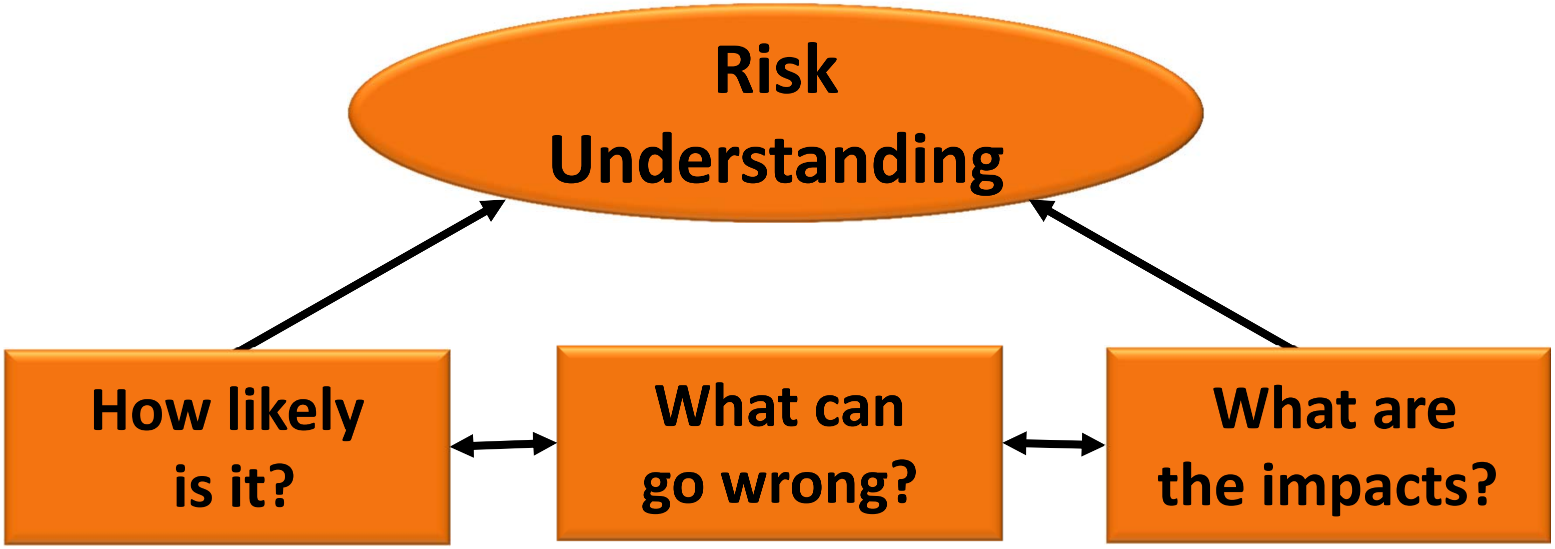
Framing the Discussion: *A World of Cybersecurity Risks*

John Duncan
Vice President
Global Government Sector
ABS Group

Basic Elements of Risk



Risk Understanding

How likely is it?

What can go wrong?

What are the impacts?

Risk = f [Threat, Vulnerability, Consequence]

Foundation for Risk Assessment

Historical Experience	Analytical Methods	Knowledge & Intuition

Simple Security Risk Model

Risk = f [Threat, Vulnerability, Consequence]

- **Scenario –** combination of a target and attack mode

What can go wrong?

- **For each scenario, assess the following:**
  - **Threat –** likelihood of a specific attack
  - **Vulnerability –** probability that the attack will be successful

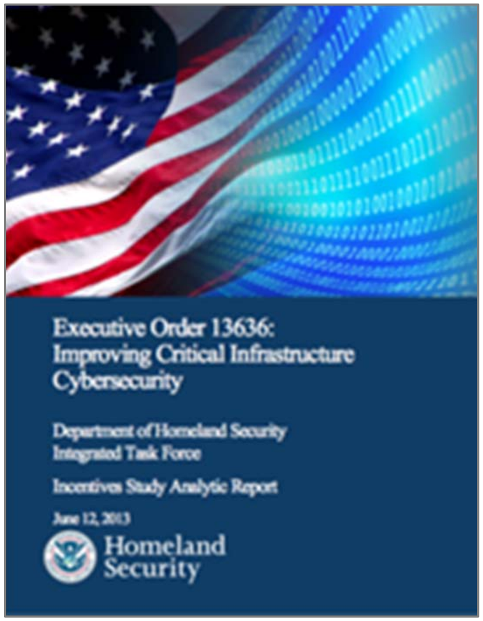
How likely is it?

  - **Consequence –** level of impact associated with a successful attack

What are the impacts?

