

MOUNT XION TECHNOLOGIES

Full report

The Cyber Risks Facing Texas Nonprofits, and How to Get Ahead of Them

What Texas nonprofits lose to fraud and breaches, and the controls that break the chain.

Donte Wong, CISSP, Founder and CEO

September 23, 2026

Evidence cutoff September 23, 2026

Full report. A shorter article accompanies it at mountxiontechnologies.com.

Evidence cutoff: September 23, 2026.

Audience: Executive directors, CFOs, board members, and IT leads of Texas nonprofits and foundations.

Scope: Public sources only. Organizations whose incidents are public through courts, regulators, or the press are named. The seven organizations known only from their own Form 990 filings are described by type, with their losses in bands, because each one disclosed on its own. Individuals are not named, and no leaked records or personal data are reproduced. Each “What could have” list, the “not enough on its own” list, and every recommendation in this study is a defensive design judgment, not a finding that a named organization lacked a control. Evidence labels, counts, and method are in Appendix D.

The floods and the copycat accounts

After the July 4, 2025 floods in the Texas Hill Country, scammers set up Venmo accounts impersonating the [Center Point Volunteer Fire Department’s newly created donation account](#), American Banker reported, and Venmo, which gave no official reason, froze the department’s real account until July 7. For the days that mattered most, the real channel was closed and the copycats were open. No one inside the department had to be deceived for the loss to happen. The copycats needed only its name.

Texas nonprofits hold three things worth stealing: money in motion, records about the people they serve, and a name that donors trust. This study follows each through Texas cases from 2018 to 2026, then sets out what a proportionate defense looks like, what it costs, and who should own it. One pattern runs through all of it: a control set up in advance can break the chain, whether or not anyone was deceived. A callback, a second approver, a record that was never stored, or a giving page claimed before the disaster can each do it.

The short version

1. **Money moves on one message.** A bounded search of Texas e-filed returns found seven Texas 501(c)(3)s that disclosed phishing, social engineering, cyberattack, or wire fraud losses for 2021 through 2024, and attackers also write to a nonprofit’s bank or tell its funders the account changed (Part 1). *Decision:* no single message, call, or sign-in can move money. Require a callback on a number already on file, a hold on the first payment to a changed account, and a second approver at the bank.
2. **One sign-in can reach everything.** Ascension’s Texas hospitals ran [almost a month without electronic health records](#) after an attack that, by Ascension’s account, began on one laptop, and state-sponsored groups target advocacy organizations’ mailboxes; a federal indictment alleges one such campaign against a Texas human rights group (Parts 2 and 3). *Decision:* the people who move money, run systems, or speak for the organization use phishing-resistant sign-in, and the Microsoft 365 license tier is chosen on purpose.
3. **Records you keep are records you report.** In the cases reviewed, letters reached people seven to fourteen months after the intrusion, at two organizations mostly because of file review, and in the Blackbaud incident what each nonprofit had stored set the size of its notice

(Part 2). *Decision*: keep less, delete on a board-approved schedule, and write breach notice and certified deletion into vendor contracts.

4. **Your name can be used without touching your systems.** Copycat donation accounts follow Texas disasters (Part 3). *Decision*: one named person owns the email domain, giving page, payment-app accounts, social handles, and published bank-change rules before the next disaster.
5. **The fixes cost staff time more than money.** Microsoft 365 Business Premium costs nonprofits \$5.50 per user per month now that the donated grant has ended, while one Texas security analyst at the median wage costs more than the security budget the CIS planning rule gives a \$5 million organization (Part 4). *Decision*: a Security Program Manager inside, outcomes bought outside, results in the board minutes, and about 1 percent of revenue as a budget check.

Part 1: The money

In 2023, thieves got into the bank accounts of a Texas faith-based social services nonprofit and moved between \$500,000 and \$1 million to international accounts. The organization reported recovering most of it from its bank and through insurance, and the filing does not split the recovery between the two. The same filing reports staff training, stronger sign-in, and security monitoring, without dates or order. It does not say how the thieves got in.

