Disaster Recovery Journal
Fall World
San Diego, California — 2014

Disaster Recovery Journal
Fall World
San Diego, California — 2014

Cyberwise CP

# Business Continuity for Cyber Threat

Hands on Workshop to Build and Exercise Cyber Contingency Examples

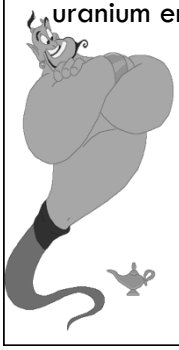
September 7, 2014
Workshop Session #5
1:00 – 3:30 PM

Susan Rogers, MBCP, MBCI
Cyberwise CP




## What happens when a computer program can activate physical machinery?

Between 2009-2010 the Stuxnet cyberweapon is estimated to have destroyed 1,000 Iranian nuclear-fuel centrifuges at the Natanz uranium enrichment plant.




2014, Telsa Model S car hacked in Chinese security contest. Students able to make car doors & sun roof pop open & head lights turn on while the car is in motion.

## Future Cyber Protection..

### Internet of Things (IoT)

- Where objects or people are provided with unique identifiers that can transfer data over a network without human interaction.
- Technology: wireless, micro-electromechanical systems (MEMS) and the internet

http://www.cisco.com/web/tomorrow-starts-here/anthem/index.html

### Medical Device Security

- An increased vulnerability to malware attacks and potential to serve as an entry point for attacks into the trusted network
- A risk to patient safety and protection of patient sensitive information

## Cyber Threat to Critical Infrastructure

Richard Clarke tells *Fresh Air* host Terry Gross.
former Counter Terrorism Chief under Presidents Clinton and Bush





# Agenda & Goals

**Part 1** **NIST Cybersecurity Critical Infrastructure Framework and other standards…**

*(1:00 – 1:30)*

**Part 2** **Cyber Event Exercise Team Work**

- Teams presented with crisis scenario
- Debate ramifications of cyber event
- Identify cyber threat joint planning (internal & third party)
- Identify function-based contingency activities

*(1:30 – 2:30)*

**Part 3** **Share Team Results**

- Cyber specific contingency planning
- Critical success factors: challenges & key stakeholders

*(2:30 – 3:30)*

# Part I - Framework

## NIST Cybersecurity Risk Framework For Critical Infrastructure

NIST Risk Framework

Mapping BC Process

Motivation to Adopt

# Framework to Motivate Market Interests

| 2/12/2013 U.S. **Presidential policy & Executive Order** signed to enhance Cyber security Critical Infrastructure (CI) Protection | **DHS & NIST** charged to work with private sector to build voluntary standards & practices to increase cyber protection of CI | **Cyber Framework Workshops** open to the public produce: 1) Risk framework 2) Basic activities 3) Gaps to close 4) Incentives | **Entrepreneurs & business encouraged** to deploy the framework and bring innovation to close gaps | **Breach, Threat Motivation** 2013-2014 breach, threats have created and environment of urgency to strengthen CI and third party cyber controls |
|---|---|---|---|---|

# Value of a Risk Framework

1. Cyber risk = Emerging Enterprise Risk
2. Baseline activities to strengthen critical infrastructure
3. Integrate into risk & vendor management practices


NIST Cybersecurity Risk Framework

http://www.nist.gov/cyberframework/index.cfm


COSO ERM

ITIL®

FFIEC

AICPA-Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports

# NIST Framework

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| IDENTIFY (ID) | **Asset Management (AM):** The personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. | **ID.AM-1**: Physical devices and systems within the organization are inventoried | • **ISA 99.02.01** 4.2.3.4<br>• **COBIT** BAI03.04, BAI09.01, BAI09, BAI09.05<br>• **ISO/IEC 27001** A.7.1.1, A.7.1.2<br>• **NIST SP 800-53 Rev. 4** CM-8<br>• **CCS CSC**1 |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | • **ISA 99.02.01** 4.2.3.4<br>• **COBIT** BAI03.04, BAI09.01, BAI09, BAI09.05<br>• **ISO/IEC 27001** A.7.1.1, A.7.1.2<br>• **NIST SP 800-53 Rev. 4** CM-8<br>• **CCS CSC** 2 |
| | | **ID.AM-3:** The organizational communication and data flow is mapped | • **ISA 99.02.01** 4.2.3.4<br>• **COBIT** DSS05.02<br>• **ISO/IEC 27001** A.7.1.1<br>• **NIST SP 800-53 Rev. 4** CA-3, CM-8, CA-9 |

# Motivation to Adopt NIST Cybersecurity Framework & Third Party Controls

| Viewpoint | |
|---|---|
| Critical Infrastructure | ✔ |
| Coordinating Councils | ✔ |
| Law Firms | ✔ |
| Insurance Co. | ✔ |
| Auditors | ✔ |
| Technology / Consultants | ✔ |
| Regulators | ✔ |
| Vendors | ✔ |
| Security Firms | ✔ |
| Regulated Entities | ✔ |
| Regulators | ✔ |
| Education | ✔ |

"The FINRA assessment addresses a number of areas related to cybersecurity, including firms': business continuity plans in case of a cyber-attack"




# Business Continuity Messages

SUSTAIN CONTROL QUALITY

Business Continuity activities are updated annually and can be used to improve & sustain the quality of cybersecurity controls.

