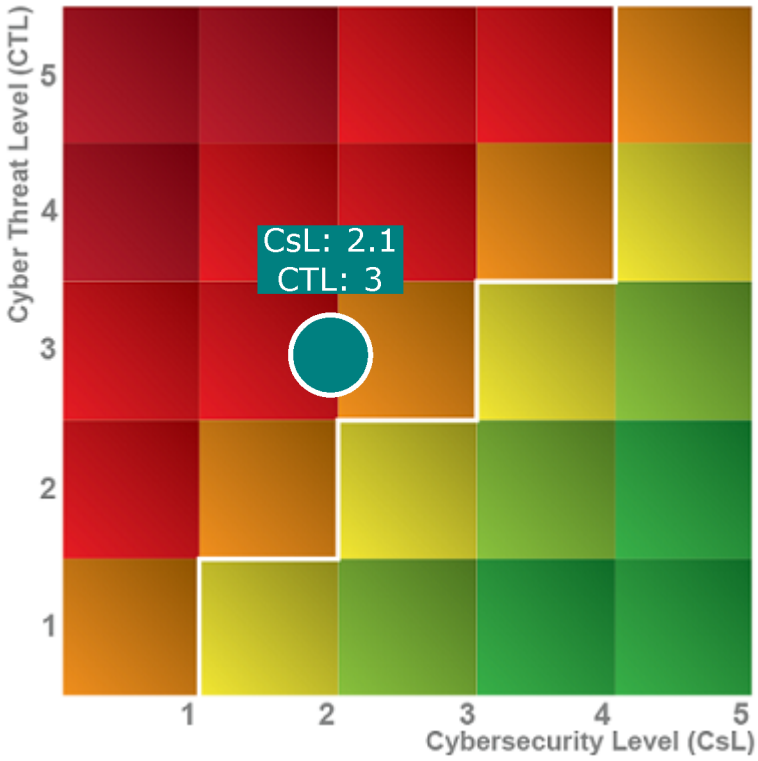
Cyber RiskScope™

Results for Telco Co

Your Cyber Risk Profile

The Cyber Risk Profile is designed to quickly provide a visual indication of your cybersecurity risk. In the Cyber RiskScope™ methodology, your Cybersecurity Level (CsL) should be equal to or greater than your Cyber Threat Level (CTL) in order to provide the minimum recommended cyber protection. This minimum recommended protection is represented by the white “stair step” line on the Cyber Risk Profile. Moving further to the left of this line (more towards the red) indicates increasing risk, while moving further to the right (more towards the green) indicates decreasing risk.

The CTL scale is based on open-source, cyber incident data that is collected on a daily basis and correlated to industries. A higher CTL simply means that recent activity indicates an industry is experiencing a higher degree of cyber incidents and therefore warrants a higher level of protection (or CsL) to mitigate the threat. SelfAssure uses the industry you selected in your profile to establish your CTL. More advanced CTL assessments are available via Cyber RiskScope™ QuickLook and DeepDive assessments.

