Agenda

- Initial Thoughts
- The Premise
- So Where Do You Start?
- Step 6: [Business] Impact Analysis
- Potential Negative Impact
- That Detective, is the right question
- You Make it Sound So Easy!
- Technology Overkill?
- Summary

Initial Thoughts

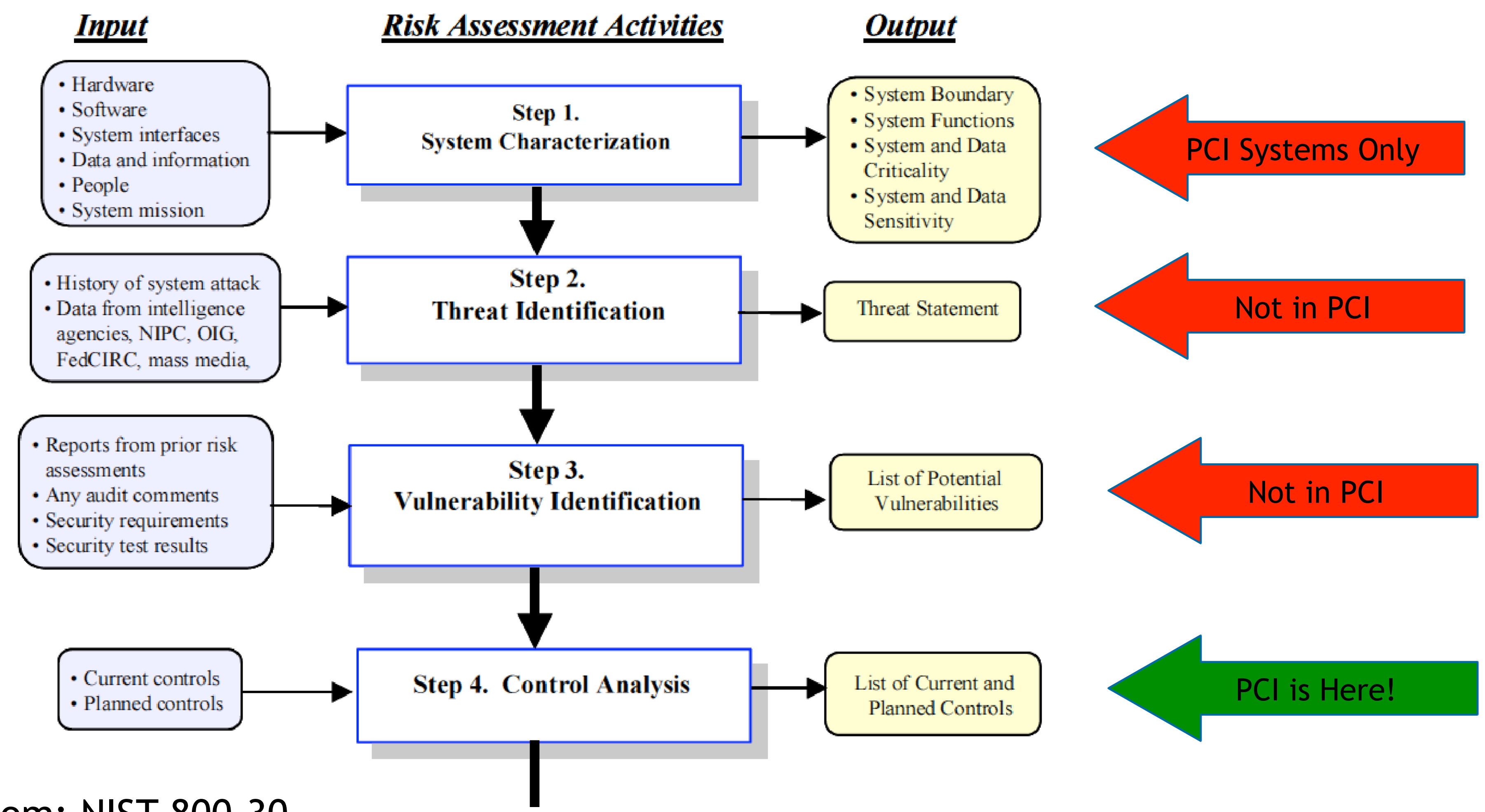
- I am a big fan of technology as long as it’s part of a *known* business need, and not a reaction to a *perceived* one
- Technology purchased before a risk assessment has a good chance of becoming an expensive paper-weight
- Regulations like PCI, and whatever come after it, are ‘forcing’ organisations into bad purchase decisions
- Even when a technological need makes sense, it is rarely integrated correctly, and may even reduce your current security posture
- ISO and COBIT have been out for a long time, yet are very rarely followed correctly

