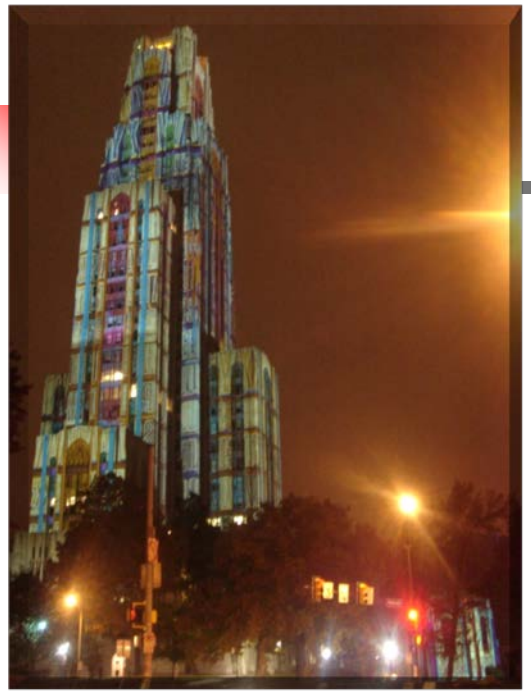
University of Pittsburgh Cybersecurity Center (*CyRes*)

A proposal (work-in-progress)



Individual initiating the proposal:
Ron Larsen,
Dean, School of Information Sciences

A proposal for CyRes

*This proposal aims to establish a cyber security research center at the University of Pittsburgh whose goal will be to foster **highly integrated, holistic and interdisciplinary undertakings** that push the boundaries of cyber security research and development.*

*It will leverage and build upon the **synergies** that exist among various units within Pitt.*

*The center will focus on **both basic research and contributions to solving real-world** cyber security, privacy, trust and resiliency related challenges.*

Pitt has the potential to establish one of the best, truly multidisciplinary and holistic cyber security research and education agenda

Urgent need for Cybersecurity Research & Development

- Many factors for growing cybersecurity problems:
  - Increasing Interconnectivity
  - Rapid IT Evolution
  - Increasing Threats and Sophistication of Attacks
  - Human Factors and Usability
  - Information Explosion, its Ubiquitous Flow and Aggregation
  - ….
- Some indicators of “growth”
  - Market to grow from $75 billion in 2015 to $170 billion by 2020 (Forbes)
  - Cybersecurity shortage is expected to rise to 6 million globally by 2019
  - Increased Gov investment in cybersecurity

LERSAIS - background

- Established in 2003/04
- NSA/DHS designated CAE since 2004
  - 5 CNSS IA certifications (one of about 15 institutions)
  - Re-designated in 2014 (till 2021)
    - National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD)
- NSA/DHS designated CAE-Research since 2008
  - first group of 21 in US
  - Re-designated in 2014 - valid till 2021
- IA Scholarships (NSF CyberCorp)
  - In the Second round of funding (total of ~$2.5M)
  - Applied for the 3rd round
- Lab fundings: Cisco, DoD/NSA, Internal

Pitt Cybersecurity in Context

- Pitt Cybersecurity:

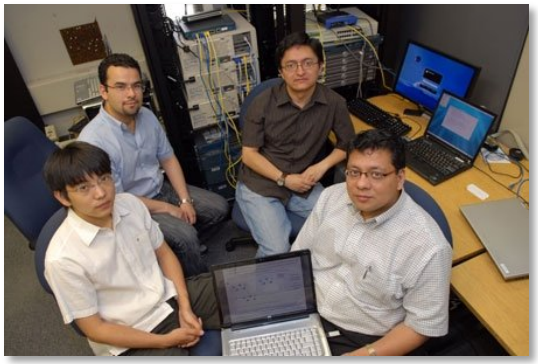
  Primary Security & Privacy Faculty:

  - **CS and SIS**: Adam Lee, James Joshi, Balaji Palanisamy, David Thaw (Law & SIS) primary faculty

  Others with varying levels cybersecurity research efforts:

  - David Tipper, Prashant Krishnamurthy, Eric Hatleback, Vladimir Zadorozhny, Michael Spring, Taieb Znati (CS), Daniel Mosse (CS), Alex Jones (ECE), Bambang Parmanto, Leming Zhou (HIM), ….