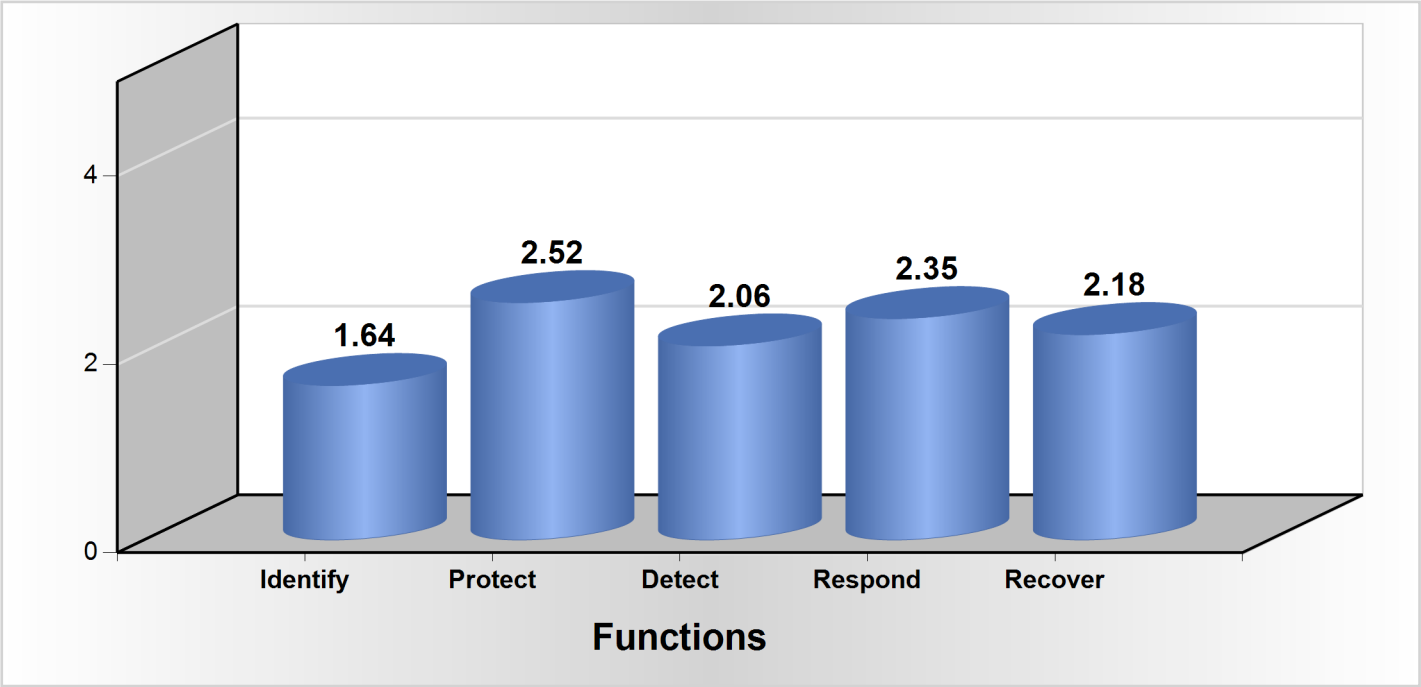


The following table provides definitions for the CsL Scale.

Weak (1.0)	Limited (2.0)	Effective (3.0)	Strong (4.0)	Very Strong (5.0)
Weak or non-existent security posture; likelihood and impact of successful exploitation is extremely high; requires urgent attention	Limited or poorly integrated security posture, large gaps exist; likelihood and impact of successful exploitation is high; requires immediate attention	Reasonable security posture, lacks formality and consistency, gaps exist; likelihood and impact of successful exploitation is moderate; requires priority attention	Strong security posture, integrated and managed, some layered defense; likelihood and impact of successful exploitation reduced; requires attention and continuous monitoring	Very strong security posture, best-in-class and continuous improvement incorporated; likelihood and ipact of successful exploitation is minimal; requires continuous monitoring

Cybersecurity Results By Function

This composite score is based on how you score within the 5 core Functions of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond and Recover).



Identify 1.64

The Identify Function includes understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Identify covers Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

Category	Name	
Risk Assessment (ID.RA)	ID.RA-1	1.5
	ID.RA-2	1.7
	ID.RA-3	3.1
	ID.RA-4	1.1
	ID.RA-5	2.5
	ID.RA-6	2.5
Business Environment (ID.BE)	ID.BE-1	0.0
	ID.BE-2	5.0
	ID.BE-3	0.0
	ID.BE-4	1.7
	ID.BE-5	0.0
Risk Management Strategy (ID.RM)	ID.RM-1	0.0
	ID.RM-2	0.0
	ID.RM-3	1.0
Governance (ID.GV)	ID.GV-1	5.0
	ID.GV-2	4.0
	ID.GV-3	5.0
	ID.GV-4	0.0
Asset Management (ID.AM)	ID.AM-1	2.5
	ID.AM-2	2.5
	ID.AM-3	3.0
	ID.AM-4	2.0
	ID.AM-5	0.0
	ID.AM-6	1.4

