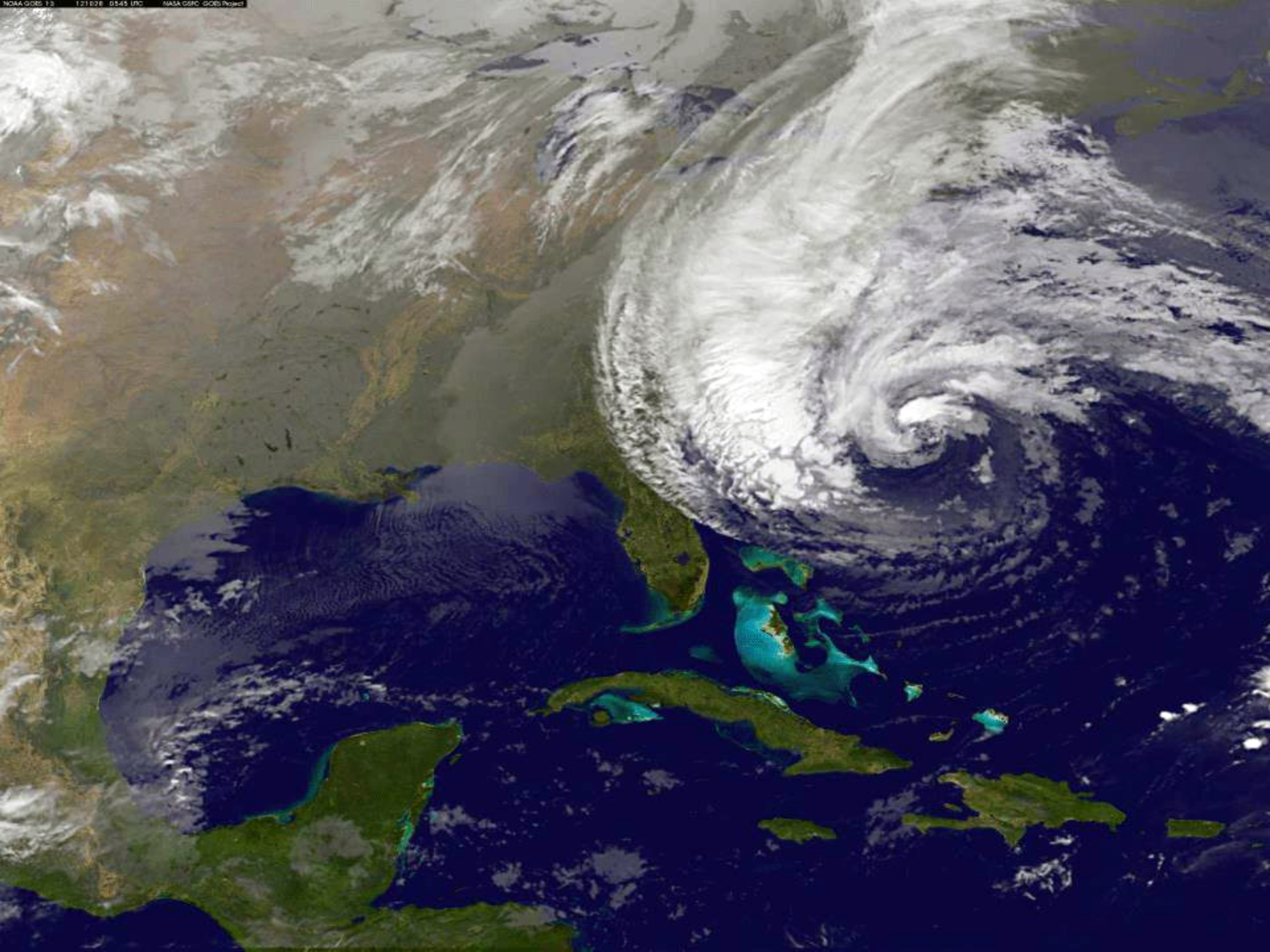
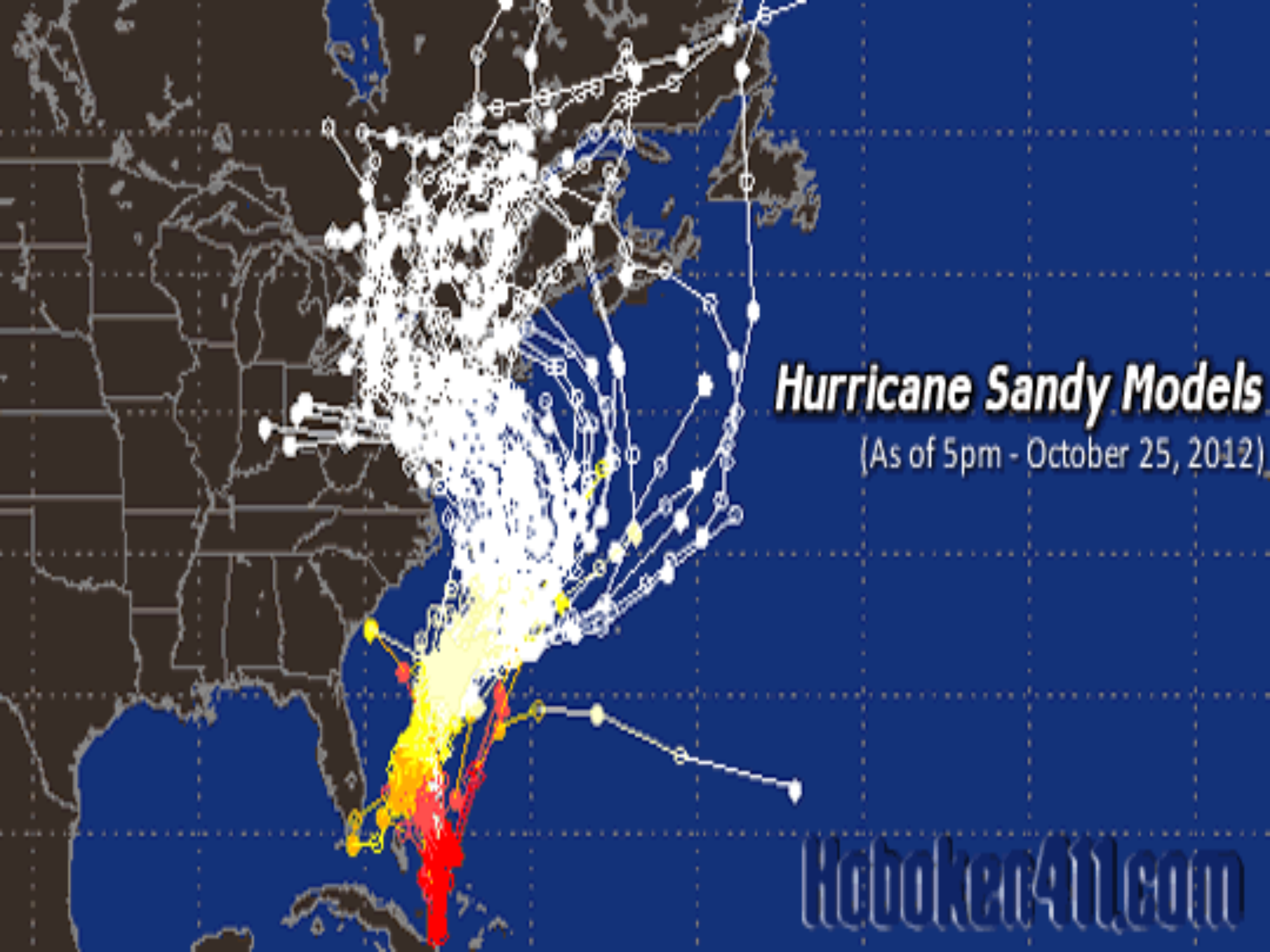
Information Security: part I

