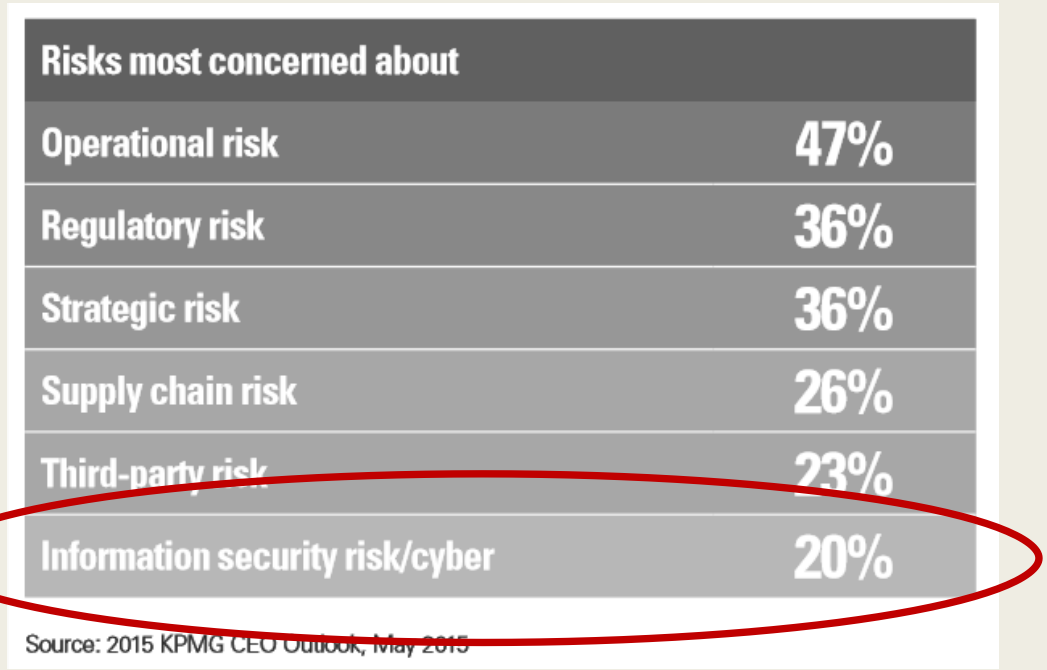
WHEN CYBER-SECURITY & CRISIS MANAGEMENT MEET

ASIS NYC - Session 1204
April 27, 2016 – 10 am

Top Executive Risk Concerns

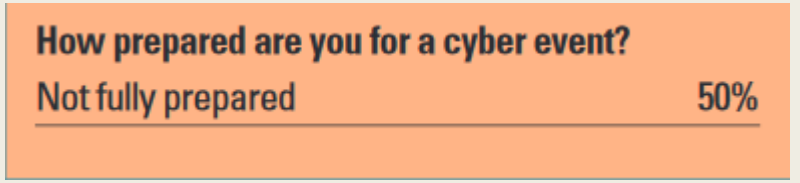


Risks most concerned about	
Operational risk	47%
Regulatory risk	36%
Strategic risk	36%
Supply chain risk	26%
Third-party risk	23%
Information security risk/cyber	20%

Source: 2015 KPMG CEO Outlook, May 2015

"Any CEO who really understands risk knows that cyber is possibly the most unpredictable risk there is,"
- Malcolm Marshall, KPMG's Global Head of Cyber Security.

"Half of the CEOs in our survey report they are not fully prepared for a cyber event. Yet, cyber security was named by 20 percent of respondents as one of the top five risks"

