Documenting a Breach Management Plan

Dustin Mooney, Managing Consultant
Coalfire Labs

Linda Wilson, Financial Systems & Services Manager
Gonzaga University

September 9, 2014

Higher One
A shared course for success

Housekeeping

- You may submit questions throughout the webinar using the question area in the control panel on the right side of your screen.

  We will address as many questions as possible during the Q&A portion of the webinar until the top of the hour. All remaining questions will be responded to via email after the webinar.

- Attendees will receive a PDF of the slide presentation and a link to the recorded webinar.

Higher One
A shared course for success

Speaker Introductions

Dustin Mooney, ACE/AME, GCFA, GPEN
Managing Consultant, Coalfire Labs
Mr. Mooney leads the digital forensics group at Coalfire Labs. He performs forensics investigations with technical insight and problem solving skills on projects that involve breach identification, malware identification and analysis, client theft, proprietary information theft, employee misconduct, litigation, and evidence collection and preservation.

Linda Wilson
Financial Systems & Services Manager, Gonzaga University
Linda has been at Gonzaga University for 11yrs. She leads a team of functional business analysts and administrators and is tasked with the day to day and long term planning for operations involving CASHNet, Concur, and Ellucian. Along with those responsibilities she partners with the IT Security Director to administer PCI on our campus. Linda loves Gonzaga and is currently a season ticket holder for both the men's and women's basketball teams. Go Zags!

Higher One
A shared course for success

Agenda

- Incident response planning overview
- Understanding assets and liabilities IR plan preliminaries
- Incident response plan development
- Gonzaga University-a campus ahead of the game!
- Questions

About Coalfire

We help our clients recognize and control IT-related risk, and maintain compliance with all major industry and government standards.

- Our approach and methods have been validated by more than 5,000 projects worldwide.
- Accurate and ***independent*** audit and assessments.

Higher One
A shared course for success

Higher education breaches

Credit card data, PII, intellectual property are all targets

- Privacy Rights Clearinghouse recorded 551 breach reports from colleges and universities from 2005 to 2013
- The University of Maryland (309,079 records)
- Indiana University (146,000 records)
- University of Delaware (74,000 records)
- 2014 Ponemon Study - Cost of a Data Breach report $237/record for education
- Incidents end up being a major financial and reputational blow to the nation's colleges and universities
- According to Bitsight, higher education is now at greater risk of security breaches than the healthcare and retail industry
- Kroll Inc. estimates that less than half of the breaches within higher education are actually reported

Higher One
A shared course for success

IRP – the haves and have-nots

Why do you need an IR plan?

- Preparedness
- Clear understanding of roles and responsibilities
- Establishment of what constitutes an incident
- Consistency

Consequences of missing or lacking a plan

- Mismanagement and/or mishandling of incident
- Evidence stomping
- Confusion
- Loss of reputation/financial/data
- Employee terminations

