US experience: Laws, Compliance, and Real Life - When everything seems right but simply does not work

Special research prepared by Rubos, Inc. team

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

Prepared for DeepSec 2011

Presented by Mikhail Utin, CISSP, Ph.D.

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

Improving information security

- **- Vulnerability discovery**
- **- - white hat hacking**
- **- - -individual contribution**
- **- - -minimal resources**
-
- **- New protective methods for defense in depth**
- **- - researched and implemented by large corporations and require significant resources**
-
- **Foster child – SMB (this is our research concern):**
- **- Grass level security – computer users having minimal resources, minimal security options and minimal protection (perimeter firewall and end-point security set)**
- **- FBI shut down Estonian botnet – limited and temporary success?**

US business landscape

Specific business organization:

- **- 90% small businesses - less than 100 employees**
- **- Freedom of doing business**
- **- - simple registration process**
- **- - low cost registration**
- **- Small business psychology – strict focus only on business matters, very limited security concerns**

PI protection is growing global concern – avoiding pitfalls

Two regulations affecting small businesses
General consideration

- **- Federal – HIPAA/HITECH – covers all businesses having Personal health Information, not only medical;**
- **--Medical is one of the most insecure business sectors - data loses from http://datalossdb.org:**
- **-- Medical sector had 30% in 2010 and 25% in 2011 of total US data losses (all other businesses – 39% and 46% respectfully)**
- **- State of Massachusetts (MA) 201 CMR 17.00 Standards/M.G.L. Chapter 93H Security Breaches: first in US history and possibly around the world covering almost all businesses in the state**
- **-- medical and supporting services sector is very important part of MA economy**

Information Security Implementation Model

- - Regulations (laws, standards, policies, etc.) - government
- - Regulation Enforcement - government
- - Implementation - business
- - Audit – government – all stick and no carrot

Government controls three phases, but excludes itself from Implementation completely

Rules of compliance enforcement are not clearly identified - affects Regulation Enforcement and Audit

The US laws protecting personal information

US laws require protection of personal information. We are discussing private sector.

Security situation in the US is defined by business and medical sector

Data Loss/incidents from http://datalossdb.org

- **Incidents by business type:**
- **2010 2011**
- **- Business 39% 46%**
- **- Medical 30% 25%**
- **- Government 17% 16%**
- **- Education 14% 12%**

US Regulations Protecting Personal Information (1)

Mostly used for protecting personal health information:

- **- HIPAA – Health Insurance Accountability and Portability Act, 1996 with Security Rule, 2003; covers businesses dealing with personal health information (PHI) – more than emdical sector**
- **- HITECH (Subtitle D) – Health Information Technology for Economic and Clinical Health Act, 2009**
- **- - Extends HIPAA enforcement, because the required compliance was largely ignored**
- **- - Increases penalties up to $1.5 million**
- **- - Extends provisions of the law to associated businesses**
- **- - Requires notification of authorities in a case of PHI loss.**

US Regulations Protecting Personal Information (2)

Additional regulations:

- **- GLBA – Gramm-Leach-Bliley Act, 1999; Financial Privacy Rule and Safeguard Rule, and Pre-texting Protection; covers US financial services businesses**
- **- SOX – Sarbanes-Oxley Act, 2002; it has some peripheral involvement in data protection and, by extension, in personal information, by requiring it to be certified by executive's financial report;**
- **- FACTA – Fair and Accurate Credit Transaction Act, 2003; in its Disposal Rule the law requires appropriate destruction of customer data;**
- **- ITADA – Identity Theft and Assumption Deterrence Act, 1998; set up penalties for usage of stolen identity or related identification documents;**
- **- FERPA – Family Educational Rights and Privacy Act, 2009; requires protection of student's educational records.**

State of Massachusetts 201 CMR 17.00 Standards for protection of Personal Information (PI)

First in human history:

- **- Covers at least 99% of the state businesses, plus out of state businesses having PI of Massachusetts residents**
- **- Released in September, 2008, and had FOUR compliance deadlines**
- **- Requires Comprehensive Information security Program document**
- **- Combines management level requirements (maintain a comprehensive information security program) together with technical ones (reasonable up to date firewall protection)**
- **- *Service providers required by a contract to implement and maintain appropriate security measure***

Laws' imperfectness and short-sighting
What are we trying to answer?

Complex laws and standards cause confusion and drive businesses to ignore them. How to resolve the deadlock?

