Information Security Governance

Information Security Governance

What is Information Security Governance and What it is Not

IT security governance is the system by which an organization directs and controls IT security (adapted from ISO 38500). IT security governance should not be confused with IT security management. IT security management is concerned with making decisions to mitigate risks; governance determines who is authorized to make decisions. Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks. Management recommends security strategies. Governance ensures that security strategies are aligned with business objectives and consistent with regulations.

NIST describes IT governance as the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

Enterprise security governance results from the duty of care owed by leadership towards fiduciary requirements. This position is based on judicial rationale and reasonable standards of care [1]. The five general governance areas are:

1. Govern the operations of the organization and protect its critical assets
2. Protect the organization's market share and stock price (perhaps not appropriate for education)
3. Govern the conduct of employees (educational AUP and other policies that may apply to use of technology resources, data handling, etc.)
4. Protect the reputation of the organization
5. Ensure compliance requirements are met

"Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business." [1]

Governance: doing the right thing.

Management: doing things right.

Governance	Management
Oversight	Implementation
Authorizes decision rights	Authorized to make decisions
Enact policy	Enforce policy
Accountability	Responsibility
Strategic planning	Project planning
Resource allocation	Resource utilization

Characteristics of effective security governance [1]

The eleven characteristics of effective security governance are critical for an effective enterprise information security information program. They are:

1. It is an institution-wide issue
2. Leaders are accountable
3. It is viewed as an institutional requirement (cost of doing business)
4. It is risk-based
5. Roles, responsibilities and segregation of duties are defined
6. It is addressed and enforced in policy
7. Adequate resources are committed
8. Staff are aware and trained
9. A development life cycle is required

10. It is planned, managed, measureable and measured
11. It is reviewed and audited

Appendix A lists some excellent comparisons of effective and ineffective governance characteristics from the CERT GES [1].

The following principles describe preferred behavior to guide governance decision making [7].

- Responsibility: Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.
- Strategy: The organization's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy.
- Acquisition: IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.
- Performance: IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.
- Conformance: IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.
- Human Behavior: IT policies, practices and decisions demonstrate respect for Human Behavior, including the current and evolving needs of all the 'people in the process'.

Listed below are challenges of ineffective governance [1]. These challenges can be very useful in presenting rationale to leadership for implementing an effective institution security governance model.

1. Understanding the implications of ubiquitous access and distributed information
2. Appreciating the institution-wide nature of the security problem
3. Overcoming the lack of a game plan
4. Establishing the proper institutional structure and segregation of duties
5. Understanding complex global legal compliance requirements and liability risks (the word global may or may not apply to education)
6. Assessing security risks and the magnitude of harm to the institution
7. Determining and justifying appropriate levels of resources and investment
8. Dealing with the intangible nature of security
9. Reconciling inconsistent deployment of security best practices and standards
10. Overcoming difficulties in creating and sustaining a security-aware culture

Outcomes of effective information security governance should include: [4]

- Strategic alignment of information security with institutional objectives
- Risk management - identify, manage, and mitigate risks
- Resource management
- Performance measurement - defining, reporting, and using information security governance metrics
- Value delivery by optimizing information security investment

Defining the Information Security Program (so as to define what needs to be governed) [1]

Activities of an information security program directly support/trace to an institutional risk management plan. In other words, the information security program is targeted to managing institutional risk. An effective information security program requires the development and maintenance of:

1. A long-term information security strategy
2. An overarching institutional security plan (which may be supported by underlying academic/administrative unit security plans and security plans for individual systems)
3. Security policies, procedures, and other artifacts
4. The system architecture and supporting documentation

Information Security Program hierarchical relationships

- Institutional Risk Management Plan is supported by
- Institutional Security Strategy is supported by
- Institutional Security Plan is supported by
    - Academic and administrative unit security plans
    - System security plans
    - Policies and procedures
    - System architecture

Some colleges and universities employ risk managers and some do not. Of those institutions that do employ a risk manager, there are few that appear to have an institution-level risk management plan.

The reference to an information security program serving as a business plan for securing digital assets is a simple yet effective communication technique.

Information Security Governance Best Practices [5]

- Information security activities should be governed based on relevant requirements, including laws, regulations, and organizational policies.
- Senior managers should be actively involved in establishing information security governance framework and the act of governing the agency's implementation of information security.
  Information security responsibilities must be assigned and carried out by appropriately trained individuals.
- Individuals responsible for information security within the agency should be held accountable for their actions or lack of actions.
- Information security priorities should be communicated to stakeholders of all levels within an organization to ensure a successful implementation of an information security program.
- Information security activities must be integrated into other management activities of the enterprise, including strategic planning, capital planning, and enterprise architecture.
- Information security organization structure should be appropriate for the organization it supports and should evolve with the organization, if the organization undergoes change.

- Information security managers should continuously monitor the performance of the security program/effort for which they are responsible, using available tools and information.
- Information discovered through monitoring should be used as an input into management decisions about priorities and funding allocation to effect the improvement of security posture and the overall performance of the organization.

Why Information Security Governance is Needed

Why is IT governance important [3]

- Financial payoffs
- IT is expensive
- IT is pervasive
- New technologies
- IT governance is critical to learning about IT value
- Not just technical - integration and buy-in from business leaders is needed for success
- Senior executives have limited bandwidth, especially at large institutions, so they can't do it all
- Governance patterns depend on desired behaviors
    - Top revenue growth - decentralized to promote customer responsiveness and innovation
    - Profit - centralized to promote sharing, reuse and efficient asset utilization
    - Multiple performance goals - blended centralized and decentralized governance

Directors could be held accountable for breaches of [7]:

- security standards;
- privacy legislation;
- spam legislation;
- trade practices legislation;
- intellectual property rights, including software licensing agreements;
- record keeping requirements;
- environmental legislation and regulations;
- health and safety legislation;
- accessibility legislation;
- social responsibility standards.

