

Managing New York State's Cyber Risks

A Pilot Program Between Agencies and OITS

Fran Reiter

Executive Deputy Director of
State Operations
New York State

Peter Bloniarz

Executive Director and
Senior Policy Advisor
NYS Cyber Security
Advisory Board

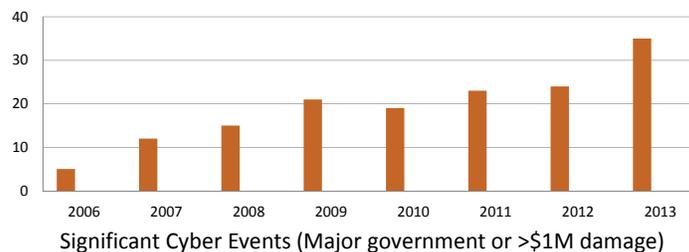
Deborah Snyder

Acting Chief Information
Security Officer
New York State

Today's Agenda

- Cyber Security: It's Everyone's Job
- Overview of Pilot Project
- Data Classification Overview
- Collaborative Approach
 - Success Factors & Challenges
 - Process
 - Next Steps
- Discussion & Questions

Cyber Incidents in 2013



- 43% growth in significant cyber events
- 91% growth in targeted attack campaigns
- 62% increase in number of breaches
- 500% increase in Ransomware attacks

Sources: Center for Strategic and International Studies, Verizon, Symantec

Some Relevant Examples

- **South Carolina tax department**, Fall 2012. 3.6M Social Security numbers; 387,000 credit card numbers; 800,000 companies. Est. \$20-50M.
- **Edward Snowden**, June 2013. Confidential NSA documents.
- **JP Morgan Chase**, December 2013. Account info for unemployment and social service benefits. 450,000 in U.S., 40,000 in New York.
- **Montana public health department**, May 2014. Up to 1.3M personal records, including health care and bank account information.
- **Federal Office of Personnel Management**, March 2014. Alleged target: Employees who have applied for top-secret security clearances.

Characteristics of breaches

- In 66%, the breach wasn't discovered for months or years.
- 69% were identified by a third party.
- 22% took months to remediate.
- Antivirus only catches 45%.
- Targeted:
 - Pick targets and relentlessly push
 - Look for weakest link in chain and go from there
- Opportunistic:
 - Attempt to break into multiple targets
 - Exploit vulnerable targets

Who's behind cyber attacks?

- Other nations & organized terrorist groups
- Large and small crime cells, with distribution networks
- Activists
 - Anonymous, Lulzsec
 - Chelsea Manning
 - Edward Snowden



New York's Risk

- New York State government information, especially Personally Identifiable Information
- Disruption to NYS government operations
- Impact on NYS public and private sectors
 - Est: \$5-10B GDP, 35,000 jobs
- Potential for damage to NYS Critical Infrastructures

Source: Center for Strategic and International Studies

Recommendations to Governor

- Adopt collaborative and resilient risk-based approach – OITS and Agencies
- “Know your data” – Prioritize protective efforts
- “Know your threats” – share information and intelligence
- Automate as much as possible
- Create a culture of cybersecurity – Oftentimes, human beings are the “weak link”
- Pay attention to supply chain
- Be prepared for cyber attacks

NIST Cybersecurity Framework

- **Identify**
Identification of assets, threats, and risks.
Governance and risk management strategy.
- **Protect**
Develop and implement appropriate safeguards.
- **Detect**
Detect the occurrence of a cyber security event.
- **Respond**
Take action after a detected cyber security event.
- **Recover**
Restore capabilities after an event.

Pilot Project on Cyber Risk Management: Objectives

- Improve the way New York State manages its cyber risks – collaborative and resilient
- Ensure that our policies and practices give all State agencies the tools they need to remain vigilant against cyber threats
- Immediate Goal: Discuss and validate the State's policies on information classification and control

Today's Agenda

- Cyber Security: It's Everyone's Job
- Overview of Pilot Project
- Data Classification Overview
- Collaborative Approach
 - Success Factors & Challenges
 - Process
 - Next Steps
- Discussion & Questions



Information Asset Classification
Jumping in Together...

