Ekaru Connecting People With Technology

201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth

February 28, 2013

Microsoft Small Business Specialist

Microsoft CERTIFIED Partner

Agenda

- Why? Genesis of the MA law
- Law went into effect March 1, 2010
- Review of ALL requirements, focus on technical requirements
- Steps to meet requirements
- Q&A

Why?

- Many High-Profile breaches in Massachusetts:
  - TJX Corporation – Exposed over 100million credit/debit numbers and thousands of drivers' license numbers to hackers
  - Hannaford – Exposed over 4 million credit/debit numbers to hackers
  - …

Real World Example: BlueCross/BlueShield Breach

- BCBS employee took home a spreadsheet on a laptop to work on it after hours.
- The laptop was stolen from a car
- No one knew exactly what was on the laptop. Several weeks later, they realized that personal information for just about all BCBS Physicians nationwide were on the laptop.
- The laptop was NOT encrypted.
- 39,000 MA physicians notified of breach at BCBS (estimate 850,000 nationwide!)
- Physicians not notified for several months because laptop content was unknown.
- BCBS needed to review/improve security.

Laws already in effect:

- Federal – Red Flags Rule
- HIPAA
- …
- Massachusetts General Law: Security Breach Requirements – 93H (2007)
- The notifications to the Office of Consumer Affairs and Business Regulation and to the Attorney General must include:
  - A detailed description of the nature and circumstances of the breach of security or unauthorized acquisition or use of personal information;
  - The number of Massachusetts residents affected as of the time of notification;
  - The steps already taken relative to the incident;
  - Any steps intended to be taken relative to the incident subsequent to notification; and
  - Information regarding whether law enforcement is engaged investigating the incident.

93I – Data Destruction…

- When disposing of records, each agency or person shall meet the following minimum standards for proper disposal of records containing personal information:
- (a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;
- (b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.
- Any agency or person who violates the provisions of this chapter shall be subject to a civil fine of not more than $100 per data subject affected, provided said fine shall not exceed $50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties.

Statistics

- 2007-2008:
  - OCABR received reports of nearly 320 incidents
  - Incidents affected 625,365 Massachusetts residents.
  - Sixty percent of the cases involved criminal and/or unauthorized acts, with a high frequency of laptops or hard-drives being stolen.
  - The remainder of the breaches resulted from employee error or poor internal handling of sensitive information.
  - Approximately 75% of the reported incidents involved data that was not encrypted or password protected.

201 CMR 17.00

- In response to some high profile data theft cases, the MA government introduced a new law to help protect individuals from identity theft.
- The name of the law: 201 CMR 17.00 Standards for The Protection of Personal Information of Residents of the Commonwealth
- The law affects just about every business in MA, but there has been very little publicity on it.
- **The new law went into effect MARCH 1, 2010**

What does the law say?

- The regulation states that “(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

…New Law

(a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;

(b) the amount of resources available to such person;

(c) the amount of stored data; and

(d) the need for security and confidentiality of both consumer and employee information.

…New Law

…The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated."

Definition of “Person”

- Person is a
  - natural person
  - Corporation
  - Association
  - Partnership or other legal entity
  - Other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches or political subdivision thereof.

Definition of "Personal Information"

- A Massachusetts resident's first name and last name or first initial and last name in combination with any of the following:
  - Social Security Number
  - Drivers License or State Issued ID
  - Financial Account number or credit or debit card number

Q: Who is covered by the new law?

- All businesses with employees
- All businesses who receive credit card payments

- *A: Just about all businesses in Massachusetts! The goal is to prevent identity theft.*

Step 1: Data Audit

- What data do you have?
  - Employees, customers, prospects, donors… etc
  - Where is the data stored (physical AND electronic?
  - Types of data:
    - I-9 Forms
    - Retirement plan documents
    - Direct deposit forms
    - Credit card payments… etc.
    - …

2. Requirements..

- (a) Designate one or more employees to maintain the security program
- (b) Identify/Assess current risks to the security of all electronic, paper or other records
  - Ongoing training
  - Compliance with policies and procedures
  - Means to detect and prevent security system failures

Requirements…

- (c) Security policies for storage, access, and transportation outside of the business
- (d) Impose disciplinary measures
- (e) Prevent terminated employees from access to restricted records
- (f) Take steps to ensure third party providers follow security measures

Requirements…

- (g) Reasonable restrictions for physical access – storage in locked facilities or containers
- (h) Regular monitoring and upgrading of safeguards
- (i) Review scope of security measures at least annually
- (j) Document responsive actions taken in connection with a breach

Computer System Security Requirements

What's new about this law is that it goes into great detail regarding computer system requirements.

Technology requirement #1

1. **“Secure user authentication protocols including:**

   (a) control of user IDs and other identifiers;

   (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

   (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

   (d) restricting access to active users and active user accounts only; and

   (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;”

… Technology Requirement #1

- *Strong Passwords include 8 or more characters, include uppercase letters, lowercase letters, numbers, and symbols. Never use a word in the dictionary.*
  - *GOOGLE: Microsoft Strong Password Checker…. You can actually see the strength of the password grow with increased character types, etc.*
- *90 Day Password Policy.*
- *Domain authentication should be used for businesses with a server.*
- *"Technically feasible" – not all applications have password policies*