Higher One
A shared course for success

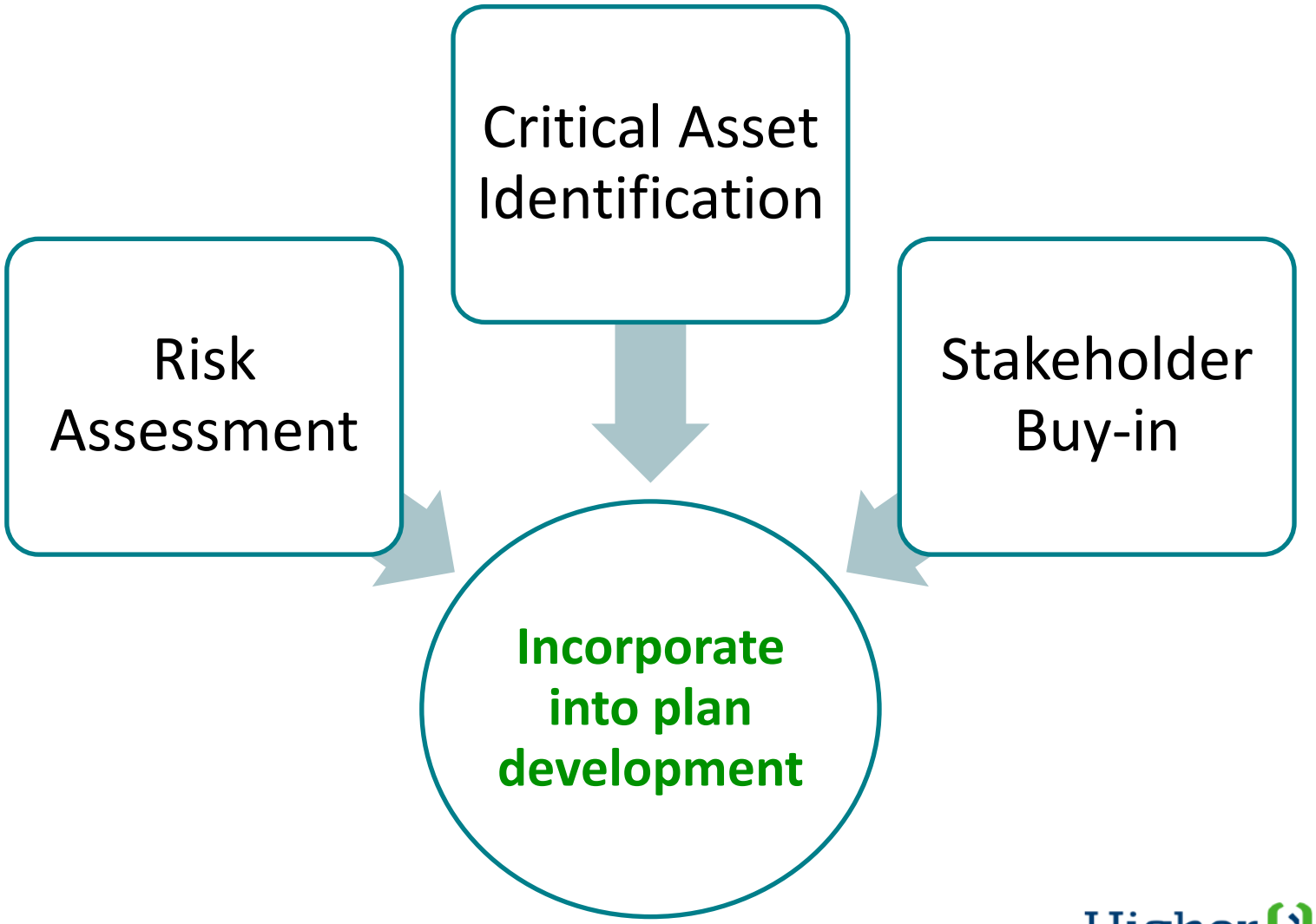
Pick a side….

- Well-trained staff
- Experience and leadership
- Financial support
- Stakeholder engagement
- Necessary resources
- High-integrity findings
- Rehearsed and well-understood actionable items

- Unstaffed
- “Blind leading the blind”
- Unfunded
- Lack of executive support
- Lack of resources
- Ad hoc and un-repeatable procedures
- Unpreparedness and confusion

HigherOne
A shared course for success

Incident Response Plan Preliminaries



IRP Preliminaries Development

Critical asset identification

- Define key data sets and where they reside on the network
- Leverage Business Impact Assessment (DR Plan)
- Determine critical systems and requirements (availability and access)
- Inventory systems and gather network diagrams
- Categorize data and assign sensitivity levels – i.e. Card Holder Data - HIGH

Risk Assessment

- Align with Business Objectives
- Define and categorize threats and vulnerabilities to business units
- Assign a probability rating of threats
- Analyze vulnerabilities, assets, and liabilities to determine risk rating

Stakeholder buy-in

- Coordinate all critical business units for planning
- Ensure the IR team and plan are sufficiently funded
- Allocate team members to participate, develop, update, and test the plan.
- Ensure management of departments, systems, and people understands their roles and responsibilities

Higher One
A shared course for success

IRP Development Process

IRP Planning Resources

Create plan to align with company posture

- What are your risks?
- What data is most sensitive?
- Where is this data?
- Who is on the IR team?
- What constitutes and incident?
- How will the team respond to an incident?
- What does the team do in the situation of data or financial loss?