Risk – Bad Things That Can Happen

- A laptop containing 100,000 confidential records is lost/stolen...
 - Property loss impact - \$2,000
 - Cost to mitigate event ~ \$18,000,000+
 - Operational cost of disclosure mailing ~ \$75,000
 - Impact on operations, resources
 - Impact on agency funding, additional regulatory oversight, penalties
 - Reputational impact - bad publicity, public perception

Risk – Bad Things That Can Happen

- An unscrupulous vendor steals 15,000 case files containing PPSI while making authorized repairs...
- Your agency web site is hacked taking it offline during critical high-volume business operations...
- A web application design error exposes confidential records of 65,000 individuals including minors...
- A user falls for a phishing scam, downloading malware that corrupts your critical databases...
 - Costs to investigate and mitigate
 - Reporting and costs to notify affected parties
 - Regulatory, financial and legal impact
 - Reputational impact - bad publicity, public trust

Risk Comes in Many Forms

- Is the situation any different if the device never leaves the building, but the data does?
- If the individual is an employee versus a vendor?
- If the data is on a flash drive, DVD or other forms of portable media?
- If the data is destroyed versus stole?
- If the data is on paper, rather than in electronic form?



Current Influencing Factors

- New business models and processes
- Critical dependencies on technology
- Growing threats (number and sophistication)
- “Environmental” risks
 - Inventory gaps
 - Unclear data ownership and classification
 - Aged, outdated systems
 - Poorly crafted and managed applications
 - Skills and resources
 - Data sprawl
 - External connections and 3rd party services

What Can We Do

- We can't protect against all threats
- A "Risk-based" approach is needed
 - Some information assets require more protection than others
 - Identify and prioritize events that could put data/systems at risk
 - Prioritize based on likelihood and impact
 - Implement controls to mitigate risk to acceptable levels
- Classification is a vital 1st step in protecting assets
 - Information is classified based on *criticality* (value to the business) and *sensitivity*



High-Level Process

Efficiently classifying information based on risk level identifies business-critical data and systems, and guides prioritizing security controls to protect these assets.

Identify

- **Inventory all information assets**



Classify

- **Classify by 3 principles: Confidentiality, Integrity and Availability (CIA)**
 - Business-driven process - requires data-owner knowledge and decision making
 - Each principle is categorized as "low," "moderate," or "high"
- **Assess business impact of security risk**
 - Consider information asset *criticality* (e.g., impairment of business functions, financial loss, non-compliance, legal exposure)
 - Consider data *sensitivity* (e.g., disclosure of PII)



Controls

- **Based on Classification**
 - Determine that appropriate administrative, physical and technical controls are in place to protect assets and mitigate risk