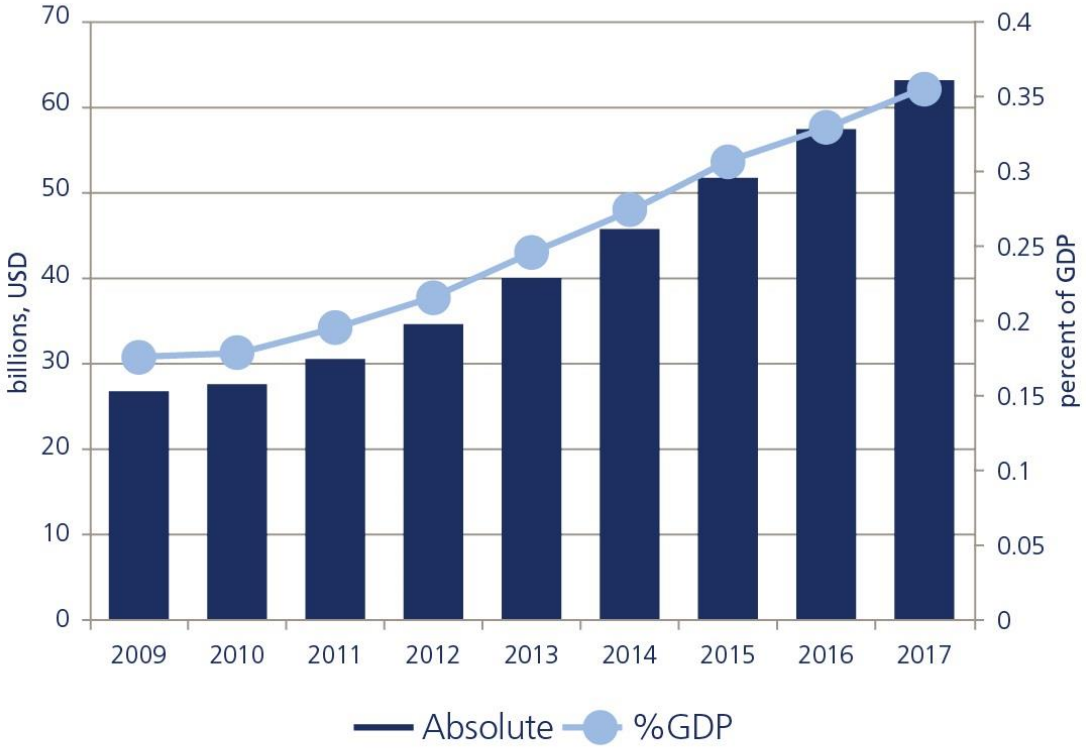


How prepared are you for a cyber event?	
Not fully prepared	50%

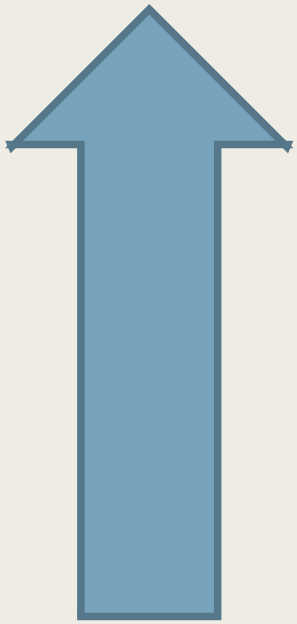
Source: KPMG Global CEO Outlook 2015 – www.kpmg.com/CEOoutlook

