Helping Government and Education with Security and Compliance

Background

zSecure's role

In the battle for information security, the public sector is **more vulnerable** and **more of a target.**

Over 50% of data security breaches reported since 2005 were through state and local government and educational institutions.

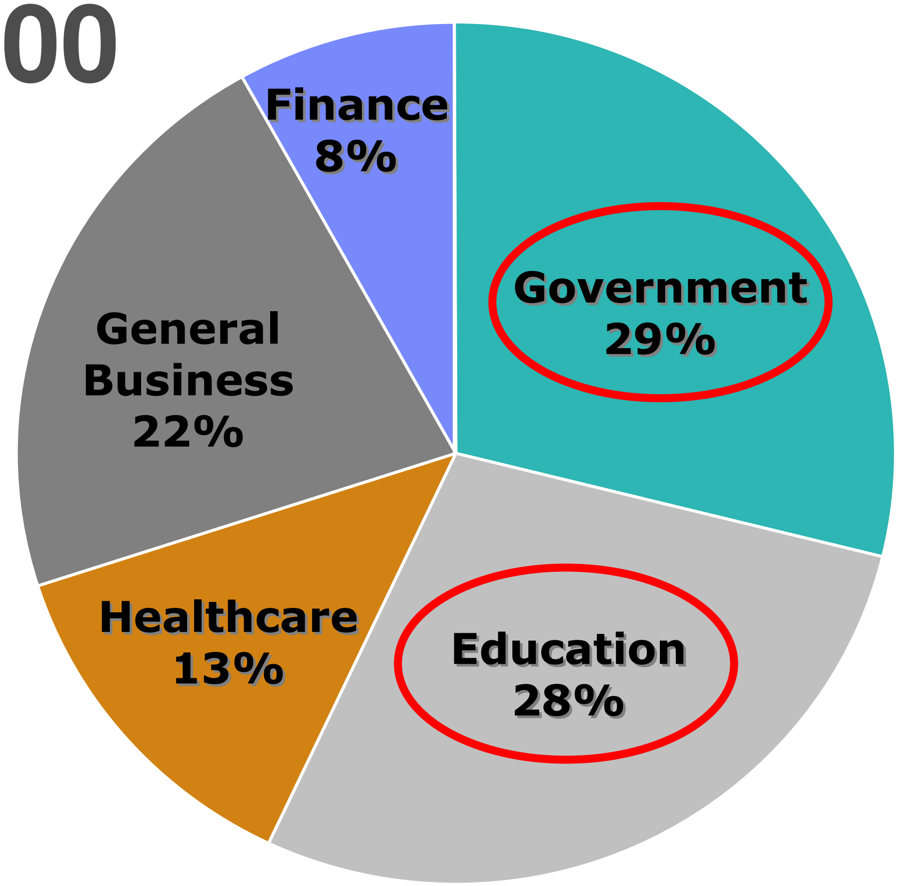
Security is constantly number one or two on NASCIO's priority list for strategies, management processes and solutions.

Bearing Point; National Association of State Chief Information Officers

2006.

More than 300 breaches.

More than **20 million** people.



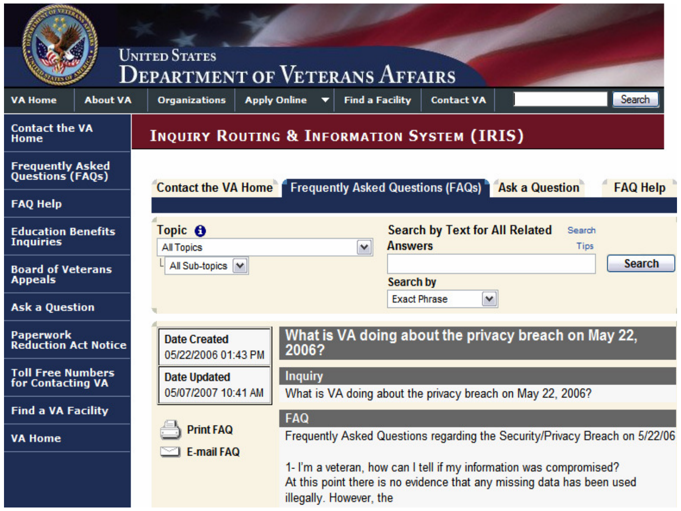
Between January 2003 and August 2004 the Commonwealth of Pennsylvania experienced cyber attacks that resulted in the following business impacts:

Millions in revenue lost due to interruptions in government operations

Hundreds of hours in productivity lost due to resource reallocation to address security vulnerabilities and system outages

The inability to use technology to address these types of attacks because of disparate and non-aligned technology solutions and insufficient enterprise-wide standardization and planning

In May 2006 personal records of 26.5 million veterans were compromised


United States
Department of Veterans Affairs
VA Home
About VA
Organizations
Apply Online
Find a Facility
Contact VA
Search
Contact the VA Home
Frequently Asked Questions (FAQs)
FAQ Help
Education Benefits Inquiries
Board of Veterans Appeals
Ask a Question
Paperwork Reduction Act Notice
Toll Free Numbers for Contacting VA
Find a VA Facility
VA Home
Inquiry Routing & Information System (IRIS)
Contact the VA Home
Frequently Asked Questions (FAQs)
Ask a Question
FAQ Help
Search Tips
Search
Print FAQ
E-mail FAQ

Topic: All Topics
All Sub-topics

Search by Text for All Related Answers

Search by: Exact Phrase

Date Created
05/22/2006 01:43 PM

Date Updated
05/07/2007 10:41 AM

What is VA doing about the privacy breach on May 22, 2006?

Inquiry

What is VA doing about the privacy breach on May 22, 2006?

FAQ

Frequently Asked Questions regarding the Security/Privacy Breach on 5/22/06

1- I'm a veteran, how can I tell if my information was compromised?
At this point there is no evidence that any missing data has been used illegally. However, the

An employee routinely took records home – and the laptop was stolen

Senior management remained unaware for two weeks

$2000 theft may cost $100M to remedy

Washington Post 08/06

July 2007.

A ten day period.

Reported.

Yuba County Health and Human Services

A laptop stolen from a building contained personally identifiable information of individuals whose cases were opened before May 2001. The laptop was being used as a backup system for the county's computer system. The data include Social Security Numbers, birth dates, driver's license numbers and other private information.

Flexible Benefits Administrators, Virginia Beach

A former employee allegedly stole Virginia Beach city and school district employees' personal information and used it to commit prescription fraud. Police discovered a list of names and Social Security Numbers at the employees home

USMC/Penn State

Names and Social Security Numbers of Marines were found through Google Internet search engine

Hidalgo County Commissioner's Office

The private medical information, including Social Security Numbers and treatment details of people who sought medical assistance from the county was posted on the Hidalgo County website.

