Cyber Security in Higher Education
Esteemed Panel … Cyber Security in Higher Education

Tom DeChiaro
Vice President, CIO
Drexel University

Ken Makoid
Regional Vice President Northeast Sales
Flexential

Frank Yako
CIO, Director of Strategic Initiatives
ASMGi

MOMERATOR

Steve Roesing
CEO
ASMGi
Cyber Landscape in Higher Education
Discussion Topic #1 – Strategy
Discussion Topic #2 – Assessments
Discussion Topic #3 – Solutions
Discussion Topic #4 – Data Center
Conclusion + Key Points
Questions + Closing Remarks
Cyber in Higher Education is Challenging because …

Vulnerabilities and unique challenges in higher education

Data variety: Any business must protect employees, customers and internal data. This is true for higher education as well, but institutions also house, feed and protect people. They administer financial aid, accept donations, conduct research involving people and animals and create inventions and intellectual property (IP). This results in a breadth of data types rarely seen in other kinds of organizations.

Decentralization: In corporate environments, a select few manage the majority of data. Higher education operates in a largely decentralized manner. Many people with different skill sets and needs collect, process and store the data, which heightens the challenge of protecting data.

Varied rules and regulations: The wide scope of work being carried out in educational institutions is subject to many different standards, regulations and legal requirements that make it difficult to follow a single regulatory framework.

Higher education sits at a nexus. These institutions deal with innumerable compliance requirements across disciplines. While the Family Educational Rights and Privacy Act (FERPA) is an obvious exception, most cyber and privacy laws are not designed to address higher education institutions specifically. Educational institutions are nevertheless impacted. For example, the Health Information Portability and Accountability Act (HIPAA) was designed for hospitals and healthcare providers, but any campus health center or research institute may also be subject to its privacy and security requirements. Similarly, the Gramm–Leach–Bliley (GLBA) Act was meant to regulate financial institutions, but on-campus departments collecting financial information or taking payments are legally bound to restrictions related to financial privacy and safeguards.

Funding: Most organizations struggle to secure large allocations for preventative measures like cybersecurity management. For higher education, the challenge is severely magnified. In many cases, funds are influenced by lawmakers, trustees and donors. Sometimes, regulations hinder what can be done.

Educational institutions also face more difficult decisions related to funding allocations than private sector entities. It is not a simple matter of diverting funds from a marketing campaign or even shareholder dividends. For a university, funding choices often come down to decisions about specific investments in the health and wellbeing of students. Choosing between expenditures like capital improvements or scholarships and cybersecurity initiatives will never be an easy decision to make.
Cyber in Higher Education is Challenging because …

Cyber threats to higher education
A United States Department of Homeland Security assessment on cybersecurity risks in academia does not mince words: "We have high confidence in our primary judgment that U.S. university and college networks face a persistent threat as targets of opportunity for unwitting hosting of malicious cyber activity and cybercrime."

In the face of considerable cyber risk, institutions need to consider four main threat actors:

- **Nation states** – These are countries and nation-state actors looking for IP or intelligence, from cancer research to defense information such as research on missile guidance defense systems. Their primary interests are research data and personally identifiable information (PII).

- **Criminal syndicates** – These actors are going after data they can monetize – credit cards social security numbers and other PII.

- **Hacktivists** – Hacktivists are not typically driven by a monetary goal. They seek to embarrass institutions or otherwise reveal information to defame institutions.

- **Insiders** – Every institution deals with people who are employed or have a relationship with the institution. Colleges and universities are no different. Disgruntled employees or otherwise misled internal actors are always a threat for fraud, unauthorized information disclosure or other breaches.
Cyber in Higher Education is Challenging because …

Threat vectors in higher education

Educational institutions face many of the same vulnerabilities as other organizations, but they are often intensified. Following are a few of the most common threat vectors:

Phishing: The average institution must contend with phishing attacks on hundreds or thousands of employees. A successful phishing attack might hit just one percent of them. Universities have tens of thousands of students, faculty, staff and alumni. More potential victims exist due to the sheer numbers and the dispersal of data throughout an institution. Phishing also presents an additional threat for universities given their historical openness for the dissemination of knowledge. For example, names, titles and contact information for university personnel are often included in publicly available online directories and organizational charts. Imagine then, how easy it would be for an attacker to contact an accounting clerk pretending to be the clerk’s supervisor that is requesting an urgent wire transfer.

