Gemini Observatory CyberSecurity Program

Chris Morrison & Tim Minick

CTSC/NSF CyberSecurity Summit 2016

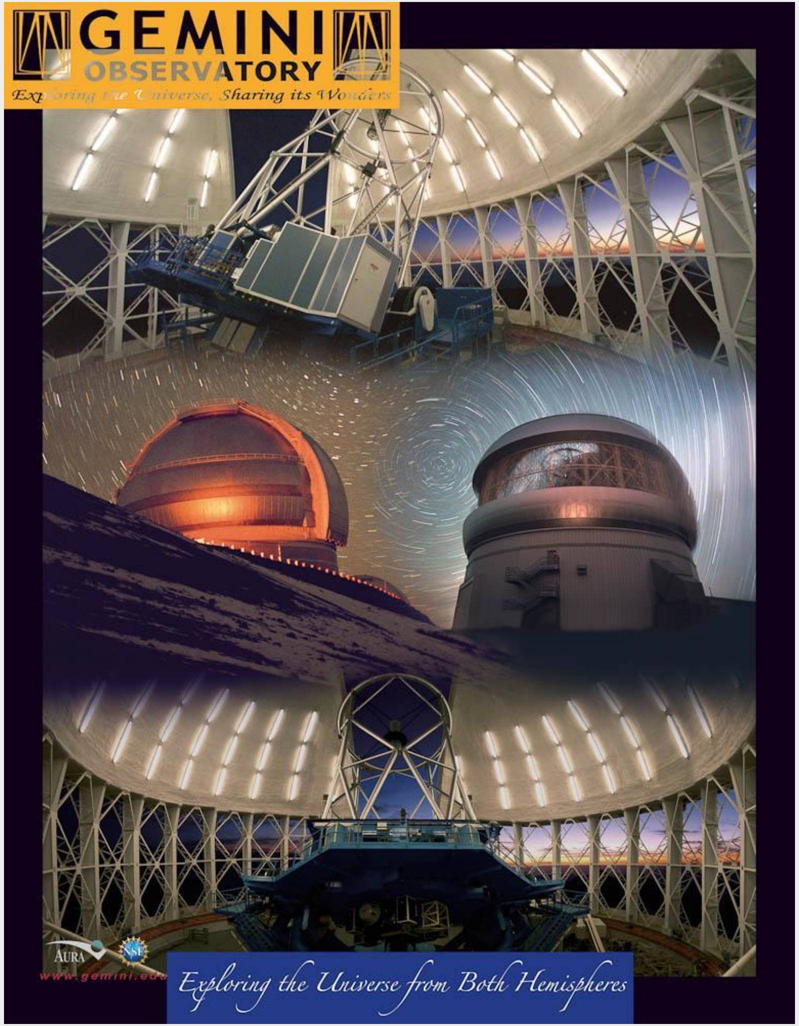
Disclaimer

- This presentation is provided "as is", with no expressed or implied warranty. Your success cannot be guaranteed. Not legal in all states. Restrictions apply.
- The strategies, tactics and experiences are those of Gemini alone.
- There is certainly more than one right (or wrong) way to solve problems and address issues.

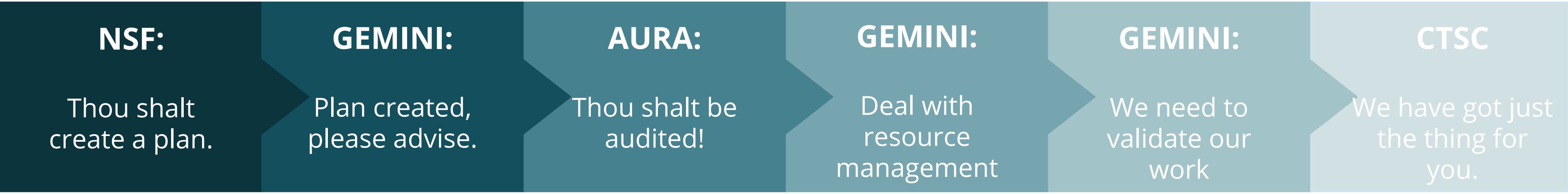
About Gemini

The Gemini Observatory consists of twin 8.1-meter diameter optical/infrared telescopes located on two of the best observing sites on the planet. From their locations on mountains in Hawai‘i and Chile, Gemini Observatory’s telescopes can collectively access the entire sky.

www.gemini.edu


GEMINI
OBSERVATORY
Exploring the Universe, Sharing its Wonders
AURA
NSF
www.gemini.edu
Exploring the Universe from Both Hemispheres

The Timeline



NSF:

Thou shalt create a plan.

