Incident Response Plans: The Emergency Shutoff Control for Cyber Risk

Tabitha Greiner, Acumera

Chris Lietz, Coalfire

Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

Housekeeping

This webinar is being recorded and will be made available in approximately 30 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions

Email: **info@conexxus.org**

Presenters

Conexxus Host

Allie Russell
Conexxus
arussell@conexxus.org

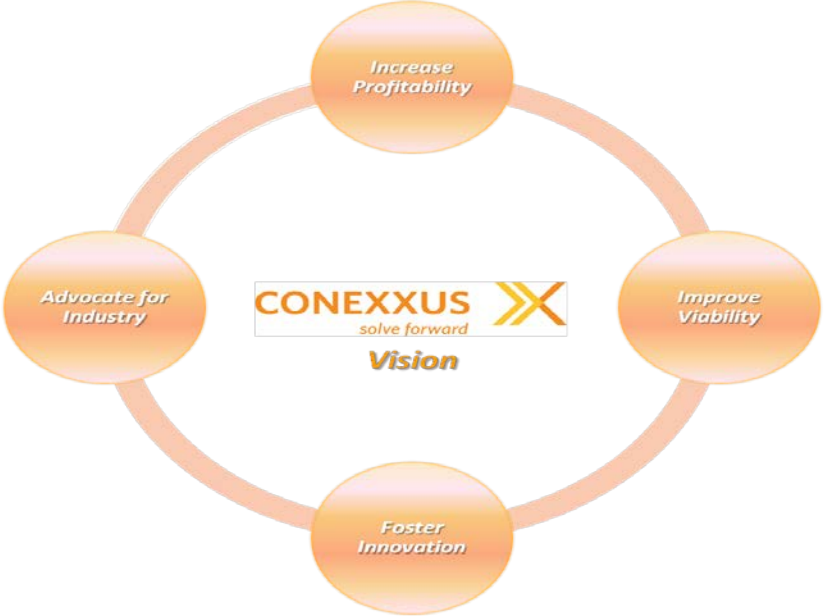
Speakers

Chris Lietz,
CISSP, CRISC, CISM, CISA, CTPRP
Principal, Coalfire
Chris.Lietz@coalfire.com

Tabitha Greiner
CISSP, ISA
CSO, Acumera
tabitha.greiner@acumera.net

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy



2016 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
August 25, 2016	Incident Response Plans: The Emergency Shutoff Control for Cyber Risk	Chris Lietz Tabitha Greiner	Coalfire Acumera
September 15, 2016	Protecting Retail ATMs: A guide to preventing and detecting skimming	Al Jamir Bruce Renard	Cash Depot National ATM Council
November 17, 2016	Cyber Security		Hughes
December, 2016	TBD		

If you have a suggestion for a webinar, please contact Conexxus at info@conexxus.org.

Join Conexxus in Atlanta for Technology Edge at the NACS Show

NACS Show

October 18-21, 2016

Atlanta, GA

nacsshow.com/technologyedge

TECHNOLOGY
EDGE

In partnership with
CONEXXUS

2017 Conexxus Annual Conference

Loews Annapolis Hotel

Annapolis, Maryland

April 23 – 27, 2017

CONEXXUS

solve forward

Agenda

- The Case for Being Prepared
- Developing and Implementing an IRP

The Case For Being Prepared

Recent Headlines

- Impacts:
- Fraud / Theft
- Loss of Sensitive Information (e.g., PII, ePHI, Card Data Trade Secrets)
- Third-Party Security Lapses
- Disruption (e.g., Ransomware)
- Reputational Harm
- Fines / Penalties

