

Verizon Business Security: **Powered by Cybertrust**

Compliance, Standards and Security in the Government Sector

Tony Maupin
Senior Security Engineer

PROPRIETARY STATEMENT

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed, or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

The Verizon and Verizon Business names and logos and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.

Agenda

Introduction

What

- Understanding the Compliance Agenda
- Security Standards De-mystified
- What is a Baseline Security Assessment
- What is a Balanced Report Card

How

- From Here to Secure: A Risk (Evidence) Based Roadmap
- Managing Security versus Managing Risk

Why

- What Didn't Work - The Data Breach Reports
- Start with finding and protecting the important data
- Essential Practices Universally Applied

The Compliance Agenda: Security Mandates

- **CIPA – Child Information Protection Act**
- **HIPAA – Health Information Portability and Accountability Act**
- **NERC/FERC – Energy Security Baseline**
- **PCI – Payment Card Industry**
- **SOX- Publicly Traded Company Standard**
- **GLBA and FFIEC – Banking Industry Regulations**

Security Standards De-mystified



All just a method to security and “Best Practice” ideas

- DSS for PCI – Payment Card Industry
- NIST (800 series) – Government Recommendations
- ISO 27001 – Security Management
- ISO 27002 – Security Controls
- CoBIT – Control Objectives for IT
- ITIL – Management Framework
- HiTrust for HIPAA – Emerging Security Controls Framework
- Proprietary Standards and Certifications

1. Broad Cross Reference
2. Map to Risk
3. Use Evidence Based Approach

Baseline Assessment Deliverables

A Report Card with an A-B-C-D or F grade for your overall security program. Each of the 12 control objectives will be broken out to determine the most critical areas along with where there may be weaknesses (the Grade will be assessed with a green – yellow – red score representing acceptable – needs improvement - requiring immediate attention).

Information Technology Security Report Card		
Overall Status	ISO 27001 Guidelines with VzB K to 12 Program Overview	
 <div style="text-align: center; font-size: 2em; font-weight: bold;">D</div> <p>Over all grade</p>	<p>ISO/IEC 27001:VzB K-12 Program establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in K-12 Educational organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27001:VzB K-12 contains best practices of control objectives and controls in the following areas of information security management controls for K-12 Educational organization in the following areas of information security management.</p> <p>The control objectives and VzB K-12 Essential Controls in ISO/IEC 27001:VzB K-12 are intended to be implemented to meet the requirements identified by a self assessment risk profile questionnaire and perimeter vulnerability scan. This VzB K to 12 Program is intended as a common basis and practical guideline for developing K-12 Educational organization security standards and effective security management practices, and to help build confidence in inter-organizational activities.</p> <p>This report presents Dallas ISD's 'As Is' status to aligning with the ISO/IEC 27001:VzB K-12 Program self declared IT Security Essential Controls and perimeter vulnerability scan as of January 10, 2009.</p>	
ISO / IEC 27001:VzB K-12 IT Security Essential Controls	As Is	'09 Plan
Risk Assessment and Treatment		
Security Policy		
Organization of Information Security		
Asset Management		
Human Resources Security		
Physical and Environmental Security		
Communications and Operations Management		
Access Control		
Information Systems Acquisition, Development & Maintenance		
Information Security Incident Management		
CIPA Compliance		
TOTAL		
		 <small>Security Solutions powered by CyberTrust</small>
<small>Copyright © 2008 Verizon Business. Proprietary and confidential. Not for disclosure to outside parties without written permission of Verizon Business. www.VerizonBusiness.com</small>		

Baseline Assessment Deliverables

A *Security Roadmap* lays out information security projects that have been identified to mitigate risks, accounts for business factors, highlights underlying problems, and culminates with a prioritized remediation plan with recommended timelines and clear goals



Managing Security versus Managing Risk

Ask the “Risk Question”

How

		Simplified Threat Categories							
Perpetrator / Vector / Target		Malcode	Hacking	Fraud	Misuse	Error	Compliance	Physical	Environment
Who	Executive								
	Privileged IT								
	Employee								
	Partner								
	Student								
	Opportunity Outsider								
	Choice Outsider								
Infrastructure Target		Infrastructure Building Blocks (cont.)							
Inf. Building Block (IBB)		Malcode	Hacking	Fraud	Misuse	Error	Compliance	Physical	Environment
Online Structured Data Repository		Indirect Access Device			Application Administration Service				
Online Unstructured Data Repository		Uncontrolled Access Device			Discovery (Domain Name) Service				
Replica Online Structured Data Repository		Process Control Access Device			Directory Service				
Replica Online Unstructured Data Repository		Dynamic Web Application / Services			Gating Service				
Exported Structured Data Repository		Static Web Application / Services			Storage Area Network Service				
Exported Unstructured Data Repository		Internal Business Application			Middleware Services				
Online Data Warehouse		Client Application			Processing Service				
Offline Electronic Data Repository		Messaging Application			Operational support services				
Portable Electronic Data Repository		Process Control / SCADA Application			Activity Logging / Monitoring Service				
Non-electronic Data Repository		Dedicated Wired Network Service			Identification and Authentication Service				
Exported Non-electronic Data Repository		Local Area Network Service			Data Proxy Service				
Services Administration Data Repository		Wireless Access Network Service			Certificate / Signing Service				
Direct Access Device		Remote Access Network Service			Physical Facility				
Impact Type		Malcode	Hacking	Fraud	Misuse	Error	Compliance	Physical	Environment
Legal & Liability									
School District Damage									
Loss of Assets									
Investigative									
Response/Recovery									
Productivity Impacts									
Business Interruption									
Fraud & Secondary Attacks									