NIST Framework Overview

- In February 2013, President Obama issued Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*
- Called for NIST to lead a collaborative effort to develop voluntary, risk-based Cybersecurity Framework
  - Set of existing standards, guidelines and practices to help organizations manage cyber risks.



Executive Order 13636:
Improving Critical Infrastructure Cybersecurity

Department of Homeland Security
Integrated Task Force

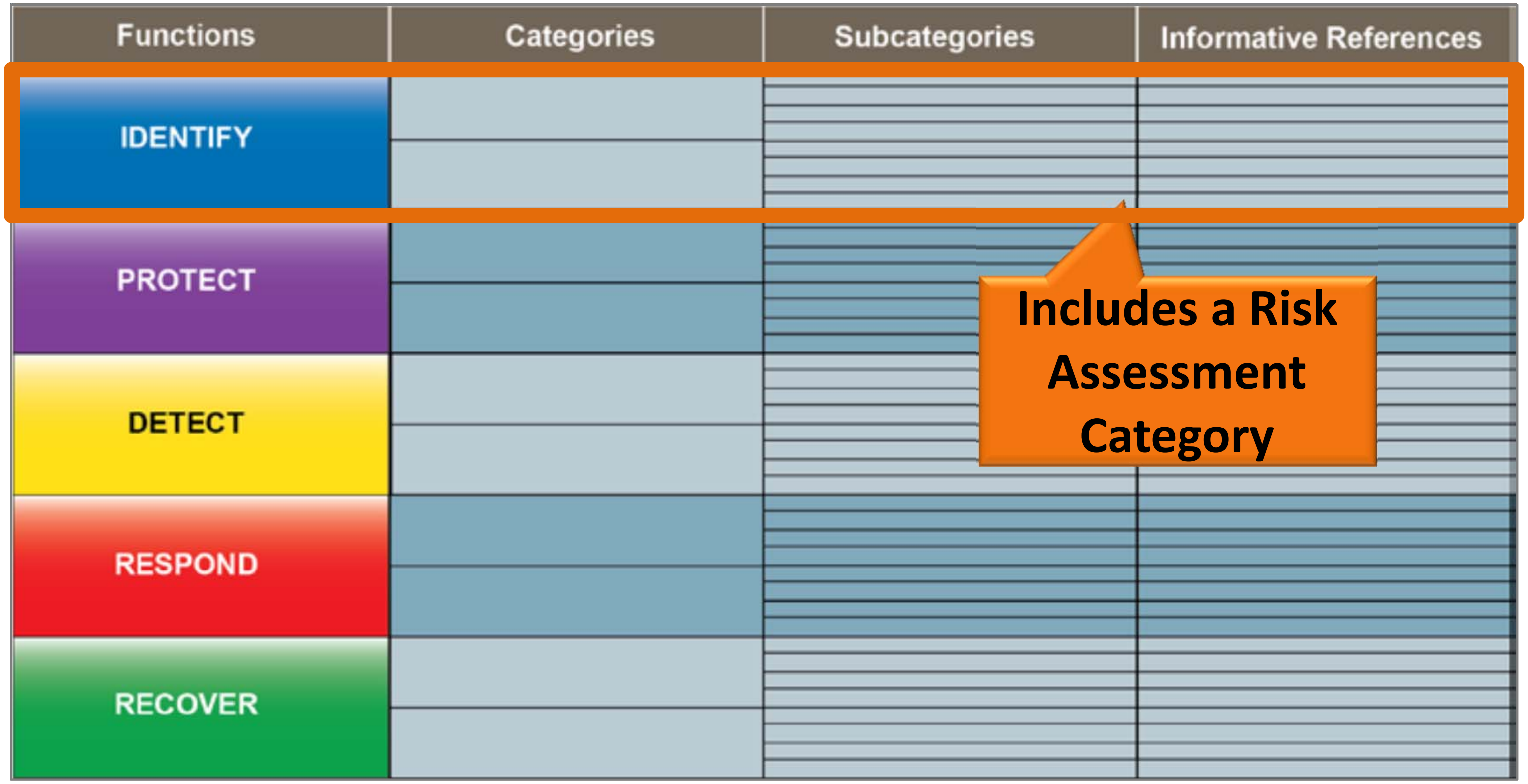
Incentives Study Analytic Report

June 12, 2013

Homeland Security

NIST Framework Core

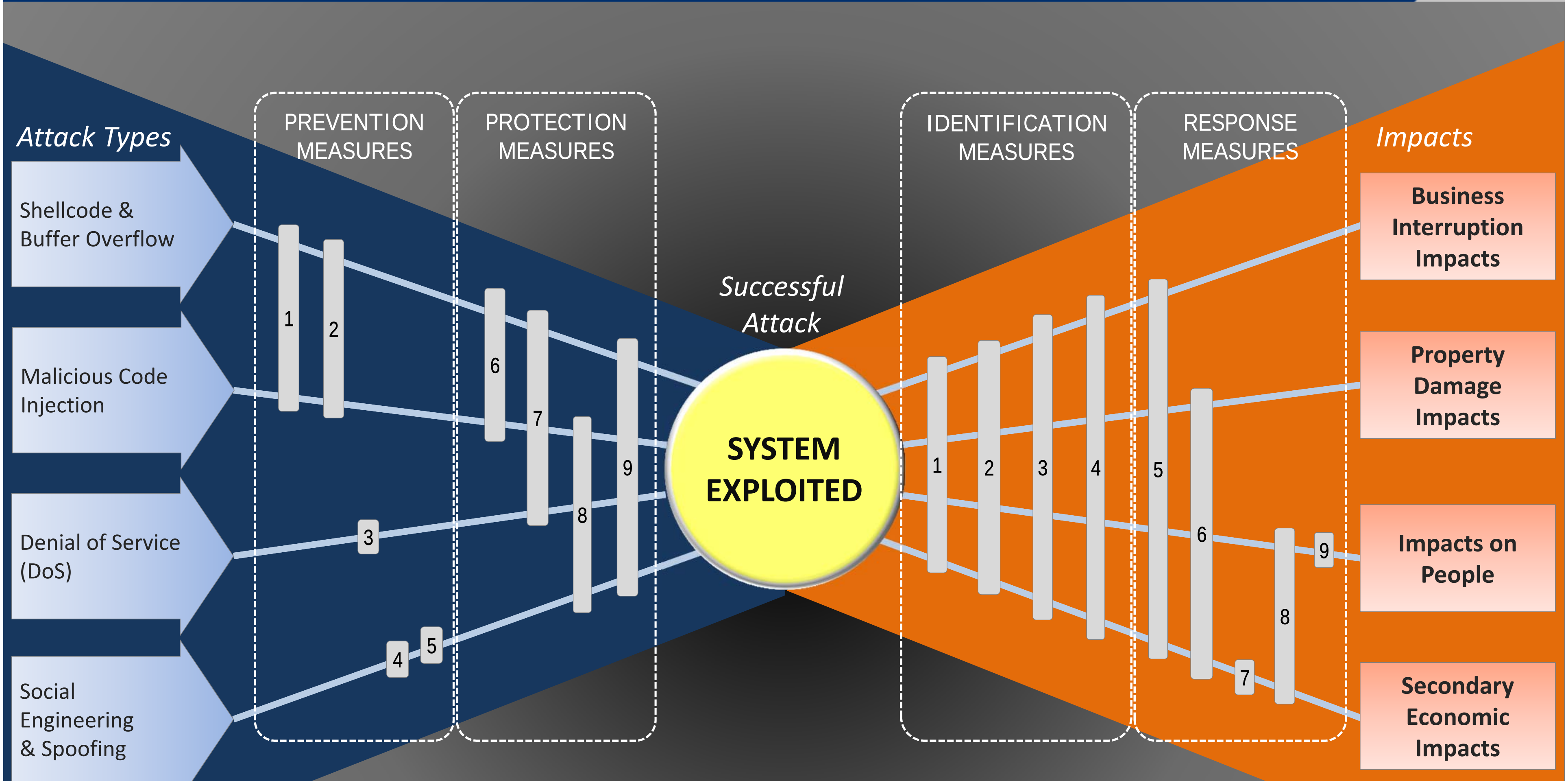
- Developed as guidance for a specific critical infrastructure component
- Contains valuable information for government agencies
- NIST framework identifies 5 major cybersecurity functions



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Includes a Risk Assessment Category

Notional Cybersecurity Bow-Tie Analysis Framework



Countermeasures

1. Secure Input/Output Handling
2. Data Execution Prevention
3. Intrusion Prevention System
4. Social Engineering Training
5. Access Control
6. Executable Space Protection
7. Anti-Virus Software
8. Firewalls
9. Security Protocols

Identification & Response Measures

1. Intrusion Detection System
2. Deep Packet Inspection
3. Network Analyzer
4. Honeypots
5. Firewall Modification
6. System Backup Restoration
7. DoS Defense System
8. Operating System Reinstallation
9. Hardware Replacement

