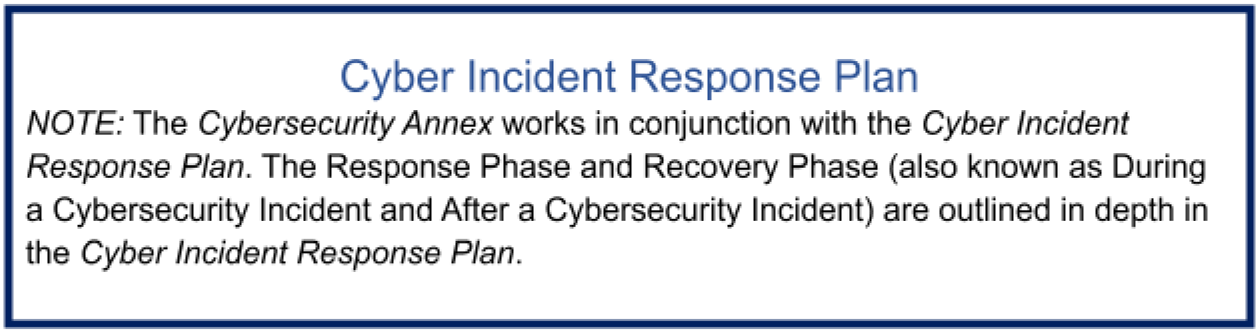
La Vernia ISD
Cybersecurity Annex

2024- 2025



Cyber Incident Response Plan

NOTE: The *Cybersecurity Annex* works in conjunction with the *Cyber Incident Response Plan*. The Response Phase and Recovery Phase (also known as During a Cybersecurity Incident and After a Cybersecurity Incident) are outlined in depth in the *Cyber Incident Response Plan*.

SPECIAL ACKNOWLEDGEMENTS

The Texas School Safety Center is grateful for the contributions of the specialists in directing the subject matter knowledge for this annex. We appreciate your help in creating this template, which is for use by colleges and K-12 districts throughout the state. Your knowledge was invaluable in creating this template and subsequent completion guide.

A special thank you goes to:

Todd Pauley, CISSP, CISM
Deputy CISO and Cybersecurity Coordinator, Texas Education Agency

Ernesto Ballesteros, JD, MS, CISSP, CISA
Cybersecurity State Coordinator of Texas, Cybersecurity, and Infrastructure Security Agency

Tony Sauerhoff, CISSP, GSLC
Deputy CISO and State Cybersecurity Coordinator, Texas Department of Information Resources

RECORD OF CHANGES AND REVIEW

The Cybersecurity Annex will be reviewed periodically, *but no less than every three years*, and be properly coordinated with the district's other plans.

The Cybersecurity Annex's notable modifications are included in the table along with the date of the Annex's review. Add additional rows as needed.

This Record of Changes and Review identifies only significant changes made to this Annex. If no significant changes were made, the phrase "Cybersecurity Review Conducted" has been placed in the *Summary of Significant Changes and Review* column.

Change Number	Date of Change	Name of Person or Agency Making the Change	Summary of Significant Changes and Review
1	8/7/24	T. Armstrong & A. Ramirez	Responsibility Assignments
2	9/5/24	T. Armstrong	Applied recommended edits

Section 1 – Purpose and Scope

1.1 Purpose

This annex establishes the policies and procedures under which the district will operate in the event of a cybersecurity incident by addressing planning and operational actions for the five phases of emergency management (prevention, mitigation, preparedness, response, and recovery) regarding actual or potential cyber-related threats and attacks to the district.

1.2 Scope

This annex is meant to address district planning for cybersecurity incidents and applies to the whole district community and all district property.

Section 2 – General Information

2.1 Hazard Overview

Cybersecurity establishes the measures taken to protect a computer, computer network, or computer system against unauthorized use or access, otherwise known as a cyber incident. According to the Presidential Policy Directive (PPD) 41, a cyber incident is

> “An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.”

A cyber incident could affect building access, phone systems, security systems, learning management systems, human resources, payroll, student records, school nutrition services, visitor management systems, printing services, library services, staff information, and other systems that use a computer network.

2.2 District-Specific Hazard Risk

La Vernia ISD notes the level of risk concerning cybersecurity incidents using a *Cybersecurity Risk Evaluation Tool*.

La Vernia ISD identifies the following cyber incidents as a high priority. If needed, these hazards are addressed in an appendix to this annex.

Data Breach

A data breach occurs when private, sensitive, or protected information is spilled or leaked from a safe setting into an unsecured one, where it is subsequently seen, copied, communicated, stolen, or used without authorization. Confidential information, like student records, is frequently the subject of data breaches because it might be improperly seen or used by someone who should not have access.

Denial of Service attacks (DOS and DDoS)

A Denial of Service (DOS) attack occurs when hackers use false requests and traffic to overwhelm a system and shut it down. A Distributed Denial of Service (DDoS) attack is the same type of attack, except the hacker uses multiple breached devices at the same time.

Fraudulent Instruction

Fraudulent Instruction usually occurs as a targeted phone call or email that convinces an employee to alter the direct deposit information for a worker, or more seriously, for a district-funded building project.

Malware-based attacks (Ransomware, Trojans, etc.)

Malware refers to “malicious software” that is designed to disrupt or steal data from a computer, network, or server.

Man-in-the-Middle (MitM)

A Man-in-the-Middle attack (MitM) occurs when attackers intercept data or compromise your network to “eavesdrop” on you. These attacks are especially common when using public Wi-Fi networks, which can easily be hacked.

Password attacks

Password attacks are any cyberattack that uses brute force, guesswork, or deception to get you to divulge your passwords.

Phishing (spear phishing, whaling, etc.)

