



Minutes for Delaware Continuity Coordinator Council

August 25, 2016

1 p.m. – 3 p.m.

Attendees: Lori Gorman, Claudette Martin-Wus, Heather Volkomer, Lynn Hooper, Karen Smith, Robert Denton, Jackie Keel, Peter Korolyk, Lauren Copeland, Edward Lee, Staci Marvel, Catherine Oravez, Mercedes Rooks, Karen Smith, Vicki Smith, Doyle Tiller, Susan Mateja, Gwenn Anderson, Dan Cahall, Judy Everett, Tim Li, Sharon Poole, Max Keiper, Nancy Skubik, Mark DeVore, Anthony Manson, Dawn Minor

➤ **DECCC Updates**

- Upcoming 2015 Events
 - ❖ FEMA's National Preparedness Month: www.ready.gov
 - ❖ Family Preparedness Day- Sept. 24th: www.preparedde.org
- 2015 Survey Results
- House Bill 380
- Steering Committee Changes

➤ **Real Life COOP Events that Impacted Delaware Organizations** (PPT presentations below)

- Fire: Facilities Management- Mark Devore
 - ❖ Batteries can be dangerous
 - ❖ Always store files and materials in their appropriate place
 - ❖ The state does NOT reimburse personal items destroyed at work
- Shooting: Court of Common Pleas- John Manus
 - ❖ Review decision making policies prior to an event
 - ❖ Keep Crisis Communication systems up to date
 - ❖ Employee training is vital: visit <http://extranet.dti.state.de.us/COOP/information/deccc.shtml> for suggested methods for training employees on Emergency Procedures for your location.
- Cyber Attack/ Ransomware: Dept. of Technology and Information- Max Keiper
 - ❖ Ensure McAfee agents and definitions are updating and current
 - ❖ Ensure you are receiving software patches
 - ❖ User awareness and training!!
 - ❖ ENSURE YOUR SYSTEMS ARE BACKED UP AND YOU HAVE A PLAN FOR THE INEVITABLE.

➤ **Cyber and Its role in COOP Plans** (PPT presentations below)

- High Technology Crimes Unit/ DIAC: DSP Detective Nancy Skubik
 - ❖ Disconnect an infected PC from the Network but do NOT shut it down.
 - ❖ Register to receive alerts from the DIAC at www.DEDIAC.org
- Incorporating Cyber into LDRPS COOP plans: DTI Lori Gorman
 - ❖ Get your Management and IT personnel involved
 - ❖ Create Work-arounds for ALL of your CRITICAL processes

- ❖ Review your allowable delays, Recovery Point Objectives (RPO) and Recovery Time objectives (RTO)
- ❖ Review your dependency mapping for all systems related to Critical processes.

DECCC Steering Committee members:

Lori Gorman – Co-Chair

Tony Lee – Co-Chair

Vacant – Vice-Chair

Vacant – Education and Training Officer

Vacant – IT Systems Officer

John Mancus – Disaster Preparedness Officer

Mark Devore – Facilities Officer

Vacant – Vital Records Officer

****If interested in the vacant position(s), please contact any one of the Steering Committee members****

Qualifies as 1 CEU per hour towards COOP certification(s)



Delaware Continuity Coordinator Council (DECCC)

August 25, 2016

Agenda

- Welcome/Introductions
- DECCC Updates
 - Upcoming Events
 - 2015 Survey Results
 - House Bill 380
- Elections
- Real Life COOP Events and Impact on Delaware Organizations
 - Fire- Facilities Management
 - Active Shooter- Court of Common Pleas
 - Cyber Attack/Ransomware- Dept. of Technology and Information
- Cyber and It's Role In COOP Plans
 - DIAC: Detective Nancy Skublik, DSP
 - Incorporating Cyber in a COOP plan: Lori Gorman, DTI
- Q&A

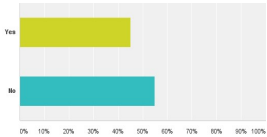
DECCC Updates

- Upcoming 2016 meetings
 - December 1st - Winter Weather Preparedness
 - COOPsgiving: A Time to Reflect
- Upcoming Events
 - FEMA's National Preparedness Month: September
 - <https://www.ready.gov/september>
 - Family Preparedness Day - September 24th
 - Cyber Workshop (Secure Delaware)- September 7
 - Cyber Exercise - October

2015 Survey Results

DECCC

Claudette Martin-Wus



Response	Percentage
Yes	45%
No	55%

DECCC Updates: House Bill 380

This Act is the first leg of a constitutional amendment that would alter the continuity of government provisions of the Delaware Constitution to enable the effective continuance of government following a variety of emergency situations.

