Digital Boundary Group

Proposal

IT Security Assessment

Prepared For:

Township of Malahide
87 John Street South
Aylmer, Ontario

Prepared By:

Bryan Parr

Date:

October 1, 2019

Proposal Number:C19-01461-01-1

Contents

Corporate Overview

Digital Boundary Group (DBG) is an information technology security assurance services firm serving clients worldwide.

DBG provides information technology security auditing and compliance assessment services. In addition, we offer information security consulting, network security assessments, penetration testing (PCI), application security testing (web and mobile), vulnerability scanning, wireless security assessments, SCADA security assessments, and physical security assessments. Our training offerings include hands-on Hardening Windows Networks courses and Network Security training.

DBG's operational security testing provides organizations with a comprehensive assessment of their security posture, both externally and internally. We are vendor neutral regarding hardware and software solutions but maintain ongoing relations with Tier-One and other vendors in order to stay current with relevant technology developments. We do not sell hardware or software and do not sell network design, installation, management, or remediation services.

Our client experience includes: Federal, Provincial/State, and Municipal governments; Law Enforcement; Utilities (including electricity generation and distribution and water/wastewater treatment facilities); Mining; Oil & Gas / Energy sectors; Financial / Insurance Services firms; Healthcare; Retail; Casino / Gaming; Education (Post-Secondary and K-12); Transportation / Logistics Firms; and Professional Services firms.

We are a National Partner of (MISA/ASIM) Municipal Information Systems Association of Canada and Associate Members of British Columbia, Prairie, Ontario, and Atlantic Canada chapters. We are an Associate Corporate Member of The Canadian Association of Chiefs of Police (CACP). We are a Corporate Partner Member of the Canadian Electricity Association (CEA) and Commercial Member of The Electricity Distributors Association (EDA) of Ontario.

We maintain Certified Information Systems Security Professional designations for our senior technical staff and are authorized by the global security standards organization, $(ISC)^2$, as a Continuing Professional Education Provider for information security professionals.

Digital Boundary Group operates from our offices in London, ON and Dallas, TX.

Digital Boundary Group Municipal Government Qualifications

DBG has been conducting operational security assessments of Canadian Municipalities since the company's incorporation in 2003. DBG has been engaged by over 150 municipalities across Canada.

Canadian Municipalities served include (sampling):

- City of Brandon
- City of Calgary
- City of Courtenay
- City of Edmonton
- City of Fredericton
- City of Kelowna
- City of Kitchener
- City of London
- City of Lethbridge
- City of Medicine Hat
- City of Moncton
- City of Penticton
- City of Peterborough
- City of Regina
- City of Saint John
- City of Toronto
- City of Trail
- City of Waterloo
- City of Vernon
- City of Whitehorse
- County of Brant
- County of Grande Prairie
- County of Elgin
- County of Grey
- County of Wellington
- Halifax Regional Municipality
- Municipality of Chatham-Kent
- Regional District of North Okanagan
- Regional Municipality of Durham
- Town of The Blue Mountains
- Regional Municipality of Halton
- Town of Truro

DBG has been elected to the MISA Ontario Board of Directors as one of two Partner Representatives on two separate occasions. DBG's second 2-year term was completed in 2018. DBG has attended all MISA Chapter Conferences since 2005.

Proposed Scope of Work

Malahide requires a security assessment and penetration test against their internal and external network. The objective of this engagement is to identify and qualify any discovered threats and recommend mitigation strategies and/or compensating controls to reduce or eliminate risk.

External Penetration Test

An External Penetration Test provides independent verification of the security status of an organization's Internet presence. The test will allow DBG's security consultants to identify vulnerabilities, validate the effectiveness of safeguards, demonstrate existing risks, and provide remediation strategies to improve Township of Malahide's security posture. DBG's penetration test methodology is based on a number of industry standards and best practices including OWASP Top 10 project, ISO 27000 series, NIST, OSSTMM, and PCI DSS. Through both manual and automated testing, DBG's consultants will identify known vulnerabilities as well as deficiencies with the installation, configuration, or management of external-facing network components and services. An electronic social engineering campaign is also conducted in an attempt to solicit confidential information and measure Township of Malahide's response to a simulated phishing attack. DBG's testing includes the following steps: Discovery, Enumeration, Research, and Exploitation. Coverage includes:

Public Information Disclosure

Discovery or intelligence gathering is the act of performing reconnaissance against a target to gather as much information as possible. This section focuses on the information that is harvestable from public sources and could be utilized during the vulnerability assessment and exploitation phases.

