

Information Technology Security Metrics
The Information Technology Services Department
Claremont McKenna College
Date: July 2009

The Information Technology Services Department at Claremont McKenna College bases its information security protocols on the thirteen essential information security practices determined by the Corporate Information Security Working Group report's on the best practices and metrics team subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census (Revised January 10, 2005).¹

Of these thirteen essential information security practices, the Corporate Information Security Working Group identifies a set of "Fundamental Five" Minimum Essential Practices, which are considered collectively to be an appropriate minimum starting point for SMEs (Small and Medium Enterprises), defined by the U.S. Department of Commerce as having less than 500 employees. After achieving the Fundamental Five, SMEs are urged to develop a more mature information security program over time by achieving eight additional security milestones.

The "Fundamental Five" practices are:

1. Malware protection, including worms and viruses
2. Change management, including patch management
3. Identity and access management, including privilege assignment and authentication
4. Firewalls including workstation, host, sub-network, and perimeter as required
5. Configuration management

CMC is fully compliant with all "Fundamental Five" basic information security management practices recommended for SMEs. Of the remaining eight, we are fully compliant with four other suggested practices. We have also made excellent headway on the remaining practices of the thirteen baseline goals.

CMC Progress on the Thirteen Essential Information Security Practices

"Fundamental Five" Basic Information Security Management Practices:

1. Malware protection including Anti-virus software is installed on all systems. Signature updates and scans are performed automatically (daily). **ACHIEVED.** Sophos Virus protection runs on most of our servers and it is set to update automatically. The exceptions are our Microsoft Exchange servers, for which we use F Secure, which is also set to update automatically. For faculty and staff workstations, we use Trend Micro, which is set to update automatically, so that updates are applied automatically upon

1 <http://www.educause.edu/ir/library/word/CSD3661.doc>

receipt of virus signature files from the vendors. For students, via our Resident Technician Assistants, we enforce that all students must use an anti-virus system, but do not dictate which they choose.

2. A change management process is operational for all IT hardware and software. Changes are managed, deployed, and can be rolled back in accordance with a defined process. Security patches are subject to this process. **ACHIEVED.** Our Change Management Policy was formally adopted in May 2008.² We have implemented a thorough patch management system (HfNet Check Pro) to enforce patch management regularly. HfNetCheck is used to deploy all patches to server systems during scheduled, announced, server down-times.

3. In terms of privilege assignment and authentication, the organization has implemented various levels of electronic and physical protection for its information assets (information, systems, networks, applications) including critical assets requiring the greatest level of protection and oversight. Protection actions are based on some form of risk assessment. **ACHIEVED.** CMC's network is hierarchical and segmented into VLANs. Our VLAN segmentation allows us to isolate infected systems. CMC has implemented several network monitoring systems (What'sUpGold and OpManage) and we perform network monitoring with an alert system that informs us of any unusual activity.

4. Firewalls are used as an architectural component to at minimum separate public servers from internal organizational networks. Firewalls may also be used to separate internal sub-networks where access restriction is important. **ACHIEVED.** The main firewall, a Cisco ASA device, applies to any traffic coming into the campus from external sources. The Cisco ASA has a default setting to deny all incoming network traffic and only allow that traffic which is needed by a specific application. We require credentialing and access is allowed only via encrypted protocols. We have enabled firewalls on individual servers. We also maintain network access lists on all internal switches and routers.

5. A configuration management process is operational. All workstations, servers, laptops, routers, firewalls, and other network devices are built using a minimum essential configuration benchmark. This includes disabling all services that are not required, eliminating vendor supplied defaults for passwords, accounts, and security parameters, and continuous monitoring of system and device configuration status. **ACHIEVED.** We also enforce strong passwords with 380 days forced change.

Additional Minimum Recommended Standards:

6. Basic identity management mechanisms (authentication, authorization, access control) for access to both physical and electronic assets are implemented and regularly reviewed.