Cyber Threats to Maritime Entities

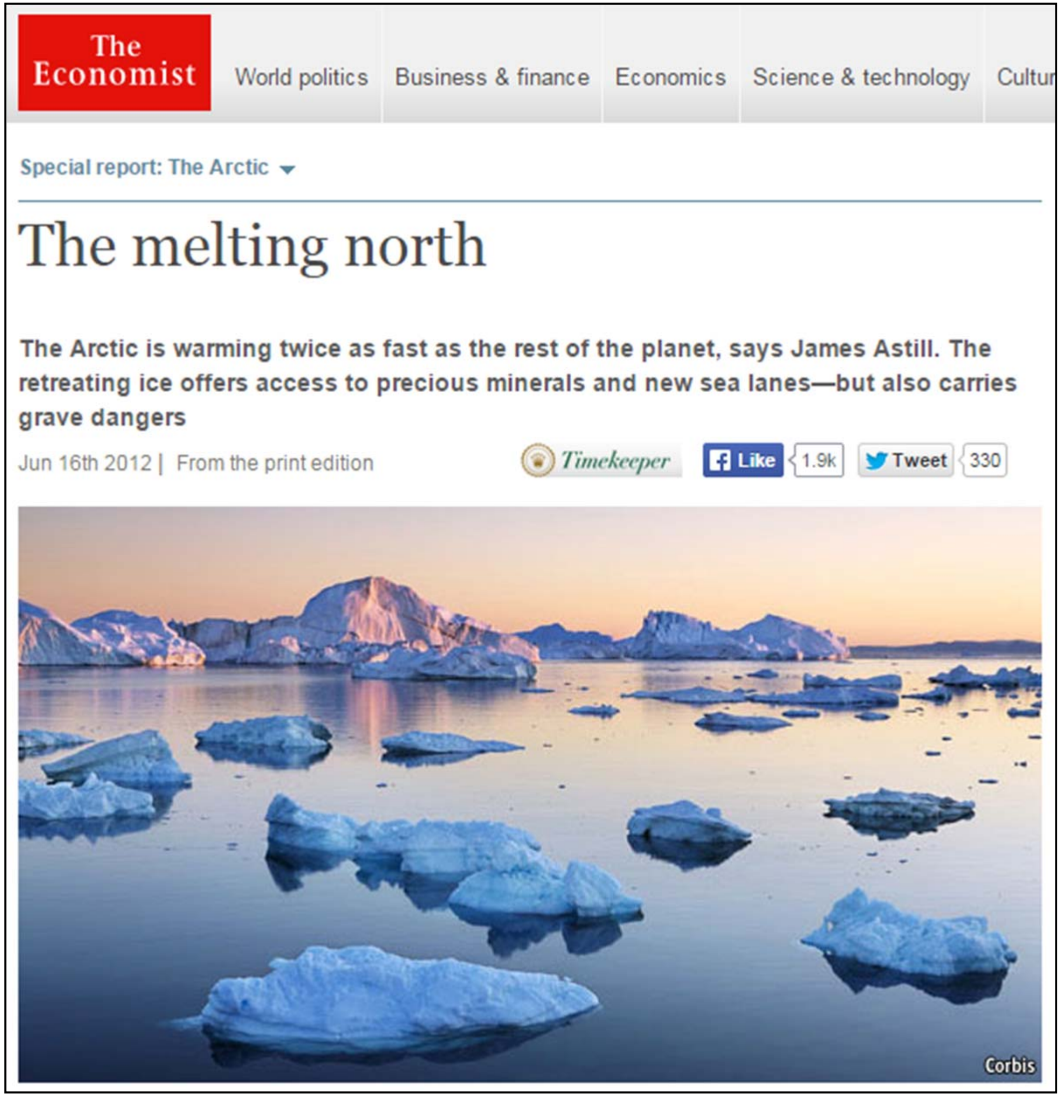
Tiffany Jones, CISSP, CIPP

SVP & Chief Revenue Officer, iSIGHT Partners

tjones@isightpartners.com

Primary Threat Categories

Scenarios: Setting the Geopolitical Context