A phishing attack occurs when a cybercriminal sends you a fraudulent email, text (called “smishing”), or phone call (called “vishing”). These messages look like they are from someone official or a person or business whom you trust, such as your bank, the FBI, or a company like Microsoft, Apple, or Netflix.

Ransomware

Malevolent software that locks user access by encrypting data while extorting payment (a “ransom”) from the victim to de-encrypt and restore the files.

Spoofing

Email messages sent from a fraudulent account masquerading as a legitimate and trusted source to gain access to a user’s system or confidential information.

Spyware

Criminal malware on the hard drive is used to covertly monitor user activities.

Virus

A type of malware that when executed spreads from computer to computer by replicating its programming and infecting user programs and files to change the way they operate or to stop working altogether.

Zero-day exploits and attacks

Zero-day exploits are cybersecurity vulnerabilities that exist in software or network without the manufacturer’s knowledge.

2.3 Hazard Preparedness and Warning

La Vernia ISD has committed to being prepared for high-priority incidents as identified in the *District-Specific Hazard Risk* (section 2.2). The following are steps that the district will take to prepare for an incident.

Backup Data

Employ a backup solution that automatically and continuously backs up critical data and system configurations. Backup files are either stored in the cloud or if backed up to a local, portable drive, maintained off the network for secure storage. If the backups are stored off-site, but still on the network, they would still be susceptible to an attack.

The district recognizes that if backup files are stored in the same place where the primary files are stored, then there is a high probability that in an incident, both sets will be destroyed.

Multi-Factor Authentication (MFA)

Require Multi-Factor Authentication (MFA) for accessing systems whenever possible. MFA is required with privileged, administrative, and remote access users, and will eventually be required by all users.

Patch and Update Management

Replace unsupported operating systems, applications, and hardware. Test and deploy patches quickly.

Suspicious Activity

Watch for suspicious activity that asks a user to do something right away, offers something that sounds too good to be true, or requests personal information.

Inadvertent Loss to Environmental Factors

Servers and other critical network infrastructure are not in rooms subject to water leaks (overhead plumbing) or accidental sprinkler damage. Additionally, adequate air conditioning is maintained in rooms in which network equipment is used.

Section 3 – Cyber Incident Stakeholders

3.1 Cyber Incident Stakeholders Chart

La Vernia ISD has listed all stakeholders and decision-makers during a cyber incident.
**The list of individuals below is provided for informative reasons and does not indicate the order or necessity to be called for every situation.*

Contact Role	Contact Name	Phone Number	Email
Superintendent	Dr. Hensley Cone	830-779-6600	hcone@lvisd.org
Campus Principal HS	Jeffrey Clouse	830-779-6630	jclouse@lvisd.org
Campus Principal JH	Charles Caughlin	830-779-6650	ccaughlin@lvisd.org
Campus Principal Int	Brandi Hanselka	830-779-6640	bhanselka@lvisd.org
Campus Principal Primary	Shelley Keck	830-779-6660	skeck@lvisd.org
IT Director	Todd Armstrong	830-779-6616	tarmstrongr@lvisd.org
Network Manager	Alex Ramirez	726-201-0397	aramirez@lvisd.org
Legal Counsel	Walsh Gallegos	210-979-6633	eneally@wabsa.com
Critical Vendor	Intech Southwest	210-690-0000	slopez@intechsouthwest.com
Critical Vendor	Ascender - ESC 20	210-370-5321	samuel.bravo@esc20.net
Cyber Insurance Provider *Policy #: 247-903*	La Vernia Insurance Agency - Frank Pruski	830-779-2595	lvins@lv-insurance.com
Education Service Center	Dale Harville	210-370-5740	dale.harville@esc20.net
FBI Internet Crime Complaint Center (IC3) https://www.ic3.gov	N/A	202-324-3000	https://complaint.ic3.gov/
Department of Homeland Security - CISA https://www.cisa.gov/report	N/A	1-844-Say-CISA	https://www.cisa.gov/forms/report
Texas Dept. of Information Resources (DIR) Management and Reporting	John Hoffman	877-DIR-CISO	security-alerts@dir.texas.gov
Texas Education Agency	Todd Pauley	512-463-9734	todd.pauley@tea.texas.gov
Police	Chief Keil	830-581-9316	dkeillvpd@lavernia-tx.gov
Utilities- Electric	FELPS GVEC	830-216-7000 800-223-4832	customerservice@felps.us www.gvec.org
Utilities- Water	City of La Vernia	830-779-4541	jbegole@lavernia-tx.gov
Utilities- ISP	Region 20 ESC	210-370-5324	samantha.palacios@esc20.net

3.2 Build a Cyber Incident Response Team and Define the Roles

La Vernia ISD has defined roles for the execution and management during a cyber incident.

Role	Responsibilities	Contact Name	Phone Number	Email
Cyber Incident Response Team Lead	Manage incident operations Identify and apply resources	Todd Armstrong	830-779-6616	tarmstrong@lvisd.org
Team Administrator	Document incident Compile data Contact list Distribution Point of Contact for outside agencies	Todd Armstrong	830-779-6616	tarmstrong@lvisd.org
District Cybersecurity Coordinator	Liaison between the district and the agency	Todd Armstrong	830-779-6616	tarmstrong@lvisd.org
Team Lead Investigator	Coordinate response activities Technical aspects	Dale Harville	210-370-5740	dale.harville@esc20.net
First Responder	Investigation Reporting Arrest	Todd Armstrong	830-779-6616	tarmstrong@lvisd.org
Public Relations	Contact List All inbound and outbound communication	Hensley Cone	830-779-6600	hcone@lvisd.org
Federal Government Liaison	Contact list Request resources National reporting and tracking system of cybersecurity incidents	Todd Armstrong	830-779-6616	tarmstrong@lvisd.org

Section 4 – Actions and Responsibilities

District Actions and Responsibilities Table

Responsible Role refers to a ***single*** responsible role associated with the district action. This individual will oversee the action's completion and any necessary general training. However, this individual may not be the same as the individual or individuals that perform the action.

