



The North Carolina Office of the State Controller

Assessing IT Security Risks and Evaluating Security Controls in Your Organization

April 15, 2014

My Background

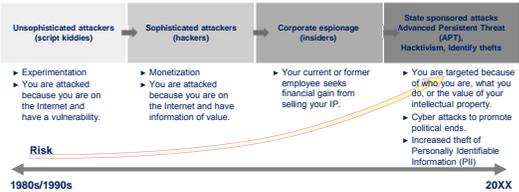
- Chip Wentz
- Ernst & Young, LLP - Executive Director, Advisory Services
 - Serves as the Americas Information Protection and Privacy services leader and the Southeast Region Information Security leader
 - Experience in IT risk management, information security, data protection, privacy, compliance, controls and governance, with a focus on enabling the business to achieve its objectives through risk mitigation and process improvement.

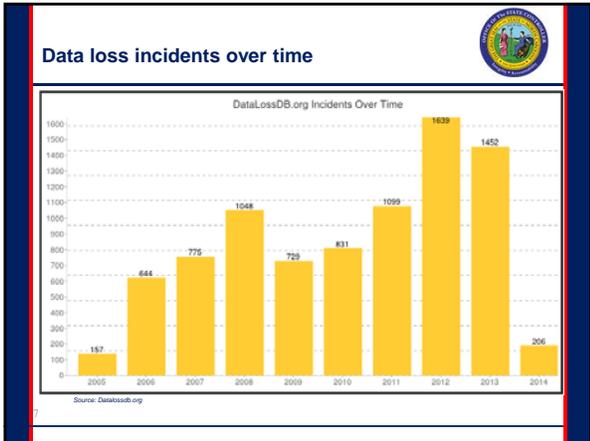


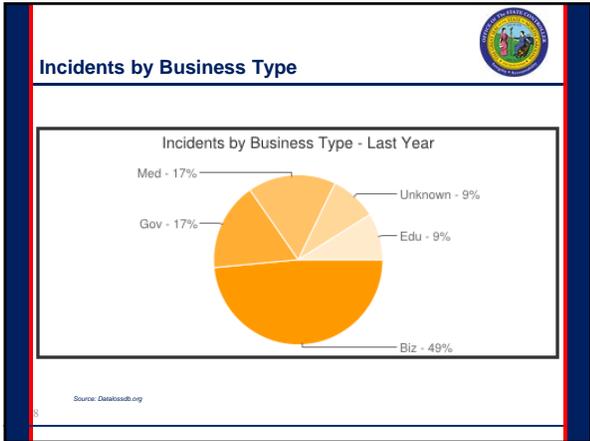
Cyber threats are constantly evolving

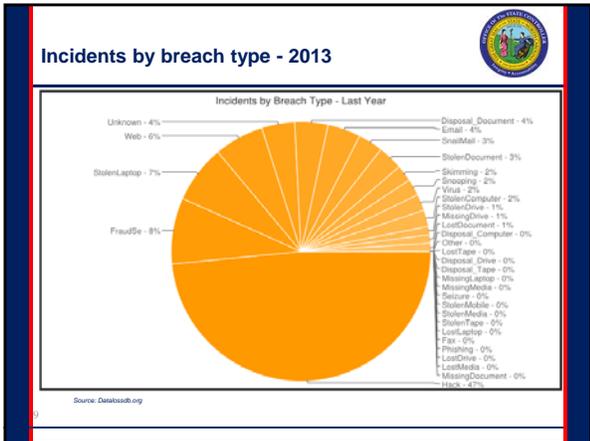
Today's information security programs are challenged to effectively deliver value while managing business risk. Cyber security threats are constantly evolving. Attackers today are patient, persistent, and sophisticated, and attack not only technology, but increasingly, people and processes. The challenges faced today have altered expectations, strained resources, and caused a paradigm shift in information security processes.

Consequently, organizations today need to alter their mindset on how to think about information security threats, risks, and capabilities.