CiCi's Pizza

Wendy's

TARGET

Anthem Blue Cross

SONY PICTURES

INSPECTOR GENERAL U.S. OFFICE OF PERSONNEL MANAGEMENT

THE HOME DEPOT

Eddie Bauer

ORACLE

micros

Attacks are Increasing

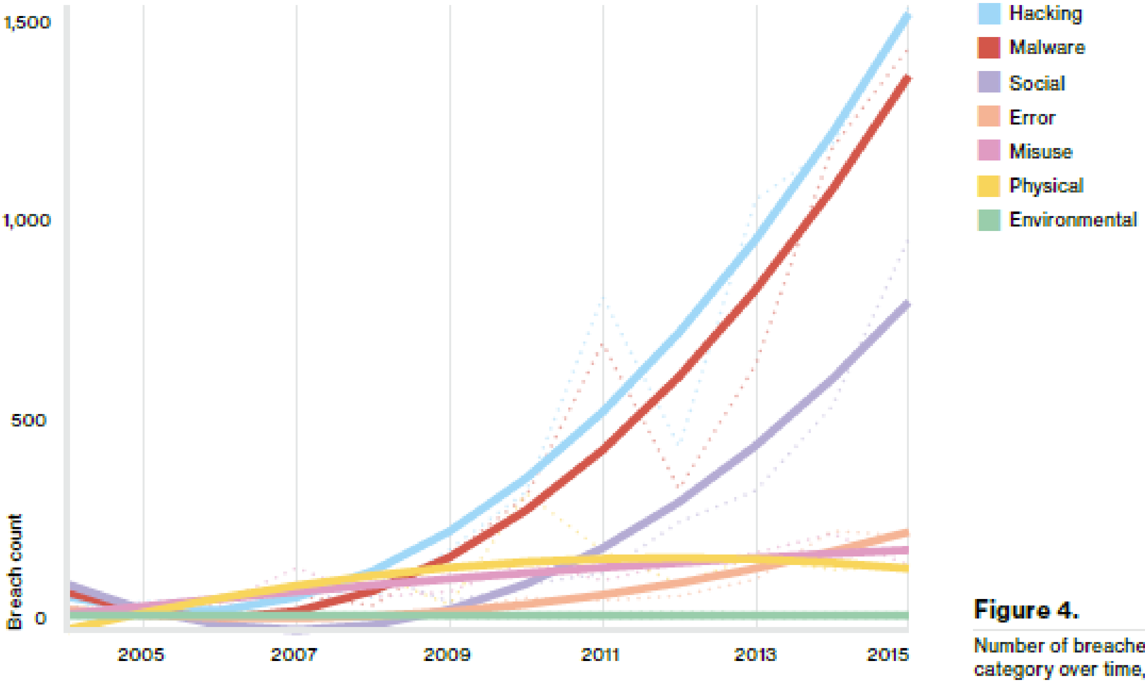


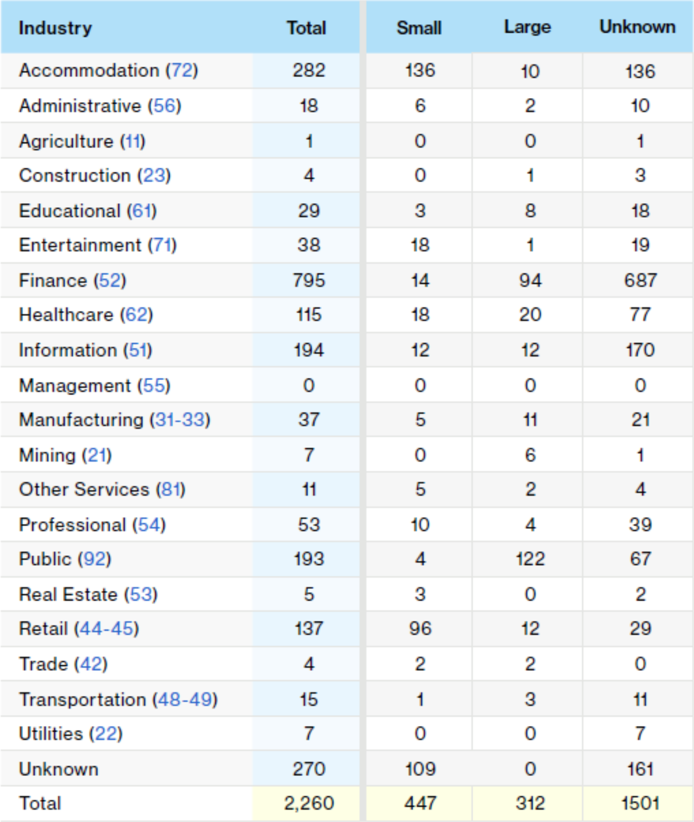
Figure 4.

Number of breaches per threat action category over time, (n=9,009)

Source: Verizon 2016 Data Breach Investigations Report

Everyone is at Risk

Your size will not protect you!



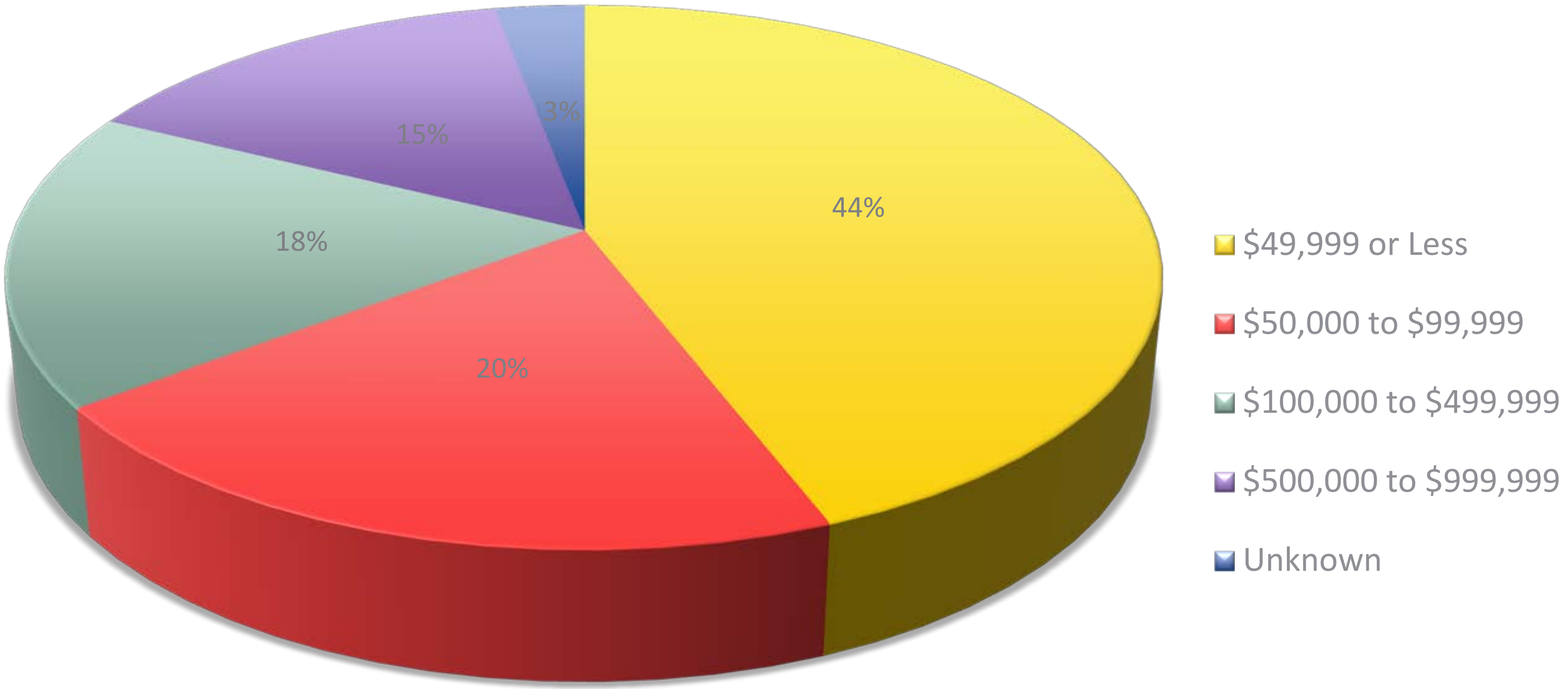
Industry	Total	Small	Large	Unknown
Accommodation (72)	282	136	10	136
Administrative (56)	18	6	2	10
Agriculture (11)	1	0	0	1
Construction (23)	4	0	1	3
Educational (61)	29	3	8	18
Entertainment (71)	38	18	1	19
Finance (52)	795	14	94	687
Healthcare (62)	115	18	20	77
Information (51)	194	12	12	170
Management (55)	0	0	0	0
Manufacturing (31-33)	37	5	11	21
Mining (21)	7	0	6	1
Other Services (81)	11	5	2	4
Professional (54)	53	10	4	39
Public (92)	193	4	122	67
Real Estate (53)	5	3	0	2
Retail (44-45)	137	96	12	29
Trade (42)	4	2	2	0
Transportation (48-49)	15	1	3	11
Utilities (22)	7	0	0	7
Unknown	270	109	0	161
Total	2,260	447	312	1501

Table 2.

