

Emergency Response

Doug Langley

Director – BellSouth Security Strategy and Planning

June 8, 2006

Critical Infrastructure

Over 100k Dispatches/Day



56 Military Bases



950 Hospitals



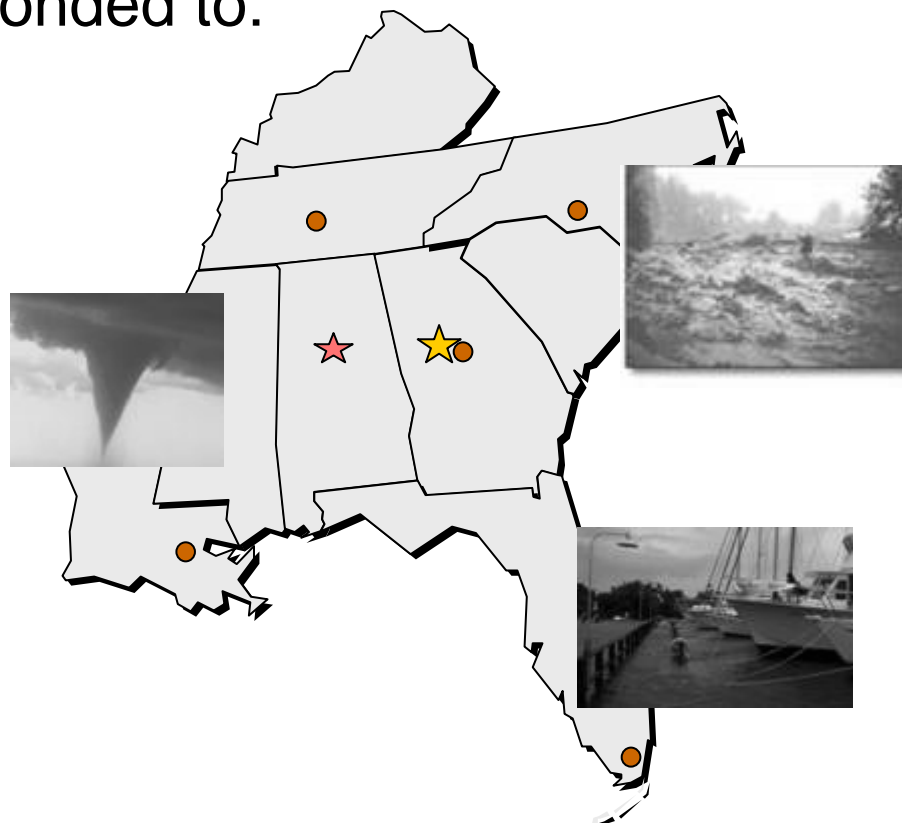
276M Calls/Day

20% of the Nation's Critical Telecom Infrastructure

History of Response

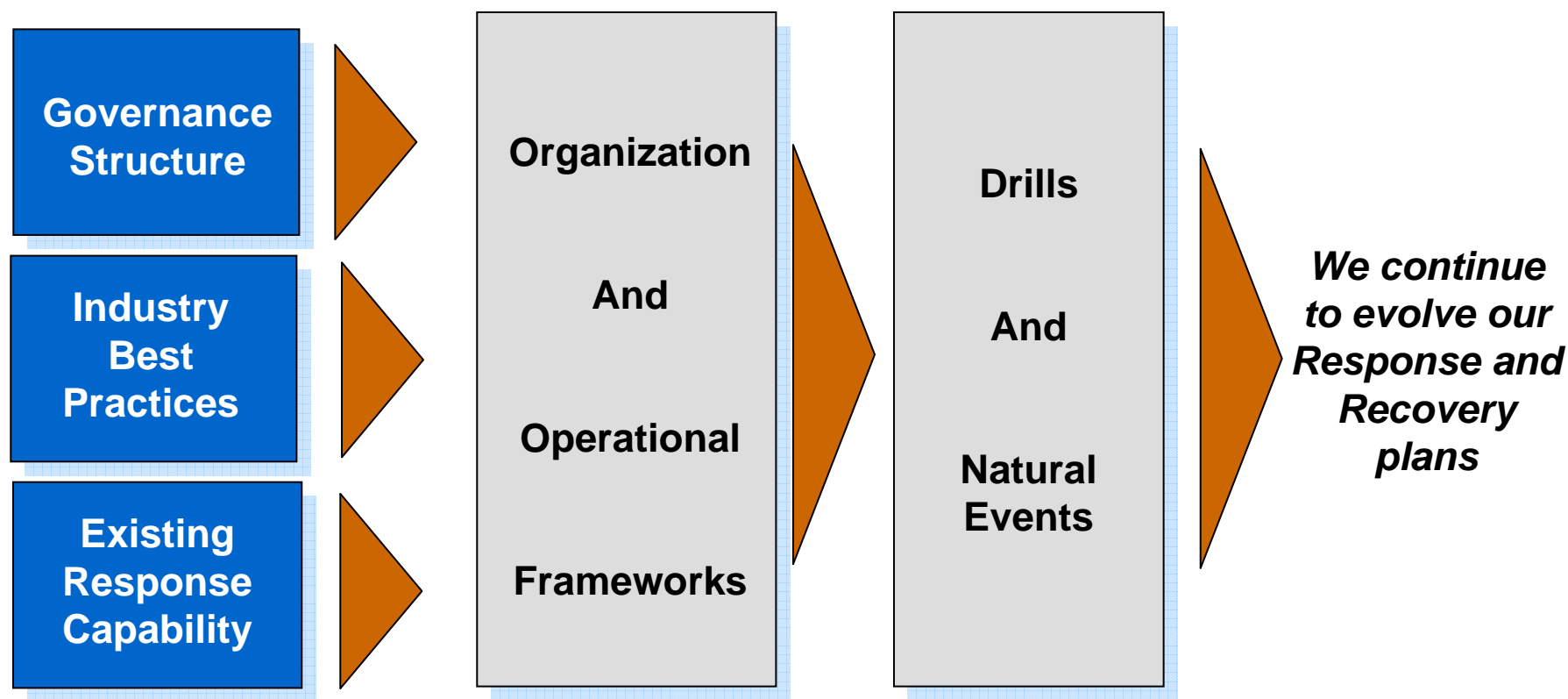
From 1992 – 2006, we have responded to:

