SVP/Senior Lead Security Engineer SVP/Senior Lead Security Engineer SVP/Senior Lead Security Engineer Colonia, NJ Seeking a career in Information Security to utilize the skills developed through experience and education. Be part of a team that focuses on protecting the company's assets and preventing future implications in gaps within the IT department. Work Experience SVP/Senior Lead Security Engineer Marsh and McLennan Companies - Hoboken, NJ April 2018 to August 2019 for Security Architecture Work on all of our entities project globally and helping these entities build out projects to ensure they are secure, meet policy standards, policies, and won't put the company at risk. Developed an entire life cycle for our project teams should integrate, privacy, compliance, legal, sourcing, contracting, risk, third party prior to company to architecture and Infrastructure Engineering. Built a gap analysis we are utilizing to fill gaps. Creating a process for the flow of what project teams need to do prior to coming to architecture so privacy, compliance, legal, risk mgmt., third party risk are all found prior to our review as it is taking up extreme resource and the gaps or direction have no workflow or process/guidelines. Also the developing if we do find the ones that escape that process who and how it's documented and reported. Who needs to follow up with remediation and mitigation plans. That is all manual as of now no GRC. And being developed currently. Working with AppDev teams to real nail down secure protocols for encryption in transit, at rest, and while waiting for batch process or SFTP. Working on fixing port 80 to a reroute 443 or 8080 or other secure protocols. Checking Oracle, SQL, PostGresXL, and other applications and the security of their ports. Working on O365. Analyzed, documents, and proposed a plan for F5 load balancers and now utilizing the ASM function. Working on the process and implanting a version 8 to 13 update so we can utilize the ASM. We do not have DR's on all of them so active/passive is being implemented. After that is done with F% we will hand over to SOC with my documentation but we have to fix the configurations, syncing ability and get the business, AppDev, Engineering and SOC/NOC on track with processes I will be creating. The process will be for how long they have to monitor issues and breaks in apps, then fixing them to go from monitoring mode to detecting/blocking, as well as making sure the business know why this is important, and monitoring/logging for SOC/NOC. A process for reporting will be created as well. Working with

blockchain and docker containers something new but we utilize a lot so I am learning the containers and how to secure them with products and SDLC lifecycle. Some tools: used are Jenkins, pluralsight, f5, SharePoint, Artifactory, Workday, CA which we developed for service desk, Istio, and many other apps developed by our app teams. Tools: F5 LTM and ASM, DLP Symantec, Ironport, Zscaler, CASB, Palo Alto NGFW, LogRhythm, Oracle, SQL, Application testing, Pen Testing, Qualys, and many more systems. Enterprise Security Architect Horizon Blue Cross Blue Shield of New Jersey - Newark, NJ January 2017 to April 2018 Aveska Integration with Varonis to do recertification on all share drives as well as systems and applications. This is for both vendors and internal systems. Unstructured Data Project with Varonis going through 3,000 servers to identify sensitive data, stale data and removing global access. Fixing Access Control lists and group cleanup amongst the file servers, SharePoint, AIX, Unix, and LINUX systems. Guiding the process and procedures around ACLs (creating groups, adding users, etc.) Identifying privileged users, SID accounts, everyone access and stale accounts or data. Working on enforcing the retention policy and ensuring compliance with all data within the environment. Threat Analysis and Security Assessment for an Electronic Data interchange platform within the cloud. O365 Threat Analysis and Security Architecture review for the cloud infrastructure. Implementing security mechanisms that the platforms lacks or needs to have prior to full implementation. Fixing security holes within a main vendor's infrastructure and helping them remediate due to the risk exposure for us. eDiscovery platform and working to get it operational. Try to automate process where applicable without sacrificing integrity. Process is manual from forensic images to manual collections of data. Security architecture reviews and project reviews roughly 40 a week to make sure security requirements are integrated early and thought about throughout. Deep Dive Security architecture reviews for large, new vendor, new application, or issue existing processes. We review the diagrams to make sure proper controls are implemented. I used Jenkins, Fortify, CheckMarx had to determine the false positives from real. Looked at the source code and created the templates. Reviewed the pen tests from the vendor for dynamic scanning on external facing web apps. Reviewing projects to determine if Security Architecture is needed after all the requirements and