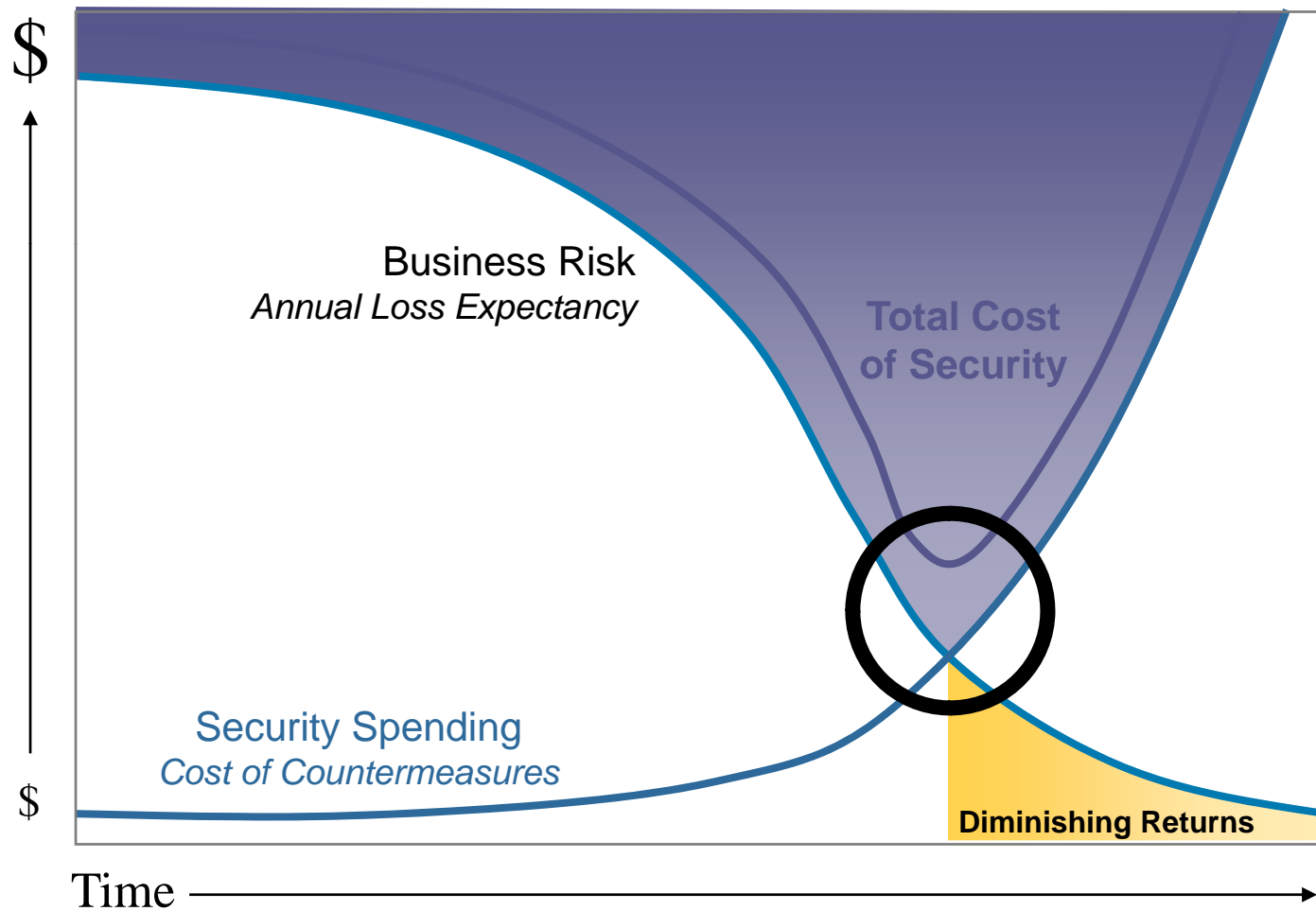


The Steel Door on a Grass Hut Syndrome

Focused only on technology as “The Solution”



Minimizing the total cost of effective security



Data Breach Investigations Reports - Highlights

- Over 600 cases spanning 5 years with cross section of industries represented
- 87% of cases could have been avoided with basic security measures.
- 66% of cases involved a system the organization did not even know contained sensitive data.
- 39% of the breaches involved business partners.
- Breaches involving partners increased five-fold from 2004
- Different Attacks from different parts of the globe (APAC – EMEA)
- Span of Events of a Breach
 - Compromise – Hours/Days
 - Discovery – Months (Logs had the data)
 - Mitigation – Weeks
- 52% of the cases came from low level attacks
- 70% of the time notification of breach came from a third party entity