IT Partners 11/2013

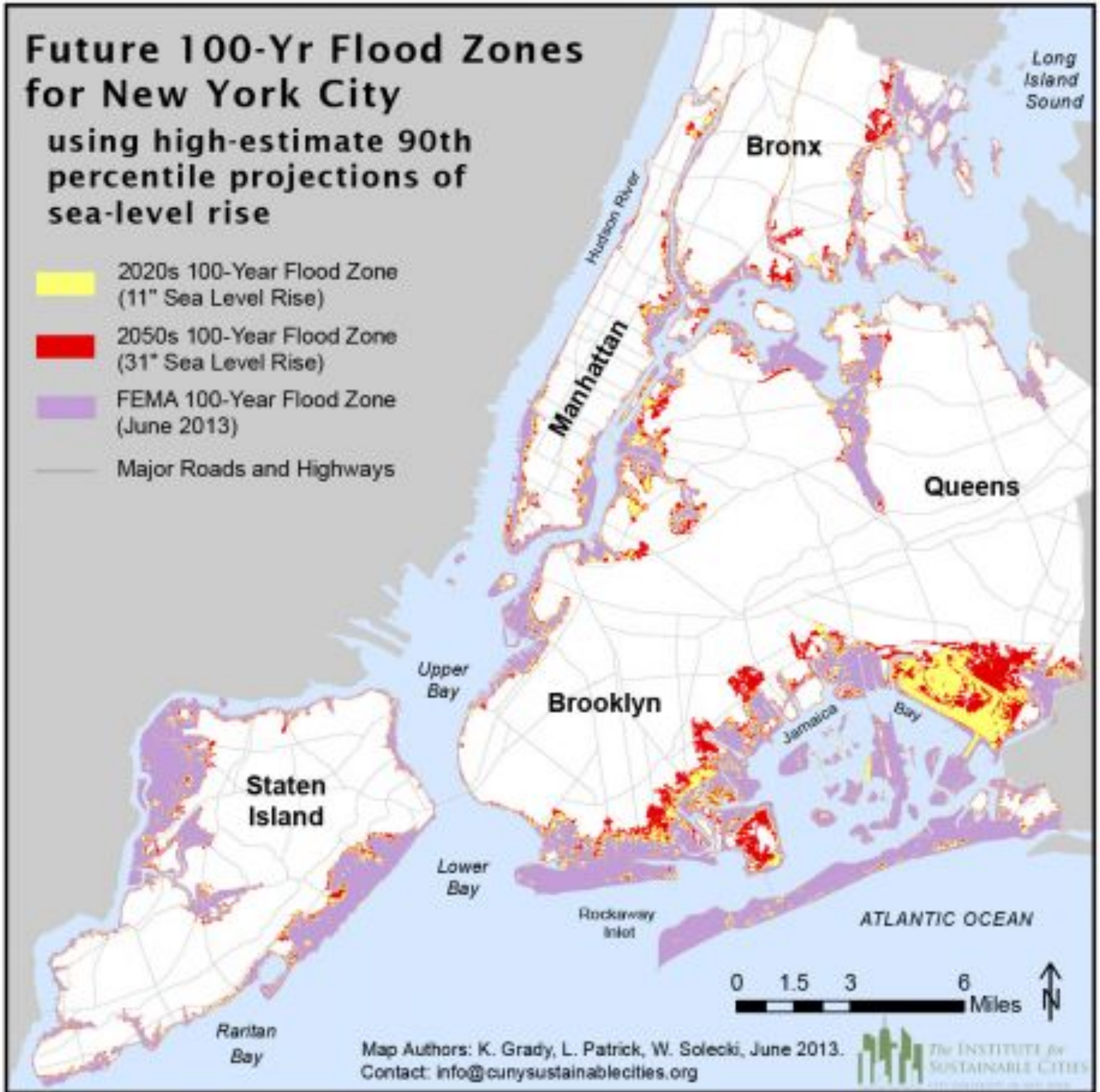

NOAA GOES 13
121028 0545 UTC
NASA GSFC GOES Project



Hurricane Sandy Models

(As of 5pm - October 25, 2012)

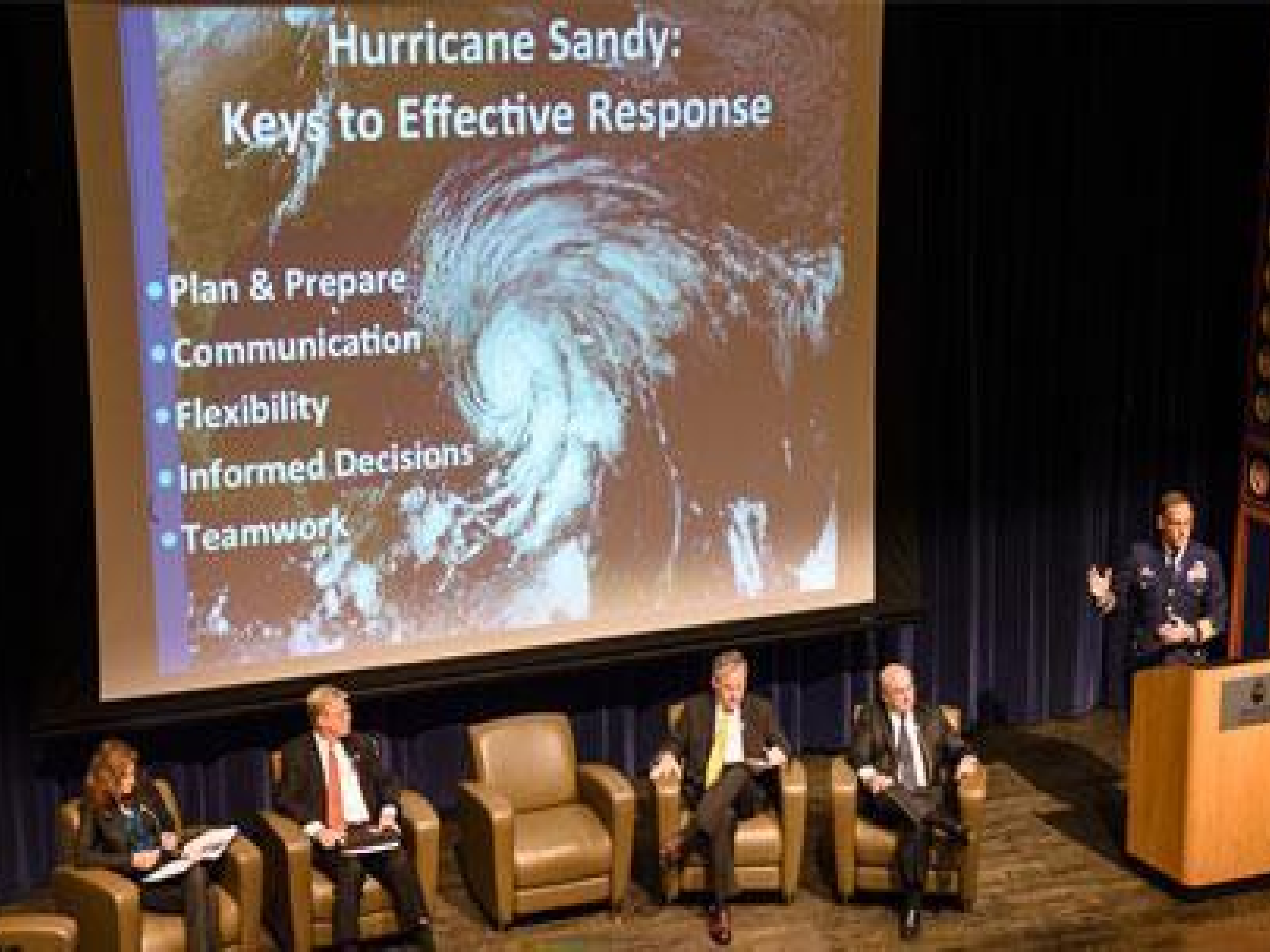
NYU



Future 100-Yr Flood Zones for New York City

using high-estimate 90th percentile projections of sea-level rise

Map Authors: K. Grady, L. Patrick, W. Solecki, June 2013.
Contact: info@cunysustainablecities.org