- **- In response government is imposing additional requirements and penalties. Does it really help to improve security?**
- **- Could compliance be achieved at all, and by small and medium businesses in particular?**
- **- Enforcement, i.e. penalties: good intentions may lead to unexpected results**
- **- Can business and government really join efforts? Who delivers the message?**

Information Security Implementation Model

- **- Regulations (laws, standards, policies, etc.) – complex and confusing**
- **- Regulation Enforcement – large indiscriminate penalties driving to hide data losses, rules of enforcement are unknown**
- **- Implementation – business is alone, no government involvement**
- **- Audit – government – all stick and no carrot –no incentives to disclose losses**

Verizon Data Breach Investigation Report, 2011 (DBIR) Statistics in support of this research

- In cooperation with US Security Services
- - Verizon – communication services and Internet services provider
- - Includes 667 US Security Services cases
- - 94 Verizon own cases (one third is European and Asia Pacific, the rest is US)
- - 96% are US related cases

Why HIPAA/HITECH and 201 CMR? Two widely applicable regulations

- **Federal – HIPAA/HITECH**
- **- More than 25% of US data loss cases are from "compliant" medical and related services organizations (http://datalossdb.org**
- **- Covers hundreds of thousands small medical offices, practices and supporting businesses; small and medium size businesses are likely 90% of medical and supporting US economy sectors**
- **State of Massachusetts – 201 CMR 17.00/M.G.L.93H**
- **- Covers 99% of more than 700,000 businesses, 90% are Small and Medium size**
- **Laws are challenging businesses, and businesses are challenging laws.**

Should we bother requiring security for the masses?

- **- SMB masses statistically define information security level in the US - SMBs as major target – 67% of incidents in entities having less than 100 employees by Verizon DBIR**
- **- Low level of understanding of threats and information security**
- **- Gaps in basic security controls – Verizon DBIR "…96% of breaches were avoidable through simple or intermediate controls."**
- **- SMBs are the foundation for botnets**
- **- Easy to break in and steal information**
- **- Easy way of making money – will discuss below**
- **- Attacks switching to SMBs:**
- **-- dropping the number of compromised records (from Verizon DBIR):**
- **---- 2008 – 360,000,000, 2009 – 143,000,000, 2010 – 3,800,000**
- **---- 2010 – 5,000 records per incident, 76 % from servers – SMB infrastructure**

Achieving compliance – are there some problems?

- **Yes, SMBs have persistent security problems as discussed**
- **NO compliance statistics neither from federal nor from state government**
- **Example: PCI DSS, which is private regulation**
- **- Clear and straightforward implementation, HOWEVER**
- **- “89% of data loss victims WERE NOT COMPLIANT” (Verizon DBIR) meaning failing to implement rudimentary security controls (OS patching, AV software, etc.)**
- **HIPAA:**
- **- High level of standards not easy to translate into technical requirement and then implement**
- **201 CMR 17.00:**
- **- Mixed high and low level requirements – not easy to translate and then implement**
- **Our estimate – 1% or lower of really compliant SMBs**
- **Major requirement – Information Security Program – requires professional knowledge of security professional and lawyer**
- **Major problem: no resources to implement sophisticated government requirements**
- **Government efforts to enforce information security by compliance are failing simply because 1) - compliance requires unusual activities and significant efforts, which 2) - are not compatible with SMB resources.**

What is the cost of compliance? Going practical

Small company of 10 employees wants to be HIPAA and 201 CMR compliant

- **What does it mean to start implementing regulations?**
- **- HIPAA: “Standard: Security management process: Implement policies and procedures to prevent, detect, contain, and correct security violations.”**
- **- 201 CMR: “… shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts …”**
- **The company lacks expertise and resources for implementation.**
- **Is there outside help/guidance?**
- **- Government provides NO guidance to “decode” requirements**
- **- Inexpensive commercial framework documents require professional help to complete and interpretation for implementation**
- **While requiring mandatory compliance, the government does not provide any help.**

Turning the company to a security professional help
Cost estimate (1)

- **Compliance path:**
- **- Security Program development:**
- **-- HIPAA – 40 documents/policies, 200 pages set**
- **-- 201 CMR - Fewer documents/pages, but very mixed nature of high and low level controls, 20 pages set**
- **- Implementation of controls**
- **- Assessment of the implementation compliance**
- **Security Program content and size depends on the company size and available resources**