Number of security incidents with confirmed data loss by victim industry

Source: Verizon 2016 Data Breach Investigations Report

Incidents Are Costly



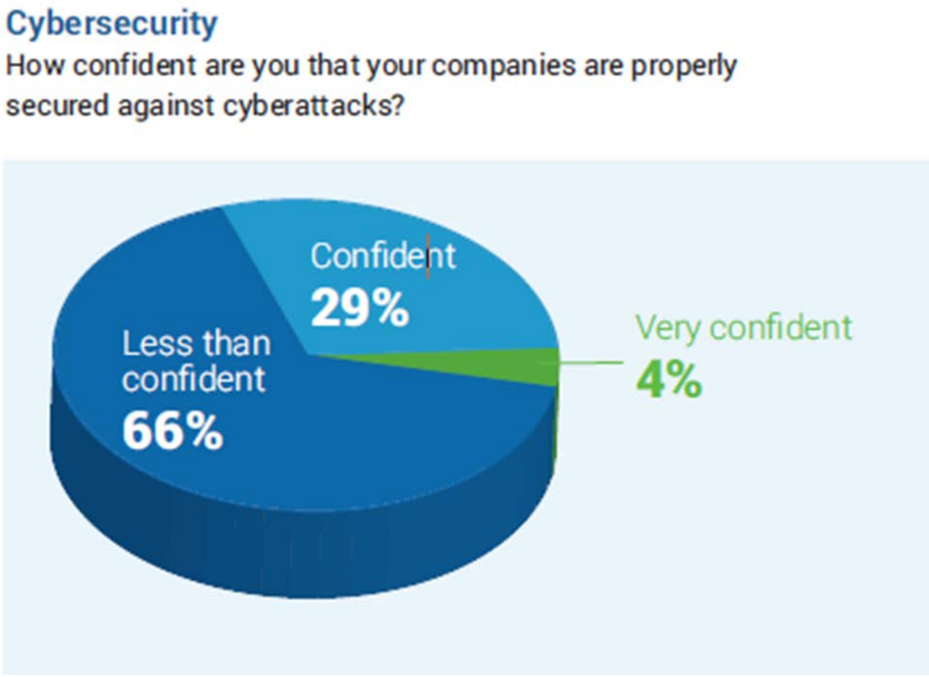
Source: The Global State of Information Security Survey 2016

CONEXXUS solve forward

Management is Concerned

- More than 80% of public company board members report that cybersecurity is discussed at most or all boardroom meetings

- A surprising 66% of them are not fully confident their companies are properly secured against cyberattacks



Cybersecurity

How confident are you that your companies are properly secured against cyberattacks?

Source: 2015 Survey Cybersecurity in the Boardroom, NYSE Governance Series

PCI Compliance Requirement

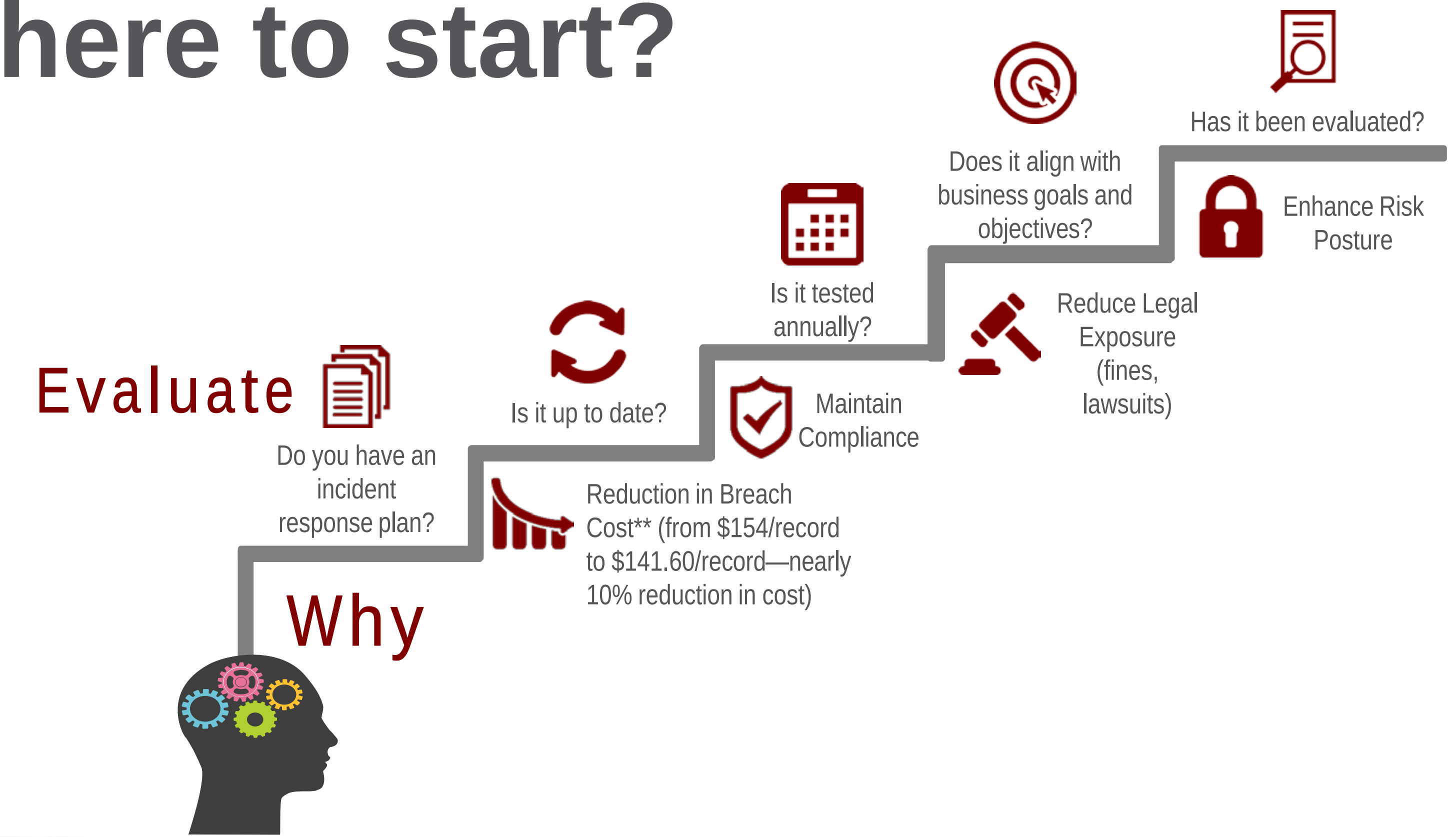
- 11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.