Prevention Phase

Safeguard against consequences unique to a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Designate a cybersecurity coordinator to serve as a liaison between the district and the agency in cybersecurity matters.	Chief Instructional Officer
Conduct annual training for the District Cybersecurity Coordinator.	Chief Instructional Officer
Conduct a risk assessment of cybersecurity threats and vulnerabilities. ● Identify the attractiveness of potential targets. ● Identify critical district processes and assets.	Cybersecurity Coordinator
Install host-based firewalls and endpoint security products.	Cybersecurity Coordinator
Configure network firewalls to block unauthorized IP addresses.	Cybersecurity Coordinator
Install antivirus software.	Cybersecurity Coordinator
Employ a backup solution that automatically and continuously backs up critical data and system configurations.	Cybersecurity Coordinator
Regularly test the restoration of data.	Cybersecurity Coordinator
Disable port forwarding (disable the ability to connect over the internet with other public or private computers).	Cybersecurity Coordinator
Sign up for Dorkbot web application vulnerability notification service.	Coordinator of Communication
Prepare a contact list of roles for the execution and management (*Section 3.2: Build a Cyber Incident Response Team and Define the Roles*) during a cyber incident and disseminate it to relevant parties.	Cybersecurity Coordinator

Mitigation Phase Reduce the impact of a cybersecurity incident.	
District Actions	Responsible Role (Position responsible for this action)
Conduct continuous scans on devices for additional vulnerabilities.	Region 20 ESC
Provide updates on all systems, including all internet connected devices (i.e., smartphones and tablets), whenever possible. Replace unsupported operating systems, applications, and hardware. Consider testing a small percentage of systems before patching all systems.	Cybersecurity Coordinator
Set antivirus and anti-malware solutions to automatically update and conduct regular scans.	Cybersecurity Coordinator
Separate student networks from other sensitive district networks where possible.	Cybersecurity Coordinator
Apply the Principle of Least Privilege (PoLP) to all systems and services so that users only have the access they need to perform their jobs.	Cybersecurity Coordinator
Require Multi-Factor Authentication (MFA) for accessing critical systems and consider using for all systems.	Chief Instructional Officer
Enable the most secure authentication tools available, such as biometrics, security keys, or a unique one-time code through an app on the mobile device.	Cybersecurity Coordinator
Close or block network ports that are not in use to reduce the threat landscape of potential attacks.	Cybersecurity Coordinator

Preparedness Phase

Regularly review district readiness for a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Create an annual training plan for all employees and students.	Director of Human Resources / Campus Principals
Train faculty, staff, and students on cybersecurity incidents annually.	Cybersecurity Coordinator/ Campus Principals
Conduct cybersecurity training for Board Members.	Cybersecurity Coordinator
Join an information sharing program.	Network Manager
Document information flows by learning where data is located and how it is used for the district.	Cybersecurity Coordinator
Maintain hardware and software inventory.	IT Director/ Curriculum Department
Ensure proper audit logs are created and reviewed routinely for suspicious activity.	Network Manager
Monitor privacy settings and information available on social networking sites.	Coordinator of Communications
Test and update response plans by conducting tabletop exercises.	Cybersecurity Coordinator
Perform annual penetration testing and routine vulnerability assessments.	Cybersecurity Coordinator
Ensure all students and employees understand and sign a network use agreement that explicitly outlines bad behaviors and consequences.	Director of Human Resources/ Campus Principals/ Superintendent
Develop business continuity plans, as part of your Continuity of Operations Plan (COOP), for each department with essential functions.	Chief Financial Officer
Establish an Interagency Contract with the Department of Information Resources (DIR).	Cybersecurity Coordinator
Consider purchasing cyber insurance for the district.	Chief Financial Officer
Learn what actions to avoid that could disrupt the insurance process	Chief Financial Officer

Response Phase

District actions during a cybersecurity incident.

Refer to ***Section 5 - Document 4: Cyber Incident Response Plan*** when a cyber incident occurs. This plan is specific to cyber incidents and clarifies roles and responsibilities as well as provides guidance on key activities that must be performed. This plan must be carried out quickly so make sure to practice it before an actual incident occurs. This plan helps prevent data and monetary loss and to resume normal operations.

This plan is attached to the back of this annex due to the need to access the steps quickly and easily.

Recovery Phase

Return to normal district operations following a cybersecurity incident.

Refer to ***Section 5 - Document 4: Cyber Incident Response Plan*** for the recovery phase. The plan specifies steps to help resume normal operations.

Section 5.0 - Documents

Document 1: Anomalies Report *(optional)*

Reporting System for Anomalies

It is important to report computer anomalies, system performance issues, strange defects in operation, etc. to the school IT director or division. Early warning signs of Indication of Compromise (IoC), reported early, can prevent possible cascading outages. Staff should be encouraged and empowered to report such system behaviors.

When reporting attempt to provide the following:

Anomalies Reporting Table

Point of Contact	**Name**	**Email**	**Phone Number**
Date of Indication of Compromise		**Time of Indication of Compromise**	
Manufacturer		**Operating System (OS)**	
Description of Behavior			

Document 2: Services Restoration Priority Worksheet *(optional)*

This restoration worksheet identifies the services and systems used the district to conduct its internal and external operations. Prioritization of services and systems are critical to support restoration priorities during incident response and recovery activities. These may be listed and prioritized as part of the business continuity or disaster recovery planning process.