A PROVEN PROCESS

BC Engages critical stakeholders, therefore can be a platform to expand cybersecurity activities and education.

TEAM APPROACH

Cybersecurity needs a team approach: Info Sec, HR, Risk Mgmt., BC, DR, Physical Security, Critical Business, IT, Infrastructure etc. BC engages all teams for crisis response.

# BC Activities that Engage Stakeholders

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | AM | Asset Management |
| | | BE | Business Environment |
| | | GV | Governance |
| | | RA | Risk Assessment |
| | | RM | Risk Management |
| PR | Protect | AC | Access Control |
| | | AT | Awareness and Training |
| | | DS | Data Security |
| | | IP | Information Protection Processes and Procedures |
| | | PT | Protective Technology |
| DE | Detect | AE | Anomalies and Events |
| | | CM | Security Continuous Monitoring |
| | | DP | Detection Processes |
| RS | Respond | CO | Communications |
| | | AN | Analysis |
| | | MI | Mitigation |
| | | IM | Improvements |
| RC | Recover | RP | Recovery Planning |
| | | IM | Improvements |
| | | CO | Communications |

BC Actions for Cyber

- BIA identify critical assets & process
- BIA identifies impact
- Existing governance engages all LOB
- Include in RCSA –risk control self assessment
- Identifies Critical staff to build contingency plans
- RTO, prioritize systems, business & vital records
- Leverage DR vendor & 3rd party assessment/exercise
- Leverage DR system mapping, interdependencies
- Existing crisis command with business triggers
- Expand crisis communication
- Business & Vendor Contingency plans

# NIST Mapping for BC Process & Controls

BC Actions for Cyber

| Function | Category | Sub-Category | BC Support Process |
|---|---|---|---|
| **IDENTIFY** | Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | Business units include cyber threat in their risk assessment, with the intent to identify areas of contingency planning. |
| | | ID.RA-6: Risk responses are identified and prioritized | Business units identify their processes and assets that are high risk based on cyber threat actor motivation. |
| | Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders | Results of risk assessments are aggregated, and approved by senior leadership. |
| | | ID.RM-2: Organizational risk tolerance is determined and clearly expressed | An organization's risk tolerance includes funding and approval of technology and business contingency planning activities that will reduce impact of cyber threat. |
| | | ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | The organization will meet their Regulator, and Customer's level of standards and practices for information security, business continuity and vendor management. |

# Lessons Learned From DDOS Attacks

BC Actions for Cyber

| Feedback from Financial Industry | BC Planning Takeaway |
|---|---|
| Break Down Silos - There is a need to bring all together to address cyber, physical impact: business teams, fraud, BC, Incident response, corporate messaging. | Tech + Business Incident Command |
| Need to adapt and respond to cyber impact quickly. | Cyber based tabletop exercises<br>Expand BC & Incident response plans |
| During crisis response, decision making cannot be done by committee. | Incident command to define: roles, activities & decision authority |
| During an attack you need to know what is normal versus and abnormal impact to critical assets. | Identify critical asset thresholds<br>Crisis monitoring & anomaly detection reporting |
| Prioritize business & customer impact and identify actions that will be taken in worst case or poor scenarios. | Extreme case scenario planning |