- 12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

- 12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.
  - 12.10.1 Create the incident response plan to be implemented in the event of system breach.
  - 12.10.2 Test the plan at least annually.
  - 12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.
  - 12.10.4 Provide appropriate training to staff with security breach response responsibilities.
  - 12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.
  - 12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

Developing and Implementing an IRP

Where to start?



Evaluate

Do you have an incident response plan?

Is it up to date?

Is it tested annually?

Does it align with business goals and objectives?

Has it been evaluated?

Why

Reduction in Breach Cost** (from $154/record to $141.60/record—nearly 10% reduction in cost)

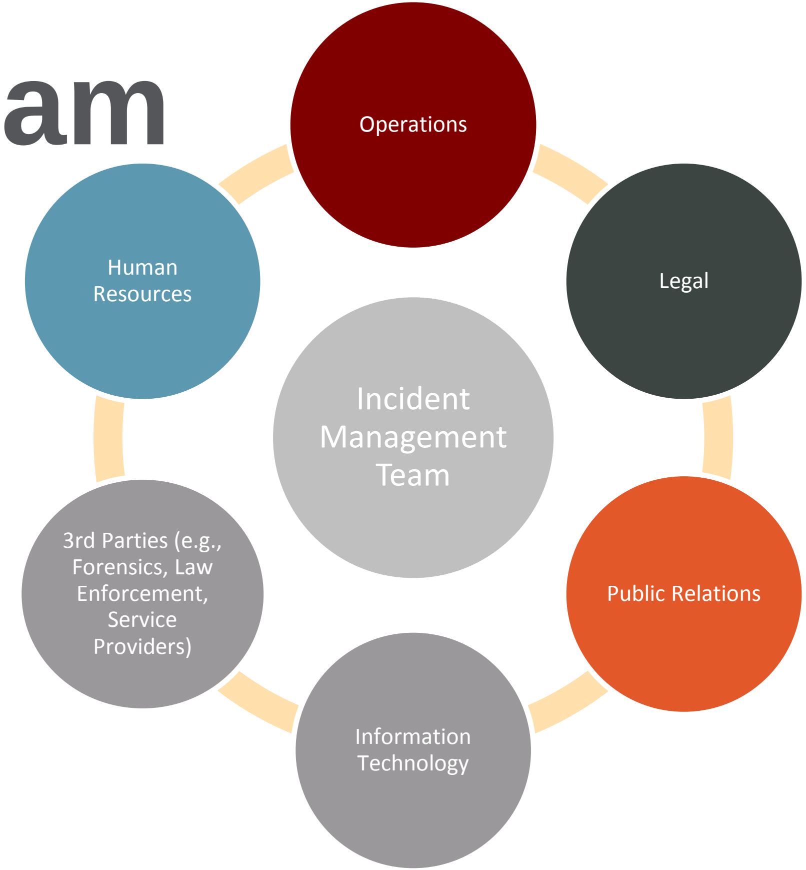
Maintain Compliance

Reduce Legal Exposure (fines, lawsuits)

Enhance Risk Posture

Assemble Your Team

- Cross-functional team
- Multiple third parties
- Specialty skills / contacts



Incident Management Team

Operations

Legal

Public Relations

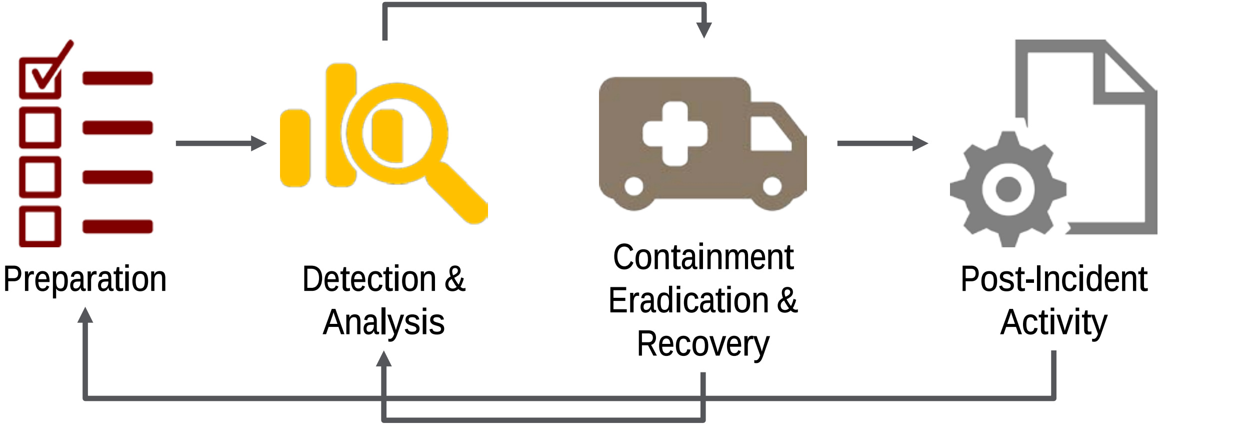
Information Technology

3rd Parties (e.g., Forensics, Law Enforcement, Service Providers)

