can *easy explain new “Private Cloud” in old and easily understood terms – LAN, WAN, or Outsourced Infrastructure* (LAN, WAN, etc.) and such well established terms are much easier to comprehend and to use than “Private Cloud”

4.1. Cloud Computing misconceptions (4)

CC Deployment Model (continued):
3. “Community Cloud” – quote: “… *the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security, and regulatory considerations, rather than a single organization.*” . A “community” is not a legal entity and cannot sign an agreement, unless organizations within form such entity legally. In this case, we again see one-to-one relationship, and “public cloud” – Hosting Service. So far, since Roman time, there was no legal practice of signing service agreement by a vaguely defined “community” with a service provider.
4. “Hybrid Cloud” – it is a composition: “*… more complex than the other deployment models, since they involve a composition of two or more clouds (private, community, or public). Each member remains a unique entity, but is bound to the others through standardized or proprietary technology that enables application and data portability among them.*” .”
As far as services are concerned, this model is a composition of LAN/WAN (private cloud), and a hosting service (public cloud). “Community”, as we discussed above, is either a hosting service or cannot legally exist.

4.1. Cloud Computing misconceptions (5)

The following tables show what CCS really are:

CC SM	As Hosting Service	As Dynamic Hosting Service
IaaS	Hosting Service	Dynamic Hosting Service (DHS)
PaaS	API Hosting Service	Dynamic API Hosting Service (DAPIHS)
SaaS	Application Hosting Service	Dynamic Application Hosting Service (DAHS)

CC DM	What is it concerning services?
Public Cloud	Hosting Service
Private Cloud	LAN, or WAN, or Outsourced Infrastructure (LAN, WAN, etc.)
Community Cloud	Legal Nonsense
Hybrid Cloud	Interconnected LAN, WAN, and Hosting Service

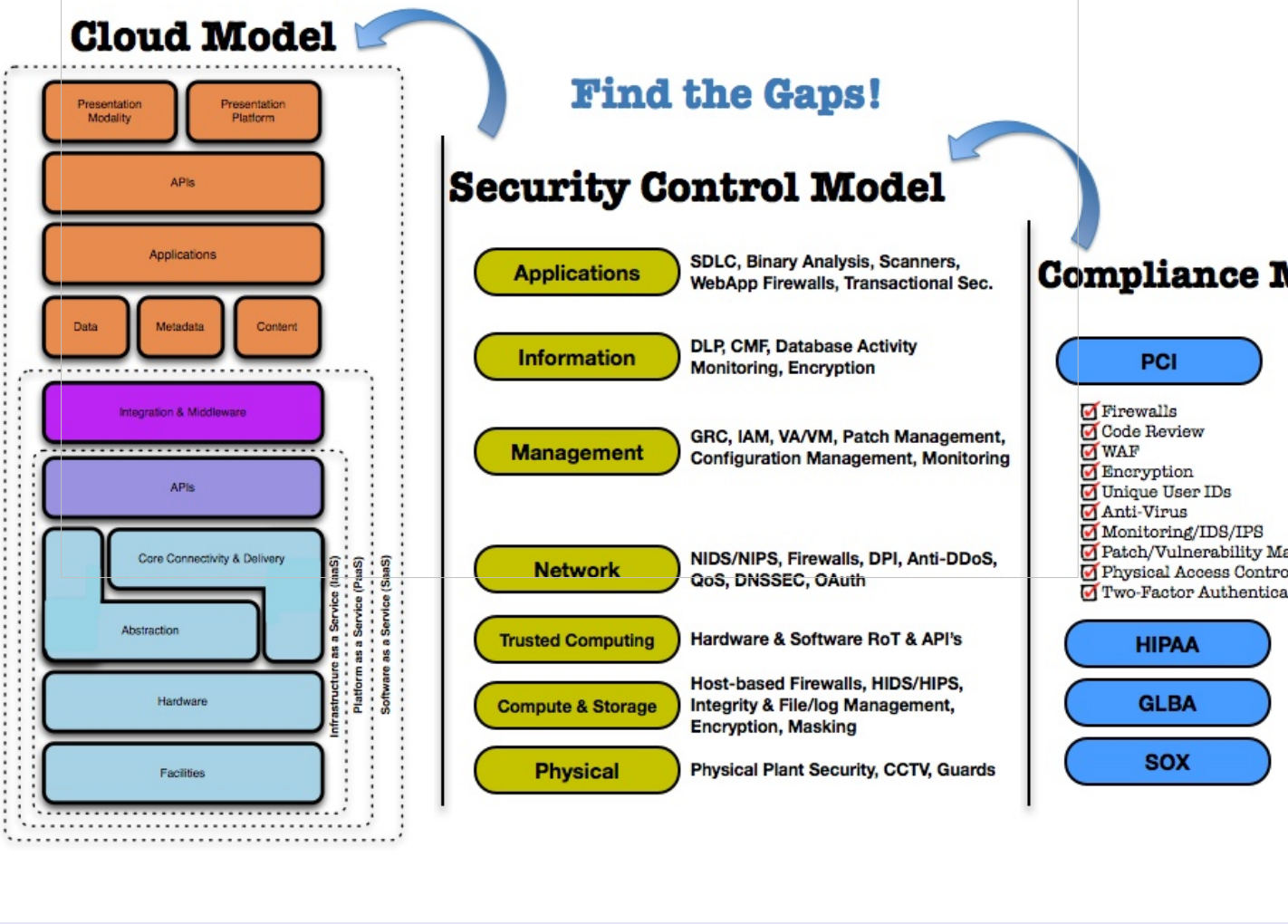
4.2. CC models’ consideration conclusion (1)