St Vincent Hospital, Indianapolis

A security lapse compromised names, addresses and Social Security Numbers.

University of Michigan

University databases were hacked. Names, addresses, Social Security Numbers, birth dates, and in some cases, the school districts where former students were teaching were exposed.

Jackson Local Schools, Ohio

The Social Security Numbers of present and former Jackson Local Schools' employees were at risk of public access on a county maintained Web site.

Connecticut General Assembly Transportation Committee

Social Security Numbers of former employees of defunct L.G. Defelice Inc. posted on CT transportation committee website.

Objective – don’t be “that guy”.

GLBA / PCI

Wells Fargo
Lost server caused first $M notice cost

DSW
Wireless attack $6.5m reserve on 10K records

Privacy

TJX
45m stolen customer records

Choice Point
$10 million FTC fine

SOX

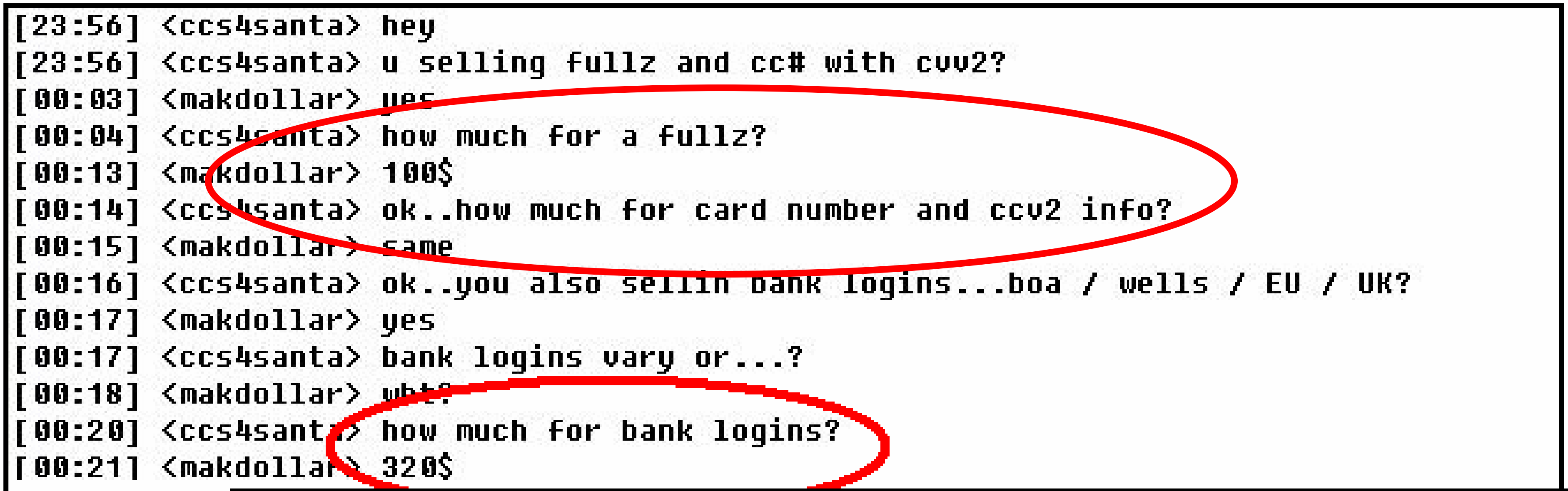
ALL
Poor planning wastes $M

X REIT
Could not complete a planned merger because of poor controls

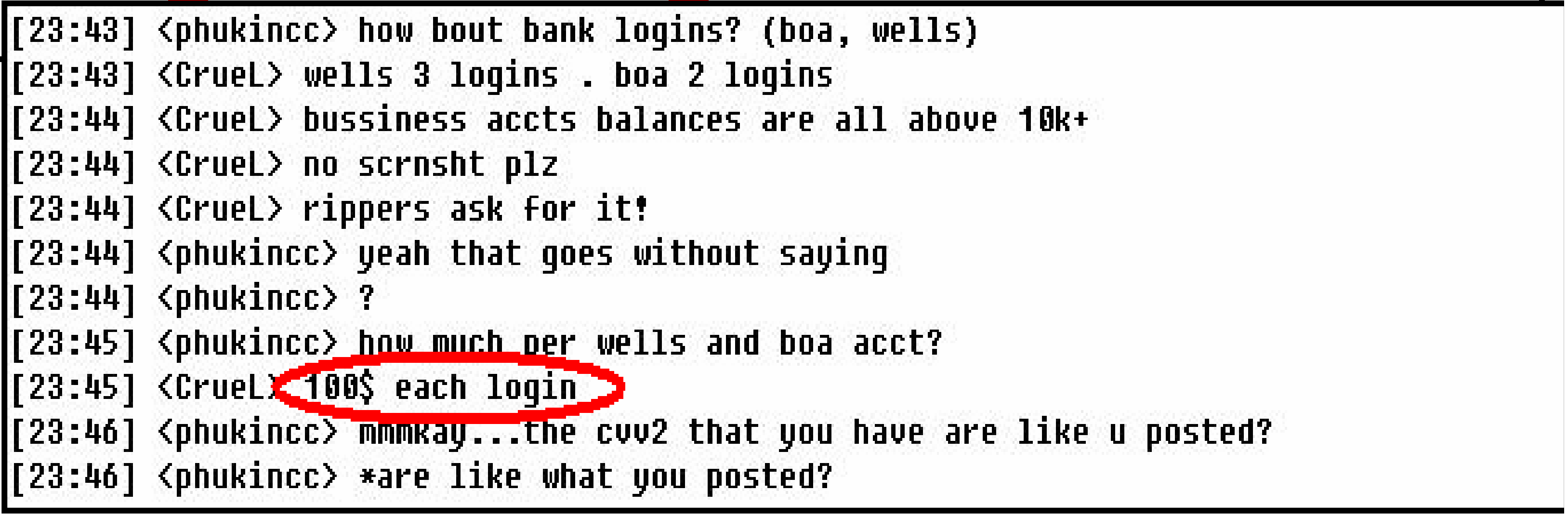
e-discovery

Intel
Failure to produce email and other records => fine

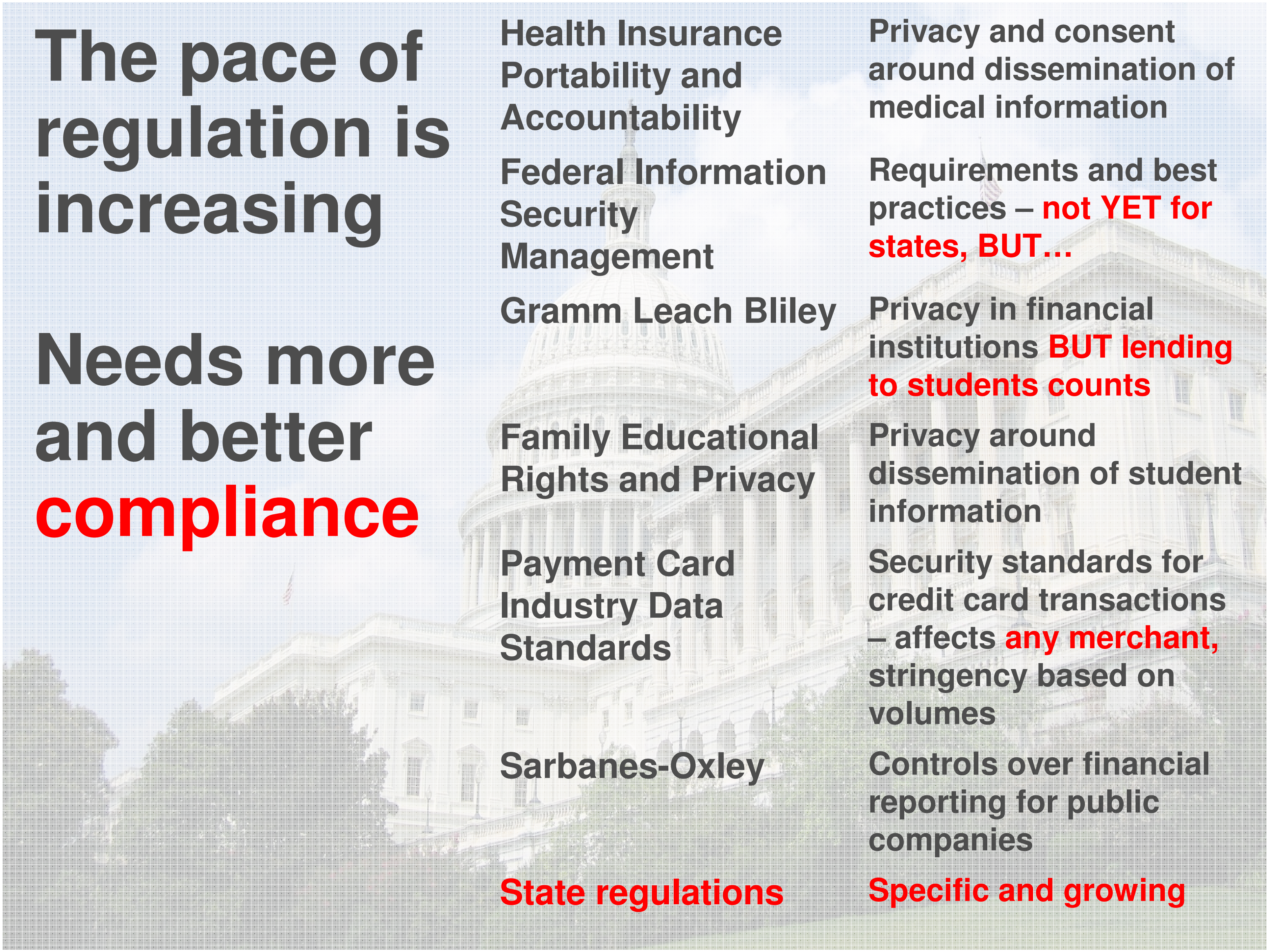
Qwest
Disgruntled IT staff recovered CEO’s email



```
[23:56] <ccs4santa> hey
[23:56] <ccs4santa> u selling fullz and cc# with cvv2?
[00:03] <makdollar> yes
[00:04] <ccs4santa> how much for a fullz?
[00:13] <makdollar> 100$
[00:14] <ccs4santa> ok..how much for card number and ccv2 info?
[00:15] <makdollar> same
[00:16] <ccs4santa> ok..you also sellin bank logins...boa / wells / EU / UK?
[00:17] <makdollar> yes
[00:17] <ccs4santa> bank logins vary or...?