Protect 2.52

The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Protect covers Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

Category	Name	
Access Control (PR.AC)	PR.AC-1	1.8
	PR.AC-2	1.9
	PR.AC-3	3.6
	PR.AC-4	0.0
	PR.AC-5	3.5
Data Security (PR.DS)	PR.DS-1	1.8
	PR.DS-2	2.5
	PR.DS-3	1.7
	PR.DS-4	5.0
	PR.DS-5	0.0
	PR.DS-6	3.0
	PR.DS-7	1.7
Maintenance (PR.MA)	PR.MA-1	2.5
	PR.MA-2	2.5
Information Protection Processes and Procedures (PR.IP)	PR.IP-1	2.3
	PR.IP-2	0.0
	PR.IP-3	1.1
	PR.IP-4	2.3
	PR.IP-5	1.7
	PR.IP-6	3.5
	PR.IP-7	5.0
	PR.IP-8	2.2
	PR.IP-9	1.6
	PR.IP-10	1.8
	PR.IP-11	3.5
	PR.IP-12	2.3
Protective Technology (PR.PT)	PR.PT-1	2.1
	PR.PT-2	3.5
	PR.PT-3	3.7

	PR.PT-4	5.0
Awareness and Training (PR.AT)	PR.AT-1	4.0
	PR.AT-2	4.0
	PR.AT-3	4.0
	PR.AT-4	4.0
	PR.AT-5	2.0

Detect 2.06

The Detect Function enables timely discovery of cybersecurity events. Detect is concerned with processes for handling Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

Category	Name	
Security Continuous Monitoring (DE.CM)	DE.CM-1	2.2
	DE.CM-2	1.9
	DE.CM-3	2.2
	DE.CM-4	1.7
	DE.CM-5	2.5
	DE.CM-6	1.0
	DE.CM-7	2.5
	DE.CM-8	1.0
Anomalies and Events (DE.AE)	DE.AE-1	2.2
	DE.AE-2	2.5
	DE.AE-3	1.9
	DE.AE-4	2.7
	DE.AE-5	1.2
Detection Processes (DE.DP)	DE.DP-1	2.2
	DE.DP-2	2.2
	DE.DP-3	1.9
	DE.DP-4	2.3
	DE.DP-5	1.0

Respond 2.35

The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Respond is concerned with Response Planning, Communications, Analysis, Mitigation, and Improvements.

Category	Name	
Mitigation (RS.MI)	RS.MI-1	3.5
	RS.MI-2	3.5
	RS.MI-3	2.4
Analysis (RS.AN)	RS.AN-1	3.5
	RS.AN-2	1.0
	RS.AN-3	2.5
	RS.AN-4	2.3
Improvements (RS.IM)	RS.IM-1	2.3
	RS.IM-2	2.3
Communications (RS.CO)	RS.CO-1	2.3
	RS.CO-2	3.1
	RS.CO-3	2.2
	RS.CO-4	2.3
	RS.CO-5	1.7
Response Planning (RS.RP)	RS.RP-1	2.3

Recover 2.18

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Recover is concerned with Recovery Planning, Improvements, and Communications.

Category	Name	
Improvements (RC.IM)	RC.IM-1	2.3
	RC.IM-2	2.3
Recovery Planning (RC.RP)	RC.RP-1	2.9
Communications (RC.CO)	RC.CO-1	0.0
	RC.CO-2	2.3
	RC.CO-3	0.0

Weaknesses and Mitigation Strategies

Based on your answers, these are our findings.