The Premise

I’m not picking on PCI, but;

- It’s the first compliance regime to actually draw a line in the sand with regard controls
- The risk assessment is built in, and I’m fairly sure your business was not consulted
- No other regulation in history has caused such a demand for technology, and not provided the guidance from which to make the right decisions
- It stops where you need to be most concerned …STAYING in business (the real reason for technology)

So Where Do You Start? Part 1



Input

- Hardware
- Software
- System interfaces
- Data and information
- People
- System mission

- History of system attack
- Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,

- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results

- Current controls
- Planned controls

Risk Assessment Activities

Step 1.
System Characterization

Step 2.
Threat Identification

Step 3.
Vulnerability Identification

Step 4. Control Analysis

Output

- System Boundary
- System Functions
- System and Data Criticality
- System and Data Sensitivity

Threat Statement

List of Potential Vulnerabilities

List of Current and Planned Controls

PCI Systems Only

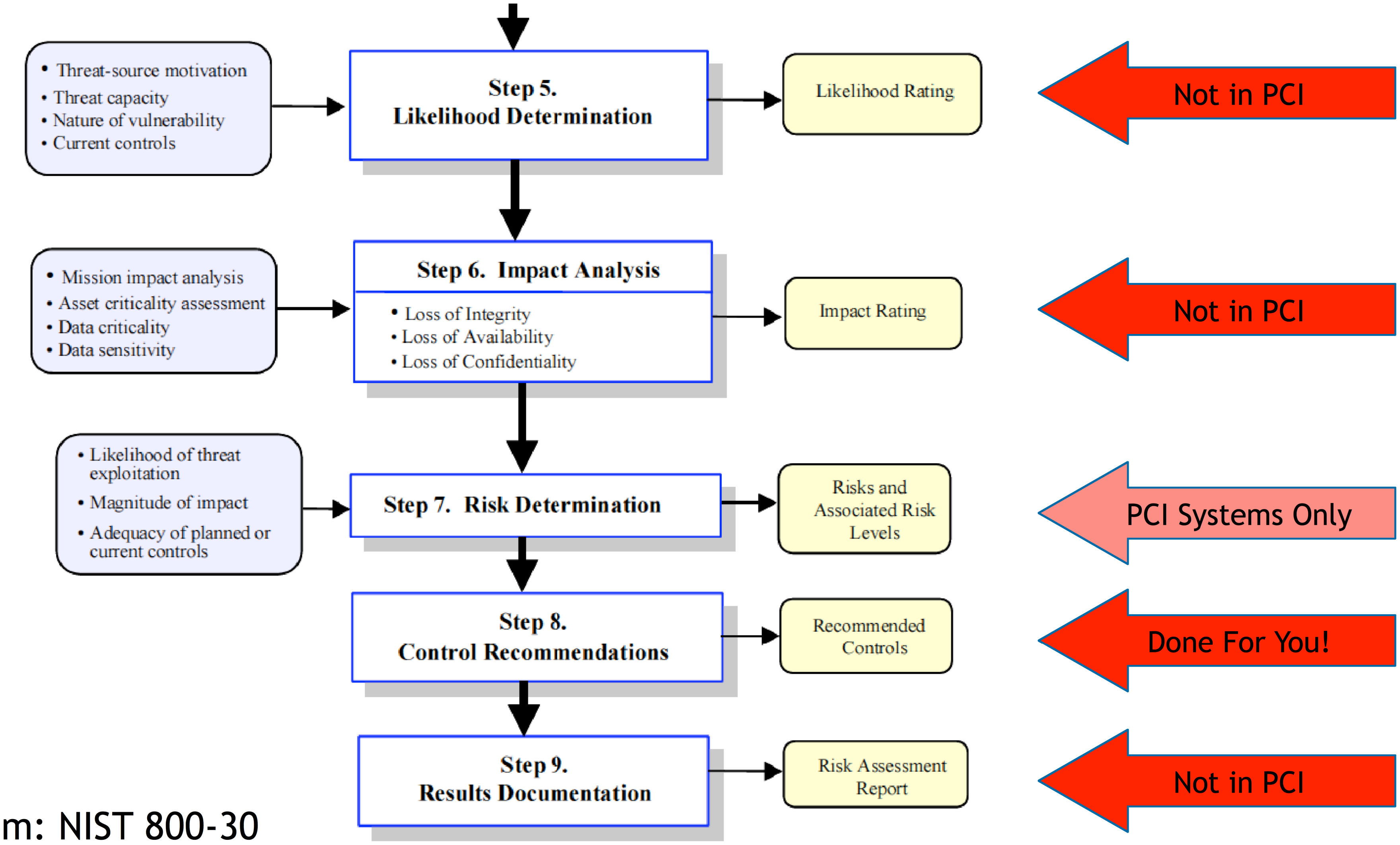
Not in PCI

Not in PCI

PCI is Here!