Technology requirement #2

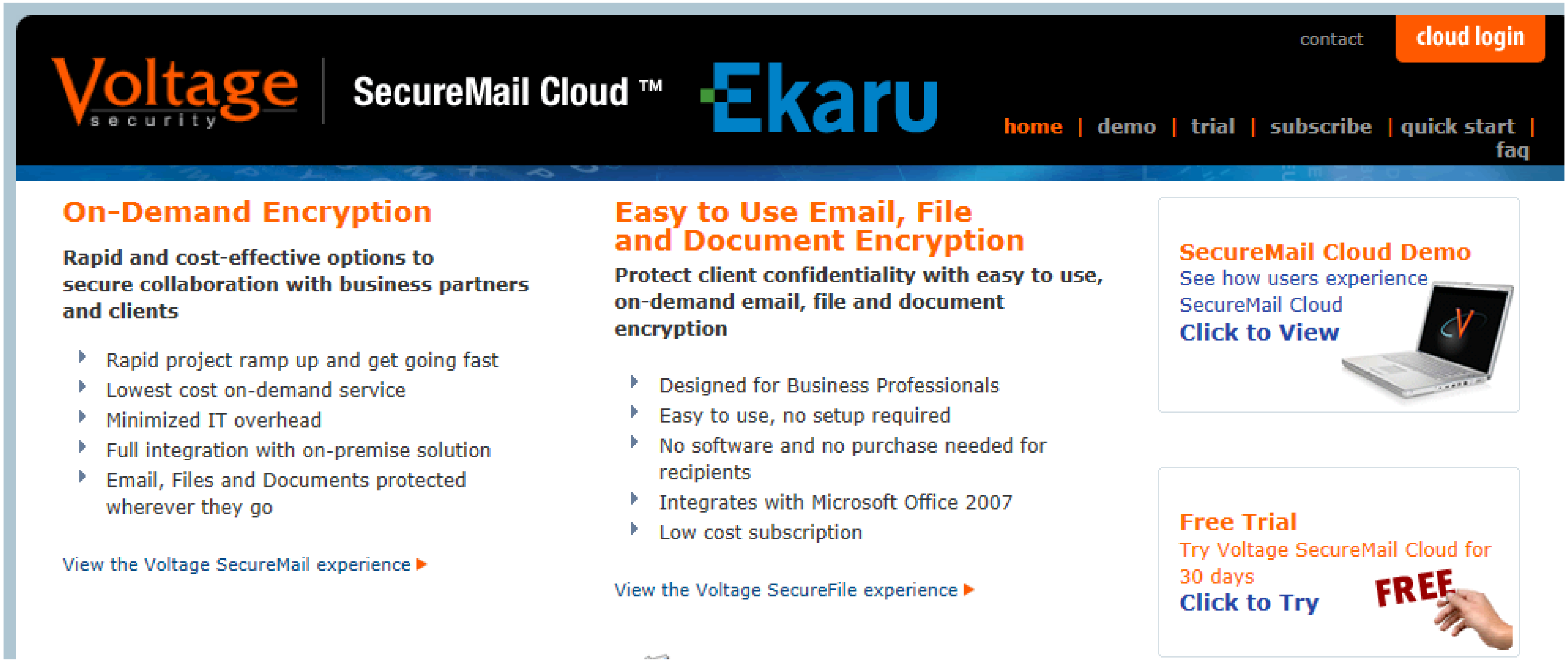
- **"Secure access control measures that:**
- (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;"

Technology requirement #3

- “(3)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.”
- *Do not email personal information. Instead use encrypted email or encrypted file transfer.*
- *Maintain wireless network encryption.*
- *WPA <u>NOT</u> WEP Encryption*
- *Password protection is NOT encryption!*

eMail Encryption

- Sign up for a free trial at http://voltage.ekaru.com/



On-Demand Encryption

Rapid and cost-effective options to secure collaboration with business partners and clients

- Rapid project ramp up and get going fast
- Lowest cost on-demand service
- Minimized IT overhead
- Full integration with on-premise solution
- Email, Files and Documents protected wherever they go

View the Voltage SecureMail experience ▸

Easy to Use Email, File and Document Encryption

Protect client confidentiality with easy to use, on-demand email, file and document encryption

- Designed for Business Professionals
- Easy to use, no setup required
- No software and no purchase needed for recipients
- Integrates with Microsoft Office 2007
- Low cost subscription

