Alyssa

MILLER

Shooting Your Shot

The Fallacy of Shooting Your Eye Out

19 – Programmer (FinTech)

28 – Penetration Tester

31 – Leading Testing & VM

35 – Most Profitable Team

37 – Head of Practice

41 – Passed over for promotion

BISO

Business Information Security Officer

Derailing women in their careers

Work is secondary

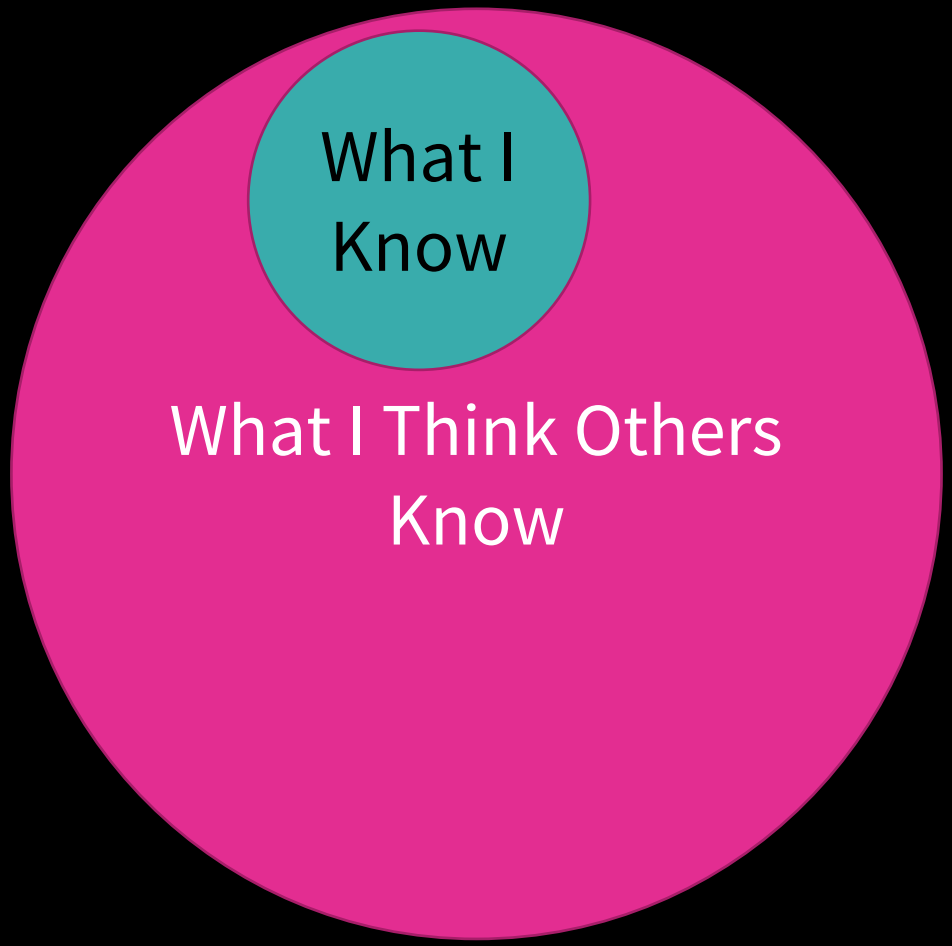
Value on overwork

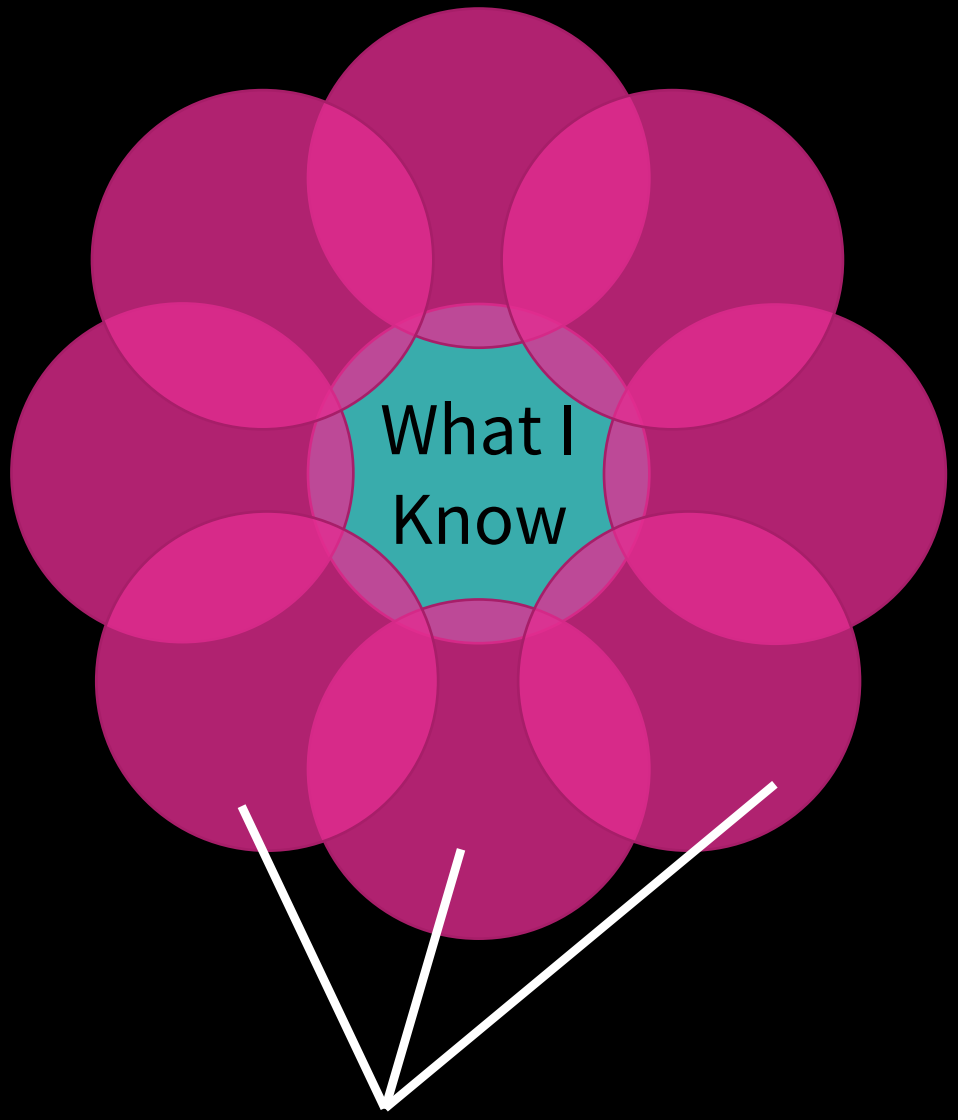
“Off ramps”

Lack of Role Models

Source: https://hbr.org/2020/03/whats-really-holding-women-back

The Role of Impostor Syndrome





Job descriptions suck

Information Security Architect

[redacted]

NEW • Posted 10 hours ago • Be among the first 25 applicants

This is an environment *unlike anything* in the high-tech world and the secret of [redacted]success is its culture. The value [redacted]puts on its employees is well documented in articles from a variety of publishers including Bloomberg and Forbes. Our employees and our members come FIRST. [redacted]is well known for its generosity and community service and has won many awards for its philanthropy. The company joins with its employees to take an active role in volunteering by sponsoring many opportunities to help others. In 2018, [redacted]ontributed over $39 million to organizations such as United Way and Children's Miracle Network Hospitals.

[redacted]T is responsible for the technical future of [redacted]Wholesale, the second largest retailer in the world with wholesale operations in twelve countries. Despite our size and explosive international expansion, we continue to provide a family, employee centric atmosphere in which our employees thrive and succeed. As proof, [redacted]consistently ranks in the top five of Forbes "America's Best Employers".

The Information Security Architect plays an integral role in defining and assessing the organization's security strategy, architecture and practices. The Information Security Architect will be required to effectively translate business objectives and risk management strategies into specific security processes enabled by security technologies and services.

If you want to be a part of one of the BEST "to work for" companies in the world, simply apply and let your career be reimagined.