GEMINI:

Plan created, please advise.

AURA:

Thou shalt be audited!

GEMINI:

Deal with resource management

GEMINI:

We need to validate our work

CTSC

We have got just the thing for you.

2007

NSF Request
“The Awardee is required to provide a summary of its IT Security program”

2009

The Plan
Gemini delivered the summarized and approved CyberSecurity plan to NSF

2011

AURA Audit
AURA commissions an internal audit of multiple centers.

2011

Project Plan
Gemini implements CyberSecurity as a Project (CaaP)

2014

CTSC Summit
Gemini identifies the possibility to engage CTSC to audit the work so far.

2015+

CTSC + Gemini
Gemini and CTSC successfully complete engagement.

Developing the CyberSecurity plan

Turning requirements, recommendations and organizational needs into a documented plan

The Spark

“The Awardee is required to provide a summary of its IT Security program”

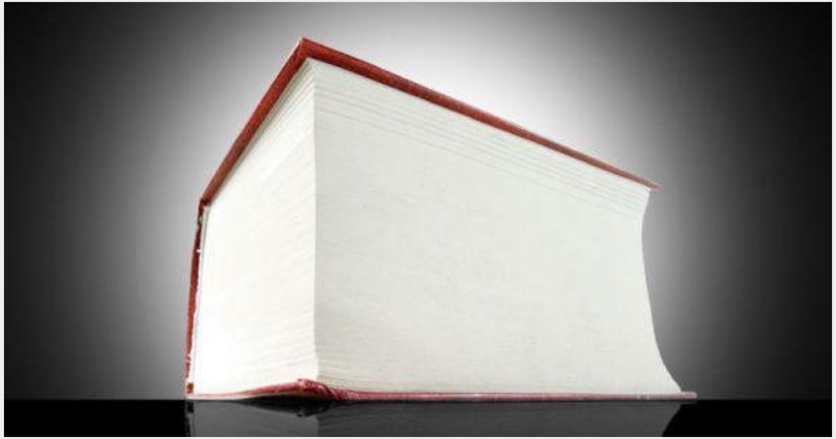
NSF, 2007

NSF Large Facilities Cooperative Agreements Article 51, states that:

“Security for all IT systems under the award, including equipment and information, is the Awardee’s responsibility.”

The Plan

- Multi-month intensive research exercise.
- Write-review-edit-wash-rinse-repeat.
- 85+ pages. It was a thing of beauty.



That's no moon...it's a space station. -Obi Wan Librarian

NSF:

"Very nice work. But please provide us something that we can read and understand."

The Plan v2

- Condensed version.
- High level scope, goals, responsibilities, roles, escalation, etc.
- 13 pages. A smaller thing of beauty.

NSF:

“Now THAT’S what we were talking about!”

Gemini Observatory Cybersecurity Plan

September 21, 2009

The AURA Audit

Accountability, Responsibility, and Authority trickle down...

Independent Audit

- AURA Commissioned in 2011.
- Gemini's first external IT audit.
- Findings primarily focused on policy gaps.

Take-aways:

- We didn’t understand requirements before we began!
- To be successful we needed to identify, appoint, and task leaders and owners.
- We should have immediately structured our cybersecurity initiative as a program.
- We didn’t initially realize that part of program evolution involved revising/re-writing our plan.
- Audits can be a positive experience.

Obtaining Budget and Staff

Creating a team:
Someone has to “own” CyberSecurity

Staffing

- Like many other initiatives (such as safety): "Not my job!" attitude.
- Key to understand that a cybersecurity program must led by someone or something.
- It's a journey, not a destination, and is therefore evolutionary, requiring effort to sustain.
- Formally framed as a project, with a .5FTE ISSE.

Budget

- Actual photo of Gemini office with 2015 CyberSecurity program funding.
- Projects or Programs require tangible items; labor alone will not suffice. More about the project/program coming up...
- Ongoing software and subscription M&S costs.