The loss is public because the organization reported it. A Form 990 filer must answer Yes on Part VI, line 5 when it learns of a [significant diversion of its assets, including theft by any person](#), once gross diversions exceed the lesser of 5 percent of gross receipts, 5 percent of total assets, or \$250,000. A bounded full-text search of Texas e-filed returns found seven Texas 501(c)(3)s that disclosed phishing, social engineering, cyberattack, or wire fraud losses from 2021 through 2024. The list is not complete, and each organization deserves credit for disclosing, so none is named here.

Organization	Reported loss	How it happened, as disclosed	What followed
Faith-based social services nonprofit	\$500,000 to \$1 million	Bank accounts accessed; funds sent to international accounts	Most recovered; training and new controls added
Youth organization	\$500,000 to \$1 million	Fake sign-in page; unauthorized transfers	Most recovered; ongoing training
Senior living community	\$500,000 to \$1 million	Wire fraud; incident not described	Not described
Private school	\$500,000 to \$1 million	Vendor impersonation	No recovery disclosed; internal controls added
Church-affiliated ministry	\$250,000 to \$500,000	Phishing; a contractor payment redirected	About a quarter recovered by the end of 2024
Nonprofit service provider	\$250,000 to \$500,000	Payment to a false contractor	Recovered through insurance; vendor verification added
Volunteer-run arts group	Under \$1,000	Phishing	Not described

Four of the seven involved a spoofed sign-in page or a misdirected vendor or contractor payment. Some attackers skip the staff entirely.

The attacker does not need your staff

Project 4031, a small Fort Worth 501(c)(3) that [assists families burdened by hospice care](#), is the only Texas nonprofit named as a business email compromise victim in the federal releases this study reviewed. The Fifth Circuit found that a ring member [emailed Origin Bank pretending to be Project 4031](#) and obtained cashier's checks drawn on its account. The request went to the bank, not to the charity's staff.

The same move works on funders. Attackers controlling a Fresno nonprofit finance director's email [told Fresno County](#) that the nonprofit's bank account had changed. In Kentucky, impostors [posing as a nonprofit](#) persuaded a Lexington city official to wire \$3,905,837.05 owed to it to a shell company; the bank and the city recovered all of it. Criminal complaints also allege that a look-alike domain [asked a foundation's grantee to email its bank details](#) instead of uploading them to the grant portal.

Texas churches see it by phone and in their clergy's names. The Texas Annual Conference of the United Methodist Church [said in September 2026](#) that its churches had been targeted by scams, including calls whose caller ID showed the church's own bank, and that some had lost money. An Episcopal diocese in North Texas [warned of emails impersonating its bishop and clergy](#).

Each of these is a party a nonprofit can brief in advance: its bank, its funders, its grantees, and its members. Greater Houston Community Foundation does this for donors, telling them it [will never update or request changes to wiring instructions by email](#).

Paper still counts. Houston Landing [reported](#) that the Houston Public Library Foundation found fraudulent checks drawn on its account late in 2022 and adopted positive pay with its bank in early 2023, and KSAT [reported](#) that San Antonio police said a \$95,000 donation check meant for a church was cashed by someone else.

The same script, nationally

St. Ambrose Parish in Ohio, which [FBI Cleveland confirmed](#) was a business email compromise victim, [paid a changed account twice](#), about \$1,750,000, before its real contractor called. The San Francisco Chronicle [reported](#) that One Treasure Island lost \$650,000 after its outside bookkeeper's mailbox was hacked; the money went to Frost Bank in Odessa, Texas, and \$37,375 came back. The Boston Globe [reported](#) that Save the Children sent nearly \$1 million on false invoices from a hacked mailbox, and that it afterward began confirming new vendors and bank instructions by phone.

Community IT Innovators, a managed IT provider for nonprofits, found that [all three 2024 wire fraud incidents among its clients](#) also involved a compromised internal account. In that sample, the mailbox takeover and the payment fraud were one incident seen from two desks.