Turning the company to a security professional help Cost estimate (2)

- **Approximate costs:**
- **- HIPAA Program development for each new customer ($50,000 and 40 weeks)**
- **- HIPAA re-used/ re-written - $20,000**
- **- HIPAA minimal Program cost – $10,000**
- **- 201 CMR Program cost - $5,000**
- **Implementation costs – $5,000**
- **Total HIPAA + 201 CMR minimal implementation cost: $20,000**
- **Small medical office/company expectation: $5,000**
- **Thus, it reluctance to pay $20,000 for “security compliance”, because:**
- **- Market delivers confusing solutions priced from $200 to $50,000**
- **- No understanding if a solution corresponds to required “compliance”**
- **- Inability to verify what is delivered for tens of thousands of dollars**

What are the other SMB incentives to comply?

Confused by government and market, could they be forced to comply?

- **Enforcement - penalties for “non-compliance and negligence”:**
- **- Original HIPAA – no penalties (2003) – did not encourage compliance**
- **- Current practice – only AFTER a data loss had happened, on case by case basis, not by records lost**
- **- HITECH changed penalties to up to $1,500,000 (minimal - $50,000) for intentional non-compliance/negligence**
- **-- Precedent set by DHHS in 2011: Massachusetts General Hospital was penalized for $1,000,000 for the loss of 197 medical personal records**
- **- 201 CMR – up to $5,000 – insufficient penalty for driving enforcement**
- **Current government enforcement on “post-mortem” basis violates the cornerstone principle of compliance being a PREVENTIVE measure**
- **As an “encouragement”, HIPAA/HITECH calls for regular reviews of compliance (not yet 201 CMR).**

Excessive penalties and uncertainty of their application - Opposite result in practice

- **HIPAA/HITECH “covered entities”:**
- **- Non-compliant entity can be fined up to $1,500,000 even for one lost record, *there are no rules defining penalty per record lost***
- **- Business can be bankrupted by a penalty, fees and loss compensating activities**
- **- Ransom payment and coordinated silence – logical alternative to reporting to government with subsequent investigation, potential large penalties, various fees, and a chance of bankruptcy**
- **Sometimes a law in its best intentions produces a completely opposite result in practice, and uncertain rules of law enforcement set up a perfect ground for a crime.**

How to verify the compliance

SMB did to the best of its knowledge –

Is that what the government wanted?

- **- Security Program has been implemented and security controls are in place…**
- **- SMB has done self-audit and everything is implemented – is it compliant now?**
- **- The initial interpretation of government standards could be incorrect or incomplete**
- **- Is there a government compliance checklist?**
- **-- HIPAA –YES, but there is NO direct correlation between HIPAA standards and the audit checklist of security controls**
- **-- 201 CMR – NO implementation checklist**

Automated verification of compliance – The most advertised security service

- **Security solutions' vendors:**
- **- Automated verification of traditional security controls is not a policy implementation verification**
- **- There is no government checklist to verify compliance**
- **- Manually written policy cannot be automatically verified**
- **Solution for getting security program and following self-assessment:**
- **- Automated generation of professionally designed security program according to business IT and security profile**
- **- Database profile of implemented customers' security controls**
- **- Automated independent verification of implemented security controls against the database profile**
- **- Proof of concept: free security program generation for 201 CMR standards on www.201cmr1700ma.com**

Conclusion

- The goal of improving security of millions of businesses dictates close cooperation and understanding between all participants of the process. Enacting laws is not quite sufficient for millions of US small and mid-size businesses to encourage compliance. Government should be proactive and provide consulting and guidance in various forms, including documents' development. Chaotic security products market then would become more organized to address customer's need in transparent compliance services. Government should be proactive in continuing verification of compliance status as well. Prevention of incidents is a basic security principle, and "post mortem" approach of security incident government investigation does not coincide with it. Automation of policy generation and follow-up compliance verification can significantly simplify the entire process, but will work correctly only if generation and verification utilizes the same information source.
- Government should be extremely cautious in enacting drastic enforcement measures; otherwise it could trigger attacks against SMBs.
- The future of information security in the US depends on whether the government will finally understand that imposing regulations is only the first step. Guidance and helping in practical implementation is required as well.

Thank you!

All questions will be answered:

mikhailutin@hotmail.com
or
mutin@rubos.com

Our site: www.201cmr17.00ma.com

DeepSec, 2011.