have been added from the previous project review. Threat modeling for different use cases, security risk assessments and the impact it could have to the business. Raise risks on systems that have gaps or are existing processes that need security controls upgraded without holding up the project. Metrics and tracker of all project and work that is currently being done by the team. Tools: Imperva, DLP Symantec, Ironport, Zscaler, CASB, Palo Alto NGFW, Splunk, Oracle, SQL, Application testing, Pen Testing, Qualys, and many more systems. Senior IT Security Risk Management Analyst Horizon Blue Cross Blue Shield of New Jersey - Newark, NJ July 2015 to January 2017 Conducting Application Risk Assessments (ARA) and Enterprise Risk Assessments (ERA) on company systems and applications following HHS guidelines. Perform Third Party Risk assessments on-sites selected at random based on sourcing segmentation levels. Worked on Exchanged, SharePoint, and file share cleanup with Varonis and running massive scripts made by a vendor in order to clean up as much as we could without affecting business. Used Encase to decrypt encrypted share as I worked on the eDiscovery team while we found s new team for 7 months. We would use Encase to decrypt and then FTK Imager to image file shares or after searching file shares, computer hard drives and email to put them on a hard drive externally for legal counsel. Worked on building, implementing, and fixing Exterro's cloud service for eDiscovery. Performing internal risk assessments on possible security issues like access control, encryption, and platform gaps (i.e. password complexity, SSO, etc.) Perform tabletop assessments on vendors we were unable to perform onsite assessments for. Improve the Third Party Risk Assessment questionnaire which is currently 117 questions and growing which includes technical, compliance, business continuity and disaster recovery, and administrative questions. Worked on Hadoop and working to secure the protocols Review every BRD and DOU for security implications and suggest changes to the document, process, or functionalities of the security framework. If further review is needed on a more technical level our security architecture team will then be involved. Metrics for the team for open risks whether internal or for third party risk. This is given weekly to Senior Management to show workload, progress, and where to focus our attention. Working on a more elaborate metrics program as well as documentation for workflows and process. Working with

ServiceNow to build out a Risk platform to better allow for proper security approvals. Review all new vendors including RFPs or any hosted platform for security risks. Document their findings in a final risk report, send the report to the business owner, and follow up on the mitigation action plan. All risk reports must be signed off and put on company letter head once accepted and agreed upon by the third party vendor. Review all business projects for security gaps such as legal, compliance, retention, security controls, etc. BRD and DOU tracker is currently done manually and created by me. Track which ones are closed, which need to be followed up on, and which ones had our involvement and required some work from us. Following up on any issues that need further clarification when reviewing BRD/DOU documents. Built out a process in an application to review all projects before they can move into testing and production. Work on the CSO Town Hall quarterly and helped implement an anonymous survey so that people could anonymously report their feedback and feel confident about it. Ultimately, Third Party Risk involves an onsite or tabletop assessment. We review their answers and request a meeting if needed. We write the high and medium risks up and send it to the vendor where ultimately they have to send a mitigation plan back with signoffs and on company letter head. I have to follow up on this plan or risk until everything is closed on the vendor's end. Started working with LockPath GRC tool, understood the different pages and elements. Helped with segmentation, combining 2013, 2014, and 2015 reports as well as reporting all prior year risks into one tracker so that we could have a repository till a GRC is brought in. Working with vendors to close gaps such as access or CyberArk usage in order to protect sensitive data. Working out regulatory and audit issues from government program's vendors who are considered FDRs. Senior IT Security and Infrastructure Analyst United Water - Paramus, NJ December 2014 to July 2015 RSA Envision Upgrade since the system of is end of life. Implemented the POC of RSA Security Analytics. This will act as our new SIEM tool for monitoring network traffic, malicious activity, and storing logs from system and network appliances. Once POC is complete, we will implement system into production with physical equipment and a DR solution. Varonis DatAdvantage and DatPrivilege were both not being used when I got here. Upgraded and rebuilt Varonis while working with the vendor to stabilize the system. Create reports