What could have stopped the payment

- **A callback on a number already on file**, for every bank change that arrives by email, phone, or letter. The [FBI](#) and the [FTC](#) both advise it, and one of the Texas filers above and Save the Children adopted versions of it after their losses.
- **A hold on the first payment to a changed account**, released only after the callback is logged and a second person has reviewed it.
- **A second approver at the bank** for outgoing wires and new payees, so one stolen sign-in cannot move money alone. Outside bookkeepers belong under the same rules.
- **Positive pay** where checks are issued, as the Houston Public Library Foundation adopted, and the [FBI](#) and the [Postal Inspection Service](#) advise.
- **Rules agreed in advance** with the bank for requests made in the organization's name, and published to funders, grantees, and donors.
- **A recall plan**. IC3 says [time is of the essence](#): call the bank, request a recall, and file at www.ic3.gov, typed directly.
- **Insurance confirmed in writing**. Two of the Texas filers above and Save the Children recovered money through insurance, but [most insurers cannot cover voluntarily transferred funds](#). Ask the broker what pays for social engineering and funds transfer fraud.

Stewardship includes the systems

Nonprofit leaders already practice stewardship. Boards approve budgets, auditors test financial controls, and donors trust that a gift reaches the mission it was meant for. The systems that move that money and hold client records are part of the same duty. A wire sent to a false contractor is a stewardship loss whether it began with a forged invoice or a stolen password.

Employees are responsible for following procedure and reporting what looks wrong. The organization is responsible for making sure one mistake cannot become a loss.

My position is that the controls that matter most are rarely the most expensive. They are written down, owned by a named person, and tested before they are needed. A board does not need technical training to ask whether payment changes are verified, whether the people who move money sign in with phishing-resistant methods, and when a restore was last tested.

Donte Wong, CISSP, Founder and CEO, Mount Xion Technologies

Part 2: The records

When attackers want records instead of money, the cost arrives as downtime, notice letters, and lawsuits.

When the hospital goes to paper

By Ascension's account, the attack began on one laptop. A [September 2025 letter from Senator Ron Wyden to the FTC](#) sets out what Ascension told his staff: a contractor clicked a malicious Bing search result on an Ascension laptop in February 2024, and the attackers later used Kerberoasting

to take over privileged Active Directory accounts before pushing ransomware. Ascension had said in June 2024 that the file was [downloaded by someone who believed it was legitimate](#).

When the ransomware hit on May 8, it disrupted Ascension's Seton hospitals around Austin and Providence in Waco. The Austin American-Statesman [reported](#) that some Ascension Texas emergency rooms set up a process to divert ambulances; Ascension Texas did not name them, called diversions a normal course of operation, and said its local hospitals were not diverting as of May 14. [KWTX reported](#) receiving multiple reports of longer waits at Ascension Providence in Waco and said Ascension was using pen and paper. The Texas hospitals [got their electronic health records back on June 4](#), almost a month later, and some patients had been diverted to St. David's and Baylor Scott & White.

Other Texas nonprofit systems have been hit too. The reported disruption ranges from CHRISTUS's statement that patient care did not appear affected to weeks offline.

Organization	Incident	Reported disruption	Attribution	OCR count, Sept. 23, 2026	Count history
Ascension (Austin, Waco facilities)	May 2024	Diversion process at some Texas ERs; EHR down almost a month	Black Basta per CNN's sources ; no public claim as of Dec. 2024	5,466,931	5,599,699 reported to Maine AG , Dec. 2024
CommonSpirit / CHI St. Luke's (Houston)	Sept. to Oct. 2022	Six hospitals on internal disaster status ; paper orders about two weeks	None in sources cited	633,031	First reported as 623,774
CHRISTUS Spohn	Apr. to May 2022	CHRISTUS said patient care did not appear affected	AvosLocker claim	842,874	15,062 in 2022 ; Texas AG figure about 771,727, cited in a class action complaint
OakBend Medical Center (Richmond)	Sept. 2022	All systems offline ; clinical systems back in about three weeks	Daixin claim	500,000	Unchanged; Daixin claimed more than 1 million records
Hendrick Health (Abilene)	Nov. 2020	Network and EHR offline	None in sources cited	640,436	None found

OCR counts are from the [HHS OCR breach portal](#), export pulled September 23, 2026.

CommonSpirit's forensic investigation found the attackers [had been inside from September 16 to October 3, 2022](#), and OakBend [said it had implemented multi-factor authentication](#) and new threat-monitoring software afterward. The first public count is often not the last: CHRISTUS first reported 15,062 affected individuals, and the OCR portal now lists 842,874. Incident plans and board communications should expect the number to move.

