CIO Insights on Cybersecurity

Peter Murray | University of Maryland, Baltimore
Michele Norin | University of Arizona
Melissa Woo | University of Oregon
Poll:

Does your institution promote National Cyber Security Awareness Month in October?

- Yes, we’ve promoted NCSAM since 2004.
- Yes, we recently started promoting NCSAM.
- No, this is the first time I’ve heard about it.
What’s happened in the past year?

- High profile credit card breaches (Target, Home Depot)
- Widespread vulnerabilities (Heartbleed, Shellshock)
- Phishing messages continue to increase
- Direct deposit scams
- Increased public awareness of international players
Evolution of the Cybersecurity & Threat Environment

- Millions of attempts to get unauthorized access to university systems every day
- Millions of email messages are SPAM and filtered through anti-SPAM appliances
- Largest number of breaches are from malware/spyware
- Phishing attempts are more sophisticated
- Identities and individual information and data are being stolen every day.
- Targeted attacks on HE institutions continue to grow
Poll:

Do you have a unique password for each of your online accounts?

- Yes
- No
<table>
<thead>
<tr>
<th>Rank</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Improving student outcomes through an institutional approach that strategically leverages technology</td>
</tr>
<tr>
<td>2</td>
<td>Establishing a partnership between IT and institutional leadership to develop a collective understanding of what IT can deliver</td>
</tr>
<tr>
<td>3</td>
<td>Assisting faculty with the instructional integration of information technology</td>
</tr>
<tr>
<td>4</td>
<td>Developing an IT staffing and organizational model to accommodate the changing IT environment and facilitate openness and agility</td>
</tr>
<tr>
<td>5</td>
<td>Using analytics to help drive critical institutional outcomes</td>
</tr>
<tr>
<td>6</td>
<td>Changing IT funding models to sustain core service, support innovation, and facilitate growth.</td>
</tr>
<tr>
<td>7</td>
<td>Addressing access demand and the wireless and device explosion</td>
</tr>
<tr>
<td>8</td>
<td>Sourcing technologies and services at scale to reduce costs (via cloud, greater centralization of IT, cross-institutional collaborations, and so forth)</td>
</tr>
<tr>
<td>9</td>
<td>Determining the role of online learning and developing a strategy for that role</td>
</tr>
<tr>
<td>10</td>
<td>Implementing risk management and information security practices to protect institutional IT resources/data and respond to regulatory compliance mandates (tie)</td>
</tr>
<tr>
<td>10</td>
<td>Developing an enterprise IT architecture that can respond to changing conditions and new opportunities (tie)</td>
</tr>
</tbody>
</table>
Top 5 Institutional Strategic Information Security Issues

1. Developing an effective information security strategy that responds to institutional organization and culture, and that elevates information security concerns to institutional leadership. (58.75%)

2. Ensuring that members of the institutional community (students, faculty, staff) receive information security education and training. (55.00%)

3. Developing security policies for mobile, cloud and digital resources (includes issues of data handling/protection, access control, and end user awareness). (48.75%)

4. Using risk management methodologies to identify and address information security priorities. (38.75%)

5. Developing, testing, and refining incident response capabilities to respond to information systems/data breaches. (36.25%)
Would you…

- Give out your online banking password?
- Leave your home WiFi router without a password?
- Provide your SSN to a total stranger?

…then why be less vigilant about information security & privacy on campus?
Poll:

Do you use passcodes on your mobile devices?

- All of my devices
- Most of my devices
- One or two of my devices, but not all
- None of my devices
InfoSec Issues on Our Campuses: “What keeps us up at night?”

—University of Arizona

- The impending need to restrict our network environment.
- Responding to the increased number of incidents as we discover more about compromising activities.
- There never seems to be enough resources.
- Large number of compromised email accounts.
- Getting individuals used to different practices such as two-factor authentication and registering devices.
InfoSec Issues on Our Campuses: “What keeps us up at night?”
—University of Maryland, Baltimore

- The increasing number of cyber attacks.
- The expanding number of devices that are connecting to our network.
- The staffing challenges to handle a growing amount of information security work.
- The vulnerabilities that we haven’t found yet and don’t yet know about.
InfoSec Issues on Our Campuses:
“What keeps us up at night?”
—*University of Oregon*

- Awareness/training for the campus community
- Enforceable policies to protect student data and intellectual property
- Institutional governance
Poll:

Do you review your credit card transactions for unfamiliar charges every month?

- Yes
- No
What are your information security concerns?
Key Takeaways for Individuals

- Report suspicious e-mails to your help desk, IT office, or Information Security office.
- Set strong passwords, and don’t share them with anyone. Use “two-factor” authentication, if it’s offered.
- Keep your software and devices patched and up to date.
- Be cautious about what you receive or read online - if it sounds too good to be true, it probably is.
- Maintain an open dialogue about Internet safety with your family, friends, and community.
- Consult with your Information Security office!
Key Takeaways for IT Professionals

✓ Assume that there is a vulnerability that needs to be found, assessed and addressed at your institution.
✓ Work to protect and secure sensitive data.
✓ Review data policies, data stewardship, and compliance.
✓ Make sure all devices and systems are up-to-date with patches.
✓ Discontinue using systems (e.g., Windows XP) that are no longer getting security patches.
✓ Check with cloud service providers...the security of the data in the cloud is your responsibility.
✓ Use real world analogies to educate users.
✓ Take advantage of NCSAM (October) and Data Privacy Month (January/February) to educate your campus.
✓ Join REN-ISAC; volunteer to serve on a HEISC Working Group; attend the Security Professionals Conference
Considerations for Your Institution-Wide IT Security Program

- Identify, assess, and report on any information security risk or vulnerability;
- Define common areas of risk across the institution;
- Share effective information security strategies;
- Share technology solutions and technical knowledge;
- Collaborate on the improvement and enforcement of information security policies;
- Develop a global communication strategy to promote and expand information security awareness.
What else can we do?

- Shift conversations from technology to risk assessment;
- Discuss information security at all levels of the institution;
- Continue to collaborate with partners and sectors outside of your institution and HE;
- Assess programs designed to create a pipeline for skilled security staff to ensure excellence.
Success Indicators

✓ An institution-wide approach to information security, which means active participation, resource commitment, and prioritization by all areas of the institution.

✓ Information security is not just an activity that you work on as time permits or in response to an event. It is an integral part of the institution’s culture; IT architecture and support services; & academic and business processes.
Conclusion: Information Security is Everyone’s Responsibility

There is an almost overwhelming number of things we all need to pay attention to, but that’s no excuse for failing to do all that we can, and all that we must.

Please join us in making information security a personal and institutional priority.
Resources for Individuals

✓ Stop Think Connect, www.stopthinkconnect.org/
✓ National Cyber Security Alliance, www.staysafeonline.org/ncsam/
✓ OnGuard Online, www.onguardonline.gov/
✓ FTC Consumer Information, www.consumer.ftc.gov/
Resources for IT Professionals

- Security Professionals Conference, [www.educause.edu/sec15](http://www.educause.edu/sec15)
- Security Discussion listserv, [www.educause.edu/groups/security](http://www.educause.edu/groups/security)
Thank you for joining us!

For NCSAM resources, visit www.educause.edu/ncsam