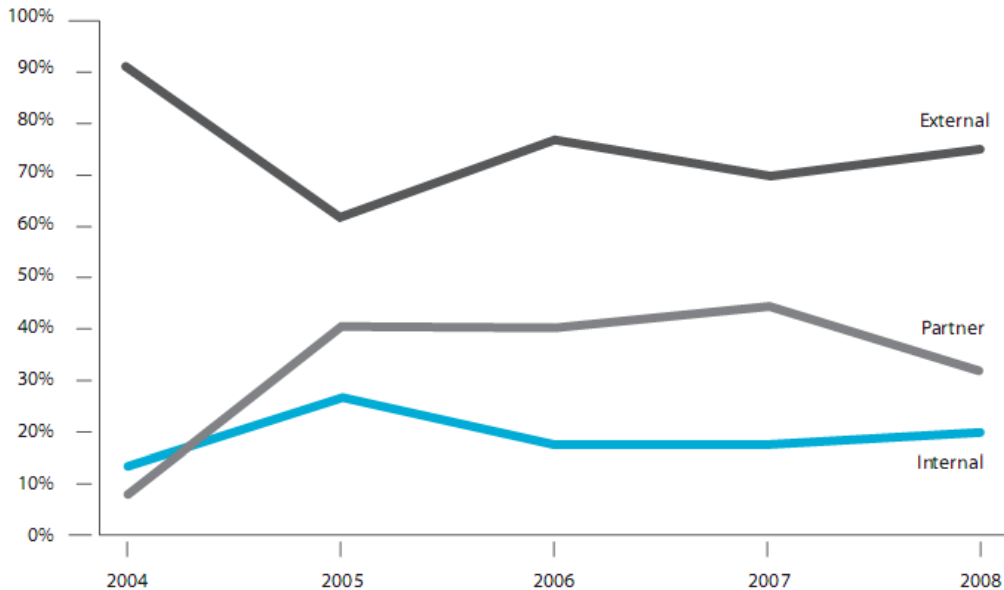
Results and Analysis

2009 Data Breach Investigations Report



Breach Sources

- **External sources**
 - Most breaches, nearly all records
 - 90+% of breached records attributed to organized crime activity
- **Internal sources**
 - Roughly equal between end-users and admins
- **Partner sources**
 - Mostly hijacked third-party accounts/connections



Likelihood

Figure 5. Single vs. multiple breach sources by percent of breaches

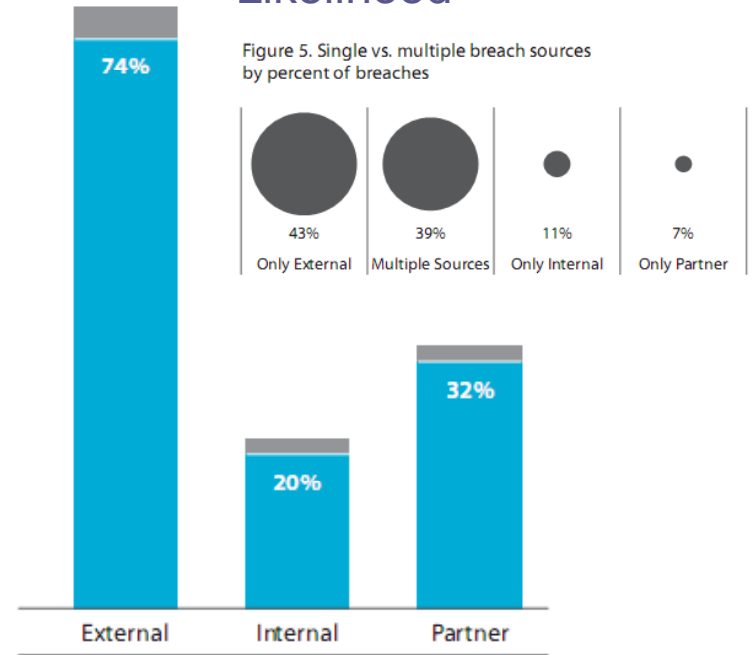
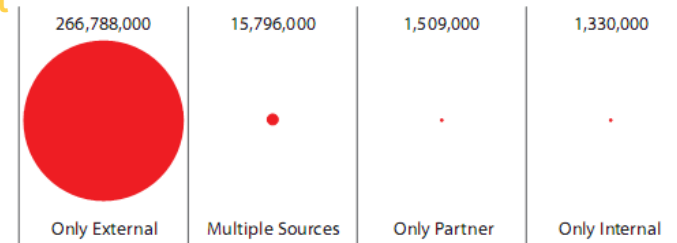


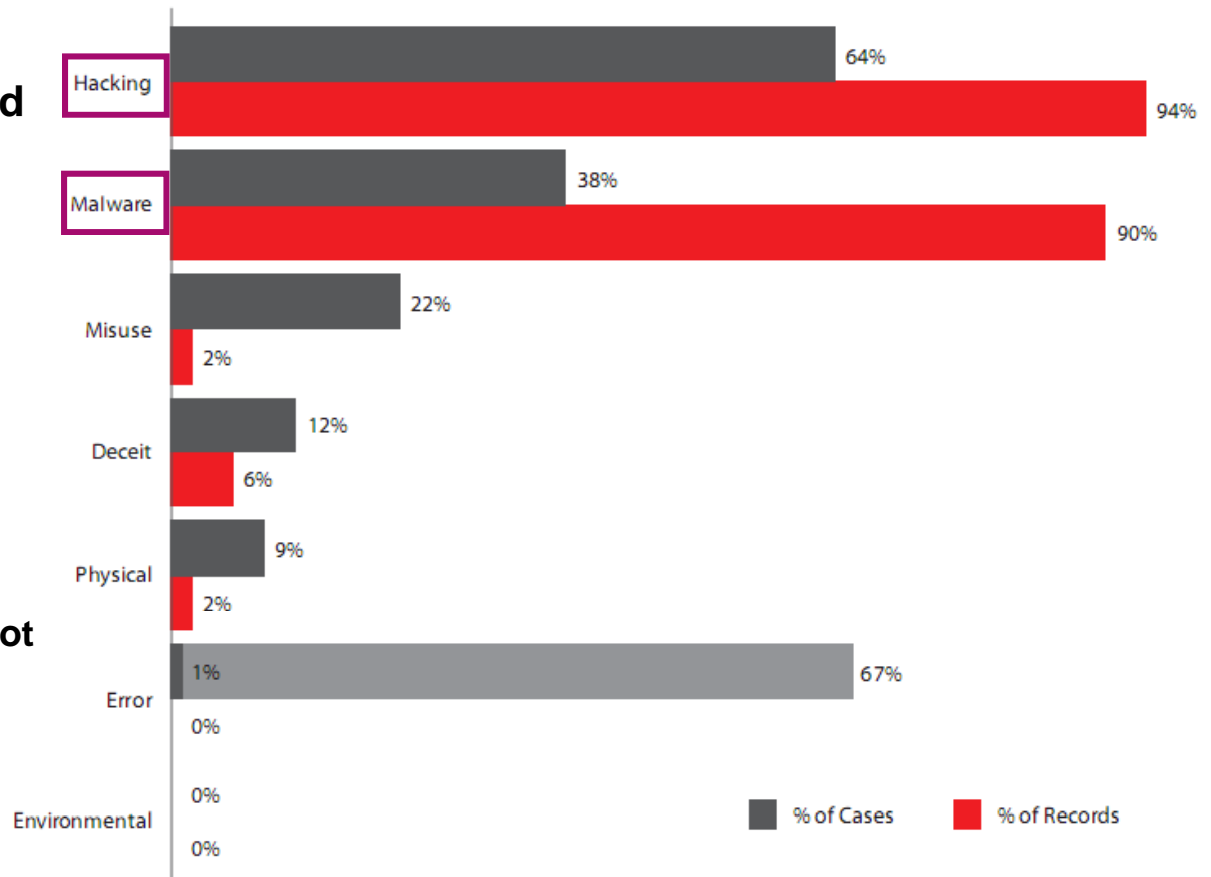
Figure 8. Total records compromised by source