Software vulnerabilities: All software has vulnerabilities. That’s why patches are constantly being issued by vendors. Universities face a special challenge due to the sheer volume of systems and vendors that they have work with and support. They’ll never have one software vendor for all of the software they require. Student information systems, web applications and payment systems are just a few of the software systems that bad actors seek to exploit.

Access control: Educational institutions typically have a large number of people with access to different systems. Different departments, contracts and mandates all have different cybersecurity requirements. Institutions need to plan for a variety of specific requirements around access, password control, multi-factor authentication and remote access.

Viruses, malware, ransomware: These are any attack designed to cause harm to a system or steal data. Typically, these are delivered through phishing, but not always. A bad actor could gain access to one system and then use it to send malware to many other people.

The internet of things: Any cyber-to-physical connected device falls into this category, including, for example: watches and fitness trackers, door-lock security systems, security cameras, HVAC, electrical, lights and other connected infrastructure. Systems like these don’t typically have the same cyber controls built into their software as an institution’s other technology systems. In other words, leaders don’t always realize these systems can be exploited or used as attack vectors.
#1 STRATEGY

Does your Cyber Strategy align with your University’s Strategic Plan?
How do you prioritize your initiatives?

Cyber Expertise prioritized Top 20

CIS Controls™

Basic
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

V7
How do you prioritize your initiatives?

The 3 most frequently affected controls from our analysis are:

CIS 14—Controlled Access Based on the Need to Know: This covers all the cases when the network was not properly segmented based on application and data sensitivity, e.g. cases when retailer’s Point Of Sale (POS) devices were on the same network as regular employee endpoints. It also includes cases when shared folders were not properly protected with access controls and unauthorized people had access to sensitive data such as IP, PII, PHI, PFI, etc. Finally, scenarios such as unencrypted hard drives lost during transport by 3rd parties, stolen unencrypted laptops, and disk drives.

CIS 13—Data Protection: This control covers all scenarios related to data stolen from undocumented or misplaced storage locations (laptops, network drives, 3rd party cloud providers, etc.), data backups, legacy databases, and applications. Additionally, it includes cases when raw data in the clear text were exfiltrated without detection.

CIS 17—Implement a Security Awareness and Training Program: Covers all cases of phishing and more general cases when the attacker requested an employee to make some action such as making a wire transfer, sending a tax form or other sensitive information. Any unintentional disclosure of sensitive data to the attacker is included as well.

Figure 1: Shows the total number of times a CIS control could have prevented a cyber breach.
How do you prioritize your initiatives?

- **Gain Continuous Visibility** into Your Security Posture
- **Prioritize** Your Resources and Responses
- **Remediate** Your Security Gaps
How do you prioritize your initiatives?

Quantifying Cyber Risk

- Leverage what you have
- Bring security closer to the business
- Create a common language to discuss cyber risks
- Prioritization = Align budgets with initiatives that provide actual economic impact
The Benefits of Quantification

**Internal:**
- Enhances CISO and CFO / CEO dialogue and understanding
- Financial measurement of balance sheet impact
- Financial accuracy and substantiation of cyber budget requirements and application
- Assimilation of cyber risk into enterprise risk management (ERM)
- Acceptance of CISO role as a strategic function

**External:**
- Enables CEO to present tangible assessment of cyber risk to stakeholders
- Enhances financing prospects
- Strengthening of company’s position with External constituents (e.g. regulators, etc.)
- M&A and other growth strategy advantages
- Enables superior risk solutions (insurance; capital markets; security tech channel sales)

At the Center is CISO, CFO & CEO Synchronicity
#2

ASSESSMENTS

How many assessments do you do to meet your Compliance and Privacy requirements?
Compliance

PCI-DSS
HIPAA
FERPA
GLBA
FISMA

Frameworks

NIST
ISO/IEC 27001, 2
CIS
# Common Controls Framework (CCF)

## Mappings to the CIS Critical Security Controls

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inventory of Assets and Asset Control</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Security Policy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Security and Access Control</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Protection of Hardware, Software and Data</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>Risk Assessment and Information System Landscape</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>Awareness and Training</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>Incident Response</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>8</td>
<td>Business Continuity Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9</td>
<td>Compliance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>10</td>
<td>Data Recovery Capability</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>11</td>
<td>Security Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>12</td>
<td>Security Continuous Monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>13</td>
<td>Security Controls Evaluation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>14</td>
<td>Security Control Implementation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>15</td>
<td>Security Control Monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>16</td>
<td>Security Control Assessment</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>17</td>
<td>Security Control Authorization</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>18</td>
<td>Security Control Configuration</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>19</td>
<td>Security Control Operation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>20</td>
<td>Security Control Evaluation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

9/25/2019
#3 SOLUTIONS

What problems are you trying to solve?
A Holistic Approach to Cyber Security

Total Solution = 3 Pillars

Program + Technology + Operations
Lots to choose from …

The Fog of More
# How do you prioritize your initiatives?