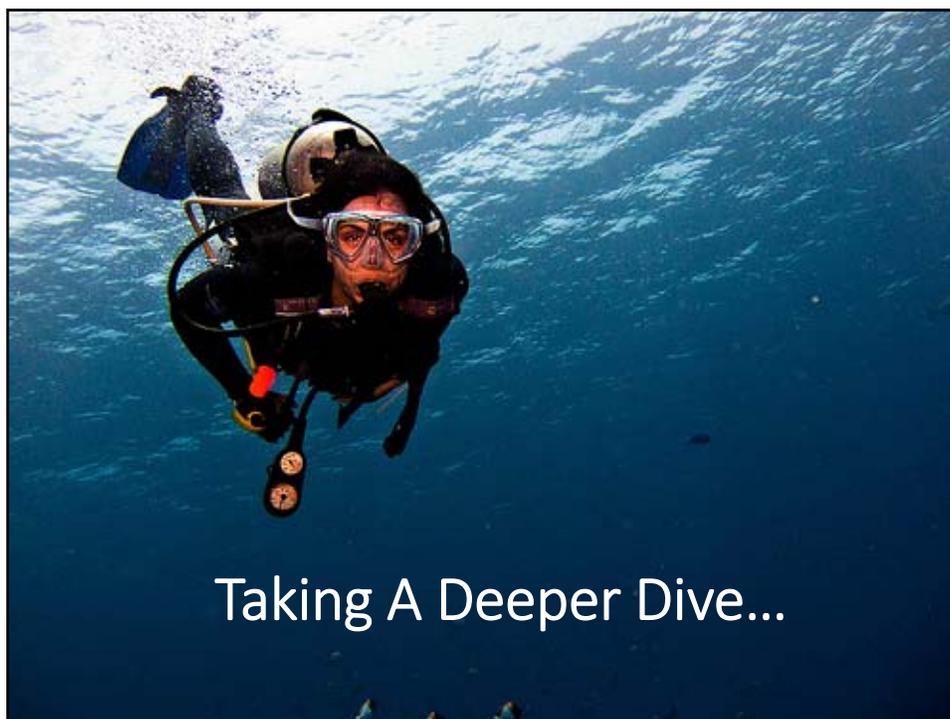
Key Take-Aways

- Understanding and managing threats to your information assets is a business risk management objective
- Classification helps protect your agency's valuable data and systems
- A risk-based, prioritized approach makes sense
- Understanding security-related risk is a critical part your overall risk management responsibilities

19

So, Where do We Stand?

AGENCY	2012 Annual NYS Policy Compliance Gap Assessment Report	2013 National Cyber Security Review (NCSR)
DPS	25%	Documented Policy/Standards
DOL	40%	Documented Policy/Standards
NYSP	49%	Risk Measured
OVS	75%	Risk Treated
DTF	95%	Documented Policy/Standards



Taking A Deeper Dive...

Success Factors

- Executive Sponsorship
- Business-led effort
- Education & Communication
- Risk-based approach
- Inventory visibility
- Methodology – Information Classification Standard
- Group & classify by type/category
- Consider information in all forms/life cycle phases
- Prioritize efforts – classify high-value assets 1st



High-Level Process

Efficiently classifying information based on risk level identifies business- critical data and systems, and guides prioritizing security controls to protect these assets.

Identify

- Inventory all information assets



Classify

- **Classify by 3 principles: Confidentiality, Integrity and Availability (CIA)**
 - Business -driven process - requires data-owner knowledge and decision making
 - Each principle is categorized as "low," "moderate," or "high"
- **Assess business impact of security risk**
 - Consider information asset *criticality* (e.g., impairment of business functions, financial loss, non-compliance, legal exposure)
 - Consider data *sensitivity* (e.g., disclosure of PII)



Controls

- **Based on Classification**
 - Determine that appropriate administrative, physical and technical controls are in place to protect assets and mitigate risk



Identify

Creating your Inventory

- Determine Asset Groups
- Identify:
 - Information Owners
 - Identify Custodian(s)
 - Identify Information Assets



Consider:

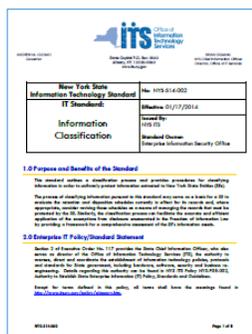
- Info in all forms/life cycle phases
- NYSARA & FOIL requirements
- Merged /data
- Meta data
- Reproductions
- 3rd Party data

The form is titled "INFORMATION ASSET IDENTIFICATION WORKSHEET" and contains a table with columns for "Asset Name", "Owner", "Custodian", "Classification", "Sensitivity", "Criticality", "Retention", and "Disposal". Below the table are sections for "Notes" and "Comments".