Spending on Cyber Security

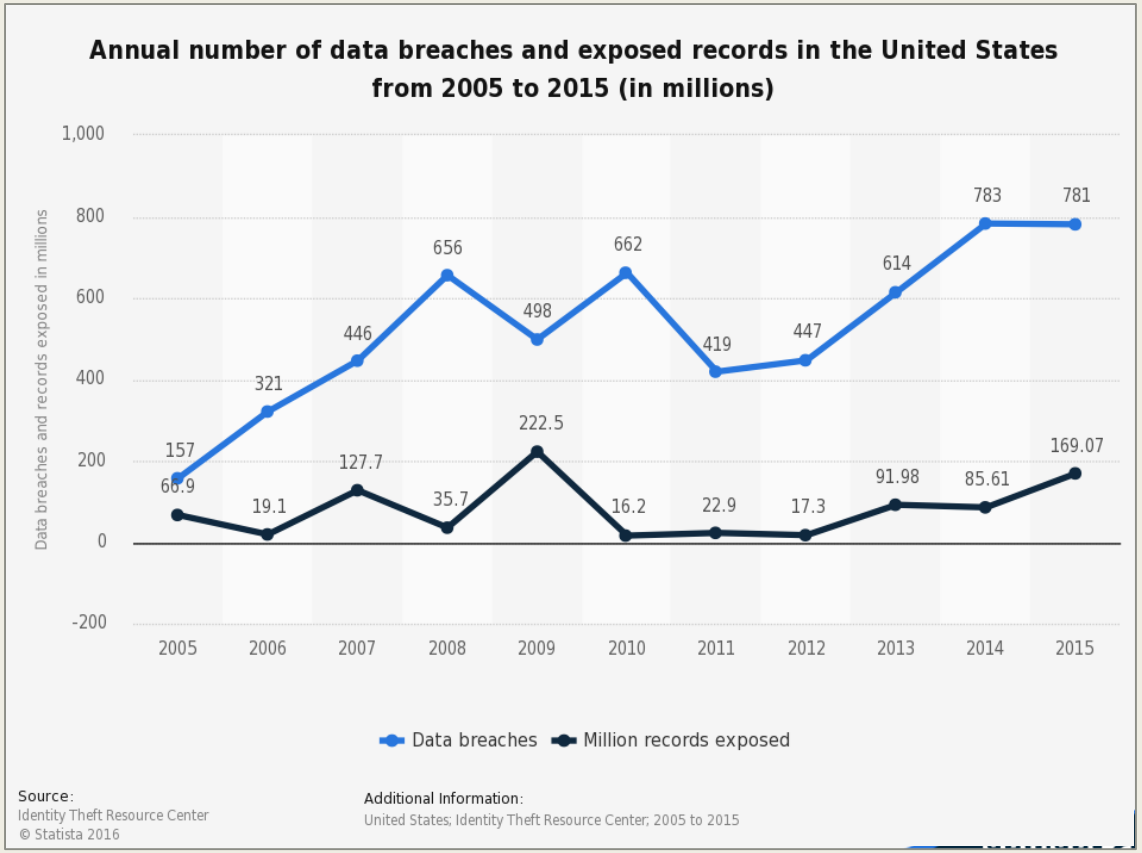
Figure 8: Cybersecurity spending in the U.S., percent of GDP and USD billions, 2009-2017

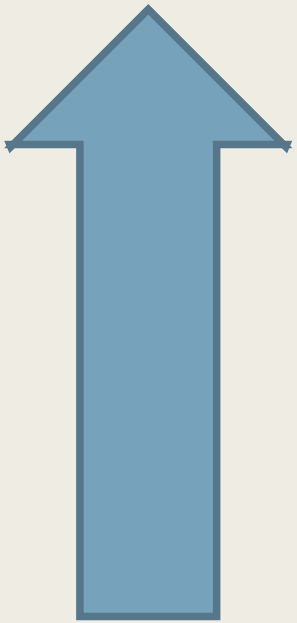


Source: TIA's 2010-2017 ICT Market Review and Forecast, available at: http://test.tiaonline.org/resources/market-forecast

