Crowe

Smart decisions. Lasting value.™

Proposal to Provide SCADA Vulnerability Assessment

June 6, 2018

Submitted to:
Mr. Ted Beck
Chief Information Security Officer
44 E. Downer Place
Aurora, IL 60505

Submitted by:
Bob Dobis
Crowe LLP
One Mid America Plaza, Suite 700
Post Office Box 3697
Oak Brook, Illinois 60522-3697
Bob.dobis@crowe.com

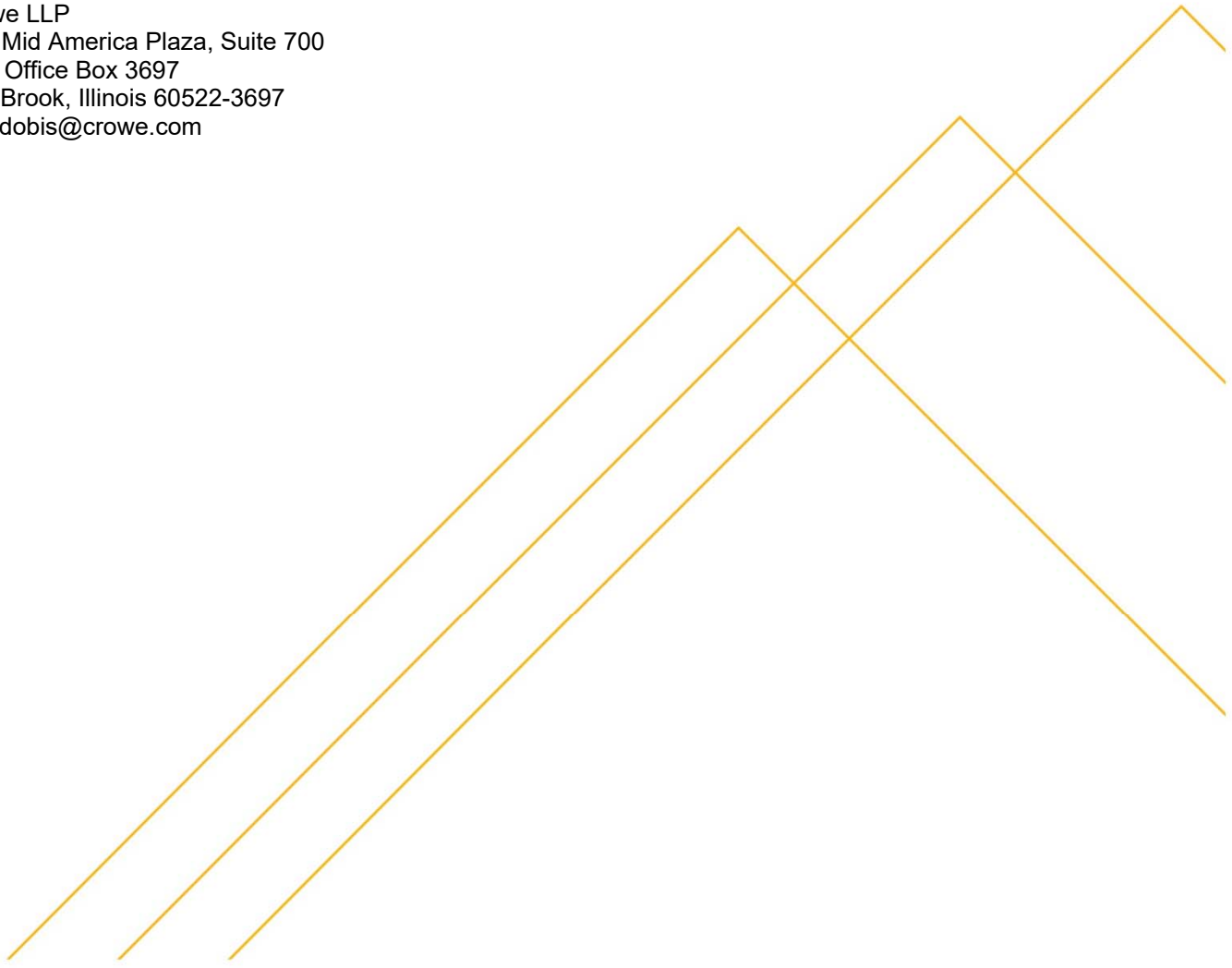


Table of Contents

Crowe LLP
Independent Member Crowe Global

One Mid America Plaza, Suite 700
Post Office Box 3697
Oak Brook, Illinois 60522-3697
Tel 630.574.7878
Fax 630.574.1608
www.crowe.com

June 6, 2018

Mr. Ted Beck
City of Aurora
Chief Information Security Officer
44 E. Downer Place
Aurora, IL 60505

Dear Mr. Beck:

Crowe LLP appreciates the opportunity to assist City of Aurora (Aurora) in assessing its IT Security Risk by providing you this proposal for Vulnerability Assessment Services of your SCADA network.