View the Voltage SecureFile experience ▸

SecureMail Cloud Demo
See how users experience SecureMail Cloud
Click to View

Free Trial
Try Voltage SecureMail Cloud for 30 days
Click to Try

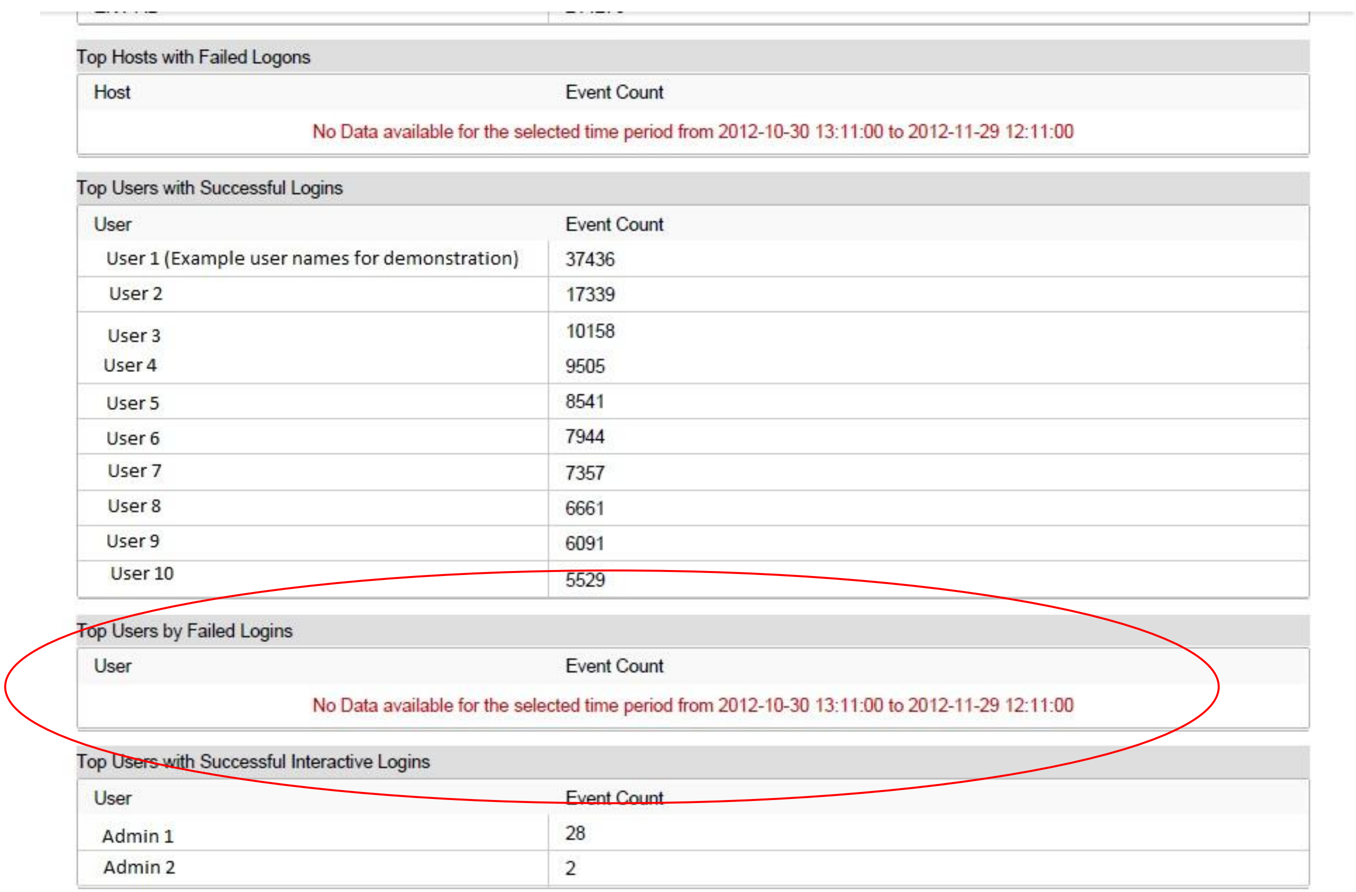
Technology requirement #4

- "Reasonable monitoring of systems, for unauthorized use of or access to personal information";

EventLog Analyzer

- Server logs can be checked for unauthorized access
- Reporting tools make review easier:

EventLog Analyzer



Top Hosts with Failed Logons

Host	Event Count
No Data available for the selected time period from 2012-10-30 13:11:00 to 2012-11-29 12:11:00	

Top Users with Successful Logins

User	Event Count
User 1 (Example user names for demonstration)	37436
User 2	17339
User 3	10158
User 4	9505
User 5	8541
User 6	7944
User 7	7357
User 8	6661
User 9	6091
User 10	5529

Top Users by Failed Logins

User	Event Count
No Data available for the selected time period from 2012-10-30 13:11:00 to 2012-11-29 12:11:00	

Top Users with Successful Interactive Logins

User	Event Count
Admin 1	28
Admin 2	2

Technology requirement #5

- "Encryption of all personal information stored on laptops or *other portable devices*;"*
- *We recommend TrueCrypt or PGP encryption to mount encrypted drives. We do not recommend full disk encryption. Education is needed to ensure users don't copy files to unencrypted areas.*