Currently, Article II, § 5 of the Delaware Constitution requires the General Assembly to meet in Dover, unless an emergency caused by insurrection, conflagration, or epidemic diseases occurs. And, Article XVII, § 1 of the Delaware Constitution provides the General Assembly with the power to enact laws providing for continuity of government following emergency situations, but only if the emergency results from an enemy attack.

Section 2 of this Act extends the General Assembly's authority under Article XVII, § 1 to disasters involving terrorism, disease, accident, and other natural or man-made disasters. This would authorize the General Assembly to extend the provisions of Chapter 77 of Title 29 of the Delaware Code (relating to the emergency location of government), Chapter 17 of Title 29 (relating to emergency interim legislative succession), Chapter 78 of Title 29 (relating to interim executive succession), and Chapter 18 of Title 10 (relating to emergency interim judicial succession) to emergencies involving terrorism, disease, accident, or other natural or manmade disasters, as well as those involving enemy attack. This change is consistent with the approach taken in at least four states, New York, Louisiana, Montana, and Utah, which have adopted an "all hazards" approach to continuity of government planning.

In addition, Section 2 of this Act makes changes to Article XVII, § 1 adopting the interpretation of this provision by the Delaware Supreme Court in Opinion of the Justices, 190 A.2d 521 (Del. 1963), so that it is clear that the General Assembly may provide for succession for those public offices that are not immediately filled by operation of the Constitution.

Section 1 of this Act would harmonize Article XVII, § 1 and Article II, § 5 so that the emergency situations exempting the General Assembly from the requirement that it meet in Dover are similar to the emergency situations in which the General Assembly may enact laws or otherwise act to provide for the continuity of government.

Finally, this Act makes technical corrections to conform existing law to the guidelines of the Delaware Legislative Drafting Manual. Specifically, lines 17 through 19 of this Act remove unnecessary legalese in and make grammatical changes to the final sentence of Article XVII, § 1.

Steering Committee Positions

- Positions:
 - Vice-Chair
 - Education and Training Officer
 - IT Systems
 - Vital Records
- Claudette Martin-Wus will be stepping down as Co-Chair effective the end of the year. Thank you for your wonderful leadership over the years. Lori Gorman will be assuming this role in the coming year.

DECCC Survey 2015

Wednesday, August 17, 2016

Powered by SurveyMonkey

Q1: Do you have a current Family Preparedness Plan?

Answered: 40 Skipped: 0

Answer Choices	Responses
Yes	45.00% 18
No	55.00% 22
Total	40

Powered by SurveyMonkey

What topics/presentations do you want to hear at DECCC meetings?

- What really happens when a disaster occurs. How do employees react. Do employees respond as procedures state.
- How one can get senior management engaged in the process.
- If a template of a presentation exists about the importance of safety preparedness, can we discuss the possibility of allowing all DECCC members to have a copy to present to their agencies? I'm thinking of hosting a 'lunch & learn' for the agency. We have an internal presentation, but it would be nice to share something a little different with them. Just a thought.
- **Delaware Experiences**
- **Determining mission essential functions during a COOP event in a division with multiple sections**
- **Maybe lessons learned from other states that went through disasters.**
- Interagency resource allocations and coordination
- Devolution information.
- **More focus on evacuation plans**
- **A State shut down**
- **Family Preparedness**
- I like to know how other agencies are responding to incidents like power outages and other incidents that happen commonly.
- **Active Shooter exercise planning**
- What to do in an earthquake
- **What supplies to have on hand at home and in the office?**
- How to prepare a site plan
- First Aid, Local Emergency issues relating to severe weather.
- Employees taking this seriously
- Planning for ways to deal with power outages
- **Crisis Communications**
- **Disaster Recovery**
- The after effects. How to start back after an event.
- Safety instructions for disasters

Powered by SurveyMonkey

What disaster-type apps do you use?