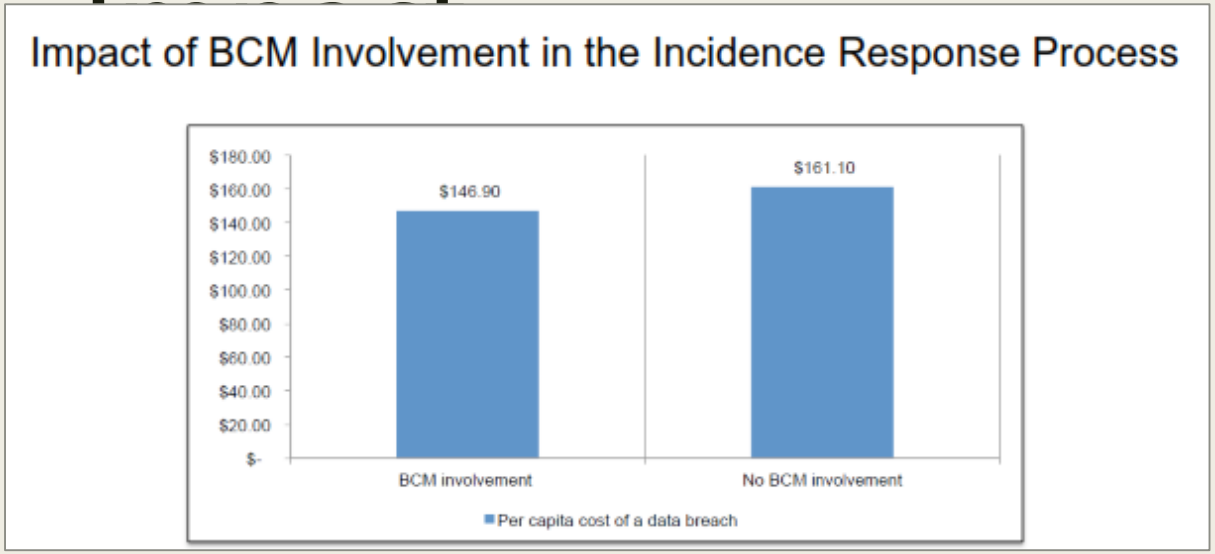


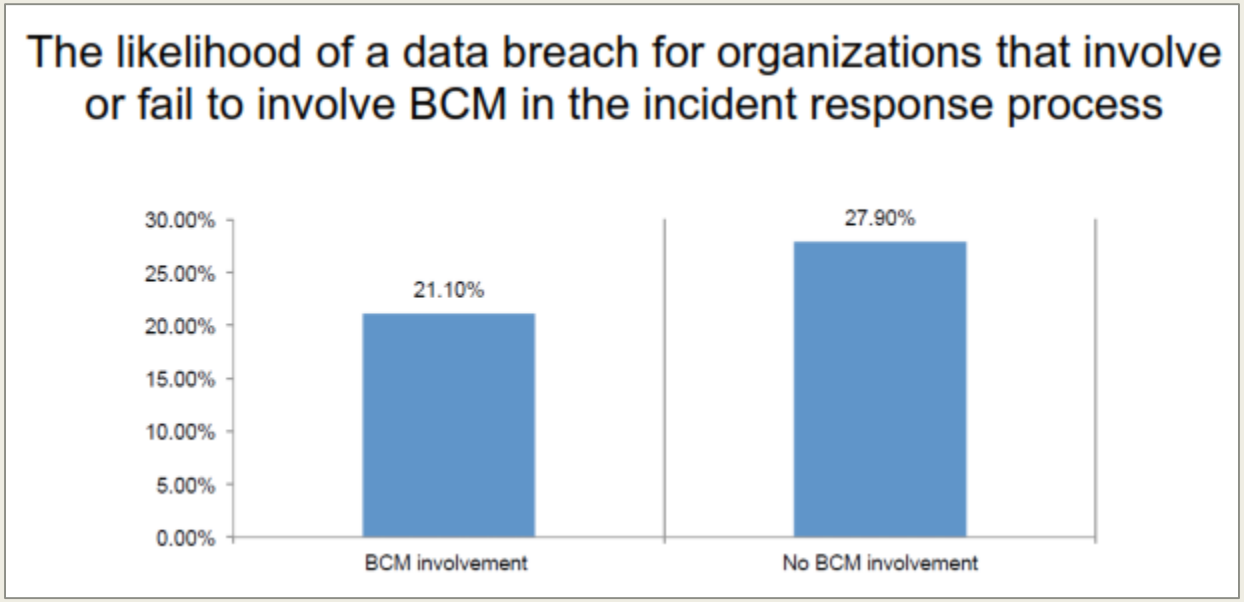
Cyber Security Incidents





Cyber Security Cost / Impact





Source: Ponemon 2015 Cost of Data Breach Study

Time To Get Prepared

"It is only a matter of the when, not the if, that we are going to see something dramatic,"

- Admiral Michael Rogers
Director , National Security Agency
Commander of U.S. Cyber Command

Preparing for a Cyber Crisis

- Q: Don’t cyber crisis events “belong” to IT?
  - *A: No*

What IS a Cyber Crisis?

- "Cyber" is not an incident, it's an environment.
  - *"...As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare. Although cyberspace is a man-made domain, it has become just as critical as land, sea, air and space.*

    - General Michael Hayden, Former Director, CIA and NSA

"Traditional" Crisis Incident	"Cyber" Crisis Incident
Critical software prototype lost to a fire in the data center.	Critical software prototype lost to a cryptolocking hack.
Customer care call center shut down due to a regional blackout.	Customer care call center shut down due to a network DDOS attack.
Manufacturing center lost for 3 days to flood	Manufacturing center lost for 3 days to SCADA system hack

It's Not Just "Information" Anymore…

Information Technology	Operational Technology
Databases	SCADA systems
Networked Servers	Networked Physical Access Control
Communications Lines	Manufacturing Lines

- June 2010 – Iran confirms Stuxnet Work halted centrifuges
- April 2011 – Hackers breach Playstation network and block access
- August 2012 – Saudi Aramco hit by a virus aimed at stopping oil and gas productions
- September 2012 – NJ PATH system hacked for free rides
- April 2013 – False AP Tweet sets off stock market sell-off
- February 2014 – WIRED story on potential issues of hacking airport x-ray machines.
- August 2014 – Hacker accesses airplane systems

