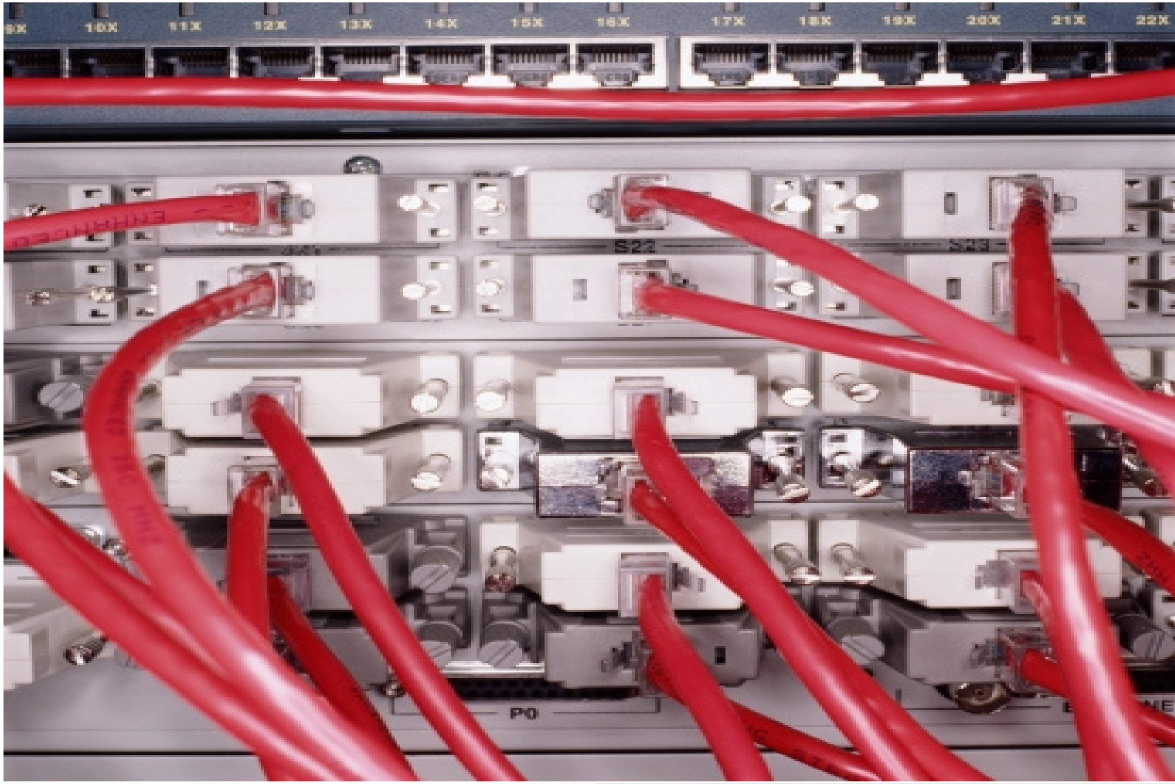
CATALYST
TECHNOLOGY GROUP
Innovating how IT is delivered.sm

Cyber Risk Assessment

Compensating Control Worksheet



CONFIDENTIALITY NOTE: The information contained in this report is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If you are not the client or addressee, you are strictly prohibited from reading, photocopying, distributing, or otherwise using this report or its contents in any way.

Prepared for:
Your Customer / Prospect
Prepared by:
Your Company Name

Table of Contents

1 Potential password strength risks

Local account passwords on 2 accounts were found to be potentially weak. Inadequate or weak passwords on local accounts can allow a hacker to compromise the system. It can also lead to the spread of malicious software that can cause business and productivity affecting issues.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
False Positive

2 Unsupported Operating Systems

Computers found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
Review Individual Entries

MYCOPATCH / 10.0.7.55 / Windows 2000 Server

Response
Mitigated through Compensating Control

Follow-up: MYCOPATCH / 10.0.7.55 / Windows 2000 Server

Enter Compensating Control

Response
We put a lot of antivirus and antispyware

ISA1 / 10.0.1.6 / Windows Server 2003 R2

Response
False Positive

REMOTE / 10.0.7.68 / Windows 2000 Server

Response
Valid

JAGA / 10.0.7.67 / Windows Server 2003

Response
Valid

PABUILD / 10.0.7.60 / Windows Server 2003

Response
Valid

THRASH2 / 10.0.1.33 / Windows 2000 Server

Response
Valid

MYCO-ATL-CORE / 10.0.1.17 / Windows Server 2003 R2

Response
Valid

DEVWIKI / 10.0.7.62 / Windows Server 2003

Response
Valid

MYCO30DEV / 10.0.7.65 / Windows 2000

Response
Valid

MmayhemON1 / 10.0.7.31 / Windows Vista (TM) Business

Response
Valid

3 Anti-spyware not installed

Anti-spyware software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

4 Anti-virus not installed

Anti-virus software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

5 Anti-virus not turned on

We were unable to determine if anti-virus software is enabled and running on some computers.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
Valid