Impact



Threats and Attacks

- Similar to previous 4 years for breach percentages
- Most breaches and records linked to Hacking & Malware
- Misuse is fairly common
 - Mostly admin abuse
- Deceit and social attacks
 - Involved a range of methods, vectors, and targets
- Physical attacks
 - Represent minority of caseload
 - Portable media in one case (but not essential to breach)
- Error is extremely common
 - Rarely the direct cause
 - Usually contributing factor (67%)



Attack Difficulty and Targeting

- Targeted attacks doubled
- Highly difficult attacks did not increase but are responsible for nearly all breached records
- Message: Some attacks are difficult to pull off but the payout appears worth it

Figure 22. Attack difficulty by percent of breaches

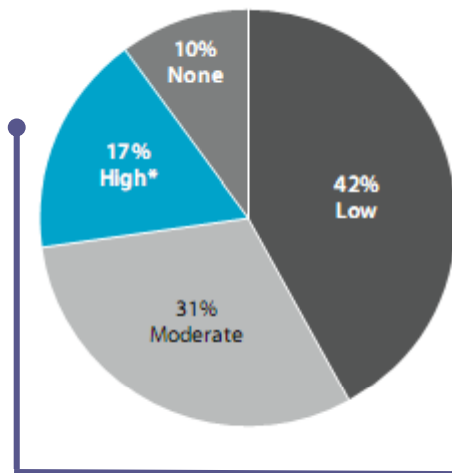


Figure 23. Attack difficulty by percent of records

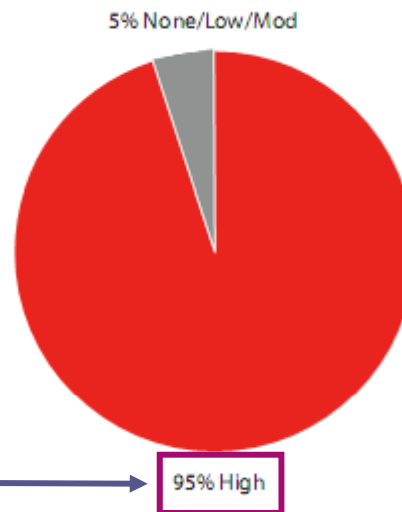


Figure 24. Targeted vs. opportunistic attacks by percent of breaches



Compromised Assets and Data

- **Most data breached from online systems**
 - Different than public disclosures
- **Criminals seek payment card data**
 - Easily convertible to cash
- **Other types common as well**
 - Auth credentials allow deeper access
 - Intellectual property at 5-year high

Figure 25. Asset classes by percent of breaches (black) and records (red)

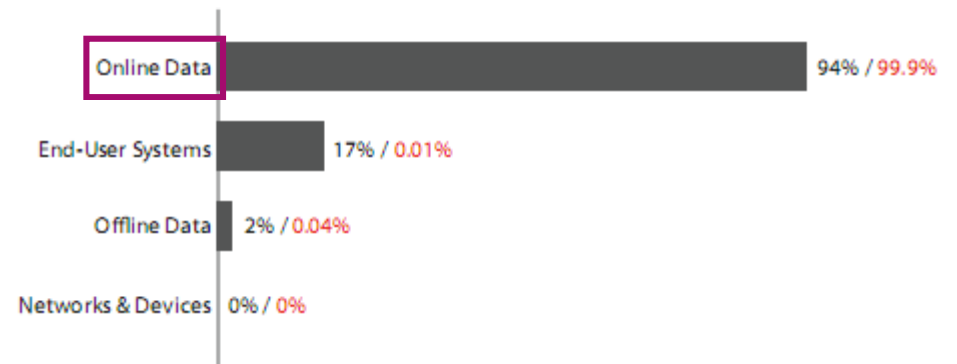


Figure 29. Compromised data types by percent of breaches (black) and records (red)*