Consider the restoration priority for your district using the following classifications:

- *Tier 1:* Critical services or systems and life safety or public safety systems.
- *Tier 2:* Core business functions and services that enable district operations.
- *Tier 3:* Routine business functions and services that support district operations.
- *Tier 4:* Non-production services or functions that do not impact the end users.

Tier	Service or System	Function and Details	End User
Ex. 3	*Library*	*Loaning and receiving multimedia, iPad registration and insurance*	*Students*
1			
2			
3			
4			

Document 3: Hardware and Software Inventory *(optional)*

It is highly encouraged to track the district's IT resources, including computers, servers, mobile devices, IP phones, other internet-connected devices, and approved and managed software. This inventory allows IT or your managed service provider to track devices to maintain and provides a starting point to prioritize disaster recovery efforts.

Hardware Tracking Inventory

Complete and maintain the following hardware asset tracking sheet. Customize the headers as appropriate.

Asset Number	Current Status	Assigned Employee	Asset Type	Model	Manufacture	Serial Number	Location	Description	Date Issued	Date Returned

Software Tracking Inventory

Complete and maintain the following software tracking sheet. Customize the headers as appropriate.

Software User	Name	Software Description	License Type	Version	Software Key	Date Purchased	Billing Cycle

Sensitive Asset Inventory

Complete and maintain the following sensitive asset tracking sheet. Customize the headers as appropriate.

File Name	File Type	Description	Type of Storage	Data Storage Location	Data Classification Label	Reason for Sensitivity	Individuals with Access	Notes

{Excerpt from "CIS Hardware and Software Asset Tracking Spreadsheet" by CIS Controls™ is licensed under CC BY 4.0}

Document 4: Cyber Incident Response Plan (IRP)

Before a Cybersecurity Incident
Refer to *Section 4 – Actions and Responsibilities* for the Prevention, Mitigation, and Preparation Phases to prepare before a cybersecurity incident occurs.

During a Cybersecurity Incident

District actions during a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Contact the IT director or team lead through established channels, as well as communication channels that do not use the ISD network (i.e., cell phones, Gmail, etc.).	Cybersecurity Coordinator
When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a compromised machine from the network.	Network Manager
Determine the appropriate power-down option. Consider disconnecting from the network rather than shutdown. Forensic data can be destroyed if the operating system (OS) executes a normal shutdown process.	Cybersecurity Coordinator
Block compromised systems from communicating with other devices or with attackers.	Cybersecurity Coordinator
Seek legal guidance ***before*** initiating communications.	Superintendent
Contact a cyber insurance provider or broker if the district has an existing policy.	Chief Financial Officer
Contact all critical software vendor(s).	Cybersecurity Coordinator/ Network Manager
Contact the FBI, Law Enforcement, and Homeland Security, if needed.	Director of Safety & Security
Contact DIR using the cybersecurity hotline which may be reached 24 hours, 7 days a week by using the SB 271 Security Incident Reporting portal. If the district needs urgent support, they should call (877) 347-2476 (877-DIR-CISO). Districts must report anomalous cyber activity and cyber incidents to DIR within 48 hours after discovery, and again within 10 days of incident closure.	Cybersecurity Coordinator
Consult with trained forensic investigators for advice and assistance ***prior*** to implementing any recovery or forensic efforts.	IT Director/ Cybersecurity Coordinator

During a Cybersecurity Incident

District actions during a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Contact banks, credit card companies, and other financial accounts to report that someone may be using the district's identity. Holds may need to be placed on accounts that have been attacked. Unauthorized credit or charge accounts will need to be closed.	Chief Financial Officer
Keep detailed notes of all observations, including dates and times, mitigation steps taken and not taken, device logging enabled or disabled, and machine names for suspected compromised equipment. More information is generally better than less information.	Cybersecurity Coordinator
Oversee and track containment and restoration activities, including actions taken, resource assignments, and notifications.	IT Director/ Cybersecurity Coordinator
Track all hazard-related expenses for state and federal reimbursement, auditing and record keeping.	Chief Financial Officer
Initiate Continuity of Operations Plan (COOP) and essential department continuity plans.	Chief Financial Officer

After a Cybersecurity Incident

Return to normal district operations following a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Ensure that personnel are made available to provide statements to law enforcement and other investigating authorities.	Director of Human Resources
Conduct a root cause analysis to pinpoint where a malicious incident took place, then report to DIR within 10 business days.	Region 20 ESC
Communicate with internal and external stakeholders and manage public relations and reputation, including parents of students, if necessary.	Superintendent
Conduct continuous monitoring of networks after a breach for any abnormal activity and make sure intruders have been inhibited thoroughly.	Cybersecurity Coordinator

After a Cybersecurity Incident

Return to normal district operations following a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Work with affected system and service owners and managers to determine resources and sequencing needed to restore operations to a normal state.	Cybersecurity Coordinator
Based on priorities and estimated recovery timelines, repair, restore, rebuild, or replace systems that were taken offline or otherwise affected by the incident after they are cleared and released by investigators.	Cybersecurity Coordinator
Track restoration efforts and provide information to the emergency management team (EMT) regarding estimated and actual time to full restoration.	Cybersecurity Coordinator
After ensuring evidence has been preserved for legal and insurance purposes, and given the all-clear, eliminate all traces of the incident.	Cybersecurity Coordinator
Activate the damage assessment team.	Cybersecurity Coordinator
Initiate cost recovery activities.	Chief Financial Officer
Conduct an After-Action Review (AAR) to identify areas of improvement for the incident response plan.	Cybersecurity Coordinator
Develop and implement an Improvement Plan that includes recommended changes from the incident debriefing and AAR.	Cybersecurity Coordinator
Share lessons learned through appropriate channels.	IT Director
Contact DIR using the cybersecurity hotline which may be reached 24 hours, 7 days a week by using the **SB 271 Security Incident Reporting portal**. If the district needs urgent support, they should call (877) 347-2476 (877-DIR-CISO). Districts must report anomalous cyber activity and cyber incidents to DIR within 10 days of incident closure.	Cybersecurity Coordinator
Districts must notify any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person no later than the 60th day after the date on which the breach was determined to occur.	Director of Human Resources