Budget

- It is easy to fall prey to salespeople pushing tools and utilities that you do not immediately need.
- How much will/should this co$t? 1%-13%, 5.6% avg.
- Focus budget where you can provide value and impact.

Take-aways:

- Dedicated staff. You need them.
- We should have initially set and established a both a labor and non-labor budget.
- Perform a reality check. You will not go from zero to awesome in the course of a year.
- Utilize industry metrics to determine funding and provide support for your case as you present to senior management.

“Sound the Alarm”

Keep senior management aware of cybersecurity incidents across various industries!

User Awareness Training

The good, the bad and the plain ugly

The Good

“I have a feeling it's really gonna be a good, long battle.” - Blondie

- Training is generally not difficult to sell.
- Directorate was on-board.
- It was understood that the observatory would benefit from helping understand the threat.
- Rock-Star status, but...

The Bad

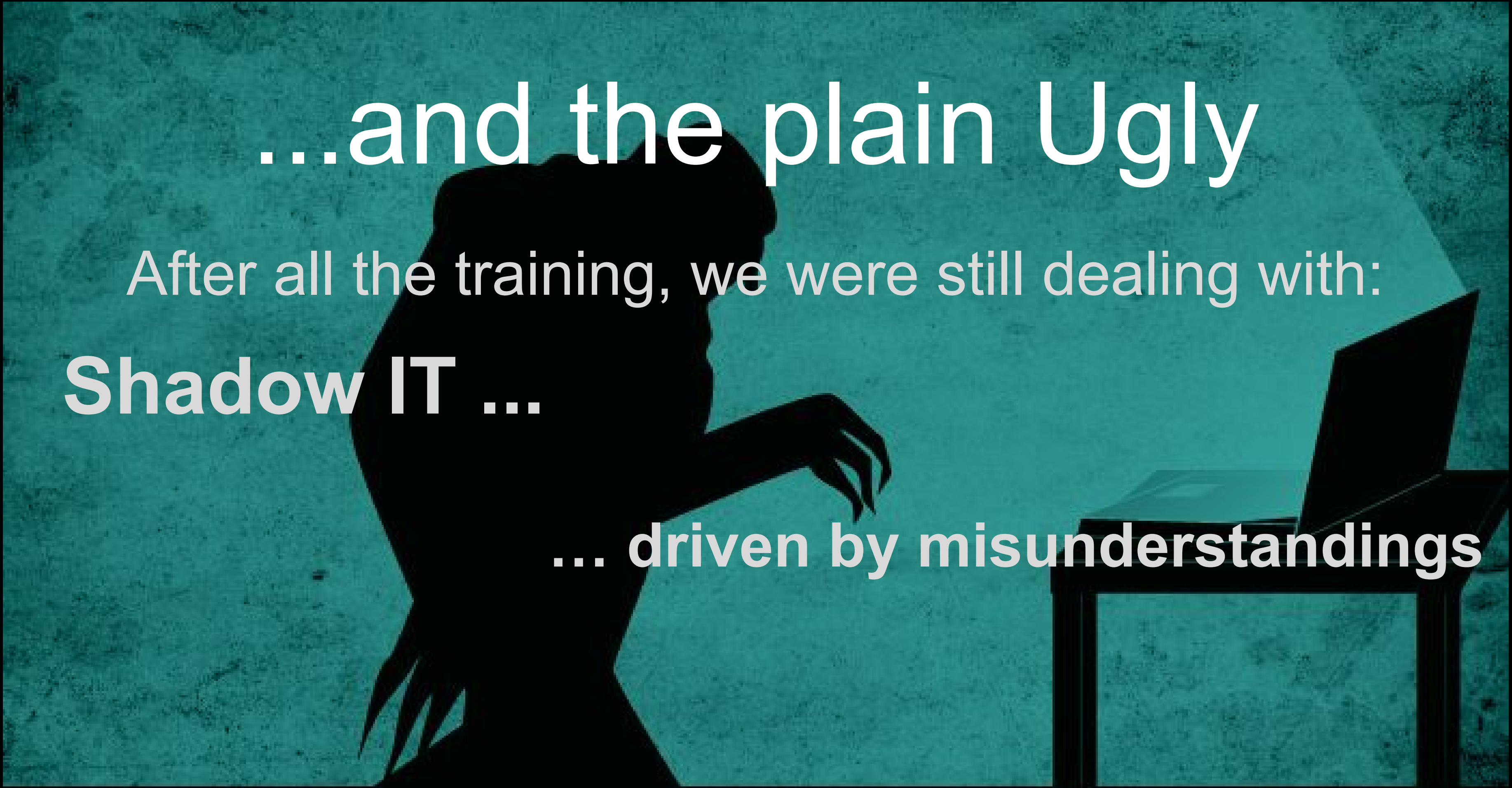
- Convincing staff that they will benefit from the training.
- Teaching them something that everybody already knows. - how dare we!
- Using the, already precious time, for *this*?!?

