Prepare your Business for 201 CMR 17.00

Standards for the protection of personal information of residents of the Commonwealth of Massachusetts

Bryley Systems Inc.

Business Technology Solutions   Since 1987

BRYLEY®

Presenters

Gavin Livingstone

- Founder and President of Bryley Systems Inc.
- Over 29 years business-technology experience
- Over 22 years at Bryley Systems
- MBA, Boston College

Paul Torchia

- Founder and President of ProsumerCorp Inc.
- Over 30 years business-process experience/consulting
- Over 7 years compliance/process work at Bryley
- MBA, Clark University

BRYLEY®

Agenda

Basics of 201 CMR 17.00

Define Personal Information

Why complying is important

Identify risk

Develop and maintain WISP

How Bryley can help

BRYLEY®

Basics of 201 CMR 17.00

Define Personal Information

Why complying is important

Identify risk

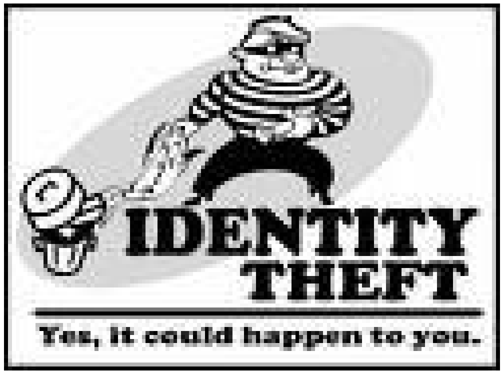
Develop and maintain WISP

How Bryley can help

BRYLEY®

Background

- Governor Deval Patrick signed legislation requiring companies to disclose data breaches to residents and the state
- Since then, more than 368 security breaches have been reported to the state
- Recently, 45.7 million credit and debit cards were exposed by TJX companies. Also, 4.5 million social security numbers and bank account numbers were exposed when an unencrypted backup tape from Mellon Bank was breached.



Related laws

- MGL 93H – Notify Attorney General and Office of Consumer Affairs and Business Regulation (OCABR) and affected residents of a security breach
- MGL 93I – Destroy hard copy and electronic Personal Information
- HIPAA – Health Insurance Portability and Accountability Act (health)
- Red Flags Rule (financial and credit firms)
- GLBA – Graham Leach Bliley Act (financial)
- Federal and state laws regulating document retention periods

BRYLEY®

Overview of 201 CMR 17.00

- Issued Sept. 22, 2008 by the Massachusetts OCABR to implement provisions of MGL 93H

- Effective date is now March 1, 2010 (several date changes)

- Establishes minimum standards to be met safeguarding privacy of Massachusetts residents

- Applies to anyone who owns or licenses Personal Information about a resident of Massachusetts

Annual cost of identity theft approaches $50 billion

BRYLEY®

Basics of 201 CMR 17.00

Define Personal Information

Why complying is important

Identify risk

Develop and maintain WISP

How Bryley can help

What is Personal Information?

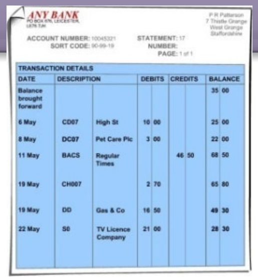
A Massachusetts resident's first and last name used in combination with any of the following items:

Social Security number

Driver's license number or state-issued ID card

Financial account number

Credit or Debit Card numbers (with or w/out access codes or passwords)



ANY BANK
PO BOX 876, LEICESTER,
LE76 7JH

P R Patterson
7 Thistle Grange
West Grange
Staffordshire

ACCOUNT NUMBER: 10045321
SORT CODE: 90-99-19

STATEMENT NUMBER: 17
PAGE: 1 of 1

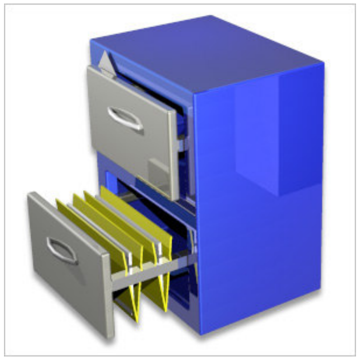
TRANSACTION DETAILS

DATE	DESCRIPTION		DEBITS		CREDITS		BALANCE	
Balance brought forward							35	00
6 May	CD07	High St	10	00			25	00
8 May	DC07	Pet Care Plc	3	00			22	00
11 May	BACS	Regular Times			46	50	68	50
19 May	CH007		2	70			65	80
19 May	DD	Gas & Co	16	50			49	30
22 May	S0	TV Licence Company	21	00			28	30