Section 6 – Resources

6.1 Abbreviations and Acronyms

AAR	After-Action Review
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations Plan
DIR	Department of Information Resources
DDoS	Distributed Denial of Service
DOS	Denial of Service
EMT	Emergency Management Team
IAM	Identity and Access Management
Infosec	Information Security
IoC	Indication of Compromise
IT	Information Technology
K12 SIX	K12 Security Information eXchange
LEA	Local Education Agency
LOA	Letters of Agreement
MFA	Multifactor Authentication
MitM	Man-in-the-Middle
MOU	Memoranda of Understanding
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIST	National Institute of Standards and Technology
Nmap	Network Mapper
OIG	Office of the Inspector General
OS	Operating System
PII	Personal Identifying Information
PoLP	Principle of Least Privilege
SSO	Single Sign-On
TASB	Texas Association of School Boards
TEC	Texas Education Code
TGC	Texas Government Code
TX-ISAO	Texas Information Sharing and Analysis Organization
URL	Uniform Resource Locator

6.2 Definitions

Antivirus Software: Responsible for scanning your files and looking for viruses. While it is often marketed as an antivirus, most antivirus software is anti-malware even though it's frequently promoted as antivirus (Ot, 2021).

Authentication: A security measure employed to confirm the identity of the person making a request or the message's originator when trying to authorize access to data or computer resources.

Brute Force Attack: A hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.

Bug: An error, flaw, or fault in the design, development, or operation of computer software.

Cyberattack: Attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system.

Cybersecurity: Measures taken to protect a computer, computer network, or computer system against unauthorized use or access.

Cyber Resilience: The capacity to foresee, endure, recover from, and adapt to unfavorable circumstances, stressors, attacks, or compromises on systems that use or enable cyber resources.

Domain Spoofing: The act of registering web domains like legitimate websites to trick individuals who mistype URLs or click on similar-looking URLs.

Doxing: The act of compiling or publishing personal information about an individual on the internet, typically with malicious intent.

Endpoint: Physical devices that connect to a network system such as mobile devices, desktop computers, virtual machines, embedded devices, and servers.

Endpoint Security: is security to protect desktops, laptops, mobile phones, etc. from malicious, unwanted software.

End of Life Software: Out-of-date software and equipment that no longer receives patches, security updates, technical support, or bug fixes, making the user vulnerable to attacks.

Firewalls: Software program or hardware device that restricts communication between a private network or computer system and outside networks.

Information Security: Protection of information and information systems from unauthorized access and disruption.

Information Technology: Development, installation, and implementation of computer systems and applications.

Malicious Cyber Actor: A person, group, or entity that creates all or part of an incident with the aim to impact an individual’s or organization’s security.

Malware-based Attacks: Malware refers to “malicious software” that is designed to disrupt or steal data from a computer, network, or server.

Multifactor Authentication: Security technology that requires multiple methods of authentication from independent categories of credentials to verify a user’s identity (such as a password and a code or fingerprint).

Patch: A software update that can be installed to correct an issue or fix security vulnerabilities.

Port Forwarding: Allows computers or services in private networks to connect over the internet with other public or private computers or services, sometimes called port mapping.

Root Cause Analysis: Investigates the core issue that kicks off a chain of events that eventually results in the problem. It also looks for a solution in such a way that the problem is treated at the "root" or fundamental cause of the issue.

Texas Education Code § 11.175(b): District Cybersecurity Each school district shall adopt a cybersecurity policy to: (1) secure district cyberinfrastructure against cyberattacks and other cybersecurity incidents; and (2) determine cybersecurity risk and implement mitigation planning.

6.3 Resources

Cyber Insurance Information

Ritchie, J.N.& A. and Jayanti, S.F.-T., and A. (2021) *What should your cyber insurance policy cover? Cyber Insurance*, *Federal Trade Commission*. Available at: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance (Accessed: 06 October 2023).

Explains why a cyber insurance policy is useful and what the policy should cover.

Cybersecurity Risk Assessment Tools

CISA. (n.d.). Guide to Getting Started with a Cybersecurity Risk Assessment. SAFECOM. Available at: https://www.cisa.gov/sites/default/files/2024-01/22_1201_safecom_guide_to_cybersecurity_risk_assessment_508.pdf

This handbook was created by SAFECOM to help public safety communications system operators, owners, and managers comprehend the processes of a cyber risk assessment to increase operational and cyber resilience. This manual contains editable reference tables that can be used by districts to identify and record the people and resources used at each stage of the assessment. Customization is encouraged.

DIR. (n.d.). *Texas Cybersecurity Framework* | *Texas Department of Information Resources*. Information Security. https://dir.texas.gov/information-security/security-policy-and-planning/texas-cybersecurity-framework

The Texas Cybersecurity Framework is a self-assessment to determine cybersecurity risks. This sample is populated with examples of how to rate yourself based on the 6 levels identified at the bottom of the first tab (SAMPLE TCF). Once you have rated yourself in all 40 objectives the graph helps determine the highest risks and prioritization for mitigation. The roadmap will help identify processes and documentation needed to reach 3.0 in each objective.