Crowe is an experienced, stable and well-respected consulting and accounting firm with a strong commitment to Cybersecurity services. We have delivered high value to our clients for decades and we feel that we are the best firm to serve Aurora. Our goal is to work with you to deliver a unique solution that exactly meets your needs and value expectations. We wish to thank Aurora for taking the time to discuss and respond to our questions. Our proposed project scope and approach was customized based on your feedback.

We understand your organization's IT Security needs to be vulnerability assessment of your SCADA network.

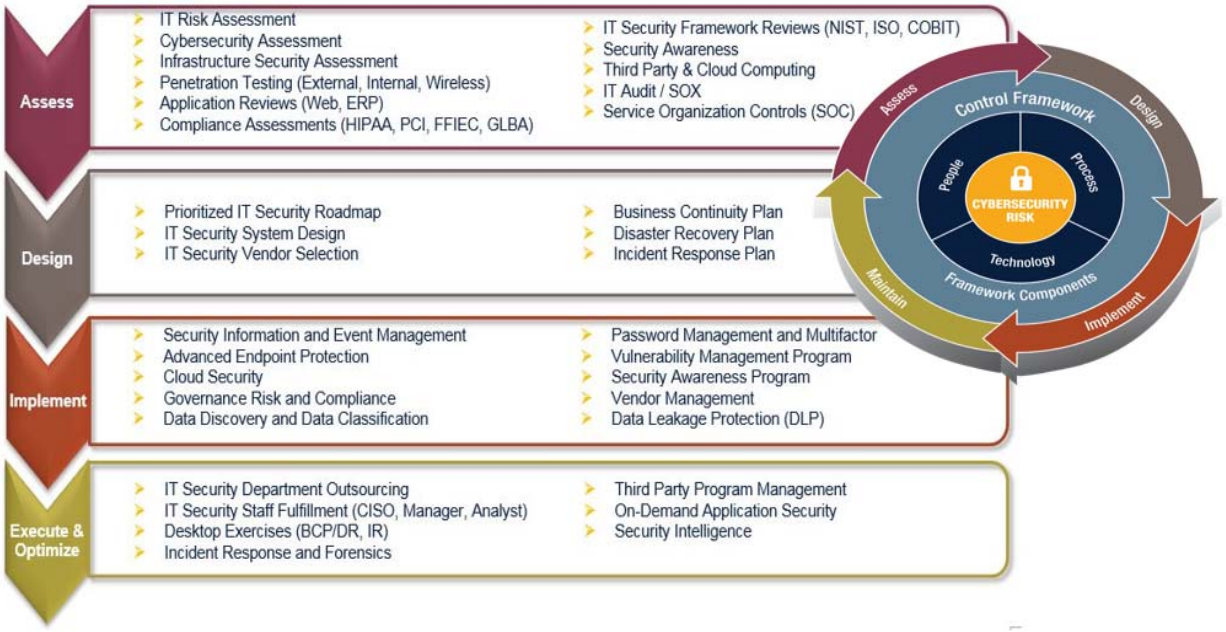
We look forward to the opportunity to assist Aurora in this project and will provide you our closest attention. If needed, we would be happy to work with you to further customize this proposal relative to scope and fees. Should there be any questions with regard to our proposal, please contact me at 630.586.5252 or via email at bob.dobis@crowe.com. We welcome further discussion with you and other representatives from Aurora regarding our proposal.