Benefits of information security governance [4]

- Increased predictability and reduced uncertainty of business operations
- Protection from the potential for civil and legal liability
- Structure to optimize the allocation of resources
- Assurance of security policy compliance
- Foundation for effective risk management.
- A level of assurance that critical decisions are not based on faulty information
- Accountability for safeguarding information

Question to engage institutional leaders [4]

Thought provoking questions that institutional leaders can ask (and should be able to answer) to determine the state of their security governance efforts.

- Questions to uncover information security issues
    - Does the head of security/CISO routinely meet or brief institutional leaders?
    - When was the last time top managers got involved in security-related decisions?
    - Do managers know who is responsible for security?
    - Would people recognize a security incident? Would they know who to call?
- Questions to find out how managers addresses information security issues
    - Is the institution clear on its position relative to IT and security risks?
    - How much is spent on information security?
    - What percentage of staff had security training last year?
- Questions to assess information security governance practices
    - Are managers confident that security is being adequately addressed in the enterprise?
    - Are managers aware of the latest information security issues and best practices?
    - Does the institution participate in an incident, threat, vulnerability notification and sharing service?
    - What is the industry best practice and how does the institution compare?
    - What can be done to successfully implement information security governance?

Questions individuals responsible for governance should ask and be able to answer.

- Questions for directors/trustees
    - Does the board understand the institution's dependence on information?
    - Does the institution recognize the value and importance of information?
    - Does the institution have a security strategy?
    - Does the board understand the institution's potential liabilities in the event of regulatory non-compliance?
- Questions for managers
    - How is the board kept informed of information security issues? When was the last briefing made to the board on security risks and status of security improvements?
    - Has someone been appointed to be responsible for developing, implementing and managing the information security program, and is he /she held accountable?
    - Are security roles and responsibilities clearly defined and communicated?

- Is there a CISO or other officer with sufficient authority and resources to accomplish security objectives?

How to Govern Information Security

The ISO position is evolving from a primary technical position to one that combines both technical and managerial functions. Today IT security is an institutional imperative with critical policy and operational aspects with attention dedicated from the CIO, general counsel, internal auditor and executive leadership. While the list of tasks for the ISO continues to grow, unfortunately the authority and challenges to that authority of the role are often institutionally handled with senior administrators, legal counsel or law enforcement. The ISO must rely on institutional policy and legal compliance in order to effectively control IT security. Building a relationship and consensus with many groups on campus is a key to having security policy compliance. One progressive step is the growing recognition of department managers to accept responsibility for their data and its protection. Shifting the role of the ISO from compliance dictator to offering assistance realizes the concept of security as a service [22].

The ISO position is limited usually where the number of staff positions limits the ability to assign exclusive roles to individuals and thus dedicating a single entity to enterprise-wide information security. Larger organizations, usually with enrollments over 8,000, recognize security as a top administrative concern and have either created an ISO position or delegated this responsibility to the CIO. However the shift from security being IT's responsibility to being everyone's responsibility seems to have a greater impact on whether an appointment has been given those specific objectives. The identification of the responsibility is clear; less clear is the manner in which it should be addressed. As this profession gradually changes and increases in visibility (unfortunately through continued breaches, incidents and responses), the need for individuals with the experience of managing these episodes will evidence themselves. As the number of skilled professionals entering this field multiplies, the hope is that the role will be better defined with the proper authority given [22].

Governance frameworks, COBIT, ITIL, the ISO 17799 information security management standard, and the ISO 9000 quality management standard - are used in the IT governance processes and structures. ITIL and ISO 17799 are the most common frameworks in use. [23]

Organizational Structure

Unplanned and uncoordinated localization of authority poses great challenges for institution-wide compliance with security, copyright, privacy, identity and other regulation. It makes it awkward for CIOs to account well for the breadth and depth of overall IT activity, and it can be inefficient. Localization of authority in some areas is critical. The question is not "to centralize or not to decentralize" but where to centralize (or not) and how to harmonize institutional efforts and investments in IT. [23]

IT governance-related committees include [23]:

- Top-level IT steering committee for oversight of major IT policies and initiatives
- IT advisory committees for administration and teaching and learning
- IT initiative specific committees for items like enterprise resource planning, security or business continuity

Governance structures depend on desired outcomes

CERT GES [3] desribes structure based on desired outcomes.

- Top revenue growth - decentralized to promote customer responsiveness and innovation
- Profit - centralized to promote sharing, reuse and efficient asset utilization
- Multiple performance goals - blended centralized and decentralized

Information Security Governance Structures

The NIST Security Handbook [5] states that governance is highly dependent on the overall organization structure.

- Centralized maintain budget control and ensure implementation and monitoring of information security controls.
- Decentralized have policy and oversight responsibilities and budget responsibilities for their departmental security program not the operating unit information security program. Reporting structures are different as well.
- Governance structures can be hybrid, with a combination of characteristics from both centralized and decentralized.

Political Archetypes

Weill and Ross use political archetypes in *IT Governance* [3] to describes people or groups who have decision rights.