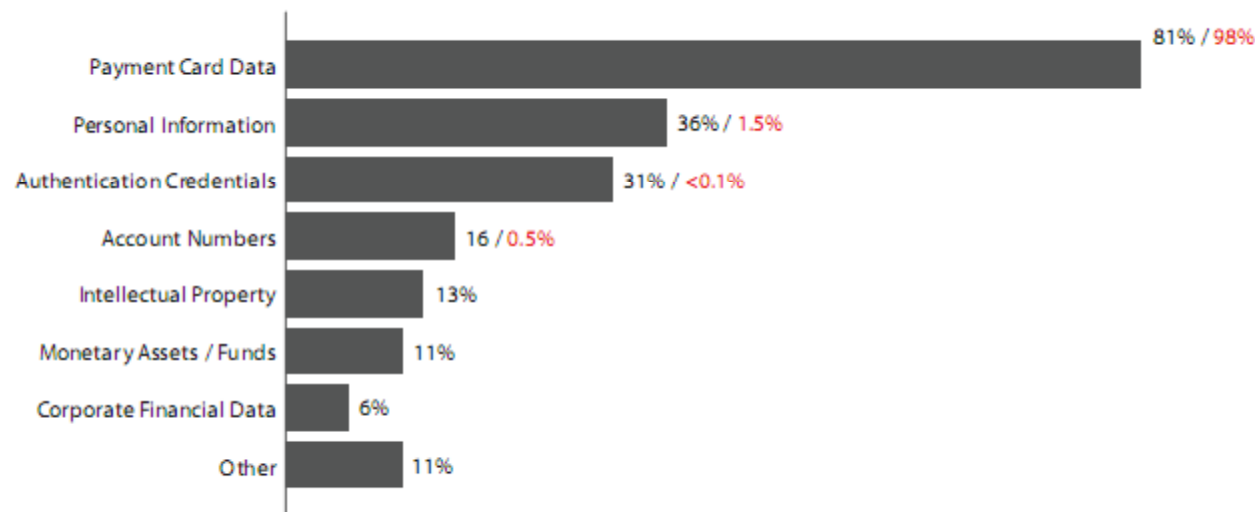
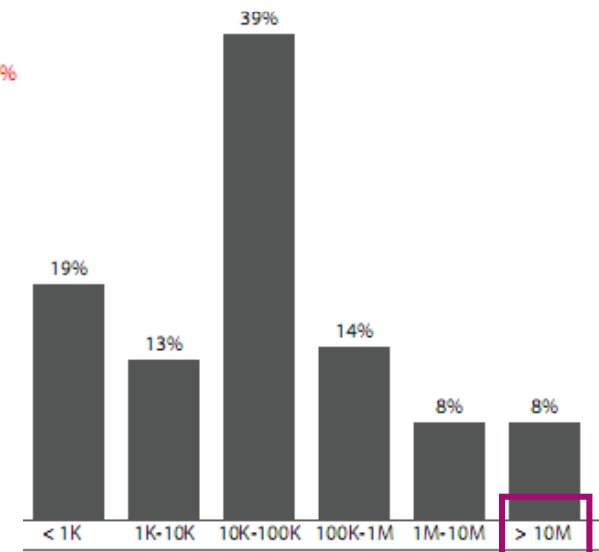


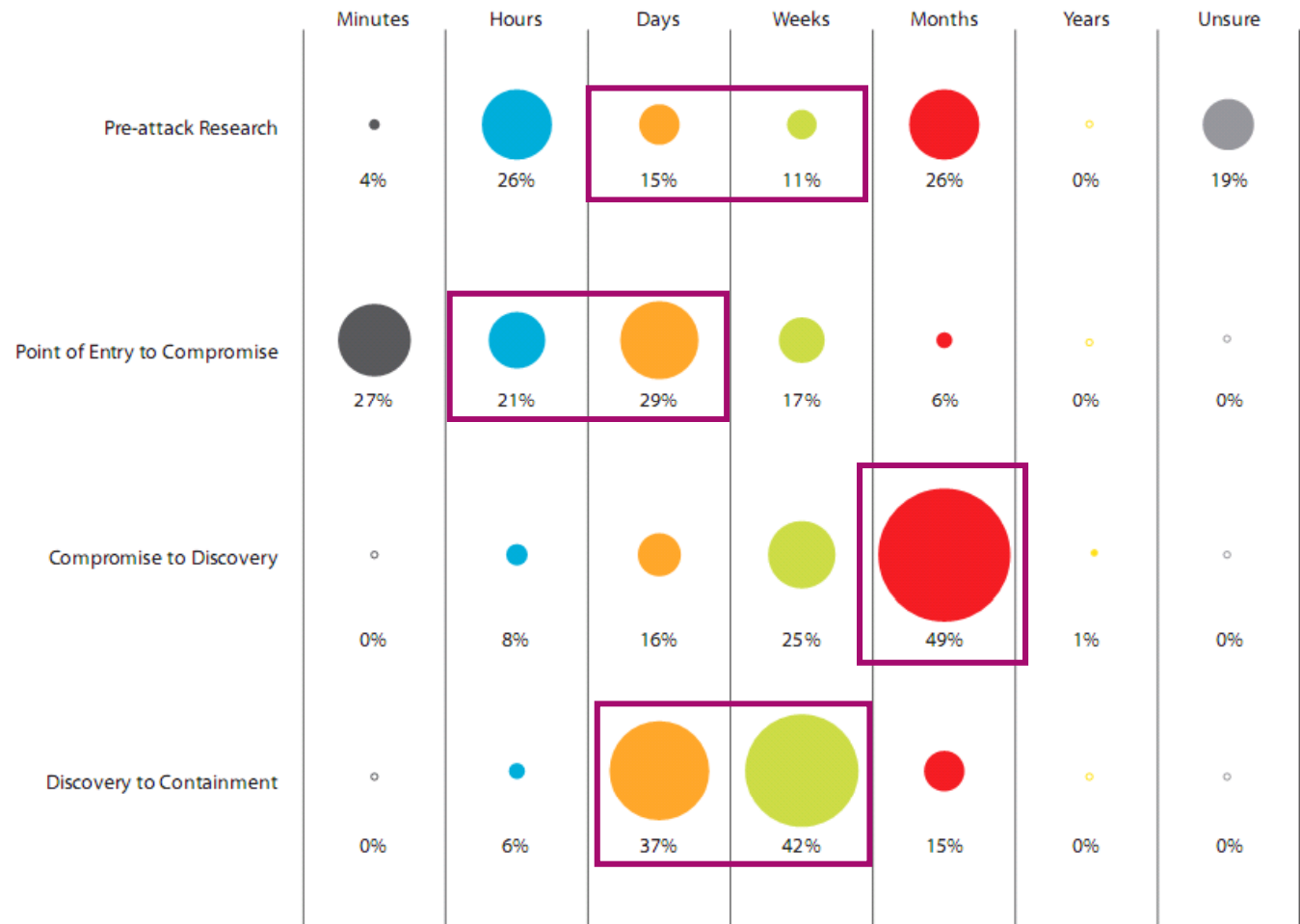
Figure 28. Distribution of breach size by number of records