BRYLEY®

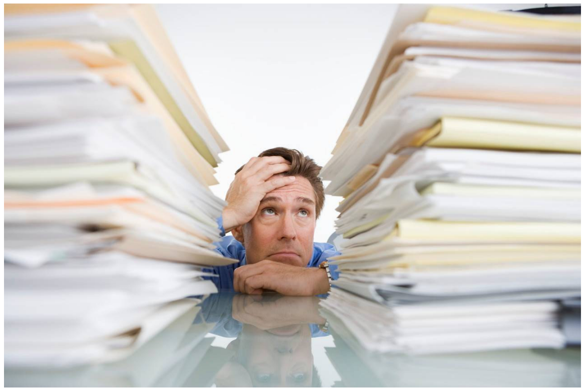
Records

- A record is any material which is written, drawn, spoken, visual, electromagnetic, or an image that is recorded or preserved, regardless of physical form or characteristics.



- A record can be either physical and non-physical

Some physical documents that contain Personal Information



- W2, W4, I9, and 1099 forms
- Direct-deposit authorization forms
- Photocopies of driver's licenses
- Applications for employment
- Insurance enrollment forms (Health, Dental, LTD, Life, etc.)
- Retirement-plan forms, documents, and data
- Payroll records and data
- Credit/debit card information

- Basics of 201 CMR 17.00
- Define Personal Information
- **Why complying is important**
- Identify risk
- Develop and maintain WISP
- How Bryley can help

BRYLEY®

How do security breaches occur?

- Copying and taking personal information offsite
- Opening email attachments and files from unknown sources
- Leaving passwords where they can be easily found (under keyboard, sticky notes on monitors, etc.)
- Leaving unencrypted notebooks where they can be taken (in a car or unattended in a public place, even if just for a moment)

Lack of awareness is a key contributor to security breaches.

BRYLEY®

201 CMR 17.00 penalties

- $5,000+ fine for delaying or failing to notify state authorities and residents affected by a security breach (MGL 93H)

- $5,000+ fine for failure to maintain a WISP (201 CMR 17.00)

- $100 fine per individual (up to $50k per incident) for failing to obtain written certification from 3rd party vendors (201 CMR 17.00)

- $100 fine per individual affected (up to $50k per incident) for improper disposal of personal information records (MGL 93I)

BRYLEY®

Basics of 201 CMR 17.00

Define Personal Information

Why complying is important

Identify risk

Develop and maintain WISP

How Bryley can help

Risk Analysis

A=Admin
P=Physical
T=Technical
	Description of Risk	Mitigation Plan	Business Impact	High impact
				Medium impact
				Low impact

A	Limit PI access to those who require it for business purposes	Written plan for access & usage of PI. Employee training for same	Time & cost to identify areas where PI resides and assess risk & policy implementation	High
P	Limit PI access to those who require it for business purposes	Locks on file cabinets, limited personnel w/keys	New & changing locks, & key issue & return	Low
T	Limit PI access to those who require it for business purposes	Password protected files & directories	Password policy & implementation	Low
T	Limit PI access to those who require it for business purposes	Data encryption for hard drives, portable media & wireless	Implement & train staff on use of encryption technologies	Medium

Your business risk

Compliance criteria

- Size, scope, and nature of business
- Types of records maintained
- Amount of resources available to the organization
- Amount of stored Personal Information
- Need for security and confidentiality of consumer and employee information
- Risk of identity theft posed by operations

Put it into context

Basics of 201 CMR 17.00

Define Personal Information

Why complying is important

Identify risk

Develop and maintain WISP

How Bryley can help

Written Information Security Plan (WISP)

Using risk analysis, write the WISP Program Plan:

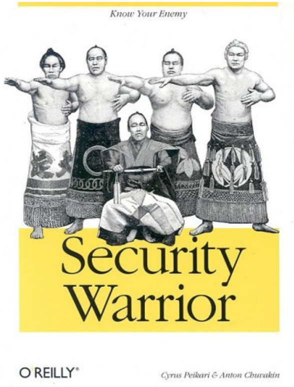
Administrative

Physical

Technical

WISP – Administrative

- Designate Security Manager to maintain the WISP
- Identify and assess internal and external risks
- Develop security policies and procedures
- Create employee awareness of Personal Information and how it should be handled
- Update employee manual, forms, and agreements