- State alert notifications
- FEMA, Red Cross Hurricane, Tornado
- GETS/WEPS, Emergency Alerts, Tornado,
- National Weather Service App
- NOAA app
- Rely on emergency notification on cell phone

Powered by SurveyMonkey

Q4: When was the last time your agency coordinated an internal COOP exercise?

Answered: 33 Skipped: 7

Answer Choices	Responses
1-6 months	24.24% 7
7-12 months	24.24% 7
1-2 years	30.30% 10
3+ years	12.12% 4
Never	15.15% 5
Total	33

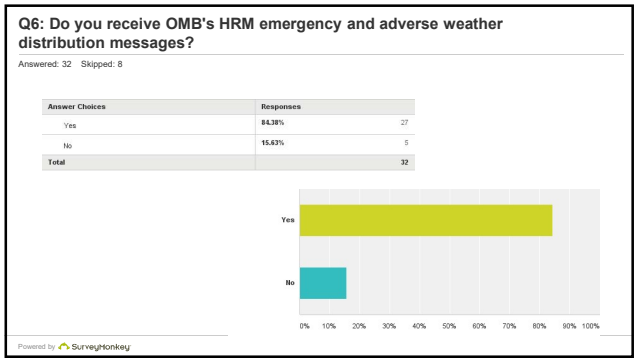
Powered by SurveyMonkey

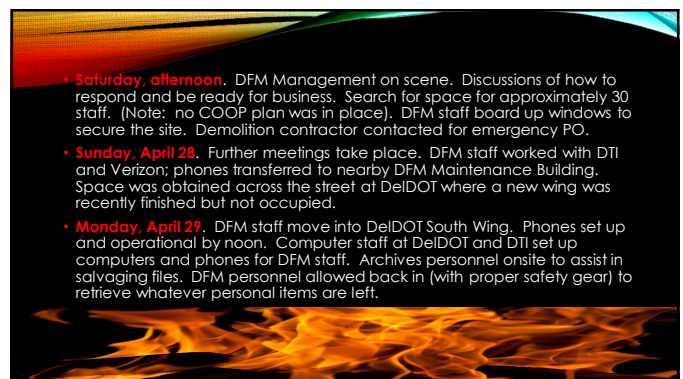
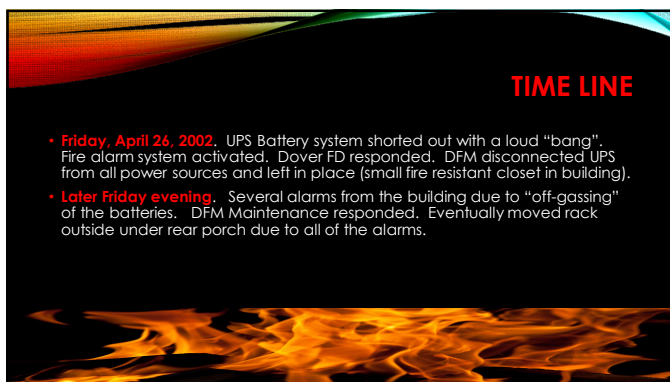
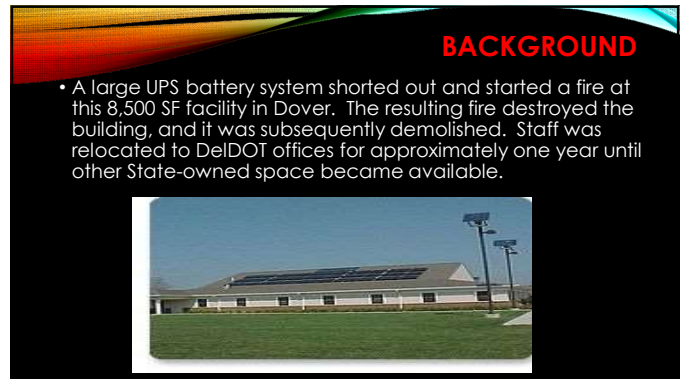
Q5: When was the last time your agency sent a crisis communications message (either/or for testing or real-life purposes)?