for several AD functions as well as scanning for PII information throughout file shares. Submitted remediation requests for findings on Penetration Tests that were performed by France for our Quarter 1 SSAE16 compliance. Working with CyberArk to implement Password Vault and Privilege Account suites. We will look to add this to the SIEM tool as well as start tracking and storing service accounts, privilege user accounts, and separately team access to multiple accounts. CyberArk will be rolled out in phases to Application and Database teams in order to make budget but comply with audit requirements. Reported and help track several high level executive spoofing attempts and notified the appropriate government agencies as well as our parent company in France, and executives. Helped in the New York State Audit for PII as creating deliverables for 2015 when they revisit us. Attended the Utility Cyber Security Summit with the Department of Homeland Security & FBI in March 2015. Implementation and deployment of Sophos Antivirus in replace of Symantec Endpoint Protection throughout the company. Documentation and Procedures for all Security and IT related processes. Old policies need revision or haven't been created. When documentation is created we pus hit out to the IT teams involved or share it with the business. Some other projects include: PeopleSoft Security for the upgrade, maintaining Websense, Security Dashboards for ISS monthly meetings, PII tracking making sure file shares stay clean, security monitoring, maintaining and fixing Envision while the POC is taking effect, Failed logins, IPS/IDS monitoring, Checkpoint implementation, SDLC Framework, IP Diagram for all Network systems/Appliances. Worked on O365 with SkyHigh, CASB, eDiscovery, Varonis, Archival implantation. F5 load balancers etc.\Heavily involved with Medicare, HIPAA, Hitrust, SOC, ISO 27001/27002, and NIST 800.53 v4. SOO/ Federation with Ping federate but you can do any SAML 2.0 integration. Supporting TLS 1.2 or 1.3 not 1.1 encryption. KMS storage and sending via SFTP to a folder and ensuring that folder was encrypted with vendors while the job waited to run to the database. Fixed incidents that occurred with cloud co-mingling. Senior IT Security Analyst LLOYDS Banking Group - New York, NY April 2013 to December 2014 Perform all logging and monitoring for system logins, system activity, and administrator changes that take place on a daily, weekly, and monthly schedule. Some of these logs are Malware Detected & Not Cleaned, DLP

Overrides, Systems Needing Antivirus Agents Updated, Printer Usage, Data Center Visitors, AV Weekly Summary, and RSA Authentication log. CyberArk being implemented as a Global Project using the Privilege Session manager and Enterprise Vault. Cleaning up the data in our current CyberArk environment and adding more details, using their DNA tool to extract accounts that are privileged, automation tool so new devices added to CyberArk have default groups and privileges, QRADAR for the extra reporting piece for CyberArk, Vaulting Passwords, gathering servers, routers, service account for the privilege access module, and much more being project lead for this project. Firewall reports for changes to the firewalls that need fixing or are in violation of Group Policy. Update logging, restrictions, gaining knowledge for the systems for M86, McAfee EPO Console, IBM MSS VSOC Portal, Utilized the Federal Reserve website to pull logs off of and examine. Varonis DatPrivilege Reviews for fileshares and user access to those shares. Working on getting all shares data owners who can signoff of people who want access to those shares. Running daily reports for AD events and reporting on it. Also using Varonis for mandatory leave users, Disabled AD accounts, and other reports we use for logging. Submit users for deletions if they have not logged into a system for 30 days and did not login after an email notification and timeframe which the login needed to be done by. Users have a certain amount of days to login after an email notification or they get deleted. Shares are often audited by each department; after gathering the user list in each group being evaluated the Data Owner will decide if access needs to be modified or revoked. Often other departments audit users in other department's access in systems in which we need to pull reports, submit the tickets for changes, and be available to help and answer questions needed about certain users and access roles. Also make changes on procedures if any are suggested after the audit. Worked on transferring the company from Blackberry use to BYOD policies. Also working RSA token into this picture and maintain all of the reporting for Blackberry, RSA, and Remote Access users. I send the tokens out, order new tokens, order new licenses, and help troubleshoot with users, make sure all users login every 30 days with an email notification, and report last 5 authentications to upper management. Track all SAFs for All Access, New Hires, and Leavers as they are submitted into our queue for approval. A way to spot check SAFs are getting

done properly, efficiently, and on time. Keep track of all Leavers and make sure that after someone leaves the company the procedures that needs to be done by the manager are followed and completed. These changes are in the process of being added to our leaver policy. Improving the contractor revalidation processing and getting notifications from HR when contractors are extended.

AD Group Revalidations and cleaning up domains as well as groups, service accounts, and vendor accounts that are stale and not being used. Also cleaning up user accounts and removing certain fields so AD can sync between the US and UK better. Created and provided documentation for all procedures, log monitoring, and tasks performed by the IT Risk department. Raised awareness on weaknesses based upon Group, Federal, and State Audits on some areas of where we can still improve. Usually help with Audit Remediation and gathering of the information for audit. Created Risk Reviews based on top priority issues that need to be addressed to better the IT department as a whole and have a more efficient workflow. Help prepare all Business Impact Assessments for all Bank Systems for their annual review. ARP (Access Review Process) reports for all of 2013 Quarters and 2014 Quarters of Privileged and All user access. This consists of gathering UARs and ACLs for all systems in the ARP system. Extracted UALs for all systems that use our Access Review Process, edited all source files into excel worksheets so they could be imported by Group without error. Any system not on the Access Review tool was done manually and sent to the Data Owner for review. All Revoked access had revocation tickets created and submitted for deletion to the Request team. Lastly, send Data Owner signoff and proof of the system before and after deletions for audit purposes. Also working on cleaning up this process and minimizing error for manual uploads and data gathered for the process. Once all the Access Reviews are completed we have a timeframe in which all changes have to be done. Then our UK Tactical Team sends us forms that need to be filled out of the System and the user changes that were completed. As well as before and after screenshots so they have the documentation of the changes and that they were done as specified by the line manager, data owner, or EXCO member. Approve or Reject System Access Forms and have continually strived to find a solution to helping the user request the appropriate access and find the correct roles for each system. Have worked with users on creating SAFs so they are aware of