- Business monarchy: Senior business executives make IT decisions
- IT monarchy: IT executives make IT decisions
- Feudal: Business unit leaders make IT decisions to optimize local needs, but does not facilitate enterprise decision-making.
- Federal: Coordinated IT decision-making between the center and the business units.
- IT duopoly: IT executives and one other group (such as senior executives or business units) make IT decisions.
- Anarchy: Individual users or small groups make IT decisions Anarchy is expensive, difficult to support and rare, but sometimes used when very rapid customer responsiveness is needed.

Different types of decisions might use different archetypes [3].

Decisions	IT Principles	IT Architecture	IT Infrastructure	Business Applications	IT Investment
Archetypes					
Business Monarchy		⊖	⊖		⊕
IT Monarchy		⊕	⊕	⊖	⊖

Feudal	⊖	⊖	⊖		⊖
Federal		⊖	⊖	⊕	⊕
IT Duopoly	⊕			⊕	⊕
Anarchy	⊖	⊖	⊖	⊖	⊖
Don't know	⊖	⊖	⊖	⊖	⊖

What Governance Arrangements Work Best [3]

- Monarchies work well when profit is a priority.
- Feudal or business monarchy arrangements might work best when growth is a priority.
- Federal arrangements can work well for input into all IT decisions. Avoid federal arrangement for all decisions since it's difficult to balance the center with the business unit needs.
- Duopoly arrangements work well for IT principles, investment decisions and business application needs. Duopolies also work best when asset utilization is a priority.

Roles and Responsibilities

The ISO or CISO is an emerging profession with highly-motivated individuals seeking their own professional development through membership in organizations, participation in training where they can find it and constant sharing of ideas and advice with others both internally and externally to their organization. There does not seem to be a clearly defined path for this new subfield within IT. The vast majority of those in an ISO/CISO position held previous positions in IT and came from higher education backgrounds. Institutions appear to be recruiting security officers from IT managerial ranks. Often these folks started with very strong technical experience and have now developed skills in business process analysis, thus moving away from hands-on activities [22].

In addition to certifications, ISOs find the following "soft skills" beneficial [22].

- Reputation building
- Campus-wide coordination and communication
- Collaboration
- Campus-wide profiles

These soft skills are critical for effective engagement with diverse campus audiences.

- Senior leader of the institution
- Deans, Department Chairs and Directors
- IT managers
- Auditors
- Attorneys
- Human Resources
- Faculty
- Staff
- Students

Primary ISO responsibilities [22]

- Development and enforcement of security policies and procedures
- Risk management
- Security awareness program
- Incident management and forensics
- Business continuity
- Disaster recovery

Supportive functions of an ISO [22]

- Application and system security
- Network security
- Access control
- Authentication and authorization
- Identity management

Decision-Making Structures

Weill and Ross [3] describe organizational units and roles responsible for making IT decisions, such as committees, executive teams, and business/IT relationship managers.

- Executive or senior management committees
- IT leadership committee
- Process teams with IT members
- Business/IT relationship managers
- IT council of IT and business executives
- Architecture committee
- Capital improvement committee

Who should be concerned with information security governance? [4]

- Board of directors/trustees - The board has fundamental responsibility to protect the interests of the organization.

- Executives - This group develops strategies and ensures integration with and cooperation of business unit managers and process owners
- Steering committee - This group includes representation across the organization and is responsible for ensuring that stakeholders concerns are addressed.
- CISO

What should the board of directors/trustees and senior executives be doing? [4]

- Understand why information security needs to be governed
    - Address risks and threats
    - Protect the organization's reputation
    - Ensure coordination and cooperation among business units
- Take board level action
    - Become informed about information security
    - Set direction (e.g., drive policy and strategy)
    - Provide resources
    - Assign responsibilities
    - Set priorities
- Take senior level action
    - Provide oversight for the development of a security framework
    - Policy development
    - Assign roles and responsibilities
    - Implement
    - Monitor
    - Ensure awareness and training

Roles and Responsibilities for an Institution-Wide Security Program

The CERT framework [1] assumes a board risk committee (or equivalent) at the highest governance level.

There are nine groups of personnel involved in developing and sustaining an effective institution-wide security program.

1. Board risk committee
2. Senior officers of the institution: chief officers such as Chief Executive Officer (CEO)/President and Chief Operating Officer (COO)/Provost
3. Cross-organizational security steering council comprised of:
    a. General Counsel
    b. Chief Information Officer
    c. Chief Security Officer and/or Chief Risk Officer
    d. Chief Privacy Officer
    e. Chief Financial Officer
    f. Deans/academic unit executives and/or other unit executives
    g. Communications executives/public relations
    h. Director of Human resources
4. Asset owners
5. Business managers
6. Operational personnel, including procurement
7. Certification agent
8. Board audit committee
9. Internal and external audit personnel

Explanations and examples of each role or team are provided in more detail in Article 2. The matrix in Table 2 of this document could be used to assist in building an institution-wide security program for higher education.

CERT GES [1] offers more detail on selected roles and responsibilities in the following documents.