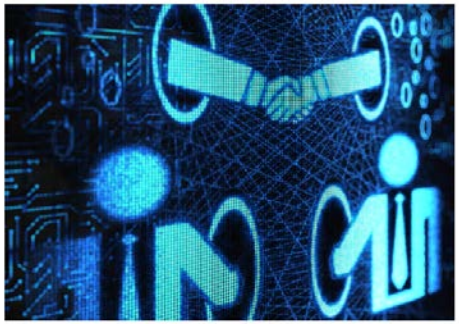
- Peers
  - Cylab at CMU has more than 50 faculty from 6 schools and departments
  - GTISC at Georgia Tech lists 36 faculty
  - CERIAS has more than 81 faculty from 6 schools and 20 departments



Pitt's Visibility in Cybersecurity

2014 Best Schools for Cybersecurity
Study of Educational Institutions in the United States
February 2014

Ponemon INSTITUTE



2014 Best Schools for Cybersecurity©

Sponsored by HP Enterprise Security
Independently conducted by Ponemon Institute LLC
Publication Date: February 2014

Ponemon Institute Research Report

professionals is outpacing the supply in both the
r Defense Secretary Robert Gates, the Pentagon is
lities (defensive and offensive cybersecurity war
ss it."[1]

Top rated schools at a glance:

University of Texas, San Antonio
Norwich University
Mississippi State University
Syracuse University
Carnegie Mellon University
Purdue University
University of Southern California
University of Pittsburgh
George Mason University
West Chester University of Pennsylvania
U.S. Military Academy, West Point
University of Washington

- Top 6 highly recommended by *ObserveIT* (http://www.observeit.com/blog/7-universities-recommend-security)
  - CMU, GMU, JHU, MIT, Stanford, Pitt (6th)
- *ExecutiveBiz* top ten (2009) Pitt (6th)
- http://blog.executivebiz.com/2009/09/top-10-universities-preparing-future-cyber-security-professionals/

CyRes Vision

- **Vision**: *The Center* will be a global leader for *inter-disciplinary* research related to security, privacy, trust, and resilience in cyberspace. *It will be among the best cyber security research centers* in the world and will be founded on the principles of:
  - *Integration and cross fertilization* of scientific, engineering, technological, policy, legal, business, sociological and human perspectives (*multidisciplinary, holistic*)
  - *Service to local, regional and global communities* by research outreach and research-driven training, awareness and education
  - *Collaboration and partnership with synergistic entities* in academia (within and outside Pitt), both public-private sectors, and global partners.
  - *Agile and efficient environment* that seamlessly supports bold and high-risk research explorations.

Strategic Goals

To realize the above vision, we set the following strategic goals, for the initial five to seven years:

- The center will develop a critical mass of core researchers that will represent both breadth and depth in various research areas related to cyber security, privacy, trust and resilience;
  - **Identify high priority areas**
- The center will provide foundational support to affiliated faculty to explore and establish closer collaborations with other research institutions/centers (academia, industry and government institutions) locally as well as globally to enable innovation and exploration in relevant research;
- The center will establish a seamless, holistic infrastructure to enable affiliated researchers and groups to serve local, regional, and global communities in cyber security and cyber defense/operations with regards to state-of the art research, training and education. Such a holistic infrastructure will include.
  - Research and education out-rearch infrastructure