[00:18] <makdollar> wht?
[00:20] <ccs4santa> how much for bank logins?
[00:21] <makdollar> 320$
```



```
[23:43] <phukincc> how bout bank logins? (boa, wells)
[23:43] <CrueL> wells 3 logins . boa 2 logins
[23:44] <CrueL> bussiness accts balances are all above 10k+
[23:44] <CrueL> no scrnsht plz
[23:44] <CrueL> rippers ask for it!
[23:44] <phukincc> yeah that goes without saying
[23:44] <phukincc> ?
[23:45] <phukincc> how much per wells and boa acct?
[23:45] <CrueL> 100$ each login
[23:46] <phukincc> mmmkay...the cvv2 that you have are like u posted?
[23:46] <phukincc> *are like what you posted?
```



The pace of regulation is increasing

Needs more and better compliance

Health Insurance Portability and Accountability	Privacy and consent around dissemination of medical information
Federal Information Security Management	Requirements and best practices – not YET for states, BUT…
Gramm Leach Bliley	Privacy in financial institutions BUT lending to students counts
Family Educational Rights and Privacy	Privacy around dissemination of student information
Payment Card Industry Data Standards	Security standards for credit card transactions – affects any merchant, stringency based on volumes
Sarbanes-Oxley	Controls over financial reporting for public companies
State regulations	Specific and growing

The types of incidents vary…

Lost or stolen laptops, computers, or other storage devices

Backup tapes lost in transit

Hackers breaking into systems

Employees stealing or allowing access to information

Poor business practices (e.g. postcards with SSNs

Malware of all kinds

Improper disposition of equipment

But what do states say are their top risks?

