Director, Information Security Director, Information Security Director, Information Security Shakopee, MN Work Experience Director, Information Security Bright Health Plan March 2017 to April 2019 Responsible for Information Security for Bright Health Plan. Ownership of security program to comply with PCI and HIPAA requirements. Act as primary security architect for development, analytics and IT infrastructure initiatives. Implement and maintain security oversight of vendors and partners. Design security controls to meet business and corporate requirements. Represent Bright Health in contract negotiations with vendors. Developed architecture for a secure ePHI environment. Created four year strategic plan for Information Security. Replaced outsourced help desk support company resulting in $100k savings a year. Implemented formal approval and access review processes for all applications. Directed internal HIPAA security risk assessment and led remediation of all 33 findings. Conducted security audits on over 50 partners/vendors. Director, Information Security Harken Health June 2016 to December 2016 Responsible for Information Security, Privacy and Compliance for Harken Health. Ownership of security program to comply with PCI, Hitrust and HIPAA requirements. Act as liaison between Harken Health and corporate Security department. Manage penetration and application security testing and remediation. Design security controls to meet business and corporate requirements. Represent Harken Health in contract negotiations with vendors. Created security monitoring requirements and program for Harken Health Amazon Web Services (AWS) environment. Documented PCI, Hitrust and HIPAA requirements for AWS deployment. Implemented formal approval and provisioning process for Identity and Access management. Created hardening standards for applications and operating systems deployed to AWS. Remediated 31 corporate security requirements/issues to gain approval for moving production environment to AWS. Director, Information Security RAZR August 2015 to June 2016 Responsible for Information Security, Privacy and Compliance for RAZR. Ownership of security program to comply with PCI and HIPAA requirements. Manage security audits and assessments. Respond to all Security and Compliance questions in RFPs. Create and maintain Security awareness training for all employees and contractors. Head of Incident Response team. Manage vendor relationships. Oversee security requirements for move to a cloud based hosting environment. Create and publish metrics to reflect effectiveness of the security program and compliance efforts. Managed security in SaaS environments in Google and Microsoft 365.   Created Vendor Management program.   Managed client relationships in conjunction with moving production environment to AWS.   Wrote and published over twenty security and compliance policies.   Implemented a security awareness program.   Initiated a vulnerability management, system hardening and code review programs.   Deployed data loss prevention to all computing devices.   Designed and executed a data ownership and classification program. Sr. Manager, Information Security Altegrity October 2013 to August 2015 Manager, Information Security Altegrity - Eden Prairie, MN October 2011 to October 2013 Manage a team of three security engineers that provide security shared services for 3,00 to13,000 users. Acting incident response manager for all business units. Create and manage department budget. Maintain short term tactical and three year strategic plan for information security. Manage security audits and assessments. Provide work direction and prioritization to the security team. Chair IT Security Council.   Improved end user experience by implementing single sign-on, soft tokens for remote access authentication, and password self-service.   Deployed vulnerability scanning that covers 18,000 hosts.   Achieved SOC 2 security certification for four data centers.   Arranged an enterprise licensing agreement with a vendor that saved the company $600,000 over three years.   Deployed global coverage of data loss prevention and intrusion prevention applications.   Created an incident response plan and program.   Developed metrics around SLAs, performance and workload.   Increased McAfee malware coverage from 32% to over 99% of managed computers. Lead Security Analyst Pearson VUE - Bloomington, MN October 2009 to August 2011 Lead a staff of four security analysts. Manage client relationships for security operations. Provide leadership and work prioritization to the team. Maintain strategic plan for security operations. Act as security subject matter expert for corporate projects. Manage the budget. Maintain metrics showing workload and performance of the team.   Created metrics that show work allocation at the staff and activity level.   Implemented processes that cut time spent managing requests by 40 percent.   Initiated a project to implement role based access controls.   Developed monitoring process for voucher fraud that saved the company over thirty thousand dollars in its first six months. Created metrics showing team accomplishments and performance against defined SLAs. Documented operational processes and worked with regional offices to ensure processes were standardized globally. Manager, Information Security MoneyGram International - Saint Louis Park, MN February 2007 to September 2009 Manage a staff of eight information security analysts. Act as security lead for responding to security incidents. Manage vulnerability testing and remediation efforts. Change control manager for security initiatives. Provide leadership and work prioritization to staff. Work with business units to develop requirements for new applications. Maintain strategic plan for security operations. Manage vendor relationships for security applications. Act as project manager for IT Security projects. Resource for developers to ensure that development efforts meet minimum security requirements. Performed security analysis and design of a new web based agent transaction application. Lead security infrastructure changes to meet PCI compliance. Implemented an extensive Internet Security monitoring program. Lead FRP process for choosing an adaptive authentication solution. Created process for analyzing and remediating security patches for applications and operating systems. Successfully managed a project to restore Active Directory. Implemented processes for integrating security into the application development life cycle. Manager, IT Security Policy and Operations Deluxe Corporation - Shoreview, MN December 2005 to February 2007 Manage a staff of eleven information security analysts at multiple locations. Responsible for security administration, SOX auditing, and policy maintenance. Identify security risks and prioritize efforts of risk mitigation. Partner with business units to develop security solutions to meet their needs. Monitor and report on security activities and performance. Provide risk analysis on new business initiatives. Create and maintain strategic plan for security operations. Lead incident rem. Act as a mediator and escalation point for security policy conflicts and exceptions. Created an incident response policy and procedure. Developed and implemented SOX testing and remediation plans. Implemented simplified processes for onboarding and terminating user access. Completed a security policy gap analysis and created policies to fill existing gaps. Synchronized Security initiatives to align with business initiatives. Sr. Manager, Information Security Metris

