Client industry

Law Practice

# Project goals

* Covertly assess damage caused by a malicious IT Director stealing intellectual property.
* Seize and secure control of network and assets.
* Manage IT department until a replacement is found.

Project Abstract:

Leaders of a law firm suspected malicious activity as well as neglect by the person responsible for their IT network and physical assets. They engaged our team to assess the validity of their suspicion without alerting the person and to bring their network to a sustainable, secure state.

Stakeholders:

Partners, Associates, Clients

## MCG Role

Program Manager, Technical Consulting, Subject Matter Experts

## The MCG Solution

MCG has cultivated a team of very experienced members in various respective areas of expertise. In this case, we deployed experts in cyber and network security to perform an assessment of the security measures in place for the internal and internet facing network.

At the request of executive management, during planned time away from the office, our team took an image of the suspected malicious person’s laptop for covert analysis to ensure this individual had no opportunity to hide information.

We reviewed malware detection, antivirus, firewall, and routing. We staged attacks on the network from the internet and from within the physical building to identify vulnerabilities.

## Findings

1. Via analysis of the IT Director’s laptop files, instant messenger logs, and emails, we determined this person had stolen information and was spreading malicious information about other employees of the firm.
2. We found vulnerabilities in the physical network that would allow for penetration by attackers on site.
3. We identified and provided recommendations for more than 20 areas of opportunity for reduction of risk to their network and data that included assessments of criticality and difficulty to cure to drive informed decisions by management on how to best deploy resources.

## Results

The IT Director was dismissed, and MCG was engaged to temporarily assume responsibility for the network and data. We immediately closed known open vulnerabilities to the physical network as well as those open to the internet. Our team developed a prioritized plan of attack for each of the areas opportunity to reduce risk and began execution with approval and oversight from the firm’s executive management. We continue to execute on this effort using our Operational Simplicity methodology that provides transparency to project champions via regular, comprehensive status updates. The result for the firm is the elimination of a serious threat and a hardening of their IT systems as a target for malicious attackers.

## *MCG brings decades of experience and a unique process to solve complex business problems.*

We believe that any business challenge can be solved via a sound process discipline and accountability.

MCG’s unique methodology combines elements of Six Sigma, Lean, TQM and Agile. Our approach has been proven to reduce costs, speed progress, and deliver results over many years of refinement and real-world implementation.

## *The MCG Operational SimplicityTM Process:*

* Increases the quality of deliverables
* Deploys most important features quickly
* Provides clients with high visibility into state of progress on a daily basis.
* Builds better systems based on hard information versus speculation
* Provides better estimates and predictable cost controls
* Provides superior control over timeframe and schedule

**Phone: 512-669-1576 | Matt.Merritt@MCGllc.net www.mcgllc.net**

