

Michael Miora, CISSP-ISSMP, FBCI

Summary of Qualifications



- Founder InfoSec Labs, Inc., providing InfoSec, BC/DR and related services (acquired by Rainbow Technologies in 1999). **Developed web based products**, including Security Awareness For Employees (SAFE), Web Information Security Education (WISE), and consulting products.
- Designed and assessed secure systems including nation's most sensitive public and private systems. Consulted and provided seminars to NSA.
- Originator of **General Cost Consequence (GCC) Model** for streamlined Business Continuity and Disaster Recovery Planning which formed the basis for numerous software and consulting products.
- **Information Assurance, Business Continuity (BC) and Risk Management**
- Founder ContingenZ Corp, maker of **Continuity Commander**; provides consulting services to Global 2000 companies.
- Cofounder ePrivacy Group, Inc. Participated in development of **TurnTide** security and privacy appliance. Acquired by Symantec 2004.
- Adjunct Professor, Norwich University, Northfield, VT

Education & Certifications

1974 - 1976 **University of California, Berkeley**
Masters of Arts, Mathematics

1970 - 1974 **University of California, Los Angeles**
Bachelor of Arts, Mathematics

- Certified Information Systems Security Professional (CISSP)
- Information Systems Security Management Professional (ISSMP)
- Fellow of the Business Continuity Institute (FBCI)

Professional Experience

2002 - Present **ContingenZ Corporation** **Los Angeles, CA**
Founder, Chief Consultant

- Provides Security and Incident Management consulting major companies
- Managed compliance requirements including SOX, HIPAA, GLB, PCI, DPD
- Developed security and Business Continuity plans for healthcare, pharmaceutical and financial companies.
- Performed security and BC/DR audit and compliance verification assessments
- Developed ContinuityCommander BC/DR planning software.
- Conducted BC/DR walkthrough exercises, drills and tests
- Clients include American Express, Avery Dennison, Alexza, and many others

2002 – Present **Norwich University** **Northfield, VT**
Adjunct Professor, MSIA & MSBC Programs

Providing distance learning and on site lectures.

2000 - 2002 **ePrivacy Group, Inc.** **Playa del Rey, CA**
Co-Founder, Sr. Vice President and Managing Director

Providing privacy consulting, technology & training for Global 2000 companies.

Managed the consulting operations to achieve the goal of becoming a significant provider of privacy and trust products and services.

1989 - 2000 **InfoSec Labs, Inc.** **Playa del Rey, CA**
Founder, President & CEO

Specializing in Information Security Assessment and Improvement, and Security Education and Awareness. Rainbow Technologies acquired InfoSec Labs in 1999; Mr. Miora continued as Vice President of InfoSec Services.

1994 - 1997 **NCSA TruSecure Corp.** **Reston, VA**
Director, Consulting Services (Outsourced)

Managed all NCSA (ICSA/TruSecure Corp./Verizon) security-consulting services, personnel and projects including establishing requirements, preparing proposals, and performing technical consulting to U.S. and Canadian companies.

1988 - 1989 **Hughes Aircraft Co.** **El Segundo, CA**
Project Manager

Managed proposals and developed product technical concepts and designs for secure Department of Defense computer systems.

Responsible for marketing of AF Space Systems Division, including Navstar GPS, C&DP Program, ES&MC, and related projects. Managed teams of designers, artists, and other engineers in their preliminary design efforts.

1987 - 1988 **Horizons Technology, Inc.** **Torrance, CA**
Program Manager

Managed proposals and developed top-level designs for tactical and strategic systems. Developed a business plan to build annual business area revenue.

This company was a major support contractor for the Defense Nuclear Agency. Goal was to guide this company to a wider variety of federal projects and, eventually, into the commercial sector.

1984 - 1987 **Ultrasystems, Inc.** **El Segundo, CA**
Director Technology Development

Managed technical and support personnel performing security requirements definition, systems and software engineering, hardware integration, and testing and security requirements verification testing.

As Project Manager of the Milstar Independent Security Verification and Validation Project, guided prime contractors and advised government to secure the Milstar communications system against compromise, denial and spoofing attacks.

1977 - 1983 **System Development Corp.** **Santa Monica, CA**
Systems Analyst

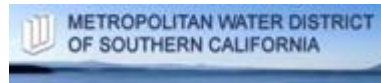
Responsibilities included requirements analysis, design reviews, and evaluation of test and integration plans and procedures. Performed systems engineering and analyses on space operations hardware and software for ground systems supporting low earth orbit (LEO) satellites requiring secure communications, processing, and control.

Systems were developed in special, closed environments and subjected to extensive security evaluations and testing. Uptime requirements were stringent, and recovery requirements were important to avoid loss of control systems and, thereby, the satellite or its data.

Publications

- Computer Security Handbook, 4th & 5th Edition (Contributor)
- Network World
- Norwich University Journal of Information Assurance
- Disaster Recovery Journal

Clients



Summary of Selected Projects

Johnson & Johnson (ASP) (2011)

- Evaluated resiliency and made specific recommendations for improving security, resiliency and recovery of mission critical functions.
- Designed and implemented test plans and procedures for testing BC/DR capabilities.
- Conducted tests of hot sites and other recovery capabilities.

Kryterion (2010)

- Evaluated security by performing logical penetration tests on in-house and outsourced data centers, including Rackspace and Microsoft Azure.
- Performed physical security evaluation and recommended specific mitigations.
- Developed security policies, procedures and practices to ensure compliance with relevant regulatory requirements as well as federal, state and local laws.
- Made specific Security Information and Event Management (SIEM) recommendations to enhance security posture.

