Physical Security Assessment (PSA) Plan

(Steve Jaques)

5 Steps

1 - Capture the purpose

* Assess physical security minimums for certain areas (Dion Munk)

2 - Capture the benefits

3 - Capture the costs

4 - Analyze the Benefits and Costs

* Is the performance of the system worth it? Compare effectiveness to cost of implementation. (Dion Munk)

5 - State PSA Plan and Return on Investment (ROI)

My bad - Reference. Why I should never start a document.

http://www.cisco.com/en/US/services/ps2961/ps2952/ps9909/Services\_Overview\_Video\_Surveillance.pdf

PSA should provide guidance, assign responsibility, and set minimum standards for the security of the organization. Please feel free to blow this up - my simple stab at it. (Steve Jaques)

(Scott H)

Shouldn’t the plan be more like

1. Planning
2. Discovery
3. Attack
4. Reporting

Its an assessment not an actual incident.

I think we want to list any references we used.

http://www.slideshare.net/agent0x0/physical-security-assessments-presentation

(Rob Healy)

Here is something I just came up with after thinking for a bit…

1. Discovery/Research
2. ATTACK
3. white box discovery/research
4. Reporting/Vulnerability analysis

(Jared Hallows)

The Dept of Agriculture has a nice [write up](http://www.dm.usda.gov/physicalsecurity/riskmanagementapproachpresentation.pdf) of what they expect in a PSA. Here are the steps they list:

1. Management Approval, Planning and Preparation
2. Identification of Critical Assets Requiring Protection
   1. Rank assets by potential harm done if infiltrated (EK)
3. Identify who accesses these assets and how (EK)
   1. Find alternative ways an employee may access these assets (non malicious) (EK)
4. Analysis of current security systems (EK)
5. Threats Analysis
6. Gap Analysis
7. Analysis of Vulnerability (Scenario Development)
8. Risk Calculation/Assess Risk
9. Countermeasure Identification/Risk Recalculation
10. Mitigation

I think step 7, countermeasure identification/risk recalculation, is pretty important. I hadn’t thought of trying to think out countermeasures an adversary might use. <http://www.dm.usda.gov/physicalsecurity/riskmanagementapproachpresentation.pdf>

(Parker Grimes)

A physical security assessment plan should probably start with some kind of inventory of what we are trying to protect, what is high value vs. low value, what are the current physical characteristics surrounding what we are trying to protect, and what techniques/hardware/detection/delay/response tools are available.

Google has a nice [white paper on how they approach IT security](https://static.googleusercontent.com/media/www.google.com/en/US/work/pdf/whygoogle/google-common-security-whitepaper.pdf). In the evaluation of what could go wrong if someone gained physical access, Google’s plans shows that it is important to think about the physical distribution of the data you are trying to protect. Google has distributed their datacenters geographically for security reasons in addition to physical disaster contingency plans. We usually think about geographically separating our backups from our production systems in case of some physical disaster like floods, fires, earthquakes, hurricanes, etc. It may also be wise to think about geographically separating data for security reasons as well.

Google, not surprisingly, uses a variety of automated detection systems with smart algorithms. Other things to consider in the PSA plan include redundant power systems and environmental controls, fire detection and suppression, limited personnel access, layered physical barriers, and multi factor physical access authentication.

(Mark Whittaker)  
I agree with Parker, and by extension Jared’s post. Asset Identification should be near the top. In fact, the USDA’s PSA seems like a pretty solid starting point. I like the inclusion of Risk Calculation/Evaluation. If physical security is compromised, it is important to know what that is going to cost us. This step seems to tie into Steve’s ROI point in his suggested list. More often than not the results of these assessments will be delivered to executives. If we want to be able to take action with proper mitigation, we may need to spell out the financial risks so we can get some of the money we would need to get the job done.

I like what Jared posted. I feel this is going to be like our vulnerability assessment 1.0. Everything I have been looking at in regards to Physical security assessment involves some sort of incidence response team for both physical and cyber domains. I think our assessment should include a formation and roles of incident response team. <http://www.bankinfosecurity.com/how-to-perform-physical-security-risk-assessment-a-694/op-1>

<http://www.sans.org/reading-room/whitepapers/incident/creating-managing-incident-response-team-large-company-1821>

<http://modulo.com/security-risk-management/>

(Alexander Cannell)

(Bryce Caine)

Here's my attempt at distilling some of these thoughts down to a high-level list:

* Take inventory of physical assets
* Evaluate current security (i.e., security systems, physical access, etc.)
* Conduct a compromise-impact analysis
* Identify potential threats

This omits the obvious planning and cost-benefit analysis in order to focus on the actual assessment. I'm sure this over-simplifies some areas, but I thought I'd try to capture the essential aspects of a physical security assessment.