Breach Timeline

- Amount of pre-attack research varies
- Data compromised within hours/days after breaching perimeter
- Breaches go undiscovered for months
- It typically takes days to weeks to contain a breach

Figure 31. Time span of breach events by percent of breaches



Breach Discovery

- Most breaches discovered by a third party
- Event monitoring caught few breaches

Figure 32. Breach discovery methods by percent of breaches

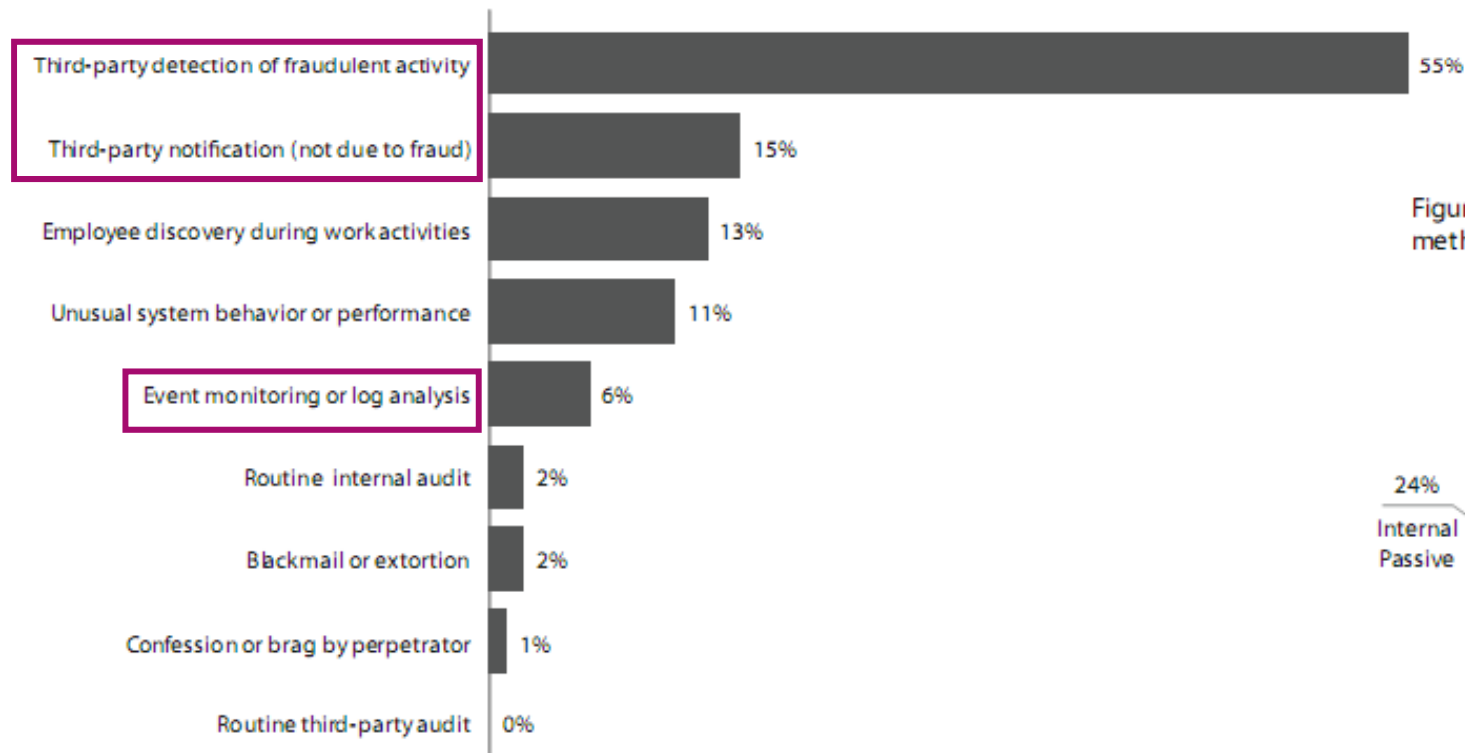
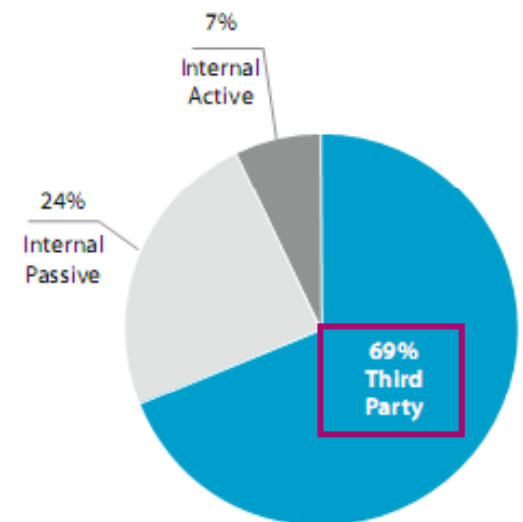