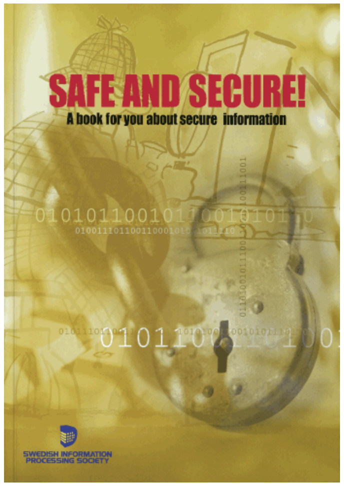


WISP – Administrative

- Impose disciplinary measures for violations
- Prevent terminated employees from accessing records
- Verify third-party service providers have their own WISP
- Limit the amount of Personal Information collected and retained within the organization

WISP – Administrative

- Review status against the WISP (at least annually)
- Document any actions taken involving breach-of-security incidents
- Mandate post-incident reviews of events and actions taken, resulting in changes to business policies and/or practices


SAFE AND SECURE!
A book for you about secure information
SWEDISH INFORMATION PROCESSING SOCIETY

WISP – Administrative

- Periodically monitor WISP, which helps to prevent unauthorized access and usage of Personal Information

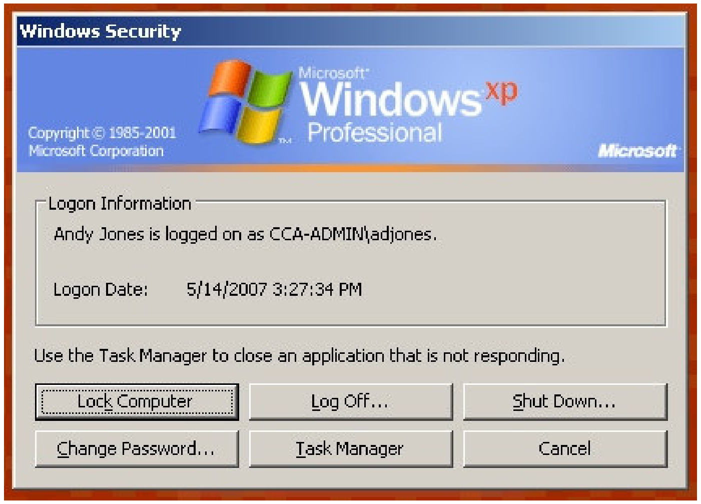
- Educate and train employees on the importance of securing Personal Information, both physically and electronically

WISP – Physical

- Identify all paper-based Personal Information and its locations
- Restrict physical access to these records
- Maintain secure storage and disposal
- Lock-down vulnerable equipment

WISP – Technical

- Deploy secure user-authentication protocols:
  - Active Directory
  - Strong passwords
- Perform other security measures:
  - Configure security settings (IE)
  - Disable file sharing on endpoints
  - Screen-lock computer when away
  - Logout or restart systems at end of day
  - Encrypt vulnerable data



Windows Security

Copyright © 1985-2001 Microsoft Corporation

Logon Information

Andy Jones is logged on as CCA-ADMIN\adjones.

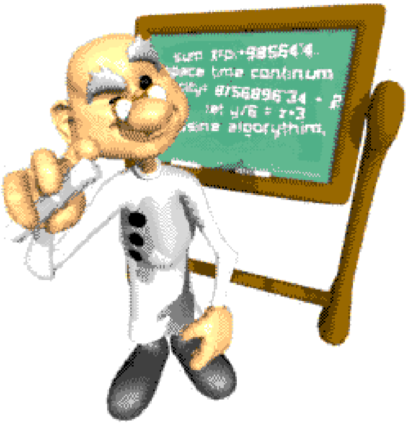
Logon Date: 5/14/2007 3:27:34 PM

Use the Task Manager to close an application that is not responding.

WISP – Technical

Encryption

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text* ; encrypted data is referred to as *cipher text*.