2 The Change Management Policy is located at:
<http://www.claremontmckenna.edu/its/Policies/ITPolicies/PDF/changemgmt.pdf>

This includes in-house access, remote access, and third party access. **ACHIEVED.** Wireless networks use Radius to achieve AAA functionality. Wired network admission control system, NetReg, provides simple NAC functions such as AD/Windows account to MAC/IP address translation. In addition to this, we use Trusted Network Technologies' Identity product to enforce granular Identity Management policies for access to administrative applications. Recent purchases will enable us to make further progress.

7. Information security policies are in force for acceptable use, incident response/reporting, and each of the baseline areas included in this document. Management visibly supports and enforces these policies. All users understand the consequences of non-compliance. **ACHIEVED.**³

8. Regular monitoring and review is conducted for: alert mechanisms, system logs for critical systems, firewall logs, incident reports, configuration violations; vulnerability assessment results; the overall security program. **ACHIEVED.** We have alert mechanisms in place, system logs, firewall logs, and incident reports and configuration violations. We have an internal Intrusion Prevention System, and we practice Netflow accounting as one of the methods to identify potential sources of malicious activities.

9. A business continuity plan is implemented and regularly tested. All critical assets are routinely backed up. Ability to selectively restore from backups is tested regularly. **Current situation at CMC:** We have fully fleshed out our 2009 Information Technology Services Disaster Situation Response and Data Protection Plan, but we do not have a full-blown business continuity plan. All critical assets are routinely backed up. Ability to selectively restore from backups is tested on a regular basis when we restore data for our clients, however, we have not yet implemented an official testing schedule. We back up every server and storage sub-system, and we suggest to all staff and faculty to save to their user drive so that all of their data is backed up. All databases, e-mail systems, and local server file systems undergo a daily full backup. All network attached storage undergo daily incremental backup, weekly full back up, monthly full back up, semi-

3 Relevant security policies are located at:

<http://www.claremontmckenna.edu/its/Policies/ITPolicies/PDF/pempeua.pdf>

<http://www.claremontmckenna.edu/its/Policies/ITPolicies/PDF/psuacca.pdf>

<http://www.claremontmckenna.edu/its/Policies/ITPolicies/PDF/ppupcmc.pdf>

<http://www.claremontmckenna.edu/its/Policies/ITPolicies/PDF/prnuse.pdf>

<http://www.claremontmckenna.edu/its/Policies/ITPolicies/PDF/ppupcuc.pdf>

annual and annual full back up.⁴ In terms of automation, we have a Dell PowerVault ML6010 Control Module, LTO-3 1- Drive SCSI, Redundant Power, 5U-R with a networker autochanger with all necessary Legato software and licensing. We have backward capability to read tapes located at our secure off-site storage site at Iron Mountain.

10. All users are required to attend security awareness training prior to being granted access to the organization's networks and periodically as condition of continued access. **Current situation at CMC:** For students, ITS receives confirmation via our Jenzabar CX system that a student has been admitted to the College. ITS creates network accounts for all students. Before being granted access to the network, students are required to attend security awareness training. For each new staff and faculty member, Human Resources personnel fill out a standard form and then submit a formal, written request for additions and deletions electronically to ITS via our Helpdesk software, Footprints. We do not require users to attend security awareness training periodically as a condition of continued access, but we do widely distribute information to the community and we also enforce security protocols.

11. All information security management, technical, and user roles and responsibilities are explicitly assigned and assignments acknowledged. **Current situation at CMC:** We do not have a dedicated information security position, however, the responsibilities are divided among ITS personnel and assignments acknowledged.

12. Compliance with external (legal, regulatory) requirements is regularly demonstrated via internal and external audit. Audit findings are resolved in a timely manner. **Current situation at CMC:** We undergo a fairly minimal external audit, and we have not had staff to devote to many of these issues. However, we do work in concert with in-house counsel to ensure we fulfill external requirements. As but one example, we helped craft our Red Flag Policy, and we use a third-party vendor (IATS) to process secure online transactions to minimize risk. Every incident is explained in detail to affected community members according to our Incident Management protocols.

13. The practices noted above are required in all third party service level agreements for those parties having access to organizational networks. **ACHIEVED.**

4 Please see here for our Backup policy:
<http://its.claremontmckenna.edu/Policies/ITPolicies/PDF/psrbcka.pdf>