Figure 33. Breach discovery methods, simplified

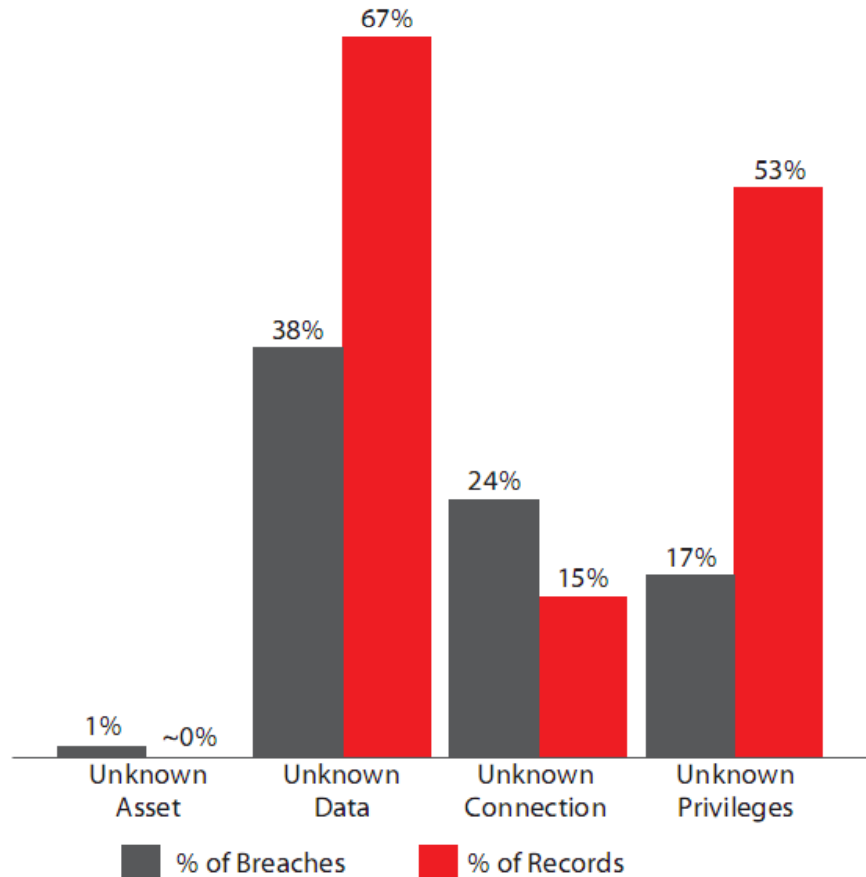


Unknown Unknowns

- **Unknown data lower than '04-'07 rates but still accounts for 2/3 of compromised records**
 - Discovery and classification
- **Unknown privileges up**
 - Account review

An **asset** unknown to the organization
Data unknowingly stored on an asset
Unknown or forgotten external IT **connections**
Accounts and **Privileges** not known to exist

Figure 30. Unknown unknowns by percent of breaches



Recommendation Summary

- **Policy and Process Reviews**
- **Security Assessments**
- **Develop and Security Management Program**
- **Monitor event logs (Security, OS and Application)**
- **Create an Incident Response Plan and Test the Plan**
- **Increase Awareness**
- **Secure Business Partner Connections**
- **Reduce Unknown Unknowns**
- **Identity and Access Management Program**

Recommendations: Plans, Policies and Assessments

Policy and Process Reviews

Security Assessments

- Create a Data Classification Scheme
- Create a Data Retention Plan
- Control data with transaction zones
- Define and review district (State) security policy
- Ensure that processes and procedures are aligned with policy
- Application Testing and Code Review
- **Review controls for Web access**

Recommendations: Implement Essential Controls

Security Management Program

- Evaluate adherence to “Essential” security control practices
- Evaluate adherence to compliance controls
- Measure and report on control status and progress
- Strive for “Smart” Patch Management Strategies
- Drive towards Excellence through risk based prioritization

Compliance ScoreCard

All Standards	ISO 27002	SMP ENT	SMP PER	SMP SP	COBIT 4.1	GLB	FFIEC	BITS AUP 3.0	PCI DSS 1.1	PCI DSS 1.2	NERC CIP	21 CFR 11	HIPAA	ISO 27799	NIST SP 800-66	SOX 404
Sort	▼															
SMP Parent - Demo	98	73	76	76	59	48	50	93	49	44	52	25	52	50	44	82
SMP Demo VA Datacenter	64	77	92	90	35	43	45	50	45	41	56	21	52	32	40	12
(AVERAGE) SMP Parent - Demo	54	55	62	61	29	33	35	37	37	32	39	14	36	27	28	21
SMP Demo Headquarters	52	51	56	55	28	33	34	25	37	31	38	14	35	25	28	5
SMP Demo Consumer Credit	40	36	42	42	17	29	31	16	35	30	32	4	29	19	25	2
SMP Industry Average: Financial Services	36	36	38	37	19	25	27	23	28	25	34	11	26	18	23	12
SMP Demo LA Datacenter	14	36	44	42	5	14	14	2	19	16	18	4	10	8	5	3

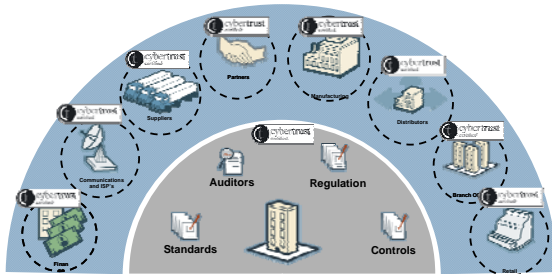
Color Key: ■ 100-80% ■ 79-50% ■ 49-0%

Recommendations: Event/Log Monitoring

Managed Security Services (Monitored / Managed)

- Ensure 24/7 monitoring with both automated and “live” review
- Enable Application Logs and Monitor

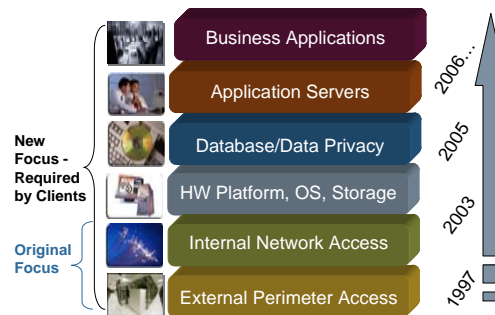
‘Wider’