- Board Risk Committee: Missions, Goals, Objectives, and Composition
- Cross-Organizational Team (X-Team): Missions, Goals, Objectives, and Composition
- Roles and Responsibilities for an Enterprise Security Program

Summary Roles and responsibilities [2]

Chief Executive Officer	- Oversee overall corporate security posture (accountable to the Board) - Brief Board, customers and public
Chief Security Officer Chief Information Officer Chief Risk Officer Department/Agency Head	- Set security policies, procedures, program and training - Incident management - Responsible for independent annual audit coordination - Compliance
Mid-Level Manager	- Compliance - Communicate policies and program (training)
Enterprise staff /employees	- Implement policies - Report vulnerabilities and breaches

To Whom Does the ISO Report [25]

	2007	2008	2009	2010	Percent Change
Chief Information Officer	38	34	32	23	-39%
Board of Directors	21	24	28	32	+52%
Chief Executive Officer	32	34	35	36	+13%
Chief Financial Officer	11	11	13	15	+36%
Chief Operating Officer	9	10	12	15	+67%
Chief Privacy Officer	8	8	14	17	+113%

Appendix B lists descriptions of information security roles and responsibilities from the NIST Security Handbook [5].

<Also see CERT EBK, http://www.us-cert.gov/ITSecurityEBK/ >

Strategic Planning [5]

Strategic Plans, annual performance plans and annual program performance reports equal the recurring cycle of reporting, planning and execution.

Each security plan must include:

- Mission, vision, goals, objectives and how they relate to the agency mission
- High-level plan for achieving information security goals and objectives including short-, mid-term objective and performance targets and performance measures.

The plans must be revisited when major changes happen including legislation, regulations, directives, agency mission priorities, emerging information security issues.

Policy

Information Security Policy and Guidance [5]

Information security policy is an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information. Information security policy is an essential component of information security governance---without the policy, governance has no substance and rules to enforce.

Information security policy should be based on a combination of appropriate legislation, such as FISMA; applicable standards, such as NIST Federal Information Processing Standards (FIPS) and guidance; and internal agency requirements.

Information security policy at the institutional level should address the fundamentals of institution's information security governance structure, including:

- Information security roles and responsibilities;
- Statement of security controls baseline and rules for exceeding the baseline; and
- Rules of behavior that agency users are expected to follow and minimum repercussions for noncompliance.

Candidate policy topics at the governance level (which could be sections in existing, broader policies) may include: [1]

- Policy calling for a security strategy, an institution-wide security program, and governance of such a program
- Code of conduct specifying what is meant by due diligence and standard of due care with respect to information security
- Security ethics
- Security risk specifying risk appetite, tolerance, scope and period of risk assessment, and ongoing risk management process
- Social responsibility with respect to security
- Business case specifying the decision making process for security investments
- Security roles and responsibilities
- Asset classification and inventory
- Data protection
- Asset access specifying access rights to categories of assets and how these are managed
- Change management
- Security standards
- Business continuity
- Disaster recovery
- Managing external parties (vendors, suppliers)
- Incident response
- Security awareness, training, and education
- Security measurement including measuring policy compliance and effectiveness
- Adherence to policy, policy waivers and exceptions, and consequences of non-compliance

Compliance

IT and data within higher education information systems are becoming increasingly regulated and scrutinized. This regulation ranges from pressures for disclosure and transparency to pressures for privacy. These pressures accent the need for common approaches, common solutions, and consistent high-quality data. [23]

Challenges and Keys to success [5]

- Balancing extensive requirement originating from multiple governing bodies.
- Balancing legislation and agency specific policy.
- Maintain currency
- Prioritizing available funding according to requirements.

Risk Management

Higher education information systems continue to be subject to a large number of security threats. The ability to secure the gamut of intuitional IT resources and data has become a compelling and increasingly urgent need. [23]

Risk management is the ongoing process of identifying information security risks and implementing plans to address them. Often, the number of assets potentially at risk exceeds the resources available to manage them. It is therefore extremely important to know where to apply available resources to mitigate risk in an efficient and cost-effective manner. ***Risk assessment***is the part of the ongoing risk management process that assigns relative priorities for mitigation plans and implementation. These sorts of decisions are institutional in nature (and not technical) and require a governance structure to address them. Depending upon the governance model selected, the governance group may be able to make such institutional priority decisions itself or may make recommendations to even higher decision-making bodies. Please see the Risk Management Framework for a more complete description and a well-defined process outline. See the Risk Management section in the Information Security Guide for more information.

Asset inventories and asset ownership

Before an effective risk management problem can be established, critical assets must be identified, documented and tracked. Engaging senior administration to review asset value provides a good opportunity to get security on their agenda. [24]

The following resources provide more information about asset management.

- The Asset and Data Management section of the Information Security Guide
- NIST FIPS 199 provides an in-depth description of a process for categorizing information and information systems
- The Asset Definition and Management Process Area of CERT's Resiliency Management Model provides comprehensive coverage of asset management

Acquisition and Procurement

IT products that are expensive or will have a significant impact on an institutions liability should be reviewed for IT security risks before purchase. In large institutions, IT product acquisition provides an opportunity to evaluate centralization vs. proliferation of IT resources and the resulting impact on security. Acquisition also serves as a good control point for information security evaluation before investments are made. Contract language might be needed to protect the institution's data, especially with products known as 'software as a service' or SaaS.

Listed below are resources for the acquisition of IT products.

- SAS70, Type II third party certification
- The BITS Shared Assessments program for assessing the capabilities of external parties before contracting for service and during the performance of a service contract
- The SEI's CMMI-DEV and CMMI-SVC include a process area (Supplier Agreement Management) for managing suppliers of software and hardware (-DEV) and all other types of services (-SVC)

Measuring and Reporting Performance

Performance [4] measurement should be a system of measuring, monitoring and reporting information security governance metrics to ensure that institutional objectives are achieved. Development/maintenance of a security and control framework that consists of standards, measures, practices, and procedures is essential to the metric evaluation of the governance structure.