- 24 Hurricanes
- 6 Ice Storms
- 5 Floods
- 2 Chemical Spills
- Florida Wildfires
- Countless Tornadoes

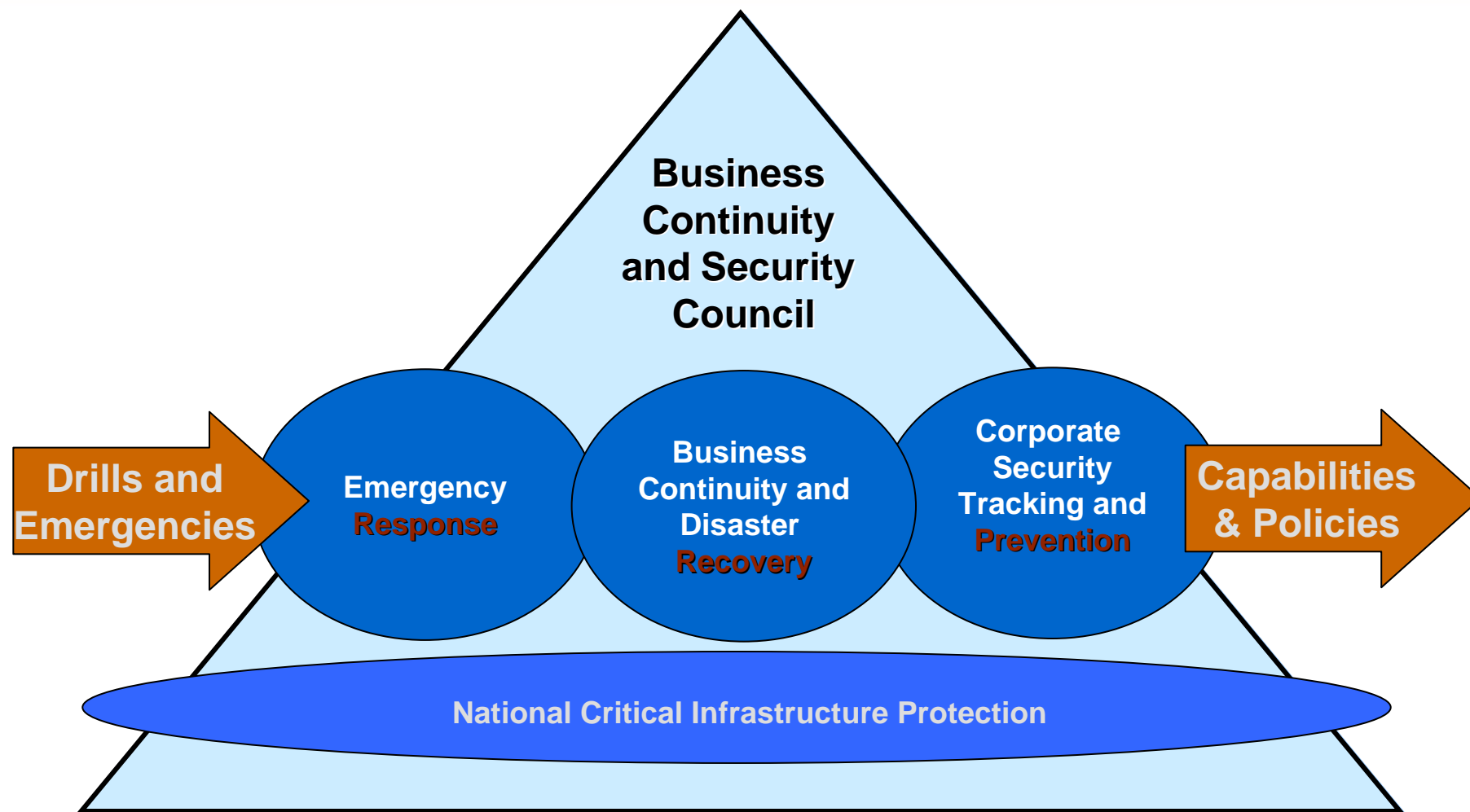


We had a good foundation but recognized that there continue to be new sets of challenges.