* *If technically feasible*

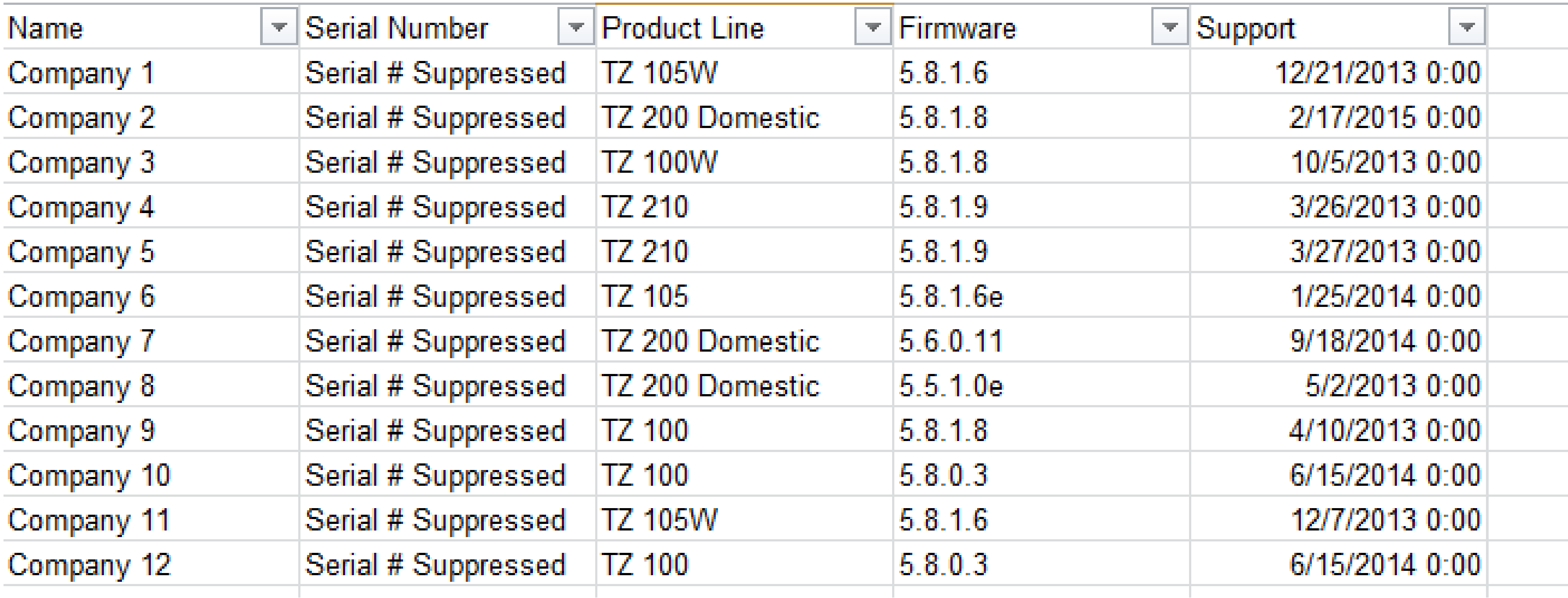
Technology Requirement #5

- Do all portable devices need to be encrypted? - YES – whenever technically feasible. Also, DVDs and flash drives should be encrypted.
- Laptops: PGP or Truecrypt – You MUST remember your encryption key!

Technology requirement #6

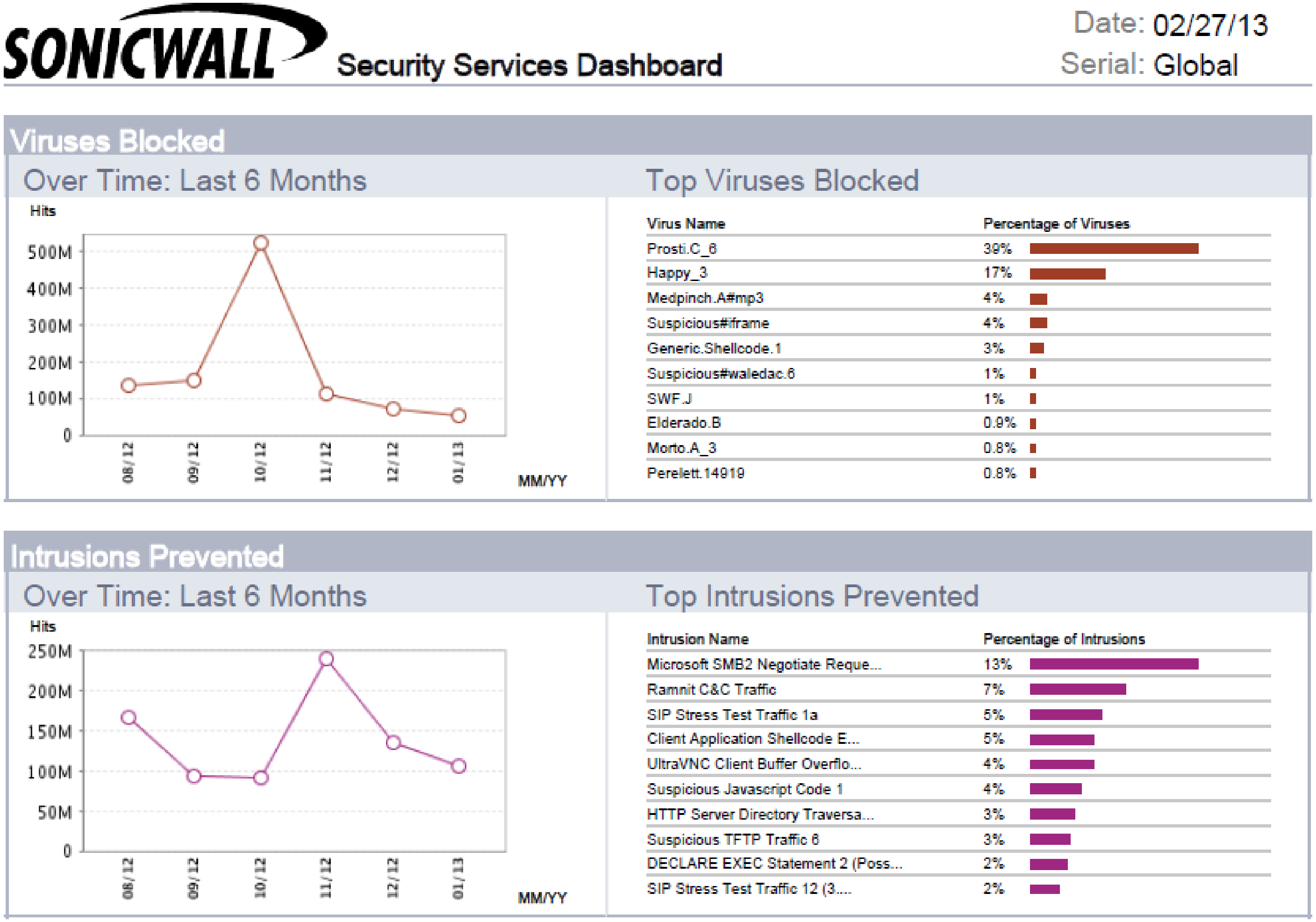
- "For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information."