A key metric is the adverse impacts of information security incidents experienced by the institution. An effective security program will show a trend of impact reduction. Quantitative measures can include trend analysis of impacts over time.

Measuring, monitoring and reporting on information security processes ensure that institutional objectives are achieved. Some example metrics might include:

- Number of incidents damaging the institution's reputation with the public
- Number of systems where security requirements are not met
- Time to grant, change and remove access privileges
- Number and type of suspected and actual access violations
- Number and type of malicious code prevented
- Number and type of security incidents
- Number and type of obsolete accounts
- Number of unauthorized IP addresses, ports and traffic types denied
- Number of access rights authorized, revoked, reset or changed

What Governance Models are Used by EDUCAUSE members

University at Buffalo, New York, Information Security Advisory Structureand IT Policies

University of Florida, Office of the Chief Information Officerand IT Security Regulations

Success Stories

We asked others how they successfully engaged senior management support for security initiatives-- "What methods worked at your institution? We've suggested some methods below. Let us know which ones have worked for you and identify others ideas not listed:

- Fear, uncertainty and doubt
- Metaphors and analogies
- Comparison with peer institutions
- Financial benefits such as ROI (return on investment)
- Leverage an incident
- Metrics
- Working behind the scenes
- Ask forgiveness rather than permission
- Little by little baby steps
- Relationship building with key players? Who are the key players
- Other ideas"

Here are some of the responses we received:

Risk Avoidance

For senior management, I would say, "It's all about risk" and risk mitigation.

Performing a risk assessment helps us out. If you can get them to commit a few hours of staff time to an RA then you can provide some assurance that whatever steps you recommend are well reasoned and show a risk-based strategy for identifying solving security problems. This helps me to avoid the impression that an initiative is just the security people being paranoid.

Leverage an Incident

While I don't recommend it, a breach certainly helped get upper management's attention! After the clean up and notification, we were able to garner some addition resources.

On occasion, an audit issue or an incident will also help drive something forward. In my experience though you have to capitalize on those pretty quickly otherwise priorities will shift and they'll be forgotten about.

Work Behind the Scenes

Years ago I learned the technique of 'digging in front' as in, "If you want to move a large boulder, digging in front of it before pushing from behind makes it much easier to move the boulder." When I want to make something happen, I spend time talking individually with every key player who might have a stake in it (especially those who might be uncertain or against to the idea). Digging in front goes a long way.

In advance, evaluation and testing of new security tools and bringing very colorful graphs to senior management, before ask for anything.

What also helps - Working behind the scenes, lots of 1-1 engagement in the community (even if not defined as 'key' players), incremental steps and not trying to make the issue so big, encompassing, or scary that it loses credibility, or asking for disproportionate funding or level of authority - it helps to work within the culture.

On the policy front, we've used several methods to achieve support from senior management. When we put a policy in place to address HIPAA security requirements, we worked up-front with the Office of General Counsel to ensure the policy accurately reflected regulatory requirements and then it was simply a matter of saying, hey this is required by law. The policy was accepted by the University without a hitch. It helped that it was our General Counsel that said that to the President's Council (was approves all policies). We also spent a lot of time building relationships with HR and Student Health since they were the primary stakeholders.

We're currently having a lot of success with our Information Security Policy proposal. Our technique there has really just been understanding business requirements, being flexible and selling it in a manner that makes sense for whichever audience we're presenting to. Letting people talk through their concerns and taking a real interest in addressing those concerns is also very valuable. We've really had little resistance to this point and we're moving along much faster than I would have originally anticipated. I guess this fits into relationship building with key players. There are just a lot of key players when dealing with something that impacts the entire university.

We realized that nearly every department on campus has departmental meetings (larger ones may have more than one kind - a more frequent one for supervisors and another for all staff). These meetings were often looking for agenda items and special speakers. We started calling and got ourselves invited to make small presentations. After a few of these we had a kit full of ready-made presentations that we could modify and use over and over. These visits went a long way to building relationships, raising awareness, and giving others a voice in what we were planning.

Compliance

Compliance with laws can be a major driver - state data breach law was a motivator here.

We found that having Internal Auditing do an audit and issuing a report an excellent way to get what we need for security. Complying with IA is always a powerful motivator.

Our university is required to have guidelines that are compatible with State IT security policies and, as a result, our IT security officers developed a comprehensive set of guidelines that address risk management, security policy, access controls, network security, nonpublic information, encryption, and other areas. These guidelines were vetted with the State legislative auditors and are periodically updated to align with revisions to the State IT Security Policy. All of our campuses are required to report on the status of implementation of these guidelines annually and some of the institutional security officers have taken advantage of this reporting process to engage senior management.

Relationships

I regularly send out breach reports to senior management and even though I am a member of senior management - I use these to get my points across and it is quite effective. I was able to obtain funding for whole disk encryption just recently.

Development, adoption, deployment, and compliance monitoring of an IT Security Governance Industry Standard such as ISO 17799. Concurrent with this - Enterprise ITSEC Strategy (ITSEC is a risk management issue not a technical one!), enabling programs, federated compliance monitoring tools, and performance metrics.

Suggested approach includes:

1. Articulate and approve an overall security strategy.
2. Develop a security technical architecture to support the strategy.
3. Establish needed policies to support the strategy and architecture.
4. Acquire additional tools to support the architecture.
5. Establish an organizational structure to deploy the tools and monitor policy adherence.
6. Establish a management reporting mechanism to inform unit and executive management about unit adherence to the strategy and policies as well as to compromised systems.
7. Prioritize activities into implementation phases.
8. Communicate the overall security program to the campus community.