Sincerely,

Bob Dobis
Partner

Crowe's Cybersecurity Team

Crowe has worked with hundreds of companies across the United States and internationally to improve the quality of their Cybersecurity posture through risk assessments, penetration testing, vulnerability assessment, Cybersecurity assessments, and the implementation of security/technology solutions. Crowe's Cybersecurity team consists of nearly 60 professionals in seven office locations who deliver the following services:



The team that would be constructed to assist you includes professionals who have functioned as CISOs, served as security administrators, and managed internal risk assessment functions. A large majority of our professionals, including all of our Managers and above, are certified and regularly speak on information security issues at national security conferences such.

Crowe maintains multiple consultants that hold the following certifications:

- Certified Information System Security Professional (CISSP)
- Offensive Security Certified Professional (OSCP)
- Offensive Security Certified Expert (OSCE)
- Certified Ethical Hacker (CEH)
- GIAC Penetration Tester (GPEN)
- DIAC Web Application Penetration Tester (GWAPT)
- Certified in Risk and Information Systems Control (CRISC)
- CompTia Security+

A sample of Crowe's presentations and contributions to the Information Security community include:

Blackhat - US 2015:
At the prestigious Blackhat Security Conference, Cybersecurity Consultants Mike McAtee and Lucas Morris unveiled "Cracklord", a new distributed password cracking system. This tool was built as a management platform that load balances CPU/GPU resources from multiple hardware systems into a single queuing system.

Blackhat - US 2012:
During Blackhat 2012 Ryan Reynolds, a Senior Manager at Crowe, spoke about a flaw in the current de facto standard algorithm logic for extracting password hashes from the Windows registry. Similar logic is used by many popular password extracting utilities. Ryan's research has led to many bug fixes in these popular tools used by security professionals every day.

DerbyCon 4:
At DerbyCon 4 Ryan Reynolds spoke on the topic of advanced traffic manipulation techniques such as NetBIOS-NS/LLMNR, ARP-Spoofing, and IPv6 Stack precedence. These techniques are used by hackers to manipulate network traffic with the goal of gathering unauthorized access to sensitive data traversing the network during Internal Penetration Assessments.

Also at DerbyCon 4, Lucas Morris showcased "RavenHID". RavenHID is a combination Arduino board/IOS application that can be used to collect badge information for cloning. This method is used to advance Crowe's social engineering testing for corporate client environments.

DerbyCon 3:
Crowe continues its security community contributions at Derbycon 3, where Piotr Marszalik spoke about leveraging Windows tools including PowerShell to maintain persistence on a compromised machine during phishing assessments. This custom Trojan is a great example of how Crowe brings advanced technical skills to Penetration Assessment engagements that not only test the human element but also the technical aspects of phishing attacks on client environments.

DEFCON 22 & DEFCON 20:
At Defcon 22 as well as Defcon 20; Lucas Morris and Mike McAtee contributed to the Windows security world with a panel on their tool "Shareenum". It is a tool that can be used to enumerate Windows SMB shares, fingerprint systems, as well as test password re-use. "Shareenum" is made with speed and scalability in mind for bulk system testing.

BSides DFW 2013, 2016 and 2017:
At BSides DFW; Ryan Reynolds, Chris Wilkinson, Brad Hannah, Mitch Hennigan and John Alves have presented throughout the years on the latest tools and techniques used by consultants and attackers in the Cybersecurity community. Crowe continues to speak at local events on a regular basis on a variety of Information Security topics.