Supporting the extended enterprise beyond the perimeter

- Business Partners
- Customers
- Remote Offices
- (Mobile) End Points

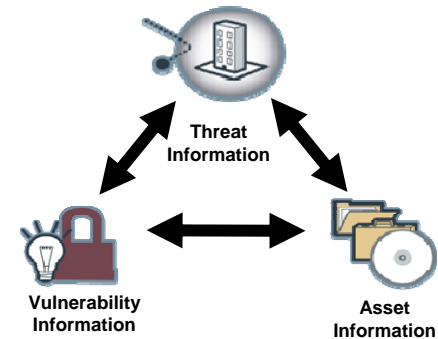
‘Deeper’



Moving up the stack ... beyond the network

- Business Applications
- Information Chain of Custody
- Data Loss Prevention

‘Smarter’



Understanding the business risk ... beyond threat management

- Security Events
- Vulnerability Management
- Asset Criticality
- The Risk Equation



Recommendations: IR, Awareness and Forensics

Incident Response Review and Forensic Retainer Security Awareness Training Forensic Investigations

- Create an Incident Response Plan
- First responder training
- Engage in mock incident testing
- Implement effective user awareness training
- Secure investigative team to be prepared for forensic response

Recommendations: Partner Security

Partner Security Program

- Secure Business Partner Connections
- Evaluate risk introduced by business partners

verizonbusiness
Security Solutions powered by Cybertrust

Partner Security Program Executive Dashboard

Home Start navigating with this dropdown

Partner Security Program homepage Dave Bilder - 06 June 2009 2:22:52 PM

Partner Overview

Filter by partner group or tag: ----- no filter -----

Current [More details](#)

Partners by compliance status

(graph updated hourly)

Compliance Status	Count
Fully Compliant	41
Partially Compliant	31
Not Compliant	10
Compliance Unknown	18

Legend: Fully Compliant (Green), Partially Compliant (Yellow), Not Compliant (Red), Compliance Unknown (Grey)

Currently provisioned partners: [69](#)
Currently running assessments: [99](#)

Worst 5 performers

Rank	Performance	Partner Name
1.	0%	Mason Medical Suppli...
2.	0%	DotRight Electrical-G...
3.	0%	DotRight Electrical-IS...
4.	33%	Beautiful Baths Inc.-...
5.	34%	Crystal Cleaners S.A...

History

Partner Compliance in Time

(graph updated daily)

Date	Unknown	Compliant	Not compliant	Partially compliant
Thu May 07 00:00:00 GMT 2009	0	0	0	0
Wed May 13 00:00:00 GMT 2009	0	0	0	0
Tue May 19 00:00:00 GMT 2009	0	0	0	0
Mon May 25 00:00:00 GMT 2009	0	0	0	0
Sun May 31 00:00:00 GMT 2009	0	0	0	0
Sat Jun 06 00:00:00 GMT 2009	0	0	0	0

Legend: Unknown (Grey), Compliant (Green), Not compliant (Red), Partially compliant (Yellow)

Assessments expired in the last month: [3](#)

Notifications

May 25, 2009
Assessment for ISO 27002:2005 is now expired.

May 24, 2009
Your assessment has been automatically submitted

May 18, 2009
Assessment for ISO 27002:2005 is now expired.

Quick links

- Dashboard User Guide
- Manage partner groups
- Create a partner group
- Manage compliance standards
- Manage compliance assignments
- Manage partners
- Create a partner
- Follow-up partner compliance
- Manage users
- Customize your settings

Document links

No document links

Recommendations: Reduce Unknown Unknowns

Security DLP Program

Virtual Discovery and Classification

- **Create a Data Classification Scheme**
- **Reduce Unknown Unknowns**
 - **Locate sensitive data (data discovery)**
 - **Track sensitive data inside the corporate domain**
 - **Track sensitive data leaving the corporate domain**
 - **Identify and investigate suspicious connections and traffic to the rest of the world**
- **Define “Suspicious” and “Anomalous” (then look for whatever “it” is)**

Recommendations: Identity and Access Mgt

Identity and Access Management Program

- **Create an IAM roadmap**
- **Perform User Account Reviews**
- **Automate RBAC initiation and termination**
- **Integrate HR termination procedures with IDM**
- **Change default credentials and avoid shared credentials**
- **Create audit and accountability process for system/data access**

Verizon Business Security Portfolio

Carrier	Enterprise	
In-The-Cloud Services: Notification Services Network Intelligence Service Managed Email Content Managed Web Content Managed Secure IM Managed Authentication (RSA) DOS Defense - Mitigation - Detection	Perimeter and End Station Security Management/Monitor <ul style="list-style-type: none"> • Managed Firewall * • Managed HIPS/NIPS * • Managed HIDS/NIDS * • Managed (SSL) VPN * • Managed Security Appliance Security Assessment Scanning <ul style="list-style-type: none"> • SaaS Vulnerability Management Security Product Resell <ul style="list-style-type: none"> • Managed Application Firewall • Managed AV (Gateway & CPE) • Managed Proxy Servers • Managed Content Screening • Log Monitoring • Managed RSA • Managed SOC • Video Surveillance 	
Professional Services		
Strategy Planning Architecture & Design Compliance & Governance Services	Application Security Services Assessment Services Implementation Services	Forensics/Incident Response Network Security Wireless/VOIP Security PCI Audit and Consulting
Identity Management	Strategic Programs	
Hosted Credential Services (UniCERT) Managed Credential Services Root Signing (Omniroot) Code Signing EV SSL and SSL Certificates NAC Implementation Services	Security Management Program (SMP) Partner Security Program (PSP) Online Compliance Program for the Payment Card Industry Disaster Recovery and Business Continuity Planning Secure Application Lifecycle	

