

Physical Security and Social Engineering



PROTECT
SERVICE

Improve corporate risk reduction with strategic security and privacy services.

Is the Physical Security and Social Engineering Service right for your company?

- Do current physical security controls, and the way that they are implemented, provide adequate safety for your personnel and security for your data?
- Are you considering adopting access controls based on new technologies, such as biometrics?
- Are your employees trained to identify and resist social engineering attacks?

Overview

It is generally accepted that if someone has physical access to any computing resource, that system can inevitably be compromised; therefore, physical security has evolved as one of the most important security controls that can be applied across the network.

However, in today's world, the convergence of physical security and logical security solutions requires IT directors to manage far more information than ever before. The complexity of physical security, including operational management issues, make it difficult to implement.

DigitalDefence's Physical Security and Social Engineering service has three immediate goals:

1. Ensure a safe working environment for all employees;
2. Ensure that physical access controls, data centres, server rooms, environmental controls, and key facilities are secure; and,
3. Ensure that employees have received the training required to recognize and respond to a social engineering attack.

Benefits of strong physical security include:

- Highlights employee safety; builds trust between employees and the organization
- Ensures the integrity and availability of vital network resources and data
- Provides protection against social engineering attacks—the most successful means of obtaining information from an organization
- Minimizes corporate liability
- Reduces or eliminates financial and reputational costs of a data breach
- Standards-based assessment complies with Canadian Federal government (RCMP) standards

Scenario-Based Social Engineering Training includes:

The only effective way to train employees to recognize and respond to social engineering attacks is scenario-based training. This training is customized to each client; however, previous scenarios have included:

- Physical intrusions, including dumpster diving, piggy backing, and various means of by-passing access controls
- Using technological aids, such as CDs, USB keys, and computers to gain network access
- Attacks against help desks, IT staff to gain access and escalated privileges
- Malware-assisted attacks to remotely install backdoors, keyloggers
- Email attacks (e.g. phishing)

About Digital Defence

Digital Defence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss

Service Description

DigitalDefence's Physical Security service, which may or may not be combined with a social engineering assessment, is based on Canadian Federal Government security standards and industry best practices. It includes:

- Analysis of information gathered from interviews with key stakeholders
- Review of organization's IT security processes and documents related to physical security, incident response, HR processes, emergency plans
- Review of operational controls, such management of on-site contractors and visitors
- On-site inspection of external physical security controls, including environmental design (CPTED), fencing and lights, access points, guards, alarm systems, and closed circuit TV (CCTV) monitoring
- On-site inspection of internal physical security controls including access controls (locks and keys, badge and electronic key access, biometrics), use of security zones, doors, windows
- Review of data centre, server rooms, wiring closets and other spaces supporting the network infrastructure
- Review of environmental controls including HVAC, fire detection and suppression systems, water leakage control
- Physical security of servers, workstations, mobile devices, backup media, and other endpoints
- Physical security of non-electronic data (printer rooms, records storage areas)

DigitalDefence can also review the client's ability to withstand attacks that target their employees with our **Social Engineering** service. These attacks assess the extent to which employee actively follow the corporate information security policy.

DigitalDefence uses methods such as staff impersonation, "pretext" calling, controlled phishing attacks, and attempts to break physical security controls (piggy backing behind a legitimate employee entering a door, or lock picking) to assess employee awareness, training, and honesty.

Following completion of a social engineering assessment, we provide customized social engineering awareness training, based on customized scenarios, to guard against future attacks.

NOTE: We do not conduct sweeps to find covert listening or transmission devices ("bugs"); however, we have partnerships with several reputable firms that can provide this service if needed.

For more information please visit www.digitaldefence.ca



Digital Defence Inc

Toll-Free 866-677-1337 | Tel 905-681-3310
302 - 3310 South Service Road,
Burlington, Ontario L7N 3M6

Disclaimer

© 2010 Digital Defence. All rights reserved.
This document is for informational purposes only.
Digital Defence makes no warranties, express or implied, in this document.