Cyber Security Assessment

Client Name:	City of Port Lavaca, TX
Partner Name:	VC3
Prepared By:	AJ Siebert
Prepared On:	11/04/2022

Agenda

Overview 3

Compliance Summary 4

Vulnerability Summary 5

Dark Web Exposure Details........ 6

Anti-Spam Configuration Details........ 9

Endpoint Health Details 10

Endpoint Hygiene/Asset Details 11

Users with Possible Policy Violation Details........ 12

User Login Details 13

NIST Assessment Details 14

Overview

City of Port Lavaca, TX has engaged VC3 to perform a cybersecurity assessment to provide findings, summary analysis and recommendations based on this high-level assessment.

The scope of this project includes the review of all data networks, IT systems, and policies as they pertain to cybersecurity. This information allows VC3 to determine the security readiness of the organization's IT infrastructure, applications, systems, and core processes.

The result of this assessment is for VC3 to understand the organization's overall cybersecurity posture and understand where critical gaps exist.

This assessment is not intended to provide a complete "end-to-end" cybersecurity assessment, but rather is designed to illustrate City of Port Lavaca, TX's posture related to core cybersecurity compliance.

Executive Summary

✓ Fully Compliant

? Unable to Assess – *item was not apparent at time of assessment.*

✗ Not Compliant

✓ Security Assessment

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

Date: ____________

✗ Spam Email

Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.

✗ Passwords

Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.

? Security Awareness

Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

✗ Multi-Factor Authentication

Utilize Multi-Factor Authentication whenever you can including on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

✓ Computer Updates

Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.

✗ Dark Web Research

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

✗ SIEM/Log Management

(Security Incident & Event Management)

Uses big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.

? Firewall

Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call us today!

✓ Web Gateway Security

Internet security is a race against time. Cloud-based security detects web and email threats as they emerge on the internet, and blocks them on your network within seconds – before they reach the user.

? Backup

Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.

✗ Advanced Endpoint Detection & Response

Protect your computers data from malware, viruses, and cyberattacks with advanced endpoint security. Today's latest technology (which replaces your outdated antivirus solution) protects against file-less and script-based threats and can even rollback a ransomware attack.

Vulnerability Summary

What is this?

Organizations must implement layers of security to minimize cyber attack risks.
VC3 has provided a vulnerability summary based on the items that we assessed from the scan and questionnaire that follow NIST guidance:

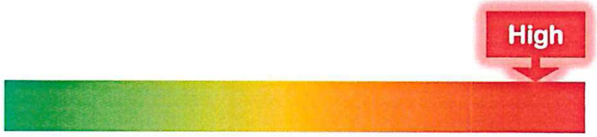
- **Identify** – Risk Assessment
- **Protect** – Firewall, Web Filtering, Passwords, Security Awareness Training, Email Security, MFA, Patching
- **Detect** – SIEM/Log Management, Dark Web Monitoring
- **Respond** – Advanced Endpoint Detection and Response
- **Recover** – Backup

What does this mean?

Typically, an environment that is considered "low risk" will have a score of **20 or less**. This indicates that the majority of cybersecurity mitigation measures are in place.
Scores **21-60** are considered "medium risk", which may indicate there are some basic and advanced cybersecurity mitigation measures in place.
Scores higher than **60** indicate "high risk" because there are critical cybersecurity mitigation measures missing from the environment.

What should we do?

Identify the areas that are missing protections! Budget, Plan and Implement those critical cybersecurity mitigation measures that are missing.
Measures like MFA help prevent 99% of account compromises thus protecting the organizations productivity and reputation and providing greater piece of mind.



The Importance of Dark Web Monitoring

What is dark web monitoring?
Dark web monitoring is the process of tracking your organization's information on the dark web. Dark web monitoring tools help find leaked or stolen information such as compromised passwords, breached credentials, intellectual property, and other sensitive data that is being shared and sold among malicious actors operating on the dark web.