Special report: The Arctic

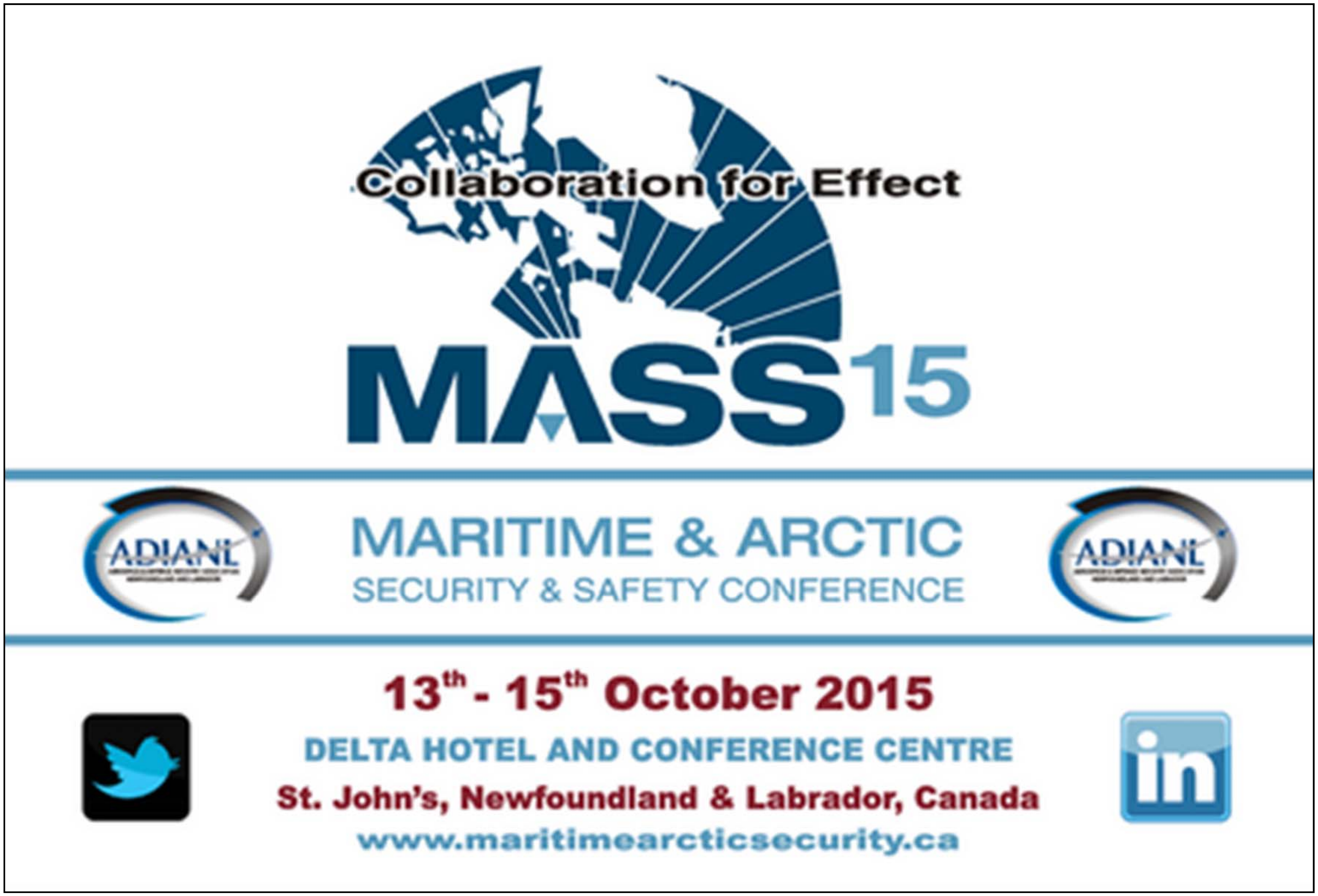
The melting north

The Arctic is warming twice as fast as the rest of the planet, says James Astill. The retreating ice offers access to precious minerals and new sea lanes—but also carries grave dangers