Emergency Management - Evolution



Governance Structure



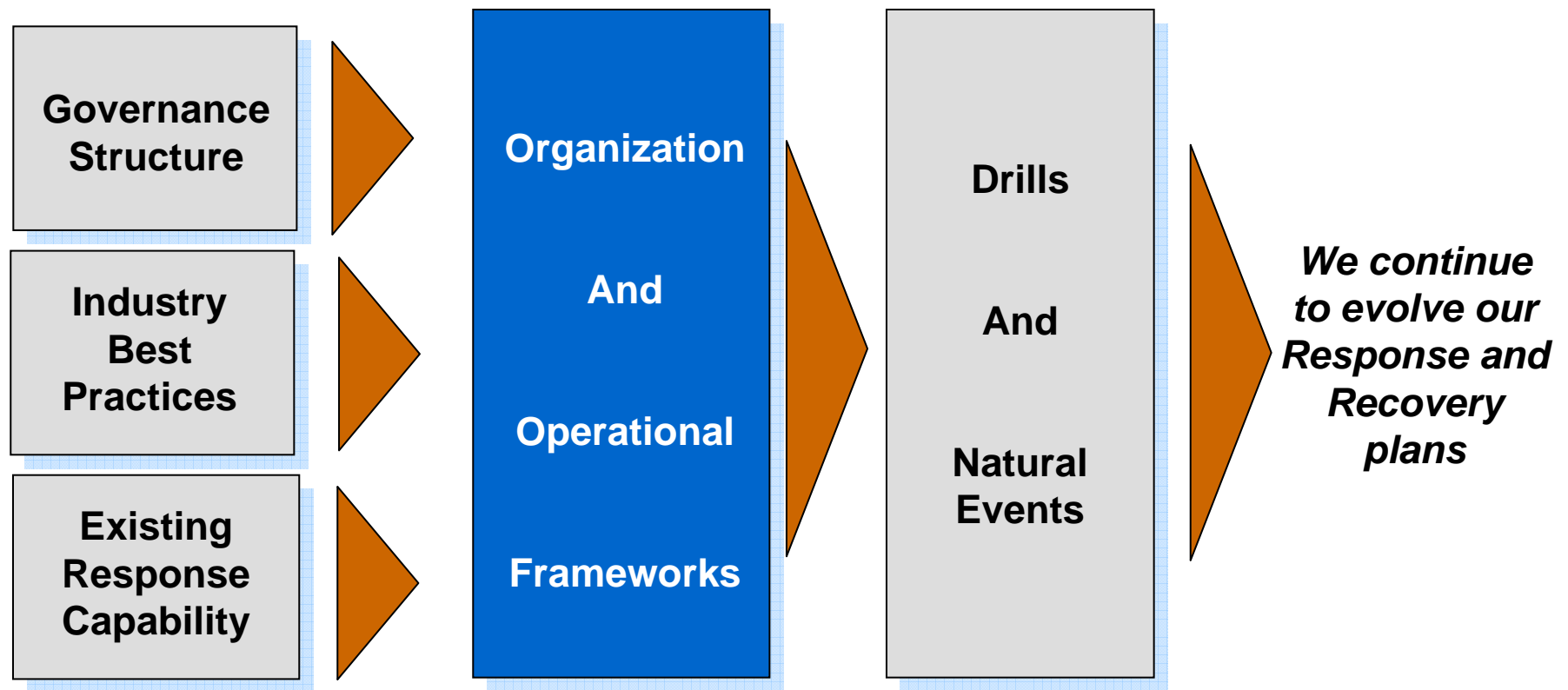
Response Capabilities

- 1200 Generators
- Primary and Backup Emergency Control Centers

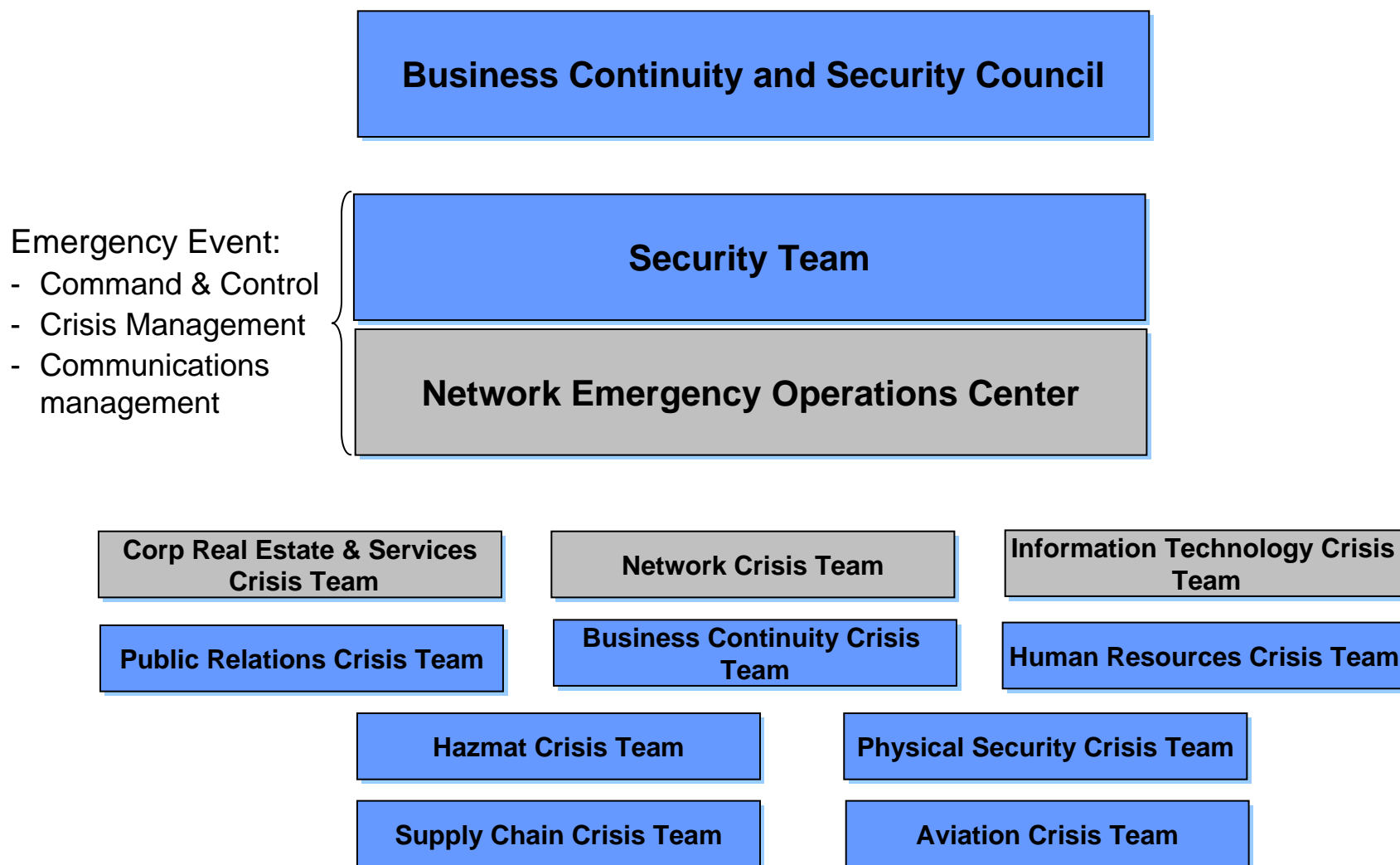


- 5 State-wide Emergency Operations Centers
- Portable Microwave Tower

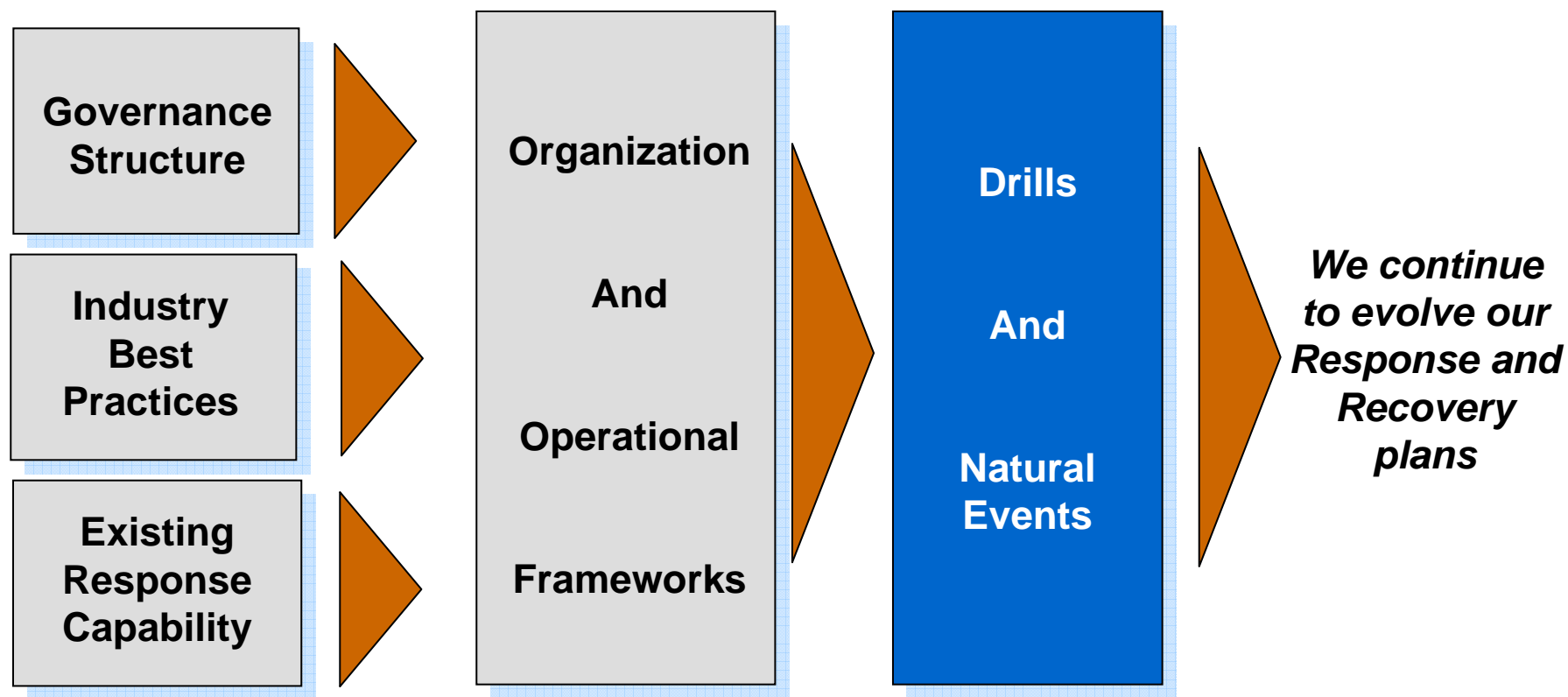
Emergency Management - Evolution



Emergency Management - Structure



Emergency Management - Evolution



BellSouth Threat Assessment

Threats

Cyber: Intrusions Attacks	Crime: Workplace Violence Violent Crime Fraud Theft Misuse	Terrorism: Chemical Biological Radiological Nuclear Explosive	Natural Disaster: Hurricane Tornado Earthquake Flooding	Industrial Accidents: Hazardous Materials Transportation	Medical: Epidemic Pandemic	Civil Unrest Riots Looting Breakdown of local authority
Cyber: Nov 05 – Email Worm & Compromised Data Drill May 04 – Sasser Worm Feb 04 – Broadband DoS attack Drill	Crime: June 05 - Workplace Violence Drill Mar 05 – Threats from Fla ex-employee with firearm	Terrorism: June 05 – Anthrax in mailroom Drill Mar 05 – Bombs in 2 BLS Buildings Drill Mar 04 – 911 style attack in Atlanta Drill	Natural Disaster: July 05 – Dennis Aug 05 - Katrina Sept 05 - Rita Oct 05 - Wilma 2004 - 4 hurricanes	Industrial Accidents: Jan 04 & May 04 – Chemical fires in Ga. June 04 – Chemical spill Jan 05 – Chemical spill in Graniteville	Medical: Feb 06 – Pandemic Drill	Civil Unrest Aug 05 - Katrina