Preparing for a Cyber Crisis

- Q: Don't cyber crisis events "belong" to IT?
  - *A: No*

- Q: Does IT have a role in planning and responding to a cyber crisis?
  - *A: Yes!*

  … *And so does*
    - Public Relations
    - Customer Care
    - Operations
    - Executives
    - Any impacted business group

Preparing for a Cyber Crisis

- Q: What's security's role in crisis management for cyber crisis events?
  - *A: The same as security's role in all crisis management*
  - *Enterprise Security Risk Management*
    - Ensuring risk identification and prioritization
      - *Work with your strategic partners in IT and with critical risk stakeholders*
    - Ensuring mitigation and response planning
      - *Assist in determining tasks and in performing security task management*
    - Coordinating the response with the crisis team
      - *Crisis calls, notifications, awareness, administration*

Preparing for a Cyber Incident

- Q: How are cyber incidents different than other types of incidents?
  - *A: They really aren't… except where they are.*

  - *… and don't bring an earthquake plan to a cyber event.*

Preparing for a Cyber Crisis

- What do you need to prepare for a cyber crisis?
  - *A Prevention and Mitigation Program*
    - Identify risks
    - Identify mitigation tactics
    - Enact mitigations
  - *A team*
  - *A response plan*
  - *Continual improvement*

- The difference is in the details…

Prevention and Mitigation Program:
IT - Cyber Defense Center

- Objective: contain and mitigate cyber security incidents in a timely manner.
  - *24 x 7 Surveillance*
  - *Reporting path for incidents*
  - *Initial incident handling*
  - *Incident escalation*

- Keep an Incident From Becoming a Crisis

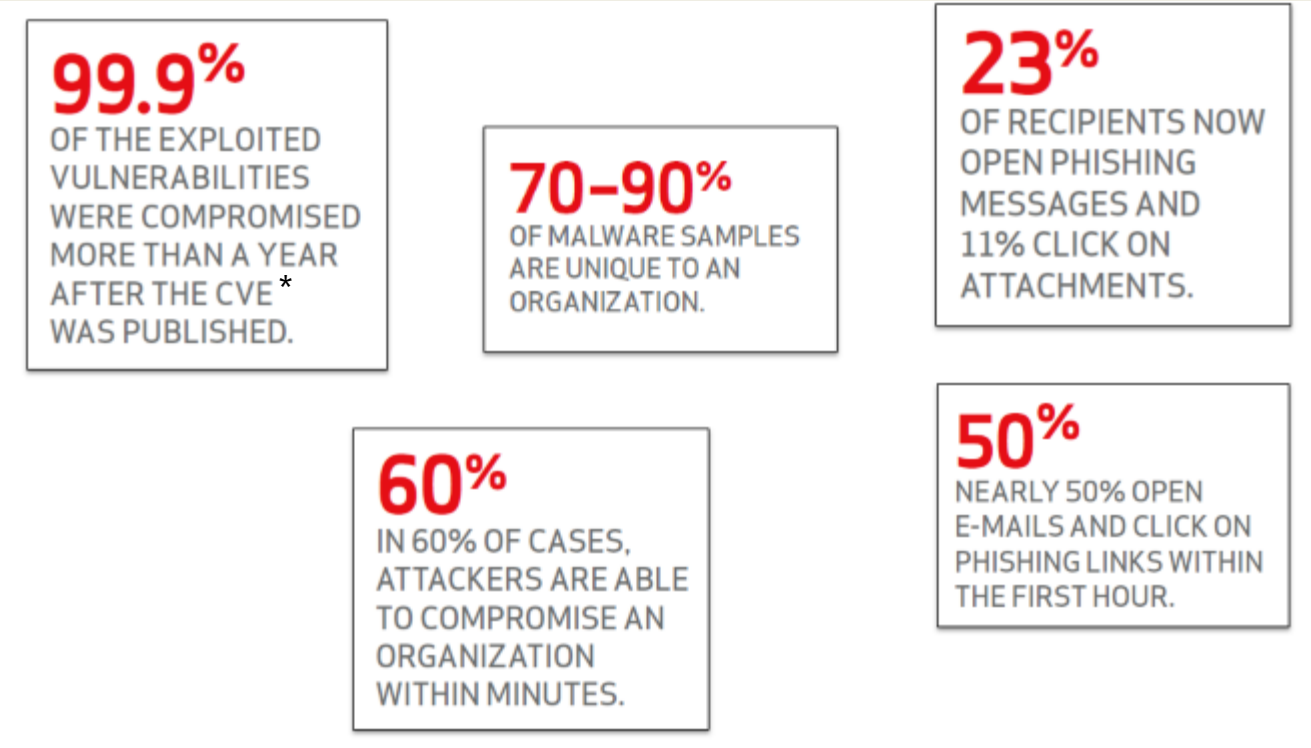
Prevention and Mitigation Program: IT – Monitoring