The goal of our consideration of CCS was to identify if there is any value in this concept, and if its models would help us in implementation of privacy controls.
Vague and complex models with no real technical value cannot help is our case. Laws are complex, implementation is complex, and any extra complexity will make the implementation unmanageable.
1. Cloud Computing Service Model utilizing IaaS, PaaS and SaaS models is *over sophisticated presentation of a hosting service*; our concept of Dynamic Hosting Service and its extensions (DHS->DAPIHS->DAHS) is based on traditional hosting service model; it is simple and explains interconnection relationship in Internet computing environment as connection between various hosting services and processes transmitting PI.
2. Cloud Computing *Deployment model is irrelevant to the consideration of interconnecting and utilizing PI processes;* in fact new DHS model represent higher abstraction layer, thus infrastructure level can be easy explained in old terms of LAN, WAN, outsources LAN/WAN, and hosting service.

4.2. CC models’ consideration conclusion (1)

Numerous CCS security models do not include what is our core concern – protection of PI in a form of privacy controls. In most cases they are a *derivation of 7-layers OSI model*, and, as in one of the most complex cases below (see picture below), *include cloud model, various security controls (Security Model), references to regulations (Compliance Model), but completely missing what is related to PI protection*. As we see on the picture below, Cloud Model (on the left) does not help at all to understand what is missing concerning privacy protection.

When we talk about DHS, we completely understand that this service should be protected as well, not just infrastructure, nodes, etc. The following paragraph explains our PI protection model.