## Cyber Expertise prioritized Top 20

### Basic
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

### Foundational
7. Email and Web-Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

### Organizational
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises
How do you prioritize your initiatives?

The 3 most frequently affected controls from our analysis are:

**CIS 14—Controlled Access Based on the Need to Know:** This covers all the cases when the network was not properly segmented based on application and data sensitivity, e.g. cases when retailer’s Point Of Sale (POS) devices were on the same network as regular employee endpoints. It also includes cases when shared folders were not properly protected with access controls and unauthorized people had access to sensitive data such as IP, PII, PHI, PFI, etc. Finally, scenarios such as unencrypted hard drives lost during transport by 3rd parties, stolen unencrypted laptops, and disk drives.

**CIS 13—Data Protection:** This control covers all scenarios related to data stolen from undocumented or misplaced storage locations (laptops, network drives, 3rd party cloud providers, etc.), data backups, legacy databases, and applications. Additionally, it includes cases when raw data in the clear text were exfiltrated without detection.

**CIS 17—Implement a Security Awareness and Training Program:** Covers all cases of fishing and more general cases when the attacker requested an employee to make some action such as making a wire transfer, sending a tax form or other sensitive information. Any unintentional disclosure of sensitive data to the attacker is included as well.
Do you outsource your data center? How does your data center impact your Security?
How many of your data centers look like this?
**Fully compliant solutions**

Our compliance expertise runs deep with over 50 compliance-focused engineers.

- ITIL® V3 Certified
- AICPA Certified Public Accountants Trust Services Principles for security, and availability
- SOC 1 dual-standard report
- Level 1 PCI DSS service provider for colocation and cloud
- ISO 27001 Certified
- Information Security Management System standard
- HIPAA Health Insurance Portability and Accountability Act Security Rule
- HITRUST CSF Certified
- HITRUST CSF service provider for colocation and cloud
- SOC 3 Trust Services Report

---

American Institute of Certified Public Accountants Trust Services Principles for security, and availability

Health Insurance Portability and Accountability Act Security Rule

HITRUST CSF Certified

FLEXENTIAL
Colocation capability highlights

Nationwide presence and offerings for all customer types

Unique Density Footprint
- Density up to 50kw per cabinet in newer facilities

Flexible Service Options
- Inventory and terms to meet customer growth

Pricing Models To Match Customer Needs
- Fixed and variable billing options

Support points:
- 40 Datacenters
- Wholesale and Retail Colocation capability
- 100% Power SLA
- Team of Experts Available for Design, Implementation and Maintenance Needs
Flexential capabilities

We help organizations optimize their IT transformation journey while simultaneously balancing cost, scalability and security.

- 21 Domestic markets
- 40 Data centers
- 4,000 Customers
- 170 MW critical load UPS capacity
- 1,000 Employees
- 100Gb Network backbone
- 3.1M SqFt Data center footprint
- 31+ Industries
Conclusion + Key Points

- Don’t recreate the wheel
- Map controls to complete one assessment that meets all requirements
- Quantify Risks to establish priority
- Orchestration + Automation will help meet growing demands
- Leverage Cyber Insurance
- Outsource to trusted partner when capacity or expertise is lacking
- There is strength in numbers! Let’s work together to help you ALL succeed!
QUESTIONS?
Upcoming Webinars and Events

Events

- **September 25th 4PM - Cyber Security Issues in Higher Education**
  panel discussion at the Union League of Philadelphia

- **October 21-25 - Information Security Summit**
  at The Cleveland I-X Center

Webinars

- **September 18 - Setting the Trap: Crafty Ways The Bad Guys Use Pretexting To Own Your Network**
  presented by KnowBe4

- **October 3 - Securing Your Endpoints – Why Are Businesses Getting Hit With So Much Malware?**
  presented by ASMGi and Malwarebytes

- **October 10 - Where Will You Compute Securely?**
  presented by ASMGi and Flexential

- **October 17 - Do You Know Where Your Data Is And Who Is Accessing?**
  presented by ASMGi and Heureka