how to submit them in the future. Check for proper roles, systems, and line manager signature. Continually set up Remote Access Tokens and send credentials to the users for their blackberry and laptop. Help troubleshoot any Remote Access and help the user logon if they have difficulty. Maintain a strict policy about logging onto Remote Access Systems on a monthly basis or access is revoked for DR process issues that may occur. Attend Change Control Meetings to be informed of changes taking place for Firewall Monitoring. Also to be aware of system changes that could affect IT and the end user. Approve Change Control Tickets so they can be implemented. Review the tickets and ask questions with concerns or wanting to understand better what change is taking place. Spot check all opened tickets and check that all deletions submitted are properly done. If they are not done completely the ticket is reopened and reason of reopening the ticket is noted. Organize priorities and constantly making sure projects are done on time. Review and analyze Audit findings as a way to keep on top of what is being done so we can comply with all regulations and audit policies. Breakdown Non Window Patches and SPNS and make sure the server team has a list of changes so rollouts to all users go smoothly. Then we report the completion of the changes and that all users have received all the new changes that were supposed to be implemented to Group so they know that the patches have been completed and updated. Updated such processes like the Electronic SAF, leaver process, ITEC DOCUMENT Compliance Checklist for new system implementation, access for systems. Also have down work on DLP Issues, ITSEC Policy, Mandatory Leave Double Check, Audit Remediation, EXCO IT Management Pack, Business Intelligence Review Issue, Federal Reserve OAL Rework, Decommissioning our Miami branch, End User Computing Reporting, NETX360 Entitlement reworks, and QUEST Tool implementation. Information Security Analyst Becton Dickinson - Franklin Lakes, NJ June 2012 to April 2013 Responsible for providing first-level support across multiple security issues as they relate to current employees and new hires. Used several Lotus Notes Databases to process requests for new hires, modify requests for access to servers or drives on any of the BD servers, Site Transfers, ID Validations, across sites in the Americas, Asia, Europe and Other Countries. Provided reliable and accurate information security advice to the team and addressed their security questions and

concerns. This included working with several users to better understand their necessary access requirements, from Vice Presidents to new hires across different departments as well as remote users. Escalated security problems when more specific subject matter expertise was required and coordinated requests with the appropriate person accordingly. Prioritized new security requests and evaluated and assessed approvals to issues such as access controls. This sometimes meant updating and improving existing info-sec policy and identifying and escalating when policies are being violated. Updated documentation for best practice security procedures with detailed notes and screenshots for any new employees to have a better guide of all our processes. Clearly defined the procedures for my department and added more descriptive- detailed notes so all processes were explained in detail and no information was missing. Worked with Global Incident Security to ensure Consultants and Vendors have contracts for Audit purposes. Terminated users from Blackberry Devices according to our Bring Your Own Device Policy. Removed users from mobile servers so no access can be given through our network. Creation of Y: Drive Directories on our Enterprise Share, creating read only and read-write AD groups for departments. Added users to AD groups once approvals from manager and Data Owner were received Managed the Remote Vendors and the Remote Vendor Database to make sure secure emails are sent between both parties and user credentials are encrypted. Used SafeNet Tokens with SSL VPN users by activating and deactivating the tokens. Lotus Notes and Microsoft Exchange Email Account Creation. Microsoft Exchange Migration: Creating Exchange accounts Secure the SharePoint website used for all documentation and sharing of documents not wanting to be seen on Y Drive, where Non Employees don't have access too. Separations: Access to email files and P Drives; then deletion of account and deprovisioning of user access. Send appropriate team emails based on user's access and what else needs to be terminated. Managing all emails in the Security Mailbox and ensure all go to the correct person filed in the correct folder. Managed 10 SAP systems including QDMS, ENOC, FCM, PR1, CRM, and Trackwise. SAP/S&E databases are on Lotus Notes where requests are approved for roles, transferred from Temp to Perm associates, and either reapproved, or terminated access. Managed SharePoint Site for HP Quality Center testing for our