Consult with a third party

- NIST Special Publication 800-61, 800-84
- USCERT
- SANS Institute
- Carnegie Mellon CERT

Use industry best practices

- IR Plan development
- IR Plan Review
- Table top testing
- Functional testing
- Consultation and advisors

Test and share the plan

- Exercise IR readiness through testing
- Update the plan with lessons learned
- Ensure employees have received and reviewed the plan

Gonzaga University

We knew we needed a plan when…

- We experienced a couple scares
- High profile breaches started to surface more often
- We realized our industry is highly targeted
- Hacks are significantly more sophisticated
- Knowing that it is our responsibility to protect our students

Development of the plan

We considered

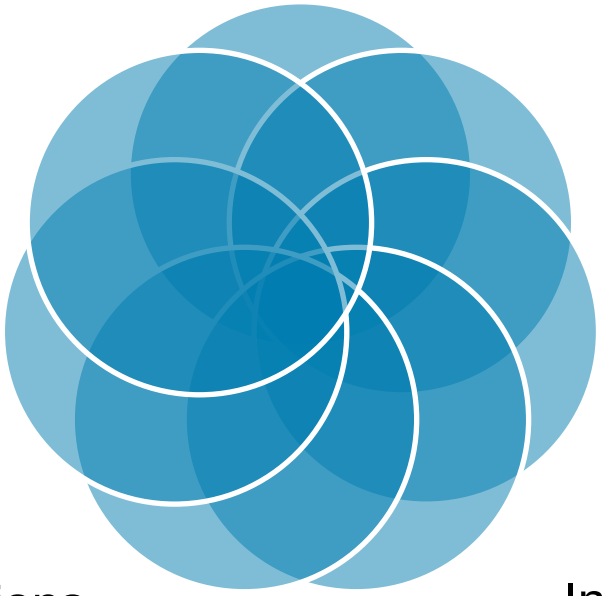
- Who would be a part of the taskforce?
- What the responsibilities were of each team member?
- Accountability
- Availability outside of normal business hours
- Researched various templates
- Communications & Reputation Management
- Budget

Incident Response Task Force

CIO

Finance Systems and Services Manager

VP for Finance



Controller

Corporate Council

Communications Director

Information Security Director

Plan Outline

Gonzaga University developed a plan using the AICPA group template, but there are various resources and you should pick one that best fits the way your campus is organized. **Our plan includes:**

- List of action items to do immediately upon discovering that there has been a breach
- Resources in the plan we included are the VISA, Discover, AMEX, and MasterCard guides documenting how to report a breach
- Steps detailing the communication plan and assigning Group 1 and 2 for escalation
- External notification that includes law enforcement agencies
- Detailed outline for an Executive Summary

Key Takeaways

- **Develop a PCI Incidence Response Team (know you are a target)**
  - Take care to involve those at a high level who are familiar with PCI and will work as a team to identify if an incident truly exists and the degree of the incident
  - Must be readily available 24x7
  - If you have a contract with a QSA firm, notify them immediately for guidance
- **Develop plan of action, rules and responsibilities within the team**
  - Do not over react and work as a team
  - Follow agreed upon response plan step by step
  - Make sure each member knows their responsibilities
  - Include the Brand links in your PCI Incidence Response Plan for easy access as their requirements are subject to change
  - Be diligent about documenting all decisions and actions
  - Be diligent about preserving evidence
- **Practice**
  - While we have not had a breach , we have had a few scares that helped create these guidelines and overall IT Incidence guidelines
- **Keep your plan current**
  - Assess your plan annually or as needed depending on technology, PCI changes, and/or new breach or data information

As the late Walt Conway said "There are universities that have been breached, and there are universities that are going to be breached so pay attention to PCI!"

Higher One
A shared course for success

QUESTIONS

Dustin Mooney
Coalfire Labs
dustin.mooney@coalfire.com
877.224.8077 ext. 7010

Linda Wilson
Gonzaga University
wilsonl@gonzaga.edu
509.313.6359

HigherOne
A shared course for success