US experience: Laws, Compliance, and Real Life - When everything seems right but simply does not work

Special research prepared by Rubos, Inc. team

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

Prepared for DeepSec 2011

Presented by Mikhail Utin, CISSP, Ph.D.

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

Improving information security

- **- Vulnerability discovery**
- **- - white hat hacking**
- **- - -individual contribution**
- **- - -minimal resources**
-
- **- New protective methods for defense in depth**
- **- - researched and implemented by large corporations and require significant resources**
-
- **Foster child – SMB (this is our research concern):**
- **- Grass level security – computer users having minimal resources, minimal security options and minimal protection (perimeter firewall and end-point security set)**
- **- FBI shut down Estonian botnet – limited and temporary success?**

US business landscape

Specific business organization:

- **- 90% small businesses - less than 100 employees**
- **- Freedom of doing business**
- **- - simple registration process**
- **- - low cost registration**
- **- Small business psychology – strict focus only on business matters, very limited security concerns**

PI protection is growing global concern – avoiding pitfalls

Two regulations affecting small businesses
General consideration

- **- Federal – HIPAA/HITECH – covers all businesses having Personal health Information, not only medical;**
- **--Medical is one of the most insecure business sectors - data loses from http://datalossdb.org:**
- **-- Medical sector had 30% in 2010 and 25% in 2011 of total US data losses (all other businesses – 39% and 46% respectfully)**
- **- State of Massachusetts (MA) 201 CMR 17.00 Standards/M.G.L. Chapter 93H Security Breaches: first in US history and possibly around the world covering almost all businesses in the state**
- **-- medical and supporting services sector is very important part of MA economy**

Information Security Implementation Model

- **- Regulations (laws, standards, policies, etc.) - government**
- **- Regulation Enforcement - government**
- **- Implementation - business**
- **- Audit – government – all stick and no carrot**

Government controls three phases, but excludes itself from Implementation completely

Rules of compliance enforcement are not clearly identified - affects Regulation Enforcement and Audit

The US laws protecting personal information

US laws require protection of personal information. We are discussing private sector.

Security situation in the US is defined by business and medical sector

Data Loss/incidents from http://datalossdb.org

- **Incidents by business type:**

	2010	2011
- Business	39%	46%
- Medical	30%	25%
- Government	17%	16%
- Education	14%	12%

US Regulations Protecting Personal Information (1)

Mostly used for protecting personal health information:

- **- HIPAA – Health Insurance Accountability and Portability Act, 1996 with Security Rule, 2003; covers businesses dealing with personal health information (PHI) – more than emdical sector**
- **- HITECH (Subtitle D) – Health Information Technology for Economic and Clinical Health Act, 2009**
- **- - Extends HIPAA enforcement, because the required compliance was largely ignored**
- **- - Increases penalties up to $1.5 million**
- **- - Extends provisions of the law to associated businesses**
- **- - Requires notification of authorities in a case of PHI loss.**

US Regulations Protecting Personal Information (2)

Additional regulations:

- **- GLBA – Gramm-Leach-Bliley Act, 1999; Financial Privacy Rule and Safeguard Rule, and Pre-texting Protection; covers US financial services businesses**
- **- SOX – Sarbanes-Oxley Act, 2002; it has some peripheral involvement in data protection and, by extension, in personal information, by requiring it to be certified by executive's financial report;**
- **- FACTA – Fair and Accurate Credit Transaction Act, 2003; in its Disposal Rule the law requires appropriate destruction of customer data;**
- **- ITADA – Identity Theft and Assumption Deterrence Act, 1998; set up penalties for usage of stolen identity or related identification documents;**
- **- FERPA – Family Educational Rights and Privacy Act, 2009; requires protection of student's educational records.**

State of Massachusetts 201 CMR 17.00 Standards for protection of Personal Information (PI)

First in human history:

- **- Covers at least 99% of the state businesses, plus out of state businesses having PI of Massachusetts residents**
- **- Released in September, 2008, and had FOUR compliance deadlines**
- **- Requires Comprehensive Information security Program document**
- **- Combines management level requirements (maintain a comprehensive information security program) together with technical ones (reasonable up to date firewall protection)**
- ***- Service providers required by a contract to implement and maintain appropriate security measure***

Laws' imperfectness and short-sighting

What are we trying to answer?

Complex laws and standards cause confusion and drive businesses to ignore them. How to resolve the deadlock?