Even with support from directorate...

100% attendance was out of the question!

vacation & sick leave was taken into account.

...and the plain Ugly



After all the training, we were still dealing with:

Shadow IT ...

... driven by misunderstandings

Take-aways:

- Helping staff understand the importance of awareness training, is half the battle.
- A constant flow of training is less time consuming and better received that single, “forced” events.
- Keep is short - simple works too.
- Open and maintain a well established framework of communication between all parties.

Policy Development

Help Wanted: Governance!

Policy Constipation™

Policies are a cornerstone of CyberSecurity, so why the struggle in releasing and updating them?

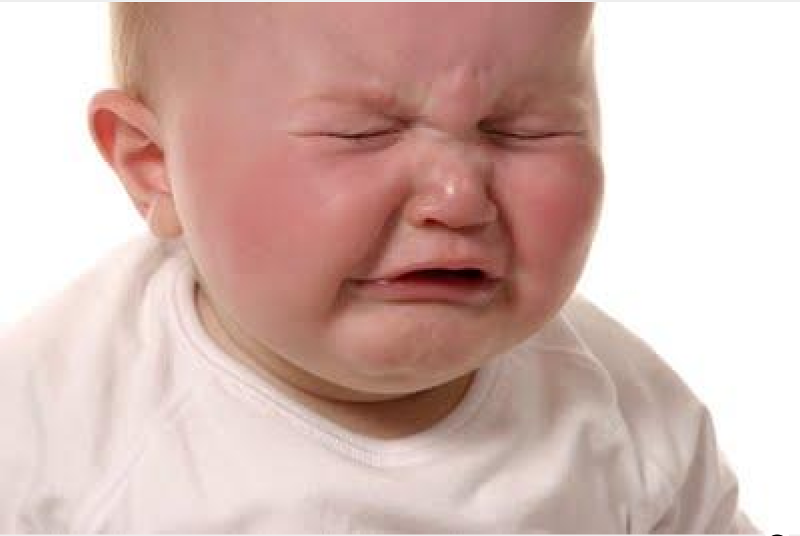
Obstacles

- No formal processes or protocols.
- Building a modern policy portfolio based upon legacy.
- Deadlock.

Policy Constipation™

Obstacles

- ITPRB
- Score:
  - Convenience: 1
  - Security: 0
- Policy Development Protocol (back to point 1)



Policy Constipation ™

Take-aways:

- CTSC Reference Policy Suite. Check it out.
- Understand the difference between stakeholder involvement and a hostage situation.
- Be comprehensive, but less is more. Manage by exception. Brevity increases the level of readership.
- ITPRB. Don’t.
- Policy Development Protocol. Use it or develop your own.

“Sound the Alarm”

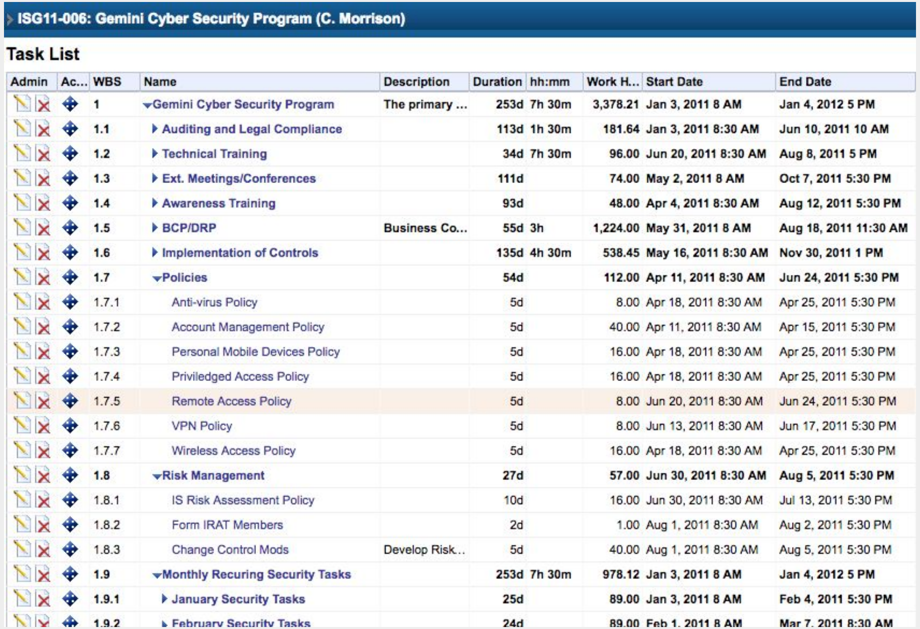
Keep senior management aware of cybersecurity incidents across various industries!

