GEORGE S. ANTONIOU, PhD

16950 North Bay Road, Sunny Isles Beach, FL 33160
Telephone 716·517·5330
E-mail drgeorgeantoniou@gmail.com

EDUCATION

2010 – 2015 Nova Southeastern University Ft. Lauderdale, Florida
PhD in Information Security

Dissertation topic - Designing an effective information security policy for exceptional situations in an organization: An experimental study.

2003 – 2005 Nova Southeastern University Ft. Lauderdale, Florida
M.S in Information Security

1987 – 1988 New York State University Utica, New York
B.S. in Telecommunications

1985 – 1987 New York State University Utica, New York
B.S. in Computer Science

1983 – 1985 Frederick Polytechnic Nicosia, Cyprus
H.D. in Computer Science

COURSE INTERESTS

Computer Security Networks	Ethical Hacking	Cyber Security	Digital Forensics	IS Audit	Security Management
Privacy and Ethics	Cyber Security Policy Design	IS Governance	Risk Management	IS Project Management	Enterprise Information Security
Blockchain Security	Identity Access Management	Research & Design	Security Operation Center	IS Fundamentals	ISO 27000
Cloud Security	Database Security	OS Security	Secure Mobile Technology	Secure Telecommunications	Secure Software Development
Security Incident Analysis and Response	Health Care Security	Systems Security Engineering	Systems Security Administration	SETA - Security Education Awareness Training	Data Security Analysis - Machine Learning

RESEARCH INTERESTS

Design and implement an effective information security policy.

Blockchain Security Technologies utilizing Identity Access Management

SETA - Design an effective SETA program utilizing illustrations

Cloud Security - Data analysis utilizing machine learning

CISO - Grooming the next generation of CISO leadership

ACADEMIC EXPERIENCE

St Thomas University, Miami Gardens, Florida (*August 1, 2017 – Present)*

Assistant Professor of Cyber Security Management

St Thomas University, Miami Gardens, Florida (*January 1, 2016 – April 1, 2017)*

Adjunct Professor -- of Cyber Security Management

PROFESSIONAL EXPERIENCE

Delaware North, Buffalo, New York (*April 1, 2015 – July 1, 2017)*

Director Information Security

• Provide leadership, vision, direction, development and maintenance of information security policies and programs that impact Delaware North systems and/or business strategies.

• Establish direction for monitoring and advising management of industry and regulatory changes affecting cyber information security, working proactively to help IT and Business divisions to understand and implement appropriate changes such as PCI, ISO 27000, etc., where applicable.

• Set architecture and engineering strategy direction in the area of Cyber Information Security and PCI.

• Establish Cyber Security risk assessment programs for data security and data privacy protection to meet internal organizational needs and Client's requirements.

• Establish corporate oversight assessment for closure of Cyber Information Security technology, PCI and data privacy audit items.

• Microsoft Azure cloud services, piloting Microsoft 365 cloud components.

• Amazon hosting services, incident response programs and contract negotiation with third party vendors and clients.

Sodexo, Williamsville, New York (*October 1, 2005 – April 30, 2015)*

Global Group Director Information Security

• Advice executive officers on information security risks and serve as an expert advisor to global business unit CIO's in the development, implementation and maintenance of information security programs.

• Establish and implement the company's global information security program. Ensure the development, testing and implementation of appropriate information security plans, products and control techniques. Identify protection goals, objectives and metrics consistent with the global information technology and security strategic plan.

• Provide leadership for the information technology and security governance, and compliance of the global security policy, standards, procedures, and guidelines to prevent the unauthorized use, release, modification, or destruction of data across multiple ecosystems and environments.

• Implement Data Security awareness program providing guidance to employees.

• Manage the development and implementation of PCI Standard compliance. Follow ISO 27001 standard in regard to implementation of information security policies, standards and guidelines.

ADT Security Services, Boca Raton, FL **(***January 1, 2002 - September 30, 2005)*

Senior Information Security Manager

• Manage the administration of various encryption, authentication and public/private key management technologies and certificate/digital authority.

• Security Compliance – Manage information risk assessment, vulnerability and penetration testing, virus control, internal and external security reviews, monitoring/analysis/follow-up of security incidents, security alert communication and follow-up, security breach investigation and forensics.