- **- In response government is imposing additional requirements and penalties. Does it really help to improve security?**
- **- Could compliance be achieved at all, and by small and medium businesses in particular?**
- **- Enforcement, i.e. penalties: good intentions may lead to unexpected results**
- **- Can business and government really join efforts? Who delivers the message?**

Information Security Implementation Model

- **- Regulations (laws, standards, policies, etc.) – complex and confusing**
- **- Regulation Enforcement – large indiscriminate penalties driving to hide data losses, rules of enforcement are unknown**
- **- Implementation – business is alone, no government involvement**
- **- Audit – government – all stick and no carrot –no incentives to disclose losses**

Verizon Data Breach Investigation Report, 2011 (DBIR) Statistics in support of this research

- **In cooperation with US Security Services**
- **- Verizon – communication services and Internet services provider**
- **- Includes 667 US Security Services cases**
- **- 94 Verizon own cases (one third is European and Asia Pacific, the rest is US)**
- **- 96% are US related cases**

Why HIPAA/HITECH and 201 CMR?
Two widely applicable regulations

- **Federal – HIPAA/HITECH**
- **- More than 25% of US data loss cases are from "compliant" medical and related services organizations (http://datalossdb.org**
- **- Covers hundreds of thousands small medical offices, practices and supporting businesses; small and medium size businesses are likely 90% of medical and supporting US economy sectors**
- **State of Massachusetts – 201 CMR 17.00/M.G.L.93H**
- **- Covers 99% of more than 700,000 businesses, 90% are Small and Medium size**
- **Laws are challenging businesses, and businesses are challenging laws.**

Should we bother requiring security for the masses?

- **- SMB masses statistically define information security level in the US - SMBs as major target – 67% of incidents in entities having less than 100 employees by Verizon DBIR**
- **- Low level of understanding of threats and information security**
- **- Gaps in basic security controls – Verizon DBIR "…96% of breaches were avoidable through simple or intermediate controls."**
- **- SMBs are the foundation for botnets**
- **- Easy to break in and steal information**
- **- Easy way of making money – will discuss below**
- **- Attacks switching to SMBs:**
- **-- dropping the number of compromised records (from Verizon DBIR):**
- **---- 2008 – 360,000,000, 2009 – 143,000,000, 2010 – 3,800,000**
- **---- 2010 – 5,000 records per incident, 76 % from servers – SMB infrastructure**

Achieving compliance – are there some problems?

- **Yes, SMBs have persistent security problems as discussed**
- **NO compliance statistics neither from federal nor from state government**
- **Example: PCI DSS, which is private regulation**
- **- Clear and straightforward implementation, HOWEVER**
- **- "89% of data loss victims WERE NOT COMPLIANT" (Verizon DBIR) meaning failing to implement rudimentary security controls (OS patching, AV software, etc.)**
- **HIPAA:**
- **- High level of standards not easy to translate into technical requirement and then implement**
- **201 CMR 17.00:**
- **- Mixed high and low level requirements – not easy to translate and then implement**
- **Our estimate – 1% or lower of really compliant SMBs**
- **Major requirement – Information Security Program – requires professional knowledge of security professional and lawyer**
- **Major problem: no resources to implement sophisticated government requirements**
- **Government efforts to enforce information security by compliance are failing simply because 1) - compliance requires unusual activities and significant efforts, which 2) - are not compatible with SMB resources.**

What is the cost of compliance? Going practical

Small company of 10 employees wants to be HIPAA and 201 CMR compliant

- **What does it mean to start implementing regulations?**
- **- HIPAA: "Standard: Security management process: Implement policies and procedures to prevent, detect, contain, and correct security violations."**
- **- 201 CMR: "… shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts …"**
- **The company lacks expertise and resources for implementation.**
- **Is there outside help/guidance?**
- **- Government provides NO guidance to "decode" requirements**
- **- Inexpensive commercial framework documents require professional help to complete and interpretation for implementation**
- **While requiring mandatory compliance, the government does not provide any help.**

Turning the company to a security professional help
Cost estimate (1)

- **Compliance path:**
- **- Security Program development:**
- **-- HIPAA – 40 documents/policies, 200 pages set**
- **-- 201 CMR - Fewer documents/pages, but very mixed nature of high and low level controls, 20 pages set**
- **- Implementation of controls**
- **- Assessment of the implementation compliance**
- **Security Program content and size depends on the company size and available resources**