BRYLEY®

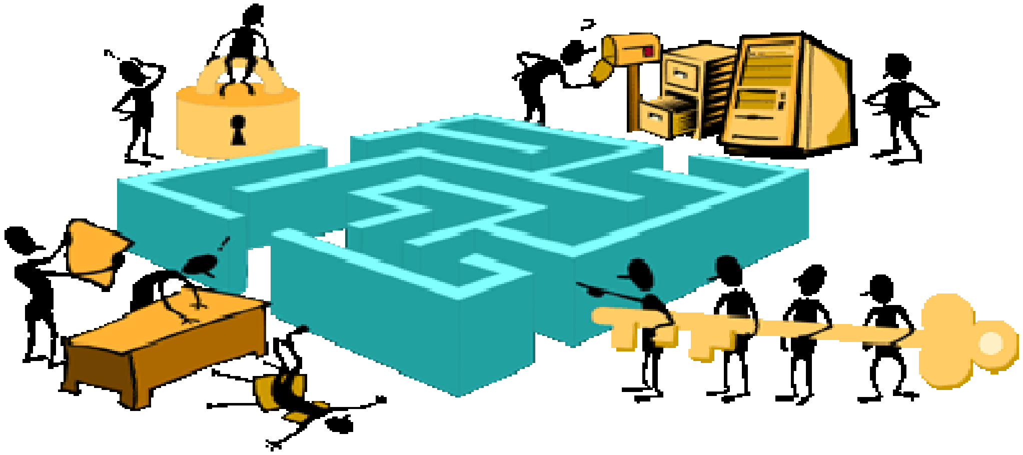
WISP – Technical

By 3/1/2010, encrypt all Personal Information:

- Transmitted over the public networks
- Transmitted wirelessly
- Stored on laptops
- Stored on mobile and other portable devices

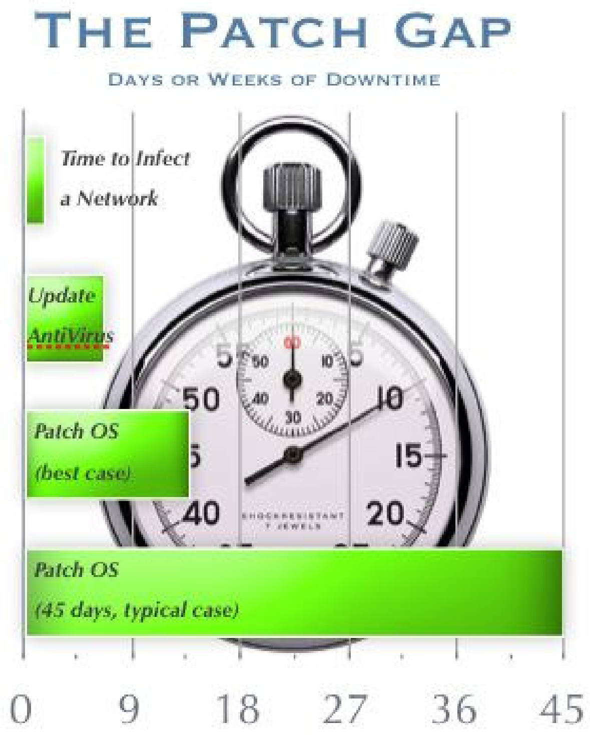
WISP – Technical

- Deploy current firewall protection and operating-system security patches
- Deploy current versions of system-security software (anti-virus, anti-spyware, anti-malware, anti-spam, etc.)
- Perform ongoing patches, updates, and scheduled scans
- Monitor updating and scanning processes



WISP – Technical

- Subscribe to a Managed Technology service (like those from Bryley Systems)
- Deploy agent software for patching, updates, and monitoring
- Review management reports proactively



BRYLEY®

WISP – Technical

Data Backup

- Complete daily backups of server(s)
- Encrypt data on backup tapes and drives
- Lock-up physical backup media
- Store both onsite and offsite

BRYLEY®

Basics of 201 CMR 17.00

Define Personal Information

Why complying is important

Identify risk

Develop and maintain WISP

How Bryley can help

Bryley Systems Inc.

- Bryley Systems has been providing Business Technology Solutions as a trusted business partner since 1987.
- We've made significant Managed-Technology investments in patching and monitoring, Backup/Disaster Recovery, and network security.
- We focus on continuous improvement of services to our clients.

Performance, Reliability, Security, and Compliance!

