Agenda

• Use of third party vendors
• Need to assess risk
• Assessment methodologies
• Challenges
• PITT’s process (past, now, future)
• Recommendations
• Questions
Use of third party vendors

Support scientific work on cyberinfrastructure

Examples:

- Globus
- Fisher Scientific
- Qualtrics
- AWS/Google/Azure
- Electronic Lab Notebooks
- Bill & Ted’s Excellent Web Developers
Need to assess risk

- **Everyone has breaches**
- Will the vendor protect your information?
- Does your vendor have sufficient security to detect if/when they have a breach?
- Can you trust your vendor to notify you if/when they have a breach involving your information?
Goals of security assessment

• Be affordable

• Ensure all vendors are regularly assessed

• Provide reliable results that support risk-based decisions
Assessment Methodologies

• Vendor self-assessment (SIG, HECVAT, NIST RMF, OCTAVE)

• Security ratings (BitSight/SecurityScorecard)

• Security Audit/Certification (SOC2, ISO, NIST 800-53/171, COBIT, FedRAMP)

• Vulnerability assessments

• Questionnaires
Pitt’s process - Past

- Questionnaire based off ISO 27001 controls (loosely)
- Word Document
- All vendors got the same questionnaire

<table>
<thead>
<tr>
<th>Application and Information Access Control - Sensitive System Isolation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Describe your network configuration.</td>
<td></td>
</tr>
<tr>
<td>b) Are systems and networks that host, process and or transfer sensitive information 'protected' (isolated or separated) from other systems and or networks?</td>
<td></td>
</tr>
<tr>
<td>c) Are internal and external networks separated by firewalls with access policies and rules?</td>
<td></td>
</tr>
<tr>
<td>c) Is there a standard approach for protecting network devices to prevent unauthorized access/ network related attacks and data-theft?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encryption</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Describe how encryption is used to protect data at rest and data in transit. (Include protocols, algorithms and bit strengths).</td>
<td></td>
</tr>
<tr>
<td>b) Describe how your private keys are protected and who has access to them.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability Assessment and Remediation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a) How often do you perform periodic vulnerability scans on your information technology systems, networks and supporting security systems?</td>
<td></td>
</tr>
<tr>
<td>b) Has any in-house written application undergone a source code security review?</td>
<td></td>
</tr>
<tr>
<td>c) Are those scans performed internally or by an independent third-party?</td>
<td></td>
</tr>
<tr>
<td>d) What is the security patch management criteria used to prioritize vulnerability remediation?</td>
<td></td>
</tr>
<tr>
<td>e) What is the frequency for routine patch deployment?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Monitoring</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Are connections to your network monitored and reviewed to confirm only authorized access and appropriate usage? (This includes internal and external connections)</td>
<td></td>
</tr>
<tr>
<td>b) How long are those logs retained?</td>
<td></td>
</tr>
</tbody>
</table>
Pitt’s process – Past (continued)

Not risk based – low risk engagements were treated the same as high risk

Process not formalized, publicized or enforced

No recurring assessments

No formal scoring
Pitt’s process - Current

- Questionnaire - Based on NIST 800-171
- Online (Qualtrics)
- Risk based – low risk vs high risk
- Different assessment based on risk
- More formal scoring
- Onboarding process more formalized
University of Pittsburgh

Please check any types of information that the vendor will have access to as part of the product or services that they will be providing.

- Financial Donor information
- Student information (Demographic identifiers and/or FERPA data)
- Financial Aid information
- Healthcare
- Human Resources
- Public information
- Research (list type of research)
- Personally identifiable information (PII)
Q16. Is access to storage media (ex. USB flash drives, CDROM's, External Disk Drives, Laptops, Desktops, and Server Disk Drives) controlled such that only authorized individuals have access to it through its lifecycle?

Yes
No

Q17. Indicate where data is encrypted at rest (check all that apply):

Server
Desktops
Laptops
Portable Storage (i.e. USB, CDROM, External Hard Drives, etc)
Smart Phones & Tablets
Other
Check the following items which are included in the access management policy and procedures.

- Process to grant access based on job duties
- **Process to, at a minimum, review access annually**
- Process to review or terminate access when an employee is terminated or changes positions
- Process to grant access to and monitor shared and system accounts
- Process to grant access to and monitor third party accounts
- Process to change default system or application account credentials prior to implementation
- Process to assign, review, and monitor administrative access to operating systems
- Process to limit access to source code to authorized individuals
- Other (Describe):
Pitt’s process - Future

• Formal University Procurement Policy
• Better data management
• Continuous vs point in time assessments
• Automated scoring

“Weak but continuous assessment processes are more reliable than rigorous assessments conducted once” - Gartner
Recommendations

• Develop ‘some’ process
• Decide what you want to accomplish
• Risk based – level of effort to assess and remediate risk should be commensurate with the threat to your institution
Questions???
Thank You