Turning the company to a security professional help
Cost estimate (2)

- **Approximate costs:**
- **- HIPAA Program development for each new customer ($50,000 and 40 weeks)**
- **- HIPAA re-used/ re-written - $20,000**
- **- HIPAA minimal Program cost – $10,000**
- **- 201 CMR Program cost - $5,000**
- **Implementation costs – $5,000**
- **Total HIPAA + 201 CMR minimal implementation cost: $20,000**
- **Small medical office/company expectation: $5,000**
- **Thus, it reluctance to pay $20,000 for "security compliance", because:**
- **- Market delivers confusing solutions priced from $200 to $50,000**
- **- No understanding if a solution corresponds to required "compliance"**
- **- Inability to verify what is delivered for tens of thousands of dollars**

What are the other SMB incentives to comply?

Confused by government and market, could they be forced to comply?

- **Enforcement - penalties for "non-compliance and negligence":**
- **- Original HIPAA – no penalties (2003) – did not encourage compliance**
- **- Current practice – only AFTER a data loss had happened, on case by case basis, not by records lost**
- **- HITECH changed penalties to up to $1,500,000 (minimal - $50,000) for intentional non-compliance/negligence**
- **-- Precedent set by DHHS in 2011: Massachusetts General Hospital was penalized for $1,000,000 for the loss of 197 medical personal records**
- **- 201 CMR – up to $5,000 – insufficient penalty for driving enforcement**
- **Current government enforcement on "post-mortem" basis violates the cornerstone principle of compliance being a PREVENTIVE measure**
- **As an "encouragement", HIPAA/HITECH calls for regular reviews of compliance (not yet 201 CMR).**

Excessive penalties and uncertainty of their application - Opposite result in practice

- **HIPAA/HITECH "covered entities":**
- **- Non-compliant entity can be fined up to $1,500,000 even for one lost record, *there are no rules defining penalty per record lost***
- **- Business can be bankrupted by a penalty, fees and loss compensating activities**
- **- Ransom payment and coordinated silence – logical alternative to reporting to government with subsequent investigation, potential large penalties, various fees, and a chance of bankruptcy**
- **Sometimes a law in its best intentions produces a completely opposite result in practice, and uncertain rules of law enforcement set up a perfect ground for a crime.**

How to verify the compliance

SMB did to the best of its knowledge –

Is that what the government wanted?

- **- Security Program has been implemented and security controls are in place…**
- **- SMB has done self-audit and everything is implemented – is it compliant now?**
- **- The initial interpretation of government standards could be incorrect or incomplete**
- **- Is there a government compliance checklist?**
- **-- HIPAA –YES, but there is NO direct correlation between HIPAA standards and the audit checklist of security controls**
- **-- 201 CMR – NO implementation checklist**

Automated verification of compliance – The most advertised security service

- **Security solutions' vendors:**
- **- Automated verification of traditional security controls is not a policy implementation verification**
- **- There is no government checklist to verify compliance**
- **- Manually written policy cannot be automatically verified**
- **Solution for getting security program and following self-assessment:**
- **- Automated generation of professionally designed security program according to business IT and security profile**
- **- Database profile of implemented customers' security controls**
- **- Automated independent verification of implemented security controls against the database profile**
- **- Proof of concept: free security program generation for 201 CMR standards on www.201cmr1700ma.com**

Conclusion

- The goal of improving security of millions of businesses dictates close cooperation and understanding between all participants of the process. Enacting laws is not quite sufficient for millions of US small and mid-size businesses to encourage compliance. Government should be proactive and provide consulting and guidance in various forms, including documents' development. Chaotic security products market then would become more organized to address customer's need in transparent compliance services. Government should be proactive in continuing verification of compliance status as well. Prevention of incidents is a basic security principle, and "post mortem" approach of security incident government investigation does not coincide with it. Automation of policy generation and follow-up compliance verification can significantly simplify the entire process, but will work correctly only if generation and verification utilizes the same information source.
- Government should be extremely cautious in enacting drastic enforcement measures; otherwise it could trigger attacks against SMBs.
- The future of information security in the US depends on whether the government will finally understand that imposing regulations is only the first step. Guidance and helping in practical implementation is required as well.

Thank you!

All questions will be answered:

mikhailutin@hotmail.com
or
mutin@rubos.com

Our site: www.201cmr17.00ma.com

DeepSec, 2011.