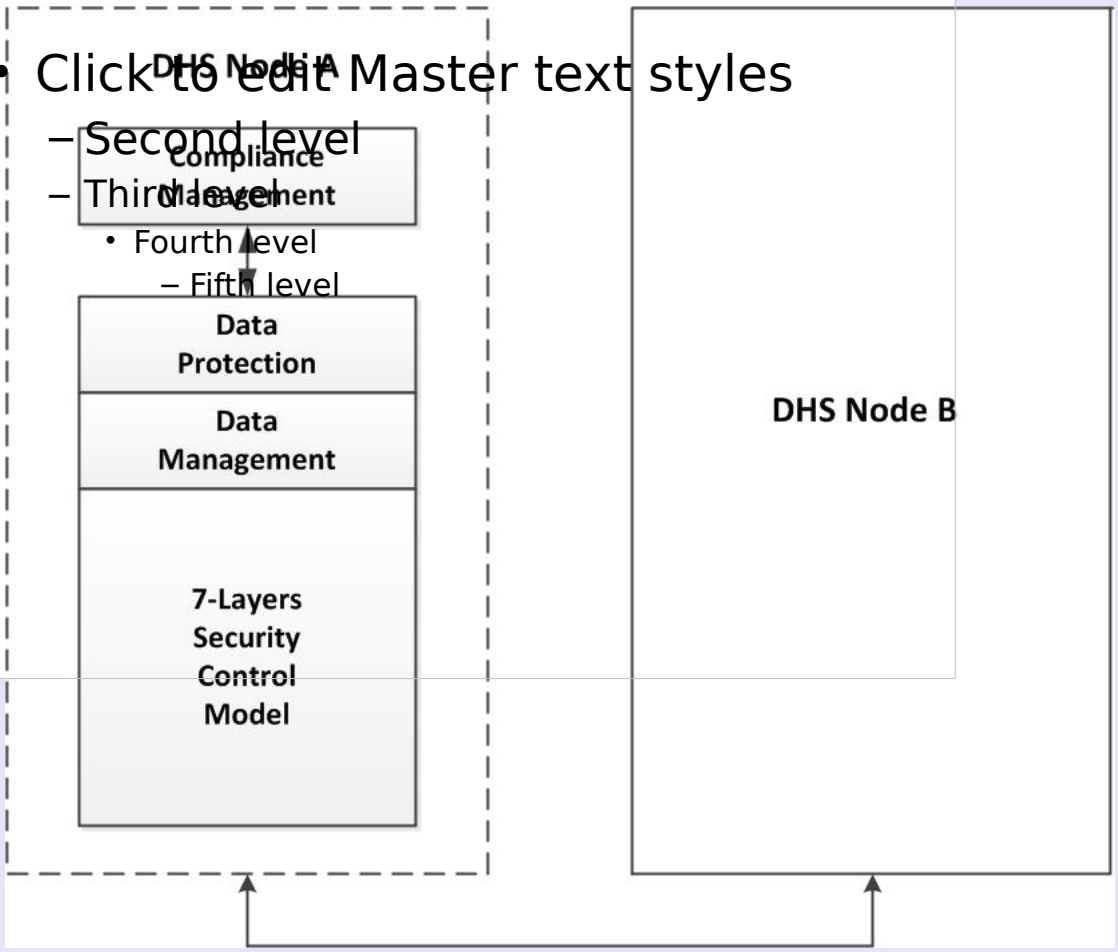

Cloud Model
Presentation Modality
Presentation Platform
APIs
Applications
Data
Metadata
Content
Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Find the Gaps!
Security Control Model
Applications
SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information
DLP, CMF, Database Activity Monitoring, Encryption
Management
GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network
NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing
Hardware & Software RoT & API's
Compute & Storage
Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical
Physical Plant Security, CCTV, Guards
Compliance M
PCI
Firewalls
Code Review
WAF
Encryption
Unique User IDs
Anti-Virus
Monitoring/IDS/IPS
Patch/Vulnerability Ma
Physical Access Contro
Two-Factor Authentica
HIPAA
GLBA
SOX

4.3. PI Protection 9-layer Security and Compliance Model (PIP9 Model) (1)

There are *two privacy protection processes running in between infrastructure nodes providing DHS. They are Data Protection (DP) and Data Management (DM)*. First process - DP - is concerned of various controls providing confidentiality, integrity and availability of PI. The second – DM - *provides necessary controls for manipulation and movement of PI*. Various control information data structures participate in such processes, which identify the status and the location of PI in distributed environment, and we include them in DM as well. Our model also includes Compliance Management (CM) layer, which we place above 9-layer structure with our proposed DP and DM layers. *CM is universal and controls compliance with all involved regulations and internal policies.*
Next table explains the relationship between NIST 800-53 PI controls and layers of our model.

4.3. PI Protection 9-layer Security and Compliance Model (PIP9 Model) (2)

- Click to edit Master text styles
  - Second level
  - Third level
    - Fourth level
      - Fifth level



4.3. PI Protection 9-layer Security and Compliance Model (PIP9 Model) (3)

ID	NIST Privacy Control	PI Protection Model
AR-1	Governance and Privacy Impact	CM
AR-2	Privacy Impact and Risk Assessment	CM
AR-3	Privacy Requirements for Contractors and Service providers	CM
AR-8	Accounting of Disclosures	DM
DI-2	Data Integrity (DI) and DI Board	DP
DM-2	Data Retention and Disposal	DM
IP-1	Consent	DM
IP-2	Individual Access	DP
IP-3	Redress	DM
SE-1	Inventory of Personal Identifiable Information	DM
SE-2	Privacy Incident Response	DP
TR-3	Dissemination of Privacy Program Information	CM
UL-2	Information Sharing	CM

4.4. PIP9 Model conclusion

1. We considered CCS as they are well-known through various sources, including three official US Government NIST standards. *Unfortunately, market driven approach affected the most of associated industries and security professionals,* and NISTs usually balanced position as well. *We cannot use vague models and recommendations if we want to address such challenge as EU GDPR*. We *proposed our simple to understand and getting right to the point Dynamic Hosting Services Model*, which includes two extensions for API and application implementation.
2. *Our high level presentation of processes in Internet computing environment as DHS running on interconnected nodes permitted us to introduce new 9-layer PI protection and Compliance Model*. Such logical and common sense approach *is confirmed by easy fitting of NIST 800-53 privacy controls in our model.*
3. *Our DHS and corresponding PIP9 models give us a change to consider a framework of PI protection implementation* in Internet computing environment