Companies - Minnetonka, MN September 2004 to December 2005 Manage a staff of six information security specialists and administrators. Responsible for security administration, enterprise security and security projects. Perform in-depth security analysis, consulting, implementation, and support of systems and applications. Research and evaluate new or improved security measures and develop plans to support the security needs of the organization. Manage the information security vendor management risk assessment process. Respond to RFPs and security audit questions. Maintain information security roadmap and strategic plan. Managed project to remove world writable files from systems. Implemented synchronization of users and groups between Active Directory and Oracle OID. Automated administration and reporting processes to increase administrator efficiency. Metris Companies September 2000 to December 2005 Manager, Information Security Metris Companies March 2003 to September 2004 Responsible for developing an enterprise wide security monitoring program. Responsible for managing authentication certificates. Manage a staff of two information security specialists. Develop and conduct a formalized plan for conducting application and operation system security assessments. Manage vendor management security program. Administer the secure file transfer system. Implemented host based intrusion detection software. Established dedicated server environment for information security. Transitioned administration of Unix security management to information security. Created security policies for Oracle 10g, Linux and Intranet systems. Developed relationships with business units to better understand and meet their security needs. Managed security aspect of project to upgrade to Active Directory. Initiated process for review of user access and server security settings. Facilitated separation of spun off company from Metris computing environment. Obtained CISSP designation Information Security Specialist Metris Companies September 2000 to March 2003 Primary contact for LAN and WAN security. Conduct due diligence reviews of current and potential business partners and vendors. Consult with business units on all new file transmissions. Perform audits of internal systems. Write corporate security policy. Develop system security standards for applications and operating systems. Provide coaching and technical support for other Information Security personnel. Maintain disaster recovery reporting. Work with business partners to audit and harden their security and business continuity infrastructure. Monitor and maintain the Intrusion Detection System. Designed a corporate security awareness program. Part of a team that selected and implemented an intrusion detection system. Lead a project to design and implement a system for centralized logging of multiple operating system security messages. Lead project that selected and implemented an Internet content filtering system. Assisted in creating a corporate Incident Response program and team. Instituted encryption policy for confidential email transmissions. Created policy and procedures for the vendor management security program. Designed NT security standards to meet OCC regulations. Information Security Analyst Lutheran Brotherhood - Minneapolis, MN August 1998 to September 2000 Primary contact for LAN administration and security. Create, maintain, and document user, group, and directory configuration and access rights. Conduct audits on LAN security to detect potential threats from internal and external sources. Conduct Security Awareness training for employees. Assist end users with system access difficulties. Consult with Help Desk, PC Support, and LAN Technicians in troubleshooting network problems. Consult with department heads regarding new system installations to insure the proper security and integrity of the data contained in the systems. Administered 200 Windows NT 4.0 servers, 7 Novell Intranetware servers. Supported 2000 Home Office users and 2000 remote users in field force. Automated weekly Disaster Recovery Reports to ensure the data is as current as possible. Lead a project to evaluate a centralized interface for user management across multiple operating systems. Provided backup support for ACF2 mainframe security. Implemented Shiva VPN system for 2500 users. Lutheran Brotherhood June 1994 to September 2000 Personal Computer Analyst Lutheran Brotherhood February 1998 to August 1998 Part of a team of four analysts that provided PC hardware, software, and network connectivity support for approximately 800 users. Consulted with department heads regarding support requirements. Provided initial training on Windows NT 4.0 for new users. Documented procedures and resolutions for trouble tickets and software installations. Competencies Intrusion Prevention, Security Event Monitoring, Cloud Security, Firewalls, Identity and Access Management, Malware Controls, Vulnerability Scanning, Project Management, Web Content Filtering, Mobile Device Management, Policies and Standards, Cost Savings, Two Factor Authentication, Incident Response, Audits and Client Relations, Metrics, Regulatory Compliance. Education Bachelor of Arts in Psychology Saint Olaf College - Northfield, MN September 1988 to June 1992 Skills SECURITY, FIREWALLS, INCIDENT RESPONSE, AUTHENTICATION, INTRUSION, MALWARE, AUDITS, METRICS, SCANNING, CLIENT RELATIONS, REGULATORY COMPLIANCE

Name: Marilyn Romero

Email: rodriguezrachel@example.net

Phone: 542.247.7564