Human Resources

Adopt a Framework

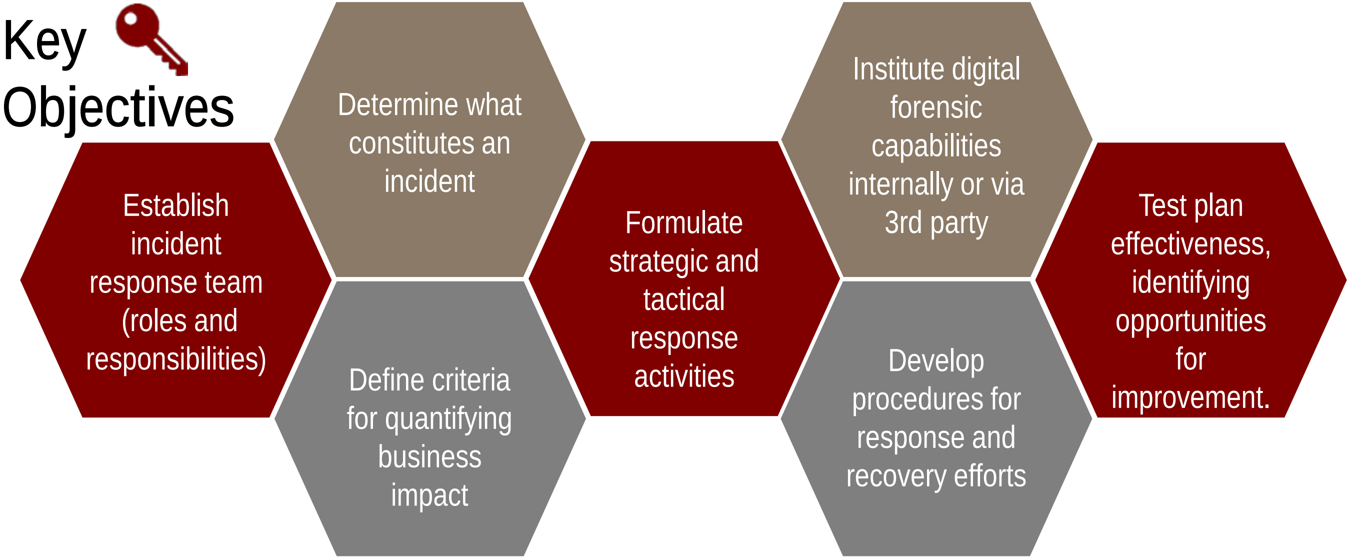
E.g., NIST 800-61R2



Preparation

Enabling more efficient recovery from events and incidents.

Key Objectives



Establish incident response team (roles and responsibilities)

Determine what constitutes an incident

Define criteria for quantifying business impact

Formulate strategic and tactical response activities

Institute digital forensic capabilities internally or via 3rd party

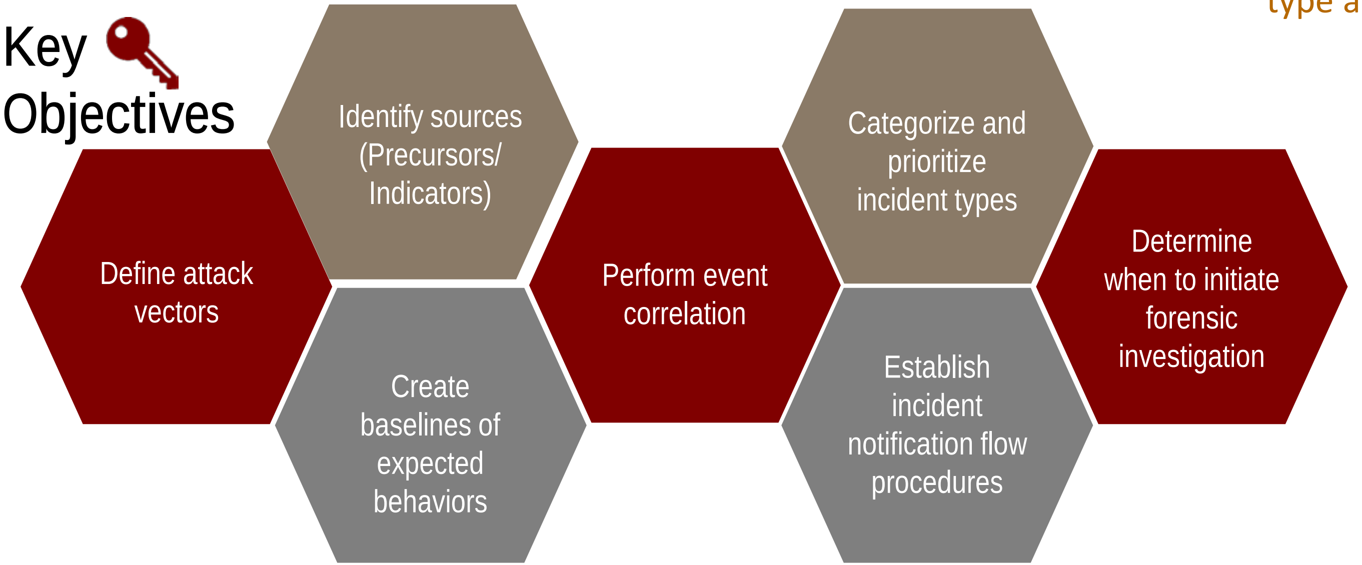
Develop procedures for response and recovery efforts

Test plan effectiveness, identifying opportunities for improvement.