A CyberSecurity Gantt chart

Selling the cybersecurity program with concepts ~~stolen~~ borrowed from project management

CS As a Project

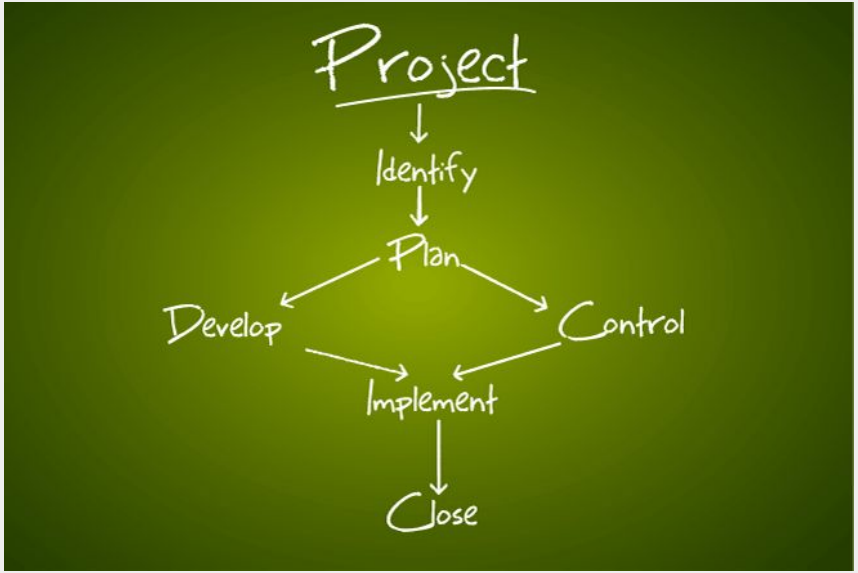
- Why Project Management?
- Resource Management
- Task Management



ISG11-006: Gemini Cyber Security Program (C. Morrison)