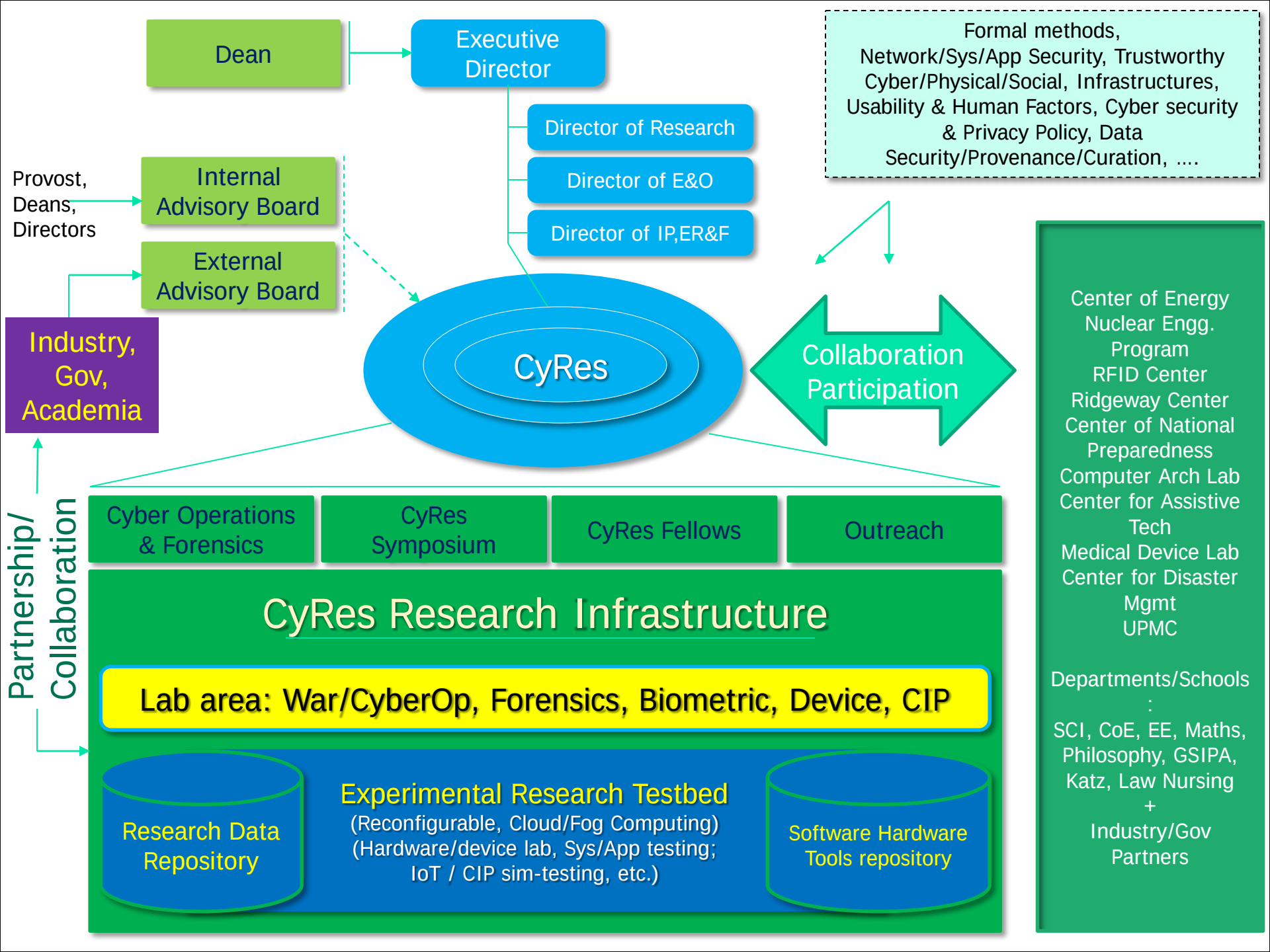
Potential Expanded Collaborations

School of Information Sciences	**James Joshi, Professor**
	Prashant Krishnamurthy, Associate Professor
	Balaji Palanisamy, Assistant Professor
	Konstantinos Pelechrinis, Assistant Professor
	Michael Spring, Associate Professor
	David Tipper, Associate Professor
	Vladimir Zadorozhny, Associate Professor
	Eric Hatleback, Research Associate Professor
School of Arts and Sciences: Department of Computer Science	**Adam Lee, Associate Professor**
	Rami Melham, Professor
	Daniel Mosse, Professor
	Taieb Znati, Professor
	Youtaou Zhang, Associate Professor
Department of Mathematics; Department of Philosophy	Kiumars Kaveh, Assistant Professor ---
School of Health and Rehabilitation Sciences: Department of Health Information Management	Bambang Parmanto, Professor
	Leming Zhao, Assistant Professor
School of Law	David Thaw (Secondary appointment with SIS)
School of Engineering: Nuclear Engg Program	Daniel Cole, Associate Professor
Department of Electrical Engineering	Alex Jones, Associate Professor
	Yiran Chen, Associate Professor
(Some centers for potential collaborations)	Gregory Reed, Professor
Potential centers or other units that will be affiliated: Center for Energy, Ridgeway Center, Center of National Preparedness, Center for Medical Innovation, John A. Jurenko Computer Architecture Laboratory, Center of Assistive Technologies, Medical Device Lab/Prototype Lab, RFID Center of Excellence, DBMI, UPMC	
Graduate School of Public and International Affairs	Louise Comfort, Professor
	Phil Williams, Professor
	Lisa Nelson, Associate Professor
Katz School of Business	Michael Donohoe, Clinical Associate Professor
School of Nursing	Rose Constantino, Associate Professor
SEI/CERT	**Sidney Faber, Adjunct Professor at SIS**
	Jonathan Spring, Adjunct Professor at SIS