Inadequate statewide policies, standards, and guidelines

Inability to stay current with existing policies and laws

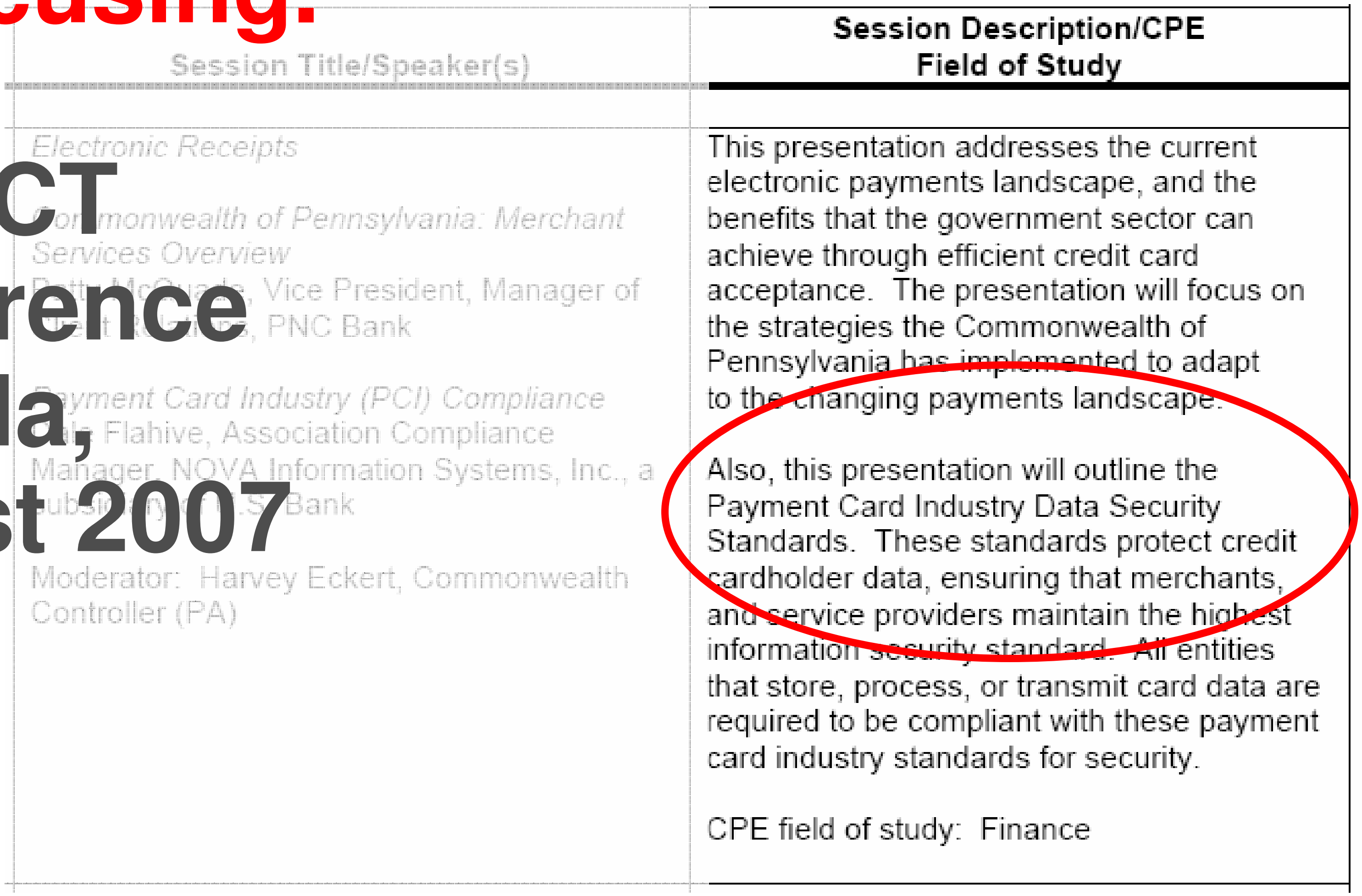
Failure to comply with policies, regulations, and laws

Limited training and education for employees and contractors

Increased risks, threats and vulnerabilities

State officials are **focusing.**

NASACT Conference Agenda, August 2007



Session Title/Speaker(s)	Session Description/CPE Field of Study
Electronic Receipts *Commonwealth of Pennsylvania: Merchant Services Overview* Betty McQuade, Vice President, Manager of [illegible], PNC Bank *Payment Card Industry (PCI) Compliance* Dale Flahive, Association Compliance Manager, NOVA Information Systems, Inc., a subsidiary of U.S. Bank Moderator: Harvey Eckert, Commonwealth Controller (PA)	This presentation addresses the current electronic payments landscape, and the benefits that the government sector can achieve through efficient credit card acceptance. The presentation will focus on the strategies the Commonwealth of Pennsylvania has implemented to adapt to the changing payments landscape. Also, this presentation will outline the Payment Card Industry Data Security Standards. These standards protect credit cardholder data, ensuring that merchants, and service providers maintain the highest information security standard. All entities that store, process, or transmit card data are required to be compliant with these payment card industry standards for security. CPE field of study: Finance

State legislators are taking action.

AR SB 1167

AZ SB 1338

CA SB 1386

CO HB1119

CT SB 650

DE HB 116

FL HB 481

GA SB 230

HI SB2290

ID Title 28-51

ILLINOIS

(H.B. 1633)

IN SB 503

KS SB196

LA SB 205

ME LD 1671

MI SB 309

MN HF 2121, Business,
HF 225, Government

MT HB 732

NE LB 876 Section 87-803

NV SB 347, Business
AB 334 Government

NH RSA 359-C:20

NJ A4001

NY 4254-A

NC SB 1048

ND SB 2251

OH HB 104

OK 74.49.3113.1

PA SB 712

RI H 6191

TN SB 2220

TX SB 122

UT 13-44-202

VT 9-62 §2435

WA SB 6043

WI 895.507

At 2/07

What are some typical initiatives?

Ensuring that legislative language is established

Updating and revising existing policies

Continuing education and training awareness for information security and privacy

Developing more tools for risk self-assessment

Developing Information Security roles and responsibilities

Developing Internet usage policy and guidelines

Coordinating efforts to align operational recovery and business continuity plans

What benefits are they looking for?

Reduce malicious code targeting desktops and servers

Protect mission critical, legally and personally sensitive information

Reduce drags on productivity

Enhance systems stability and availability

Increase flexibility and reduce complexity though standardization

Proactive assessments

Broad awareness programs around physical and information security

Reduce exposure to liabilities and costs of remediation

It is a broadening challenge

PCI

SOX

HIPAA

GLBA

ISO-17799

Privacy Laws

Training

Security Policy

Quality

Penetration Testing

Security Design

Code Review

N/HIDS

Firewall

Hosting

What can you do?

A sound security program does many things…

Focuses on HR

Hiring and retention policies for IT/security staff and end users
Adequate staffing, authority, responsibility, succession
Key training policies
Termination procedures

Performs electronic testing

Firewalls and routers
Devices visible to the Internet
Network segmentation
Active/inactive modems
OS levels and patches
Anti virus software

Reviews network architecture

Segmentation
Critical devices
User rights and permissions

Institutionalizes InfoSec

IT in enterprise governance
Management philosophy
Enterprise culture
Periodic training and review for all
Policy development

Reviews business policies and procedures

Backup and failover contingency
Redundancy, disaster recovery and continuity planning
Current equipment inventory
Vendor, partner and provider SLAs and liability
User rights and permissions
End user computing policies

Inspects physical security

Door locks and alarms
Security cameras and monitoring
Visitor access logs
HVAC, fire suppression, etc
Racks and cabling

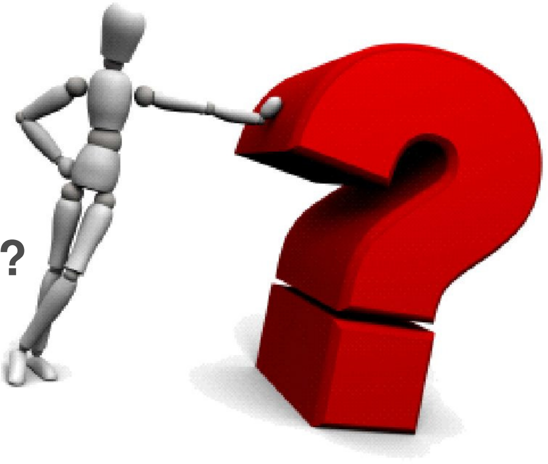
Think about your current security position and programs

What is your biggest information security concern?