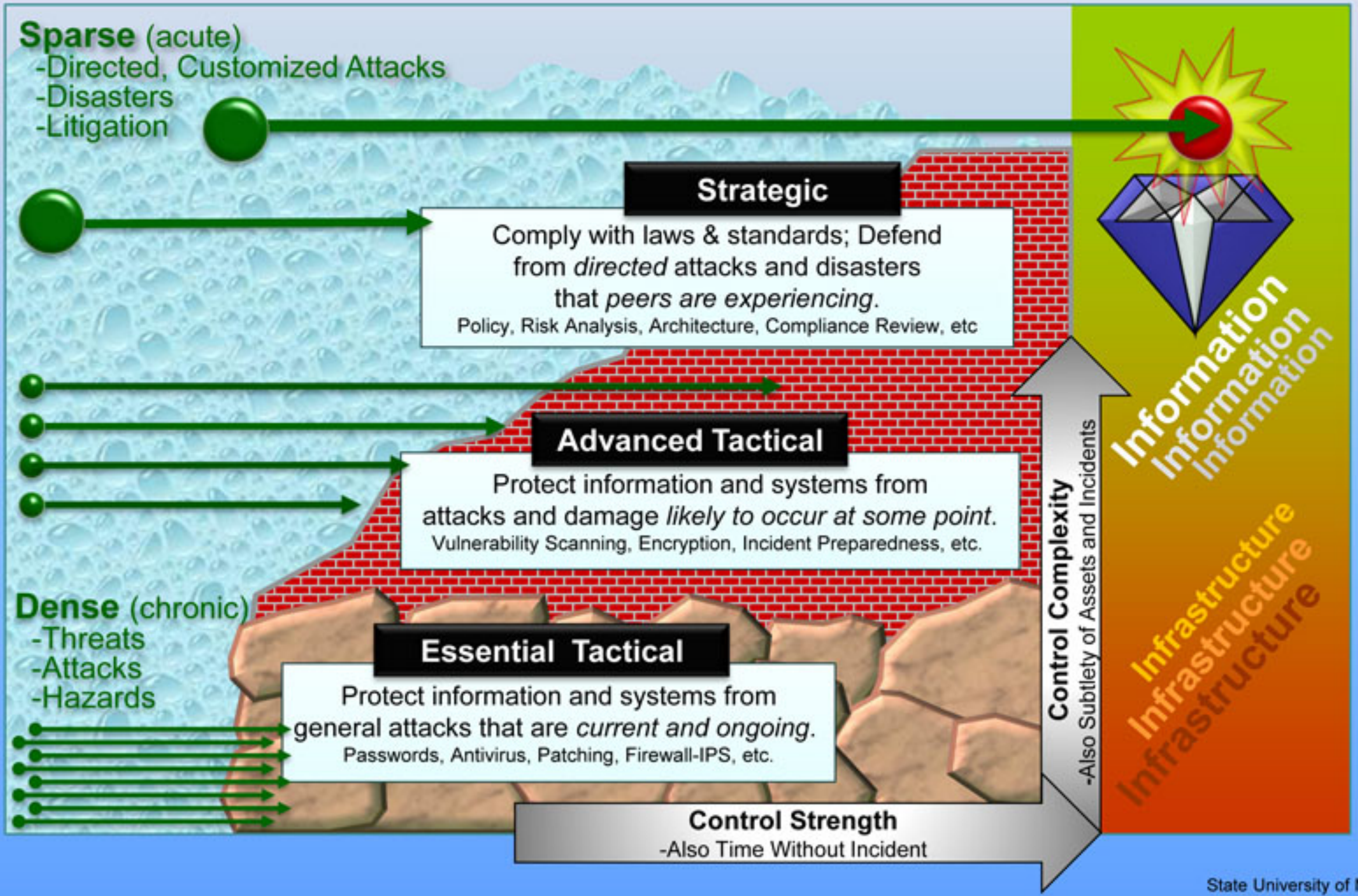
Hurricane Sandy:
Keys to Effective Response

- Plan & Prepare
- Communication
- Flexibility
- Informed Decisions
- Teamwork

Levee Model of Security

-Information Security's Layered Threats, Controls, and Assets

Threats Controls Assets



Sparse (acute)
-Directed, Customized Attacks
-Disasters
-Litigation

Dense (chronic)
-Threats
-Attacks
-Hazards

Strategic

Comply with laws & standards; Defend from *directed* attacks and disasters that *peers are experiencing*.

Policy, Risk Analysis, Architecture, Compliance Review, etc

Advanced Tactical

Protect information and systems from attacks and damage *likely to occur at some point*.

Vulnerability Scanning, Encryption, Incident Preparedness, etc.

Essential Tactical

Protect information and systems from general attacks that are *current and ongoing*.

Passwords, Antivirus, Patching, Firewall-IPS, etc.