(Mark Walton)

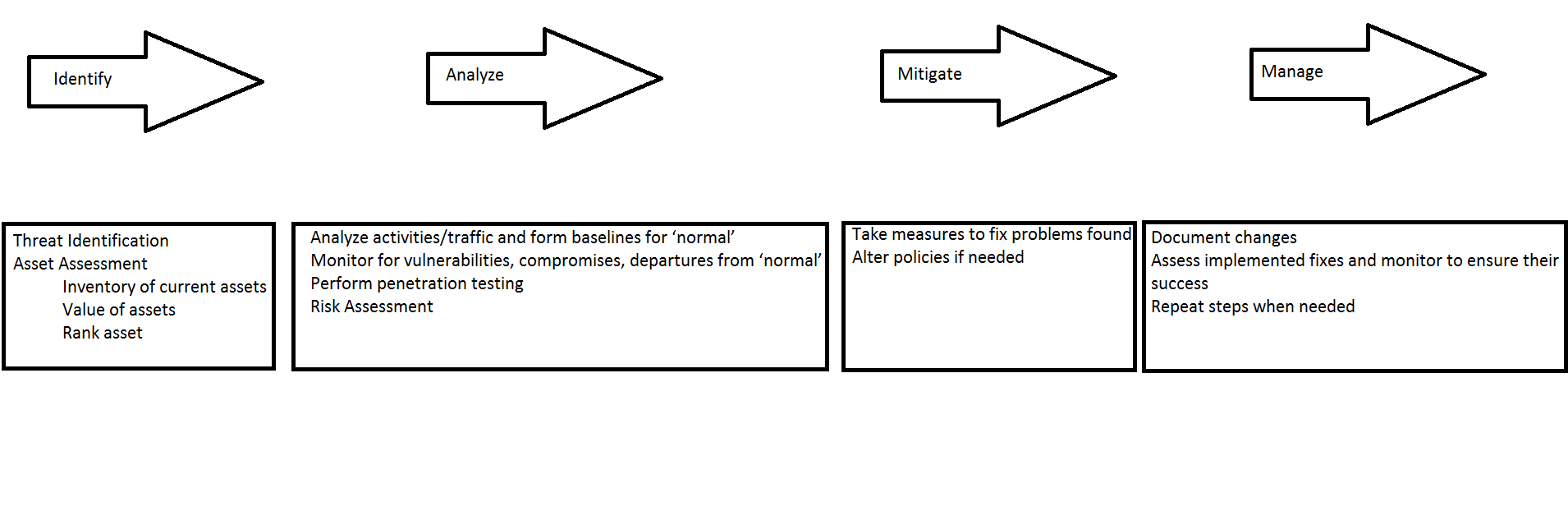
Yes, I agree with Bryce. I don’t think the PSA should include a cost-benefit analysis. This isn’t a plan to decide what physical security controls should be put in place. This is a plan to assess what’s already in place. That assumes that the organization has already decided what is of value, and what controls they think they needed to protect the assets.

I would add to Bryce’s list that we include recommended solutions and a repeat step. Just like the VAMs we discussed earlier, it’s important to repeat the process to test suggested improvements. Any type of assessment should be part of a regular cycle to promote continual improvement.

I like the simple plans of Rob H, Scott H, and Bryce C. In fact, do the same steps used for the VAM work in this situation? Do we really assess physical security any differently in terms of the methodology? For the security assessments I’ve been involved with, physical security was just one of the aspects of the overall assessment.

Honestly I feel like we are going back to the four essential steps we listed in the previous VAM Module Identify, Analyze, Mitigate, and Manage.

1. Identify
   1. Threat Identification
   2. Asset Assessment
      1. Inventory of current assets
      2. Value of assets
      3. Rank asset
2. Analyze
   1. Analyze activities/traffic and form baselines for ‘normal’
   2. Monitor for vulnerabilities, compromises, departures from ‘normal’
   3. Perform penetration testing
   4. Risk Assessment
3. Mitigate
   1. Take measures to fix problems found
   2. Alter policies if needed
4. Manage
   1. Document changes
   2. Assess implemented fixes and monitor to ensure their success
   3. Repeat steps when needed

(Alexander Cannell)

Alex, I think the VAM and this plan are really much the same. (Scott H).

I agree. These are very similar, just adapted for the certain type of assessment. (Dion M.)