• Security Awareness/Policies – Manage the development and maintenance of ADT specific information security policies and standards, regulatory requirements and compliance, using CoBIT and ISO 17799 framework standards.

• Develop an Information Security Awareness presentation module to be used for SoX training by all ADT SSO team members. Tyco adopted this presentation to be used by all segments for SoX awareness training compliance.

• Develop a comprehensive corporate information security enterprise strategy for ADT.

• Member of the Tyco Digital Security Council.

• Tyco One Antivirus Initiative – TFS Program Manager, lead global coordination effort to migrate to one common antivirus platform.

• Coordinate security assessments and risk analysis for new product and services (GuardTour, MobileSafety) for ADT strategy product department.

• Implemented Computer Incident Response Team procedure for compliance with service level agreement between ADT and Arrowsight (hosting facility for ADT security video product).

• Review information security infrastructure and controls and provide recommendations for improvements to minimize risk.

• Manage information security vendor relations.

• Develop and execute user training and awareness programs to educate users on new technologies and information security issues at the enterprise.

• Research, test, and recommend information security products.

Office Depot, Delray Beach, FL (*August 1, 1999 - January 31, 2002)*

Internet & E-Commerce Security Manager

• Manage a team of 5 people responsible for detailed security reviews to assess risk, recommend countermeasures and develop action plans to mitigate risks.

• Work closely with Change Management team to ensure compliance to corporate policies and procedures, while meeting tough client deadlines and maintaining quality work.

• Devise and deploy an infrastructure of security tools to support a strategy for routine security reviews of the corporate technology environment to ensure compliance with best practice policies and procedures and recommend migration to more secure network configuration and architecture.

Praxair, Tonawanda, NY (*March 1, 1995 - August 31 1999)*

Internet Manager

• Administer Windows NT, machines including OS and software installation and configuration.

• Test and evaluate security-related products including firewalls (Firewall-1), IDS (RealSecure), scanning tools (ISS), VPN.

• Perform security analysis of the enterprise network architecture and provide recommendations for improving security through redesigning the corporate network infrastructure.

• Design and implement a test lab for information security technology testing.

• Responsible for planning and execution of Internet and Intranet related projects, including deployment of VPNs in Europe and Asia, resulting in annual savings of over one million dollars.

• Prepare documents on VPN Architecture and Strategy, Internet Security Policy, and Internet Practices,

MetLife, New Hartford, NY (*October 1, 1988 - February 27, 1995)*

Telecommunications Manager

• Develop and implement the Telecommunications department operating procedures. Review technical specifications for the telecommunications equipment and software proposals.

• Budget, plan, design, and set-up a Voice Telecommunications network. The network consisted of Automated Attendants, Call Prompters, Call Vectoring, an Automatic Call Distribution system, a Voice Mail system, AT&T SYSTEM 75 & G3iV2 PBX switch systems, and an Interactive Voice System.

• Coordination of all primary installation and initialization system functions and all WAN connectivity (T-1s, 56Ks, CSU/DSUs). Manage the Installation of a Voice Response Unit System (AT&T Conversant) for a customer support unit. Maintenance and troubleshooting of an OS/2 Local Area Network and a voice and data communication network.

• Evaluate and recommend telecommunication methods, network components, data communication protocols, network equipment range usage and other network application system particulars.

PUBLICATIONS

• Antoniou, G. (2018, Spring-Summer). [Review of the book InSecurity, by J. Frankland]. Journal of Multidisciplinary Research, 10(1-2), 203-204.

• Antoniou, G. (2018). A framework for the governance of information security: Can it be used in an organization. Poster presented at: IEEE SoutheastCon 2018 ; 2018 Apr 19-22; St. Petersburgh, FL

PRESENTATIONS

• Antoniou, G., (2014, May). Grooming the Next Generation CISO, PowerPoint Presentation, CDM Media CISO, Miami, FL

• Antoniou, G., (2011, June). Risk Assessment, Not Just A Paradigm Shift, PowerPoint Presentation, Evanta CISO Conference, New York, NY

• Antoniou, G., (2011, February). The Critical Leadership Skills for CISOs, Interview, Evanta CISO Meeting, New York, NY

• Antoniou, G., (2008, January). Identity and Access, Panel Discussion, Microsoft CISO Summit, Redmond, WA

REVIEWS

• Barnum, C.M., Team building and single sourcing: Building a team for user-centered design, IEEE PCS, 2000

• Straub, D.W. Computer Abuse and Computer Security: Update on an Empirical Study, Security, Audit, and Control Review (4:2), 1986, pp. 21-31.