Have you experienced a data breach? How did it affect you?

Does your organization have the skills and experience to handle security breaches? What are your current resource constraints?

How would you handle a computer security incident? What is the state of your incident response plan?



Are you affected by legislation or regulation around security and data protection – HIPAA, PCI (where do you accept credit cards?) etc?

What kind of security assessments do you conduct on a regular basis?

How do you assure stakeholders that your network and information stores are secure?

Improving information security programs

Watch: Monitor and act

Central management of security events

Correlation of events into threats

Action to prevent malicious threats

Assess the environment

Detailed analysis of security posture enables understanding of exposures

Governance management

Scheduled and ad hoc assessments

Control access to assets

Control and manage user identities and privileges

Manage access authorities

Manage policies

Defend outside and inside

Pre-emptive perimeter protection against external threats

Protection inside the enterprise against malicious insiders

Tivoli zSecure Suite

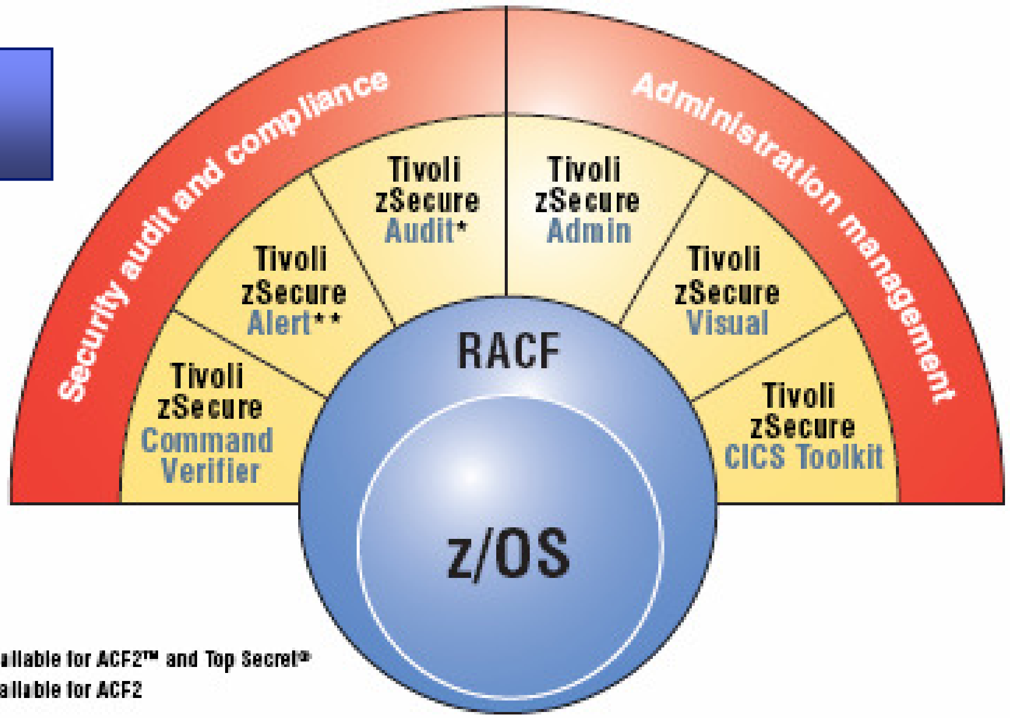
Security Management and Administration for z/OS and RACF

Administration and provisioning:

- Reduce administration time, effort and cost
- Reduce training time needed for new administrators

Audit, monitoring and compliance:

- Helps to pass audits more easily
- Can improve security posture
- Save time and costs through improved security and incident handling
- Can increase operational effectiveness


Security audit and compliance
Administration management
Tivoli zSecure Command Verifier
Tivoli zSecure Alert**
Tivoli zSecure Audit*
Tivoli zSecure Admin
Tivoli zSecure Visual
Tivoli zSecure CICS Toolkit
RACF
z/OS

*Also available for ACF2™ and Top Secret®

**Also available for ACF2

Components

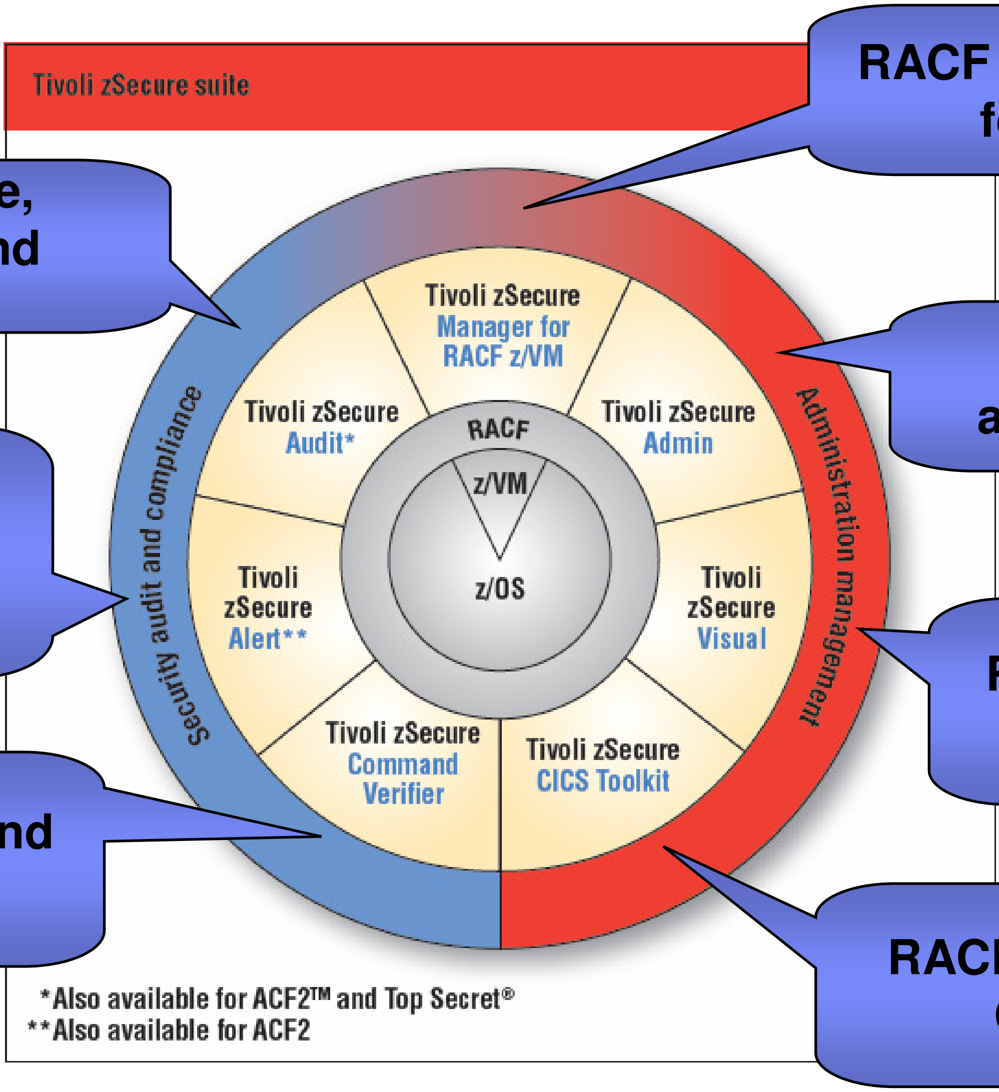
Administration and provisioning:

