An Ongoing Conversation With The Boss About Security

Shirley Payne, University of Virginia

Securing the eCampus 2008 Conference
Dartmouth
November 11-12, 2008
Copyright Shirley C. Payne; 2008.

This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.
We must all become much more vigilant in the provision of secure systems, in intrusion detection, in rapid response, and especially in education. We must practice, teach, and infuse all aspects of security into campus lives.

Dr. Linwood H. Rose
President, James Madison University
“Information Security: A Difficult Balance”
EDUCAUSE Review, September/October 2004
Agenda

- Establishing the conversation
  - Benefits
  - Obstacles
  - Paths to success

- Taking the conversation (and the security program) to the next level
  - Defining “the next level”
  - Paths to success
  - U.Va. starts the climb
The Executive Audience

- Boards of Trustees
- Presidents
- Vice Presidents & Provosts
- Deans
- CIOs
- Key executive advisors, e.g. Audit, General Counsel, Compliance, Risk Management
- Your boss
Perceived Barriers To IT Security

- Individual Privacy
- Technology Issues
- Lack of policy enforcement
- Lack of Senior Management Support
- Culture of Decentralization
- Absence of Policies
- Sophistication of Threats
- Lack of Awareness
- Culture of Openness & Autonomy
- Lack of Resources

“Safeguarding the Tower: IT Security in Higher Education”
EDUCAUSE Center for Applied Research, October 2006
Perceived Barriers To IT Security

1. Lack of Resources
2. Culture of Openness & Autonomy
3. Lack of Awareness
4. Sophistication of Threats
5. Absence of Policies
6. Culture of Decentralization
7. Lack of Senior Management Support
8. Technology Issues
9. Individual Privacy

Executives can help define appropriate security, privacy, openness balance.

“Safeguarding the Tower: IT Security in Higher Education”
EDUCAUSE Center for Applied Research, October 2006
Privacy and academic freedom are critical components of campus culture; it is vital that decisions on policies and procedures regarding security and related issues be carefully vetted, understood, and authorized by both the highest levels of the campus leadership and the representatives of the campus community. The executive role in all of these matters is crucial if internal dissension and unnecessary strife are to be avoided.

“Presidential Leadership for IT”
David Ward and Brian L. Hawkins
EDUCAUSE Review, May/June 2003
Perceived Barriers To IT Security

- Individual Privacy
- Technology Issues
  - Lack of policy enforcement
  - Lack of Senior Management Support
  - Culture of Decentralization
- Absence of Policies
- Sophistication of Threats
- Lack of Awareness
- Culture of Openness & Autonomy
- Lack of Resources

Executives can enhance policy quality & acceptance

“Safeguarding the Tower: IT Security in Higher Education”
EDUCAUSE Center for Applied Research, October 2006
Perceived Barriers To IT Security

- Individual Privacy
- Technology Issues
- Lack of policy enforcement
- Lack of Senior Management Support
- Culture of Decentralization
- Absence of Policies
- Sophistication of Threats
- Lack of Awareness
- Culture of Openness & Autonomy
- Lack of Resources

Executives can influence others to change

“Safeguarding the Tower: IT Security in Higher Education”
EDUCAUSE Center for Applied Research, October 2006
If you can get the president to set the right tone, a majority on campus will likely follow her or his lead in supporting the changes and improvements you recommend.

“Gaining the President’s Support for IT Initiative at Small Colleges.”
Laurence W. Mazzeno, President, Alvernia College
EDUCAUSE Quarterly, Number 1, 2004
Perceived Barriers To IT Security

- Individual Privacy
- Technology Issues
- Lack of policy enforcement
- Lack of Senior Management Support
- Culture of Decentralization
- Absence of Policies
- Sophistication of Threats
- Lack of Awareness
- Culture of Openness & Autonomy
- Lack of Resources

Executives can help determine/clarify responsibilities

“Safeguarding the Tower: IT Security in Higher Education”
EDUCAUSE Center for Applied Research, October 2006
Perceived Barriers To IT Security

- Individual Privacy
- Technology Issues
  - Lack of policy enforcement
  - Absence of Policies
- Sophistication of Threats
- Lack of Awareness
- Culture of Openness & Autonomy
- Lack of Resources

Executives can determine resources based on risks, if they know them.

“Safeguarding the Tower: IT Security in Higher Education”
EDUCAUSE Center for Applied Research, October 2006
Additional Benefits

- Opportunity to establish appropriate expectations
- Constructive executive involvement should a security incident occur
Obstacles To Effective Conversations About Security
Obstacle: Security office placed low in the organization

Is the CIO concerned?

Impressive technologist, but does he understand the real business of the institution?

# OF INFECTED COMPUTERS ARE INCREASING
Obstacle: Significant lack of awareness

So just filter them out of our in boxes!

EMAIL SCAMS POSE A SERIOUS RISK

Why is she talking about fishing?
Obstacle: Unclear terminology

IPS?
International Primatological Society?

