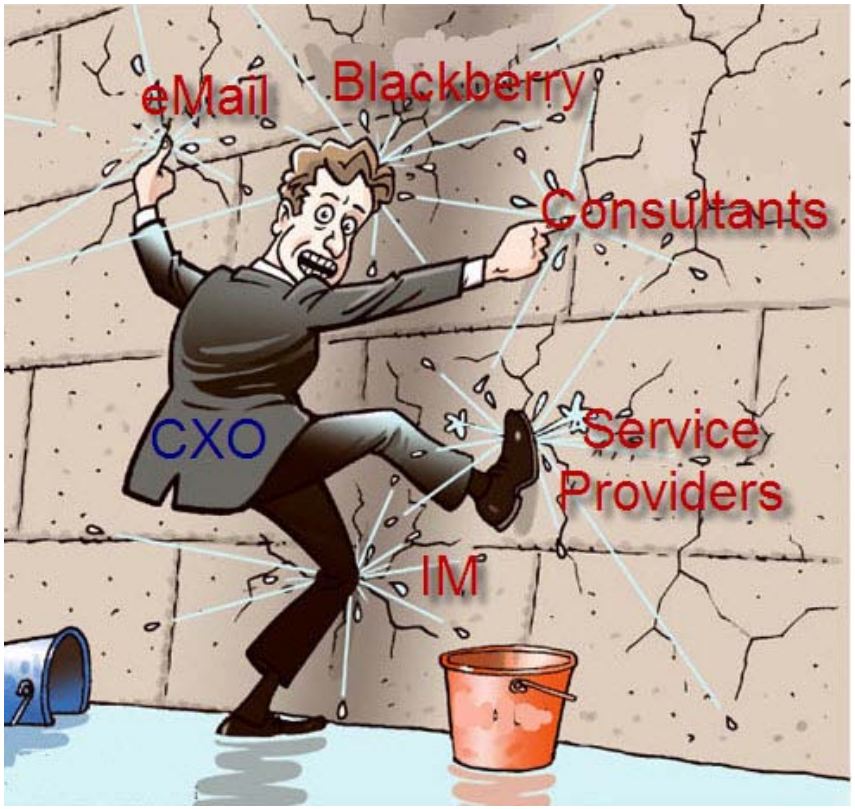
John Verry, CCSE/CISA/270001-CLA

PROTECTING YOUR CRITICAL DATA

PIVOT POINT SECURITY
Hamilton Square, NJ

Specialists in Security Assessments, Penetration Testing,
& Security Information Event Management

Why You're Here

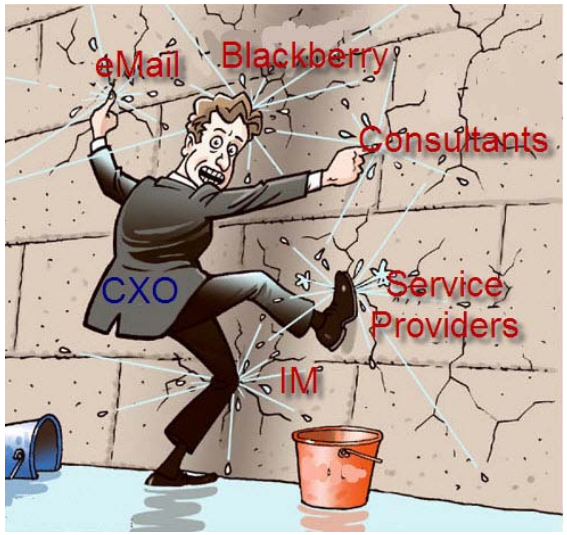


You have run out of appendages !

- **Ever increasing regulation**
  - 44+ State PII Provisions
  - Federal Red Flag Provisions
  - HIPAA has new teeth (post Piedmont & HITECH ACT)
  - Sarbanes
  - PCI DSS
  - NERC
  - What's next ??

PROTECTING YOUR CRITICAL DATA

Why You're Here



You have run out of appendages!

- **Ever increasing threat (& impact)**
  - Cloud Computing
  - US CoC 20M tele-employees
  - USTR $250 Billion/year in Trade Secret Theft (espionage)
    - Goldman Sachs (32MB trading code)
  - 1/400 email messages contain confidential information
  - $202/name lost per Ponemon
- **Ever increasing communication modalities**
  - Email, IM, Twitter, Blogs, Extranet