Some potential high impact interdisciplinary Research

- BigData/IoT Security and Privacy
- Security, Privacy & resiliency of Healthcare IT Environments
- Security, Privacy & resiliency of Critical Infrastructures

- Cyber Intelligence Analytics & Digital Cyber Forensics Research, and Cyber Security & Privacy Laws/Regulations
- Privacy Engineering, Data Curation, Archiving & Provenance, & Societal Aspects of Cybersecurity
- Usability and Human Factors in Cybersecurity
  - Science of Cybersecurity, Quantum Cryptography, Hardware/Device Security, Biomentric
  - Etc.
- Collaboration enabled by **Pittsburgh Cybersecurity Center of Excellence** (Feb, 2015 Workshop) efforts
  - Applied Research: Cyber Intelligence, Cyberforensics, real-time mitigation; malware analysis


Dean
Executive Director
Director of Research
Director of E&O
Director of IP,ER&F
Formal methods, Network/Sys/App Security, Trustworthy Cyber/Physical/Social, Infrastructures, Usability & Human Factors, Cyber security & Privacy Policy, Data Security/Provenance/Curation, ...
Provost, Deans, Directors
Internal Advisory Board
External Advisory Board
Industry, Gov, Academia
CyRes
Collaboration Participation
Center of Energy Nuclear Engg. Program
RFID Center
Ridgeway Center
Center of National Preparedness
Computer Arch Lab
Center for Assistive Tech
Medical Device Lab
Center for Disaster Mgmt
UPMC
Departments/Schools :
SCI, CoE, EE, Maths, Philosophy, GSIPA, Katz, Law Nursing
+
Industry/Gov Partners
Partnership/ Collaboration
Cyber Operations & Forensics
CyRes Symposium
CyRes Fellows
Outreach
CyRes Research Infrastructure
Lab area: War/CyberOp, Forensics, Biometric, Device, CIP
Research Data Repository
Experimental Research Testbed
(Reconfigurable, Cloud/Fog Computing)
(Hardware/device lab, Sys/App testing; IoT / CIP sim-testing, etc.)
Software Hardware Tools repository

Leadership, Oversight, Administration and Staff implications

- External Advisory Board
  - Guidance, vision
  - Include: industry partners and other centers
- Center reports to Dean of SCI
  - Budget; hiring and personnel adjustments; strategic decisions
  - Review of operational decisions
- Internal Advisory Board
  - Provost's Office and Deans/Chairs of affiliated units
    - Help in leadership and development of new initiatives

Organization Structure

- Center Director (Executive Director)
  - Overall responsibility of the center
- Directors/Leads on
  - D-Research
    - Overall research strategy; research coordination
  - D-Education and outreach
    - Educational partnerships – within and outside Pitt
  - D-Industry Partnerships, External Relations and Finances
    - Corporate & gov partnership and support
    - Support grant writing related activities
- Staff support
  - Assist in coordination and ED
  - Website and communications

Assessments: Accomplishments and Impacts

- Research
  - New research (collaborative and/or bold); new funding
  - Sustained funding
    - Conference/publications/Faculty recognitions/PhD theses
- Education & Outreach
  - Internal and external assessments
  - Recognitions/awards; visibility
  - New offerings (online, Cyber Ops, ..)
  - Community and high school outreach
- Collaboration / Impact
  - New Ind/Gov partnerships
  - Community engagements
  - Fellowship program