Smaller organizations are hit too. The [OCR portal](#) lists hacking incidents at four smaller Texas 501(c)(3) health organizations in 2025 and 2026, each affecting from 12,490 to 35,236 people. One vendor can also stall many at once. The Change Healthcare breach [affected 11,331,028 Texans](#), and Legacy Community Health, which runs clinics across Texas, [processed about half of its claims](#) through Change; its CEO at the time said it had to extend a bank line of credit.

What could have shortened the downtime

- **Downtime procedures that are drilled, not only written**, for clinical care, revenue, and client services. Ascension Texas staff described interim systems as [taking three to five times longer](#). Paper order sets, downtime registration, and diversion criteria agreed with EMS cost little to rehearse.
- **Segmentation and transfer alerts**. The CommonSpirit and [CHRISTUS Spohn](#) notices describe attackers inside for about two and nearly four weeks. Separating patient-data servers from user networks and alerting on bulk outbound transfers are designed to surface activity within a window like that.
- **Identity hardening against the Ascension path**. Long or managed service account passwords, retiring weak Kerberos encryption, and separate admin accounts narrow the route from one laptop to privileged Active Directory accounts.
- **Backups that restore on a known clock**, with offline or immutable copies and restore times tested against what clinics can tolerate.
- **A second clearinghouse connection and a cash reserve** sized to a disrupted billing cycle, so one vendor outage is survivable.

Charities, churches, and universities

On November 10, 2024, Goodwill North Central Texas [closed all of its stores](#), Comparitech reported, citing a company-wide technical issue that later reporting showed was a cyber incident. In December the Rhysida ransomware group [claimed responsibility](#). In the reporting found, Goodwill has not attributed the attack. By late February 2025 it had [begun notifying 6,274 Texans](#).

Most incidents are quieter. These Texas charities, churches, and private universities appeared on the Attorney General’s breach listing as of September 23, 2026:

Organization	Texans affected	Information types listed	AG entry
Hill Country Bible Church, Austin	1,937	Other (notice by email)	BR-0005023, 05/11/2026
Texas Access to Justice Foundation, Austin	1,339	Includes Social Security, financial, medical, and health insurance information	BR-0004851, 02/24/2026
Evelyn Rubenstein Jewish Community Center of Houston	2,953	Includes health insurance information and date of birth	BR-0005090, 06/05/2026
Gladney Center for Adoption, Fort Worth (AG entity type Other)	2,008	Includes medical information and date of birth	BR-0004819, 02/06/2026

Organization	Texans affected	Information types listed	AG entry
Theology of the Body Evangelization Team, Irving	778	Name, address, other (notice by email)	BR-0004695, 12/02/2025
North Dallas Shared Ministries (Now-Forward), Dallas	250	Includes medical and health insurance information	BR-0005325, 09/11/2026
Heart of Texas Workforce Development Board, Waco	640	Name, Social Security number, date of birth	BR-0005324, 09/11/2026
USTA Texas Section, Austin (501(c)(4))	871	Name, Social Security number	BR-0005198, 07/23/2026
University of St. Thomas, Houston	24,158	Includes health insurance information and date of birth	BR-0005066, 05/28/2026
Nelson University, Waxahachie	21,905	Includes financial and medical information	BR-0005120, 06/18/2026
University of Dallas, Irving	7,313	Includes medical and health insurance information	BR-0005077, 05/29/2026
LeTourneau University, Longview	1,072	Name, financial account or card information	BR-0005335, 09/17/2026
Southern Methodist University, Dallas	266	Name, Social Security number, other, date of birth	BR-0004619, 10/17/2025

“Includes” marks a partial excerpt; the AG [warns](#) that listed details may change after posting.