- **Incident**: 5 employees click on a phishing link and download a virus that locks their computers.
- **Crisis**: 500 employees click on a phishing link and download a virus that locks their computers.
- **Defense and Monitoring**: Block the offending email and scrub it from the email system as soon as it is discovered.

- Keep an Incident From Becoming a Crisis

Prevention and Mitigation Program: What's The Risk?

- Keep an Incident From Becoming a Crisis



* Common Vulnerabilities and Exposures

Source: Verizon 2015 Data Breach Investigation Report - http://www.verizonenterprise.com/DBIR/2015/

Prevention and Mitigation Program: Reduce The Risk

- **Harden Your Systems**

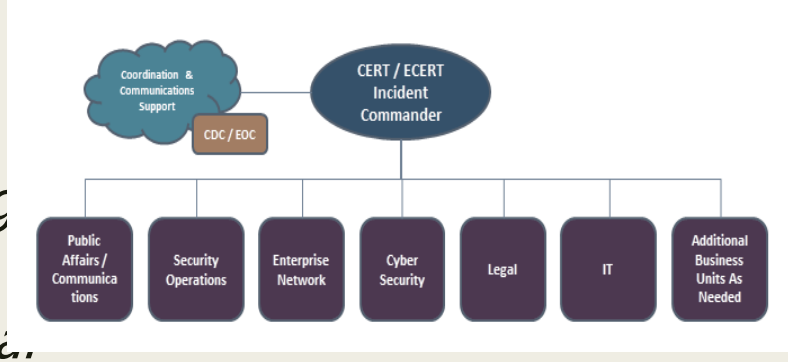
- Keep an Incident From Becoming a Crisis

- **Security Awareness!**
  - *The most important non-hardware, non-software solution available.*
  - *An informed user is a user who behaves more responsibly and takes fewer risks.*

Crisis Response: A Team and A Plan

- Cyber Emergency Response Plan
  - *Incident Criteria to Move to "Crisis"*
- Cyber Emergency Response Team (CERT)
  - *Management level, strateg group*
  - *Key individuals from critica areas of the business*
  - *Evaluates the threat and determines the best business strategy to contain, eradicate and recover from the threat.*

- This Incident Has Become A Crisis



Crisis Response: A Team and A Plan

- CERT Considerations Checklist

- This Incident Has Become A Crisis

Consider:
Does the event warrant retaining outside investigation teams?
Does the event warrant retaining outside counsel to direct the response?
Does the event require involvement from the executive level?
Does the event notification to law enforcement / customers/employees/agencies?
Does the event require a media communication?
Does the event include potential breach to customer cardholder data?
Does the event include a system that is in scope for PCI?
Is the event on-going? If so, should a system be shut down until the event is remediated?
If there is a data breach involving customers or employees, what are the resident states and how many people are within each state?
Is PII implicated? If so, notify Legal.
Should Senior Management be contacted?
Which business group owns the system that was breached and are they aware of the issue?

Crisis Response: A Team and A Plan

- Escalation Paths and Teams
- **Executive** Cyber Emergency Response Team
  - *Strategic group of key corporate executives*
  - *Primary objective is public safety and the protection of customers, employees, revenues, assets and resources.*

- This Incident Has Become A MAJOR Crisis

Continual Improvement

- Post Incident Reporting and Assessment
  - *Residual Risk?*
  - *Additional Mitigation?*
  - *New Risks?*

Lessons Learned	Recommendations
Exactly what happened and when?	Tools, resources, procedures needed?
How well did staff and management perform?	ESD – Asset Inventory Updates
How could information sharing have been improved?	Knowledge base updates
	Communication improvements