Resolution of the Trustees of Indiana University
Regarding the Leadership, Responsibility, and Security
of IU's Information Technology Infrastructure

WHEREAS, the advent of the Internet has significantly transformed the manner in which information is stored on interconnected servers throughout the world; and

WHEREAS, the Internet is an information technology environment in which it is possible to have inadvertent or intentional unauthorized access to Internet sites and related servers; and

WHEREAS, successful intrusions into Internet sites and servers can lead to the disclosure of sensitive personal and institutional information; and

WHEREAS, it is critical that Indiana University protect its institutional information and information technology infrastructure so as to reduce the possibility of unauthorized access to servers holding sensitive information or running mission-critical applications.

NOW THEREFORE BE IT RESOLVED that the Trustees direct the Office of the Vice President for Information Technology and CIO to develop and implement policies necessary to minimize the possibility of unauthorized access to Indiana University's information technology infrastructure regardless of the Indiana University office involved; and

BE IT FURTHER RESOLVED that the Trustees direct the Office of the Vice President for Information Technology and CIO, which may draw upon the experience and expertise and resources of other University offices (including the Office of Internal Audit), to assume leadership, responsibility, and control of responses to unauthorized access to Indiana University's information technology infrastructure, unauthorized disclosure of electronic information and computer security breaches regardless of the Indiana University office involved.

Unanimously approved on motion duly made and seconded.

2.

I'm interested in hearing about your success stories engaging senior management support for security initiatives. What methods worked at your institution?

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

3.

“Kathy: 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 additional resources.” (Emphasis Added)

4.

“In advance, evaluation and testing of new security tools and bringing very colorful graphs to senior management, before ask for anything. (altogether: Working behind the scene and Metrics)”

5.

“Development, adoption, deployment, and compliance monitoring of an IT Security Governance Industry Standard such as ISO 27002:2005.”

6.

“1. Policy in place to address HIPAA or other security requirements;

2. Understanding business requirements, being flexible and selling it in a manner that makes sense for whichever audience we're presenting to;

3. Comparisons with peer institutions and industry standards”

7.

“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.”

8.

“Create a Business Rationale for Cyber Security”

9.

“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.”

10.

“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.”

11.

We are required to have guidelines that are compatible with State IT security policies and, as a result, our security officers developed a comprehensive set of guidelines that address risk management, security policy, access controls, network security, nonpublic information, encryption, and other areas.

12.

“We are engaged in most of the activities listed below with some being more successful than others.  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 involved confidential data.”

13.

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