Control Complexity
-Also Subtlety of Assets and Incidents

Control Strength
-Also Time Without Incident

State University of New York
Office of Information Security

Is it Time for Such an Epiphany at Stony Brook?

Is SBU following best practices?

Do we have appropriate policies?

Does everyone understand their responsibility?

Do we have adequate training? Is it mandatory?

Do we conduct security reviews?

Do we have the appropriate tools in place to protect our assets?

When the tools we have show problems to we follow up in a timely manner?

Is assessing security part of our culture?

Is SBU following best practices?

- Do we continually review and tune our practices to respond to changing threats?
- Do we have the data to determine how effective we are?
- Have our efforts to secure data kept pace with the rising threat profile?   Or, are we falling behind?
- Are we compliant with standards and best practices

What does the Data Show?

GLOBAL DATAGUARD POC

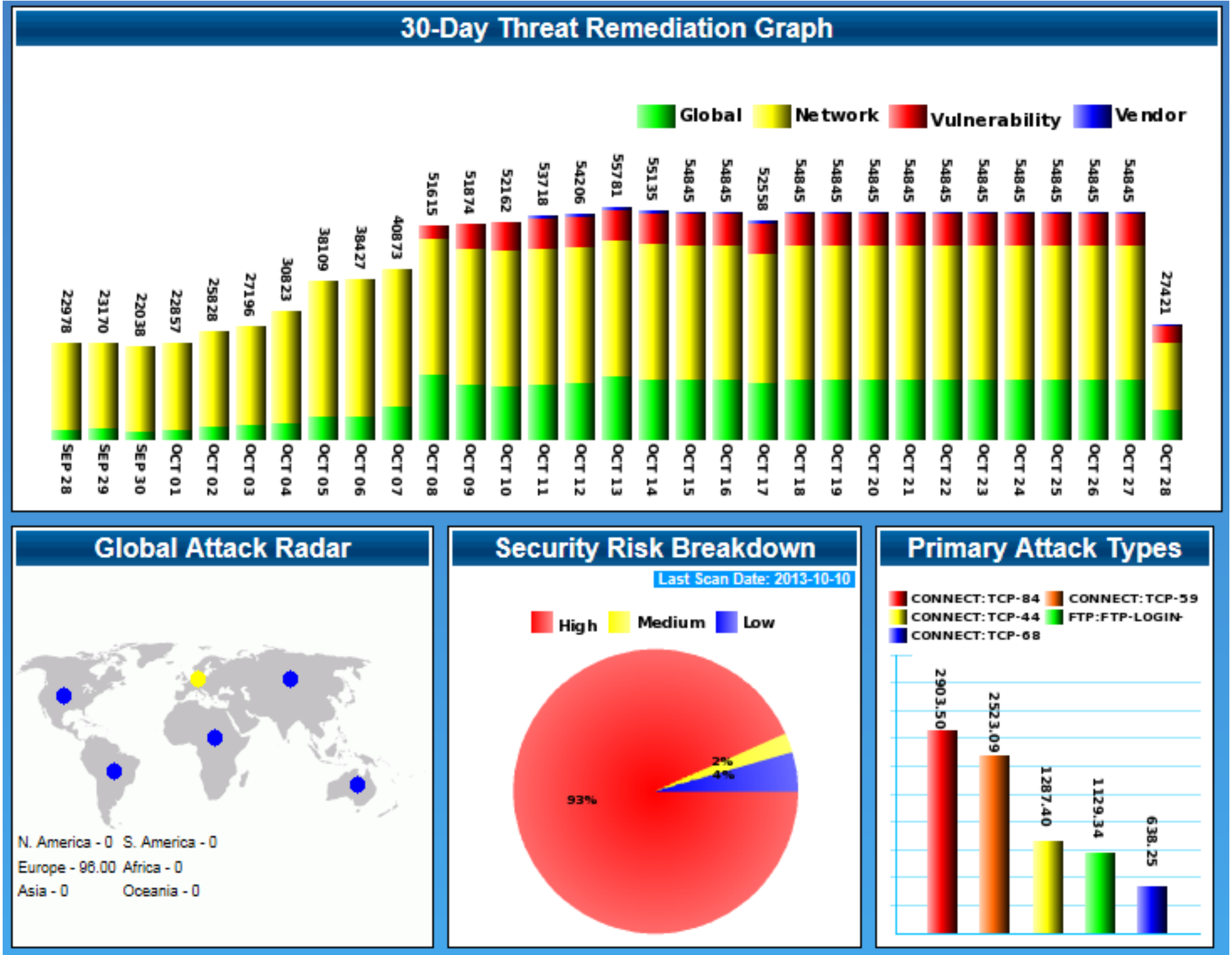
Global Dataguard is a managed service and security company that offers out of band solutions to accomplish and correlate the following:

- Scheduled/Automated Vulnerability Scans
- Network Behavior Analysis
- Log Centralization
- Signature Based IDS/IPS
- 24/7 Managed Service that evaluates collected data and prepares custom alerts/reports for internal consideration and action.

Global DataGuard
Unified Security Anywhere™

WHAT DOES THE DATA SHOW?

WE ARE BEING TARGETED.