Cybersecurity Plan Building Tools

CISA. (2023, January). *Protecting our future: Cybersecurity for K-12: CISA*. Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats. https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Reports on cybersecurity risks facing elementary and secondary schools and provides recommendations that include cybersecurity guidelines designed to help schools face these risks.

Grants

DIR. (2023, October 6). *State and local cybersecurity grant program (SLCGP)*. Information Security. https://dir.texas.gov/information-security/state-and-local-cybersecurity-grant-program-slcgp

The State and Local Cybersecurity Grant Program (SLCGP) has been given $1 billion over four years (2022-2025) to address cybersecurity risks and threats to information systems owned or run by, or on behalf of, state, local, or tribal governments.

Easterly, J. (2023, October 18). *CISA and FEMA partner to provide $374.9 million in grants to bolster state and local cybersecurity: CISA*. Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/news-events/news/cisa-and-fema-partner-provide-3749-million-grants-bolster-state-and-local-cybersecurity

For access to FY23 funding, applicants are encouraged to submit their cybersecurity plans created with FY22 money. With this financing, the Department of Homeland Security strengthens our collaboration and commitment to assisting our state, local, and territorial (SLT) government partners in developing the necessary cyber capabilities.

FEMA. (2023). *Tribal cybersecurity grant program*. Preparedness Grants. https://www.fema.gov/grants/preparedness/tribal-cybersecurity-grant-program

The Tribal Cybersecurity Grant Program provides funding to eligible entities to address cybersecurity risks and threats to information systems owned or operated by, or on behalf of tribal governments.

FEMA. (2023). *State and local cybersecurity grant program*. Preparedness Grants. https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program

The State and Local Cybersecurity Grant Program provides funding to eligible entities to address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments.

TASB. (n.d.). *About TASB Risk Fund*. Risk Management Fund. https://www.tasbrmf.org/about?rname=RMF_Benefits_And_Rewards

The TASB Risk Management Fund provides comprehensive and responsive risk solutions supporting educational excellence in Texas public school districts and other public educational entities.

Texas Education Agency. (2023, September 21). *Tx K-12 Cybersecurity Initiative Updates*. TEA. https://tea.texas.gov/about-tea/news-and-multimedia/correspondence/taa-letters/tx-k-12-cybersecurity-initiative-updates

LEAs who are interested and eligible to acquire TEA-funded Endpoint Detection and Response (EDR) may now request this service via the Service Now portal.

Information Sharing Tools

Cybersecurity & Infrastructure Security Agency. (2023). *Incident reporting system*. CISA. https://www.cisa.gov/forms/report

Provides real-time analysis and incident reporting capabilities.

Technical Assistance

Texas Education Agency. (2023, October 2). *K-12 cybersecurity initiative*. https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative

TEA in conjunction with DIR. Free Endpoint Detection & Response (EDR) subscriptions through the end of 2024-25 SY. Request for service is now open! Prioritized for small & midsize LEAs.

Texas Education Agency. (2023, November 30). *Standards for permissible electronic devices and software applications*. https://tea.texas.gov/about-tea/news-and-multimedia/correspondence/taa-letters/standards-for-permissible-electronic-devices-and-software-applications

House Bill 18 (88R) established Texas Education Code, Section §32.1021 and requires the TEA to provide these Standards for Electronic Devices and Software Applications with which school districts or open-enrollment charter schools are expected to comply.

From Section 5.0 - Response Phase Plan

District actions during a cybersecurity incident.

Prepare

Maintain offline, encrypted backups of critical data

- Maintain and regularly update "golden images" of critical systems.
- Store applicable source code or executables with offline backups (as well as escrowed and license agreements).
- Retain backup hardware to rebuild systems if rebuilding the primary system is not preferred

Create, maintain, and regularly exercise a basic cyber incident response plan (IRP) and associated communications plan that includes response and notification procedures for ransomware and data extortion/breach incidents. Ensure a hard copy of the plan and an offline version is available.

- Provide data breach notifications to third parties and regulators consistent with law.
- Ensure the IRP and communications plan are reviewed and approved by the CEO, or equivalent, in writing and that both are reviewed and understood across the chain of command.
- Include organizational communications procedures as well as templates for cyber incident holding statements in the communications plan. Reach a consensus on what level of detail is appropriate to share within the organization and with the public and how information will flow.

Implement a zero trust architecture to prevent unauthorized access to data and services.

Preventing and Mitigating Ransomware and Data Extortion Incidents

Initial Access Vector: Internet-Facing Vulnerabilities and Misconfigurations

- Do not expose services, such as remote desktop protocol, on the web

- Conduct regular vulnerability scanning to identify and address vulnerabilities
- Regularly patch and update software and operating systems to the latest available version.
- Ensure all on-premises, cloud services, mobile, and personal (i.e., bring your own device [BYOD]) devices are properly configured and security features are enabled
    - *Limit the use of RDP and other remote desktop services*
- Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi factor authentication (MFA), and log RDP login attempts.
- Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations.
- **Implement MFA on all VPN connections** to increase security.
- **Disable Server Message Block (SMB) protocol version 1** and upgrade to version 3 (SMBv3)
- Harden SMBv3 by implementing the following guidance as malicious actors use SMB to propagate malware across organizations
- Block unnecessary SMB communication
    - Block external access of SMB to and from organization networks by blocking TCP port 445 inbound and outbound at internet perimeter firewalls. Block TCP ports 137, 138, 139. **Note:** SMBv2 and later does not use NetBIOS datagrams. Continuing to use SMBv2 does not have significant risks and can be used where needed. It is recommended to update it to SMBv3 where feasible.
    - Disable the SMB Server service ("Server") on Microsoft Windows and Windows Server devices in instances where there is no need to remotely access files or to name pipe application programming interfaces (APIs).
- If SMB encryption is not enabled, require SMB signing for both SMB client and server on all systems.
- Log and monitor SMB traffic to help flag potentially abnormal, harmful behaviors.

