Initiating Security Initiatives Through System Wide IT Governance

Nathan Zierfuss
Jim Durkee
In some ways IT governance is a way to get past the “that's a great idea” stage of security project initiation. It provides security controls and a framework in which to move initiatives forward. In a distributed system it is easy to become overwhelmed by stakeholders when operating on a system wide scale in an ad hoc manner. In higher education we have a lot of independent spirit and self starters. At UA at least until recently there was no predictable place to go or path to take when you wanted to do something new. In comes IT governance and system wide information security to save the day right? Before going into all the details some history and frame of reference is necessary.

**Working with IT Governance**

- Statewide distributed system
- Independent spirit
- History of no predictable place to go when starting new initiatives
- Adopted an IT governance structure
- Instituted system wide Information Security Officer
- How do we work effectively in this environment?
The University of Alaska started as the Alaska Agricultural College & School of Mines in Fairbanks, Alaska in 1917 with a single building and 6 students. The name changed to the University of Alaska in 1935. Currently there are 3 individually accredited campuses. University of Alaska Anchorage was established in 1954 and University of Alaska Juneau in 1955, now University of Alaska Southeast. Each main campus has associated distributed campuses and colleges in rural communities. Many rural campuses and colleges are not connected to the rest of the state by road, often separated by hundreds of miles in areas where extreme weather patterns are the norm.
The geography and lack of infrastructure such as roads and right of ways requires the use of satellite and microwave connections to extend the WAN to distant community campuses not on the road system. In smaller towns and villages the experience level of staff and number of people to choose from poses challenges to information security. If distributed technicians are struggling with maintaining uptime on a departmental file server willingness to scan systems for PII on a regular basis become lower priority. Often non-IT employees have to serve IT support roles.
Our operating climate varies widely. From 90 degrees above with 22 hours of daylight in the summer down to -40 or lower with 3 to 4 hours of sun in the winter. With this geography and climate come the reality that there is not a pile of enterprise class hardware in a warehouse down the street. In fact next day air delivery to Alaska is really 2 to 3 day air. So self reliance is a quality you find in abundance in our operations and the people.
Demographics

- 33,000 students
- 500 programs of study
- Land, sea & space grant research
- 8,000 employees
- $1,000,000,000 estimated economic impact

The system serves ~33,000 students in 500 programs of study ranging from workforce training to Ph.D. University of Alaska also conducts significant research activity from the atmosphere to the ocean floor. This activity is supported by approximately 8,000 employment is ~8,000 and has an estimated economic impact of $1 billion dollars annually.
There is diversity in the system. UAA is urban and growing in the heart of Anchorage it is a metropolitan campus with new programs and facilities coming online. UAF is rich in history and tradition and the center of research activity and UAS focuses on education and community. The associated community campuses and colleges work to meet the educational needs of the communities they are in and as well as offering college prep.

This may sound like a University of Alaska sales pitch but it is meant to set the stage for what is to come and emphasized that you need to know your environment! How it evolved, the current state and be aware of its diversity.
In getting to know your environment organizational structure is key. This is an oversimplification of UA’s organizational structure but it illustrates 2 things.

1) There are multiple IT groups in the system

2) None of them report to each other or have a centralized IT leadership structure

So how do we get things done that benefit the whole? Committees have commonly been used in the past. In most cases there are multiple stakeholder committees or groups are needed for any IT or information security imitative. By functional area Finance, HR and Student Services are some that come to mind and from a system wide level the number of committees can be come large quickly. This introduces a problem.
The “Are we there yet” problem. You have an idea or initiative and as you start moving it through the maze of constituent committees it changes and there are competing interests. One committee wants something removed that another committee put in and before you know it you are negotiating between them and are you are never really sure when it is done and forward movement can begin on implementation. A lot of times money being allocated or going away is the impetus to move an initiative out of discussion and into implementation. But this is not a good indicator of worthiness. So good things, in this case security initiatives, don’t get done as fast as might be necessary and the path they take in unpredictable.