Sample Data Loss Events – Govt



Organization	Incident Details
Fulton County Georgia, City of Burlington, Vermont	An undisclosed number of names, Social Security numbers, and dates of birth exposed on public court website
City of Detroit	1,700 employee names, dates of birth, and Social Security numbers compromised after a malware infection
Texas Comptroller's Office	Personal details for 3.5 million teachers and other employees of the state of Texas were accidentally published on the Internet. Information released included names, social security numbers and birthdates. This data had been posted on the Internet for over a year without the organization realizing it.
California DMV	An unknown number of credit or debit card numbers with expiration dates and three digit security codes compromised due to a security issue with the credit card processing service
NC DHHS	<ul style="list-style-type: none"> 45,752 names, dates of birth, and Medicaid identification numbers exposed when children's Medicaid insurance cards were sent to the wrong addresses Missing flash drive contained unencrypted names, SSN, dates of birth and addresses for more than 50,000 medical providers
NC DOR	Files on 30,000 taxpayers on stolen laptop
NC ABC	Malware has compromised multiple stores point-of-sale systems
NC Dept of State Treas	As many as 26,000 envelopes mailed in January partially or fully exposed the retirees' Social Security numbers

Source: DataLossDB.org

Incidents involving "North Carolina"



- http://datalossdb.org/search?utf8=%E2%9C%93&query=North+carolina&show_fringe=no&commit=SEARCH

Organizations	Incidents	Records
Johnson County North Carolina	2	61,000
Mecklenburg County North Carolina	1	400
University of North Carolina	3	242,000
North Carolina State University	1	1,800
North Carolina Utilities Commission	1	???
North Carolina Department of Revenue	1	30,000
North Carolina Department of Transportation	1	25,000
North Carolina Department of Correction	1	???
North Carolina Community College System	1	51,000
North Carolina Employment Security Commission	1	1,771
Wake County North Carolina Emergency Medical Services	1	4,842
University of North Carolina at Greensboro	3	2,815
University of North Carolina School of Arts	1	2,700
North Carolina Division of Medical Assistance	1	???
North Carolina Division of Motor Vehicles	2	16,013
University of North Carolina at Charlotte	3	350,148
North Carolina Department of State Treasurer	1	26,000
North Carolina Alcoholic Beverage Control Commission	1	???
State Crime Office of North Carolina	1	2,608
North Carolina Division of Aging and Adult Services	1	85,045
University of North Carolina Lineberger Comprehensive Cancer Center	1	3,500
North Carolina Department of Health and Human Services	5	100,520

Common risks associated with sensitive information – What could go wrong?



- Considering what could go wrong is important for understanding what needs to be done to effectively manage and protect sensitive information. However, these challenges are often tactical challenges or symptoms of broader issues.
- Common challenges**
 - Lost or stolen media
 - Over-sharing of personal information
 - Good intentions but misused data
 - Third party service provider weaknesses
 - Web site leakage
 - Hackers (inside and outside)
 - Unwanted marketing communications (telephone, email)
 - Fraudulent transactions
 - Social engineering, including phishing

Business drivers - Staying out of the headlines



Impact of data loss incidents:

- ▶ Reputational damage
- ▶ Regulatory fines
- ▶ Loss of customer confidence
- ▶ Direct loss of business
- ▶ Loss of competitive advantage

The cost of a breach



The cost of a breach, broken out for three sample companies

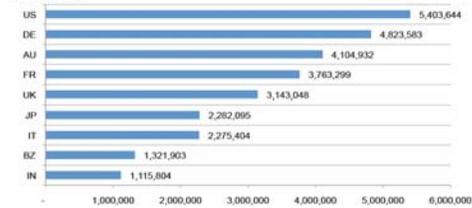
Category	Description	Cost per record		
		Company A: Low-profile breach in a non-regulated industry	Company B: Low-profile breach in a regulated industry	Company C: High-profile breach in a highly regulated industry
Discovery, notification, and response	Outside legal counsel, mail notification, calls, call center, and discounted product offers	\$50	\$50	\$50
Lost employee productivity	Employees diverted from other tasks	\$20	\$25	\$30
Opportunity cost	Customer churn and difficulty in getting new customers	\$20	\$50	\$100
Regulatory fines	FTC, PCL, SOX	\$0	\$25	\$50
Restitution	Civil courts may ask to put this money aside in case breaches are discovered	\$0	\$0	\$30
Additional security and audit requirements	The security and audit requirements levied as a result of a breach	\$0	\$5	\$10
Other liabilities	Credit card replacement costs. Civil penalties if specific fraud can be traced to the breach	\$0	\$0	\$25
Total cost per record		\$90	\$155	\$305

Source: Forrester Research, Inc.