What We Are All Hoping for …

Divine Intervention

… or …

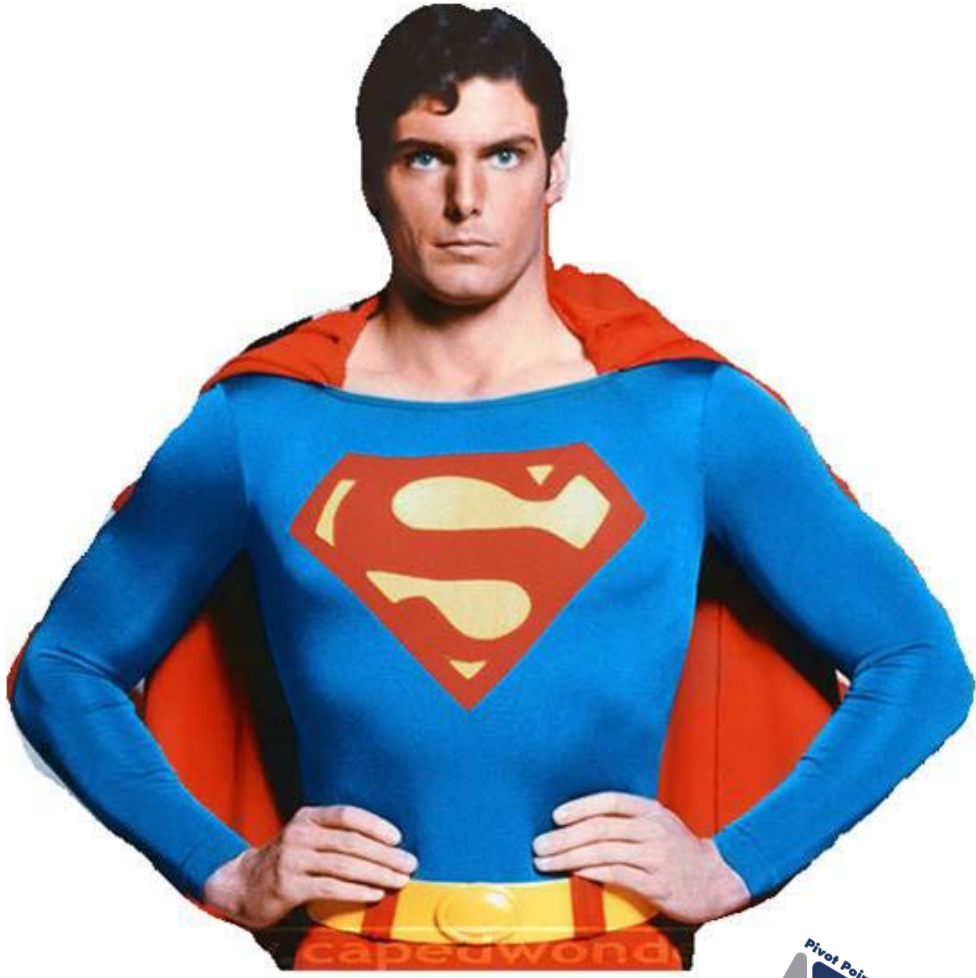
What We Are All Hoping for …

Divine Intervention

… or …

Data Loss Prevention Super Powers

(able to clear tall compliance requirements in a single bound …)



Getting Realistic …

Superman has kryptonite & Were Wolves have silver bullets

No "Silver Bullet" for Data Protection

- Business objectives, sources, regulations, threats, and conduits are too diverse and continually evolving

"Point" Solutions are great but implemented non-holistically are vulnerable to

- Coverage gaps
- Process Gaps
- Monitoring Gaps
- **People !!!**

You Need a Road Map…

to know

WHICH point solutions,

in WHAT order,

with WHAT supporting

policies, standards,

and procedures …

PROTECTING YOUR CRITICAL DATA

Develop an Understanding …

Understand what information needs special treatment (employee, client intellectual property, Credit Cards, financial information, medical information)

Understand what the risk scenarios and business impact are, for example:

- Legal, brand impact, mitigation costs relating to malicious exposure of info violating compliance with PII (@ $202 /name)
- Non-Technical risks are often overlooked (e.g., Choice Point)

Develop an Understanding …

Evaluate existing controls and identify where residual risk has unacceptable business impact:

- Data at rest (databases, files, local machines, file servers, **transit points, printed documents, business partners, DR sites**)
- Data in transit (intranet, extranet, internet) via IM, FTP, email, HTTP, HTTPS, etc.
- Data on endpoints (laptops, USB hard drives, PDA's, **printers/copiers**)

Understanding Risk/Control "Gaps" Yields a Roadmap

- Determine (and preferably document) the control treatments required for each "unacceptable risk"
- Prioritize based on risk with consideration of cost, implementation ease/cost, etc. *(consider AS-NZS 4360)*
- Align your efforts with existing Information technology Control Frameworks (e.g., COBIT, ITIL) and or with prevailing good security (e.g., OWASP, SO-17799)