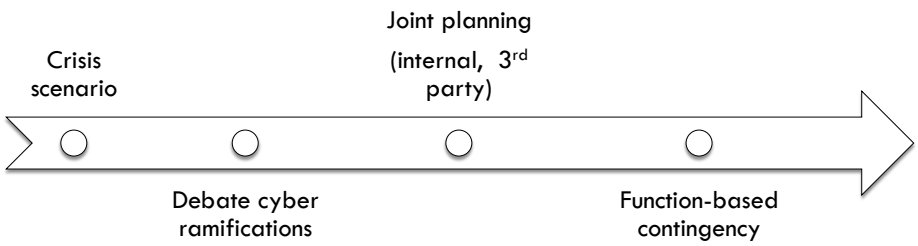
# Lessons Learned From Cyber Exercises

BC Actions for Cyber

| Cyber Exercise After Action Report | BC Planning Takeaway |
|---|---|
| Enhance response playbook to better account for a industry specific incident with the goal of strengthening the integration between industry groups. | Sector & enterprise playbooks |
| Improve coordination between business and technology leaders during cyber incident analysis and response. | Tech + Business Incident Command |
| Enhance the role of exchanges, clearing firms, and trusted government partners in cyber incident response and crisis management. | Formalize 3rd party & government crisis routines |
| Augment existing guidelines and decision frameworks to determine if cyber incidents are systemic in nature. | Crisis monitoring reporting |
| Institutionalize procedures for market open/close decisions during times of cyber incident response & crisis. | Procedures for worst case scenario BC Plannng |

# Part II

## Cyber Event Exercise Team Work



# Cyber Threat Assessment

**Threat Source**

- Nation States
- Terrorists
- Economic Espionage
- Criminals
- Activists/Hacktivists
- External Opportunists
- Insiders

**What We Can Do**

1. Join ISAC
2. Think like a bad guy
   - Learn how they act; motivation
   - Your assets they will target
3. Educate Business…add more eyes over process & controls

There are 18 Critical Infrastructure sectors identified by DHS that facilitate: cyber education, information sharing and crisis response. ISAC – Information Sharing and Analysis Center.

Chemical Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

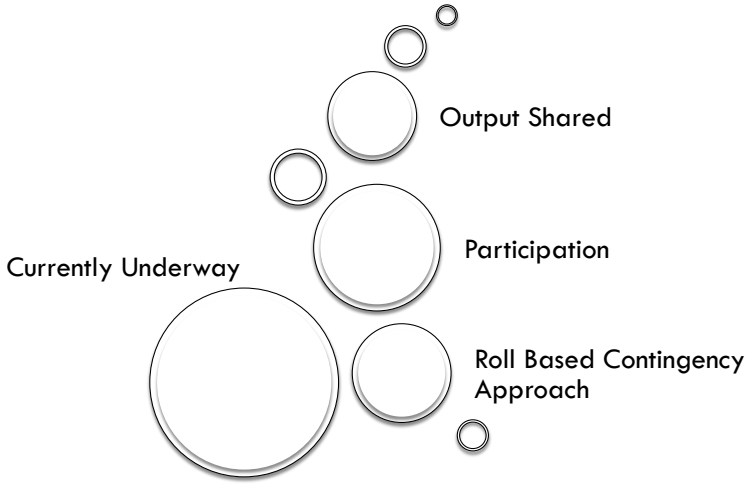
Financial Services Sector
The Department of Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Healthcare and Public Health Sector
The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Information Technology Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

# Cyber BC Planning Case Study

## Use Case: Cyber BC/DR Planning & Response

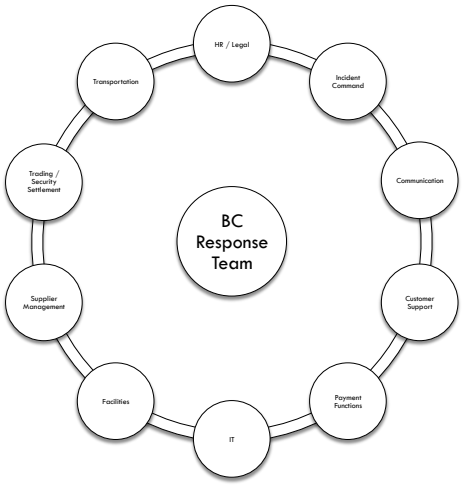


# Role Based Use Case Planning

Content Scope

Sample Use Case Questions:

- What can fail?
- What must I protect?
- What can I prepare today?
- What are biggest obstacles?




# Set the Stage


- ***Bipartisan Policy Center Convenes Former Senior Administration Officials to Respond to Simulated Cyber Attack.*** The simulation was created by former CIA Director General Michael Hayden and the BPC's National Security Preparedness Group, led by the co-chairs of the 9/11 Commission, Governor Thomas Kean and Congressman Lee Hamilton. Cyber ShockWave was developed in partnership with General Dynamics Advanced Information Systems, SMobile Systems, Southern Company, Georgetown University, and PayPal, with contributions from Symantec Corporation.
- https://www.youtube.com/watch?v=_kiIxSLDbzQ

## Cyber Exercise

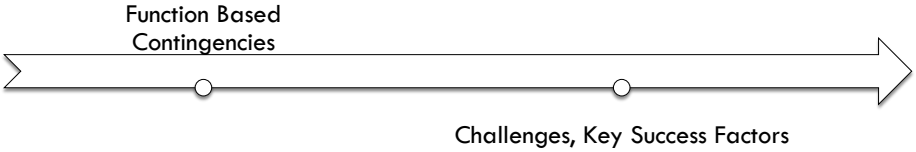
Content for this slide will be provided to participants during the DRJ exercise workshop