INSTALLING AN IPS WOULD DECREASE # OF COMPROMISED SERVERS

What does “compromised server” mean?
Obstacle: Security viewed as one-time fix-it project

But we trained the workforce three years ago!

You’ve already had your turn at the well.
Obstacle: Lack of meaningful security metrics

Probably because there’s now a policy requiring incidents to be reported

10% INCREASE IN REPORTED DATA BREACHES SINCE 2005

How do we compare with others?
Obstacle: Cultural factors

But that’s less cost effective!

Did he get the buy-in of our faculty?

RESEARCH SERVERS SHOULD BE MANAGED BY SKILLED IT PROFESSIONALS
Obstacle: Executive role unclear

I’m not a techie. How could I possibly help?

So what are we paying the CIO to do?
Paths to success

Security office low in organization
- Build trust among those with access to executives
- Ask for boss’ presence in selected meetings

Significant lack of awareness
- Craft the message carefully
- Use message delivery mechanisms that reach executives

Unclear terminology
- Drop the jargon
- Learn to speak theirs
Paths to success - continued

Security viewed as on-time, fix-it project

- Set appropriate expectations

Lack of meaningful metrics

- Solidify business case with metrics that executives “get”
Paths to success – continued

**Cultural issues**
- Leverage institutional culture
- Use security incidents to initiate examination of cultural influences and possible need for change.

**Executive role unclear**
- Ask for what you need from executives
- Be specific
Be Prepared For...

- Additional Work To:
  - tailor the information
  - provide status reports, probably including development of new metrics
  - respond to inquiries

- Increased accountability
Taking the conversation and the security program to the next level
Defining the next level

- IT mainly accountable for security
- Security $$$ considered “sunk costs”
- Resources focused on reactive, band-aid tactics
- Accountability across the institution
- Viewed as investment in business of institution
- Resources focused on proactive, risk management based strategies
Paths to success

- Link security strategies to institutional needs and objectives
- Zero in on assets and processes critical to the institution
Executives care about:\n\- Meeting institutional goals
\- Efficient, uninterrupted operational processes
\- Positive public image
\- Compliance with statutes, regulations, contractual obligations
\- Managing risks

\(^1\text{Not a complete list!}\)
Paths to success – continued

- Link security strategies to institutional needs and objectives
- Zero in on assets and processes critical to the institution
- Set achievable goals and manage the risks
- Define and communicate the planned state of security
- Leverage institutional capabilities, e.g. risk management, compliance, public affairs, emergency management, audit, business process improvement, business units, etc.
- Report progress in meaningful ways
Case Study
University of Virginia
U.Va. steps it up

- University-wide “data minimization” initiative
  - Comprehensive strategic plan based upon EDUCAUSE/I2 Confidential Data Handling Blueprint
  - Goal is to significantly reduce collection, use, storage, and reporting of SSNs, credit card numbers, HIPAA data, etc.
Planned End State of Data Minimization Efforts

- Confidential data requested only when essential
- Confidential data access authorized to least # of people
- Confidential data stored only in highly secured devices and file cabinets
- Clear confidential data use policy exists
- Responsibilities for data protection well communicated
- Compliance verification processes in place
University-wide “data minimization” initiative
- Risk-driven in concept and implementation
- Supports compliance with stricter new Commonwealth of Virginia law regarding collection of personal information
- Uses phased approach to make goal achievable
- Every department involved and accountable for outcome
- Security office has leadership, management and guidance, rather than technical implementation, role. Utilizing various experts throughout institution.

New combined physical and electronic records management program
Moving security programs to the next level requires:

- A shift from emphasis on infrastructure protection to enabling the mission of the institution.
- Risk-based strategic planning
- New role of collaborator, orchestrator, communicator
- And obviously executive involvement and support
At this new level, having an ongoing conversation with the boss about security happens as a matter of course.

You speak the same language and have the same concerns and goals.
Questions
References

Developing Security Education and Awareness Programs

Gaining the President’s Support for IT Initiatives at Small Colleges
http://www.educause.edu/apps/eq/eqm04/eqm0417.asp

Governing for Enterprise Security
http://www.sei.cmu.edu/pub/documents/05.reports/pdf/05tn023.pdf

EDUCAUSE Information Security Governance Assessment Tool
http://www.educause.edu/LibraryDetailPage/666?ID=SEC0421

EDUCAUSE/I2 Confidential Data Handling Blueprint
https://wiki.internet2.edu/confluence/display/secguide/Confidential+Data+Handling+Blueprint

Information Security: A Difficult Balance
http://www.educause.edu/pub/er/erm04/erm0456.asp

Information Security Governance: A Call to Action
http://www.cyberpartnership.org/InfoSecGov4_04.pdf

Information Technology Security: Governance, Strategy, and Practice in Higher Education
http://www.educause.edu/LibraryDetailPage/666?ID=ERS0305

Presidential Leadership for Information Technology

Safeguarding the Tower: IT Security in Higher Education 2006
http://connect.educause.edu/Library/ECAR/SafeguardingtheTowerITSec/41170