DNS and SMTP

This section will focus on the configuration of the electronic messaging and domain name systems including:

- Mail forging, relay, and validity checks
- DNS zone transfer
- Subdomain discovery and bypassing of wildcard entries through brute force

Intrusion Prevention

- Identify the differences between tests carried out from a whitelisted source IP and a non-whitelisted source IP, to show how security devices handle malicious activities
- The inability to scan systems for vulnerabilities due to a security system's auto-blocking feature

Firewall

- Review Malahide's firewall implementation as it pertains to the ability to access services (open ports), identify exposed services with increased risk, and assess the exposed attack surface

Password Strength and Authentication

- Evaluate the length and complexity of passwords harvested
- Evaluate the efficacy of the authentication mechanism, including identifying processes that disclose information useful to obtain access
- Perform a password guessing attack in an attempt to obtain access

Host Security

- Inspect the external-facing network devices and servers for missing security patches, out-of-date or unsupported software, default settings, and other system/service misconfigurations

Transport Layer Security

- Evaluate the communications protocols, certificate trust status, and encryption cipher suites available

Social Engineering

- Determine the susceptibility of company staff to an email-based social engineering attack
- Leverage information gained to exploit identified external security vulnerabilities

Deliverables

The results of the engagement will be presented in a report format that is divided into two sections:

Executive Summary – Written for senior management, this section briefly describes the assessment process, key findings, and a prioritized list of action items.

Detailed Findings – Observations, implications, and recommendations are documented in this section for each of the key assessment areas. Diagrams, tables, scanning tool output, procedures, and detailed technical instructions are also referenced in this section.

Network Security Assessment

A Network Security Assessment combines penetration testing, vulnerability assessment, and security architecture review into a single onsite engagement.

Penetration Testing

The goal is to simulate an attack from the perspective of an internal attacker by locating and exploiting vulnerabilities without assistance.

Exploitation of systems will be attempted only if the outcome is predictable, and will not cause disruption of service. Should the team identify exploits that have the potential to cause disruption, approval will be requested prior to proceeding.

Testing is initially performed without credentials to identify pre-authentication vulnerabilities and transitions to testing with credentials to simulate exploitation of an end-user host or the discovery of credentials. The covert nature of the penetration testing phase provides the client with an opportunity to test intrusion detection and incident response systems.

Vulnerability Assessment

Following the penetration testing phase, the team will perform a thorough vulnerability assessment using the top commercial, open-source, and in-house tools. The results are analyzed to ensure only exploitable vulnerabilities are reported, including combinations of low risk or informational vulnerabilities that form an exploit chain and represent a measurable risk.

Security Architecture Review

Deploying layers of security provides redundancy in the event of a single control failure or successful exploitation. Layers include personnel, physical, technical, and procedural components that combine to form defense-in-depth. Our security professionals encounter a wide range of defense-in-depth strategies across multiple sectors and organizations, allowing us to evaluate which strategies represent best practice.

The following domains are included in the security architecture review:

Physical Security

Physical security in this audit will focus primarily on IT assets.

- Server rooms, wiring closets, and communication rooms
- Access to the network from areas such as boardrooms and public spaces
- Access control mechanisms such as card entry and biometrics
- Surveillance, alarms, and monitoring
- Sign-in and sign-out procedures
- Visitor and subcontractor procedures

Network Management and Monitoring

Review of management and monitoring tools that are required to maintain a secure network.

- Event log management of servers and workstations
- Logs from key devices such as routers, switches, and firewalls
- Network traffic monitoring for bandwidth, top talkers, top protocols, etc.
- Secure configuration of management protocols such as SNMP, RMON, etc.
- Remote control of desktops, laptops, and servers
- Network inventory
- Patch management

Firewall Security

The firewall section involves a review of the firewall implementation including rules, monitoring, and ongoing assessment of vulnerabilities.

- Review overall design and implementation
- Review firewall rules, routes, and objects
- Review change management procedures
- Review logging and reporting processes
- Review program for firewall evasion tests
- Review program for port scans between interfaces

Authentication and Authorization

The methods of establishing a user's identity on the network are reviewed, including:

- Password strength
- Enforcement of password complexity
- Account lockout
- Password history
- Password age
- Authentication protocols

File System Security

File systems store various types of information which range in sensitivity from public knowledge to top secret. The security and integrity of these documents while at rest on a network are the responsibility of the file system. This section examines the following file system components:

- File and disk level encryption
- Integrity
- Share level access controls
- Local file system access controls
- Scan to locate open shares.