Legend

Cultural Impact		Financial Impact		SW / HW Required	
☹	High	$$$	High	✔	Yes
😐	Moderate	$$	Moderate	?	Maybe
☺	Low	$	Low	✖	No

Identify

ID	Weakness
98	By not maintaining an inventory of all hardware on the network, your organization is unaware of unauthorized or unmanaged devices and is therefore unable to remove them in a timely manner and prevent them from gaining access to the network.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Low	✔	?	☺	$$

Mitigation Strategy

Actively manage all hardware devices on the network using an automated, on schedule implementation so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s). Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.
Deploy dynamic host configuration protocol (DHCP) server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information.
Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.

ID	Weakness
124	If you don't manage configuration changes to the information system, vulnerabilities could be introduced that puts your organization at risk of compromise.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Moderate	✖	✖	😐	$

Mitigation Strategy

	Manage configuration changes to your information systems by: - Requiring a security impact analysis to determine potential security impacts prior to change implementation - Requiring approval for configuration-controlled changes - Documenting approved configuration-controlled changes - Retaining records of configuration-controlled changes - Auditing the activities associated with configuration-controlled changes
ID	Weakness
158	If you don't manage configuration changes to network devices, vulnerabilities could be introduced that puts your organization at risk of compromise.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Moderate	✖	✖	☺	$

Mitigation Strategy
Manage configuration changes to your network devices by: - Requiring a security impact analysis to determine potential security impacts prior to change implementation - Requiring approval for configuration-controlled changes - Documenting approved configuration-controlled changes - Retaining records of configuration-controlled changes - Auditing the activities associated with configuration-controlled changes

ID	Weakness
141	Failure to develop terms and conditions for authorized people to process, store, or transmit company-controlled information externally, severely limits your ability to manage the security of your data. Additionally, it prevents you from effectively communicating the level of security you expect from authorized personnel.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Moderate	✖	✖	☺	$

Mitigation Strategy
Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: - Access the information system from external information systems; and - Process, store, or transmit organization-controlled information using external information systems. Restrict access to your information systems externally to only authorized personnel.

ID	Weakness
142	Not forcing external information system service providers to comply with your information security policies renders them ineffective.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Moderate	✖	✖	☺	$

Mitigation Strategy
Require external information system services to comply with organizational information security requirements and employ security controls that you have identified as necessary to maintain your information system at an acceptable level of risk.

ID	Weakness
143	External service providers that are not required to implement security controls in accordance with some form of governance may not adequately protect the information that you entrust to them.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact

	Moderate	✖	✖	☺	$
	Mitigation Strategy				
	Ensure that external service providers are required to meet a level of security that meets or exceeds your acceptable level of risk or at a minimum, those security controls mandated by federal laws, regulations and standards.				

Protect

ID	Weakness				
41	Failure to patch operating systems on a regular basis to the latest version leaves your organization vulnerable to a host of possible exploits that have been identified by the manufacturer and eliminated or mitigated through release of the patch. Cyber adversaries are keenly aware of these vulnerabilities and continually scan the internet for such weaknesses.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	High	?	?	☺	$$
	Mitigation Strategy				
	Implement a patch management program that includes a systematic approach to periodic patching of installed operating systems. A systematic approach implies pre-testing of patches in a sandbox or on isolated systems prior to full production deployment.				
ID	Weakness				
45	Unsupported operating systems, by definition, do not receive updates or patches. Numerous vulnerabilities exist on unsupported operating systems that are never going to be eliminated or mitigated by the manufacturer and present an easy target for even the least experienced cyber adversary.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	High	✔	✖	☺	$$
	Mitigation Strategy				
	Eliminate all unsupported operating systems from the organization. If absolutely necessary for hosting outdated applications that can't be upgraded, ensure these systems are not accessible remotely through the network or through a wireless connection. If possible, limit and manage physical access to the system.				
ID	Weakness				
46	Unsupported operating systems, by definition, do not receive updates or patches. Numerous vulnerabilities exist on unsupported operating systems that are never going to be eliminated or mitigated by the manufacturer and present an easy target for even the least experienced cyber adversary.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	High	✔	✖	☺	$$
	Mitigation Strategy				
	Even at less than 1% of your enterprise, consideration should be taken to eliminate all unsupported operating systems from the organization. If absolutely necessary for hosting outdated applications that can't be upgraded, ensure these systems are not accessible remotely through the network or through a wireless connection. If possible, limit and manage physical access to the system.				
ID	Weakness				
50	User applications are a prime target for cyber adversaries. Failure to harden the configurations of user applications could allow an attacker access to your enterprise.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	High	✖	✖	😐	$
	Mitigation Strategy				