Letters come months later. Our Lady of the Lake University’s notice came [about seven months](#) after its August 2022 intrusion, and the AvosLocker group had [posted a claim](#) in between. The Houston JCC’s [consumer notice](#) followed an employee mailbox intrusion by about eight months, and the Texas Access to Justice Foundation’s [file review](#) ended about eight months after its intrusion. The University of St. Thomas and the University of Dallas [reached the Attorney General](#) about nine months after their summer 2025 intrusions, and Nelson University about fourteen. At the Texas Access to Justice Foundation and Nelson, most of that time was file review: working out whose records were in the files. Texas deadlines run from the date the organization [determines that the breach occurred](#). This study makes no finding about whether any notice was timely.

Lawsuits follow. Plaintiffs’ lawyers said in a court filing that [41,825 class members were eligible](#) under Our Lady of the Lake’s preliminarily approved settlement; final approval could not be verified. The University of St. Thomas settlement, which the university entered while denying wrongdoing, lets class members claim [up to \\$4,500 in extraordinary losses](#), with a [final approval hearing on October 5, 2026](#).

How attackers got in is mostly unknown. The public record rarely shows initial access. Texas Wesleyan University’s notice shows the fix list instead: it [reset credentials for all community users and raised the minimum password length to 14 characters](#), and said it was working toward MFA for all external access to web services. Appendix D lists the organization types for which no incident was found.

What could have limited the theft

- **MFA on every external door, starting with mail**, with alerts on unfamiliar sign-ins and new forwarding rules.
- **A current data map**, with breach counsel and a forensic firm chosen before they are needed, so file review ends sooner.
- **Monitoring for the organization’s name on leak sites**, since claims often surface before letters.

Someone else’s platform

In 2020, ransomware hit Blackbaud, a for-profit public company whose customers, the [Texas Attorney General said](#), included educational institutions, healthcare groups, cultural organizations, and nonprofits holding Texans’ data. The FTC [alleges](#) that the attacker “purportedly” started with one customer’s login and password, moved across Blackbaud-hosted environments, and took customer data, and that Blackbaud paid 24 Bitcoin for a promise to delete it. Blackbaud’s first notices said donor bank and Social Security numbers were not accessed; the SEC [found](#) that by the end of July 2020 its staff knew the attacker had reached that data, in unencrypted form, for some customers. Blackbaud [neither admitted nor denied](#) the FTC’s allegations.

Action	Date	Outcome
SEC cease-and-desist order	March 9, 2023	\$3,000,000 civil penalty for misleading disclosures; Blackbaud consented without admitting or denying the findings
Multistate settlement	Announced October 5, 2023	\$49.5 million in total to 49 state attorneys general and the District of Columbia
Texas Assurance of Voluntary Compliance	October 18, 2023	Texas share of \$2,766,155.00, payable to the State
FTC Decision and Order	Dated May 17, 2024; announced final May 20, 2024	No fine or payment ; delete data no longer needed; publish and follow a retention schedule

What each nonprofit had stored set its exposure. The Dallas Morning News [reported](#) that the George W. Bush Presidential Center, the Boy Scouts of America, Communities Foundation of Texas, UT Austin, and others notified donors. UT Austin [told donors](#) that its development office does not store card, bank, or Social Security data, and Communities Foundation of Texas said the same of its Blackbaud data, the [Dallas Morning News reported](#). Texas Children’s Hospital said, as [KPRC 2 reported](#), that free-text fields in its fundraising database may have held patient names, dates of birth, treating physicians, and limited clinical information. The SEC order records concerns from customers that they had put donor Social Security and bank numbers into [fields that were not otherwise encrypted](#).

What the customer controls	What only the vendor controls
Who can sign in to its own account, and whether that login uses MFA (FTC complaint)	Whether one customer’s credential can reach other customers’ environments (FTC order IV.E.10)

What the customer controls	What only the vendor controls
Whether Social Security numbers, bank numbers, and clinical details go into the platform at all, including notes, custom fields, and attachments (SEC order; Texas Children's)	Whether the fields designed for those identifiers are encrypted (SEC order)
Its own retention schedule and purge of old records	How long backups are kept, and whether a former customer's data is deleted (Texas AVC; FTC complaint)
What its own notices promise donors, including any statement that stolen data was destroyed, which should rest on what the vendor can verify (FTC complaint)	The accuracy and timing of scope findings passed to customers (SEC order; FTC complaint)
Contract terms on notice, roles, and cost (Texas AVC 38(d))	Per-record logging detail after an incident (Beacon customer notice)
Patching of self-hosted plugins such as GiveWP (Wordfence)	Fix timing, storage configuration, cloud keys, and file-transfer software (Wordfence; The Register; Beacon customer notice; CISA)
Exit, and a demand for certified deletion at exit (FTC order, Provision II.A)	Whether deletion actually happens (FTC complaint)