Task List

Admin	Ac...	WBS	Name	Description	Duration	hh:mm	Work H...	Start Date	End Date
		1	Gemini Cyber Security Program	The primary ...	253d	7h 30m	3,378.21	Jan 3, 2011 8 AM	Jan 4, 2012 5 PM
		1.1	Auditing and Legal Compliance		113d	1h 30m	181.64	Jan 3, 2011 8:30 AM	Jun 10, 2011 10 AM
		1.2	Technical Training		34d	7h 30m	96.00	Jun 20, 2011 8:30 AM	Aug 8, 2011 5 PM
		1.3	Ext. Meetings/Conferences		111d		74.00	May 2, 2011 8 AM	Oct 7, 2011 5:30 PM
		1.4	Awareness Training		93d		48.00	Apr 4, 2011 8:30 AM	Aug 12, 2011 5:30 PM
		1.5	BCP/DRP	Business Co...	55d	3h	1,224.00	May 31, 2011 8 AM	Aug 18, 2011 11:30 AM
		1.6	Implementation of Controls		135d	4h 30m	538.45	May 16, 2011 8:30 AM	Nov 30, 2011 1 PM
		1.7	Policies		54d		112.00	Apr 11, 2011 8:30 AM	Jun 24, 2011 5:30 PM
		1.7.1	Anti-virus Policy		5d		8.00	Apr 18, 2011 8:30 AM	Apr 25, 2011 5:30 PM
		1.7.2	Account Management Policy		5d		40.00	Apr 11, 2011 8:30 AM	Apr 15, 2011 5:30 PM
		1.7.3	Personal Mobile Devices Policy		5d		16.00	Apr 18, 2011 8:30 AM	Apr 25, 2011 5:30 PM
		1.7.4	Priviledged Access Policy		5d		16.00	Apr 18, 2011 8:30 AM	Apr 25, 2011 5:30 PM
		1.7.5	Remote Access Policy		5d		8.00	Jun 20, 2011 8:30 AM	Jun 24, 2011 5:30 PM
		1.7.6	VPN Policy		5d		8.00	Jun 13, 2011 8:30 AM	Jun 17, 2011 5:30 PM
		1.7.7	Wireless Access Policy		5d		16.00	Apr 18, 2011 8:30 AM	Apr 25, 2011 5:30 PM
		1.8	Risk Management		27d		57.00	Jun 30, 2011 8:30 AM	Aug 5, 2011 5:30 PM
		1.8.1	IS Risk Assessment Policy		10d		16.00	Jun 30, 2011 8:30 AM	Jul 13, 2011 5:30 PM
		1.8.2	Form IRAT Members		2d		1.00	Aug 1, 2011 8:30 AM	Aug 2, 2011 5:30 PM
		1.8.3	Change Control Mods	Develop Risk...	5d		40.00	Aug 1, 2011 8:30 AM	Aug 5, 2011 5:30 PM
		1.9	Monthly Recuring Security Tasks		253d	7h 30m	978.12	Jan 3, 2011 8 AM	Jan 4, 2012 5 PM
		1.9.1	January Security Tasks		25d		89.00	Jan 3, 2011 8 AM	Feb 4, 2011 5:30 PM
		1.9.2	February Security Tasks		24d		89.00	Feb 1, 2011 8 AM	Mar 7, 2011 8:30 AM



Problems

- There was no clear path.
- We knew the cost (time / money) - but not the product.
- We needed to prioritize - it was never going to end.