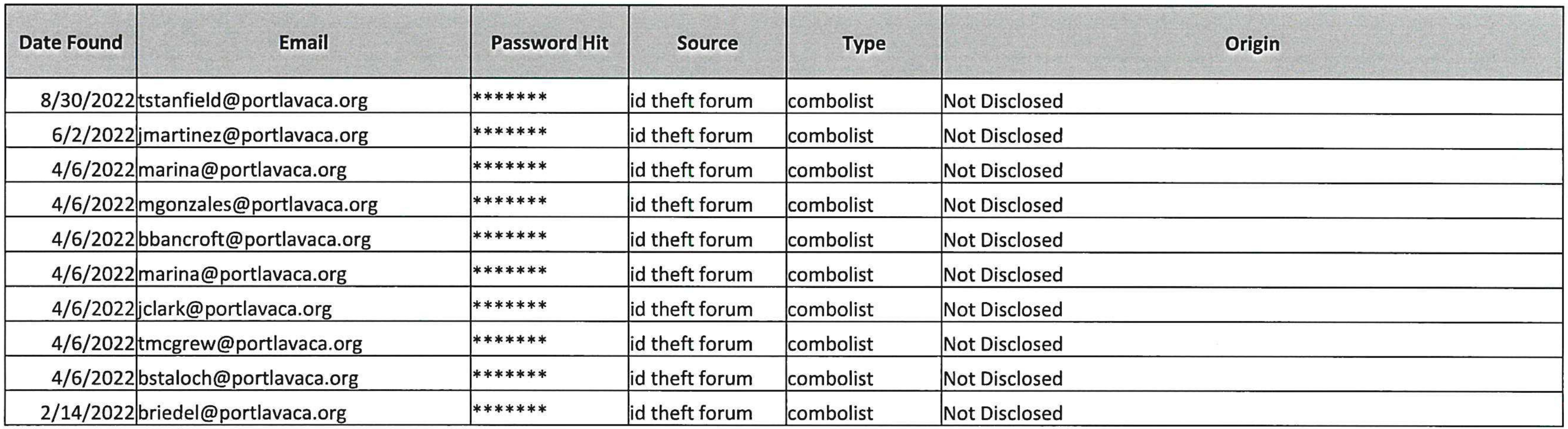
What is the impact?
For individuals, this usually means they should change all their passwords, keep an eye on their credit reports, and consider replacing their credit cards. The reality is that everybody's personal information, or at least some of it, has been for sale for a while. So, while consumers should take protective measures, they shouldn't panic.

Businesses and local governments, however, need to respond much more aggressively. They are the guardians of their customers' data. If they expose those customers to risk, they have failed. At stake is litigation, lost brand reputation, regulatory penalties, auditing costs, and the increased risk of future attacks.

What should we do?
Compromised credentials are not the only thing that businesses need to worry about. Chatter and activity on the dark web can tip off a business that it is under attack, has already been attacked, or is associated with some other activity that poses a threat to the business (such as a breach at one of its supply chain partners). As part of an overall security strategy, dark web monitoring is akin to sending a canary into a coal mine.

In addition to scanning for data breach information, a dark web monitoring service can be used to classify risks from unknown sources. Businesses that receive alerts when their data appears on the dark web can connect those mentions to other threat sources and use that information to profile and mitigate threats faster.

Dark Web Exposure Details



Date Found	Email	Password Hit	Source	Type	Origin
8/30/2022	tstanfield@portlavaca.org	*******	id theft forum	combolist	Not Disclosed
6/2/2022	jmartinez@portlavaca.org	*******	id theft forum	combolist	Not Disclosed
4/6/2022	marina@portlavaca.org	*******	id theft forum	combolist	Not Disclosed
4/6/2022	mgonzales@portlavaca.org	*******	id theft forum	combolist	Not Disclosed
4/6/2022	bbancroft@portlavaca.org	*******	id theft forum	combolist	Not Disclosed
4/6/2022	marina@portlavaca.org	*******	id theft forum	combolist	Not Disclosed
4/6/2022	jclark@portlavaca.org	*******	id theft forum	combolist	Not Disclosed
4/6/2022	tmcgrew@portlavaca.org	*******	id theft forum	combolist	Not Disclosed
4/6/2022	bstaloch@portlavaca.org	*******	id theft forum	combolist	Not Disclosed
2/14/2022	briedel@portlavaca.org	*******	id theft forum	combolist	Not Disclosed

**Partial scan results. Full Details can be found in the Report titled: Live Search @portlavaca.org.*

The Importance of Email Anti-Spam Configuration

What is this?

Protection against phishing & spoofed emails starts with 3 email standards:

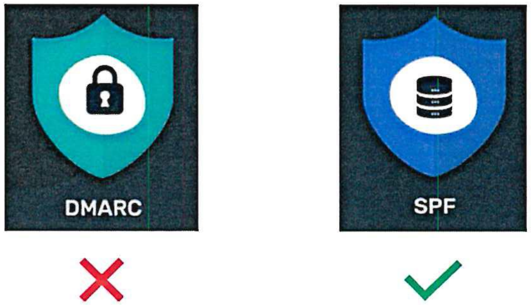
- **DomainKeys Identified Mail (DKIM)**: Designed to detect forged sender addresses in email, a strategy often used in phishing emails.
- **Sender Policy Framework (SPF):** Specifies the domains and servers that are authorized to send email on behalf of your business.
- **Domain-based Message Authentication, Reporting, and Conformance (DMARC):** Enables email domain owners the ability to protect their domain from unauthorized use.