Firewall / Firmware Updates



Name	Serial Number	Product Line	Firmware	Support
Company 1	Serial # Suppressed	TZ 105W	5.8.1.6	12/21/2013 0:00
Company 2	Serial # Suppressed	TZ 200 Domestic	5.8.1.8	2/17/2015 0:00
Company 3	Serial # Suppressed	TZ 100W	5.8.1.8	10/5/2013 0:00
Company 4	Serial # Suppressed	TZ 210	5.8.1.9	3/26/2013 0:00
Company 5	Serial # Suppressed	TZ 210	5.8.1.9	3/27/2013 0:00
Company 6	Serial # Suppressed	TZ 105	5.8.1.6e	1/25/2014 0:00
Company 7	Serial # Suppressed	TZ 200 Domestic	5.6.0.11	9/18/2014 0:00
Company 8	Serial # Suppressed	TZ 200 Domestic	5.5.1.0e	5/2/2013 0:00
Company 9	Serial # Suppressed	TZ 100	5.8.1.8	4/10/2013 0:00
Company 10	Serial # Suppressed	TZ 100	5.8.0.3	6/15/2014 0:00
Company 11	Serial # Suppressed	TZ 105W	5.8.1.6	12/7/2013 0:00
Company 12	Serial # Suppressed	TZ 100	5.8.0.3	6/15/2014 0:00

Perimeter – Intrusion Prevention



SONICWALL Security Services Dashboard

Date: 02/27/13
Serial: Global

Viruses Blocked

Over Time: Last 6 Months

Top Viruses Blocked

Virus Name	Percentage of Viruses
Prosti.C_6	39%
Happy_3	17%
Medpinch.A#mp3	4%
Suspicious#iframe	4%
Generic.Shellcode.1	3%
Suspicious#waledac.6	1%
SWF.J	1%
Elderado.B	0.9%
Morto.A_3	0.8%
Perelett.14919	0.8%