	Ensure the configuration of user applications is restricted to only needed features.
ID	Weakness
65	Failure to segment the organizations valuable assets, such as internet-facing hosts, into separate security zones may allow cyber adversaries to propagate throughout your network as part of the second stage of a cyber intrusion.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
High	?	✔	☺	$$$

Mitigation Strategy

Network segmentation involves partitioning the network into smaller networks. Network segregation involves developing and enforcing a ruleset controlling which workstations and servers are permitted to communicate with which other workstations and servers.
Network segmentation and segregation should be based on the connectivity required, user job role, business function, trust boundaries and sensitivity of information stored.
Network controls that can assist with implementing network segmentation and segregation include switches, virtual LANs, enclaves, data diodes, firewalls, routers and Network Access Control.
Constrain VPN and other remote access, wireless connections, as well as user-owned laptops, smartphones and tablets which are part of a “Bring Your Own Device” implementation.
Organizations using operating system virtualization, (especially third party) cloud computing infrastructure, or providing users with “Bring Your Own Device” or remote access to the organization's network, might require controls that are less dependent on the physical architecture of the network. Such controls include personal firewalls and “IPsec Server and Domain Isolation”.
The use of IPsec provides flexible network segmentation and segregation. For example, IPsec authentication can ensure that a specific network port or ports on a sensitive server can only be accessed by specific workstations such as those workstations belonging to administrators.
Sensitive servers such as Active Directory and other authentication servers should only be able to be administered from a limited number of intermediary servers referred to as “jump servers”. Jump servers should be closely monitored, be well secured, limit which users and network devices are able to connect to them, and typically have no Internet access. Some jump servers might require limited Internet access if they are used to administer defined workstations or servers located outside of the organization's local network.
Organizations with critically sensitive information might choose to store and access it using air-gapped workstations and servers that are not accessible from the Internet. Security patches and other data can be transferred to and from such air gapped workstations and servers in accordance with a robust media transfer policy and process.

ID	Weakness
75	Failure to implement and properly configure a web application firewall increases the possibility of web-based attacks such as cross-site scripting and SQL injection that Intrusion Prevention System's cannot prevent.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Moderate	✖	✔	☺	$$

Mitigation Strategy

Implement and properly configure a web application firewall to protect your internet-facing web applications.

ID	Weakness
89	A company that doesn't enforce a strong passphrase policy is at risk of having their passwords compromised by even the most unsophisticated cyber adversary.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
High	✖	✖	☹	$

	Mitigation Strategy
	Enforce a strong passphrase policy covering complexity, length, expiry, and avoiding both passphrase reuse and the use of a single dictionary word. This is especially important for service accounts and all other accounts with administrative privileges. It is more challenging for cyber adversaries to crack passphrase hashes and propagate throughout an organization's network as part of the second stage of a cyber intrusion if passphrases are complex, long and hashed with a cryptographically strong algorithm.
ID	Weakness
153	If users are not required to periodically change their login password, a compromised password can allow a cyber adversary to persist on the enterprise indefinitely.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
High	✗	✗	😐	$

Mitigation Strategy
Develop and enforce policy that requires users to change their passwords on a periodic basis. The industry best practice is at least every 6 months.