What does this mean?

These measures help protect your outgoing email from being marked as spam and are effective in protecting your email domain from forgery and spoofing. Without these standards in place, attackers can potentially use your email address(es) to either socially engineer their way into your environment or impersonate you to gain access to other systems, thus causing a breach and ultimately affecting productivity and reputation.
Until recently, the core functionality of email services on a server did not require DMARC. Configuring anti-spam, spoofing and phish protection services are included in all new VC3 Advanced Email Protection solution implementations.

What should we do?

If these standards are not properly applied to your organization's DNS records, you are at risk. These standards are of no cost to implement but the peace of mind it brings to an organization is invaluable.



The Importance of Endpoint Health

What is this?
This report demonstrates how protected the individual devices are that exist in your environment today. As these devices are used in the day-to-day operation of your organization, they are subject to many different methods that cyber attackers use to gain access to your environment.

What does this mean?
Protecting your organization's endpoints is arguably one of the most effective means of securing your entire IT infrastructure, as endpoint defense can safeguard users from the risks of connecting to the internet.

What should we do?
Every endpoint (servers, desktop PCs, laptops, tablets, etc.) should minimally be fully protected by a firewall, antivirus software, DNS filtering, controlled remote access, and the latest security patches to safeguard the asset from being compromised.

Endpoint Health Details (Workstations)

Device Name	Overall Risk	Advanced Virus and Malware Protection	Missing Critical & Important Patches	Web Filtering	System Aging	Supported OS
PUBLICWORKS5-PC	Ok	Ok	Ok	Ok	Ok	Ok
PUBLICWORKS6-PC	Ok	Ok	Ok	Ok	Ok	Ok
PUBLICWORKS7-PC	Ok	Ok	Ok	Ok	Ok	Ok
PWDIR112019	Ok	Ok	Ok	Ok	Ok	Ok
RICOHADMIN-PC	Ok	Ok	Ok	Ok	Ok	Ok
ST2LT082019	Ok	Ok	Ok	Ok	Ok	Ok
PLFD-12	Critical	Critical	Critical	Ok	Critical	Critical
ACCOUNTANT	At Risk	At Risk	Ok	Ok	Ok	Ok
ACCTCLERK	At Risk	At Risk	Ok	Ok	Ok	Ok
ASSTCITYSEC	At Risk	At Risk	Ok	Ok	Ok	Ok

***Partial scan results. Full Details can be found in the Report titled: Excel Export.**

Endpoint Health Details (Servers)

Device Name	Overall Risk	Advanced Virus and Malware Protection	Missing Critical & Important Patches	Web Filtering	System Aging	Supported OS
AD2	Ok	Ok	Ok	Ok	Ok	Ok
DS1	Critical	Critical	At Risk	Ok	Critical	At Risk
FS1	Critical	Critical	Ok	Ok	Ok	Ok
INC	Ok	Ok	Ok	Ok	Ok	Ok
PLAD	Critical	Critical	Ok	Ok	Ok	Ok
PT	Ok	Ok	Ok	Ok	Ok	Ok
SERVER1	Critical	Critical	Critical	Ok	Critical	Critical

The Importance of User Policies

What is this?
This report contains an inventory of all user accounts currently configured in your environment and illustrates how they're being used to access data and systems within your network.

What does this mean?
Constant "access pruning" assures that methods to access data and systems are up to date with the organization's access and control policies, assuring that legacy user accounts are properly managed.

What should we do?
VC3 follows a "Minimal Functional Access" policy, where the lowest level of access is granted to users and accounts required to achieve the function of their role. Essentially, we assure that all user accounts are configured in such a way that only the rights and privileges required are granted, and all other rights and privileges to access data and systems are granted on an "as needed" basis.

It's important to disable then delete inactive accounts to minimize brute force attacks, where a bad actor or bot will continuously attempt to crack a password to gain unauthorized access to systems.