Initial Access Vector: Compromised Credentials

- **Implement phishing-resistant MFA for all services**, particularly for email, VPNs, and accounts that access critical systems
- **Consider subscribing to credential monitoring services**
- **Implement identity and access management (IAM) systems** to provide administrators with the tools and technologies to monitor and

manage roles and access privileges of individual network entities for on-premises and cloud applications.

- **Implement zero trust access control** by creating strong access policies to restrict users to resource access and resource-to-resource access. This is important for key management resources in the cloud.
- **Change default admin usernames and passwords.**
- **Do not use root access accounts for day-to-day operations**. Create users, groups, and roles to carry out tasks.
- **Implement password policies that require unique passwords of at least 15 characters**.
- **Enforce account lockout policies after a certain number of failed login attempts**. Log and monitor login attempts for brute force password cracking and password spraying.
- **Disable saving passwords to the browser in the Group Policy Management console**.
- **Implement Local Administrator Password Solution (LAPS)** where possible if your OS is older than Windows Server 2019 and Windows 10 as these versions do not have LAPS built in.
- Protect against Local Security Authority Subsystem Service (LSASS) dumping:
  - **Implement Credential Guard for Windows 10 and Server 2016**.
  - **Implement the Attack Surface Reduction (ASR) rule for LSASS**
- **Educate all employees on proper password security in your annual security training** to include emphasizing not reusing passwords and not saving passwords in local files.
- **Use Windows PowerShell Remoting, Remote Credential Guard, or RDP** with restricted Admin Mode as feasible when establishing a remote connection to avoid direct exposure of credentials.
- **Separate administrator accounts from user accounts**. Only allow designated admin accounts to be used for admin purposes. If an individual user needs administrative rights over their workstation, use a separate account that does not have administrative access to other hosts, such as servers.

Initial Access Vector: Phishing

- **Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents.**
- **Implement flagging external emails in email clients.**

- **Implement filters at the email gateway to filter out emails** with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the email scanner.
- **Enable common attachment filters to restrict file types** that commonly contain malware and should not be sent by email.
- **Implement Domain-based Message Authentication, reporting and Conformance (DMARC) policy and verification** to lower the chance of spoofed or modified emails from valid domains. DMARC protects your domain from being spoofed but does not protect from incoming emails that have been spoofed unless the sending domain also implements DMARC. DMARC builds on the widely deployed Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email.
- **Ensure macro scripts are disabled for Microsoft Office files transmitted via email**. These macros can be used to deliver ransomware.
- **Disable Windows Script Host (WSH)**. Windows script hosting provides an environment in which users can execute scripts or perform tasks.

Initial Access Vector: Precursor Malware Infection

- **Use automatic updates for your antivirus and anti-malware software and signatures**. Ensure tools are properly configured to escalate warnings and indicators to notify security personnel. Use a centrally managed antivirus solution. This enables detection of both “precursor” malware and ransomware.
- **Use application allowlisting and/or endpoint detection and response (EDR) solutions** on all assets to ensure that only authorized software is executable and all unauthorized software is blocked.
    - For Windows, enable Windows Defender Application Control (WDAC), AppLocker, or both on all systems that support these features.
    - § WDAC is under continuous development while AppLocker will only receive security fixes. AppLocker can be used as a complement to WDAC, when WDAC is set to the most restrictive level possible, and AppLocker is used to fine-tune restrictions for your organization.
    - Use allowlisting rather than attempting to list and deny every possible permutation of applications in a network environment.

Initial Access Vector: Advanced Forms of Social Engineering

- **Create policies to include cybersecurity awareness training** about advanced forms of social engineering for personnel that have access to your network. Training should include tips on being able to recognize illegitimate websites and search results. It is also important to repeat security awareness training regularly to keep your staff informed and vigilant.

- **Consider implementing sandboxed browsers** to protect systems from malware originating from web browsing. Sandboxed browsers isolate the host machine from malicious code.

Initial Access Vector: Third Parties and Managed Service Providers

- **Consider the risk management and cyber hygiene practices of third parties or managed service providers (MSPs)** your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting numerous client organizations.
- **Ensure the use of least privilege and separation of duties when setting up the access of third parties**. Third parties and MSPs should only have access to devices and servers that are within their role or responsibilities.

Ransomware and Data Extortion Response Checklist

Detection and Analysis

1. **Determine which systems were impacted, and immediately isolate them.**
    - If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
    - Prioritize isolating critical systems that are essential to daily operations.
    - If taking the network temporarily offline is not immediately possible, locate the network cable (e.g., ethernet) and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
    - For cloud resources, take a snapshot of volumes to get a point in time copy for reviewing later for forensic investigation.
    - After an initial compromise, malicious actors may monitor your organization’s activity or communications to understand if their actions have been detected. Isolate systems in a coordinated manner and use out-of-band communication methods such as phone calls to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access or deploy ransomware widely prior to networks being taken offline.

2. **Power down devices if you are unable to disconnect them from the network to avoid further spread of the ransomware infection.**

Note: This step will prevent your organization from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. **It should be carried out only if it is not possible to temporarily shut down the network or disconnect affected hosts from the network** using other means.

3. **Triage impacted systems for restoration and recovery.**
   - Identify and prioritize critical systems for restoration on a clean network and confirm the nature of data housed on impacted systems.
   - Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.

4. **Examine existing organizational detection or prevention systems (e.g., antivirus, EDR, IDS, Intrusion Prevention System) and logs.** Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.

5. **Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis**.