Hands down the activity that has shown the most success and has proven the most beneficial to our security cause is our incident response strategy when an incident involves confidential data. When this is the case I stand up before our data incident response team to talk through the situation and determine what actions the university needs to take. Since the team involves the appropriate data steward, Dean or unit head where the incident occurred, technical staff in that unit, CIO, University Counsel, Audit, Risk Management, Police and a couple of others, all the right people get to hear first hand our challenges and the consequences of when things don't go right.

After doing this for well over three years I don't need to spend much time around campus trying to sell the need for security.

At our state university, the Vice Chancellor for IT and CIO sits on the Executive Cabinet and periodically briefs the Chancellor and senior management on IT security and policy matters on campus, and in the higher education community. In addition, we had an external security review conducted by a group of experts in IT security and policy from other higher education institutions in 2005, and again early in 2008. The review team provided a report with a number of recommendations that helped "raise the awareness" of the importance of IT security at the institution. We also formed an IT Security & Policy Advisory Committee with representatives from all over campus and have had success in moving forward with a number of security initiatives.

Metrics

I say, bombard them with information. There are several sites but this one deals with Educational Security Incidents

We have a couple of real-time graphics that help to convey the message without a lot of tech-talk.

We depict the traffic crossing our border with a 256x256 grid of dots for every possible IP address here. When a packet passes the border, the corresponding dot for the sender/recipient on our end lights up. So, we see how busy various parts of our network are. We also see when we get scanned.

In a 5 minute presentation to one or a group of VPs, you can usually see a scan. Sometimes it's a sequential scan and is pretty obvious, and the rest of the time it's "snow" from a randomized scan that hits our darknet areas as well as the subnets that are assigned. We include in the display the probes that are blocked by border firewall rules. That shows how much we are pre-emptively blocking as well as how much is still getting through. We've talked about having an outside machine that we could use to launch a scan (with a small TTL) during a presentation, but we've never needed to go to the trouble. The hackers are always very accommodating. This is a useful tool for talking with local reporters who can then help get the word out to our users about the importance of patches, updates, firewalls, virus protection, etc.

The second graphic is a dynamic visualization of a subset of our traffic, selected by port or IP range, showing the source and destination and bandwidth in use. We can show unauthorized email servers (like hacked spammers), or unusual DNS queries, or remote desktop connections to unusual outsiders or to sensitive insiders, etc. (We mention that we are careful to not show this second display to reporters.)

With these tools we can visually demonstrate to administrators that we are always subject to probes and frequently have "misbehaving" systems. A picture is worth a thousand words and, for us, a realtime dynamic visualization is worth a thousand pictures.

In general, comparisons with peer institutions and industry standards also goes a long way for us in anything we do. Its pretty much expected that we evaluate what other universities are doing.

Other EDUCAUSE Resources

Information Security Governance
IT Governance
Process and Politics: IT Governance in Higher Education, ECAR study
EDUCAUSE Information Technology Governance Summit (September 10-11, 2007)

Appendices

Appendix A

Effective/Ineffective Governance Compared

Effective Governance	Ineffective Governance
Board members understand that information security is critical to the organization and demand to be updated quarterly on security performance and breaches.	Board members do not understand that information security is in their realm of responsibility, and focus solely on corporate governance and profits.
The board establishes a risk committee that understands security's role in achieving compliance with applicable laws and regulations, and in mitigating organization risk.	Security is addressed adhoc, if at all.
The board risk committee conducts regular reviews of the enterprise information security.	Reviews are conducted following a major incident, if at all.
The board's audit committee ensures that annual internal and external audits of the security program are conducted and reported.	The BAC defers to internal and external auditors on the need for reviews. There is no audit plan to guide this selection.
The board risk committee and executive management team set an acceptable risk level. This is based on comprehensive and periodic risk assessments that take into account reasonably foreseeable internal and external security risks and magnitude of harm.	The CISO locates boilerplate security policies, inserts the organization's name, and has the CEO sign them.
The resulting risk management plan is aligned with the entity's strategic goals, forming the basis for the company's security policies and program.	If a documented security plan exists, it does not map to the organization's risk management or strategic plan, and does not capture security requirements for systems and other digital assets.
A cross-organizational security team comprised of senior management, general counsel, CFO, CIO, CSO and/or CRO, CPO, HR, internal communication/public relations, and procurement personnel meet regularly to discuss the effectiveness of the security program, new issues, and to coordinate the resolution of problems.	CEO, CFO, general counsel, HR, procurement personnel, and business unit managers view information security as the responsibility of the CIO, CISO, and IT department and do not get involved. The CSO handles physical and personnel security and rarely interacts with the CISO. The general counsel rarely communicates particular compliance requirements or contractual security provisions to managers and technical staff, or communicates on an ad-hoc basis.
The CSO/CRO reports to the COO or CEO of the organization with a clear delineation of responsibilities and rights separate from the CIO.	The CRO does not interact with the CISO or consider security to be a key risk for the organization.
Operational policies and procedures enforce segregation of duties and provide checks and balances and audit trails against abuses.	The CISO reports to the CIO. The CISO is responsible for all activities associated with system and information ownership.
Risks (including security) inherent at critical steps and decision points throughout business processes are documented and regularly reviewed.	All security activity takes place within the security department, thus security works within a silo and is not integrated throughout the organization.
Executive management holds business leaders responsible for carrying out risk management activities (including security) for their specific business units. Business leaders accept the risks for their systems and authorize or deny their operation.	Business leaders are not aware of the risks associated with their systems or take no responsibility for their security.
Critical systems and digital assets are documented and have designated owners and defined security requirements.	Systems and digital assets are not documented and not analyzed for potential security risks that can affect operations, productivity, and profitability. System and asset ownership are not clearly established.
There are documented policies and procedures for change management at both the operational and technical levels, with appropriate segregation of duties.	The change management process is absent or ineffective. It is not documented or controlled.
There is zero tolerance for unauthorized changes with identified consequences if these are intentional.	The CIO (instead of the CISO) ensures that all necessary changes are made to security controls. In effect, separation of duties is absent.
Employees are held accountable for complying with security policies and procedures. This includes reporting any malicious security breaches, intentional compromises, or suspected internal violations of policies and procedures.	Policies and procedures are developed but no enforcement or accountability practices are envisioned or deployed. Monitoring of employees and checks on controls are not routinely performed.