The cost of a breach (continued)



Figure 3. The average total organizational cost of data breach



Source: Symantec & the Ponemon Institute - May 2013: Cost of a Data Breach Study

Factors that affect cost

Seven factors that raise / reduce cost of a data breach

<p>Cost goes up when...</p> <ul style="list-style-type: none"> Third party error (+\$19) Lost or stolen devices (+\$8) Quick notification (+\$7) 	<p>Cost goes down when...</p> <ul style="list-style-type: none"> Strong security posture (-\$15) Incident response plan (-\$13) CISO appointment (-\$8) Consultants engaged (-\$5)
---	--

2013 Annual Study: Global Cost of a Data Breach - June 5, 2013 | Symantec

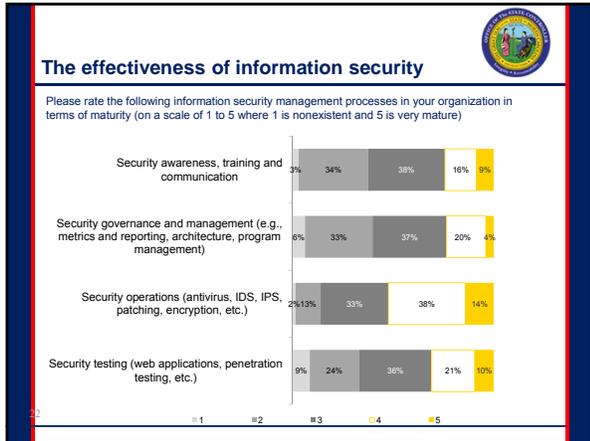
Organizations are fighting to close the security gap of the advancing threat.

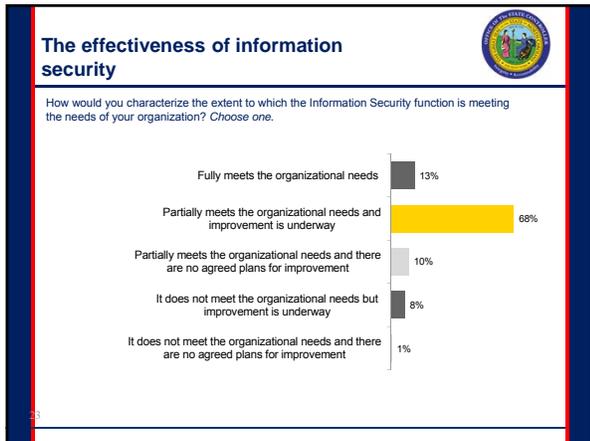
- ▶ Companies have implemented "point solutions" to respond to known security threats.
- ▶ However, the number and sophistication of threats has also increased.
- ▶ Organizations are challenged to grow its security controls at pace with the rising threats.
- ▶ As a result, the gap between what the information security function is doing and *should* be doing has widened.

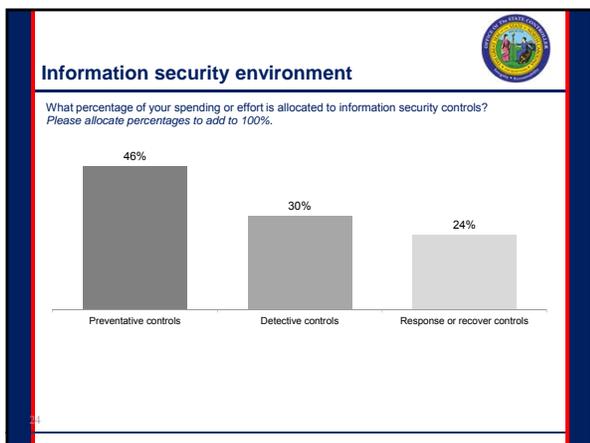
The graph shows two upward-sloping lines from 2006 to 20XX. The upper line is labeled 'Enhancements needed based on accelerating threats' and the lower line is 'Actual enhancements in information security'. A vertical double-headed arrow between the lines is labeled 'The Gap', indicating that the gap between what is needed and what is actually done is widening.