Users with Possible Policy Violation Details

User Name (Enabled)	User Role	Last Login Timestamp	Password Last Set	Password Expires
PORTLAVACA1.LOCAL\Administrator	Admin	17-Oct-2022 9:26:30 AM	**15-Feb-2020 11:46:25 PM**	**<never>**
PORTLAVACA1.LOCAL\localit.doien	Admin	04-Oct-2022 1:55:14 PM	27-Sep-2022 9:51:56 AM	26-Dec-2022 9:52:34 AM
PORTLAVACA1.LOCAL\localit.jordan	Admin	13-Oct-2022 5:09:20 PM	**29-Jun-2020 12:00:49 PM**	**<never>**
PORTLAVACA1.LOCAL\localit.josh	Admin	20-Oct-2022 1:54:03 AM	**29-Apr-2020 3:35:56 PM**	**<never>**
PORTLAVACA1.LOCAL\localitadmin	Admin	04-Jul-2022 9:40:39 PM	15-Jun-2022 1:38:47 PM	13-Sep-2022 1:39:25 PM
PORTLAVACA1.LOCAL\slang	Admin	20-Oct-2022 3:13:17 PM	14-Sep-2022 8:33:59 AM	13-Dec-2022 8:34:37 AM
PORTLAVACA1.LOCAL\tyler.tech	Admin	**27-Dec-2021 3:34:35 PM**	27-Sep-2022 2:03:03 PM	**<never>**
PORTLAVACA1.LOCAL\aenglish	User	**24-Jul-2020 12:31:38 PM**	**24-Jul-2020 12:30:37 PM**	**22-Oct-2020 12:31:15 PM**
PORTLAVACA1.LOCAL\agarza	User	**30-Mar-2022 6:08:13 AM**	**05-Jan-2022 8:04:36 AM**	**05-Apr-2022 8:05:14 AM**
PORTLAVACA1.LOCAL\bhogan	User	20-Oct-2022 3:06:11 PM	**17-Feb-2020 1:58:37 PM**	**<never>**
PORTLAVACA1.LOCAL\bstaloch	User	20-Oct-2022 9:50:58 AM	**10-Apr-2020 2:10:10 PM**	**<never>**
PORTLAVACA1.LOCAL\ccastro	User	**15-Mar-2022 12:48:10 PM**	**<never>**	**<never>**

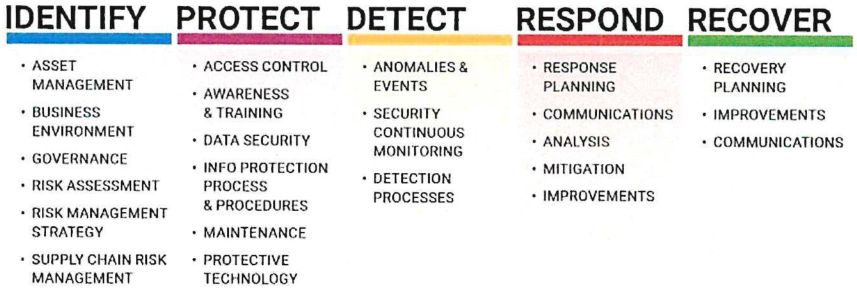
**Partial scan results. Full Details can be found in the Report titled: Excel Export.*

NIST Assessment Details

Thank you for taking the time to participate in this risk assessment process. The goal of this assessment is to identify your security strengths and weaknesses, and to provide advice as to the improvements you should be considering relative to your security posture.

The assessment and your results are aligned to the National Institute of Standards and Technology, Cybersecurity Framework v1.1, (NIST CSF), considered to be a best practice for firms such as yours.

The assessment spanned the five core areas of the framework as detailed below, and this report will show you results against the framework, as well as how your business aligns to other firms with respect to size, location, and industry.



IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• ASSET MANAGEMENT • BUSINESS ENVIRONMENT • GOVERNANCE • RISK ASSESSMENT • RISK MANAGEMENT STRATEGY • SUPPLY CHAIN RISK MANAGEMENT	• ACCESS CONTROL • AWARENESS & TRAINING • DATA SECURITY • INFO PROTECTION PROCESS & PROCEDURES • MAINTENANCE • PROTECTIVE TECHNOLOGY	• ANOMALIES & EVENTS • SECURITY CONTINUOUS MONITORING • DETECTION PROCESSES	• RESPONSE PLANNING • COMMUNICATIONS • ANALYSIS • MITIGATION • IMPROVEMENTS	• RECOVERY PLANNING • IMPROVEMENTS • COMMUNICATIONS

For you reference, we have provided the results of your NIST Cyber Security Framework Assessment in the full reporting package included with this report.