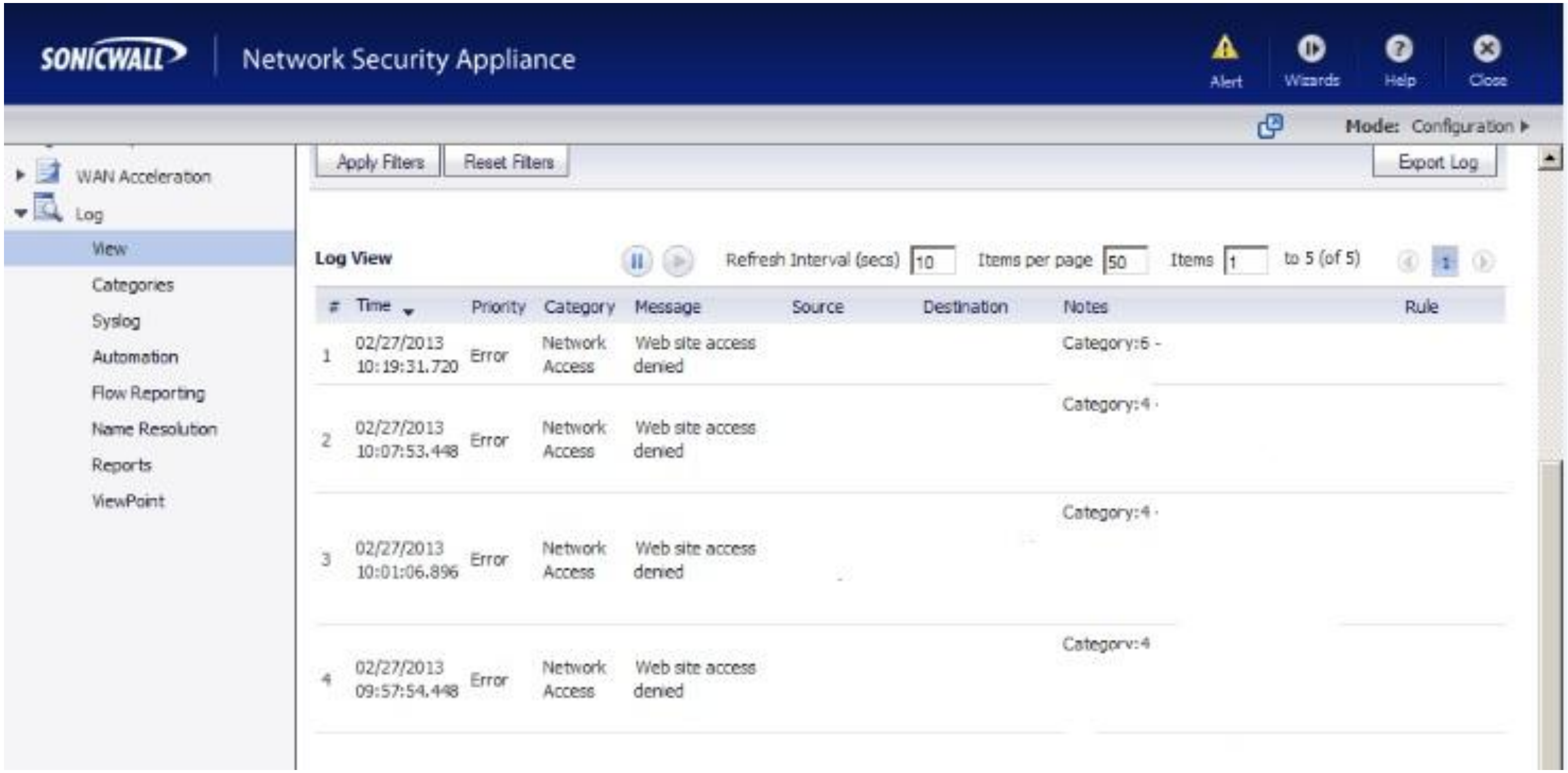
Intrusions Prevented

Over Time: Last 6 Months

Top Intrusions Prevented

Intrusion Name	Percentage of Intrusions
Microsoft SMB2 Negotiate Reque...	13%
Ramnit C&C Traffic	7%
SIP Stress Test Traffic 1a	5%
Client Application Shellcode E...	5%
UltraVNC Client Buffer Overflo...	4%
Suspicious Javascript Code 1	4%
HTTP Server Directory Traversa...	3%
Suspicious TFTP Traffic 6	3%
DECLARE EXEC Statement 2 (Poss...	2%
SIP Stress Test Traffic 12 (3....	2%

Perimeter Security



Log View

Refresh Interval (secs) 10 Items per page 50 Items 1 to 5 (of 5)

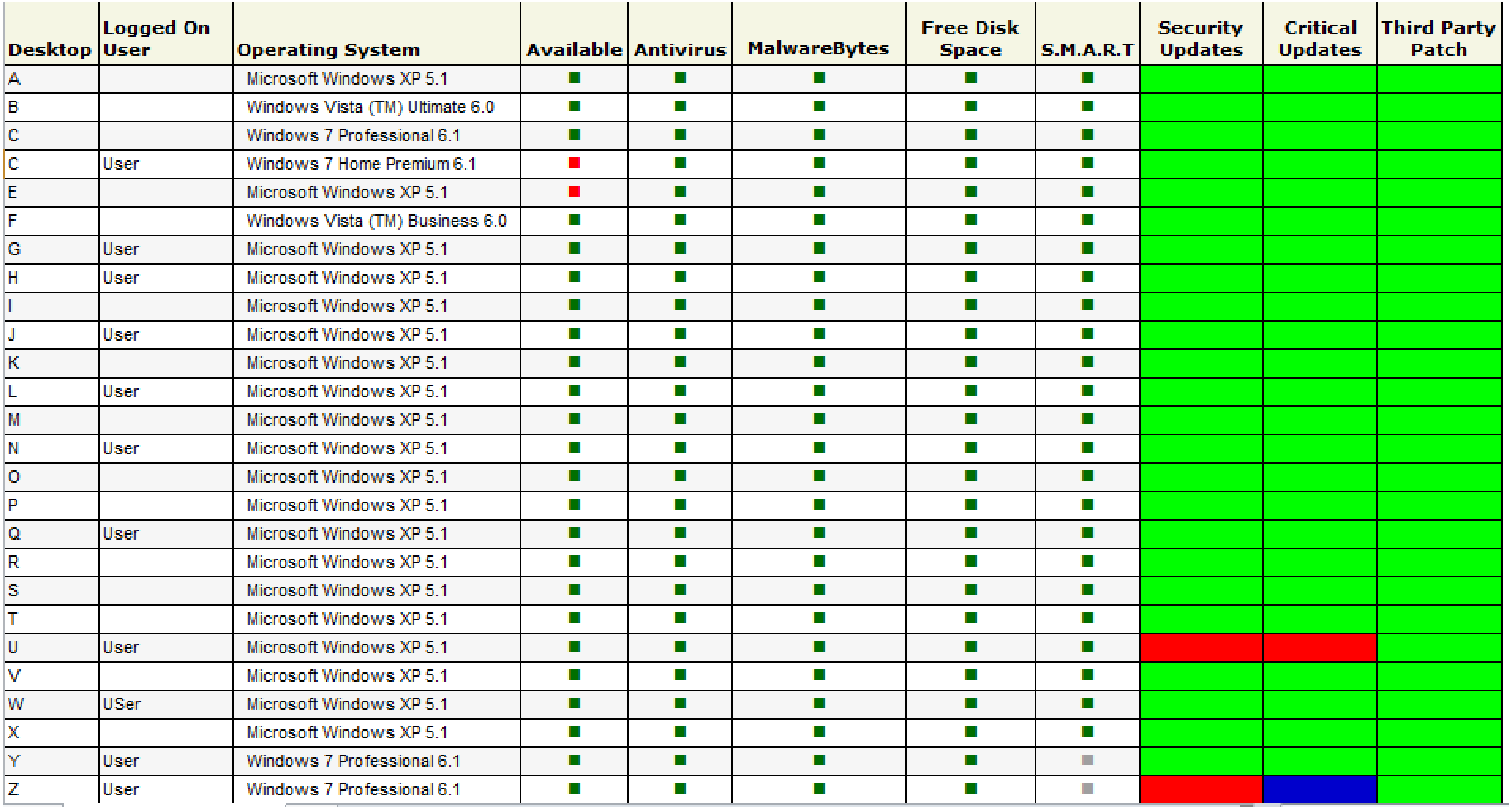
#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	02/27/2013 10:19:31.720	Error	Network Access	Web site access denied			Category:6 -	
2	02/27/2013 10:07:53.448	Error	Network Access	Web site access denied			Category:4 -	
3	02/27/2013 10:01:06.896	Error	Network Access	Web site access denied			Category:4 -	
4	02/27/2013 09:57:54.448	Error	Network Access	Web site access denied			Category:4	