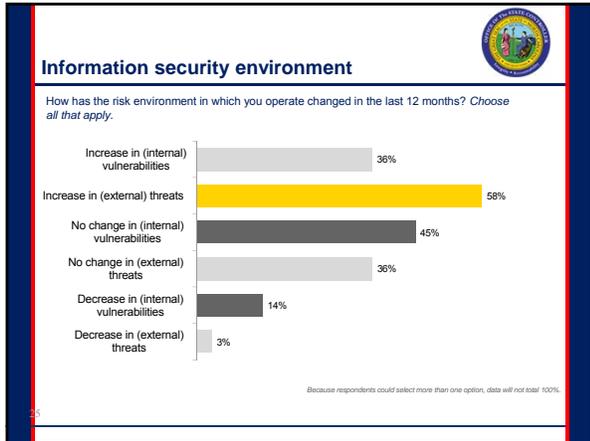
Introduction to EY's Global Information Security Survey Results

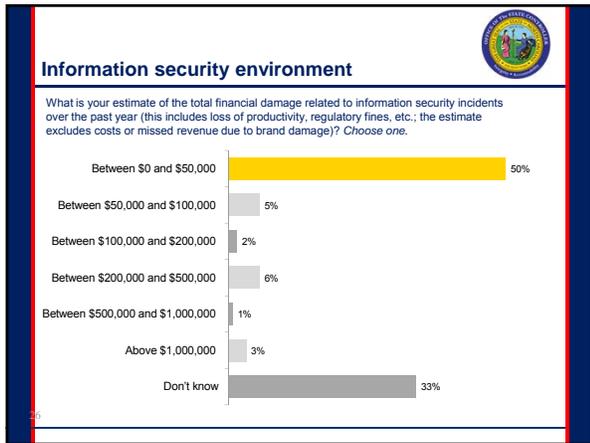
- Now in its 16th year, EY's Global Information Security Survey is among the world's leading sources of information and insight into the global state of information security.
- This year's 1,909 respondents (128 from Govt and Public Sector) from 64 countries represent most of the world's largest and most-recognized global companies, and include some of the world's leading information security authorities.
- Strong data, blended with EY's industry-leading perspectives help our clients focus on the most critical risks, identify their strengths and weaknesses, and improve their information security.
- The following slides are related to the Government and Public Sector respondents data.

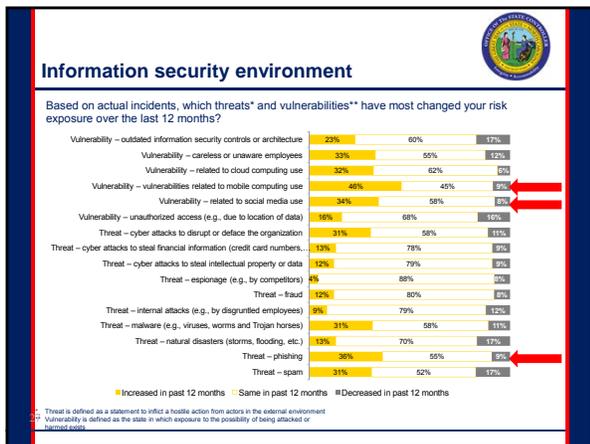








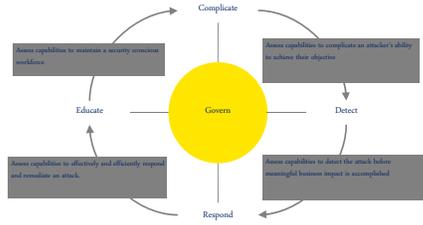




A new approach to assessing cyber security resiliency



- Assume you are a target and you will be compromised
- Take "prevent" out of your dictionary – there is a high likelihood of success if you are targeted
- Protect what matters most



What needs to be discussed



- Top four risks
 - State-sponsored attacks
 - Cloud computing and new data risks
 - Social media and reputation risks
 - Mobile device security breaches
- Broadening discussion with CIO of IT risks beyond financial controls
- Hot topics:
 - Protecting sensitive information
 - Changing focus of information security
 - Monitoring compliance

What executives are asking



- Is information security focused on protecting the assets that make money for our organization?
- How do we measure the effectiveness of our information security program?
- How has the Information Security program kept pace with the evolution of our IT landscape (e.g., cloud, mobile, social, BYOD)?
- Is the information security organization appropriately organized, trained, equipped, staffed and funded?
- What are other companies like us doing?