APENDIX C – Information Asset Identification Worksheet

Classify

- Follow Information Classification Standard (NYS-S14-002)
 - Classification scheme
 - Procedures
 - Baseline controls
- Group and prioritize assets
- Consider criticality and sensitivity
- Consider risks & business impact
- Use Templates & Tools available



<http://www.its.ny.gov/tables/technologypolicyindex.htm>

Classification Scheme

- Assessment determines if the business impact of risk events are **LOW**, **MODERATE** or **HIGH**

Questions cover 3 areas:

- Confidentiality – unauthorized disclosure
- Integrity – unauthorized modification or destruction
- Availability – no or unreliable access

	INFORMATION CLASSIFICATION CATEGORIES		
	LOW	MODERATE	HIGH
CONFIDENTIALITY Consider impact of unauthorized disclosure on factors such as: • Health and Safety • Financial Loss • SE • Mission/Programs • Public Trust	The unauthorized access or disclosure of information would have limited impact to the organization, its critical functions, workloads, business partners and/or its customers.	The unauthorized access or disclosure of information would have some impact to the organization, its critical functions, workloads, business partners and/or its customers.	The unauthorized access or disclosure of information would have a severe or catastrophic impact on the organization, its critical functions, workloads, business partners and/or its customers.
INTEGRITY Consider impact of unauthorized modification or destruction on factors such as: • Health and Safety • Financial Loss • SE • Mission/Programs • Public Trust	The unauthorized modification or destruction of information would have limited impact to the organization, its critical functions, workloads, business partners and/or its customers.	The unauthorized modification or destruction of information would have some impact to the organization, its critical functions, workloads, business partners and/or its customers.	The unauthorized modification or destruction of information would have a severe or catastrophic impact on the organization, its critical functions, workloads, business partners and/or its customers.
AVAILABILITY Consider impact of unavailability or unreliable access to information on factors such as: • Health and Safety • Financial Loss • SE • Mission/Programs • Public Trust	The alteration of access to or use of information would have limited impact to the organization, its critical functions, workloads, business partners and/or its customers.	The alteration of access to or use of information would have some impact to the organization, its critical functions, workloads, business partners and/or its customers.	The alteration of access to or use of information would have a severe or catastrophic impact on the organization, its critical functions, workloads, business partners and/or its customers.

Classification Decisions

- Information Owner – the individual in business/program area responsible for the data, determines classification

- Supported by Classification Team:
 - Executive Policy-Makers
 - Legal Counsel
 - FOIL Officer
 - Business Analysts
 - Chief Information Officer
 - Information Security Officer
 - Information Custodians



Potential Pitfalls

- Wrong players
- Restricted Scope
- Over-Classification
- Thinking it's an IT function

- Biting off too much...
- Not documenting rationale
- Failure to build classification in
- Failure to consider 3rd party risk
- Considering it "done"



Classification Toolkit



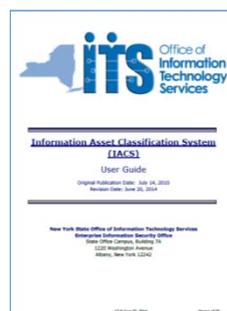
- Data Classification Overview
- Process training and support

- NYS Classification Standard NYS-S14-002
- NYS Information Security Controls Standard NYS-S14-003
- *Information Asset Classification Tool (IACS)*
- IACS General Info-Sheet & User Guide

- NYSARA guidance on Classifications for General and Disposition Schedules for Government Records

Information Asset Classification System (IACS)

- Secure web-based classification tool
- Automates the process
- Turbo-Tax-like feel - walks you through the classification questions
- ‘Traffic light’ display of classification
- Lists baseline controls to protect asset
- Control “gap analysis” feature
- Includes NYSARA classification templates for common record series



Controls

- Information Security Controls Standard (NYS-S14-003)
- Baseline controls to uniformly protect
 - Confidentiality
 - Integrity
 - Availability
- Easy-to-follow control charts
- Control explanations