Detection and analysis

Outlines the framework
for detecting and
correlating events,
defining incidents,
and designating incident
type and priority

Key Objectives



Define attack vectors

Identify sources (Precursors/ Indicators)

Create baselines of expected behaviors

Perform event correlation

Categorize and prioritize incident types

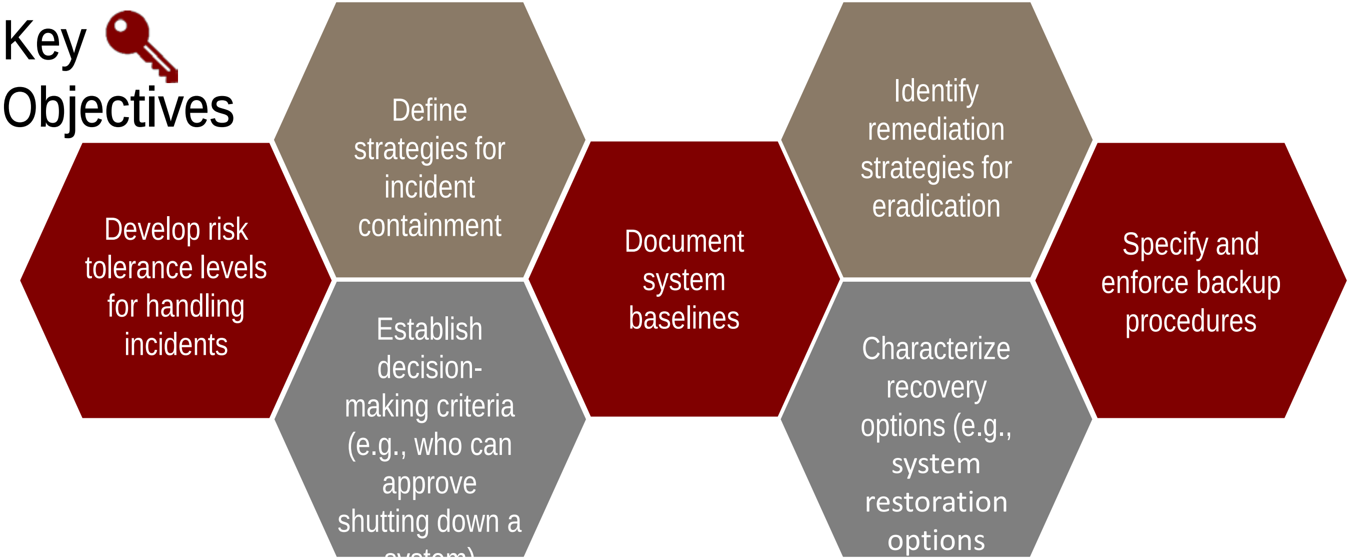
Establish incident notification flow procedures

Determine when to initiate forensic investigation

Containment, eradication, and recovery

Limits damage via isolation,
source removal, and
system restoration.

Key Objectives



Develop risk tolerance levels for handling incidents

Define strategies for incident containment

Establish decision-making criteria (e.g., who can approve shutting down a system)

Document system baselines

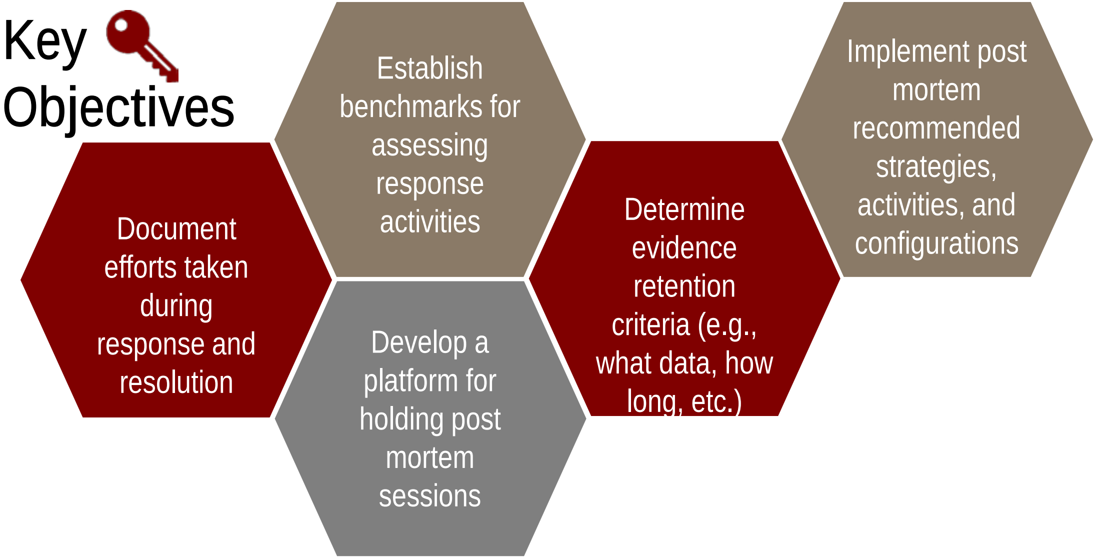
Identify remediation strategies for eradication

Characterize recovery options (e.g., system restoration options

Specify and enforce backup procedures

Post incident activity

Key Objectives



Document efforts taken during response and resolution

Establish benchmarks for assessing response activities

Develop a platform for holding post mortem sessions

Determine evidence retention criteria (e.g., what data, how long, etc.)

Implement post mortem recommended strategies, activities, and configurations

Determinations of root cause, evaluation of plan,
team efficiency and areas for improvement.