Evolution of cybersecurity threats

Summary of key points



- Cyber risks are very real and emanate from a wide range of sources:
 - APT, cyber spies and criminals, foreign intelligence, wire transfer fraud, poor software development methods, malware, botnets, third-party business partners, vendors, malicious insiders, underfunded IT, etc.
- Securing "data" and "processes" from cyber attack must be one of your highest priorities — the "network" cannot be secured.
 - Threats emanate from both internal and external sources, so don't forget about an insider threat program
- Knowledge of what attackers are doing must inform your defenses:
 - Anticipate that certain attacks will occur – prepare for them now.
 - Malware has developed to the point that it enables attackers to monetize their botnets and steal valuable IP.
 - Weaponized malware now enables governments to use cyber capabilities to produce desired effects in the physical world.
 - Terrorists will have these capabilities in the future.
- Users are key — they are both the primary target and the first line of defense.
- New strategies require strong governance.

34

Challenges others are facing

Assess whether such challenges exist and begin working on them as soon as possible



Cultural

- Establishing and maintaining a sense of urgency
 - Effective remediation is a marathon, not a sprint
 - Combating false sense of security that stagnates improvement (e.g., we have ABC tools)
- Working through a change-resistant culture
 - Negative IT/Information Security reputation and/or perceived as not relevant to business
 - Difficult to establish rapid changes
 - Long lead time to establish new policies
 - Long test and approval cycle to implement end-point or infrastructure changes
- Coordinating across the enterprise
 - Silos of asset ownership
 - Competing projects/demands
- Setting effective staffing and resource levels
 - Resistance to increased headcount in IT or information security
 - No history of outsourcing or co-sourcing key responsibilities

35

Challenges others are facing

Assess whether such challenges exist and begin working on them as soon as possible



Technical

- Gaps in ability to deploy software and patches across the enterprise
- Network bandwidth limitations
- Legacy operating systems and hardware
- Poor documentation of service/application account ownership and life cycle management
- Poor asset inventory and management system

Other

- No intellectual property/crown jewel inventory
- No formally established incident response capability
- No CISO or single point of focus for cybersecurity
- European Works Council notification/approval time lines
- Ineffective project management practices
- Finalizing terms and conditions with vendors/procurement



36



Thank You!

Chip Wentz
 Ernst & Young
 Executive Director
 Raleigh, NC

Phone: +1 (919) 349-4957
 E-Mail: chip.wentz@ey.com



Further information

- See the full report: **Under cyber attack: EY's Global Information Security Survey 2013**
on: www.ey.com/giss2013
- For further GRC thought leadership, please refer to our Insights on governance, risk and compliance series on: www.ey.com/GRCinsights






Want to learn more?

Security Operations Center expertise: From the cyberline to the boardroom
www.ey.com/oc

Beating cybercrime: Security Program Management
www.ey.com/spm

Privacy trends 2013: the global cross-border
www.ey.com/privacy2013

Mobile device security: understanding vulnerabilities and managing risk
www.ey.com/mobiledevice

Protecting and strengthening your brand: social media governance and strategy
www.ey.com/socialmedia

Information security as a borderless world: time for a rethink
www.ey.com/information_security

Identity and access management (IAM): beyond compliance
www.ey.com/iam

Bring your own device: security and risk considerations for your mobile device program
www.ey.com/bod

Key considerations for your internal audit: enhancing the risk assessment and addressing emerging risks
www.ey.com/audit

Please visit our *Insights on governance, risk and compliance series* at ey.com/GRCinsights