QA, DEV, and Production systems. Add users to HPQC systems Work with Hyperion, ITSM, and firefighter to record major changes in production systems. Information Security Analyst Bed Bath and Beyond - Union, NJ November 2011 to June 2012 Created User Credentials for users in systems, such as, Active Directory, Lotus Notes, Kronos, Lawson, SSL VPN, ImageNow, JDA, AS 400, WSFTP, and other systems access was needed too. Heavily documented all procedures and standards for IT Security so new employees would know how processes run step by step with no gaps. Helped put firewall requests in for Vendors who accessed our systems via SSL VPN. Made sure Access controls were in place for Auditors, worked closely with Auditors to improve processes that were questionable for PCI as well as SOX. PCI requires 3 factor authentication for Network Connect VPN users, so ordered more Security Tokens to be given and handed to all Network Connect Users securely. Worked on PCI and SOX Compliance by running scans of password resets, failed logins, failed attempts, password resets, and terminated users for SSL VPN, AS 400 Systems, etc. Worked with Blue Coat, Blue Cat, and Proteus to do Anonymous Proxy Authentication Server Requests, DNS request, and DHCP requests, as well as, analyzed logs and ran reports on both systems. Assisted in managing the SSL VPN by doing daily logs, adding users, role mapping, creating groups, and configuring the users on Cisco Secure so that they could authenticate. Controlled the Symantec Administrator Console. Managed threats, intrusion detection incidents, and removed or contacted the appropriate them to take care of the incident immediately. Updated all antivirus on all company servers. Provided the Desktop Team information about the type of intrusion, how to remove the infected file or files, and provided the team on where to find the removal tools. Also sent new virus files to Symantec if no information was found on the virus. Reviewed all PCI logs for Oracle, Ecommerce, Teradata, AS 400, SSL VPN, and Store Database Servers. Made sure to contact the appropriate people when there was an issue. Worked with Secureworks to identify and manage threats, risks, and vulnerabilities in the company's systems and was notified when an alert needed a solution. Worked as a Lawson Receiving Administrator, where information on purchasing and approvals for these purchases were kept for IT Security. Organized and helped improve documentation of everyday procedures and manuals for

IT Security. Helped create and maintain usage of a new FTP program, Accellion. Worked with Store and Corporate Employees through Customer 1 to troubleshoot issues with, Passwords, Network, SSL VPN, e-Links, Citrix, Intranet, Software, and any issues involving what IT Security was responsible for. Processed Terminations, Leave of Absences, and Return of Leave of Absences for all employees in the company, warehouses, and stores. Worked with Customer 1 Tickets to help the end user that needed help with credentials or systems IT Security managed. Met with Vice President's to improve documentation and the process within IT Security to make the department more efficient and productive. Such as the company used paper requests and filed all documentation in the filing cabinet while mentioning to create a lotus notes database. Organized the filing cabinet based on the type of request, 4 weeks of the month, and color coordinated the folders so documentation was easier to find for the Auditors when asked to pull requests. Was given control over ISDCLEAR which is on our AS 400 Systems ISD A and ISD B and allows employees to view unencrypted credit card information. Made sure properly Vice President Approval was given for this access since PCI Audit would want all documentation needed to meet their audit requirements.

Continue working with Internal Audit to divide and control menus on the AS 400 systems and QSYOPR profiles which allows employees to have all control over profiles. Audit also wanted new JDA Levels within the AS400 systems made in order to make sure that nothing was being seen by employees that shouldn't be seeing certain information within the levels after I brought to their attention there were holes within the levels and too much access was being given to many employees. Employees had the wrong menus, too much access, or levels weren't broken down enough to give employees the appropriate viewing menu. Several new group menus and group profiles are being created in order for an employee to do a job function but enable more access then the employee actually needs. Menus are being moved, changed, broken into segments and restricting access in menu control now. Information Security Intern Pearson Education - Old Tappan, NJ June 2011 to August 2011 Worked with the UK and SharePoint Specialist's in order to help create a new SharePoint site for the Data Privacy and Security Team. Reviewed the DLPM (Data Loss Prevention Manual) to ensure accuracy. Assisted with special project on Neo (a social

networking site for Pearson Employee's) /Intranet/ and SharePoint, which included making observations and recommending improvements. Reviewed policies and procedures that had not been updated. Worked with all of the Pearson Groups on PCI Compliance, including, oversight of compliance surveys and assisting groups that needed help with PCI compliance. Education Master's Certification Information Systems Security New York University December 2011

Name: Angela Taylor

Email: rodney20@example.net

Phone: +1-314-662-1252x45758