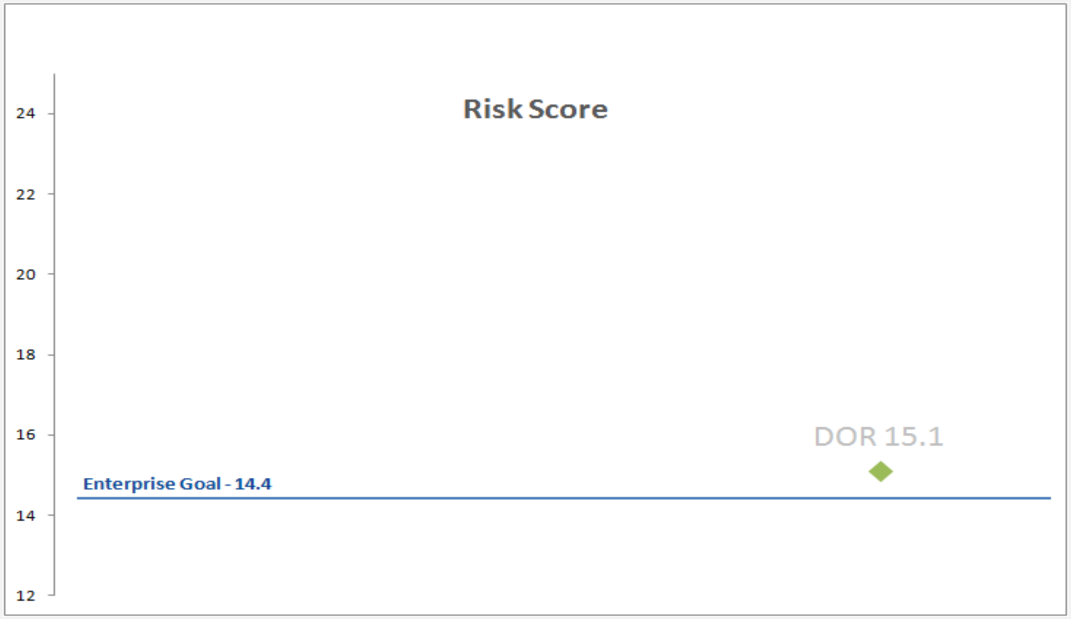
Sample Security Risk Report

Deborah Blyth - CISO

COLORADO
Information Security
Governor's Office of Information Technology



Risk Score: **15.1**

You are ranked 15 for risk out of the 16 agencies OIT supports. One agency has a lower risk score.

Risks Mitigation

Critical ways to reduce your agency risk

1. Make remediation of the top 10 vulnerabilities a weekly priority
2. Update and tighten firewall infrastructure
3. Work with OIT to implement a strong vendor management oversight program
3. Work with OIT to obtain database encryption
3. Work with OIT to ensure all staff are trained on cyber security

70%

Compliance with Hardening standards

150

Open IT Audit Findings

2

82% of threats remediated of

1181

threats detected

0%

# of Staff Trained

Risk Report Card Reference Guide

OIT
COLORADO
Information Security
Governor's Office of Information Technology

Your Risk Score Explained

Risk is defined as the potential of a threat to exploit vulnerabilities of an asset and cause damage or unintended consequence. OIT has implemented the McAfee Risk Advisor for consolidated agencies for both qualitative and quantitative approaches to describe the nature of the risk and the associated numerical values. The risk score is directly proportional to certain attributes such as applicability, vulnerability, and criticality, and inversely proportional to protection or countermeasure presence.

For example, the risk score for an asset increases if an identified threat in the OIT environment is applicable to the asset, the asset is vulnerable, or the asset criticality is High. When OIT puts a countermeasure in place such as security hardening of the servers and desktops / laptops, and consistent and up to date patching, the result of implementing that countermeasure is a reduction in the risk score.

Each system that has been integrated into the McAfee solution receives a risk score from 0 to 100, 0 indicating that there is no risk to the system and 100 indicating the highest level of risk to the system.

< 20 = Low Risk
>20 - < 60 = Medium Risk
> 60 = High Risk

Compliance and Hardening Standards

The CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia.

The Benchmarks are:

- Recommended technical control rules/values for hardening operating systems, middleware and software applications, and network devices.
- Unique, because the recommendations are defined via consensus among hundreds of security professionals worldwide.

Audit Findings

Outstanding audit findings cover areas such as general computer controls, federal and state compliance, penetration and vulnerability assessments, and state policy violations.

Threats Remediated vs. Detected

Threats to the desktops, laptops and servers include but are not limited to Malware, Viruses, Hoax (pop up ads), PUP (potentially unwanted programs), Trojans and malicious behavior at the endpoints.

While McAfee detects the threats, remediation of the threats is dependent on the policies that have been put in place at each department. For higher remediation percentages, stricter security policies will have to be implemented.

Cyber Security Awareness Training

Cyber security awareness is the first line of defense for any department against insider threats, social engineering and unintentional security breaches. The CISO has a goal of training 95% of all staff in the consolidated agencies by June 30, 2016.

Patching Levels

Patching is the easiest and most effective way to prevent viruses and malware from infecting the desktops / laptops and servers that support your business. 99% of the attacks that hackers use leverage weaknesses that could be fixed with existing patches.