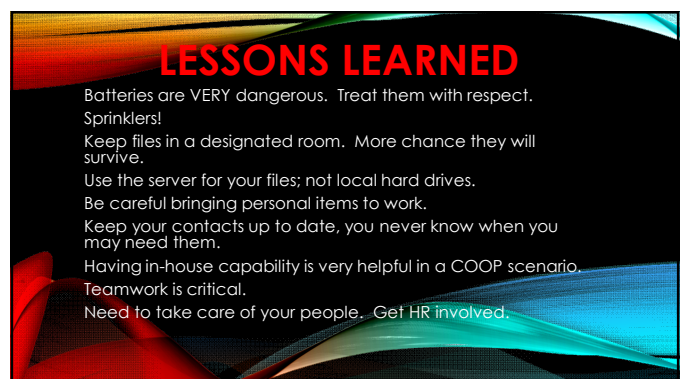
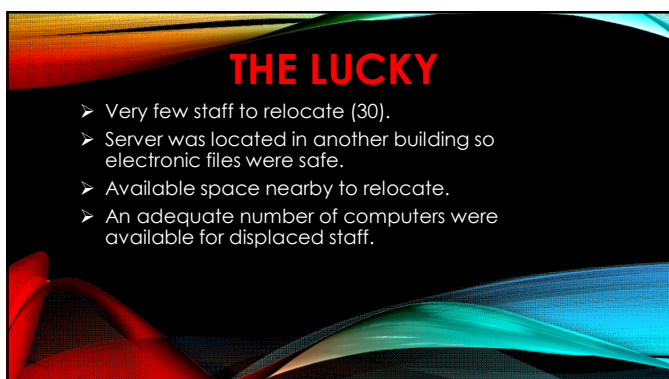
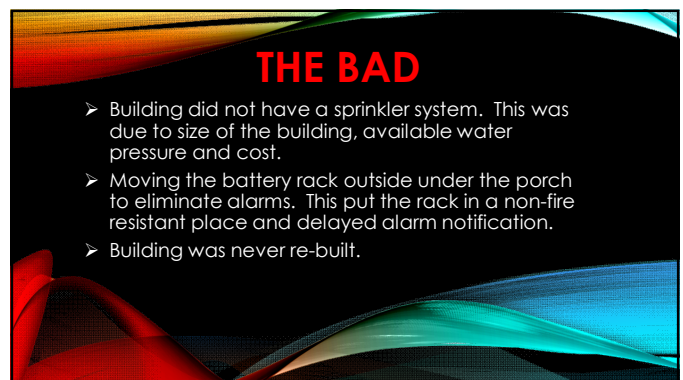
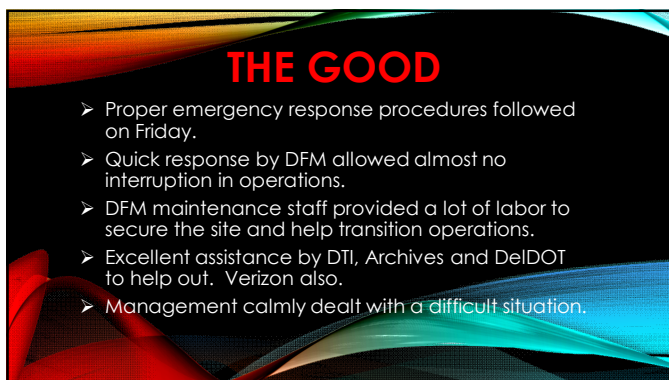
Answered: 32 Skipped: 8

Answer Choices	Responses
1-6 months	25.00% 8
7-12 months	25.00% 8
1-2 years	28.13% 9
3+ years	0.00% 0
Never	21.88% 7
Total	32

Powered by SurveyMonkey







Active Shooter, Noun \ 'ak-tiv\ \ 'shu-ter\

The agreed-upon definition of an “active shooter” by US government agencies (including the White House, US Department of Justice, FBI, US Department of Education, US Department of Homeland Security, and Federal Emergency Management Agency) is “an individual actively engaged in killing or attempting to kill people in a confined and populated area.” In most cases, active shooters use firearms and there is no pattern or method to their selection of victims.

Active shooter situations are unpredictable and evolve quickly. Because active shooter situations are often over within 10 to 15 minutes, before law enforcement arrives on the scene, individuals must be prepared both mentally and physically to deal with an active shooter situation. In most cases, active shooters use firearms(s) and there is no pattern or method to their selection of victims. Individuals have been known to act without firearms such as the case in on April 2014 at Franklin Regional High School where 21 students were stabbed. It's for this reason that ALICE also uses the terms: Active Killer; Violent Intruder; and Active Assailant.

