Cyber Risk – Emerging Trends and Regulatory Update

June 12, 2013
Mike Cullen, Senior Manager  
CISA, CISSP, CIPP/US

> Leads the firm’s Technology Risk Services team in Washington, DC, focused on IT risk consulting and internal auditing.

> Performs IT risk assessments and audits, developed information privacy and security programs, performed ethical hacking of IT systems, and conducted digital forensic investigations.

> Presents to a variety of audiences, including ACUA, various IIA chapters and regional conferences, and at multiple universities.
Jennifer Zanone, Manager
CISA, PMP

- Performs IT risk assessments, IT audits, system implementation reviews, and application control reviews for a variety of higher education, not for profit, and research institution IT environments of varying sizes.

- Strategically analyzes clients’ mission, systems, and risks by applying best practice standards such as Control Objectives for Information and Related Technology (COBIT).
> Overview of cyber risk and its importance
> Emerging trends in cyber security
> Changes to data privacy/security laws and regulations
> Resources
Objectives

> Provide an overview of cyber risk and describe its importance
> Describe emerging cyber security trends
> Describe new or changed data privacy/security laws or regulations
> Describe potential strategies that can be incorporated into audits
Polling Question #1

Cyber is derived from cybernetics, which was originally defined as the theory of what?

A. Brain wave patterns
B. Baseball statistics used in *Moneyball*
C. Communication and control in the animal and the machine
D. Computer warfare tactics
> The term was coined in 1948 by U.S. mathematician Norbert Wiener to mean the theory/science of communication and control in the animal and the machine. (Source: Wiktionary)

> By the 1970s, the Control Data Corporation sold the "Cyber" range of supercomputers, establishing the word cyber- as synonymous with computing. (Source: Wikipedia)
Overview of cyber risk and its importance
The responsibility that any organization who connects to or utilizes the Internet has to protect business and consumer data.
Definitions – Privacy

> The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.

Source: American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles
> The processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

Source: SANS Information Security Resources: www.sans.org/information_security.php
Are Privacy and Security Synonymous?

> Privacy is concerned with enabling individuals to have say over how their personal information is collected, used, retained, and disclosed.

> Security is concerned with protecting information from inappropriate access, modification, or destruction.

> To achieve privacy, you must have security.

> Both security and privacy are business issues.
Privacy in Higher Education

> An exceptional volume and variety of personal information (e.g., transcripts, financial aid, health centers, retail operations).

> Increased complexity and oversight challenges in a decentralized environment.

> Subject to many privacy and security laws and regulations due to:

  > Breadth and nature of business operations
  > Faculty, staff, students, and alumni from many states and countries
There are several regulations related to privacy and security with which institutions need to be familiar:

- FERPA
- GLBA
- HIPAA / HITECH
- Identity Theft Red Flags
- FISMA
- PCI DSS
- International Laws
- US Data Breach Notification Laws
  - 46 states + DC, Puerto Rico and others
Polling Question #2

How does your institution manage cyber risk today?

A. It is IT’s problem
B. We don’t manage it all
C. In some areas we attempt to manage it, in others we do not
D. We have a comprehensive, multi-faceted approach
Emerging trends in cyber security
What is it?

- The growing challenge of securing data and information systems through collaboration with third parties providing services to the organization
Cloud Security

What are the issues?

> Is Cloud security different than other Information Security?

> How can you be sure that data is secure in the Cloud?

> Who is responsible for what during a security breach?

> The Big Question: Is the Cloud more or less secure?
How can you audit/provide value?

> Conduct a Risk Assessment before moving a service to the cloud

> Review Vendor’s Independent Certifications (e.g., SSAE 16, PCI)

> Ensure there are strong internal Data Security policies and procedures

> Thought: What is the “right” amount of due diligence to perform for a cloud provider?
Hacktivism

What is it?

> Hacking + Activism:

The use of computers and computer networks as a means of protest to promote political ends (Wikipedia).
Hacktivism

What are the issues?

> Universities are both targets of “hacktivism” AND ideal incubators for those wishing to participate in these movements.
Hacktivism

How can you audit/provide value?

> Ensure traditional information security controls are maintained and up to date with emergent threats

> Ensure there is an incident response team trained and prepared to engage with law enforcement officials in the event of student, faculty, or staff involvement in criminal hactivism
What is it?

> 56% of American adults now own a smartphone of some kind; Android and iPhone owners account for half of the cell phone user population (Source: Pew Research Center)

> By the end of 2013, the number of mobile-connected devices will exceed the number of people on earth, and by 2017 there will be nearly 1.4 mobile devices per capita (Source: Cisco)
Mobile Devices

What are the issues?

> People

> Devices

> Applications

> Data

> Thought: Portability is the biggest risk and biggest benefit, does one outweigh the other?
How can you audit/provide value?

> Bring Your Own Device (BYOD) is becoming standard

> Help develop a comprehensive mobile device policy including:

  > Full device lifecycle support program

  > Data protections based on data classifications

  > Desktop virtualization

  > User awareness of their personal risks & responsibilities
Polling Question #3

Which of the following emerging trends do you think is most likely to impact your institution?

A. Cloud Security
B. Hacktivism
C. Mobile Devices
Changes to data privacy/security laws and regulations
Health Information Technology for Economic and Clinical Health Act


> Subtitle D addresses privacy and security concerns related to the electronic transmission of health information, including extending HIPAA Privacy and Security Provisions to business associates of covered entities.

