
WILLIAM DONALD BADERTSCHER

6011 Pimlico Road
Baltimore, MD 21209

(410) 358-1327
wcouch@comcast.net

VICE PRESIDENT FOR PHYSICAL & INFORMATION SYSTEMS SECURITY University Safety ▪ Private Sector ▪ Public Sector

Expert in Enterprise Project Management (PMP Certified) and Security & Emergency Management (CPP Certified) with extensive enterprise-level planning experience at Johns Hopkins University. 10+ years of progressive experience in all facets of physical security, information technology and emergency response management. Well prepared to lead Disaster Recovery and Business Continuity planning efforts, applying cutting-edge best practices in physical security assessment, audits and emergency response planning. Develop advanced Crisis Management Plans and Integrated Physical Security Plans for higher education users. Draw heavily on authoritative materials published by Federal Emergency Management Agency (FEMA), Department of Homeland Security (DHS), Government Accountability Office (GAO) and General Services Administration (GSA).

- Risk Management and Emergency Preparedness
- IT and Physical Security Convergence
- Law Enforcement and Government Liaison
- Contract and Guard Force Management
- Results- and Standards-Oriented Planning
- Security Policy and Procedure Development
- Technology Evaluation and Implementation
- Database Development and Administration
- System Design, Installation and Maintenance
- Budgetary Compliance and Strategic Planning

PROFESSIONAL EXPERIENCE

Georgetown University – University Information Services (UIS), Washington, DC

2006 – Present

UIS operates an extensive network/computer systems infrastructure, the foundation for a wide array of applications and services that supports the university's many missions.

Senior Engineer for Safety & Facility Control Systems

Direct physical and IT security programs for the university's teaching, research and administrative facilities including systems for building access, alarm, environmental management and emergency communications. Lead strategic planning for security programs. Technical authority for assessing new techniques/security arena advanced to development of solutions for critical or unyielding problems. Evaluate impact of new security legislation and regulations on programs, mission and strategic plans.

- Implementing the Department of Public Safety (DPS) Communications Command Center Systems Upgrade project – provides a strong foundation for future growth and development in DPS.
- Developing plans to replace a critical alarm management system (Toye) – involves major restructuring of alarm management practices within DPS and Facilities Management.
- Collaborating with Auxiliary Services to examine ID-badge production and access control to better meet enterprise business needs – requires strong leadership to successfully migrate alarm monitoring functions from Auxiliary Services to DPS.
- Monitoring the development of strategic security plans and technology use for the McDonough School of Business and School of Foreign Service in Qatar.

Johns Hopkins University – Bloomberg School of Public Health (JHSPH), Baltimore, MD

1998 – 2006

Leading international authority on public health. http://www.jhsph.edu/school_at_a_glance/index.html

Security Administrator

Senior staff member overseeing security and emergency response management for JHSPH enterprise-wide human, physical and intellectual property assets. Ensured physical security of multiple university facilities including access control, identity management, alarms and communication. Served as subject matter expert for physical security, emergency planning and critical event response. Managed executive protection and event security, internal/external and confidential investigations, background checks, security badges, training and relationships with law enforcement and security professionals. Administered \$3M annual budget and professional development of 30-indirect reports.

- Developed, implemented and managed the school's entire security program. Created Security Operations Manual, widely regarded and used as model across the Johns Hopkins enterprise. Instituted standards-based policy and procedures. Implemented JHSPH security website (Intranet accessible only).
- Provided cost-effective protection of JHSPH assets by applying cutting-edge best practices in physical security

inspections, audits, emergency response and business continuity planning. Conducted benchmarking projects for gap analysis purposes.

- Effectively managed IT and physical security convergence issues. Negotiated service level agreement (SLAs) and other enterprise contracts for products and staff resources.
- Evaluated and recommended products that would be beneficial to the security program, decisions impacting multimillion-dollar operating and capital budgets.
- Motivated JHSPH leadership to adopt recommended security strategies and invest in security technology. Consulted with C- and VP-level leadership on significant incident response and highly confidential matters.
- Authored JHSPH Security Operations and Crisis Response manuals. Drafted numerous policies for Johns Hopkins Health, Safety and Environment Department: <http://www.hopkinsmedicine.org/hse/Policies.htm>.
- Designed security systems for 5M+ sq. ft. of new building construction projects and major renovations of existing research, teaching and office space.
- Coordinated with local and federal law enforcement agencies to direct responses to major security incidents that included numerous “white powder” incidents, bomb threats and suspicious packages post 9-11.
- Led multiple high-level security investigations. One notable case involved a several-month investigation and subsequent termination of 50-unionized Hopkins employees for fraud.

EDUCATION & PROFESSIONAL TRAINING

B.S. in Information Systems (2005) and M.S. in Information Systems (targeted 2008)
Johns Hopkins University, Baltimore, MD

Certified Protection Professional (CPP), American Society of Industrial Security (ASIS), 2003
Project Management Professional (PMP), Project Management Institute (PMI), 2006

American Management Association. 320+ hours advanced training in Strategic Leadership, Project Management, Finance, Information Technology, Physical Security and Communications (1998-present)

AFFILIATIONS

Security Law, Trafford Publications, Inc. Editorial Board Member <http://www.traffordpub.com>
American Society of Industrial Security (ASIS) <http://www.asisonline.org>
International Association for Healthcare Safety and Security (IAHSS) <http://www.iahss.org>
Project Management Institute (PMI) <http://www.pmi.org>
National Fire Protection Association (NFPA) <http://www.nfpa.org>
Educause <http://www.educause.edu/>
IEEE Computer Society (IEEE) <http://www.computer.org>
Computer Security Institute (CSI) <http://www.gocsi.com>
BICSI Telecommunications Association (BICSI) <http://www.bicsi.org>

TECHNOLOGY EXPERTISE

Hardware: Advanced understanding of hardware components/peripherals including desktop PCs and servers (motherboard, power supply, memory, storage), input devices (keyboard, mouse, joystick), output devices printer, monitor, speakers, headsets).

Software: Advanced understanding of numerous proprietary and open-sourced applications including expert user of all Microsoft Office applications (Word, Excel, Access, PowerPoint, Visio, Outlook), Adobe applications (PhotoShop), Autodesk products (AutoCAD).

Networks: Advanced understanding of networking (LANs, WANs, Wireless, Internet), shared resources (i.e. printers), shared data collected on central servers, email communication, information exchange via internal networks, staff access to Internet, business data access by staff via network/Internet, integrated business and network operations.

Languages: Advanced understanding of programming languages, scripting languages, job control languages/shells, GUI scripting, application specific languages, Web programming, server/client side languages, general purpose dynamic languages.