Active Shooter Online Resources

<http://www.dhs.gov/activeshooter>

<http://extranet.dti.state.de.us/COOP/information/deccc.shtml>

FBI Studies of Active Shooter Incidents

A Study of Active Shooter Incidents in the United States Between 2000 and 2013

<https://www.fbi.gov/file-repository/active-shooter-study-2000-2013-1.pdf/view>

Active Shooter Incidents in the United States in 2014 and 2015

https://www.fbi.gov/file-repository/activeshooterincidentsus_2014-2015.pdf/view



RUN/ESCAPE

IF POSSIBLE



HIDE

IF ESCAPE IS
NOT POSSIBLE



FIGHT

ONLY AS A
LAST RESORT

Ransomware-aware

Enterprise Security Operations
Mark Bailey & Max Keiper

Get to know us....

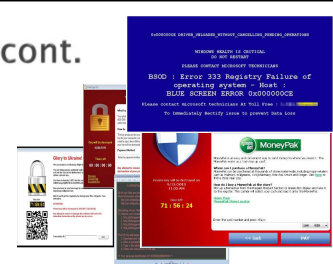
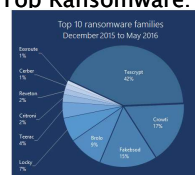
- ▶ **Mark Bailey**
 - 17 years experience within the State.
 - Vast experience with the States Vulnerabilities and Security posture.
 - Serves on the Architecture Review Board.
 - Lead Incident Handler.
- ▶ **Max Keiper**
 - CISSP, GISF, GSEC, GCED, GCIA, GISP, GMON
 - Under a year with DTI and ESO
 - 15 years of IT and Security experience in Private Industry and Higher Education.

Ransomware

- ▶ **Definition:**
 - "A malware that stealthily gets installed on your PC or mobile device and holds your files or operating system functions for ransom." (Microsoft, 2016)
- ▶ **Actions:**
 - Prevent you from accessing Windows.
 - Encrypt files so you cannot use them.
 - Stop certain apps(web browser, AV) from running.
 - Renamed files.
 - Locked browser or screen.

Ransomware cont.

▶ Top Ransomware:



▶ Types:

- **Lockscreen**
 - Shows a fill-screen message preventing access to your PC
- **Encryption**
 - Changes files so you cannot use them either by encryption or renaming.

How does it start? Who's affected?

- ▶ Victims fall into ransomware traps by:
 - Browsing untrusted websites.
 - Not careful about downloading email attachments that could contain malicious code from spam.
 - Executables.
 - Office files that support macros.
 - Unpatched, outdated software or operating systems.
 - User Accounts not following Principle of Least Privilege.
 - Systems that are connected to an already infected network.
- ▶ Attackers specifically research and target a victim.

To Pay or Not to Pay?

- ▶ **FBI recommends not to pay the ransom.**
 - Some pay and take the chance...
 - Will it encrypt again?
 - Will the system be clean from infection?
 - Was any data stolen?
- ▶ Files and Folders are targeted by Attackers.
- ▶ Reverse-engineering is practically impossible.
- ▶ Prevention is key.
- ▶ Ensure important files are backed up.

It happens to the best of us!

- ▶ CSIRT Activated June 23rd to July 6th.
- ▶ Phishing emails hooked State users.
 - Emails of different variants (senders, receivers, subjects, attachments and body).
 - A campaign received by hundreds of state employees.
- ▶ Parties Involved
 - 6 Agencies involved.
 - User workstations infected.
 - File Servers with shared/map drives.
 - Technical resources to identify, contain and recovery.

The face of evil.

- ▶ **W32/Zlader**
 - Detected in the wild April 27, 2016.
 - Stops you from using your PC and accessing data.
 - Distributed by countless email variants.
 - Payload file name samples:
 - Invoice####.zip
 - ATT00001.bin
 - Confirmation####.zip or Confirmation#.doc
 - Invoice###.scr(with Word icon)
 - state.de.us_order_invoice.doc
 - Hot links in emails to malicious payloads.
- ▶ **Encrypted these file types:**
 - .lcd, .cdf, .cdr, .dbf, .doc, .docm, .docx, .dwg,
 - .jpge, .jpg, .mdb, .pdf, .psd, .rtf, .sqlite, .xls, .xism,
 - .xlsx, .zip

Evils many heads.