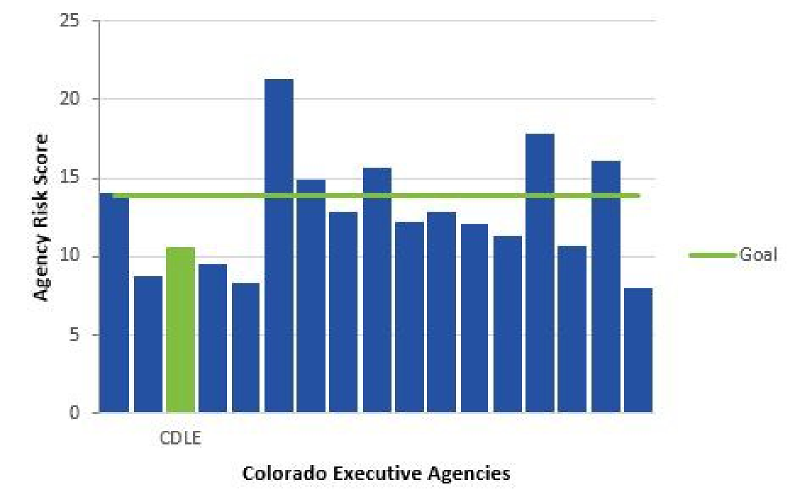
Once a patch has been released, it's usually reverse engineered in order to create an exploit. This will take anywhere from 24-hours to 4 days. You have this period of time to ensure that your system is patched and therefore immune from any exploit that is subsequently created.

Department of Labor & Employment

COLORADO
Information Security
Governor's Office of Information Technology

IT Security Risk Report

Deborah Blyth, Colorado Chief Information Security Officer



CDLE Risk Score: **10.58**

Recommended Mitigation

Highest-Impact Risk Reduction Strategies

- Review encryption needs with OIT Security Team
  - Encryption minimizes impact of data breaches
- Maintain up-to-date systems
  - Refresh outdated systems
  - Retire old, unsupported systems
- Promote Security Awareness Training. Both Module 1 and Module 2 training still need to be completed for the agency. All modules should be 100% complete.
  - Module 1 - 89% Complete
  - Module 2 - 73% Complete

33%
Compliance
State Hardening Standards

98
Open IT
Audit Findings

98%
threats remediated of
107,551 detected

98%
System Patching

Your Risk Score Explained

What is “risk”?

Risk is defined as the **potential of a threat** to exploit vulnerabilities of an asset and cause damage or unintended consequence.

How is OIT measuring risk?

OIT has implemented the **McAfee Risk Advisor** to calculate a “Risk Score”, based on both qualitative and quantitative data.

Scoring

- Each asset in the environment has a **risk score from 0 to 100** (0 indicating no risk and 100 indicating the highest possible level of risk)
- **Calculated** based on
  - applicability
  - vulnerability
  - criticality
  - countermeasure presence (ex: security hardening of servers and desktops, as well as up-to-date patching, will reduce an asset’s risk score)
- **Scale**

  < 20 = Low Risk
  >20 - < 60 = Medium Risk
  > 60 = High Risk

Your Report Explained

COLORADO
Information Security
Governor's Office of Information Technology

Compliance and Hardening Standards

What is hardening?
Hardening is the process of securing a system by reducing its surface of vulnerabilities.

Why compliance matters
OIT holds the state accountable for meeting best practice levels of cyber security controls that safeguard Colorado data and systems from threats.

What standards are we complying with?
OIT holds its customers to comply with the Center for Information Security (CIS) Benchmarks https://benchmarks.cisecurity.org/, which are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia. OIT currently requires systems to be 60% compliant with a 100% goal in future.

Open Audit Findings

What is included in this number?
For the purpose of this report, Open Audit Findings include general computer controls, federal and state compliance, penetration and vulnerability assessments, and state policy violations

Why open audit findings matter?
Audit findings help identify risks in the environment. Non remediated audit findings can lead to breaches, sanctions, loss of goodwill and other legal matters.

Your Report Explained

Threats Remediated/Detected

What is a threat?
A threat is a possible danger that could cause possible harm.

Threats to the desktops, laptops and servers include but are not limited to Malware, Viruses, Hoax (pop up ads), PUP (potentially unwanted programs), Trojans and malicious behavior at the endpoints.

How is a threat detected?
The McAfee Risk Advisor tool detects threats in the environment based on the user activity in a system. If a user download a malicious file, it will be detected by the McAfee tool.

How is a threat remediated?
While McAfee detects the threats, remediation of the threats is dependent on the technical configuration that have been put in place at each department. For example, if a malicious file is downloaded, but an agency has an appropriate technical configuration, the download would be quarantined and deleted automatically without any user interaction.

How can my agency remediate more threats?
Stricter technical security configuration must be implemented. You can achieve this by ensuring all projects with a technical component go through OIT's gating process and working with OIT's Information Security Team, who can help educate staff to integrate configuration standards.

Are threats prioritized according to risk? How do I know which are most critical?
McAfee uses global threat intelligence to assign risks to the threats identified.

Your Report Explained

Patching Levels

What is a patching?
A patch is a software update that improves the software's function, including updates that mitigate security vulnerabilities and system bugs. A patch typically takes 1-4 days to become effective in your system.

Why is patching important to security?
Patching is the easiest and most effective way to prevent viruses and malware from infecting the desktops / laptops and servers that support your business.

99% of the attacks that hackers use leverage weaknesses that could be fixed with existing patches.