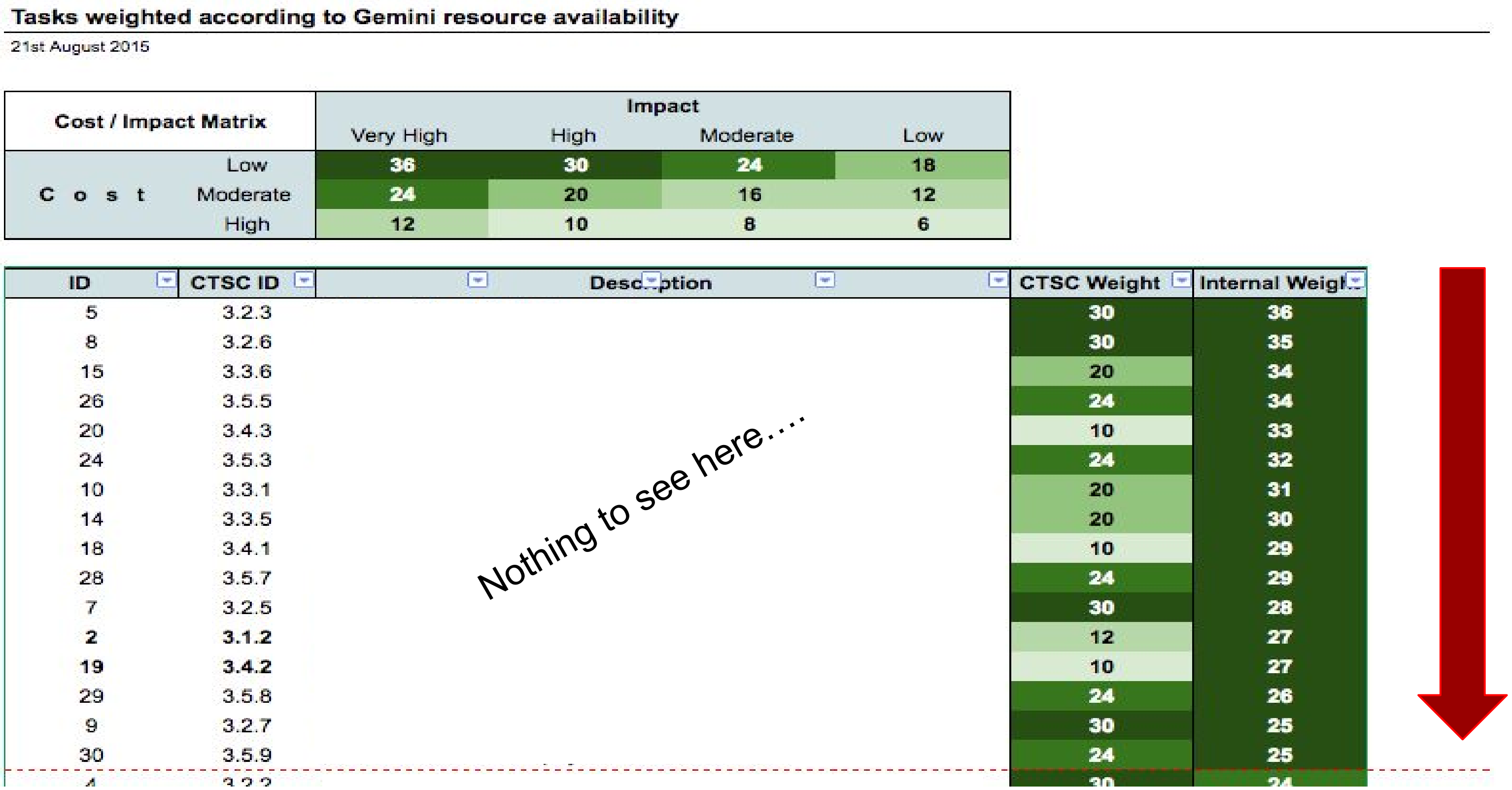
Solutions

- A more focused list.
- A long term CyberSecurity roadmap - IT Governance.
- A project end-date.

“Project” prioritization and scoring system

Determining where to start,
and what not to do - for now

Where is the waterline?



Tasks weighted according to Gemini resource availability

21st August 2015

Cost / Impact Matrix		**Impact**			
		Very High	High	Moderate	Low
Cost	Low	36	30	24	18
	Moderate	24	20	16	12
	High	12	10	8	6

ID	CTSC ID	Description	CTSC Weight	Internal Weight
5	3.2.3		30	36
8	3.2.6		30	35
15	3.3.6		20	34
26	3.5.5		24	34
20	3.4.3		10	33
24	3.5.3		24	32
10	3.3.1		20	31
14	3.3.5		20	30
18	3.4.1		10	29
28	3.5.7		24	29
7	3.2.5		30	28
2	3.1.2		12	27
19	3.4.2		10	27
29	3.5.8		24	26
9	3.2.7		30	25
30	3.5.9		24	25
4	3.2.2		30	24

Nothing to see here….

“Sound the Alarm”

Keep senior management aware
of cybersecurity incidents!

The CTSC “check up”

...performed entirely remotely

100% Remote Engagement

- Comprehensive yet manageable CTSC questionnaire completed.
- Also focused on policy, procedure and architectural review.
- Results discussed at 2015 CTSC CyberSecurity Summit.
- Formal engagement plan drafted as a result.

The CTSC Gemini North - Hilo, Hawaii on-site visit

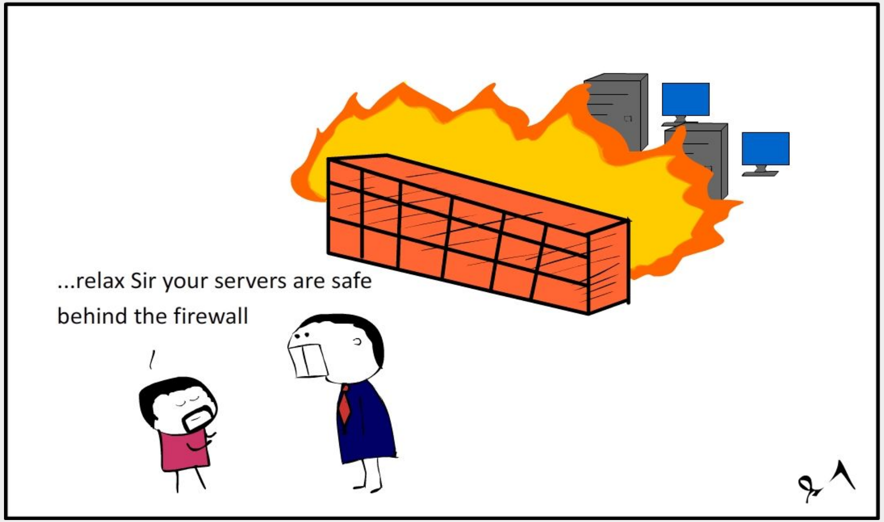
… and the outcome of the CTSC report from the check-up and on-site visit.