- ▶ **Encryption was the goal.**
 - Locally(My Documents, Desktop...)
 - Shared/Mapped directories that users had write permissions.
- ▶ **Actual Emails**

<p>From: stateofde@stateofde.com Sent: Wednesday, June 23, 2016 10:57 AM Subject: Re: legal billing contract</p> <p>Yves, Jennifer Williams State & County, LLP P: 704.2664342 F: 704.2664342</p>	<p>From: stateofde@stateofde.com Sent: Thursday, July 14, 2016 11:07 AM Subject: Re: state.de.us order</p> <p>Thank you Alex Cordoba DDCS POWERS P: 602.1184071 F: 602.8213853</p>
--	--

Thank you for your kind attention. This is to confirm that the payment for Invoice 009983 has been sent. It was deposited into checking account ending in 3622. A confirmation slip is attached. Kindly confirm if it corresponds with the total P.O.

Regards,
 Diego Lachon
Diego.Lachon@stateofde.com
www.stateofde.com

The clean up.

- Ensure McAfee agents and definitions are updating and current.
- Ensure you are receiving software patches.
- Revisit your production website architecture and not have production websites dependent on user shares.
- User awareness and training.
- Ensure user accounts are following Principle of Least Privilege.
- Report suspicious/anomalous system actions as soon as possible.
- Continued user education and awareness.
- **ENSURE YOUR SYSTEMS ARE BACKED UP AND YOU HAVE A PLAN FOR THE ENVITABLE.**

Questions?

Delaware State Police High Technology Crimes Unit

Network Intrusions Guidelines:

- What to Expect from Law Enforcement
- What Law Enforcement Expects

Presented by:

Detective Nancy Skubik, CFCE
Delaware State Police

Network Intrusion Situation

Prevention and Preparation

- Identification and apprehension of cyber criminals before they strike
 - Research of current trends, exploits, software, code
 - Train for actual events through cyber exercises
- Gain an understanding the criminal's methods and tactics
- Stay current with emerging criminal network exploits

Protection

- Maintaining up-to-date technologies, such as: new hacker exploits, virus definitions, network ports are closely monitored, IDS and firewalls are up-to-date, etc...

Law Enforcement Response

- Not all victims of intrusions notify police.
 - They want to mitigate the intrusion, patch and restore
- Result:**
 - Loss of potential and pertinent evidence of the intrusion
 - Possibility for executables to be left behind for future compromise
- If the victim notifies Law Enforcement:
 - We will work closely with the IT administrator or designee(s) to build a framework for criminal prosecution.
 - The victim is more familiar than police with the network topography, it's vulnerabilities, the logging mechanisms, etc.
- Expected Action by Victim:**
 - Prior to police arrival, the IT person(s) should conduct a complete network assessment.
 - Determine, if this is an actual breach
 - The scope of the breach
 - Is it contained?
 - Have the compromised machines been taken offline, NOT powered down.
- Determine what resources will be needed.

On-scene Actions

- We do not respond with the intention to SHUT DOWN the network.
 - That will be determined by someone other than police, unless the intrusion has threatened human lives, has the potential to threaten human lives, or there are devastating threats on financial systems, ecological systems, nuclear systems, etc...
 - If the compromise is contained to one identified computer, this must be removed from the network, but NOT powered down.
 - Police is on scene to capture as much evidence to:
 - Identify the intrusion
 - Identify and capture digital evidence (processes running, RAM dump, IPs captured, viruses, root kits, etc...)
 - Identify pertinent information to the criminal investigation, such as: IP addresses, MAC addresses, witness statements, HR statements of employees (recently fired), previous threats

On-scene Actions

- Need to Shut Down
 - Prior to Shutting Down:
 - IT personnel should attempt to at least screen capture **Netstat** results
 - Should attempt to conduct a RAM dump prior to shutdown
 - Make notes of anything determined to be pertinent.
 - If the machine that was compromised is shutdown, **do not** turn it back on
 - This changes data that we will need when we conduct forensic examination.
 - Isolate the computer.
 - Place someone in charge of the computer
 - Document when it was shutdown, who shut it down, how it was shut down (pulled the plug or proper shutdown)

IT Admin Responsibilities

- Preserving Electronic Evidence
 - One of the significant sources of evidence are the logs generated automatically by various systems throughout the network
 - Need to know what logs are kept, where they are kept, and how long are they maintained
 - It is important that log files that are copied to a CD/DVD/thumb drive are kept in their original file format
 - It is important to confirm logging system date and time with the actual date and time.