- **zSecure Admin** enhances user management
- **zSecure Visual** offers a Microsoft® Windows® GUI
- **zSecure CICS Toolkit** for simplified CICS security management

Audit, monitoring and compliance:

- **zSecure Audit** provides event detection, analysis & reporting and system integrity audit & analysis
- **zSecure Alert** provides intrusion detection and alerting
- **zSecure Command Verifier** offers automated security monitoring

Tivoli zSecure Suite


Tivoli zSecure suite
Tivoli zSecure Manager for RACF z/VM
Tivoli zSecure Audit*
Tivoli zSecure Admin
RACF
z/VM
z/OS
Tivoli zSecure Alert**
Tivoli zSecure Visual
Tivoli zSecure Command Verifier
Tivoli zSecure CICS Toolkit
Security audit and compliance
Administration management

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Compliance, auditing, and reporting

Real-time mainframe monitoring

RACF Command Controls

RACF Admin/Audit for z/VM

RACF administration

RACF Windows GUI

RACF through CICS

Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

Tivoli zSecure Admin

A user-friendly layer on top of RACF which enables security administration, user management and compliance management on the mainframe

Highlights:

- Admin can help you quickly identify problems in RACF, such as missing or inconsistent definitions, enabling you to fix or prevent mistakes before they become a threat to security and compliance, thus reducing the chances of breaches.
- Admin enables you to automate recurring, time-consuming security tasks. By implementing a repeatable process for security management, Admin can help you reduce errors and improve the overall quality of service, ensuring you are addressing your compliance requirements.
- Admin enables you to display data from the active (live) RACF database. Administrators can view current information, including recent changes by other administrators. An administrator can immediately verify the effect of the changes that have just been made, without having to wait for a refresh of an unloaded RACF database.

IBM Tivoli zSecure Audit

Compliance and audit solution that enables you to analyze, detect, and report security, z/OS, and Unix Systems Services exposures as well as cross reference events with RACF and system information

Highlights:

- Once auditing and analyzing of the z/OS and critical information, is completed, Audit prioritizes and highlights security concerns. Problems are ranked by audit priority, and describes the potential security breach or exposure.
- Audit analyzes SMF from the live SMF data sets or from extracted SMF data. By using live data sets, information from the active system can immediately be viewed interactively after an event has taken place.
- Audit allows you to send Simple Network Management Protocol (SNMP) messages to an enterprise management console for policy exceptions or violations that indicate a security breach or weakness.
- Audit can identify changes in the individual members of partitioned data sets, thus identifying potential areas where proper policies have not been followed.

zSecure Alert

Real-time mainframe threat monitoring allowing you to monitor intruders and identify mis-configurations that could hamper your compliance efforts

Highlights:

- Threat knowledge base with parameters from your active configurations, which helps isolate relevant attack patterns, detect multiple types of attacks and configuration threats. Knowledge of these configuration mistakes and attacks can help you take action before others can exploit them.
- Broad range of monitoring capabilities, including monitoring sensitive data for misuse on z/OS, RACF, and UNIX subsystems. Monitoring critical data aids in maintaining data integrity and staying ahead of potential security policy violations
- Easily send critical alerts to enterprise audit, compliance and monitoring solutions. Alert can automatically send security information from the mainframe into TCIM, TSOM and network and enterprise consoles. This provides timely alerts which helps you respond quickly to prevent further damage, ease organization-wide inclusion of the mainframe in audit and compliance reports.

zSecure Command Verifier

Policy enforcement solution that enforces compliance to organization and regulatory policies by preventing erroneous commands, and helps reduce the risk of security breaches

Highlights:

- Automates the process of ensuring mandatory values are used in RACF and prohibits the use of inappropriate default values. Using these controls, ensures important policy and naming requirements are maintained in your security environment.
- Automatically verifies command keywords against your specified policies as soon as a RACF command is issued, which enforces compliance on RACF to help reduce the risks of security breaches.
- Command Audit Trail feature stores changes to profiles in the RACF database. Quickly determine which administrator made which changes without requiring labor intensive investigation of log files, with no guessing about timeframes or searching for the information.
- By providing access to the specific commands users require to do their jobs, you reduce the risks associated with accidental or malicious actions of privileged users.

zSecure Visual

Enables efficient and effective RACF administration with a direct, easy-to-use, graphical interface which uses fewer resources and provides richer functionality.

Highlights:

- Through a user-friendly GUI you can decentralize RACF administration, enabling tasks to be performed at various levels. This provides the experienced RACF administrator the ability to focus on higher-value activities that help improve both security and compliance.
- Central administrators can customize the administrative commands shown on the interface. This provides the ability for a person to view only the commands they are allowed to perform, reducing the risk of incorrect commands and insider breaches.
- New users can be added to the system simply by duplicating standard user templates. This feature helps reduce the risk of giving incorrect authorizations to a new user — an administrator can only use existing templates and assign authorizations to groups within their scope.

zSecure CICS Toolkit

Allows you to perform mainframe administrative tasks from a CICS environment, freeing up native RACF resources

Highlights:

- RACF administration from a CICS environment. CICS Toolkit menu enables users to stay within the CICS application, rather than forcing them into another environment, to issue security commands to the mainframe.
- Web-enablement of the CICS-RACF API. By leveraging this sophisticated API, Web applications can use RACF functions for security administration, authentication and access control.
- The API facilitates access checks of more than 2,000 resources, enabling you to easily replace an application’s internal security with RACF security. CICS Toolkit also reduces the burden of maintenance programming and administration from CICS application developers, freeing them to focus on improving functionality.

zSecure RACF Offline

zSecure Admin RACF Offline product provides the possibility to issue most RACF commands against an inactive RACF database

Highlights:

- zSecure Admin RACF Offline provides the capability to issue RACF command against an offline RACF database. This allows you to make major changes to a RACF environment and review the changes before implementing them into production. This can decrease the chance of mistakes creating security exposures.