Details removed for privacy

Technology requirement #7

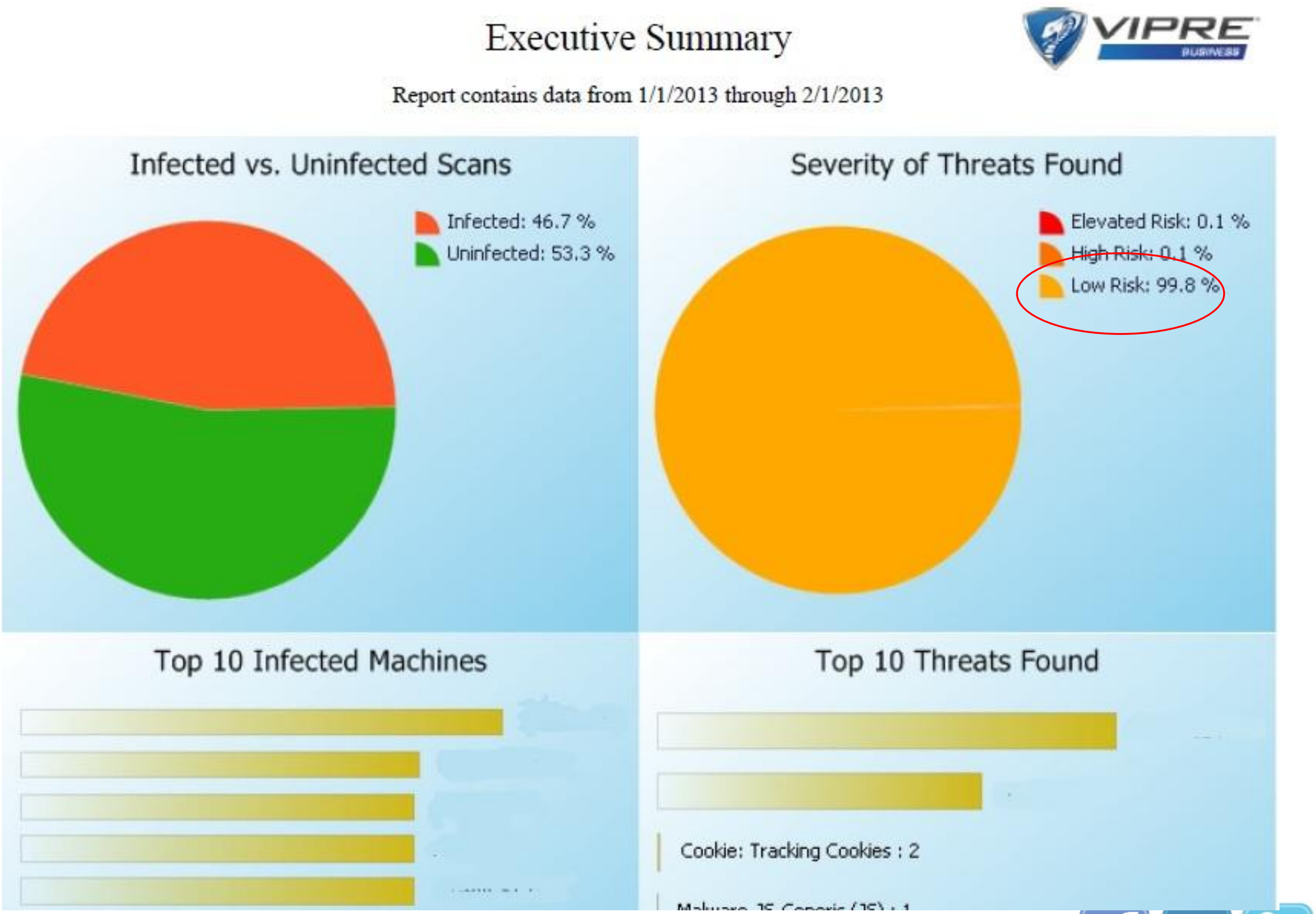
- ”Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.”

Managed Service



Desktop	Logged On User	Operating System	Available	Antivirus	MalwareBytes	Free Disk Space	S.M.A.R.T	Security Updates	Critical Updates	Third Party Patch
A		Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
B		Windows Vista (TM) Ultimate 6.0	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
C		Windows 7 Professional 6.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
C	User	Windows 7 Home Premium 6.1	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩
E		Microsoft Windows XP 5.1	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩
F		Windows Vista (TM) Business 6.0	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
G	User	Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
H	User	Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
I		Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
J	User	Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
K		Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L	User	Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
M		Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
N	User	Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
O		Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
P		Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Q	User	Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
R		Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
S		Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
T		Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
U	User	Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩
V		Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
W	USer	Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
X		Microsoft Windows XP 5.1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Y	User	Windows 7 Professional 6.1	🟩	🟩	🟩	🟩	⬜	🟩	🟩	🟩
Z	User	Windows 7 Professional 6.1	🟩	🟩	🟩	🟩	⬜	🟥	🟦	🟩

Antivirus Report



Executive Summary

Report contains data from 1/1/2013 through 2/1/2013

Infected vs. Uninfected Scans

- 🟥 Infected: 46.7 %
- 🟩 Uninfected: 53.3 %

Severity of Threats Found

- 🟥 Elevated Risk: 0.1 %
- 🟧 High Risk: 0.1 %
- 🟨 Low Risk: 99.8 %

Top 10 Infected Machines

Top 10 Threats Found

Cookie: Tracking Cookies : 2

Malware-JS-Generic (JS) : 1

Technology requirement #8

- “Education and training of employees on the proper use of the computer security system and the importance of personal information security.”
- *Users often break basic rules for “convenience”. Education is needed to prevent this.*
- Risk analysis is an <u>ongoing</u> process

