Robert (Bob) Dooling

Cybersecurity and Risk Management Leader

https://www.linkedin.com/in/robertddooling/

Austin, TX
(703) 597-1993
bob@doolings.org

Redox, Inc. — *Security Risk Manager*

August 2019 - Present (Austin, TX)

Leading the risk management function for a rapidly growing, cloud-based healthcare data exchange. Responsibilities include incident detection and response, third party risk, vulnerability management.

DISD, LLC — Founder; *Security Advisor*

January 2018 - August 2019 (Austin, TX)

Providing holistic security program assessments (primarily benchmarking against NIST CSF) and quantified risk analysis (FAIR); optimizing incident detection and response capabilities; cybersecurity leadership, risk mitigation, and related advisory services. (https://www.disdefenders.com/about.html)

- Established unified IDR capability across merged companies - including joint analysis and response platform and runbooks.
- Trained executive stakeholders and technical team members on IR policy, processes, and technologies.
- Lead team to improve detection signal-to-noise ratio, resulting in a 6x increase in rate of validated incidents.
- Developed & kick-started vulnerability management and IDR metrics programs; established foundation for quantified risk management.

Praetorian — *Practice Manager*

December 2013 - January 2018 (Austin, TX)

Trusted advisor to Fortune 1000 clients and high tech startups. Executed and managed a wide variety of security assessment and incident response projects, focused on enabling clients to identify, prioritize, and remediate technology risks across their enterprise.

- Led and executed full scope red team engagements, collaborative red / blue team services, regulatory compliance gap analyses, policy and procedure enhancements, and security program assessments.
- Managed and mentored a team of security engineers and consultants.
- Project managed multiple concurrent engagements, from scheduling through technical execution, and ensuring quality of deliverables.
- Provided advisory services for several clients on an ongoing basis, working through topics such as security posture industry benchmarks, IT security spend ratios, and cost/benefit analyses.
- Contributed to company growth by recruiting, interviewing, and partaking in consensus-based hiring decisions.
- Spearheaded deployment of formal testing methodologies for

SUMMARY

Expertise in assessments and incident management.

Blends methodical risk management with deep technical knowledge.

Excels in roles that blend business, strategy, and offensive & defensive technical aspects.

AREAS OF FOCUS

Holistic security assessments

Cyber risk management

Incident detection and response

Security architecture, operations, and automation

Security metrics

Penetration testing and adversarial emulation

Cyber insurance

numerous existing and newly developed service offerings.
- Launched several internal information security initiatives; developed and communicated security-related policies and procedures.

SANS Institute — *Author, GIAC Exam Development*

May 2011 - July 2013 (Remote; supplemental work)

Created and reviewed content for ISO/ANSI-certified cybersecurity exams.

DISD, LLC — Founder; *Security Advisor*

December 2009 - December 2013 (Austin, TX)

Provided freelance services specializing in technical security assessments, incident detection and handling, and risk assessments.

- "Full-stack hacker": executed white box and black box network and application penetration tests, physical security and social engineering tests.
- Managed client relationships and engagements, end-to-end: business development, scoping, scheduling, project execution and management, quality assurance, and account management.
- Provided advisory services for several SMB clients on an ongoing basis, working through topics such as regulatory compliance, data classification and management, and cloud migrations.
- Managed budgeting and billings - leading to average YoY revenue and profit growth of 41% and 44%, respectively.

Texas DIR — *Sr. Information Security Consultant*

October 2008 - January 2011 (Austin, TX)

Executed self-directed penetration tests for Texas state agencies, municipalities, universities, and utilities - assessing and attempting to infiltrate in-scope networks, systems, and applications.

- Presented findings, demonstrated exploits, explained potential impacts, and prioritized recommendations.

Symantec Corporation — *Sr. Information Security Engineer*

June 2006 - August 2008 (Remote)

Security specialist on a SIEM product delivery team. Leveraged monitoring / analysis background to create logic rules to identify security incidents.

Symantec Corporation — *Network Security Analyst, MSS*

November 2003 - June 2006 (Washington, DC)

Identified, escalated, and managed security incidents in a 24x7x365 Security Operations Center (SOC) environment.

Arthur Andersen, LLP / Protiviti — *Technology Risk Consultant*

June 2001 - November 2003 (Washington, DC)

Performed audit and analysis of clients' information system security controls to help ensure integrity of financial statements.

CREDENTIALS

CEH (Certified Ethical Hacker)

CISSP #121592 – (ISC)2

GAWN (Wireless Assessments)

GCFE (Forensic Examiner)

GCFW (Firewall Analyst)

GCIH (Incident Handler)

GNFA (Network Forensics)

GSEC (GIAC Security Essentials)

GSNA (Systems & Network Auditor)

GWAPT (Web Application Penetration Tester)

Open FAIR Certification

EDUCATION

James Madison University - BBA: Finance; MIS

Dual major focused on economics, financial management, and information security. (1997 - 2001)

EXTRACURRICULAR

University of Texas at Austin - Contributing Lecturer in the Computer Science Department

CS 378, Ethical Hacking: Wireless security, Incident Detection & Response. (2015 - 2017)

REFERENCES

Refer to LinkedIn Profile. Additional references available upon request.