5. PI Protection Implementation framework

Our limits of the implementation are DHS model, PIP9 model, and 13 PI protecting controls from NIST 800-53. We need to stress here that these NIST controls, which we picked up from the original set, address very common EU security community written or verbal concerns over Access, Accounting, Retention, Integrity, Consent, and Redress of PI. Additionally, our list includes Inventory and Incident Response controls.
In our proposed framework we will consider the implementation of three groups of privacy controls, which we identified above, and which correspond to our model layers: Compliance Management, Data Protection and Data Management.
We would like to mention here one *fundamental security principal*, which very often forgotten while always clear in any security regulation:
Outsourcing of security controls and privacy protection functions from Data Owner to a Service Provider does not mean outsourcing responsibility to control security and privacy. It means that Data Owner should be aware of what and where happens, ability and readiness to act, and being responsible for what happened as we see in NIST Privacy Control table.

5.1. Compliance Management (CM)

Compliance Management layer represents the legal part of PI protection implementation, which, according to our PIP9 model, has universal character and is above our DP and DM layers and general security controls (7-layers in our model), and is required by various US regulations like HIPAA Security Rule, SOX, PCI DSS, and others.
There are 5 control at this layer:
1. Governance and Privacy Impact
2. Privacy Impact and Risk Assessment
3. Privacy requirements for contractors and service providers
In this control we introduced Delegation of Trust concept (DoT), which regulates the process of guarantees' exchange and provides unified level of trust.
4. Dissemination of Privacy Program Information
5. Information Sharing

In this presentation we skip descriptions of controls' implementation to simplify fhs discussion. All descriptions provided in the presentation text.

Compliance Management conclusion

1. Having internal and service provider's privacy program, security program, and risk assessment *is the responsibility of PI data owner*.
2, In a case of distributed network of DHS providers, Delegation of Trust should be implemented by having either guarantees from ***all*** service providers, or *independent certification of providers is implemented*.
3, Risk assessment should include DO internal risk assessment, service provider's assessment, and in the provider assessment it *also should be an assessment of risks invoked by the provider's services* to the data owner.
4. Our experience shows that service providers deeply unaware of the meaning of compliance and what are privacy and security requirements, including legal part as above.
5. Each new kind or instance of PI sharing involves complete assessment of privacy controls and may be security controls as well.
6. Such controls of sharing as monitoring and audit of PI usage involves implementation of complex and costly SIEM-class system at each service provider's premises.
7. Privacy Officer should be appointed to supervise activities as above and monitor security status.

5.2. Data Protection (DP)

Per NIST opinion, and we share that, PI data protection is to be implemented mostly by utilizing security controls (which we identified as 7-layer security control model). However, both Data Owner and Service Provider should be aware how to use security controls to protect PI, and what to do in a case of privacy violation.

There are three controls:
1. Data Integrity (DI) and DI Board
2. Individual Access (IA)
3. Privacy Incident Response

Data Protection controls conclusion

1. *Data Protection controls are implemented utilizing associated security controls*. The management of both DO and SP involved in resolution of PI compromises, should be aware of regulatory requirement how to handle such incidents, including reporting to authorities and affected individuals.
2. EU GDPR considers various and complex aspects of sharing and access to PI data, and such requirements should be reflected in Individual Access implementation. In a case of PI data is moving over Internet between DHS processes, access information (like ACL) should move together with data, and is updated according to changing access requests and permissions.

5.3. Data Management (DM) – some ideas of the implementation

1.This group represents controls responsible for support of free movement of data between distributed DHS processes. Whether a transfer of data it dictated by internal status of the infrastructure (failure or overload of a node, etc.) or by a requests for data, *the transfer functions is implemented by a communication connection oriented protocol. Such protocol provides assurance that DM operation has been finished and the status of PI in distributed nodes infrastructure is always known*

*2. DM group of controls guarantee that PI free movement does not mean uncontrolled release of information. Thus, DM control(s) should permit accounting of PI movement and thus knowing where a PI record is now, where there are copies of, and what is the statu*s (active, deleted, etc.)

3. *Conceptual character of GDPR requires that the access to PI should be implemented on per individual record bases and the transfer of records across multiple nodes* rather than collecting all PI records in one central repository. The latter seems impossible to implement considering EU principals of cooperation as well.