New York State Information Technology Standard IT Standard	
Information Security Controls	No. NYS-S14-003 Effective: 01/17/2014 Issued By: ITS Standard Owner: New York State Information Security Office
1.0 Purpose and Benefits of the Standard The standard defines the baseline information security controls necessary to uniformly protect the confidentiality, integrity and availability of information processed by New York State.	
2.0 Executive IT Policy/Standard Statement Section 2 of Executive Order No. 177 provides for State Information Security. The Office of Information Technology Services, the authority in providing, operating and maintaining the information technology systems, policies, plans, and services of the State, regarding the security of the State's Information Technology (IT) Systems, Standard and Standard.	
3.0 Scope The standard is applicable to all staff and all other officials (e.g., contractors, vendors, other personnel) who have access to or manage State information.	
4.0 Information Statement	

<http://www.its.ny.gov/tables/technologypolicyindex.htm>

Now Let's Talk

- Share your past experiences...
- Best practices, pain points
- Data classification and risk management must be integrated and ongoing...
 - Requires on going commitment from the agency
 - It cannot be considered static...
 - It must be woven into business and IT processes
 - Requires risk awareness - cultural change





Cyber & Risk Management

- Industry forecast:
 - Heightened regulator and public expectations will cause increased cyber security concerns and focus.
- Global risk indexes:
 - Cyber risk jumped from 12th to 3rd place; squarely on the agenda for senior business leaders
 - Security also topped list of State CIO priorities
- Only 20% of executives are briefed frequently on cyber threats.
- Need to put business in a position of "KNOW"

Cybersecurity Framework

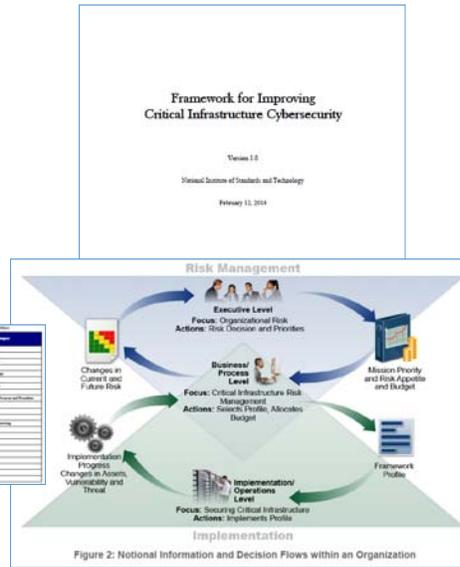
NIST Framework for Improving Critical Infrastructure Cybersecurity

5 Core Functions

- ✓ Identify
- ✓ Protect
- ✓ Detect
- ✓ Response
- ✓ Recovery



www.nist.gov/cyberframework/index.cfm



Risk Management Concepts

- **Risk Governance:** Strategic business function that helps ensure risk management activities align with business opportunity and loss capacity
- **Risk Appetite:** amount of risk an organization is willing to accept in the pursuit of its mission
- **Risk Tolerances:** acceptable level of variation allowed for a particular risk as organization pursues business objectives
- **Key Risk Indicators (KRIs):** Metrics that indicate risks, or high probability of risks that exceeds tolerances

<http://www.its.ny.gov/tables/technologypolicyindex.htm>



Next Steps

What you need to do...

- Identify and classify your information assets, following the State's Standards (Agency Cyber Risk Coordinators, Cluster CIOs, and ISOs)
- Provide feedback on the information classification standard and process.
- Watch for follow up meeting notice (2-3 wks out)

Contacts

Project Team Support

Peter Bloniarz
Peter.Bloniarz@exec.ny.gov
518.474.3522

Deb Snyder
Deborah.Snyder@its.ny.gov
518.242.5030

Nora Cronin
Nora.Cronin@dcjs.ny.gov
518.474.3522

Classification Support

NYS Enterprise Information
Security Office
iso@its.ny.gov
518.242.5200