	Consequences		
Likelihood	**Major**	**Moderate**	**Minor**
Likely	Red	Red	Amber
Possible	Red	Amber	Green
Unlikely	Amber	Green	Green

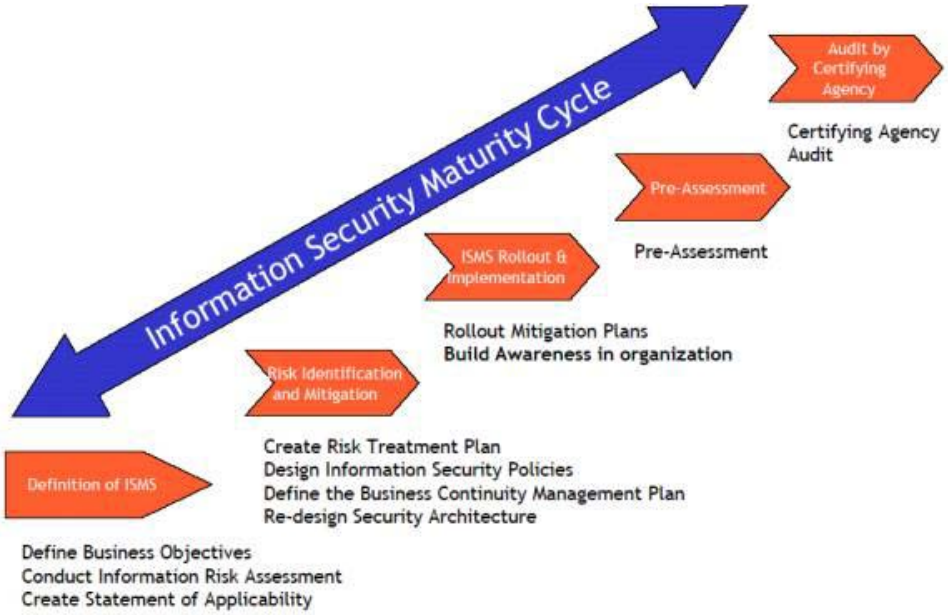
Risk Treatment Key

Red	Immediate action
Amber	Heightened action
Green	Business as usual

Sounds painful .. (but there's)

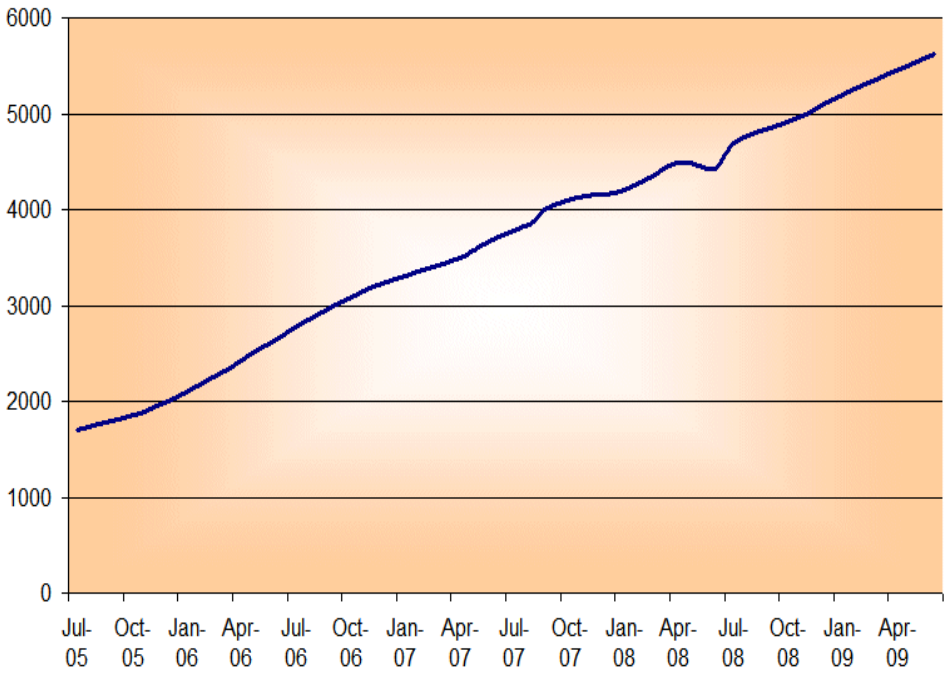
You're well on your way to 27001

- ISO-27001 is rapidly becoming the de-facto standard for Information Security attestation
  - 27001 provides guidelines and principles for **initiating, implementing,** maintaining, and improving Information Security



You're well on your way to 27001

- Accelerating adoption rate 5K+ in last few years



27001 Benefits: CXO's Perspective

It is a certifiable **standard**

- You can **prove** you're secure to a known set of criteria

It simplifies Information Security into an

- Overarching process (27001)
- Collection of good practices to use (27002)