Review

- Verify actual intrusion
- Determine scale of intrusion
- Obtain valuable information
- Preserve pertinent sources of evidence
- Abide by your company's policies and procedures
- Call Police
 - For response
 - For information
- Practice, Plan, Design, Train, Implement

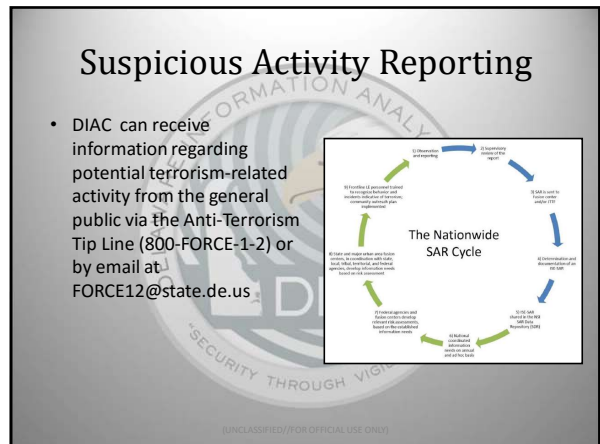
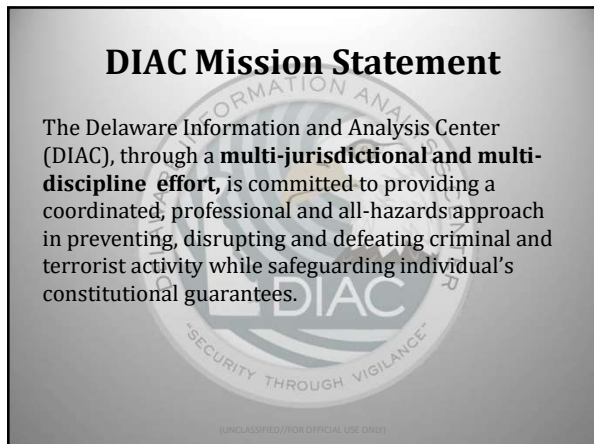
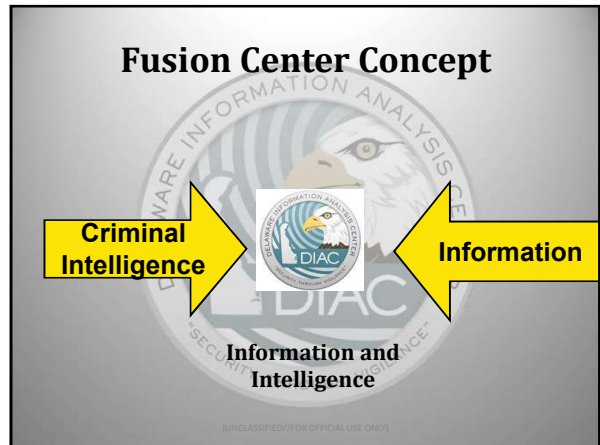
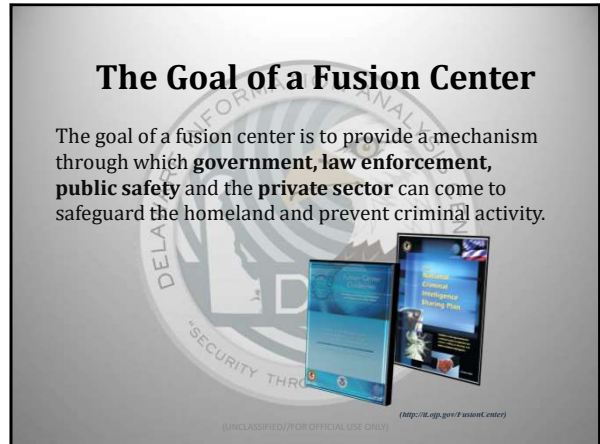
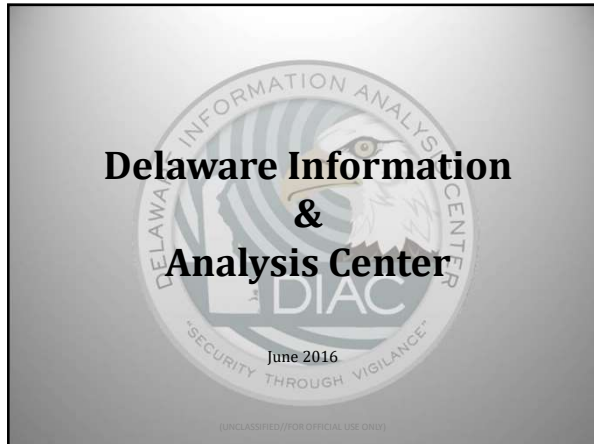
Questions