BRYLEY®

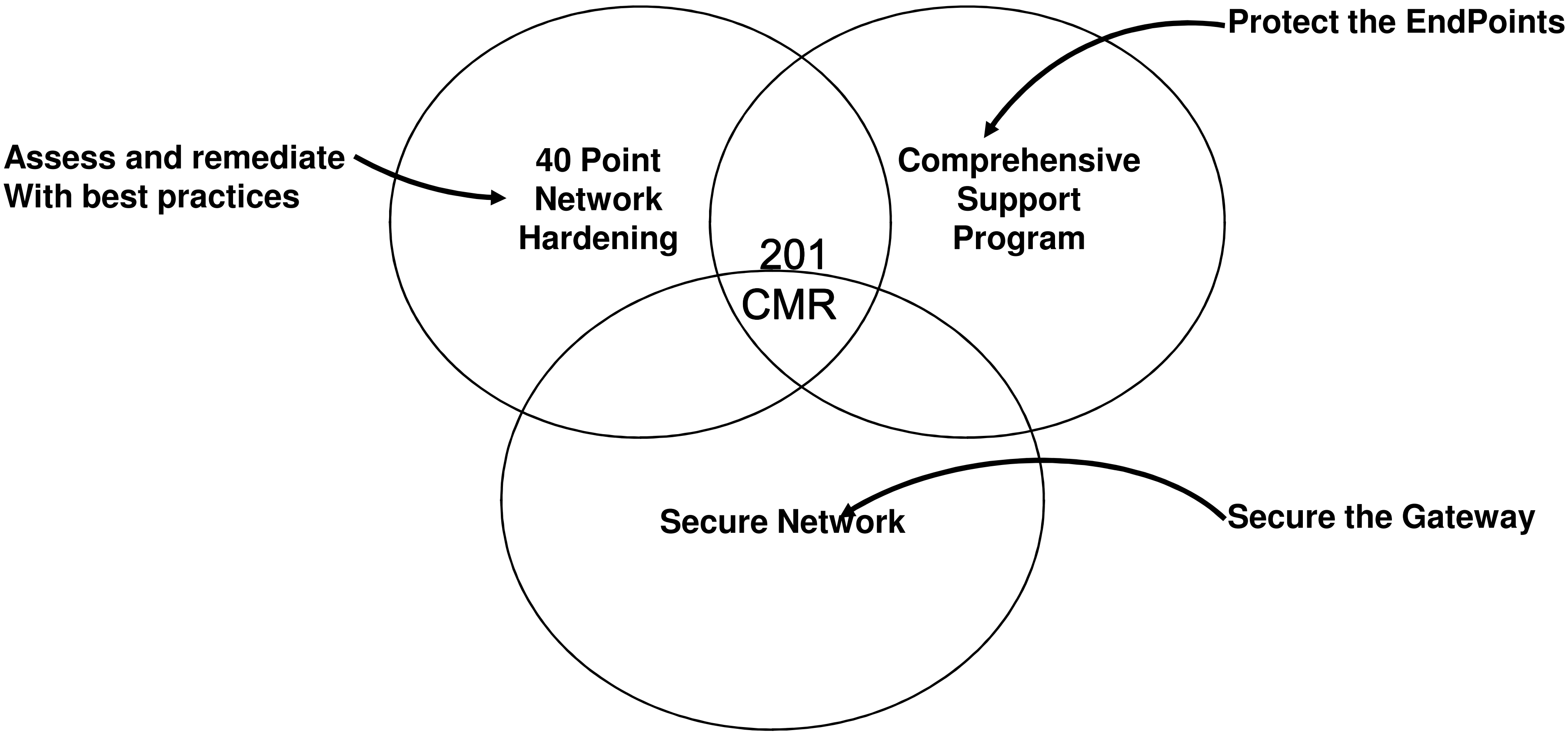
Our approach

1. Start with an assessment/analysis of risk:
    - Administrative
    - Physical
    - Technical
2. Follow-up with recommendations:
    - 40 Point Assurance
    - Encryption
    - Security settings
3. Deploy solutions:
    - Projects
    - Managed Technology Services

Balancing act of cost versus compliance

BRYLEY®

Our approach (continued)



Security, performance, reliability

Managed Technology Services

- BU/DR ™ (Backup/Disaster Recovery)
- Compliance Patching and Monitoring™
- Comprehensive Support Program™
- First-Priority Response™
- HushMail (email encryption)
- Secure Network™ (gateway hardening)
- SpamSoap

Tuned to your specific needs & budget

BRYLEY®

Projects

- WISP Consulting
- 40 Point Assurance™ (201 CMR 17.00 review)
- Wireless-network lockdown
- Computer-network deployment
- Firewall configuration and setup
- Malware elimination and remediation
- Email, laptops, and portable device encryption
- Telephone systems and unified communications

Tuned to your specific needs & budget

BRYLEY®

Questions and Answers

Downloads

Downloads found on the Office of Consumer Affairs & Business Regulation (OCABR) Web site under “For Business – Identity Theft”

- Written Information Security Program template:

http://www.mass.gov/Eoca/docs/idtheft/sec_plan_smallbiz_guide.pdf

- 201 CMR 17.00 Compliance Checklist:

http://www.mass.gov/Eoca/docs/idtheft/compliance_checklist.pdf

- 201 CMR 17.00 regulations

www.mass.gov/oca

BRYLEY®