Drills & Real Events

2002 – May 2006	Count
General & Executive Drills	29
Real Events	18
Total	47

Emergency Management 2006 Drill Plans

Scenario	Timing	Drill Focus
Flu Pandemic – infection is spreading. BellSouth response as impacts gets closer and finally when first employee is diagnosed	February	<ul style="list-style-type: none"> • Security Team Drill • Corporate response as BellSouth sees increased impact and finally has to address mass employee issues • HR, CRES, PR, etc., preparations • Gaps in existing policies and procedures
Communications Drill	May	<ul style="list-style-type: none"> • Security Team – 3N Notification test
Hurricane Preparedness – Are we ready?	May	<ul style="list-style-type: none"> • Security Team Drill • Ensure Crisis Team readiness • Katrina Lessons Learned implemented
Chemical spill at Charlotte Port due to hurricane	June	<ul style="list-style-type: none"> • Security Team / HAZMAT Crisis Team • HAZMAT Activation Decision Process • HAZMAT Chain of Command, Response, & Reporting
Corporate Airplane Crashes	July	<ul style="list-style-type: none"> • Aviation Crisis Team & Core Security Team Drill • Interaction of Aviation Crisis Team with Security Team and other Crisis Teams • Situation Management - skills and resources
Alternate communications drill – test communications capabilities with 2 way radios	July	<ul style="list-style-type: none"> • Chairman's Council & Security Team Drill • Drill utilizing 2 way radios for communications
Security Team Review of Corporate Aviation Disaster	August	<ul style="list-style-type: none"> • Security Team Drill • Understanding of policy changes • Identify corporate wide impacts and potential response gaps
Flu Pandemic – Activation of BC Plans	Aug/Sept	<ul style="list-style-type: none"> • BC Crisis Team / Security Team • BC Plans coordination across BUs – identify gaps and cross-BU issues
Communications Drill	October	<ul style="list-style-type: none"> • Security Team – 3N Notification test
Terrorism – 4 simultaneous explosions in Port of Miami and published threats of more planned across city. No BellSouth buildings involved in initial attacks.	November	<ul style="list-style-type: none"> • Security Team Drill • Building security decisions • Employee security decisions • Availability to manage all critical business functions

Emergency Management - Communication

Communications Bridges

Incident checkpoint briefings

Communications Hotlines

Ongoing status and information exchange

BellSouth Employee I'm Okay Line

Internal check to account for each employee

BellSouth Info-NOW

Ongoing status information to BellSouth employees

GETS

Increases probability of completing a wireline emergency call

Wireless Priority Telephone

Increases probability of completing a wireless emergency call

Satellite Phones

Communications via satellite technology

The collage includes several emergency communication cards and two mobile phones. The cards are:

- Security Team Emergency Communications**: A purple card with sections for Wireless Priority, Bus. Continuity Team, and Officer Emergency Communications. It provides steps for incident response and contact information for GETS Access and the Officer Emergency Bridge.
- TECH Community BC Leadership Communications**: A green card with contact information for the TECH Community Leadership Hotline (404-522-2751) and the Employee Emergency Hotline (877-257-4669).
- Security Council Emergency Communications**: A blue card with steps for incident response, contact information for GETS Access and the Security Council Bridge, and details for Wireless Priority Service.
- 1-XXX-BLS-Info-NOW (XXX-XXXX)**: A grey card with the BellSouth logo.
- 1-XXX-BLS-I'm Okay (XXX-XXXX)**: A grey card with the BellSouth logo.
- Government Emergency Telecommunications Service**: A blue card with a circular logo, a sequence of numbers (1 2 3 4 5 6 7 8 9 0 1 2), and contact information for Zachary L. Johnson at OMNCS - N2.

Two mobile phones are shown: a silver flip phone and a black satellite phone with an antenna.

Hazmat Capability

- Screened 100 Applicants, Selected 18 Members
- Completed Over 25 Training Courses
- 300 Hours of Drills



Emergency Management - Tools

Event Planning

Event Planning Home Page

Action Item Tracking

Execution Playbook

Situation Description	Actions
Virus being passed from human to human on other continents	<p>International travel restriction issued</p> <p>Internationally stationed employees evacuated</p> <p>Offshore Governance Council monitoring all offshore operations.</p> <p>Security Team placed on alert</p> <p>BC Crisis Team activated, monitoring events, working with BUs to address:</p> <ul style="list-style-type: none"> - Critical functions - Personnel availability - Supplies availability from JIT vendors - Telecommuting plans <p>HR Crisis Team activated & evaluating policies to address response to widespread flu outbreak</p> <p>EHS issued recommendations:</p> <ul style="list-style-type: none"> - Stockpile masks/gloves/protective supplies - Suppliers to utilize for protective supplies - Services changes (office cleaning, filter replacements, etc.) <p>Supply Chain ordered supplies as defined by EHS</p> <p>Contract resources utilized by Network to meet increased orders for telecommuting</p> <p>Pre-defined Employee Communications Plan activated</p>