Confidential Major Financial Client (2009)

- Evaluated security and resiliency for this major financial company serving both consumers and businesses.
- Evaluated BC/DR for compliance with federal regulations, and made specific recommendations for improving resiliency and security.
- Evaluated security information, incident and event management policies and practices.
- All software and account management are via web-based systems as this company has no conventional, brick and mortar presence

American Express (2006-2008)

- Designed, developed and implemented Computer Security Incident Response Team (CSIRT).
- Performed penetration and vulnerability assessment testing.
- All business units were included in the plan, and all technology departments and partners were part of the implementation.
- Developed security event monitoring interface for CSIRT and event monitoring processes.
- Performed various testing on the plan, including tabletop rehearsals.
- Software and account management are via web-based systems of significant size and complexity

City of Glendale, CA (2008-2009)

- Performed penetration testing on a variety of city systems, including emergency response systems, business systems, and public access systems
- Evaluated continuity and safety capabilities of the city's emergency response system
- Made specific suggestions for improving overall posture in key city systems
- Evaluated Communications Security, Connectivity with external organizations, Physical Security & Awareness, Security Policy and Management and Contingency Planning

Norwich University (2003-Present)

- Adjunct Faculty in MS Information Assurance (MSIA) program since 2003, teaching various courses in Business Continuity and Disaster Recovery, Incident Response and Information Security.
- In 2008 developed the first seminar for use in the new MS Business Continuity (MSBC) program, launched in December 2008.
- All materials are presented via web-based access and learning programs

Physicians Mutual of Omaha (2005-2006)

- Built an Incident Response Plan and formulated an Incident Response Team to handle incidents including security compromises, data loss and other disruptive events.
- Major issues included both financial regulations and HIPAA.
- Plan was implemented and handled incidents well, reducing scope of breaches significantly.
- Security Information, Incident Management and Event Monitoring implemented.

Cabelas (1998-2008)

- Performed four major information assurance evaluations and made recommendations for improvement, then returned to monitor improvements and re-evaluate.
- Points of evaluation included security and event monitoring, resiliency, continuity and privacy.
- Led effort to overhaul business continuity, privacy and security posture of online systems providing information and entertainment, and of ecommerce systems.
- Performed HIPAA evaluation for Cabelas HR and self-insurance programs.

Recall (2004-2005)

- Designed and developed a full Business Continuity and Disaster Recovery plan for major data center in Atlanta, GA.
- Performed analyses and made recommendations for evolving data center to a load balancing and near real-time failover with European data center.
- Used SLA information and penalty costs as guidelines for the project.
- All software is implemented via cloud computing.

Green Dot (2005-2006)

- Built a complete Business Continuity and Disaster Recovery plan for this financial services company.
- Identified key systems and risks impacting on those systems.
- Made specific recommendations and guided some implementation to provide failover and redundancy for technology, call centers and key personnel.
- Recommended security incident management and monitoring policies and procedures.
- Software and account management are via web-based systems

Sigue (2006-2007)

- Built a Business Continuity and Disaster Recovery plan over 16 month period for this major remitter. Plan was approved by regulators and implemented. Plan included detailed emergency procedures and step by step actions to be followed in case of an emergency.
- Services being migrated from conventional software implementations to web-based software services
- In early 2008, corporate headquarters suffered a major fire shortly after midnight. Company executed the plan and was back in operation without missing any depositor remittances/postings.

Royal Mail (2007-2007)

- Evaluated BC/DR posture for the UK Royal Mail (equivalent to USPS).
- Spent weeks gathering, validating and analyzing data.
- Provided detailed report on resiliency posture and made recommendations for improvement.

Strategic Healthcare Program (SHP) (2007-2008)

- Evaluated security and resiliency for this mid-sized medical data processor.
- Evaluated BC/DR for compliance with federal regulations, including HIPAA and general privacy.
- Made specific recommendations for improving security and resiliency posture, including IDS/IPS and security event monitoring and response procedures.

Central Bank of the Bahamas (2006-2007)

- Built a Disaster Recovery and Business Continuity plan to handle all operations of this governmental agency in case of crises and disasters, including natural disasters (e.g. hurricanes) and possible terrorism and other attacks.
- Organization had not BC/DR in place prior to this project.
- Worked with bank personnel to identify all functions, perform a BIA, train key personnel and specify required secondary processing sites.
- Built framework for emergency procedures which were to be finalized by internal personnel.

Avery (1993-2003)

Performed variety of projects during this ten year period.

- Built a full and complete disaster recovery plan for the corporate headquarters in Pasadena, CA; then converted that plan into a template and helped Avery Dennison roll out that plan template to locations across US and in Europe.
- Projects included building resiliency into internal, cloud-based software used worldwide to support corporate operations
- Developed a Security Incident and Event Management plan to handle issues ranging from system failures to attacks, and helped build a rapid prototype using Lotus Notes.
- Performed security assessments and penetration tests on newly deployed systems whose ultimate goal included ecommerce (B2B and B2C).
- Provided training on privacy regulations especially as they pertain to global companies with significant EU presence and whose main employee database is in the US. Scope of work included EU Data Privacy Directives (DPD) and US HIPAA regulations.

UST (1997-2006)

- Built DR plan for main manufacturing plant in Nashville, TN. Plan included both business continuity and disaster recovery issues for technology, manufacturing equipment and manufacturing support technology.
- Technology included SaaS services built, maintained and serviced by UST corporate headquarters.
- Updated the plan three times based on major changes to product lines and technology.
- Built corporate wide manufacturing profile highlighting areas where company evolution could mitigate risk and provide self backup of manufacturing and delivery systems.
- Evaluated corporate site in (formerly in Greenwich, CT) for security posture, including internet based and internal attack vectors.