Blackbaud is the deepest record, not the only one. When attackers exploited MOVEit Transfer in May 2023 (CISA and FBI), the National Student Clearinghouse, which [The Record](#) describes as a nonprofit, lost files for institutions on a [list](#) that includes Texas Christian University, Texas Woman's University, Texas A&M International, and Texas A&M Kingsville. Trinity University [said it did not use the tool](#), but several of its service providers told it students and employees were affected. The Register [reported](#) that a security researcher found 948,029 records exposed online in a database operated by DonorView, a cloud fundraising platform. The GiveWP donation plugin had a [remote code execution flaw](#) whose fix was [later bypassed](#). The British Deaf Association, a customer of the UK donor CRM Beacon, [said](#) Beacon confirmed that encrypted data was downloadable in readable form because the attacker used valid credentials, most likely a compromised AWS access key. The Baptist Paper [reported](#) that Beacon advertised ISO 27001:2022 certification when the breach occurred.

Texas law puts part of this on the vendor. A company holding data it does not own must [notify the owner immediately](#) after discovering a breach, and encrypted data counts as breached when the key is taken too. The owner's own deadlines still run from its own determination, so the contract should require vendor notice well inside them.

What could have limited the vendor exposure

- **Data that was never stored.** Keep Social Security, bank, and clinical details out of donor systems, free-text fields, attachments, and shared drives, and purge on a board-approved schedule. Three FTC commissioners called a retention and deletion schedule [a critical part of data security](#).
- **Contract terms Blackbaud is now bound by,** asked of every platform vendor: breach roles and notice duties (Texas AVC, [paragraph 38\(d\)](#)), a backup retention schedule with a set deletion timeframe (FTC order, [Provision III](#)), encryption of the fields that hold sensitive identifiers (FTC order, [IV.E.12](#)); also ask for certified deletion at exit.

- **An inventory of vendors' vendors**, since MOVEit reached Trinity through providers it chose, with any vendor's certification treated as a starting point, not proof.

Part 3: The name

After a Texas disaster

FBI San Antonio warned on July 9, 2025 that fraudsters were likely to pose as charities after the floods, and on July 17 the Attorney General announced an investigation into the schemes that diverted donations meant for Center Point. No outcome had been announced by this study's evidence cutoff. American Banker reported that the department's newly created account was a business profile rather than the charity profile meant for 501(c)(3)s, and could not be converted without deleting it.

The same floods produced a fake fundraiser in a grieving family's name. A Florida woman set up GoFundMe and Spotfund campaigns posing as the family of a person who died in the floods. She was charged under Texas's online impersonation statute and, according to court records KPRC reported, accepted a plea deal and was sentenced to 3 years in prison in July 2026. The Attorney General also sent a warning letter to the organizer of an unverified flood fundraiser, and News 4 San Antonio found dozens of Facebook pages mixing AI-generated images with real flood scenes to drive donations to fraudulent links.

The pattern repeats across Texas disasters:

Event	Attorney General alert	Guidance and context
Hurricane Harvey, 2017	September 1, 2017	Avoid charities that refuse details about identity, mission, costs, or use of donations. The FBI separately warned of copycat names similar to reputable charities.
Robb Elementary shooting, Uvalde, 2022	May 27, 2022, three days after the shooting	Scammers may exploit the tragedy to solicit donations.
Hill Country floods, July 2025	July 8, 2025, then the July 17 investigation	Watch for text-message solicitations (smishing); do not wire money or share bank, card, or Social Security numbers.
Texas floods, July 2026	July 17, 2026	Stay vigilant against scams, fraudulent charities, and price gouging. The Governor requested a Presidential Disaster Declaration for 28 counties that day; FEMA declared major disaster DR-4935 on September 1, 2026.