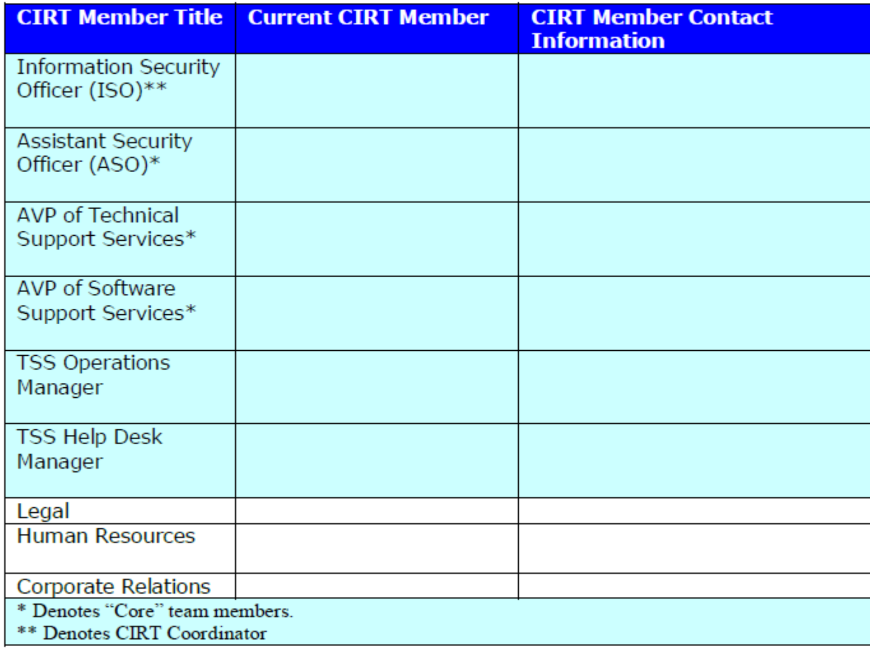
Tabletop Exercises

1. Secure management buy-in
2. Reserve several hours
3. Poll stakeholders
4. Correlate with recent breaches
5. Simulate
6. The end is not the end
7. Repeat until complete

Sources:
[1] http://www.csoonline.com/article/3041383/security/how-to-conduct-a-tabletop-exercise.html

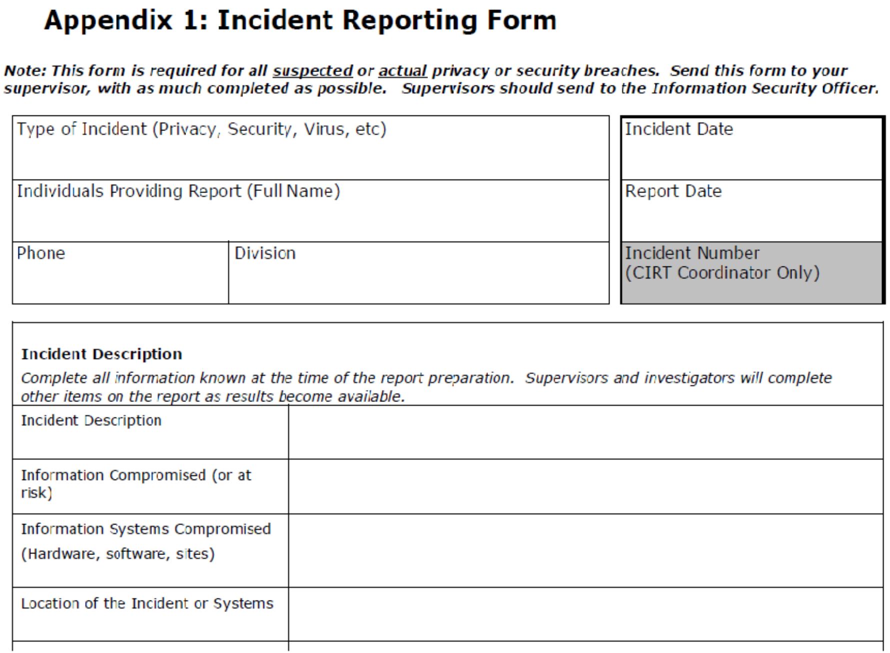
Incident Response Plan Excerpts

Incident Response Plans



CIRT Member Title	Current CIRT Member	CIRT Member Contact Information
Information Security Officer (ISO)**		
Assistant Security Officer (ASO)*		
AVP of Technical Support Services*		
AVP of Software Support Services*		
TSS Operations Manager		
TSS Help Desk Manager		
Legal		
Human Resources		
Corporate Relations		

* Denotes "Core" team members.
** Denotes CIRT Coordinator



Appendix 1: Incident Reporting Form

Note: This form is required for all <u>suspected</u> or <u>actual</u> privacy or security breaches. Send this form to your supervisor, with as much completed as possible. Supervisors should send to the Information Security Officer.

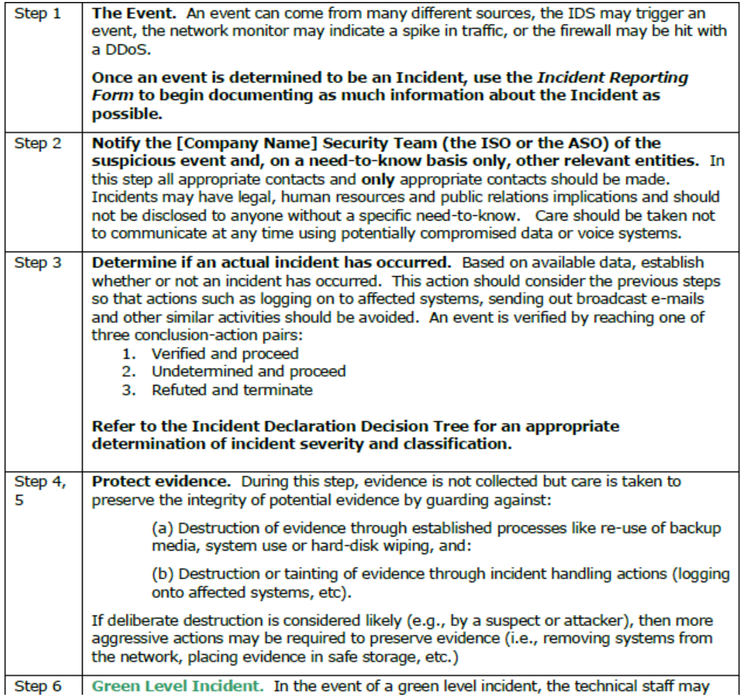
Type of Incident (Privacy, Security, Virus, etc)		Incident Date
Individuals Providing Report (Full Name)		Report Date
Phone	Division	Incident Number (CIRT Coordinator Only)