Budgetary Considerations

Area	Total ($M)
Center Start-up Costs (support for staff, faculty, etc.)	$5.00
Small Grants Funding (seed funding over 3 years)	$3.00
CyRes Fellows (Senior/Visiting fellows, Post-doc fellows)	$5.00
Seminar/Research Educational Funds (Semianrs, Annual CyRes symposium, etc.)	$1.00
Faculty Hiring (8 – 12 Core Faculty (60%))	$2.40
CyRes PhD Fellowships (first five years)	$3.00
Research Facility (experimental, data/tools repository, CyberOps/Forensics facility)	$2.00
Grand Total	$21.40

Budget summary

Table 1. Projected Distribution of Funding between University (UNI) and the External (EXT) Funding sources													
All Numbers in $ Millions	Area Total	Year 1		Year 2		Year 3		Year 4		Year 5		Total/Area/Source	
Area		UNI	EXT	UNI	EXT	UNI	EXT	UNI	EXT	UNI	EXT	UNI	EXT
Center Start-up Costs	$5.00	$1.00	$0	$1.00	$0.10	$0.75	$0.30	$0.50	$0.50	$0.25	$0.60	$3.50	$1.50
Small Grants Funding	$3.00	$0.30	$0	$0.90	$0.00	$0.90	$0.00	$0.90	$0.00	$0.00	$0.00	$3.00	$0.00
CyRes Fellows	$5.00	$1.00	$0	$0.50	$0.25	$0.50	$0.73	$0.50	$0.25	$0.25	$1.00	$2.75	$2.23
Seminar/Research Educational Funds	$1.00	$0.20	$0	$0.15	$0.05	$0.20	$0.00	$0.10	$0.10	$0.10	$0.10	$0.75	$0.25
Faculty Hiring	$2.40	$0.60	$0	$0.60	$0.00	$0.72	$0.00	$0.24	$0.00	$0.24	$0.00	$2.40	$0.00
CyRes PhD Fellowships	$3.00	$0.60	$0	$0.54	$0.06	$0.45	$0.15	$0.30	$0.30	$0.21	$0.39	$2.10	$0.90
Research Facility	$2.00	$0.40	$0	$0.40	$0.20	$0.40	$0.20	$0.00	$0.20	$0.00	$0.20	$1.20	$0.80
Total/Year/Source		**$4.10**	**$0**	**$4.09**	**$0.66**	**$3.92**	**$1.38**	**$2.54**	**$1.35**	**$1.05**	**$2.29**		
Total by Year		**$4.10**		**$4.75**		**$5.30**		**$3.89**		**$3.34**			
Total University Cost												**$15.70**	
Total Externally Funded													**$5.68**
Grand Total (All Sources)													**$21.40**

The EXT total shown is minimum needed to achieve the center's projected level of five-year budget, given the University's support. However, our aim is to strive for more EXT funding so as to replace the UNI portions, wherever possible

Budget Summary

Table 2. Estimated Center Related Revenue Generation over five years	In Millions					
	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Research Grants	$1.00	$1.30	$2.00	$2.30	$4.00	$10.60
Industry Collaboration	$0.00	$0.30	$0.40	$0.40	$0.50	$1.60
Tuition from Degree Programs	$0.50	$0.60	$0.80	$1.20	$1.40	$4.50
Training and Consulting	$0.00	$0.20	$0.40	$0.50	$0.50	$1.60
Total	$1.50	$2.40	$3.60	$4.40	$6.40	
Grand Total						**$18.30**

Cybersecurity: BS, CAS, FastTrack BS-MS, MS, PhD +Training/Consulting

Professional **IST style program**

Ongoing regional effort led by Pitt since Feb, 2015: Pittsburgh Cybersecurity Center of Excellence

Shows the projected revenue that the Center will generate over the first five years because of the Center's resources and the affiliated faculty pool, with their curricular contributions and grants/funding related to cybersecurity education and research.