The ESP implements sound, proven security practices and standards necessary to support business operations.	No or minimal security standards and sound practices are implemented. Using these is not viewed as a business imperative.
Security products, tools, managed services, and consultants are purchased and deployed in a consistent and informed manner, using an established, documented process.	Security products, tools, managed services, and consultants are purchased and deployed without any real research or performance metrics to be able to determine their ROI or effectiveness.
They are periodically reviewed to ensure they continue to meet security requirements and are cost effective.	The organization has a false sense of security because it is using products, tools, managed services, and consultants.
The organization reviews its enterprise security program, security processes, and security's role in business processes.	The organization does not have an enterprise security program and does not analyze its security processes for improvement.
The goal of the enterprise seurity program is continuous improvement.	The organization addresses security in an ad-hoc fashion, responding to the latest threat or attack, often repeating the same mistakes.
Independent audits are conducted by the BAC. Independent reviews are conducted by the BRC. Results are discussed with leaders and the Board. Corrective actions are taken in a timely manner, and reviewed.	Audits and reviews are conducted after major security incidents, if at all.

Appendix B

Roles and Responsibilities from the NIST Security Handbook

Agency Head

- Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, and on information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
- Ensuring that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the organization;
- Ensuring that information security processes are integrated with strategic and operational planning processes to secure the organization's mission;
- Ensuring that senior agency officials within the organization are given the necessary authority to secure the operations and assets under their control;
- Designating a CIO and delegating authority to that individual to ensure compliance with applicable information security requirements;
- Ensuring that the agency has trained personnel to support compliance with information security policies, processes, standards, and guidelines; and
- Ensuring that the CIO, in coordination with the other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including the progress of remedial actions.

Chief Information Officer

- Designating a senior agency information security officer (SAISO);
- Developing and maintaining an agency-wide information security program;
- Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements;
- Ensuring compliance with applicable information security requirements; and
- Reporting annually, in coordination with the other senior agency officials, to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

Senior Agency Information Security Officer of Chief Information Security Officer

- Performing information security duties as the primary duty;
- Heading an office with the mission and resources to assist in ensuring agency compliance with information security requirements;
- Periodically assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;
- Developing and maintaining risk-based, cost-effective information security policies, procedures, and control techniques to address all applicable requirements throughout the life cycle of each agency information system to ensure compliance with applicable requirements;
- Facilitating development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- Ensuring that agency personnel, including contractors, receive appropriate information security awareness training;
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities;
- Periodically testing and evaluating the effectiveness of information security policies, procedures, and practices;
- Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- Developing and implementing procedures for detecting, reporting, and responding to security incidents;
- Ensuring preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of the agency; and
- Supporting the agency CIO in annual reporting to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

Chief Enterprise Architect

- Leading agency enterprise architecture development and implementation efforts;
- Collaborating with lines of business within the agency to ensure proper integration of lines of business into enterprise architecture;
- Participating in agency strategic planning and performance planning activities to ensure proper integration of enterprise architecture;
- Facilitating integration of information security into all layers of enterprise architecture to ensure agency implementation of secure solutions; and

- Working closely with the program managers, the senior agency information security officer (SAISO), and the business owners to ensure that all technical architecture requirements are adequately addressed by applying FEA and the Security and Privacy Profile (SPP).

Inspector General (IG)
The IG is a statutory office within an organization that, in addition to other responsibilities, works to assess an organization's information security practices and identifies vulnerabilities and the possible need to modify security measures. The IG completes this task by:

- Detecting fraud or instances of waste, abuse, or misuse of an organization's funds;
- Identifying operational deficiencies within the organization;
- Ensuring that the underlying problems that permit such failings are rectified; and
- Offering recommendations for preventing problems in the future.

Chief Financial Officer
The CFO is the senior financial advisor to the investment review board (IRB) and the agency head. Information security investments fall within the purview of the CFO and are included in the CFO's reports. In this capacity, the CFO is responsible for:

- Reviewing cost goals of each major information security investment;
- Reporting financial management information to OMB as part of the President's budget;
- Complying with legislative and OMB-defined responsibilities as they relate to IT capital investments;
- Reviewing systems that impact financial management activities; and
- Forwarding investment assessments to the IRB.

Chief Privacy Officer
The chief privacy officer is responsible for privacy compliance across an organization, including privacy compliance measures that apply to information security assets and activities. The chief privacy officer works to maintain a balance between security and privacy requirements, and works to ensure that one is not compromised for the sake of the other. To this end, the chief privacy officer serves as the senior official responsible for:

- Developing, promoting, and supporting the organization's privacy programs;
- Encouraging awareness of potential privacy issues and policies; and
- Reviewing and implementing privacy regulations and legislation.