Impersonation costs the real nonprofit three ways. A gift sent to a copycat is revenue the organization never receives; FBI El Paso warns that fake charities divert donations to their creators. The donation channel itself can go dark, as Center Point's did. Donors told by the Attorney General to be wary of text solicitations bring that caution to the real appeal, which now competes with the

warning. Most Texas charities do not have to register with the state, so there is no general state registry of charities to check. The IRS Tax Exempt Organization Search confirms that an organization exists and is exempt, but it does not say which payment handle is real. The organization’s own page is the reference point. The Attorney General can act against solicitations that falsely claim a nonprofit’s affiliation, with penalties up to \$10,000 per violation, and online impersonation with intent to harm or defraud is a third-degree felony.

What could have protected the name

- **An official giving page published before the disaster**, listing every authorized donation method, payment handle, and approved third-party fundraiser, linked from the organization’s social profiles.
- **Payment-app accounts opened in calm conditions**, under the account type meant for charities, and the organization’s name and close variants claimed on the major platforms.
- **Early listing on platform verified hubs**, such as GoFundMe’s flood relief page.
- **A rapid reporting path**: one person captures evidence and reports to the platform, to the Attorney General’s Consumer Protection Division at 1-800-621-0508 or its online complaint form, and to the National Center for Disaster Fraud at 866-720-5721.
- **The freeze planned with the bank**, agreeing expected volume and a contact who can review a hold, and keeping two published channels so one hold does not take giving offline.

When the name draws a government

A public voice on human rights or religious freedom draws a different attacker. A federal indictment unsealed in March 2025 (S.D.N.Y. 24 Cr. 687) describes a victim it calls Organization-2: a Texas-based organization focused on promoting human rights and religious freedom in China. DOJ does not name it, and this study does not try to. The indictment alleges that an officer of China’s Ministry of Public Security directed the contractor i-Soon to compromise multiple Organization-2 email accounts in or around July 2018, and to compromise the organization again in or around June 2020. DOJ alleges that i-Soon charged roughly \$10,000 to \$75,000 for each inbox it successfully exploited. These are unproven allegations, and DOJ says the defendants remain at large.

Organization-2 is not unusual in kind. Microsoft’s 2025 Digital Defense Report puts think tanks and NGOs at 7 percent of the nation-state notifications it sent customers and 13 percent of Russian targeting. The May 2024 CISA-led civil society guide treats advocacy, faith-based, cultural, academic, and diaspora organizations that defend human rights and democracy as high-risk. By this study’s approximate count of the IRS exempt organization file, 2,402 Texas 501(c)(3)s carry NTEE codes chosen as a rough proxy for that profile; the proxy includes relief groups and leaves out faith, cultural, and academic groups (method in Appendix D).

The lures Microsoft has documented share a shape: a plausible invitation, then a sign-in or a scan.

Lure	Actor (per Microsoft)	Mitigation
Hotel or conference captive portal offers a browser or operating system update	Storm-2945, a Midnight Blizzard sub-cluster	Treat guest wireless networks as untrustworthy (Microsoft); install updates only from the device’s own settings

Lure	Actor (per Microsoft)	Mitigation
Fake Teams invitation, or a captive portal redirect, leading to a device code sign-in	Storm-2372; Storm-2945 since July 2026	Block the device code flow wherever possible (Microsoft)
Fake summit invitation PDF with a QR code to an adversary-in-the-middle page	Void Blizzard	Phishing-resistant MFA (baseline controls, Part 4)
WhatsApp group invitation from an impersonated US official, with a device-linking QR code	Star Blizzard	Confirm the sender through a contact looked up independently (FBI); review linked devices on messaging apps
Impersonated journalist sends a benign request for comment first	Mint Sandstorm	Confirm through the outlet; prohibit automatic forwarding to external addresses (FBI and partners)

What could have protected the mailbox

- **Close the device code path.** [Microsoft recommends](#) blocking it wherever possible. Entra ID P1 tenants can use Microsoft's managed [Block device code flow policy](#); security defaults block it only in tenants created from July 1, 2026.
- **Phishing-resistant keys for the people who travel and speak**, starting with executives, board officers, and staff who appear at policy events.
- **Conference Wi-Fi treated as hostile**, with no update ever installed from a sign-in page.
- **Invitations verified the way finance verifies bank changes.** An [FBI-led advisory](#) lists impersonated journalist interviews and conference invitations as lure themes.