Proposed Implementation Plan (initial thoughts)

- Year 1:
  - Center basic infrastructure setup
    - Establish administrative setup (Directors, staff)
    - Center by-laws and detailing of the strategic plans
    - Membership
  - Seed funding activities (every year henceforth)
  - Explore partnerships/collaborations within and outside (to continue each year)
  - Kick off CyRes Symposium
  - Initiate CyRes Research Infrastructure design and planning
  - Planning for recruitment of Faculty, CyRes PhD Fellowship, CyRes Fellowship program
- Year 2:
  - CyRes Research Infrastructure Development starts (or earlier than year 2)
  - First Cohort of CyRes fellows
  - Start faculty hiring
  - Finalize administrative infrastructure
- Year 3 & 5 onwards
  - Continue Faculty hiring (until all lines filled)
  - Seed funding
  - Symposium & Fellowships continued
  - Revisit priorities (sub-areas, strategic goals)
  - Preliminary Review in year 3 on all aspects of the center for improvements
- Year 5 onwards
  - In additional to annual activities, do assessment/evaluation of the center

Current status

- Two Meetings and feedbacks
  - Be ambitious !!
- New School issues complicate decision
  - Probably think of one year funding
    - Postdocs
    - Some infrastructure
    - Some faculty support
- Question: within the context of SCI?

SCI Context

- Cybersecurity Research as a national/global priority
- Cybersecurity as ENABLER for other subdisciplines,

METATHEME

- Cybersecurity for Pitt's PROMINENCE in SCI in the shortest timeframe,
  - its high impact on community/nation/society, and excellence in integrative, research-driven education
- Maybe one of the Best Recruiting Tool for the founding SCI Dean – *if committed* !!

Funding for Information Assurance Education

- NSF Curriculum Development Grants of over $1M
  - IS Masters Program
  - Tele Masters Program
  - Post-bac and Post masters Certificate of Advanced Studies (CAS)
  - Online CAS started in Spring, 2015
  - Security Assured Health Information Management Program (with SHRS)
- NSF CyberCorp (SFS) funding of ~$2.5M
  - Since 2006 (also DoD IASP occasionally)

Pitt Online

LERSAIS - background

- More Recent activities
  - HP-sponsored survey ranks Pitt cybersecurity program 7th in the nation
  - Re-designation of LERSAIS as CAE & CAE-Research
  - Funding to create a “Security Assured Health Informatics” curriculum (with HIM)
  - Funding from NSA related to Insider Threats in Critical Infrastructure and Cloud Computing
  - Collaboration with SEI/CERT on the Science of Cybersecurity (joint funding from Pitt and SEI to support a research asspciate professor)
- Distinguished LERSAIS IA seminar every Fall and Spring semesters since 2004
- NSF/NSA/Cisco, DoD grants on Information Security & Privacy (SIS, CS and other affiliated faculty)
  - Two CAREER Awards, MURI, etc.

First Key Feedback from Mark Redfern and Donald Shields

- The proposal should be revised to be more ambitious and avoid "evolutionary"
  - What will put us at the top? We can worry about funding later…
  - My reading: (Reach out to potential external funding/investment)
- Provide some background on the cybersecurity incidents to make case for the need (also for longer term) – make business sense
- The effort has to be independent of CyLab presence (my reading)
  - UPMC goes to CyLab – maybe they will come to us on their own afterwards!
- Are there departments to include, if possible:
  - Need to include: Psychology, DBMI, Statistics, Maths, etc.
- This is research center – how the education fits?
  - The center provides guidance and core faculty support for the educational programs ..
- Some suggestions regarding administration model
  - (e.g., like in Center of Energy --- executive director is not necessarily a faculty)

Potential Expanded Collaborations

- All departments within SCI
- Dietrich School of Arts and Sciences
  - Depts: Mathematics, Philosophy, Psychology, etc.
- School of Law
- School of Health and Rehabilitation Sciences
  - Depts: Health Information Management
- Swanson School of Engineering
  - Departments: Electrical Engineering, Nuclear Engineering (Energy Center)
- Graduate School of Public and International Affairs
- School of Nursing
  - ...