Event Management

Event Management Home Page

Questions/Issues

Crisis Team Repository

Emergency Management – Scenario Planning

	Scenario #1	Scenario #2	Scenario #3	Scenario #4	Scenario #5	Scenario #6	Scenario #7
	Virus being passed from human to human on other continents - with significant transmission levels	First cases of human to human transmission of Avian flu in the United States confirmed – not in BellSouth region.	First infection confirmed in BellSouth region - not an employee	First BellSouth Employee infection confirmed - 1 metro area reporting infections	BellSouth Employee infections resulting in 5% of workforce absent for 2 weeks (Social Distancing in effect)	BellSouth Employee infections resulting in 25% of workforce absent for 2 weeks (Social Distancing in effect)	BellSouth Employee infections resulting in 40% of workforce absent for 3 weeks (Social Distancing in effect)
Security Team	Team placed on alert	Security Team activated - daily meetings Security Council on alert and receiving daily updates from team.	Security Team remains activated - daily meetings	Security Team remains activated - daily meetings	Security Team remains activated - daily meetings	Security Team remains activated - daily meetings	Security Team remains activated - daily meetings
HR	HR Crisis Team activated & evaluating policies to address response to widespread flu outbreak	Providing general guidance	Scenario #3 First infection confirmed in BellSouth region - not an employee			HR Crisis Team providing policy guidance - continuing. Employee response center remains activated. Corporate wide absenteeism reporting remains in place.	HR Crisis Team providing policy guidance - continuing. Employee response center remains activated. Corporate wide absenteeism reporting remains in place.
PR	Employee Communications Plan activated	Continue to execute Employee Communications Plan	Security Team	Security Team remains activated - daily meetings Security Council on alert and receiving daily updates from team.	HR	HR Crisis Team providing policy guidance for: - Employees who refuse to come to work - Supervisor's ability to send employee exhibiting flu symptoms home - Employee requesting to go home due to coworkers exhibiting flu symptoms Corporate wide absenteeism reporting process activated	Continue to execute employee communications plan. Use NewsFLASH for enterprise-wide announcements. Continue InfoNOW updates. Continuous updates to both intranet and Internet web pages. Continue BTN updates and banners on BNN as appropriate.
Corporate Security	International travel restrictions issued for certain locations if risk assessment of the transmission severity indicates it is warranted. Internationally stationed employees evacuated if the risk assessment warrants evacuation. Offshore Governance Council monitoring all offshore operations	International travel restrictions issued for certain locations if risk assessment of the transmission severity indicates it is warranted. Internationally stationed employees evacuated if the risk assessment warrants evacuation. Offshore Governance Council monitoring all offshore operations	PR	Continue to execute Employee Communications Plan - Leadership Team communication via BTN - Director and above letter distributed - NewsFlash published	PR	Continue to execute Employee Communications Plan - Leadership Team communication via BTN - Director and above letter distributed - NewsFlash published	International and domestic travel restrictions remain in effect. Offshore Governance Council monitoring all offshore operations. Executive Protection leadership continuity plan remains activated. Corporate security coordinates access to restricted areas if necessary. Corp security responds to potential civil unrest - coordinates with local law enforcement. External Security monitoring information from: World Health Organization Center for Disease Control (CDC) Department of Homeland Security Health & Human Services Impacted State and Local Emergency Management
			Corporate Security	International travel restrictions issued for certain locations if risk assessment of the transmission severity indicates it is warranted. Internationally stationed employees evacuated if the risk assessment warrants evacuation. Offshore Governance Council monitoring all offshore operations. All non-essential domestic travel restricted. External Security monitoring information from: World Health Organization Center for Disease Control (CDC) Department of Homeland Security Health & Human Services Impacted State and Local Emergency Management			

Ongoing Security Awareness

The screenshot shows the 'Security at BellSouth' website within a Microsoft Internet Explorer browser window. The website has a blue header with the BellSouth logo and navigation tabs for myBellSouth, BOB, CRES, HR Plus, Our People, Security, and Technology. The main content area is divided into several sections:

- Order InfoNOW and I'M OK Tools Today:** Includes phone numbers 1-xxx-BLS-Info_NOW and 1-xxx-BLS-I'm-OK, and a link to order key chain cards or badge stickers.
- Important Security Links:** A central column of links categorized under Corporate Security and Business Continuity, Emergency Management, Information Security, Corporate Security Standards, Building Access, and PC Security.
- Security Sense:** Features a 'Security Sense Feature Article' with a graphic titled 'WHAT TO DO?' and a link to 'More Articles...'. Below this is a 'Security Initiatives' section with an overview and calendar, and a 'Security Awareness Training' section with an update on the training class.
- Security Do's and Don'ts:** A section on the left with a list of guidelines for using company property and information.
- Online Security Training:** A section on the right with a link to 'The Security Awareness Training'.
- Ask Security and FAQ's:** A section at the bottom right with links for 'Email Us!' and 'Frequently Asked Questions'.

Callout boxes with arrows point to specific elements on the page:

- Important Security Links:** Points to the 'Important Security Links' section header.
- Regular SecuritySense Articles:** Points to the 'Security Sense Feature Article'.
- Online Security Training:** Points to the 'Security Awareness Training' section.
- Ask Security and FAQ's:** Points to the 'Email Us!' and 'Frequently Asked Questions' links.
- Corporate Security Standards:** Points to the 'Corporate Security Standards' link in the 'Important Security Links' column.
- PC Health Check – Cyber Fit Link:** Points to the 'PC Health Check' link in the 'PC Security' section.
- Security Do's and Don'ts:** Points to the 'Security Do's and Don'ts' section.

The Windows taskbar at the bottom shows the Start button, several open applications (My Documents, Security Update 10-2..., Presentation1, Security at BellSouth ...), and the system clock showing 10:05 AM on Tuesday, 11/15/2005.

Ongoing Security Awareness

© BellSouth and National Security Institute, Inc.

>> SecuritySense

Shelter-in-Place® The process of staying where you are and taking shelter, rather than trying to evacuate.

You've heard the phrase 'any port in a storm' but some ports are better than others. And for some accidents or emergencies, you are better off staying put rather than trying to evacuate.

BellSouth has a reputation for being prepared for emergency situations, whether fire, medical or weather related. Unfortunately, the possibilities for other types

In case of an emergency, Shelter-in-Place at BellSouth



ing is secure and sealed from outside air intrusion.

- If you have access to a radio, turn it on and monitor emergency broadcasts.
- If you are outside or in your vehicle, seek shelter. Do not try to get closer to the incident to see what happened. If

at home or in a BellSouth facility, the best course of action is to stay in place and shelter in place.

© BellSouth and National Security Institute, Inc.

© BellSouth and National Security Institute, Inc.

>> SecuritySense



Use PDF or HTML for BellSouth Internet sites

© BellSouth and National Security Institute, Inc.

>> SecuritySense

What to do? Leave it ON or turn it OFF?



In the past, as part of BellSouth's energy conservation efforts we were told to turn off computers and monitors at the completion of each shift. But then we were all told to leave the computers on so new software or patches can be installed.

WHICH IS IT?

While we continue to be concerned with conserving energy, the ability to quickly install security patches is more important in today's environment.