From: NIST 800-30

So Where Do You Start? Part 2



- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Step 5. Likelihood Determination

Likelihood Rating

Not in PCI

- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity

Step 6. Impact Analysis

- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

Impact Rating

Not in PCI

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Step 7. Risk Determination

Risks and Associated Risk Levels

PCI Systems Only

Step 8. Control Recommendations

Recommended Controls

Done For You!

Step 9. Results Documentation

Risk Assessment Report

Not in PCI

From: NIST 800-30

Step 6: [Business] Impact Analysis

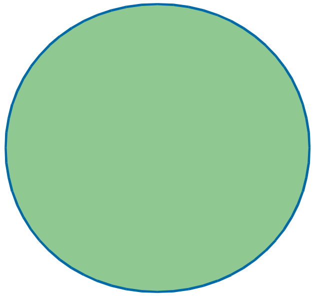
Question: Would you spend £1,000,000 to protect £1,000 worth of data?

Question: What about the other way around?

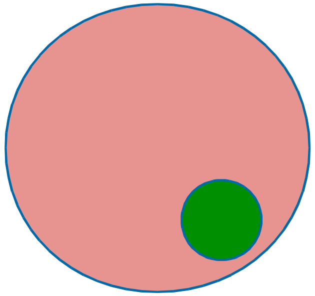
- If you have not performed a Risk Assessment and a Business Impact Analysis you have no idea what the value of your data is…
- …and if you don’t know that value, how do you know how much to spend, and what to spend it on?...
- ..and if you don’t know how much to spend, how do you know you’re spending what you DO have on the right things?

Potential Negative Impact

Let’s say you have a £50,000 for IT security across your organisation. Before PCI you would spread that fairly evenly;



But with PCI, it’s recommended that you segment your cardholder data and put robust controls around that;



What about the REST of your company’s sensitive data?!

That Detective, is the Right Question….

Assuming you have actually performed the Risk Assessment and Business Impact Analysis, you should;

- know the controls you need to put in place and how much you should/can spend
- perform all necessary due diligence on the control options
- know how the new controls will be managed and monitored
- integrate them into your business-as-usual and Governance processes

You Make it Sound So Easy!

Control Due Diligence? Managed and Monitored? Errrrr?

- How do I choose the right technology?
- How do I ensure it can be integrated?
- How do I manage and monitor it?
- Will I actually be more secure?
- How do I show the BENEFIT!?

All these questions should be ANSWERED before you spend penny one.

Technology Overkill?

- Firewalls
- File Integrity Monitoring
- Intrusion Detection/Protection (host based or network)
- Log Management
- Security Information & Event Management (SIEM)
- Encryption
- Tokenization
- Data Loss Prevention (DLP)
- Network Access Control (NAC)
- Web Application Firewall (WAF)
- Two Factor Authentication
- …and so on, and so on!

Summary

- Step1: Examine ALL business processes and classify your data types
- Step 2: Change processes to not use sensitive data [where possible], then remove legacy data from everywhere you find it
- Step 3: Conduct a risk assessment and business impact analysis across the entire enterprise
- Step 4: Agree on the controls you need in place to meet the risk
- Step 5: Make purchases of technology and services that match the controls, provides scalability, and meet these criteria;
  - Can be integrated / is interoperable with existing infrastructure
  - Can be managed centrally
  - You have the skill-set in-house to monitor it, or have outsourced
  - Meets all internal SLAs, internal audit, and reporting needs
  - Is in support of your Incident Response & Business Continuity Plans

Resources

- BSi’s ‘A Practical Approach to Business Impact Analysis’
- Control Objectives for Information and related Technology (COBIT®)
- ISO 27001 – ISMS – Requirements
- BS 25999 – Business Continuity Management
- NIST’s SP 800-30: Risk Management Guide for Information Technology Systems