30-Day Threat Remediation Graph

Global Attack Radar

N. America - 0 S. America - 0

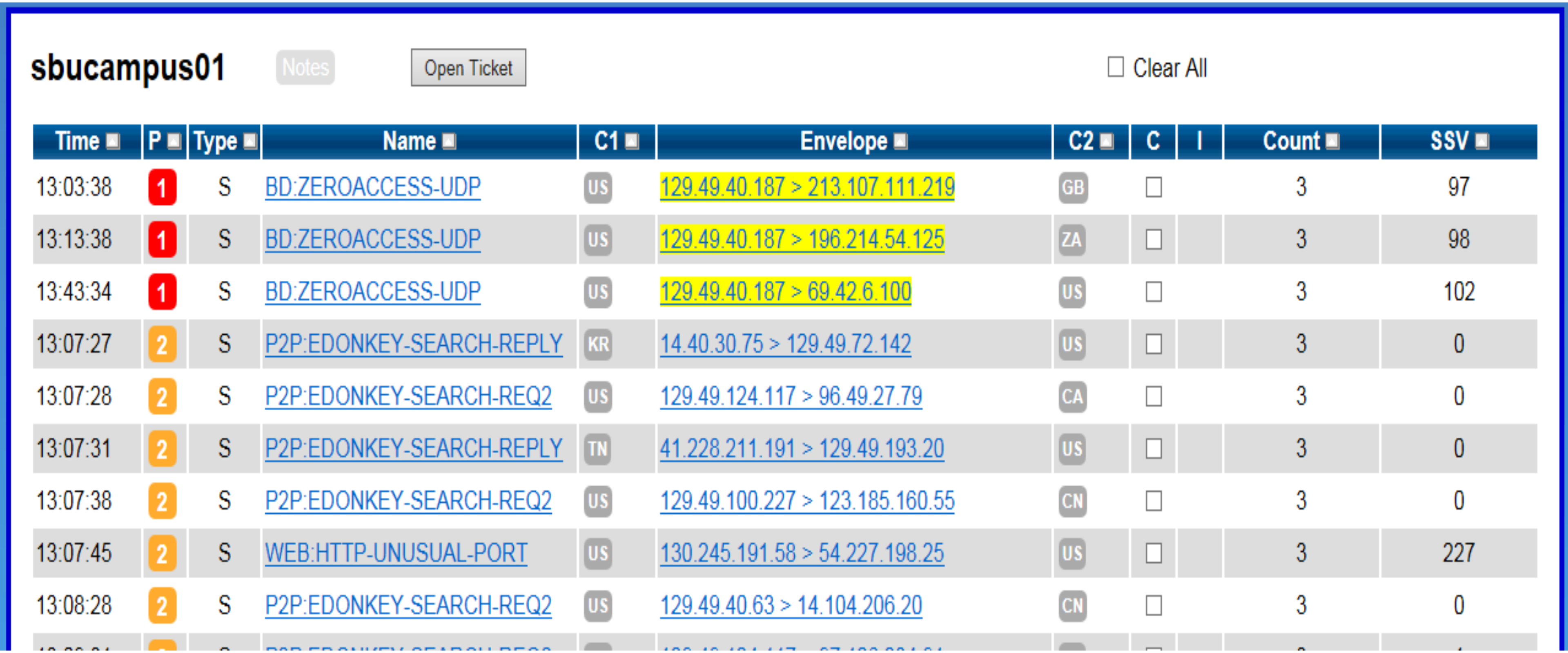
Europe - 96.00 Africa - 0

Asia - 0 Oceania - 0

Security Risk Breakdown

Last Scan Date: 2013-10-10

Primary Attack Types

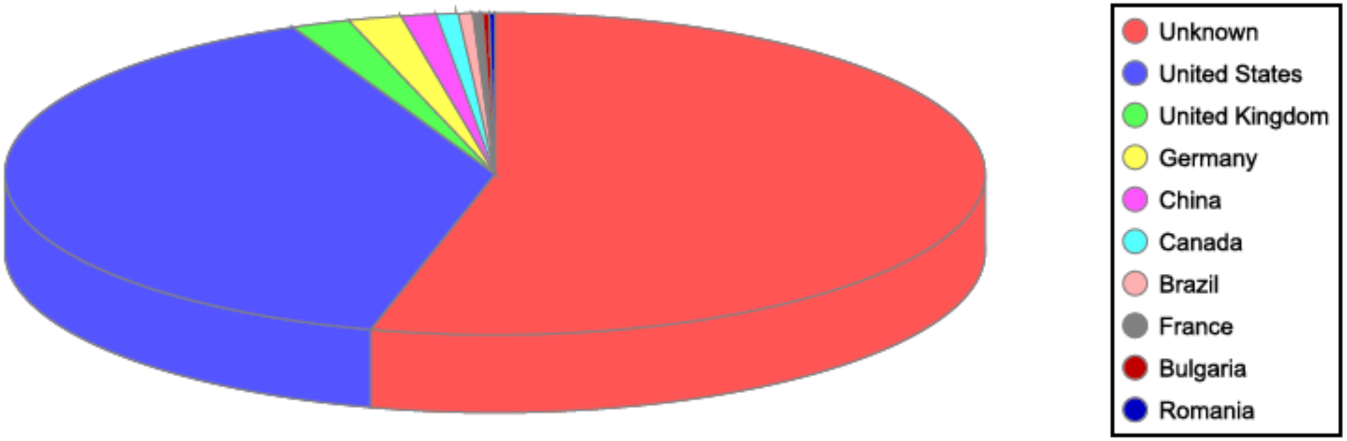


sbucampus01 Notes Open Ticket □ Clear All

Time	P	Type	Name	C1	Envelope	C2	C	I	Count	SSV
13:03:38	1	S	BD:ZEROACCESS-UDP	US	129.49.40.187 > 213.107.111.219	GB	□		3	97
13:13:38	1	S	BD:ZEROACCESS-UDP	US	129.49.40.187 > 196.214.54.125	ZA	□		3	98
13:43:34	1	S	BD:ZEROACCESS-UDP	US	129.49.40.187 > 69.42.6.100	US	□		3	102
13:07:27	2	S	P2P:EDONKEY-SEARCH-REPLY	KR	14.40.30.75 > 129.49.72.142	US	□		3	0
13:07:28	2	S	P2P:EDONKEY-SEARCH-REQ2	US	129.49.124.117 > 96.49.27.79	CA	□		3	0
13:07:31	2	S	P2P:EDONKEY-SEARCH-REPLY	TN	41.228.211.191 > 129.49.193.20	US	□		3	0
13:07:38	2	S	P2P:EDONKEY-SEARCH-REQ2	US	129.49.100.227 > 123.185.160.55	CN	□		3	0
13:07:45	2	S	WEB:HTTP-UNUSUAL-PORT	US	130.245.191.58 > 54.227.198.25	US	□		3	227
13:08:28	2	S	P2P:EDONKEY-SEARCH-REQ2	US	129.49.40.63 > 14.104.206.20	CN	□		3	0

Top Attacks by Country

Start Time:	Oct 25, 2013 12:00:00 AM EDT	End Time:	Oct 31, 2013 11:30:55 AM EDT
Action Type:	All	Severity:	All
Description:		Other:	All search criteria are in summary page



No.	Country Name	Hit Cou
1	Unknown	21,523,9
2	United States	15,585,3
3	United Kingdom	765,2
4	Germany	699,5
5	China	459,8
6	Canada	284,9
7	Brazil	187,4
8	France	124,0
9	Bulgaria	88,1
10	Romania	75,5

WHAT DOES THE DATA SHOW? WE ARE MAKING PROGRESS

- In a short period of time, this information has proved valuable.
  - Client Support and IT Partners have been working to help us locate and remediate infected machines.
    - On September 18th, the top ten offenders on the 129.49.x.x network generated 183,545 hits on our existing IPS. The same report on October 18th generated "only" 16,591 hits.
  - Networking has assisted in shutting off network access to breached computers when necessary.
    - Repeat offenders and computers that can not be located are being disabled.
  - Armed with the data GDG supplied, we are exploring how to better utilize some existing tools.
    - For example, previously we were seeing on average about 500,000 RDP successful alerts per day. It has now dropped to around 150,000 per day.

We still have much work to do

So, What is DoIT Doing to Address the threats? Planning

- Developed a three year plan to improve security
  - Policies
  - Procedures
  - Practices
  - Infrastructure
- Presented it as a Project 50 Forward Project

So, What is DoIT Doing to Improve security?

- Information Security, Client Support, Systems and Data Network Services are working together to:
  - Intervene on particular threats
  - Examine security practices
  - Better use existing tools
  - Rethink how we do business