Sergeant Kevin Perna

Kevin.Perna@state.de.us

Detective Nancy Skubik

Nancy.Skubik@state.de.us



INCORPORATING CYBER IN A COOP PLAN

DEPARTMENT OF TECHNOLOGY AND INFORMATION
LORI GORMAN, DISASTER RECOVERY SPECIALIST

BIGGEST CHALLENGES

- What information does your organization gather?
 - Personal Identifiable Information
 - Health related information
 - Financial Information
- What systems/information present the most risk? What measures are being taken to mitigate that risk?
- Does your management and IT staff speak the same language- or even speak at all?

ASSIGN PROCESSES

- Have work around procedures for ALL of your critical processes.
 - Think outside the box.
 - Down time activities
 - Old school pen and paper
 - TRACK EVERYTHING!
- Allowable Delay; Recovery Point Objectives (RPO); Recovery Time objectives (RTO)
- Accurately document Process, Hardware, and System dependencies!

PLAN ASSIGNMENTS

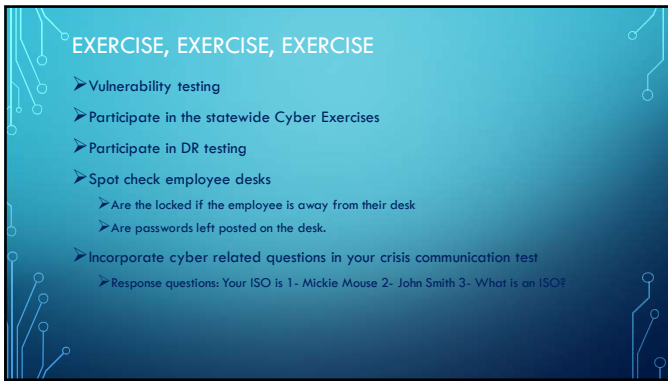
- Employees: Include IT employees in your plan (even if they don't work directly for your organization).
- Teams: Designate an IT response team to handle cyber threats.
 - Include your organization Information Security Officer
 - IT personnel familiar with your systems
 - Key managers
- Tasks: include tasks related to notifications, isolating systems, etc.
- Vendors/Customers: Include any specialized vendors.

PLAN ASSIGNMENTS CONTINUED...

- Software: have you clearly identified all of the software requirements that you use and are you using the most current versions.
 - Are there any software solutions that may better protect your systems? Virus scanning, monitoring software, Firewalls, etc.
- Equipment, Supplies, Assets: Do you need specialized equipment to complete work around procedures?
- Vital Records
 - How many of them are in electronic format?
 - Are they vulnerable?
 - Security measures and back-ups

RESTORATION PLANS WITH EYE TO CYBER

- Alternate locations- Have you tested access to critical systems from your alternate location? Do they pose additional cyber risks?
 - Free wifi
 - Shared work space
 - Open to the public
- Work from home solutions: Have you considered potential risks of personal devices?



EXERCISE, EXERCISE, EXERCISE

- Vulnerability testing
- Participate in the statewide Cyber Exercises
- Participate in DR testing
- Spot check employee desks
 - Are they locked if the employee is away from their desk
 - Are passwords left posted on the desk.
- Incorporate cyber related questions in your crisis communication test
 - Response questions: Your ISO is 1- Mickie Mouse 2- John Smith 3- What is an ISO?