ROLE

- Translates complex security-related matters into business terms that are readily understood by colleagues. Presents analyses in person and in written formats to senior leadership.
- Interprets business, technology and threat drivers, and develops practical security roadmaps to deal with these drivers.
- Demonstrates flexibility within a variety of changing situations, while working with individuals and groups. Changes his or her own ideas or perceptions in response to changing circumstances. Alters standard

- Develops and maintains a security architecture process that enables the enterprise to develop and implement identity and security solutions and capabilities that are clearly aligned with business, technology and threat drivers.
- Develops identity and security strategy plans and roadmaps based on sound enterprise architecture practices.
- Develops and maintains identity and security architecture artifacts (e.g., models, templates, standards and procedures) that can be used to leverage security capabilities in projects and operations.
- Tracks developments and changes in the digital business and threat environments to ensure that they're adequately addressed in security strategy plans and architecture artifacts.
- Participates in application and infrastructure projects to provide security-planning advice.
- Drafts security procedures and standards to be reviewed and approved by executive management and/or formally authorized by the VP of Information Security and Compliance.
- Determines baseline security configuration standards for operating systems (e.g., OS hardening), network segmentation, and identity and access management (IAM).
- Develops standards and practices for data encryption and tokenization in the organization, based on the organization's data classification criteria.
- Conducts or facilitate threat modeling of services and applications that tie to the risk and data associated with the service or application.
- Ensures a complete, accurate and valid inventory of all systems, infrastructure and applications that should be logged by the security information and event management or log management tool.
- Establishes a taxonomy of indicators of compromise (IOCs) and share this detail with other security colleagues, including Information Security VP, directors, managers and analysts, as well as counterparts within the network teams.
- Coordinates with our future DevOps teams to advocate secure coding practices.
- Validates IT infrastructure and other reference architectures for security best practices and recommend changes to enhance security and reduce risks, where applicable.
- Validates security configurations and access to security infrastructure tools, including firewalls, IPSs, WAFs and anti-malware/endpoint protection systems.
- Reviews network segmentation to ensure least privilege for network access.
- Liaise with the internal audit (IA) team to review and evaluate the design and operational effectiveness of security-related controls.
- Reviews security technologies, tools and services, and make recommendations to the broader security team for their use, based on security, financial and operational metrics.
- Liaise with other security architects and security practitioners to share

REQUIRED

- Minimum of eight years' in an engineering and architectural role.
- Experience in using architecture methodologies such as SABSA, Zachman and/or TOGAF.
- Direct, hands-on experience or strong working knowledge of managing security infrastructure — e.g., firewalls, intrusion prevention systems (IPSs), web application firewalls (WAFs), endpoint protection, SIEM and log management technology.
- Verifiable experience reviewing application code for security vulnerabilities.
- Direct, hands-on experience or a strong working knowledge of vulnerability management tools.
- Documented experience and a strong working knowledge of the methodologies to conduct threat-modeling exercises on new applications and services.
- Documented experience and a strong working knowledge of the methodologies to conduct threat-modeling exercises on new applications and services.
- Full-stack knowledge of IT infrastructure:
- Applications.
- Databases.
- Operating systems — Windows, Unix and Linux.
- Hypervisors.
- IP networks — WAN and LAN.
- Storage networks — Fibre Channel, iSCSI and NAS.
- Backup networks and media.
- Direct experience designing IAM technologies and services:
- Active Directory.
- Lightweight Directory Access Protocol (LDAP).
- Cloud (Azure) IAM.
- Strong working knowledge of IT service management (e.g., ITIL-related disciplines):
- Change management.
- Configuration management.
- Asset management.
- Incident management.
- Problem management.
- Regulations, Standards and Frameworks:
- Payment Card Industry Data Security Standard (PCI-DSS).
- HIPAA-HITECH.
- Validated Systems (e.g., GAMP).
- Sarbanes-Oxley.
- General Data Protection Regulation (GDPR).
- Privacy Practices.
- ISO 27001/2.
- NIST Cybersecurity Framework (CSF).
- ITAR.

Know your worth

Mentoring is about them, personally

See denials differently

Negotiating the job offer

@AlyssaM_Infosec

/in/alyssam-infosec

https://alyssasec.com

Thank You

Alyssa

MILLER