Objectives and agenda

Leverage lessons learned from disaster recoveries in proactively building a Cyber Incident Response Plan

Agenda

- Overview of crisis
- Characteristics of leading practice Cyber Incident Response Plans
- Lessons learned
- Activating a Cyber Incident Response Plan
- Chaos framework
- Questions & answers
A crisis is...
More than just traditional events

**Unforeseen failures that threaten a company’s very existence**
- Chapter 11 bankruptcy due to financial losses and inability to meet covenants on debt facility.

**Complex systems fail, either through accident, mismanagement or sabotage**
- A massive explosion at a chemical plant caused by a fire

**Fraud or other criminal activity**

**Legal, commercial, geopolitical, or military conflicts**
- Labor strikes due to unsafe working conditions and poor compensation.

**Deliberate acts such as identity theft, product tampering, cyber-attacks, or cyber-crime**

**Unprecedented data breach compromising multiple user accounts**

**Natural or man-made destructive events that disrupt almost everything**
- The explosion of a power plant due to a hurricane, led to massive electricity outages.
Some leadership challenges

Leaders often have to take charge and rally their troops to avoid some common stumbling blocks such as...

- Excessive focus on fixing the incident, rather than leading the response and addressing the strategic impacts
- Failing to understand or underestimating the scale, breadth, and speed of the crisis and its unanticipated consequences
- Making inaccurate decisions and unintentionally causing harm, due to bad or incorrect information in the first few hours of a crises
- Not having enough time to make sense of the chaotic inflow of information and answering all of the direct inquiries
Establish the means to collect, analyze, and disseminate situational awareness to the stakeholders that need to be informed and/or take action.

Continuous monitor the internal and external environment, leveraging technology, to adapt your response to the incident.

Establish documentation (forms and process) to track the details of the event and response actions throughout the incident.

Lead coordination between outside public and private sector entities to respond to events that may involve regulatory issues, critical infrastructure and key resources.

Carefully select the incident response team members and make sure they have the requisite skills and experience to perform the roles they may be expected to assume.

Implement a comprehensive communication plan driven by executives. Tone and leadership need to be “set from the top”.

Develop and maintain a clear and concise set of guidelines and procedures to identify the actions, issues, and responsibilities that need to be addressed before, during, and after the incident.

Define a clear structure and order around decision rights, leadership succession, and other management controls.

Maintain a structured approach for analyzing the situation, identifying issues, assessing options, and taking actions.

Crisis Management Framework

Response Enablers

Response Organization

Crisis Management Plan

Control Hierarchy

Decision Making Process

Communications

Private — Public Coordination

Common Operating Picture

Information Management

Ongoing Monitoring

RESPONSE ORGANIZATION STRUCTURE

RESPONSE

Copyright © 2015 Deloitte Development LLC. All rights reserved.
Lessons learned from disaster recoveries
“At the local level, I think the biggest failure was leadership didn’t take into account the fact that poor residents had no way of evacuating. I also think Governor Blanco should have called for a mandatory evacuation sooner and that Mayor Nagin should have coordinated better with Amtrak.”

Terrol Williams
New Orleans Citizen and Evacuee
Select Committee Hearing, December 6, 2005
A Failure of Initiative
Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina
Lead decisively

- Act – taking no action is making a decision
- Always keep in mind your goals and objectives
- Focus on what you can control; accept what you cannot
- Avoid analysis paralysis – you will never have all the information
- Establish a clear, ongoing decision-making process
- Prioritize decisions based on their crisis impact
- Manage incidents locally, and crises as enterprise-wide

In a crisis, don't hide behind anything or anybody. They're going to find you anyway.

- Paul "Bear" Bryant
“Finding: Lack of communications and situational awareness paralyzed command and control.”
Continually frame the crisis

- Quickly diagnose the crisis with the available information
- Think ahead – anticipate how the crisis might progress
- Reassess everyday – do not fall in love with the plan
- Do not let the incidents distract you from the crisis
“Media reporting made the crowds in the Superdome anxious and scared away truck drivers carrying critical commodities.”
Actively communicate

- Own the story, don’t let the media tell it for you
- Be candid – communicate with honesty and personal commitment
- Convey consistent messages internally and externally
- Back your words with actions
- Control the narrative – communicate on a regular cadence
- Choose wisely who speaks – they will be the face of the organization
“[Hurricane Exercise] Pam was so very prescient. And yet Katrina highlighted many, many weaknesses that either were not anticipated by Pam, or were lessons learned but not heeded.

“That’s probably the most painful thing about Katrina, and the tragic loss of life: the foreseeability of it all.”

Chairman Tom Davis
Select Committee Hearing, December 14, 2005
Be ready for the unexpected

- Know that individuals may act differently under extreme pressure
- Realize that normal organizational roles may not apply to a crisis
- Avoid relying on a single person for successful navigation in a crisis
- Anticipate when and how external parties may steer the crisis
- Recognize your limitations – a crisis can test everyone’s breaking point
- Prepare to work with limited (or no) technology / information

If anything can go wrong, it will

- Capt. Edward A. Murphy ("Murphy's Law")
“If you get conflicting information from people you’re not sure of, then inaction may be, from your perspective, the most prudent form of action.”
Drive toward actionable intelligence

• Beware of confusing data and intelligence
• Focus on who needs to know what and by when
• Cast a wide net – important information can come from anywhere
• Qualify your sources – misinformation is as prevalent as information
• Recognize you will never have all the information
• Ramp up your ability to process data – do not let it bury you
• Record what you knew at the time of the decision

True genius resides in the capacity for evaluation of uncertain, hazardous, and conflicting information.

- Winston Churchill
Conclusion

Crisis and cyber incident management capabilities that are rehearsed and tested through simulations are integral to an organization’s ability to manage unforeseen incidents and crises.
**Chaos framework**

**COMMUNICATIONS.** Build your formal and informal networks. Seek out whoever is most likely to have the information. Communicate up and down, and inside and outside your organization.

**HAVE A PLAN.** Be prepared to respond. Model events so you can anticipate the potential impact and develop processes for managing them. Incorporate planning for recovery. Conduct training exercises. Keep the plan current, and continually reassess the impact of fast-changing technology on it.

**ACT ON THE PLAN.** Make decisions. Resist inertia at all costs. Use the information you have to inform your decisions; it can make all the difference. Be mindful of what’s taking place outside your perimeter - the secondary and tertiary - that directly influence the effectiveness of your plan. And be prepared to adjust. Your response will determine the extent of recovery; full recovery is not guaranteed.

**ONLY THE CRISIS.** Stay focused. Keep everyone on point. Emotions are running high; don’t let yours.

**TODY THE CRISIS.** After the dust has settled, assess what the experience says about your overall approach to managing risks. What worked and didn’t work? How can we use this crisis to become stronger and more resilient?

Being **SECURE**
means having risk-prioritized controls to defend critical assets against known and emerging threats.

Being **VIGILANT**
means having threat intelligence and situational awareness to anticipate and identify harmful behavior.

Being **RESILIENT**
means being prepared and having the ability to recover from cyber incidents and reduce their impact.
Contact

Mike Wyatt  
Director | Deloitte Advisory  
Cyber Risk, US Identity Solutions Leader  
Deloitte & Touche LLP  
miwyatt@deloitte.com

Linus Akanoh, Jr.  
Senior Manager | Deloitte Advisory  
Strategic Risk | Crisis Recovery  
Deloitte & Touche LLP  
lakanoh@deloitte.com
This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.