ID	Weakness
93	Although your organization performs training semi-annually, an organization that doesn't conduct IT security awareness training quarterly increases their risk of compromise by failing to continually educate their most easily susceptible weakness…their employees.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
High	?	✗	☺	$$

Mitigation Strategy
Educate users at least quarterly, especially Most Likely Targets, about Internet threats such as identifying spear phishing socially engineered emails or unexpected duplicate emails, and reporting such emails to the IT security team. Users should also report suspicious phone calls, such as unidentified callers attempting to solicit details about the organization's IT environment. Such education should focus on influencing user behavior.

ID	Weakness
100	Defense of your network requires constant attention due to the continuously changing threat. Although you continuously monitor, failure to monitor the effectiveness of implemented security mechanisms on at least a monthly basis may increase your risk to the latest vulnerabilities.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Moderate	✓	?	😐	$$$

Mitigation Strategy
Implement a monthly examination of your security posture that includes: - Testing the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker. - Continuously acquiring, assessing, and taking action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. - Establishing, implementing, and actively managing (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

ID	Weakness

169	Failure to approve and monitor all work and diagnostic activities of maintenance activities performed remotely could lead to vulnerabilites introduced to your enterprise without your knowledge.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Moderate	✗	✗	☺	$

Mitigation Strategy
Ensure all maintenance activities performed remotely are monitored and approved prior to the work being performed.

ID	Weakness
170	Failure to maintain work records of diagnostic activities for maintenance work performed remotely could prevent you from identifying the cause of an exploited vulnerability.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Moderate	✗	✗	☺	$

Mitigation Strategy
Ensure all maintenance and diagnostic activities performed remotely are captured in a log for after-the-fact analysis of an incident.

ID	Weakness
119	Not managing a list of personnel authorized to access the areas where your information systems are located significantly increases your vulnerability to social engineering attacks and reduces the effectiveness of existing layered defenses.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Moderate	✗	✗	☺	$

Mitigation Strategy
Review the list of personnel authorized to access the areas where your information systems are located at least quarterly. To properly manage physical access authorizations, the organization should: - Develop and keep a current list of personnel with authorized access to the facility - Issue authorization credentials - Review and approve the access list and authorizations credentials at least quarterly, removing personnel no longer requiring access

ID	Weakness
126	Failure to provide automatic emergency lighting to guide people to exits could result in injury to personnel during power outages.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Low	✗	✓	☺	$$

Mitigation Strategy
The organization should employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

ID	Weakness
127	Although automatic fire detection is installed, failure to implement automatic fire suppression could result in damage/injury to equipment/personnel.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact

	Low	✗	✓	☺	$$$
	Mitigation Strategy				
	The organization should employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detector				
ID	Weakness				
133	Failure to properly locate/install information systems in a facility could result in potential damage from physical and environmental hazards or provide an opportunity for unauthorized access.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	Low	✗	✗	☺	$
	Mitigation Strategy				
	Position information system components within the facility to minimize potential damage from physical and environmental hazards and minimize the opportunity for unauthorized access. Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations should consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications.				