Highlights

- Focused on policy and ICS/SCADA review.
- Physical penetration test.
- Physical inspection and evaluation of shared mid-level facility on Maunakea.
- Physical inspection and evaluation of Gemini telescope on Maunakea summit.

Highlights

- ITS and staff interviews.
- Behold: the Mighty Firewall! (Artist's rendering)
- Formal recommendations document drafted, reviewed, and received.
- Recommendations Taxonomy: impact vs. cost.
- Memo on ICS/SCADA hardening.
- Most significant IT security assessment to date.

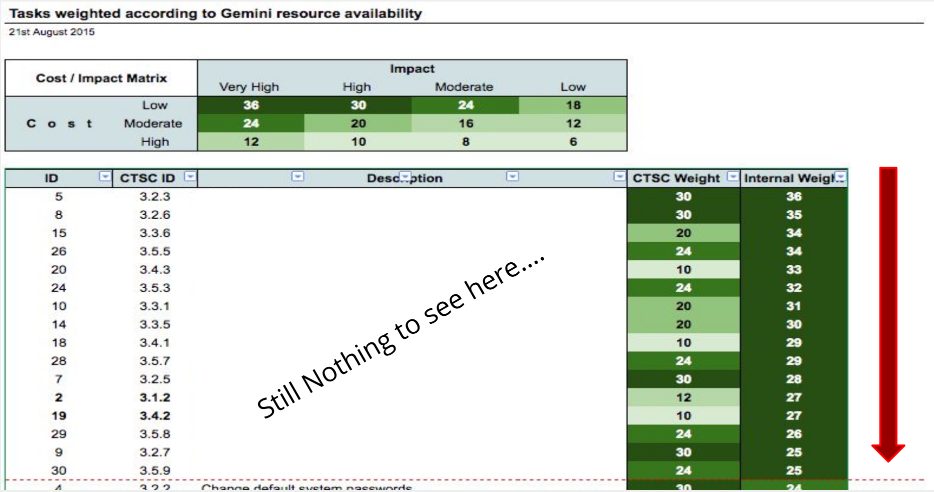


Where do we go from here?

… keeping the momentum - and budget ;)

Post CTSC

- The original list is still valid ...
- … but now there is a more focused list.
- Same principles applied ...
- … but the priorities have changed - for now
- Without losing sight of the goal, efforts are focused on the “can do’s” and “must do’s”
- We know what needs to be done and how to deliver.



Tasks weighted according to Gemini resource availability

21st August 2015

Cost / Impact Matrix		Impact			
		Very High	High	Moderate	Low
Cost	Low	36	30	24	18
	Moderate	24	20	16	12
	High	12	10	8	6

ID	CTSC ID	Desc..ption	CTSC Weight	Internal Weig...
5	3.2.3		30	36
8	3.2.6		30	35
15	3.3.6		20	34
26	3.5.5		24	34
20	3.4.3		10	33
24	3.5.3		24	32
10	3.3.1		20	31
14	3.3.5		20	30
18	3.4.1		10	29
28	3.5.7		24	29
7	3.2.5		30	28
2	**3.1.2**		12	27
19	**3.4.2**		10	27
29	3.5.8		24	26
9	3.2.7		30	25
30	3.5.9		24	25
4	3.2.2	Change default system passwords	30	24

Still Nothing to see here....

Continuity

- Key staff departure
- Continuity and visibility through PM approach
- Build the new team, focus on the plan and …
- Keep going!

Take-aways:

- Having built a plan around CTSC recommendations provided a focused path.
- Using project management concepts simplified budget planning and provided visibility into CS.
- Additional engagements or peer reviews are necessary to confirm progress.
- CTSC have done a fantastic job!

Keep Sounding the Alarm!

Keep management aware of cybersecurity incidents!

Questions?

Thank You.

GEMINI OBSERVATORY
Exploring the Universe, Sharing its Wonders

NSF

AURA