Steps to Compliance – Phased Approach

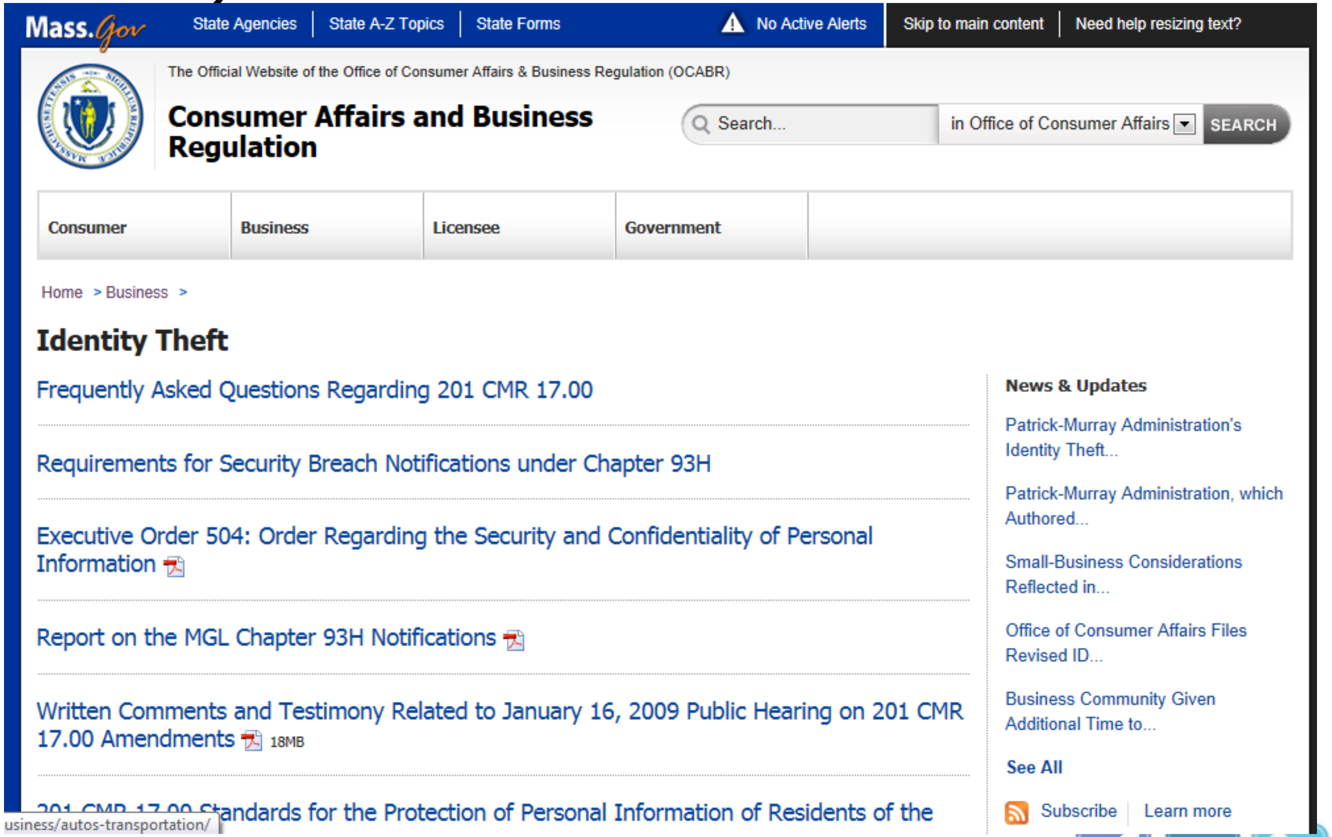
- Information audit – what data do you have and where is it?
- Review current security policies/procedures with respect to new requirements
- Identify areas for remediation
- Fix the weaknesses wherever technologically feasible
- WRITE IT DOWN! – Written Information Security Policy (WISP)

Comments:

- Note that the regulation uses language that is quite open: "reasonably secure", "to the extent technically feasible", and "reasonable monitoring". Most businesses with well-maintained infrastructure are likely to already be compliant in most areas.
- Based on experience, the most widely expected areas of current non-compliance are lack of "strong" passwords, and lack of encryption on laptops, and file transmission.
- Doesn't have to be expensive – OCR website is a bit intimidating – you are probably compliant already in most areas!
- Overall, do this because its good business practice – what would you do now if your laptop was lost or stolen?? How would you feel if someone intruded on your network and had access to all your critical files and data??

Resources

- Office of Consumer Affairs and Regulations (OCABR) web site



The Official Website of the Office of Consumer Affairs & Business Regulation (OCABR)

Consumer Affairs and Business Regulation

Identity Theft

Frequently Asked Questions Regarding 201 CMR 17.00

Requirements for Security Breach Notifications under Chapter 93H

Executive Order 504: Order Regarding the Security and Confidentiality of Personal Information

Report on the MGL Chapter 93H Notifications

Written Comments and Testimony Related to January 16, 2009 Public Hearing on 201 CMR 17.00 Amendments 18MB

201 CMR 17.00 Standards for the Protection of Personal Information of Residents of the

News & Updates

Patrick-Murray Administration's Identity Theft...

Patrick-Murray Administration, which Authored...

Small-Business Considerations Reflected in...

Office of Consumer Affairs Files Revised ID...

Business Community Given Additional Time to...

See All

Resources…

- Copy of 201 CMR 17.00
- Frequently Asked Questions

Q&A

Thank you for attending!

Call us any time with questions:

978-692-4200