This is where IT governance comes in to add definition to vetting, approval and execution. To this end UA has developed a formal IT governance structure that Jim will discuss.
IT Governance at University of Alaska is guided by the Board of Regents and the Presidents Cabinet within the Information Technology Executive Council (ITEC). ITEC identifies strategic IT priorities and monitors development of them. The Program Management Team (PMT) vets projects resulting from ITEC recommendations, identifies funding and other resources to be allocated in the commission of efforts. The CIO Management Team (CMT) manages the planning, and implementation of enterprise IT architecture. In the execution of IT Governance the Project Management Office (PMO) organizes and facilitates the ITEC, PMT and CMT groups.
This is the maturity model we use to gauge the state and progress of IT governance at University of Alaska. Currently are between 1 and 2. The Project Management Office has a goal of getting to between a 2 and 3 in the next year.
So how did we get here? In the beginning we had committees. Which were more like discussion groups and sometimes devoid of ability to execute on the things that did get approved. Early attempts at IT governance where hampered by interpersonal challenges, membership wasn’t quite right for getting things done but it was a step in the right direction. In it’s current state 2 levels of governance groups. One focusing on strategy, that is what we are going to do, and the other level being management, that is how we are going to do something, is very important to gaining support system wide and providing progression. Close monitoring of group cohesion to keep everyone playing nice together and focused is necessary. Key to IT governances success so far had been the support of the Project Management Office for the ITEC, PMT & CMT. This slide doesn’t communicate it very well but from the starting point to the current state took years and multiple attempts to get a working process.
Why do we want to get here? The Software Engineering Institute at CMU has laid out 11 elements of effective security governance that are captured in the IT governance structure, the membership of its groups and reflected in the maturity model.

Effective governance for security needs to be enterprise wide and ensure leaders are accountable.

It needs to be based on business requirements and assess projects based on risk.

Backing the IT governance process with supporting policy and enforcing its use helps adoption.

To be effective IT governance groups need to have define duties and be able to allocate resources.

Staff awareness and training on the IT governance process is also necessary.

The IT governance process needs to have and require a life cycle view that includes planning, management, measurement and review. These things make it a processes that improves and changes over time.
A history of information security gives us perspective on how we got where we are today. In 1998 information security was best effort on the part of individual system administrators, as awareness grew 2 security roles were defined in system operations. An incident response group formed, development of technical security standards started and an information security officer position focused on operational security created. As a side duty policy and procedure development was also assigned to this person.
The events in white are not happy times for UA, for the CIO or the security group. There was a worm outbreak that impacted operations and a server containing PII was discovered to have been compromised at a community campus. This raised the visibility of information security to the President, Board of Regents and community. Interest in information security increased overnight and was reinforced by a second smaller event being discovered shortly after the last one was closed out. However out of these incidents came a cycle of IT security reviews followed by remediation efforts. The first of which was conducted internally by IT an only at one location.
By this time 2 more IT security staff were added. Then came a second external security audit managed by IT but conducted by an outside firm. This review included all the major campuses IT departments and results were reported to the Board of Regents. A round of remediation and validation followed the review. As result an information security officer to cover policy, standards and guidelines was brought onboard 2010. So the evolution of awareness is not a short process either. Our third IT security audit is getting ready to take place in coming month or so. This time management is being handled by internal audit and the review preformed by an external reviewer. Now that we have the progression of IT governance and information security lets look at why we would want to use IT governance.
Leveraging IT governance for security initiatives

- Links IT strategy to information security strategy
- Streamlines approval by replacing confusion with process
- With the right people present efforts move forward
- Gives multiple levels of visibility

It links IT strategy to information security strategy by taking up challenges and opportunities early and from the top down. Management buy-in gets more accomplished then management skepticism as you move into implementing. IT governance streamlines approval by replacing the “Are we there yet?” problem with a defined path that all the players are on. With clear linkage and management support efforts move through IT governance and into implementation. The IT governance group design in this model gives multiple levels of visibility to an initiative from the system wide management and into the campuses.
What have we done with IT governance and how? I’m going to pass the mic to Jim for these first few.

description of project
historical difficulties it resolved
how it moved through the process including needed support
outcome & impact on security
I’ll wrap this up with an image of the dashboard from the project management office that illustrates where things are in this IT governance process. Notice it looks similar to the overview of how things flow through the IT governance groups. That is because IT governance groups are either involved in or informed of the status through implementation. So we aren’t just getting a rubber stamp and saying we’ll call you when it’s done.
More Details

University of Alaska Program Management Office
http://www.alaska.edu/pmo/

University of Alaska Office of Information Technology
http://www.alaska.edu/oit/

More details and contact information for any follow up questions we might not have time to answer in this session or offline this week can be found at these URLs. To summarize know your environment, its past, what hasn’t worked and why but don’t dwell on it. Use it to design governance around those issues. We think what is presented here works well and is progressing. It has great potential for security initiative initiation and completion. Getting here is not a fast process though and requires constant care and feeding to move in this direction. With that thank you for your attention and I’ll open it up for questions.
Initiating Security Initiatives Through System Wide IT Governance

Nathan Zierfuss
Jim Durkee