6 Anti-spyware not turned on

We were unable to determine if anti-spyware software is enabled and running on some computers.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
Valid

7 Excessive security patches missing on computers

Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Lots is defined as missing four or more patches.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
Valid

8 Anti-spyware not up to date

Up to date anti-spyware definitions are required to properly prevent the spread of malicious software. Some anti-spyware definitions were found to not be up to date.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

9 Anti-virus not up to date

Up to date anti-virus definitions are required to properly prevent the spread of malicious software. Some anti-virus definitions were found to not be up to date.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
Valid

10 Potential disk space issue

2 computers were found with significantly low free disk space.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
Valid

11 Significantly high number of Domain Administrators

More than 30% of the users are in the Domain Administrator group and have unfettered access to files and system resources. Compromised Domain Administrator accounts pose a higher threat than typical users and may lead to a breach.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

12 User password set to never expire

User accounts with passwords set to never expire present a risk of use by unauthorized users. They are more easily compromised than passwords that are routinely changed.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
Valid

13 Operating system in Extended Support

Computers are using an operating system that is in Extended Supported. Extended Support is a warning period before an operating system is no longer supported by the manufacturer and will no longer receive support or patches.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

14 Inactive computers

Computers have not checked in during the past 30 days.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

15 User has not logged on to domain in 30 days

Users have not logged on to domain in 30 days. A user that has not logged in for an extended period of time could be a former employee or vendor.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

16 Un-populated organization units

Empty organizational units (OU) were found in Active Directory. They may not be needed and can lead to misconfiguration.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

17 Insecure listening ports

Computers are using potentially insecure protocols.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
Review Individual Entries

RANCOR.Corp.MyCo.com (10.0.7.57)

Response
Mitigated through Compensating Control

Follow-up: RANCOR.Corp.MyCo.com (10.0.7.57)

Enter Compensating Control

Response
This one is OK

MYCO30dev.Corp.MyCo.com (10.0.7.65)

Response
Valid

ISA1.Corp.MyCo.com (10.0.7.43)

Response
Valid

pitmacmini.corp.MyCo.com (10.0.7.45)

Response
Valid

10.0.7.64

Response Valid

hp2100-ops.corp.MyCo.com (10.0.7.76)

Response Valid

10.0.7.70

Response Valid

18 Critical External Vulnerabilities Detected

Critical external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
Valid

19 Medium severity external vulnerabilities detected

Medium severity external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
Valid

20 Password complexity not enabled

Enforcing password complexity limits the ability of an attacker to acquire a password through brute force.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

21 Inconsistent password policy / Exceptions to password policy

Password policies are not consistently applied from one computer to the next. A consistent password policy ensure adherence to password best practices.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

22 Open or insecure WiFi protocols available

Open or insecure WiFi protocols may allow an attacker access to the company's network and resources.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Mitigated through Compensating Control

Enter Compensating Control

Response These wifi are safe.

23 Verified incorrect response: high risk internal vulnerabilities detected

You indicated that systems in your internal environment are secure; however, some high-risk vulnerabilities were found.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

24 Verified incorrect response: high risk external vulnerabilities detected

You indicated that systems in your Internet/DMZ environment are secure; however, an external vulnerability scan found issues with CVSS scores greater than 4 indicating a high risk.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid

25 Verified incorrect response: Unsupported Operating Systems found

You indicated that the company does not use software or hardware that has been officially retired; however, some computers with Operating Systems considered “end-of-life”.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response
Review Individual Entries

DEVWIKI / 10.0.7.62 / Windows Server 2003

Response
Valid

ISA1 / 10.0.1.6 / Windows Server 2003 R2

Response
False Positive

JAGA / 10.0.7.67 / Windows Server 2003

Response
Valid

MmayhemON1 / 10.0.7.31 / Windows Vista (TM) Business

Response
Valid

MYCO30DEV / 10.0.7.65 / Windows 2000

Response
Valid

MYCO-ATL-CORE / 10.0.1.17 / Windows Server 2003 R2

Response
Valid

MYCOPATCH / 10.0.7.55 / Windows 2000 Server

Response
Mitigated through Compensating Control

Follow-up: MYCOPATCH / 10.0.7.55 / Windows 2000 Server

Enter Compensating Control

Response
It has a lot of protection

PABUILD / 10.0.7.60 / Windows Server 2003

Response
Valid

REMOTE / 10.0.7.68 / Windows 2000 Server

Response
Valid

THRASH2 / 10.0.1.33 / Windows 2000 Server

Response
Valid

26 Verified incorrect response: Missing updated anti-virus

You indicated that anti-virus is installed and updated on computer systems in the network; however, some computers were detected as not having updated anti-virus.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Response Valid