## Exercise Team Activities

Content for this slide will be provided to participants during the DRJ exercise workshop

# Part III

## Share Team Results




# BC Takeaways

"The NIST Cybersecurity Framework, however, is a bible without a preacher if there is no one at the company who is able to translate its concepts into action plans"

June 10, 2014,
SEC Chairman Aguilar
speaking at Board of Directors Conference

# Business Continuity Messages

SUSTAIN CONTROL QUALITY

Business Continuity activities are updated annually and can be used to improve & sustain the quality of cybersecurity controls.

A PROVEN PROCESS

BC Engages critical stakeholders, therefore can be a platform to expand cybersecurity activities and education.

TEAM APPROACH

Cybersecurity needs a team approach: Info Sec, HR, Risk Mgmt., BC, DR, Physical Security, Critical Business, IT, Infrastructure etc. BC engages all teams for crisis response.

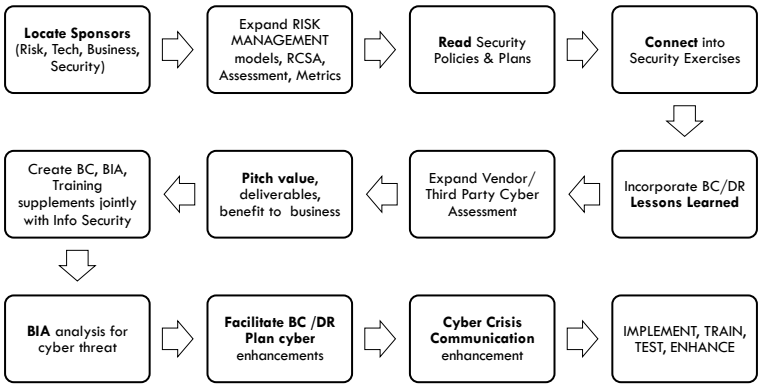
Cyberwise CP

# Cyber BC Action Plan

BC / DR

BC Planning Will help sustain Information Security Controls: expanding your annual BC Plan, BIA process, training and testing to include cyber threat contingency and communication concepts

Info Sec



# References & Resources


- The White House, Presidential Policy Directive -- Critical Infrastructure Security and Resilience, February 12, 2013, accessed August 6, 2013, www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- Executive Order 13636—Improving Critical Infrastructure Cybersecurity, www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
- ISAC http://www.isaccouncil.org/aboutus.html
- NIST Cybersecurity Framework http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf
- DHS NIP https://www.dhs.gov/national-infrastructure-protection-plan
- National Cybersecurity Alliance http://staysafeonline.org
- DHS Presidential Directive 7 https://www.dhs.gov/homeland-security-presidential-directive-7
- DHS Critical Infrastructure Sectors http://www.dhs.gov/critical-infrastructure-sectors
- US-CERT Critical Infrastructure Cyber Community Voluntary Program http://www.us-cert.gov/ccubedvp
- Stop, Think, Connect http://stopthinkconnect.org
- COSO ERM Model - http://www.compliancysoftware.com/solutions_enterprise_risk_management.html
- SIFMA Quantum Dawn 2 Exercise http://www.sifma.org/services/bcp/cyber-exercise---quantum-dawn-2/
- National Initiative for Cybersecurity Careers and Studies http://niccs.us-cert.gov/research/cybersecurity-capability-maturity-model
- What are the implications of a cyber attack http://www.intellectualtakeout.org/faq/4-what-are-implications-cyber-attack
- BiPartisanPolicy, Cybersecurity & N.Americal Electrical Grid http://bipartisanpolicy.org/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf
- Ponemon Institute Cost of Cyber Crimes Study http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf
- Verizon 2013 Data Breach Investigation http://www.verizonenterprise.com/DBIR/2013/
- Federal Reserve recommended standards http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm
- FINRA Cybersecurity Survey, Jan 2014 http://www.finra.org/Industry/Regulation/Guidance/TargetedExaminationLetters/P443219
- SANS 20 Critical Security Controls http://www.sans.org/critical-security-controls/
- Internet of Things http://whatis.techtarget.com/definition/Internet-of-Things
- Cisco Internet of Everything http://www.cisco.com/web/tomorrow-starts-here/anthem/index.html


Cyberwise CP

# Contact Information

Susan Rogers

CEO, Cyberwise CP

Susan.Rogers@cyberwiseCP.com

(610) 389-1271