Remote Access / VPN

The remote access section of the analysis deals with the various components that provide remote connectivity to the network from mobile workers, home offices, and smaller remote branches not equipped with permanent wide area connections:

- Dial-up modem access
- Telnet, SSH, VNC, Terminal Services, etc.
- Web-based email
- Virtual Private Networks
- Third-party vendor access
- Audit controls and logging
- Authentication
- Access controls

Network Security

Typical components of a local area network include switches, routers, bridges and internal firewalls. These components are responsible for the reliable and secure delivery of data as it travels over the local network. The review will focus on the following LAN related areas:

- Layer 2 security and access control
- Secure management of switches, routers, etc.
- Review protocols and transports
- DNS and DHCP Security
- Secure use of SNMP, RMON, and other network management protocols
- Access controls

Host Security

Servers represent the core computing infrastructure in most organizations and contain sensitive information such as user credentials, customer details, financial and human resource records. The audit will review the following:

- Hardening techniques of various Server Operating Systems (Solaris, Windows, Linux, AIX, HPUX, Apple OS X)
- Directory security and configuration (Active Directory, LDAP, etc.)
- Current patch levels and patching process
- Adherence to vendor and industry best practices

Workstations represent the most significant percentage of devices found in most organizations' networks and are the most frequent target of malicious code. Workstations are used by a wide range of employees who are often targets of phishing, adware, and spyware attacks. The assessment team will review the following elements of workstation security.

- Program in place to identify malicious code or other unwanted programs
- Monitoring patch levels and patching process
- Hardening techniques of workstation Operating Systems (Windows, Apple OS X)
- Adherence to vendor and industry best practices

Content Inspection

Content controls and inspection mechanisms are reviewed in this section. Content inspection and gateway antivirus scanning often overlap. Antivirus gateway inspection is covered in the antivirus section of this report. URL blocking, ActiveX blocking, malicious code inspection and end-user auditing are included in this section.

- Determine whether the content inspection system can be bypassed through the use of proxy servers or covert channels
- Assess the ability to block access to harmful content

Wireless Networks

A review of the wireless network infrastructure is conducted. The review will include the following:

- Infrastructure security
- Authentication and encryption mechanisms
- Access controls
- Isolation of wireless networks from corporate networks
- Wireless intrusion detection

Antivirus and Malicious Code

Antivirus systems are reviewed in this section, including desktop PCs, servers, email, web and FTP systems.

- Review desktop and server antivirus solutions
- Review mail server and Internet gateway antivirus solutions including SMTP, FTP, HTTP, and HTTPS
- Reporting and alerting capabilities
- Review the incident response plan and/or processes

Intrusion Detection and Prevention

Detecting and blocking malicious activity at key points on a network is a critical component of a secure network. The following will be reviewed:

- Placement of network sensors and overall design
- Detection ability through active log analysis
- Ability to detect and/or block sample attacks generated by the assessment team
- Incident response procedures

Vulnerability Assessment

The ability of an organization to perform ongoing vulnerability assessments is essential to maintaining a secure network. The following criteria will be reviewed:

- Current vulnerability assessment practices and procedures
- Vulnerability assessment tools
- Incident response and reporting
- Escalation procedures
- Regular reporting

Wide Area Network

Wide area network components include devices such as switches, routers, firewalls, and VPN concentrators. These components are responsible for the reliable and secure delivery of data as it travels between remote branch offices, remote workers and partner networks. The review focuses on the following WAN-related areas:

- Secure management of switches, routers, etc.
- Review of protocols and transports
- Security of third-party connections such as partner networks
- Encryption
- Access controls
- Virtual LANs (VLANs)

Internet Traffic Analysis

Review of the existing program to monitor all egress and ingress traffic. The team will review the following:

- Detecting malicious traffic from Trojans and worms
- Identifying covert communication channels such as tunneled traffic over common ports. An example might be peer-to-peer file sharing through UDP port 53, normally used by DNS
- Accessing the amount of bandwidth consumed by non-business traffic such as Internet radio, peer-to-peer file sharing, etc.
- Detecting business traffic that may be using cleartext passwords or transmitting sensitive traffic in cleartext
- Locating devices on the network that may be improperly configured such as DNS and DHCP servers

Policies, Procedures, and Documentation

Policies and Procedures are used to guide an organization and define day-to-day operations. The organization's policies and procedures will be reviewed and compared against industry and vendor best practices. The review will also include the organization's ability to monitor and enforce the rules defined in each policy and procedure.