Tivoli zSecure Manager for RACF z/VM

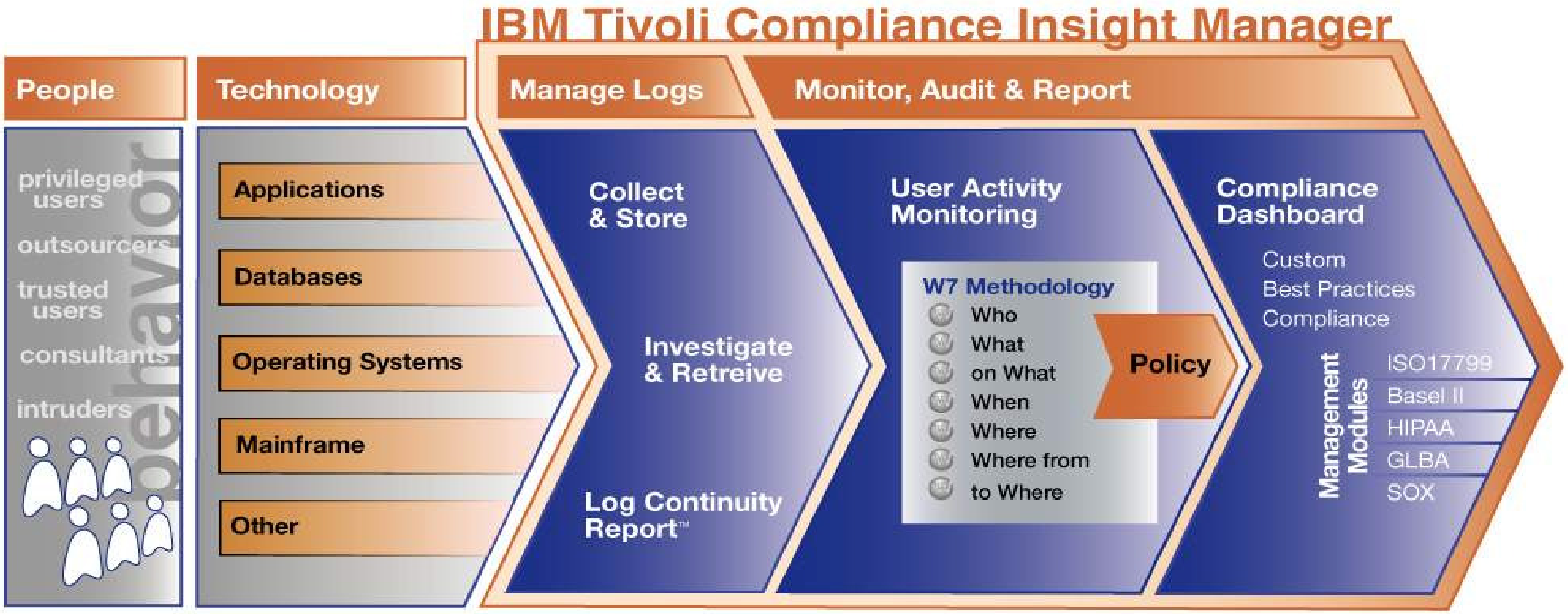
Allows you to perform mainframe administration and audit functions for RACF in the z/VM environment

Highlights

- zSecure Manager for RACF z/VM can help you quickly identify problems in RACF on z/VM, such as missing or inconsistent definitions, enabling you to fix or prevent mistakes before they become a threat to security and compliance.
- zSecure Manager for RACF z/VM provides various analyses: displaying views of vital z/VM information, indicating where problems may occur, monitoring privileged users and requesting information about individual definitions in RACF.

zSecure Compliance Insight Manager Enabler for z/OS

- **Connect the mainframe to an enterprise compliance dashboard for reporting across applications, databases and operating systems**
  – Auditors no longer need z/OS expertise to monitor activities



Conclusion

Technology has some strong solutions – but policy and culture remain critical

Ensuring that legislative language is established

Updating and revising existing policies

Continuing education and training awareness for information security and privacy

Developing more tools for risk self-assessment

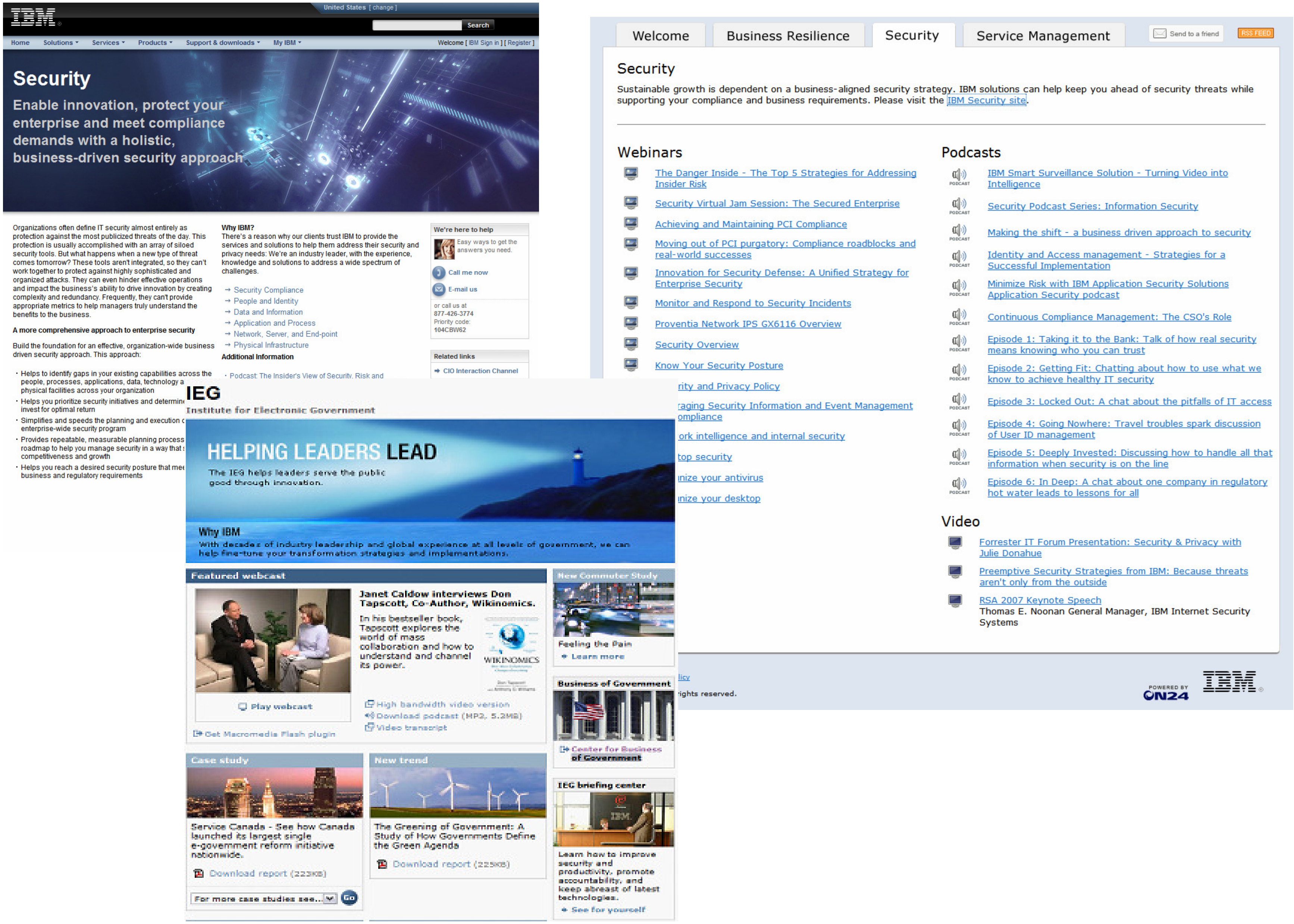
Developing Information Security roles and responsibilities