Jun 16th 2012 | From the print edition

Geopolitics drives espionage activity

Naval and Coast Guard Threats



Collaboration for Effect

MASS15

ADIANL

MARITIME & ARCTIC

SECURITY & SAFETY CONFERENCE

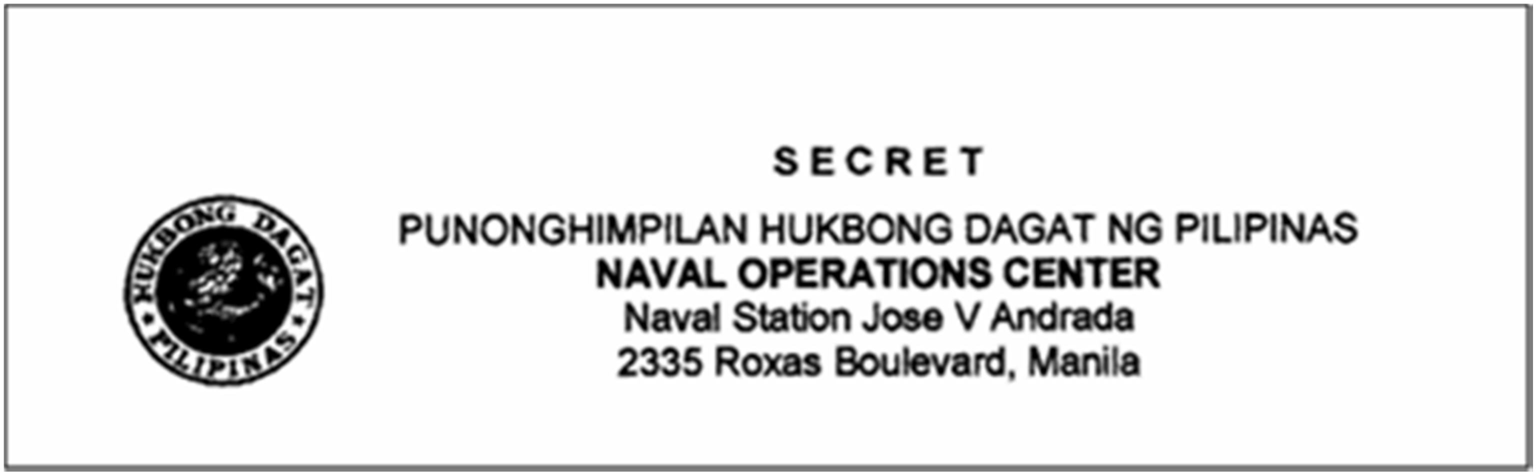
13th - 15th October 2015

DELTA HOTEL AND CONFERENCE CENTRE

St. John's, Newfoundland & Labrador, Canada

www.maritimearcticsecurity.ca

Naval and Coast Guard Threats



HUKBONG DAGAT • PILIPINAS •

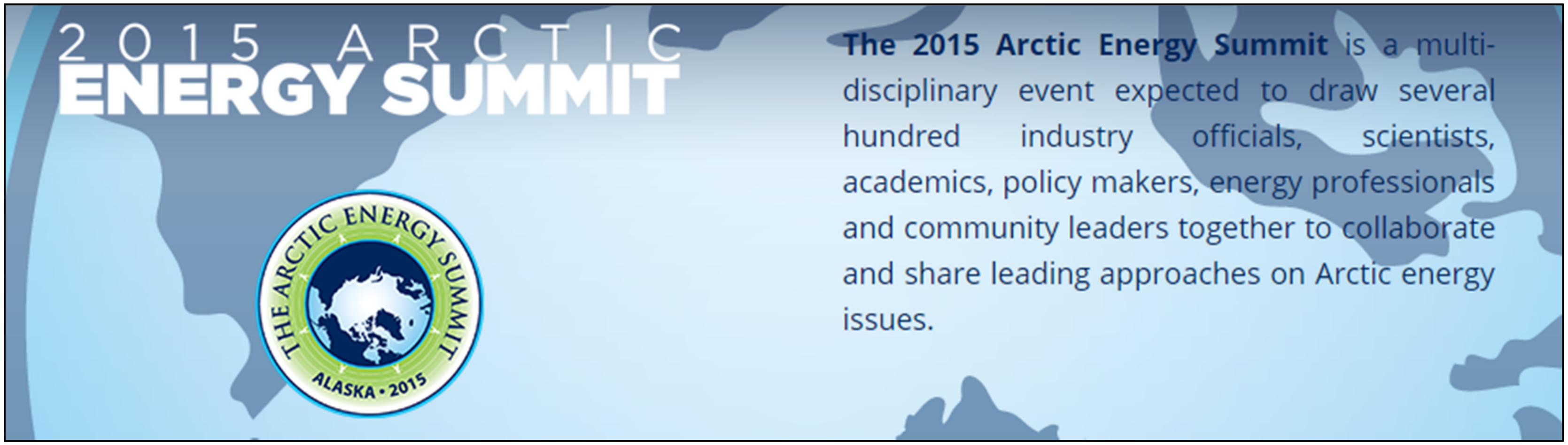
SECRET

PUNONGHIMPILAN HUKBONG DAGAT NG PILIPINAS
NAVAL OPERATIONS CENTER
Naval Station Jose V Andrada
2335 Roxas Boulevard, Manila

Benign lure document from Mirage RAT sample deployed ahead of US-Philippine defense agreement (iSIGHT Partners)