So leave your desktop computer powered on and your monitor turned off overnight and on weekends. You should never leave a laptop computer in a docking station overnight – always undock and lock it up or better yet take it with you.

Please remember to turn off lights and any power consuming devices whenever possible to save energy, but . . .

LEAVE YOUR DESKTOP COMPUTER ON WHEN YOUR SHIFT IS OVER.

>> SecuritySense



DATA PRIVACY

Are You a Security Risk?

Did you know a security breach can harm BellSouth's reputation - not to mention its profits? In a recent survey of 10,000 U.S. consumers, a whopping 92% of consumers who receive a security-breach notification blame the organization that suffered the attack. Almost a fifth – 19% – said such a notification prompts them to take their business elsewhere, and another 40% consider doing so.

The writing on the wall is hard to miss: all employees must do their part to make sure BellSouth's network and information remain secure, because a breach affects everybody.

Not only do security breaches cost businesses customers – they can cause lawsuits as well. Approximately 5% of respondents to the survey said they've hired a lawyer as a result of notifications. Legal experts point out that while 5% may not seem like a high figure, up to 50 million Americans have received notification of a security breach. That means more than 2 million U.S. consumers may have hired a legal beagle to sue businesses over security problems.

And, internal security breaches and information leakage resulting from internal personnel are a major concern. The risks of sensitive internal information leakage, and the risks posed by insiders, are most frequently identified as posing a very high compliance risk. BellSouth is giving a high priority to placing greater controls on information, such as sensitive content circulated within the organization or access to external information.

At a time when regulatory compliance and recent high-visibility security breaches continue to make headlines, BellSouth is placing a very high value on tools to secure sensitive information resources. You'll be hearing more about Data Privacy, what needs to be protected and how to protect it. Remember to protect other people's personal information you encounter everyday on your job just like it was your own.

Watch **SecuritySense** for more information on Data Privacy.

© BellSouth and National Security Institute, Inc.

>> SecuritySense

DON'T BE PHISH BAIT



In the past six months, phishing e-mails have grown much more sophisticated and difficult to spot. While early efforts were often unprofessional, typo-filled, and easy to identify, newer phishing scams tend to look extremely professional, include logos from reputable companies, and their e-mail messages are persuasive.

And, if you think of phishing as a threat to consumers only, think again: frequently, phishing victims fall for the ruses at work and give away confidential corporate data, customer records, network passwords, or trade secrets, jeopardizing their employer's intellectual property.

If you receive an e-mail that you suspect is a phishing attempt, please forward it to: Spam-Killer@BellSouth.Com. Please follow the instructions at <http://security.bls.com/spamheaders.htm> to ensure we have all the information needed to block the e-mail and any corresponding web sites.

ADDITIONAL TIPS TO KEEP FROM BECOMING PHISH BAIT:

1. When an e-mail message arrives from a company you don't do business with, delete it no matter how official it looks.
2. Check subject lines. Would Citibank ever send a legitimate e-mail with a subject like, "Citibank_account_update ACT-NOW"?
3. Think about the way genuine businesses want to interact with you. Your bank wants you to access it through its Web site, not by sending you an e-mail.
4. Read e-mails carefully. Phishers have grown much more sophisticated, but for many, English is a second language – so you're more likely to find typographical errors or awkwardly phrased sentences.
5. Never enter personal information in a form that you access by clicking a link in an e-mail. Chances are, the form is run by a phishing operation, and you are giving up your data to an ID theft ring. Either call the company's main switchboard (not a number you find in the e-mail) and ask for customer service, or visit the main Web site and click the customer service link. More information about phishing can be found at <http://security.bls.com/phishing.htm> <<http://security.bls.com/phishing.htm>>