- External Partners: UPMC, NCFTA, FBI, CMU CyLab, SEI/CERT etc
- And others from **Pittsburgh Cybersecurity Center of Excellence** efforts

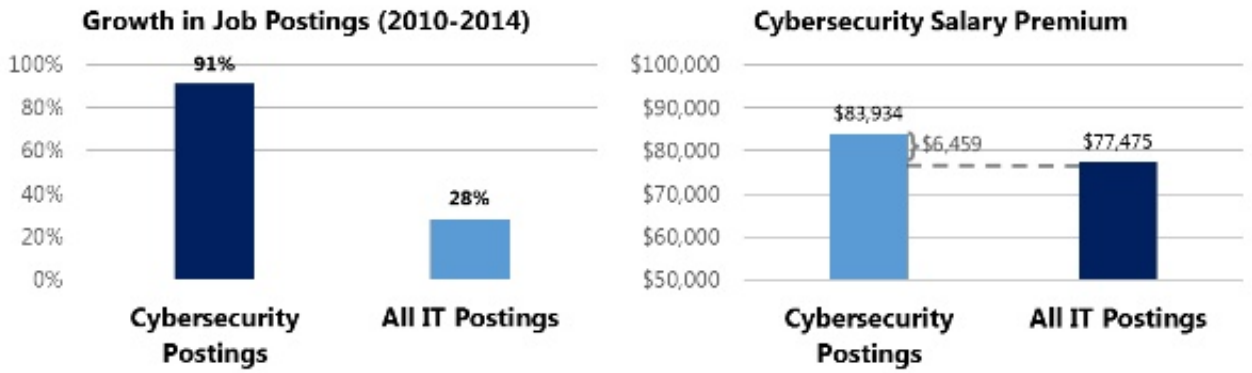
Potential other centers/units – affiliated or collaborations

- Center for Energy
- Nuclear Engg. Program
- Center of National Preparedness
- John A. Jurenko Computer Architecture Laboratory
- DBMI
- UPMC
- Center of Assistive Technologies
- Medical Device Lab/Prototype Lab
- RFID Center of Excellence
  - Etc.

Cybersecurity jobs/market

- Job market Intelligence: Cybersecurity Jobs, 2015
  (Source: http://www.slideshare.net/ghanchin/cybersecurity-jobs-report2015)

- In 2014, 238,158 cybersecurity related job postings (about 11% of IT jobs)
- About 9% salary premium over IT jobs overall
- 8% longer to fill than IT job postings overall



*According to the International Information System Security Certification Consortium, Inc., (ISC)²® membership counts as of July 14, 2015

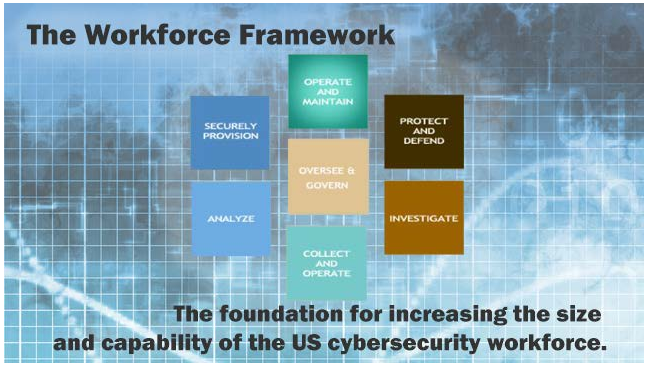
Cybersecurity jobs (Forbes, Jan 2016)

- Cybersecurity market expected to grow from $75 billion in 2015 to $170 billion by 2020.
- More than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years, according to a 2015 analysis of numbers from the Bureau of Labor Statistics
  - by Peninsula Press (March, 2016), Stanford University Journalism Program project
- A Cisco 2014 report : global shortage is 1 million
  - Demand is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million, (Michael Brown, CEO at Symantec)
- "Top Cyber Security Salaries In U.S. Metros Hit $380,000"
  - According to the IT job board DICE, the top IT security salaries go to lead software security engineers who earn an average of $233,333.