• Straub, D., & Nance, W. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study, MIS Quarterly 14(1), 45-60.

PROFESSIONAL AFFILIATIONS AND CERTIFICATES

March - 2003 - Present ISACA CISM (0300399)

January -2003 - Present ISACA Member

December - 1993 - Present ACM Member

December - 1993 - Present IEEE Senior Member

Member of AIS 2107

Member of Cloud Security Alliance

Member of Information Security Network Group

Member of Information Security Leaders Group

Member of CISM Special Interest Group

Member of Security, Risk and Compliance Professionals Group

Member of ISO27000 for Information Security Management Group

Member of Hotel Technology Next Generation (HTNG) CISO Group

MANAGEMENT EXPERIENCE

• Develop strategic vision for enterprise system security

• Analyze and recommend information security solutions

• Plan and implement enterprise security components and solutions

• Establish, implement, and enforce security policies and procedures

• Develop project plans and budgets over $1,000,000.00

• Maintain strategic vendor relationships

• Personnel management, organizational development, and professional coaching

TECHNICAL EXPERIENCE

• *Operating systems: AIX,* HP-UX, SUN Solaris, Windows, Linux, working knowledge of SAP Security.

• *System and network security:* host and network based security profiling tools, cryptography (PGP) and PKI, Firewalls, IDS, authentication mechanisms, web/mail content filter, antivirus.

• Solid knowledge of networking (routers and switches, VPN, VLAN, wireless, etc.) and security technologies (firewalls, anti-virus, intrusion detection, SSH, SSL, IPSec, PKI, DMZ, ACL, etc.)

• *Web-related application components:* Apache Web Server, IIS, NDS and Active Directory

SECURITY EXPERIENCE

• *General security skills*: proficient at methodologies for performing Internet, Intranet and Extranet security reviews; best-practices security standards; working with large heterogeneous networking and host environments to provide overall understanding of the security architecture and possible improvements to minimize the security-related risk exposures.

• *Security tools:* network-based scanning discovery, system fingerprinting, password cracking (john-the-ripper, L0phtCrack) and war dialing, secure remote connectivity (SSH).

• Knowledge and understanding of security principles, including hardened system builds, access controls, authentication methods, network separation, SMTP filtering, secure coding standards, wireless security, firewall configuration, confidentiality, integrity and availability.

• Identity and Access Management, Federation Services (ADFS, SAML 1.1/2.0), SSO.

• ITIL, ISO20000, ISO27001-2, PCI DSS.

• SEIM –logrhythm, Antivirus –Trend Micro, Bit9, Tripwire, Qualys

SECURITY MANAGEMENT

• Direct and conduct system, application security evaluations, compliance security audits, and reviews. Primary Subject Matter Expert during internal security audits, external security audits and third party partner security audits.
• Experience in information security, information security risk management, information security quality assurance compliance, and associated information security technologies in the private sector.
• Experience in strategic planning and enterprise-level security architecture, security operations, and policy development in small-medium-large, national and multi-national complex information security technology infrastructures.

• Monitor and advise management of industry and regulatory changes affecting information security, working proactively to help business to understand and implement appropriate changes such as PCI, ISO 27000, SoX, SSAE 16, HIPPA, NIST.
• Provide corporate oversight assessment for closure of Information Security technology and data privacy audit items.
• Initiate and facilitate third party security vendors to conduct risk and vulnerability assessments of planned and installed systems to identify vulnerabilities, risks, and protection needs.

PUBLICATIONS IN PROGRESS

• Antoniou, G., Carabeo, O., Hernandez, R. (2018). Blockchain Technology Point-2-Point-Encryption Device Mechanism and System Software. US Provisional Patent Application No. 62/661,69, Washington DC

• Antoniou, G., & Tejay, G., (2017). Designing an effective information security policy for exceptional situations in an organization: An experimental study. Under Development..

REFERENCES

Available Upon Request