Detect

ID	Weakness				
163	Users may inadvertently open malicious emails if your implemented security mechanisms aren't capable of analyzing them prior to delivery to the user.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	Moderate	✔	?	☺	$$
	Mitigation Strategy				
	Implement a security mechanism that is capable and configured to analyze emails prior to delivery to users.				
ID	Weakness				
63	Failure to install Host-Based Intrusion Prevention/Detection systems on servers prevents the organization from detecting malware that has yet to be identified by vendors.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	Moderate	✔	?	☺	$$
	Mitigation Strategy				
	Configure the Host-Based Intrusion Prevention/Detection systems to achieve an acceptable balance between identifying malware, while avoiding negatively impacting users and your organization's incident response team due to false positives. Endpoint protection or anti-malware software from some vendors includes HIDS/HIPS functionality.				
ID	Weakness				
64	Failure to install Host-Based Intrusion Prevention/Detection systems on all servers prevents the organization from detecting malware that has yet to be identified by vendors.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	Moderate	✔	?	☺	$$
	Mitigation Strategy				
	Although more than half your servers have this technology installed currently, it is recommended that you install this technology on all your servers beginning with servers that have the most sensitive data first. Configure the Host-Based Intrusion Prevention/Detection systems to achieve an acceptable balance between identifying malware, while avoiding negatively impacting users and your organization's incident response team due to false positives. Endpoint protection or anti-malware software from some vendors includes HIDS/HIPS functionality.				
ID	Weakness				
76	Failure to review and analyze workstation audit logs in real time by full time analysts prevents you from identifying and possibly preventing a cyber attack at the earliest possible stages.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	Moderate	?	?	☺	$$$
	Mitigation Strategy				
	We recommend all workstation audit logs are reviewed and analyzed in real time by full time security analysts.				

ID	Weakness
78	Reviewing and analyzing network device audit logs on an ad hoc basis leaves you vulnerable to full-scale cyber attacks that go unnoticed until the damage is done.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
Moderate	?	?	☺	$$$

Mitigation Strategy

Although you currently review and analyze network device audit logs on an ad hoc basis, we recommend all server audit logs are reviewed and analyzed in real time by full time security analysts.

ID	Weakness
97	An organization that doesn't capture and store network traffic severely limits it ability to determine the techniques used by cyber adversaries, and to assess the extent of damage sustained if a cyber intrusion occurs.

Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
High	✔	✔	☺	$$$

Mitigation Strategy

Capture network traffic to/from internal critical asset workstations and servers, as well as traffic traversing the network perimeter, and store it for at least 18 months to allow performance of post-intrusion analysis.
Focus on capturing traffic from workstations and servers on internal networks that store or access sensitive information. Preferably also capture traffic from the network perimeter, noting that its usefulness is diminished by exfiltrated data typically being encrypted and sent to a computer that probably can’t be attributed to cyber adversaries.
Ensure that users are aware that network traffic on the organization's network is monitored for security purposes.
When a successful cyber intrusion occurs, retain a copy of network traffic for several days prior to remediation, as well as for several days following remediation during which time cyber adversaries are likely to attempt to regain access to the organization's network.
Metadata relating to network connections can complement logging, and consumes less storage space than network packets.

Respond

ID	Weakness				
160	Failure to reach out to other groups in the security community to get training and share information could result in an inaccurate understanding of the threat and the inability to learn from others that have similar security needs to yours.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	Low				
	Mitigation Strategy				
	Reach out to other groups in the security community to get training, share information and stay up to date.				

Recover

ID	Weakness				
104	Although you retain backups of critical data for a full quarter, failure to retain backups for more than a year will prevent you from being able to restore critical data from past quarters that may be needed in case of a breach, equipment failure, or disaster.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	Moderate	✔	✔	☺	$$$
	Mitigation Strategy				
	Industry best practices recommend retaining backups of critical data for at least 18 months.				
ID	Weakness				
106	Unprotected backups could result in the compromised integrity of data you are going to rely on following a breach, equipment failure, or disaster.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	Moderate	✔	✔	😐	$$$
	Mitigation Strategy				
	Defense in-depth should be the strategy when considering how to protect your backups. A strategy that begins with offsite storage and includes some combination of segmented media, authentication protection, and encryption is our recommendation for protecting the integrity of your backups.				
ID	Weakness				
135	Not designating and training someone to manage public relations during the recovery from a cyber attack could result in damage to the organization's reputation and ultimately a successful recovery.				
	Overall Severity	SW Required	HW Required	Cultural Impact	Financial Impact
	Low	✘	✘	☺	$$
	Mitigation Strategy				
	The organization should formally designate someone to manage public relations during the recovery of a cyber attack.				