(Forbes, Jan 2016)

Summary of: why Information Security at Pitt/SIS

- Demand for Cybersecurity jobs is growing;
  - high paying jobs; global need
- LERSAIS is CAE, and CNSS certifications
  - Rigorous program acknowledged by US National Security Agency and Department of Homeland security
- Established SFS Program
- Among the top cybersecurity/InfoSec programs



Budgetary and infrastructure considerations

- Initial Research Funds ($5-10M over 5 years)
  - Seed funding for collaborative research
  - New, high-risk high-impact areas
    - 10-12 grants for 3 cycles (after 1 or 1.5 years each)
    - 1-3 will be for visionary, bold ideas (e.g., that prepares for NSF Expedition in Computing type proposals)
- Fellows Program & workshops/Seminar
  - Annual workshops to showcase and share
  - Fellows program similar to Pitt Center of History and Philosophy of Science
    - 5-10 Fellows per year: @ ~$150K/year
- Infrastructure Funds

Budgetary and infrastructure considerations

- Infrastructure Funds
  - LERSAIS Seminars (type): ($10K/year)
  - Computational Testbed to support center related educational and research activities
    - $100K (maybe through an infrastructure grant)
    - Encourage NSF proposal
    - Example: DETER testbed at UC Berkeley
  - Enhancing Educational opportunities in Cybersecurity
    - New subtracks
    - Employ 2 GSA for 2 years (~100K/year)
  - Misc ($10K/year for 5 years)
    - Annual workshop to showcase and share
    - Travel to important meetings and for exploring partnerships/funding
  - Faculty hiring
    - 3-5 new faculty over 2-5 years
    - Add to the Depth and Breadth of research
  - Physical space

Key Cyber security & privacy Research topics	Examples
Foundational theories/techniques research	e.g., formal models and methods, composability and verification, secure & trusted interoperation, cryptography and number theory, quantum cryptography, etc.;
Systems and hardware oriented research	e.g., secure processors, secure OSs, static/dynamic analysis techniques; secure software engineering or software security; secure medical devices/RFIDs
Secure and resilient Network focused research	e.g., wireless networks; secure SDN, DDoS mitigation, secure SDN,
Trustworthy cyberinfrastructure focused research	e.g., wireless networks; secure middleware; secure mobile infrastructure, security of Internet of Things/Everything infrastructure, etc.
Application focused and applied research	e.g., those related to healthcare/bioinformatics applications, database applications security and privacy, social network applications, mobile app security, etc.
Data centric security, privacy and trust research	e.g., that relates to big data security, secure data mining, secure knowledge management, anonymization techniques, data provenances and digital curation, etc.
Security, Privacy and Resilience of Cyber physical systems & Cyber social/human systems	e.g., related to critical infrastructure protection – SmartGrid security, Nuclear Cybersecurity, Transportation infrastructure security; internet of medical devices, vehicular cybersecurity, secure and resilient Smart Cities/Planets; Cyber bullying, Hactivisim, Secure and resilient disaster management, etc;
Cyber Intelligence Analytics, Cyber Operations and Forensics	e.g., intelligence data gathering/fusion and analytics for real-time detection (data driven approaches: DDoS, Honeypots, etc.), digital forensics research, CyberOp methodologies and simulation environments (war room), etc.
Trustworthy Computing Paradigms	e.g., relevant to Cloud computing, fog computing, quantum computing, high performance computing, etc;
Human Factors and Usability research in Security and Privacy	e.g., User-centric Privacy policy design/engineering; Usable Interfaces, Phishing and spam control/mitigation, Social engineering attacks, Insider behavioral modeling etc.,
Threat Modeling, Risk Management and Security Metrics	e.g., modeling of insider and outsider threats, supply chain security, quantitative techniques, risk assessments and security metrics/measurement, social engineering threats, understanding and managing advanced persistent threats;
Cyber Security and Privacy Policy, Regulations, Legal and Ethical issues	e.g., Security and privacy laws/regulations (e.g., HIPAA, etc.), Compliance tools/techniques, Multi-jurisdictional cyber crime investigation, Cyber border, etc.
Science of Cyber security	e.g., reproducible experimentation, basic laws for cybersecurity, etc.

Plan

- Education Plan (initial)
  - Maybe next 2-3 weeks to share with Edu Cmt
  - Action item: to explore interest from depts/programs
- Research Center plan
  - 1-2 weeks – to revise based on feedback
  - Meeting to solicit broader participation
    - To revise and refine
  - Workshop to further discuss after feedback from Mark/Don