Physical Security Officer or other designated official with physical security responsibilities. The physical security officer is responsible for the overall implementation and management of physical security controls across an organization, to include integration with applicable information security controls. As information security programs are developed, senior agency officials should work toensure this coordination of complementary controls. In consideration of information security, the physical security officer serves as the senior official responsible for:

- Developing, promulgating, implementing, and monitoring the organization's physical security programs, to include appropriate controls for alternate work sites;
- Ensuring organizational implementation and monitoring of access controls (i.e., authorization, access, visitor control, transmission medium, display medium, logging)
- Coordinating organizational environmental controls (i.e., ongoing and emergency power support and backups, fire protection, temperature and humidity controls, water damage); and
- Overseeing and managing controls for delivery and removal of assets.

Personnel Security Officer
This responsibility is often resident within the Human Resources or Human Capital organization. The personnel security officer is responsible for the overall implementation and management of personnel security controls across an organization, to include integration with specific information security controls. As information security programs are developed, senior agency officials should work to ensure this coordination of complementary controls. In consideration of information security, the personnel security officer serves as the senior official responsible for:

- Developing, promulgating, implementing, and monitoring the organization's personnel security programs;
- Developing and implementing position categorization (including third-party controls), access agreements, and personnel screening, termination, and transfers; and
- Ensuring consistent and appropriate sanctions for personnel violating management, operation, or technical information security controls.

Acquisitions/Contracting
The Acquisitions/Contracting function is responsible for managing contracts and overseeing their implementation. Personnel executing this function have the following responsibilities in regards to information security:

- Collaborating with the agency's SAISO or other appropriate official to ensure that the agency's contracting policies adequately address the agency's information security requirements;
- Coordinating with the SAISO or other appropriate official as required to ensure that all agency contracts and procurements are compliant with the agency's information security policy;
- Ensuring that all personnel with responsibilities in the agency's procurement process are properly trained in information security; and
- In concert with the SAISO, facilitating the monitoring of contract performance for compliance with the agency's information security policy.

References

1. Characteristics of Effective Security Governance. 2007. Julia Allen.
2. Information Security Governance: A Call to Action. 2006. Corporate Governance Task Force Report.
3. IT Governance. 2004. Peter Weill and Jeanne Ross.
4. Information Security Governance: Guidance for Boards of Directors and Executive Management. 2006. ISACA.
5. NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers. 2006.
6. Managing Enterprise Risk in Today's World of Sophisticated Threats: A Framework for Developing Broad-Based, Cost Effective Information Security Programs. Don Ross.
7. ISO/IEC 38500: Corporate Governance of Information Technology. 2008.
8. The IT Security Essential Body of Knowledge (EBK). CERT.
9. The Tower and the Cloud. 2008. Richard N. Katz.

10. E-Research is a Fad: Scholarship 2.0, Cyberinfrastructure, and IT Governance (a chapter from The Tower and the Cloud based on IT Governance by Weill and Ross). 2008. Brad Wheeler.
11. To Govern or Not to Govern. 2008. Richard Power.
    a. Cylab Survey Reveals Gap in Board Governance of Cyber Security. 2008. Richard Power.
    b. Governance of Enterprise Security: Cylab 2008 Report. 2008. Jody Westby and Richard Power.
12. Information Security Program Self-Assessment Tool. 2013. EDUCAUSE/Internet2 Higher Education Information Security Council.
13. Information Security Governance: Guidance for Boards of Directors and Executive Management. 2006. IT Governance Institute.
14. Information Security Handbook: A Guide for Managers (NIST Special Publication 800-100). 2006. Pauline Bowen, Joan Hash and Mark Wilson.
15. Information Security Governance: Standardizing the Practice of Security Governance. 2008. Tammy Clark and Toby Sitko.
16. Governing for Enterprise Security. CERT.
    a. Governing for Enterprise Security: An Implementation Guide. 2007. Jody Westby and Julia Allen.
    b. Characteristics of Effective Security Governance. 2007. Julia Allen.
    c. Governing for Enterprise Security. 2005. Julia Allen.
    d. Governing for Enterprise Security: References. 2008. CERT.
17. Making Business-Based Security Investment Decisions - A Dashboard Approach. 2008. Julia Allen.
18. Institute of Internal Auditors report titled "Information Security Governance: What Directors Need to Know. 2001. Institute of Internal Auditors.
19. ISM3 Consortium.
    a. Maturity Model
    b. ISM3, ISO, Cobit and Parkerian Hexad Information Security Criteria Mapping
20. Information Security Governance: Motivations, Benefits and Outcomes. 2006. John P. Pironti. ISACA.
21. Podcasts available from http://www.cert.org/podcast/#governing
    a. Getting Real About Security Governance
    b. The Legal Side of Global Security
    c. Why Leaders Should Care About Security
    d. Compliance vs. Buy-in
22. The Career of the IT Security Officer in Higher Education. 2009. Marilu Goodyear.
23. Process and Politics: IT Governance in Higher Education. 2008. Ronald Yanosky and Jack McGreddie. ECAR Research Study, Volume 5.
24. The Pragmatic CSO: 12 Steps to Being a Security Master. 2007. Mike Rothman.
25. PricewaterhouseCoopers. 2010.

Questions or comments? Contact us.