6. **Initiate threat hunting activities.**

   For enterprise environments, check for:

   - Newly created AD accounts or accounts with escalated privileges and recent activity related to privileged accounts such as Domain Admins.
   - Anomalous VPN device logins or other suspicious logins.
   - Endpoint modifications that may impair backups, shadow copy, disk journaling, or boot configurations. Look for anomalous usage of built-in Windows tools such as bcdedit.exe, fsutil.exe (*deletejournal*), vssadmin.exe, wbadmin.exe, and wmic.exe (*shadow copy* or *shadowstorage*). Misuse of these tools is a common ransomware technique to inhibit system recovery.
   - Signs of any unexpected usage of remote monitoring and management (RMM) software (including portable executables that are not installed). RMM software is commonly used by malicious actors to maintain persistence.
   - Any unexpected PowerShell execution or use of *PsTools* suite.

- Signs of enumeration of AD and/or LSASS credentials being dumped (e.g., Mimikatz, *Sysinternals ProcDump, or NTDSutil.exe*).
- Signs of unexpected endpoint-to-endpoint (including servers) communications, for example, Address Resolution Protocol (ARP) poisoning of an endpoint or command and control traffic relayed between endpoints.
- Potential signs of data being exfiltrated from the network, which may include:

  i. Abnormal amount of data outgoing over any port. Open source software can tunnel data over various ports and protocols. For example, ransomware actors have used Chisel to tunnel Secure Shell (SSH) over HTTPS port 443. Ransomware actors have also used Cloudflare to abuse Cloudflare tunnels to tunnel communications over HTTPS.

  ii.Presence of Rclone, Rsync, and various web-based file storage services, and FTP/SFTP, which are common tools for data exfiltration (and also used by threat actors to implant malware/tools on affected networks).

- Newly created services, unexpected scheduled tasks, unexpected software installed, unusual files created, legitimate processes with unexpected child processes, etc.

Reporting and Notification

7. Follow notification requirements as outlined in your cyber incident response and communications plan to **engage internal and external teams and stakeholders** with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.

- Share the information you have at your disposal to receive timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leader.
- Report the incident to—and consider requesting assistance from—CISA, your local FBI field office, the FBI Internet Crime Complaint Center (IC3), or your local U.S. Secret Service field office.

- As appropriate, coordinate with communications and public information personnel to ensure accurate information is shared internally with your organization and externally with the public.

If extended identification or analysis is needed, CISA, MS- ISAC and local, state, or federal law enforcement may be interested in any of the following information that your organization determines it can legally share:

- Recovered executable file.
- Copies of the readme file – DO NOT REMOVE the file or decryption may not be possible.
- Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally).
- Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally).
- Malware samples.
- Names of malware identified on your network.
- Encrypted file samples.
- Log files (e.g., Windows event logs from compromised systems, firewall logs).
- PowerShell scripts found having executed on the network.
- User accounts created in AD or machines added to the network during the exploitation.
- Email addresses used by the attackers and any associated phishing emails.
- Other communication accounts used by the attackers.
- A copy of the ransom note.
- Ransom amount and if the ransom was paid.
- Bitcoin wallets used by the attackers.
- Bitcoin wallets used to pay the ransom, if applicable.
- Copies of any communications with attackers.

8. If the incident resulted in a data breach, **follow notification requirements as outlined in your cyber incident response and communications plans.**

Containment and Eradication

If no initial mitigation actions appear possible:

9. Take a system image and memory capture of a sample of affected devices (e.g., workstations, servers, virtual servers, and cloud servers). Collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected). The contacts below may be able to assist you in performing these tasks.

   Preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).

10. **Consult federal law enforcement, even if mitigation actions are possible, regarding possible decryptors available,** as security researchers may have discovered encryption flaws for some ransomware variants and released decryption or other types of tools.

To continue taking steps to contain and mitigate the incident:

11. **Research trusted guidance** (e.g., published by sources such as the U.S. Government, MS-ISAC, or a reputable security vendor) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.

    Kill or disable the execution of known ransomware binaries; this will minimize damage and impact to your systems. Delete other known associated registry values and files.

12. **Identify the systems and accounts involved in the initial breach.** This can include email accounts.

13. Based on the breach or compromise details determined above, **contain associated systems that may be used for further or continued unauthorized access.** Breaches often involve mass credential exfiltration. Securing networks and other information sources from continued credential-based unauthorized access may include:

    Disable virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

14. If server-side data is being encrypted by an infected workstation, **follow server-side data encryption quick identification steps.**
    - Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files.
    - Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.
    - Review the TerminalServices-RemoteConnectionManager event log to check for successful RDP network connections.
    - Review the Windows Security log, SMB event logs, and related logs that may identify significant authentication or access events.
    - Run packet capture software, such as Wireshark, on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., smb2.filename contains cryptxxx).

15. **Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.**

- Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc.
- Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use of PowerShell scripts).
- Identification may involve deployment of EDR solutions, audits of local and domain accounts, examination of data found in centralized logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out.

16. **Rebuild systems based on prioritization of critical services** (e.g., health and safety or revenue-generating services), using pre-configured standard images, if possible. Use infrastructure as code templates to rebuild cloud resources.

17. **Issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility** once the environment has been fully cleaned and rebuilt, including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms. This can include applying patches, upgrading software, and taking other security precautions not previously taken. Update customer-managed encryption keys as needed.

18. **The designated IT or IT security authority declares the ransomware incident over** based on established criteria, which may include taking the steps above or seeking outside assistance**.**

Recovery and Post-Incident Activity

19. **Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.**
    - Take care not to re-infect clean systems during recovery. For example, if a new Virtual Local Area Network (VLAN) has been created for recovery purposes, ensure only clean systems are added.

20. **Document lessons learned from the incident and associated response activities** to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same.

21. **Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC** to benefit others within the community.