4. *Each PI record should have supporting data structures, which we name "descriptors". Such descriptors save and release necessary privacy control information*. We already discussed one of descriptors – ACL – while discussing the access to PI record.

Data Management conclusion

1. We considered an implementation of all NIST Data Management privacy controls in our distributed DHS environment. We suggested using high level connection oriented protocol to transfer PI and control information between nodes.
2. *We concluded that both the nature of GDPR and EU states' cooperation principals require decentralized storing of PI and associated with it information,* and that can be done utilizing DHS nodes infrastructure.
2. *Decentralized PI and control information should reside in each DHS node, which thus is considered as "parent" node for PI originated in it and all PI control information.* The latter resides in an information depository named "Parent Status Descriptor".
3. *Depository of all control information is an inventory keeping information about DHS distributed infrastructure, and information about all operations with PI and where is has been released. Parent Status Descriptor information is changed upon conclusion of each DM operation.*
4. It was possible to design implementation framework utilizing proposed solution for all NIST Data Management group control, thus proving that all standard operations with PI is possible to implement within our models and the framework.

6. The Presentation Conclusion

1. *We proved that our approach of replacing Cloud Computing services by Dynamic Hosting Service model works*. Instead of using sophisticated combination of useless models, we concentrate on one, which is high level, simple and easy to use.
2. We analyzed three major regulations concerned of PI protection – EU General Data Protection Regulation, and US NIST 800-53 Privacy Control standards and HIPAA Privacy Rule. *We identified that complex and thorough GDBR requirements can be mapped to NIST controls*, and which provide a ground for privacy controls implementation framework.
3. *We proposed new 9-Layer PI Protection Security Model (PIP9), which include considered as standard 7-layer Security Control Model and two additional of data protection and Data Management representing PI protection. The model also includes Compliance Management layer*.
4. *We divided 13 NIST Privacy Controls is three groups corresponding to our PIP9 model, and considered implementation of controls utilizing proposed models and principals*. It was possible to develop the implementation framework, which covers our list NIST privacy controls and required operations with PI, thus implementing in our framework high level GDPR requirements.

7. References (1)

1. Mikhail A. Utin, Daniil Utin. US Experience: Laws, Compliance, and Real Life – When everything seems right but simply does not work; DeepSec 2011, Vienna, November, 2011.
2. 45 CFR Subtitle A, Subchapter C, Part 164, Subpart C – Security Standards for the Protection of Electronic Protected health Information
3. Mikhail A. Utin, Daniil Utin. Private Information Protection in Cloud Computing – Laws, Compliance and Cloud Security Misconceptions, OWASP AppSec DC 2011, April, 2012.
4. Proposal for a regulation of the European parliament and of the Council on the protection of individuals with regards to the protection of personal data and on the free movement of such data (General Data Protection Regulation); COM(2012) 11 final, Brussels, 25.1.2012
5. National Institute of Standards and Technology (NIST), US Department of Commerce, NIST Special Publication 800-53 Revision 4: Security and Privacy Controls in Federal Information Systems and Organizations, February, 2012.
6. 45 CFR Subtitle A, Subchapter C, Part 164, Subpart E – Privacy of Individually Identifiable Health Information.

7. References (2)

7. Review: National Concerns over the proposed EU Data Protection regulation, Infosecurity magazine, August 6, 2012; http://www.infosecurity-magazine.com/view/27399/national-concern
8. GovTrack.us: S3333 - Data Security and Breach Notification Law http://www.govtrack.us/congress/bills/112/s3333/text
9. Code of Massachusetts Regulations: 201 CMR 17.00: Standards for protection of Personal Information of Residents of the Commonwealth - http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf
10. MGL Chapter 93H – Security Breaches - http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chap
11. Public Law 111-5, February 17, 2009 - http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.p
12. Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, December 2011.

7. References (3)

13. The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September, 2011.
14. Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146, May 2012.
15. Wikipedia: Cloud computing - http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Service_m
16. Wikipedia: Cloud computing security model - http://www.google.com/search?q=cloud+computing+security+mod
17. Computer Incident Handlinh Guide, NIST Special Publication 800-61 R1, March, 2008.

Thank you!

All questions will be answered:

- mikhailutin@hotmail.com

or

- mutin@rubos.com

Rubos, Inc. (presentations, texts, articles, etc.)

- www.201cmr17.00ma.com
- This presentation will be available on DeepSec site or on our site above