Incident Description

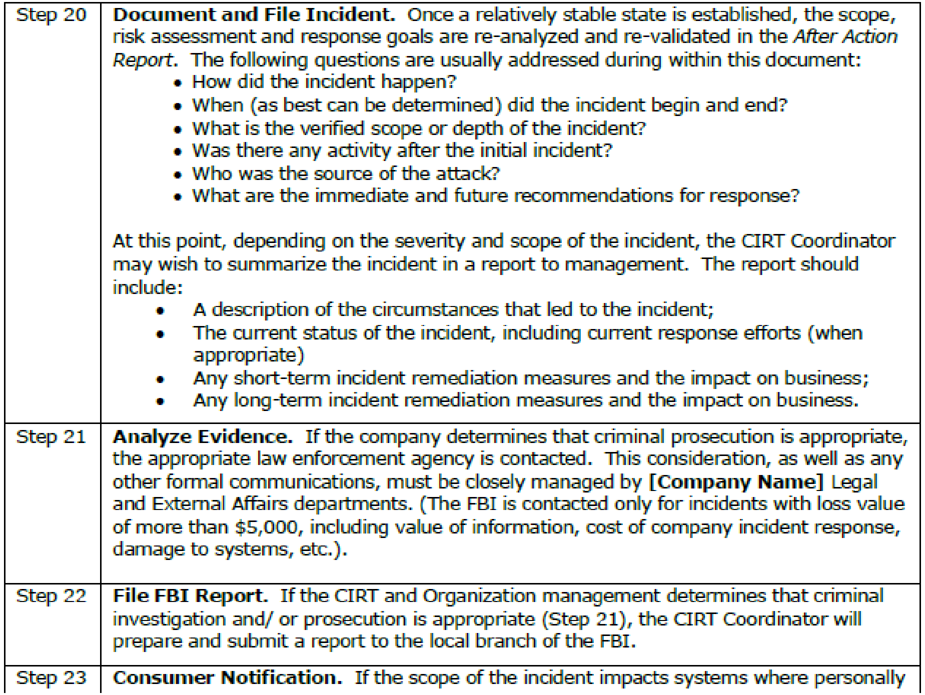
Complete all information known at the time of the report preparation. Supervisors and investigators will complete other items on the report as results become available.

Incident Description	
Information Compromised (or at risk)	
Information Systems Compromised (Hardware, software, sites)	
Location of the Incident or Systems	

Incident Response Plans



Step 1	**The Event.** An event can come from many different sources, the IDS may trigger an event, the network monitor may indicate a spike in traffic, or the firewall may be hit with a DDoS. **Once an event is determined to be an Incident, use the *Incident Reporting Form* to begin documenting as much information about the Incident as possible.**
Step 2	**Notify the [Company Name] Security Team (the ISO or the ASO) of the suspicious event and, on a need-to-know basis only, other relevant entities.** In this step all appropriate contacts and **only** appropriate contacts should be made. Incidents may have legal, human resources and public relations implications and should not be disclosed to anyone without a specific need-to-know. Care should be taken not to communicate at any time using potentially compromised data or voice systems.
Step 3	**Determine if an actual incident has occurred.** Based on available data, establish whether or not an incident has occurred. This action should consider the previous steps so that actions such as logging on to affected systems, sending out broadcast e-mails and other similar activities should be avoided. An event is verified by reaching one of three conclusion-action pairs: 1. Verified and proceed 2. Undetermined and proceed 3. Refuted and terminate **Refer to the Incident Declaration Decision Tree for an appropriate determination of incident severity and classification.**
Step 4, 5	**Protect evidence.** During this step, evidence is not collected but care is taken to preserve the integrity of potential evidence by guarding against: (a) Destruction of evidence through established processes like re-use of backup media, system use or hard-disk wiping, and: (b) Destruction or tainting of evidence through incident handling actions (logging onto affected systems, etc). If deliberate destruction is considered likely (e.g., by a suspect or attacker), then more aggressive actions may be required to preserve evidence (i.e., removing systems from the network, placing evidence in safe storage, etc.)
Step 6	**Green Level Incident.** In the event of a green level incident, the technical staff may



Step 20	**Document and File Incident.** Once a relatively stable state is established, the scope, risk assessment and response goals are re-analyzed and re-validated in the *After Action Report*. The following questions are usually addressed during within this document: • How did the incident happen? • When (as best can be determined) did the incident begin and end? • What is the verified scope or depth of the incident? • Was there any activity after the initial incident? • Who was the source of the attack? • What are the immediate and future recommendations for response? At this point, depending on the severity and scope of the incident, the CIRT Coordinator may wish to summarize the incident in a report to management. The report should include: • A description of the circumstances that led to the incident; • The current status of the incident, including current response efforts (when appropriate) • Any short-term incident remediation measures and the impact on business; • Any long-term incident remediation measures and the impact on business.
Step 21	**Analyze Evidence.** If the company determines that criminal prosecution is appropriate, the appropriate law enforcement agency is contacted. This consideration, as well as any other formal communications, must be closely managed by **[Company Name]** Legal and External Affairs departments. (The FBI is contacted only for incidents with loss value of more than $5,000, including value of information, cost of company incident response, damage to systems, etc.).
Step 22	**File FBI Report.** If the CIRT and Organization management determines that criminal investigation and/ or prosecution is appropriate (Step 21), the CIRT Coordinator will prepare and submit a report to the local branch of the FBI.
Step 23	**Consumer Notification.** If the scope of the incident impacts systems where personally

Q
&
A

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Group: Conexxus Online
- Follow us on Twitter: @Conexxusonline

September 15, 2016 @ 12:00 Eastern:

Protecting Retail ATMs:

A guide to preventing & detecting skimming