Collaborating with Faculty

Last reviewed: June 2017

A common information security issue across college and university campuses is how to engage faculty in good security practices to protect sensitive institutional data. In many cases, this is an issue because faculty do not see information security as relevant to their role in higher education. This, and other misconceptions about information security in the faculty space, can be a huge hurdle to jump for information security and privacy professionals.

Below are some guidelines in FAQ format on how to work with faculty to understand and mitigate the risks to sensitive data in the realm of academia.

Where do I start in developing an information security plan for faculty?

- Establish a relationship with the provost and deans, and introduce your ideas for outreach to the faculty community.
- Ask the provost and deans about the best approach to use for this outreach, common issues regarding information security in the faculty space, and elements that could become a barrier between you and the faculty during outreach.
- Obtain buy-in from the president and senior managers, and work with those individuals to issue a message to faculty confirming the college's or university's commitment to protecting university data.

What are some outreach venues?

- Events that cater to faculty specifically such as campus-wide faculty conferences, meetings or new employee orientations
- Departmental or faculty governance meetings
- Faculty Senate (or equivalent Faculty Governance body) often have IT-related advisory committee(s). Information security advisories to faculty might be better received if sponsored or sent by these committees.
- Faculty newsletter
- Meetings or conferences specifically developed by the information security department or office for faculty

What are some messages to include in outreach communications?

The messages for your faculty will heavily depend on the feedback from your institution's provost. However, you may want to add these general points to your messages:

- Data breaches can impact colleges and universities financially; possibly resulting in the loss of donations.
- Data breaches can happen in the academic space. Faculty can reduce this risk by preventing loss of data and not waiting until a mistake occurs to learn prevention techniques.
- Protecting data is a collaborative effort between faculty and staff.
- Student information is considered confidential and needs to be protected by anyone accessing or using it for academic purposes.
- Federal laws such as HIPAA (Health Insurance Portability and Accountability Act), FERPA (Family Educational Rights and Privacy Act), GLBA (Gramm-Leach-Bliley Act), and the HITECH (Health Information Technology for Economic and Clinical Health) Acts all have requirements regarding the protection of specific categories of data.
- To date, 48 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have state breach notification laws. It is the responsibility of each college and university to adhere the laws that affect their student population.

How do I maintain access to faculty for outreach purposes?

- Establish a list of departmental representatives for each college and meet with them on a regular basis to discuss hot topics, alerts and issues of concern.
- Establish a relationship with a technical representative from each college and meet with them regularly to discuss hot topics, alerts and best practices.
- Work with department representatives in order to make information security a part of traditional business processes (i.e., purchasing, grant applications, applications for research projects). Making information security a part of the checklist in completing these processes will generate and retain relationships with this group.

Additional Resources

- Building a Culture of Digital Self Defense (2016 guest blog)
- Toward an Academic Culture of Security (2016 guest blog)

Questions or comments? Contact us.