Real Events – Hurricane Katrina



Real Events – Hurricane Katrina



Real Events – Chemical Spill

Graniteville Crash Site



January 6, 2005

Real Events - Chemical Spill

Chemical Spill Surrounding Area



Central Office
Graniteville, SC

Approximately
200 yards

Chemical Spill Site

Real Events – Chemical Spill

CO Air Filter Replacement



Real Events – Computer Worms & Viruses

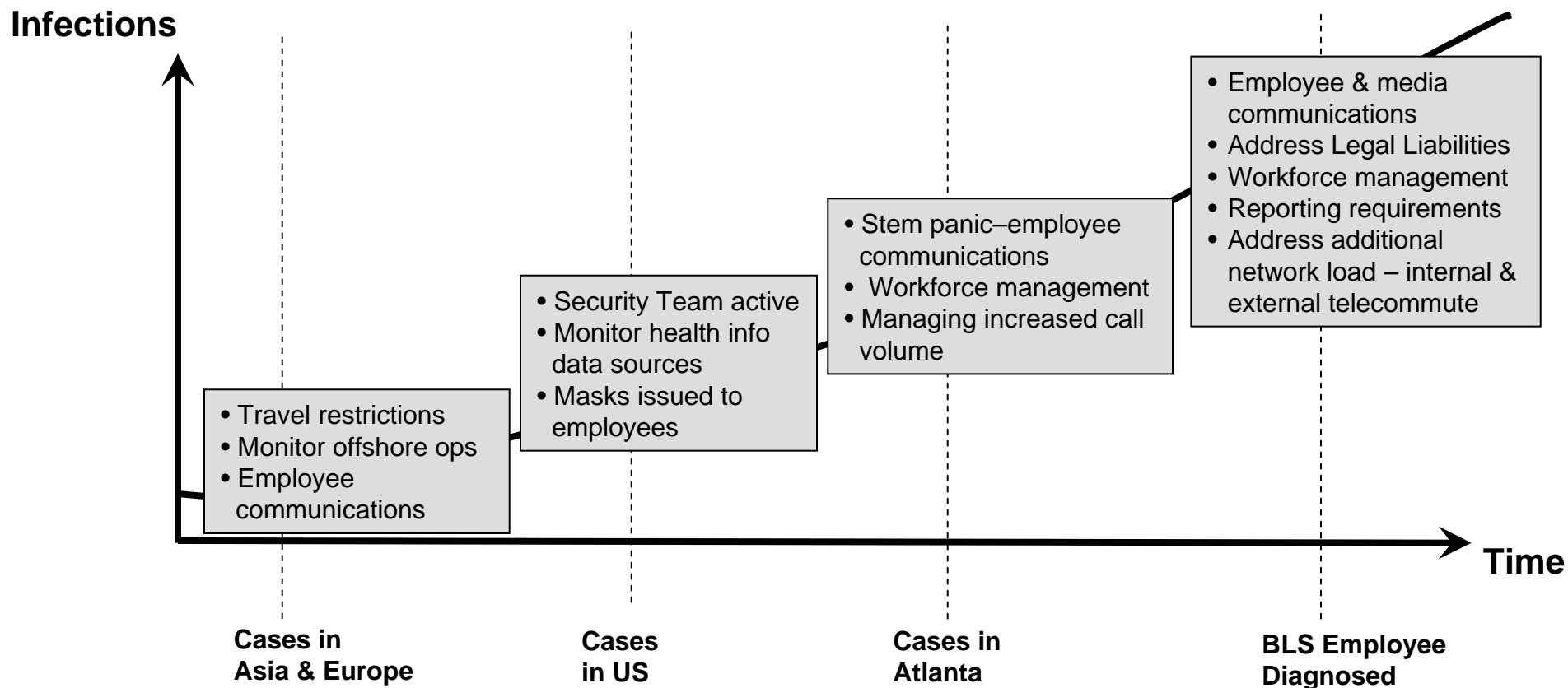
CYBER ALERT



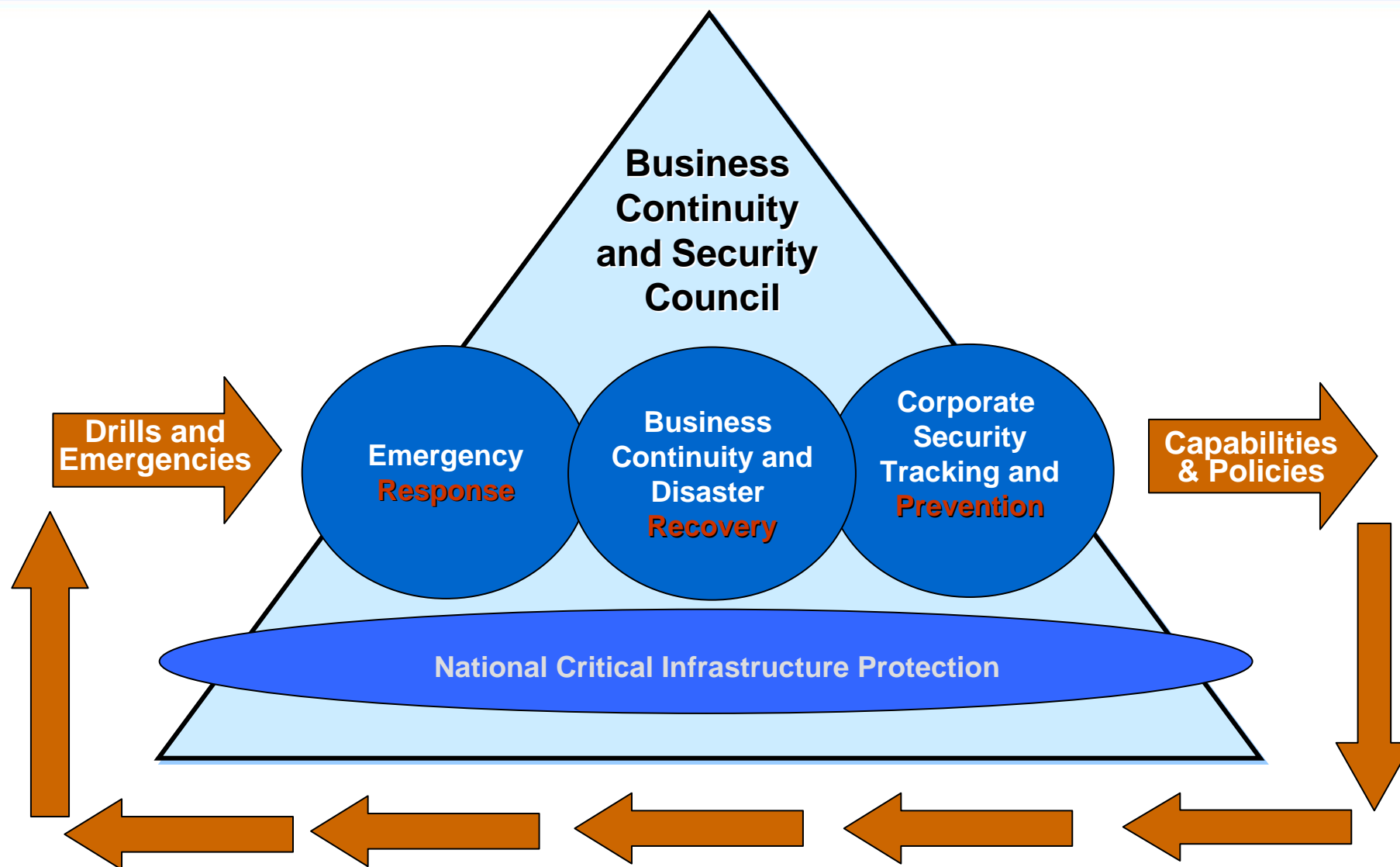
Call 1 XXX BLS Info NOW for Instructions

Pandemic Planning – Event Across Time

New Challenge - Response activities will be required over an extended period of time



Emergency Management Continuum



BELLSOUTH