Commercial Maritime Threats

ASF
OCTOBER 2015
CANADA
8TH ANNUAL ARCTIC SHIPPING FORUM
NORTH AMERICA

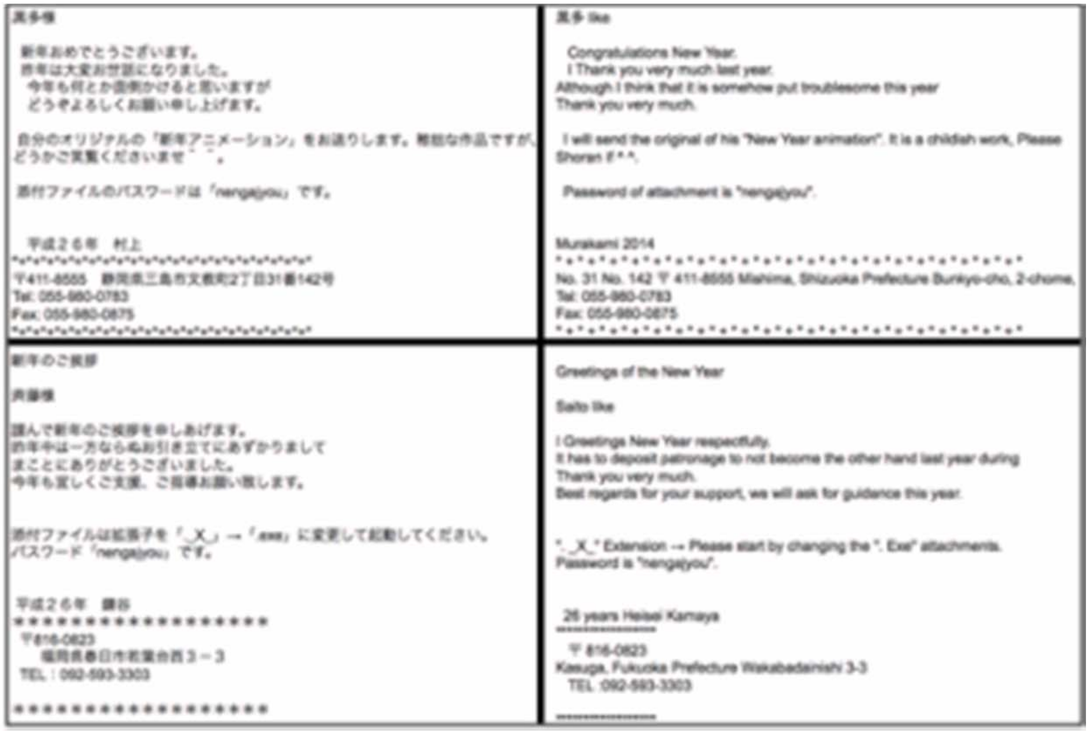


The 2015 Arctic Energy Summit is a multi-disciplinary event expected to draw several hundred industry officials, scientists, academics, policy makers, energy professionals and community leaders together to collaborate and share leading approaches on Arctic energy issues.

Commercial Maritime Threats

iSIGHTPARTNERS

謹賀新年
昨年は大変お世話になりました。
本年もよろしくお願い申し上げます
平成二十六年　元旦



黒多様

新年おめでとうございます。
昨年は大変お世話になりました。
今年も何とか面倒かけると思いますが
どうぞよろしくお願い申し上げます。

自分のオリジナルの「新年アニメーション」をお送りします。稚拙な作品ですが、どうかご笑覧くださいませ^^。

添付ファイルのパスワードは「nengajyou」です。

平成２６年　村上
・
〒411-8555　静岡県三島市文教町2丁目31番142号
Tel: 055-980-0783
Fax: 055-980-0875
・

黒多 like

Congratulations New Year.
I Thank you very much last year.
Although I think that it is somehow put troublesome this year
Thank you very much.

I will send the original of his "New Year animation". It is a childish work, Please Shoran if ^ ^.

Password of attachment is "nengajyou".

Murakami 2014
・
No. 31 No. 142 〒 411-8555 Mishima, Shizuoka Prefecture Bunkyo-cho, 2-chome,
Tel: 055-980-0783
Fax: 055-980-0875
・

新年のご挨拶

斉藤様

謹んで新年のご挨拶を申しあげます。
昨年中は一方ならぬお引き立てにあずかりまして
まことにありがとうございました。
今年も宜しくご支援、ご指導お願い致します。

添付ファイルは拡張子を「._X_」→「.exe」に変更して起動してください。
パスワード「nengajyou」です。

平成２６年　鎌谷
★★★★★★★★★★★★★★★★★★★
〒816-0823
福岡県春日市若葉台西３－３
TEL：092-593-3303

★★★★★★★★★★★★★★★★★★★

Greetings of the New Year

Saito like

I Greetings New Year respectfully.
It has to deposit patronage to not become the other hand last year during
Thank you very much.
Best regards for your support, we will ask for guidance this year.

". _X_" Extension → Please start by changing the ". Exe" attachments.
Password is "nengajyou".