Stony Brook University

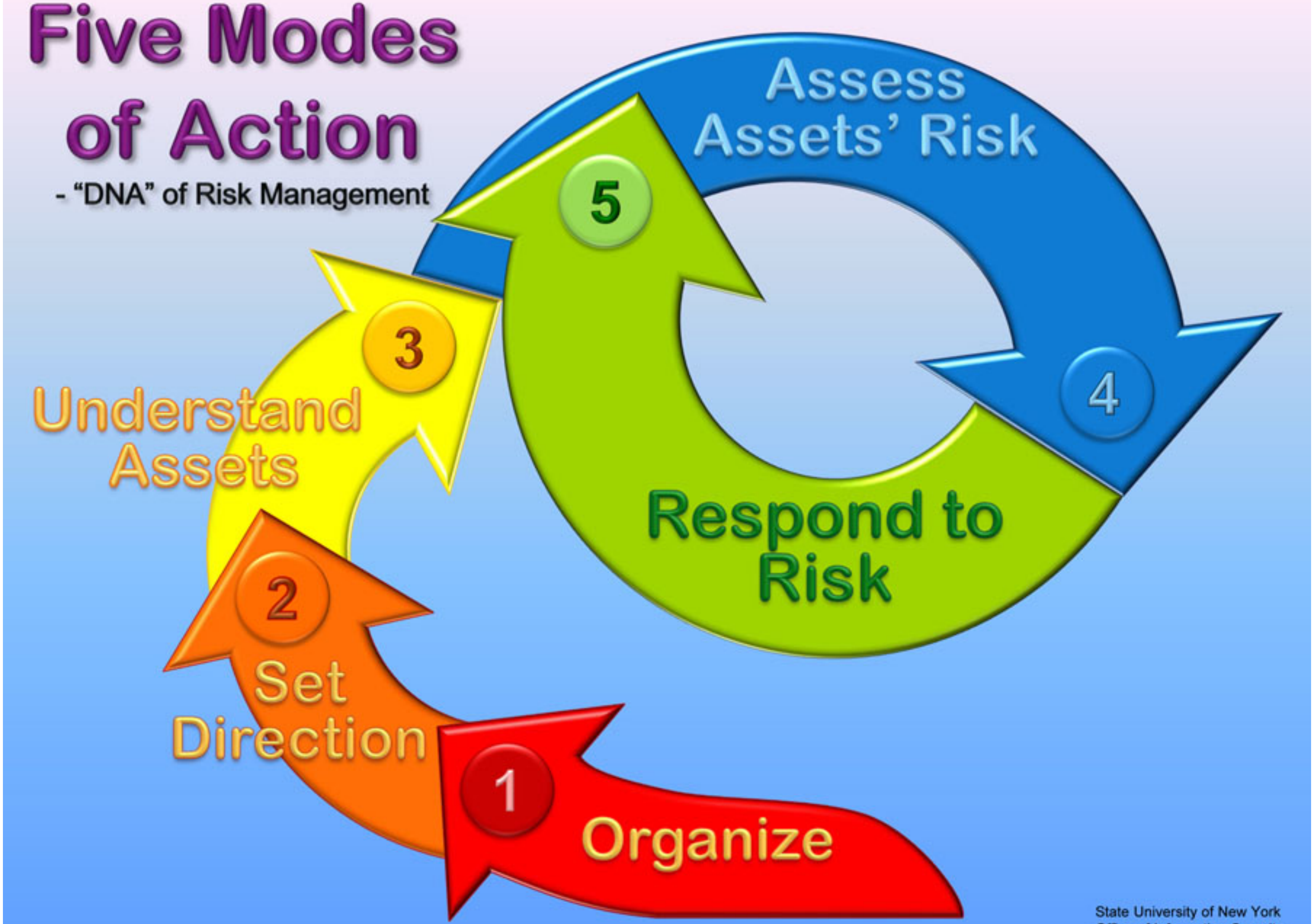
Division *of* Information Technology

Some closing thoughts

- Security is everyone’s responsibility
- Those of you who manage systems must take special precautions to assure that the data on your systems are protected.
- Assume that there are no institutional safeguards in place to protect your data.
- Any safeguards that are put in place will then provide defense in depth
- Remember that security is a process not a product.

Five Modes of Action

- "DNA" of Risk Management



1 Organize

2 Set Direction

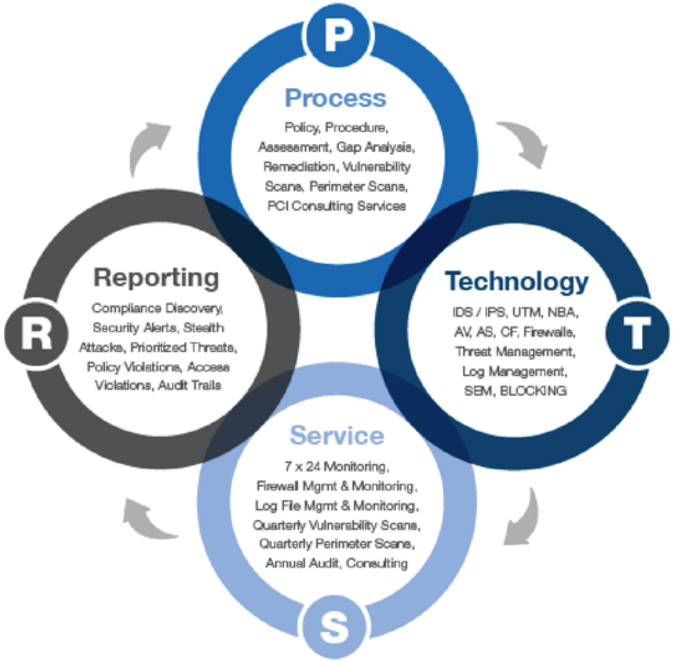
3 Understand Assets

4 Assess Assets' Risk

5 Respond to Risk

State University of New York
Office of Information Security

SECURITY IS A PROCESS



P

Process

Policy, Procedure, Assessment, Gap Analysis, Remediation, Vulnerability Scans, Perimeter Scans, PCI Consulting Services

T

Technology

IDS / IPS, UTM, NBA, AV, AS, CF, Firewalls, Threat Management, Log Management, SEM, BLOCKING

S

Service

7 x 24 Monitoring, Firewall Mgmt & Monitoring, Log File Mgmt & Monitoring, Quarterly Vulnerability Scans, Quarterly Perimeter Scans, Annual Audit, Consulting

R

Reporting

Compliance Discovery, Security Alerts, Stealth Attacks, Prioritized Threats, Policy Violations, Access Violations, Audit Trails

Information Security Contact Details

- Shared Mailbox:
  - Information_security@stonybrook.edu
- E-mail Group
  - Doit_Security@stonybrook.edu

- Philip Doesschate
  - philip.doesschate@stonybrook.edu
  - (631) 632-6238
    - Eric Johnfelt
      - eric.johnfelt@stonybrook.edu
      - (631) 632-9939
    - Matthew Nappi
      - matthew.nappi@stonybrook.edu
      - (631) 632-4856
    - Mark Velazquez
      - mark.velazquez@stonybrook.edu