Crowe has been involved a number of other presentations, including but not limited to:

- "Anatomy of a Breach" at the University of Texas at Dallas Fraud Conference in 2016
- "The Three Lines of Defense" at North American CACS in 2016
- "Forensics Investigations" at the University of Texas at Dallas Fraud Conference in 2015
- "Network Security Trends" at the AICPA National Conference in 2014
- "Anatomy of a Breach" at the San Francisco ISACA Fall Conference in 2014
- "Penetration Testing: Lessons Learned" for the Texas Bankers Association in 2014
- "CyberSecurity Trends" at the 2013 American Bankers Association National Convention
- Presentations on Penetration Testing and Business Continuity at ISACA's Geek Week

Collegiate Cyber Defense Competition
The Collegiate Cyber Defense Competition is an event held annually to assess an institutions student's depth of understanding and operational competency in managing the challenges inherent in protecting a corporate network infrastructure and business information systems. The competition is structured to score University's "Blue Team" (Defense) ability to defend their environment against a simulated hack coordinated by the "Red Team" Professional Penetration Testers.

Crowe Cybersecurity Consultants have been invited to participate on the Red Team for the following contests:

- Mid-West Region (2015, 2014, 2013)
- Northeast Region (2017, 2013, 2011,2010)
- Southwest Region (2017)

Crowe has invested a significant amount of research and development time into becoming a forefront industry leader in Information Security. Our technology risk professionals have in-depth knowledge not only of the industry standards for Information Security, but also the practical implementation of these standards in accordance with business processes and drivers.

Tool Development

A continuous development and review process is facilitated to ensure that clients are receiving the best of breed tool suites; whether commercial, in-house developed, or publicly available. A sample of the tools that Crowe has contributed to the Information Security community include:

- Ad-ldap-enum (2016)
- Go-SSHscan (2016)
- Cracklord (2015) – Presented at Blackhat
- RavenHID (2014) - Presented at DerbyCon
- Share-Enum (2013) – Presented at DEFCON

Crowe recognizes that highly technical engagements such as Penetration Testing and IT Forensic Assessments require significant investments of both key personnel and resources. In identifying this requirement, Crowe has not only created a dedicated Cybersecurity team, but also focused that team to establish the Crowe Center for Cyber Security. This Center serves as a foundation in technology assessment services, ensuring that our team stays on the cutting edge of the security field.

Vulnerability Assessment: Project Scope

SCADA Vulnerability Assessment

Crowe's Vulnerability Assessment will provide you with the following areas of testing:

Vulnerability Assessment – SCADA
SCADA environments are fragile to security testing and require an assessment approach to testing. Crowe proposes first performing a paper assessment of the design, protocols, and security controls in-use. Once complete and potential attack vectors identified, we recommend that a lab be setup to emulate the attack vectors for testing purposes. Crowe plans to follow guidance provided by standardized methodologies including the National Electric Sector Cybersecurity Organization Resource (NESCOR) Guide to security testing for Electric Utilities. The planned test will be an end-to-end assessment including serial and IP protocols, HMI, data historian, sensors or controls equipment (IEDs, RTUs, etc.). This will be a time-limited engagement designed to research and identify vulnerabilities within the overall SCADA / OT environment.

Tasks to be performed include:

- Application and Logic Vulnerability Discovery
- Firmware Sensitive Data Extraction
- Firmware Update Mechanism Review
- Device and Network Authentication Review
- Control Bypass Testing
- Protocol Analysis
- Hardware Security Testing

Some of the procedures to be performed include:

- Logic Vulnerabilities – Crowe will examine documentation and analyze device function to identify potential vulnerabilities in the device logic.
- Protocol Analysis – Crowe will perform extensive testing between the HMI and field devices in an attempt to identify vulnerabilities and attack vectors. The protocol will be analyzed for security best practices related to core cybersecurity tenets of confidentiality, integrity and availability. Protocol field fuzzing will be performed where possible and in a controlled environment.
- Firmware Update Mechanism – When evaluating the target devices, Crowe will identify vulnerabilities discovered in the firmware update process. This will identify flaws that may leave the client vulnerable to "watering hole" attacks or code injection via firmware update processes.
- NERC CIP Requirement Review – As part of the SCADA / OT environment security assessment, Crowe will review and give opinion and justification of the application of controls required under CIP-005 and CIP-007.

