ISE Northeast Executive Forum and Awards

Nominee Showcase Presentation

October 7, 2010

Company Name:	American University, Georgetown University, & The George Washington University
Project Name:	Collaborative Cyber Security Response Project
Presenter:	David Smith, Georgetown University
Presenter's Title:	Chief Information Security Officer

T.E.N.
TECH EXEC NETWORKS

Company Overview

T.E.N. TECH EXEC NETWORKS

AMERICAN UNIVERSITY
WASHINGTON, DC

Georgetown UNIVERSITY

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

- Higher Education Private Institutions
- 50,903 employees (collectively)
- $1,470,982,000 (non profit)
- Global presence
- AU - #1 on Princeton Review most politically active students
- GT – Founded in 1789, same year the U.S. Constitution took effect
- GW - largest land owners in DC

Presentation/Project Overview

Cyber Security Addendum Components

I. Scope
II. Activation through Lessons Learned
III. Appropriate Use
    a) Legal
    b) Compliance
    c) Exceptions
IV. Communication
V. Departmental Specifics
VI. Implementation Procedures
VII. Training
VIII. Maintenance and Review

Overview of Business Challenge

Our three academic institutions - signed a Memorandum of Understanding for emergency preparedness and response, cutting across all service sectors.

As the lead cyber security specialists, we felt it was important to address the opportunities to share resources in the event of a large scale cyber security event.

Project Scope/Goals

- Defined the types of events that might exhaust institutional resources
- Shared our service catalogs
- Discussed trusted communication protocols
- Selected an implementation methodology
- Defined thresholds and activation levels
- Hammered out rules of engagement
- Crafted an approach for reporting and developing lessons learned
- Reviewed training responsibilities
- Defined the maintenance and review time frames for our agreement

Project Results

- A Cyber Security MOU outlining the requirements for the successful partnering of the three universities in the event of a cyber security incident.
- Due to the dynamic nature of Cyber Security incidents, it wasn't possible to include an exhaustive list of possible attacks; instead, the universities agreed to make staff available in the case of any large-scale attack or incident where additional expertise is required.
- The decision to deploy staff to a partner institute will be at the discretion of the appropriate CISO/CSO and his/her chain of command.

Lessons Learned/Best Practices

Our experience exemplifies the importance of information sharing through partnerships and collaboration

- Consider your services and realize that you can't define every incident
- Identify your local partners – know their faces, understand their problems (they are likely the same as yours), build trust relationships
- Share ideas and solutions
- Look for opportunities to improve together and individually
- Think about strategic service partnerships that can form as you continue to work together

Thank you and Questions