The following are examples of the type of policies to be reviewed:

- Acceptable Use
- Confidential Data
- Email
- Mobile Device
- Password
- Authentication
- Data Classification
- Guest Access
- Network Access
- Physical Security
- Backup
- Encryption
- Incident Response
- Network Security
- Remote Access

Failure to properly document and diagram a network can lead to design errors and improperly configured devices such as firewalls, routers, switches, etc. Thoroughness and organization of the network documentation will be reviewed during the assessment. The greatest security concern associated with sensitive documentation is the proper encryption of the data while at rest (storage) and while in transit (over the network). The assessment team will review the following:

- The thoroughness of network documentation including network diagrams
- The storage location of documentation
- Encryption of documentation at the disk and network levels

Deliverables

The results of the engagement will be presented in a report format that is divided into two sections:

Executive Summary – Written for senior management, this section briefly describes the assessment process, key findings, and a prioritized list of action items.

Detailed Findings – Observations, implications, and recommendations are documented in this section for each of the key assessment areas. Diagrams, tables, scanning tool output, procedures, and detailed technical instructions are also referenced in this section.

Assumptions

- The proposal estimate is for work performed during normal business hours, Monday through Friday (excluding statutory holidays) during regular business hours.
- Subject to approval, should the project involve after hours and/or weekend work, additional fees will be charged. Malahide and DBG will agree to the required amount of such after-hours and/or weekend work prior to commencement of the project, and DBG will submit an addendum to the initial proposal or SOW.
- All in-scope assets are owned and managed by Malahide. If assets are hosted by a third-party, authorization will be provided.
- Project delays, errors, incompatibilities, or defects in software, hardware, systems or any third-party products may result in additional charges.
- Work will be performed both remotely and onsite at Township of Malahide

Malahide Responsibilities

Township of Malahide understands that Digital Boundary Group's performance is dependent on Malahide's timely and effective satisfaction of the following responsibilities:

Working Environment

- Provide necessary system access for Digital Boundary Group personnel, including remote access where required.
- Provide adequate working space and assume all responsibility for site preparation, including network cabling, and electrical requirements.

Communication

- Provide DBG with all the information required to perform the Services, including completed intake and evidence of third-party authorization, within 10 days of signed contract.
- Pre-arrival checklists to be completed prior to engagement start.
- Notify DBG of any relevant issues of which Malahide is aware that will impact the Services.
- Designate a Primary Contact who will be the focal point for the engagement and has the authority to act on your behalf.

Technology

- Perform all appropriate backups and be solely responsible for its data, including taking sufficient steps to protect itself against loss or corruption of data.

Fee Structure & Payment Schedule

Total fee for IT Security Assessment: **$12,950.00** CAD/USD+ applicable taxes.

The assessment will include:

External Penetration Test

$6,950.00 + applicable taxes

- Testing of 5 live IP's
- full exploitation of vulnerabilities
- Analysis, documentation and final report

Network Security Assessment

$6,000.00 + applicable taxes

- Testing of 27 servers and 40 workstations
- Full exploitation of vulnerabilities
- Analysis, documentation and final report

This proposal will remain open for acceptance for 90 days.

Expenses: Reasonable and customary travel and living expenses are not included in the fee schedule. Travel expenses including (but not limited to) airfare, lodging, rental car, gasoline, and parking will be invoiced at actual cost. Meal costs will be billed on a per diem basis of $60 per day + applicable tax per individual for each day of onsite work that is performed, and/or a full travel day is incurred.

Payment Schedule

Payment is based on the following schedule:

- DBG will invoice after the testing phase has been completed, prior to report submission.
- Each invoice is due and payable within thirty (30) days of invoice date.
- In the event Malahide delays or puts the project on hold, DBG reserves the right to bill for the portion of work performed up to that point.

Terms and Conditions

This proposal is subject to 2021945 Ontario Inc. c.o.b. Digital Boundary Group standard terms and conditions.

Acceptance

Both parties warrant and represent that they have authority to execute this proposal on behalf of their respective companies and bind them to the obligations stated within and under the Agreement.

	Township of Malahide	**2021945 Ontario Inc. c.o.b. Digital Boundary Group**
Signature:		
Name:		Joel Shapiro
Title:		Vice President of Sales
Date:		October 1, 2019