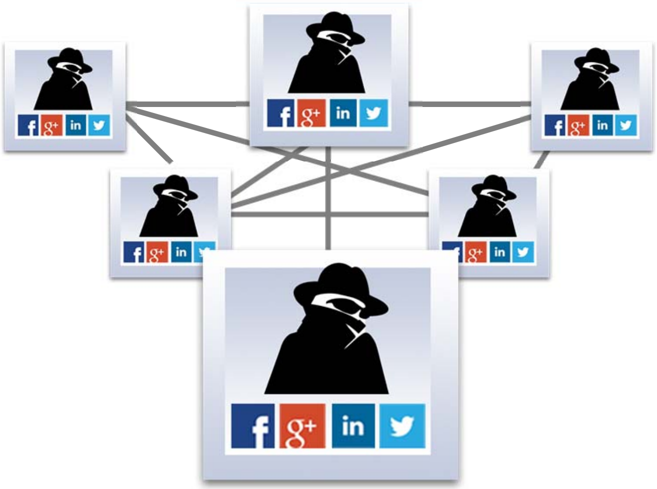
26 years Heisei Kamaya
===============
〒 816-0823
Kasuga, Fukuoka Prefecture Wakabadainishi 3-3
TEL :092-593-3303

===============

Chinese New Year-themed lure document sent to Japan Maritime United Corporation employee (iSIGHT Partners)

NEWSCASTER

- 3+ year Cyber-espionage campaign with links to Iran
- Targeting high and low ranking personnel in multiple countries – US, UK, Israel, Saudi Arabia, Iraq
  - U.S. military
  - Congressional personnel
  - Washington D.C. area journalists
  - Diplomatic corps
  - U.S. Defense contractors
  - Israeli Defense contractors
  - Members of the U.S./Israeli lobby
- Utilizing social media platforms as targeting platform
  - Facebook
  - LinkedIn
  - YouTube
  - Etc.
- More than 2,000 targets and legitimate individuals caught in the net
  - Credential harvesting
  - Access to corporate and personal emails
  - Malware with data exfiltration capabilities



Risk Panel - Vulnerabilities

Ronin Security Solutions

Andrew N Bertolazzi

RONIN
SECURITY
SOLUTIONS

Environment

- Ever-expanding cyber tools and connections
- Most popular passwords in 2013: “password”, “123456”
- “We aren't even doing the simple stuff” Sen. Coburn-2014
- CIOs: Hacking is going to happen. Plan for it (2015)
- All software has flaws
- Macro versus micro vulnerabilities
- People are the critical common factor

Maritime Terminal Realities

- Reliance on cyber-linked tools, equipment, systems
- e-Commerce and online filings
- Increasing need for tech-savvy workforce
- Shrinking margins, reduced staff, higher workload
- Make-up of IT and Security organizations
- Divergent priorities, mandates, and funding
- Port focus has been primarily on physical security
- Few Business Continuity or Disaster Recovery Plans

Typical Vulnerabilities

- Economic and strategic “soft” targets
- Flat, lean organizations – single point failures
- Cyber-connected control systems, equipment, data
- Low security of networks, WiFi, back-up, hardware
- Inadequate password practices
- Limited funds, shrinking PSGP pool
- Security is a cost – financial and operational
- People

What Can Be Done?

Processes

- Robust plans for Business Continuity & Disaster Recovery
- Regular, secure, offsite back-up
- Access controls for data – physical and cyber
- Password discipline

Tools

- Firewalls, segmented networks, intrusion detection
- Timely and complete updates, patches, & fixes

People

- Awareness, training, exercises
- Security consciousness (a bit of paranoia goes a long way)
- Outside help

Resources

- Homeport Cyber-Security Webpage
  https://homeport.uscg.mil/mycg/portal/ep/home.do
- US Computer Emergency Readiness Team (US-CERT)
  https://www.us-cert.gov
- Industrial Control Systems - Cyber Emergency Readiness Team
  https://www.ics-cert.us-cert.gov
- National Institute of Standards and Technology (NIST)
  http://www.nist.gov/cyberframework/index.cfm
- Software & Supply Chain Assurance Clearinghouse (DHS)
  https://buildsecurityin.us-cert.gov/swa/cwe

Risk Panel - Consequences

Captain Joe Kramek
Eleventh Coast Guard District
Legal Officer & Staff Judge Advocate

Commander Pacific Area

Case Study – National Impact of West Coast Port Stoppage (29 ports)

	5 Days	10 Days	20 Days
Cost to U.S. Economy	$1.9 B	$2.1B	$2.5B
Loss of Imports	$1.8 B	$3.9 B	$8.3 B
Loss of Exports	$1.5 B	$3.2 B	$6.9 B
Reduced Economic Output	$9.4 B	$21.2 B	$49.9 B
Cost to Households	$81	$170	$366
Employment Disruption	73,000	169,000	405,000

Immediate Backlog Across Economy

- Automakers – More Expensive Parts / Reduced Production
  - Honda, Toyota & Subaru
- Wal-Mart Inc. – Reduced Inventory /Earnings Hit
  - Electronics
- U.S. Meat Exporters – millions of pounds in storage
  - $85 mil per week
- Farmers – Losses estimated in hundreds of millions
  - CA citrus exports cut by half
  - WA apple crops

ABS Group

Questions for Panel