Certificate

ISO/IEC 27001:2005

www.tuv.com
TÜVRheinland
ID 9105049524

The Certification Body for Information Security Management Systems of the TÜV Rheinland Cert GmbH, hereby certifies that the organisation

Global Analytics India Pvt. Ltd.
Pacifica Tech Park, 101 A First floor,
23 Old Mahabalipuram Road, Navallur
Chennai 603103 - India

has implemented and applies a management system for information security for the scope

Analytic solutions and related software development for Banking, Finance, Consulting and HR domains.
Statement of Applicability: GAI - D – 03 Ver 1.1 dated 2008-11-27

As a result of audit, report no. 1403005570-2, it was established that the requirements according to the international standard

ISO/IEC 27001
Information technology – Security techniques - Information security management systems - Requirements

have been satisfied with respect to documentation and efficacious implementation.

This certificate is valid until 2012-02-02.

Certificate No. 01 153 11006

Cologne, 2009-02-03

Certification Body of the
TÜV Rheinland Cert GmbH
Am Grauen Stein - 51105 Cologne - Germany

Certification of Management Systems

IAF
TGA-ZM-58-95-20

TÜVRheinland®

27001 Benefits: CXO's Perspective

27001 simplifies communication with management and partners

27001 is applicable to all risks and all compliance requirements

27001 can be harmonized with COBIT, ITIL, OWASP, OSTMM, NIST

Certificate

ISO/IEC 27001:2005

The Certification Body for Information Security Management Systems of the TÜV Rheinland Cert GmbH, hereby certifies that the organisation

Global Analytics India Pvt. Ltd.
Pacifica Tech Park, 101 A First floor,
23 Old Mahabalipuram Road, Navallur
Chennai 603103 - India

has implemented and applies a management system for information security for the scope

Analytic solutions and related software development for Banking, Finance, Consulting and HR domains.
Statement of Applicability: GAI - D – 03 Ver 1.1 dated 2008-11-27

As a result of audit, report no. 1403005570-2, it was established that the requirements according to the international standard

ISO/IEC 27001
Information technology – Security techniques -
Information security management systems - Requirements

have been satisfied with respect to documentation and efficacious implementation.

This certificate is valid until 2012-02-02.

Certificate No. 01 153 11006

Cologne, 2009-02-03

Certification Body of the
TÜV Rheinland Cert GmbH
Am Grauen Stein - 51105 Cologne - Germany

Certification of Management Systems

TÜVRheinland®

Health Care Specific

"Audit Trails for Electronic Health Records" (ISO 27789) coming late 2009

Increased guidance around 27001/27002 for HIPAA (HITECH) (pre/post Assessments should identify vulnerabilities in the application as well as controls where data resides as part of the application's processing (database servers, communication protocols(s), web access, etc.)

Health Care Specific

10	(a)(2)(iv) Data Backup and Storage (addressable)	**HIPAA > ISO**	*ISO 8.4.1 Information Back-up*
	164.312 Technical Safeguards		
	(a)(1) Access Control		*ISO 9 Access Control.*
1	(a)(2)(i) Unique User Identification (required)	**HIPAA > ISO**	*ISO 9.2.1 User Registration* *ISO 9.5.3 User Identification and Authorization*
2	(a)(2)(ii) Emergency Access Procedure (required)	**HIPAA > ISO**	
3	(a)(2)(iii) Automatic Logoff (addressable)	**ISO ~ HIPAA**	*ISO 9.5.7 Terminal Time-Out*
4	(a)(2)(iv) Encryption and Decryption (addressable)	**ISO > HIPAA**	*ISO 10.3.2 Encryption* *ISO 10.3 Cryptographic Controls*
5	**(b) Audit Controls (required)**	**ISO > HIPAA**	*ISO 9.7 Monitoring System Use and Access*
	(c)(1) Integrity		
6	(c)(2) Mechanism to Authenticate Electronic Protected Health Information (addressable)	**ISO ~ HIPAA**	*ISO 10.2.2 Checks and Controls* *ISO 10.3.3 Digital Signatures*
7	**(d) Person or Entity Authentication (required)**	**ISO > HIPAA**	*ISO 9.5.3 User Identification and Authentication* *ISO 9.5.4 Password Management System*

Summary

Organizations spend more money and gain less assurance than desired with a point solution (non-holistic) approach

27001(2) provides a structured approach proven over 10+ years across thousands of organizations

Getting started with 27001 can be simple as it is largely comprised of activities you are familiar with

27001 augments your organization's other ERM activities

Any questions – **John.Verry@PivotPointSecurity.com**