Developing Internet usage policy and guidelines

Coordinating efforts to align operational recovery and business continuity plans

http://www.ibm.com/security

http://tinyurl.com/6l6j86



Security

Enable innovation, protect your enterprise and meet compliance demands with a holistic, business-driven security approach

Organizations often define IT security almost entirely as protection against the most publicized threats of the day. This protection is usually accomplished with an array of siloed security tools. But what happens when a new type of threat comes tomorrow? These tools aren't integrated, so they can't work together to protect against highly sophisticated and organized attacks. They can even hinder effective operations and impact the business's ability to drive innovation by creating complexity and redundancy. Frequently, they can't provide appropriate metrics to help managers truly understand the benefits to the business.

A more comprehensive approach to enterprise security

Build the foundation for an effective, organization-wide business driven security approach. This approach:

- Helps to identify gaps in your existing capabilities across the people, processes, applications, data, technology a physical facilities across your organization
- Helps you prioritize security initiatives and determine invest for optimal return
- Simplifies and speeds the planning and execution c enterprise-wide security program
- Provides repeatable, measurable planning process roadmap to help you manage security in a way that s competitiveness and growth
- Helps you reach a desired security posture that mee business and regulatory requirements

Why IBM?
There's a reason why our clients trust IBM to provide the services and solutions to help them address their security and privacy needs: We're an industry leader, with the experience, knowledge and solutions to address a wide spectrum of challenges.

→ Security Compliance
→ People and Identity
→ Data and Information
→ Application and Process
→ Network, Server, and End-point
→ Physical Infrastructure

Additional Information

- Podcast: The Insider's View of Security, Risk and

We're here to help

Easy ways to get the answers you need.

Call me now
E-mail us

or call us at
877-426-3774
Priority code:
104CBW62

Related links

→ CIO Interaction Channel

Security

Sustainable growth is dependent on a business-aligned security strategy. IBM solutions can help keep you ahead of security threats while supporting your compliance and business requirements. Please visit the IBM Security site.

Webinars

- The Danger Inside - The Top 5 Strategies for Addressing Insider Risk
- Security Virtual Jam Session: The Secured Enterprise
- Achieving and Maintaining PCI Compliance
- Moving out of PCI purgatory: Compliance roadblocks and real-world successes
- Innovation for Security Defense: A Unified Strategy for Enterprise Security
- Monitor and Respond to Security Incidents
- Proventia Network IPS GX6116 Overview
- Security Overview
- Know Your Security Posture
- rity and Privacy Policy
- raging Security Information and Event Management ompliance
- ork intelligence and internal security
- top security
- nize your antivirus
- nize your desktop

Podcasts

- IBM Smart Surveillance Solution - Turning Video into Intelligence
- Security Podcast Series: Information Security
- Making the shift - a business driven approach to security
- Identity and Access management - Strategies for a Successful Implementation
- Minimize Risk with IBM Application Security Solutions Application Security podcast
- Continuous Compliance Management: The CSO's Role
- Episode 1: Taking it to the Bank: Talk of how real security means knowing who you can trust
- Episode 2: Getting Fit: Chatting about how to use what we know to achieve healthy IT security
- Episode 3: Locked Out: A chat about the pitfalls of IT access
- Episode 4: Going Nowhere: Travel troubles spark discussion of User ID management
- Episode 5: Deeply Invested: Discussing how to handle all that information when security is on the line
- Episode 6: In Deep: A chat about one company in regulatory hot water leads to lessons for all

Video

- Forrester IT Forum Presentation: Security & Privacy with Julie Donahue
- Preemptive Security Strategies from IBM: Because threats aren't only from the outside
- RSA 2007 Keynote Speech
  Thomas E. Noonan General Manager, IBM Internet Security Systems

licy
rights reserved.

IEG
Institute for Electronic Government

HELPING LEADERS LEAD

The IEG helps leaders serve the public good through innovation.

Why IBM
With decades of industry leadership and global experience at all levels of government, we can help fine-tune your transformation strategies and implementations.

Featured webcast

Janet Caldow interviews Don Tapscott, Co-Author, Wikinomics.

In his bestseller book, Tapscott explores the world of mass collaboration and how to understand and channel its power.

High bandwidth video version
Download podcast (MP3, 5.2MB)
Video transcript
Get Macromedia Flash plugin

New Commuter Study

Feeling the Pain
→ Learn more

Business of Government

Center for Business of Government

Case study

Service Canada - See how Canada launched its largest single e-government reform initiative nationwide.

Download report (223KB)

For more case studies see... Go

New trend

The Greening of Government: A Study of How Governments Define the Green Agenda

Download report (225KB)

IEG briefing center

Learn how to improve security and productivity, promote accountability, and keep abreast of latest technologies.

→ See for yourself

http://www.ibm.com/industries/government/ieg