Fees and Assumptions

Fees

The following table lists proposed cost for each deliverable and the total fixed price based on Crowe's understanding of the project.

Service	Scope	Fees
SCADA Vulnerability Assessment	Technical Vulnerability Assessment	$39,400
	Total Fixed Price	***$39,400***

This engagement will be billed to Aurora on a fixed fee basis in accordance with our proposed fee structure and audit project estimates. Travel and out-of-pocket expenses will be billed to Aurora at actual cost. Any other expenses will be discussed and approved in advance by you. The pricing in this proposal will remain valid for a period of 30 days from the date of this proposal.

Assumptions

Crowe assumes the following sample sizes and assumptions as relates to the security reviews described above:

Review Area	Scope Assumption
General Project Assumptions	• Aurora accepts all statements made within this document regarding scope. • Information requested through a separate resource request letter will be gathered and available for our consultants upon arrival. • Your resources and subject matter experts will be available to participate in interview sessions, individual meetings, and conference calls as necessary to provide input about the technology, organization, and processes that are currently in place at the Aurora. • Crowe consultants will have access to all necessary systems, resources, and personnel for the duration of the engagement
SCADA Vulnerability Assessment	• Test systems will be available to conduct security testing against non-production systems. • Crowe will conduct the work with two (2) resources over two (2) weeks with access the necessary systems during this time. • The Aurora SCADA network consists of 84 total devices.

Delivery Team

The following sections describe the project roles and associated responsibilities. As with projects similar in size and structure, multiple project roles may be held by one or more individuals.

Crowe will leverage the following key resources in order to staff the engagement:

Resource	Role	Certifications	Experience
Robert Dobis	Project Executive	CPA, CDP	30 Years
Mike Del Giudice	Project Manager	CISSP, CRISC	18 Years
Mitch Hennigan	Technical Lead	OSCP	3 Years

Project Executive

The Project Executive's primary responsibilities include:

- Assuring client satisfaction
- Project Billing and Contracts
- Making available the appropriate Crowe resources to accomplish the project objectives and address other needs and requests of the project team.
- Assuring quality and direction of Crowe work in addressing the project objectives
- Soliciting feedback regarding the project and Crowe's performance
- Reviewing the overall progress of the project and assist with setting revised project direction (if required)
- Provide project 'dash-board' review

Project Manager

The Project Manager oversees the day-to-day activities of the project (in conjunction with client Project Executive). They will share joint responsibility for the planning and execution of all Project activities. The Crowe Project Manager is primarily responsible for:

- Assuring client satisfaction
- Directing, making available and managing Crowe resources to accomplish the engagement objectives
- Maintaining necessary communications with the entire Project Team
- Performing detail planning, scheduling and execution of project activities within the overall plan
- Assigning tasks to project personnel
- Monitoring staff and Project progress
- Managing risks and escalated issues from Project Team
- Monitoring budgets, preparing reports and scheduling resources
- Measuring project success against budget, original scope, business objectives
- Assuming responsibility for planning resource requirements and coordinating the daily tasks of all Project Team members
- Ensuring that all resources and their respective skills are optimally utilized
- Providing quality assurance of work undertaken by staff assigned to the Project

Project Specialists

The Crowe Project Specialists are primarily responsible for:

- Understanding the Project approach, targeted objectives and making informed decisions and recommendations throughout
- Completing tasks and deliverables assigned by the Project Manager
- Transferring the appropriate skills to your Project Team Members