> The HITECH Act also imposes new protected health information breach notification requirements on HIPAA covered entities, business associates, vendors of personal health records, and related entities.
HIPAA and HITECH Act

HIPAA Data Breach Notification Requirements

> Covered entities must provide individuals notice in written form by first class mail or email if the individual has agreed to receive such notices electronically

> Notifications must be provided no later than 60 days following the discovery of the breach

> If the entities have out of date contact information for 10 or more individuals, the entity must post notice on the homepage of its website or provide the notice in major print or broadcast media
HIPAA Data Breach Notification Requirements (continued)

> If the breach affects more than 500 residents of a state, the entity is required to provide notice to prominent media outlets serving the state or jurisdiction

> Entities must notify the State Secretary of all data breaches annually for breaches affecting less than 500 residents, or within 60 days for breaches greater than 500 residents
All states, plus Washington, D.C., have security breach notification laws of some form, except Alabama, Kentucky, New Mexico, and South Dakota.

Minnesota, Nevada, and Washington have all passed laws that codify some or all aspects of PCI DSS.

Generally these laws apply to all entities that have data about the respective state’s residents, regardless if the entity does business in that state.

Current trend is addition of medical information.
FISMA

> Federal Information Security Management Act, became law as part of the E-Government Act of 2002

> Requires federal agencies to strengthen information security programs and report on an annual basis

> Goal is to protect federal information (the data in both electronic and paper forms) and information systems (the computers and networks)

> Government contractors and grantees organizations may have to comply if they:
  – collect or maintain information on behalf of the agency
  – that use or operate information systems on behalf of the agency
  – have FISMA requirements in contract and grant terms and conditions
Federal Information Security Management Act, became law as part of the E-Government Act of 2002

Requires federal agencies to strengthen information security programs and report on an annual basis

Goal is to protect federal information (the data in both electronic and paper forms) and information systems (the computers and networks)

Government contractors and grantees organizations may have to comply if they:
- collect or maintain information on behalf of the agency
- that use or operate information systems on behalf of the agency
- have FISMA requirements in contract and grant terms and conditions
Polling Question #4

What law or regulatory change concerns you the most?

A. HIPAA / HITECH
B. Data Protection and Breach Notification Laws
C. FISMA
SIDEBAR ON SERVICE ORGANIZATION CONTROLS (SOC) REPORTING
## SOC Reports

<table>
<thead>
<tr>
<th></th>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Reports on the controls of the service organization that are relevant to the user organization’s financial reporting</td>
<td>Reports on the effectiveness of the controls of the service organization related to compliance or operations, including trust services principles and criteria*</td>
<td>Same purpose as SOC 2</td>
</tr>
</tbody>
</table>

*Trust services principles and criteria are security, availability, processing integrity, confidentiality, and/or privacy. The security, availability, and processing integrity criteria are related to the controls system and the confidentiality and privacy criteria are related to the information processed by the system.*
## SOC Reports

<table>
<thead>
<tr>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Info required</strong></td>
<td>Details on the system, controls, and tests performed by the service auditor, and results of those tests</td>
<td>Details on the system, controls, and tests performed by the service auditor, and results of those tests</td>
</tr>
<tr>
<td><strong>Audience</strong></td>
<td>User organization’s controllers, compliance officers, CFO, CIO, and financial statement auditors</td>
<td>User organization’s controllers, compliance officers, CFO, CIO, vendor management executives, regulators, other specified parties, and appropriate business partners</td>
</tr>
</tbody>
</table>
Resources
Resources

> AICPA – www.aicpa.org

> SANS – www.sans.org

> Ponemon Institute – www.ponemon.org

> NCSL – www.ncsl.org

> NACUBO – www.nacubo.org

> NACUA – www.nacua.org

> Higher Ed Compliance Alliance – www.higheredcompliance.org
Resources

> EDUCAUSE – www.educause.edu

> URMIA – www.urmia.org

> Privacy Rights Clearinghouse – www.privacyrights.org

> Identity Theft Resource Center – www.idtheftcenter.org
Upcoming Webinars

Webinars resume August 2013

Enjoy your summer!
September 22-26, 2013
Norfolk Waterside Marriott
Norfolk, Virginia

Register at: [www.acua.org](http://www.acua.org)
ACUA

> Promoting Internal Audit: www.acua.org/movie
> Listserv: acua-l@associationlists.com
> Forums: www.acua.org

Baker Tilly

> www.bakertilly.com/acua
Thank you for participating today! Remember CPE certificates will be emailed to you by ACUA Headquarters in about three weeks.

**Mike Cullen**

mike.cullen@bakertilly.com  
703-923-8339

**Jennifer Zanone**

Jennifer.zanone@bakertilly.com  
312-729-8193
The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Pursuant to the rules of professional conduct set forth in Circular 230, as promulgated by the United States Department of the Treasury, nothing contained in this communication was intended or written to be used by any taxpayer for the purpose of avoiding penalties that may be imposed on the taxpayer by the Internal Revenue Service, and it cannot be used by any taxpayer for such purpose. No one, without our express prior written permission, may use or refer to any tax advice in this communication in promoting, marketing, or recommending a partnership or other entity, investment plan or arrangement to any other party.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International. © 2012 Baker Tilly Virchow Krause, LLP.