One owner for the name

An organization's name lives in several places: its email domain, its giving page, its payment-app accounts and social handles, its bank's rules for requests made in its name, and leak sites, where claims such as [Qilin's listing of Nelson University](#) have preceded notices. DMARC set to reject decides whether someone else can send mail as the organization. When these pieces sit with different people, or with no one, gaps open between them. Naming one owner for the set is a governance decision, not a purchase.

Part 4: What to do about it

This part answers five questions in order: what is not enough, what the law requires, what to put in place at your size, what it costs, and who owns it, ending with what the board should see. Appendix B turns it into a first 90 days.

What is not enough on its own

- **Annual awareness training.** Spoofed login pages and [calls showing a church's own bank on caller ID](#) are built to deceive a careful person, and training does not add a second approver.
- **MFA that can be phished.** [Device-code phishing](#) and [OAuth consent phishing](#) get around it.

- **Insurance.** Many cyber claims close without payment (see What it costs).

The legal floor in Texas

This section, the board section, and Appendix E are general information from statute, regulation, and contract text, not legal advice.

- **Breach notice.** A person doing business in Texas that owns or licenses computerized data containing sensitive personal information must notify the individuals whose data was, or is reasonably believed to have been, acquired by an unauthorized person, without unreasonable delay and no later than 60 days after determining that a breach occurred. The Attorney General must also be notified within 30 days when 250 or more Texans are involved ([Bus. and Com. Code 521.053](#)). The [Code Construction Act](#) defines “person” to include corporations and associations, which supports applying the duty to nonprofit corporations; no court decision on the point was identified.
- **Privacy and the safe harbor.** The [Texas Data Privacy and Security Act](#) exempts nonprofits. [Chapter 542](#), added by SB 2610 in 2025, bars exemplary damages against a business entity under 250 employees that demonstrates it implemented and maintained a qualifying program at the time of the breach. The program must conform to a listed framework at every size, with CIS Controls IG1 named for 20 to 99 employees, but “business entity” is undefined, so whether nonprofits qualify is a question for counsel.
- **Duties that arrive with money.** Federal awards carry [2 CFR 200.303\(e\)](#) cybersecurity safeguards down to subrecipients, and the [Texas HHS Data Use Agreement](#), a contract term incorporated into HHS agreements, requires contractors to report a breach within 1 hour for data from a federal system of records, which includes Medicaid data, and within 24 hours for other confidential information. Health information handled on a nonprofit basis falls under [Health and Safety Code chapter 181](#), subject to its exemptions.
- **Limited state help.** The [Texas Cyber Command](#) serves governmental entities and critical infrastructure; nonprofits can use its reporting paths ([Appendix C](#)).

The full obligations table is in [Appendix E](#).

What to put in place at your size

This study sizes the program by the three headcount tiers of [chapter 542](#), which track how small organizations staff and budget, whether or not a nonprofit can claim the safe harbor itself. Find your column first.

	Under 20 employees	20 to 99 employees	100 to 249 employees
Framework	Cyber Essentials for the leader; NIST SP 1300 as the program document	CIS Controls IG1 , which chapter 542 names for this band	NIST CSF 2.0, with CISA CPG 2.0 as the goal set
Microsoft 365	Basic with security defaults, unless the risk triggers below apply	Premium is the practical line	Premium

	Under 20 employees	20 to 99 employees	100 to 249 employees
Configuration	The baseline below	Run ScubaGear; phishing-resistant MFA for all users (MS.AAD.3.1v1); two to eight Global Administrators (MS.AAD.7.1v1)	Incident response plans drilled at least annually (CPG 1.C); a named goal for managed service provider risk (CPG 1.E)
People	A named Security Program Manager and a monitoring provider	An IT generalist or managed service provider, plus monitoring	An in-house security lead becomes realistic
Budget	CIS Tier 1 ranges below	CIS Tier 2 ranges below; DIR cooperative contracts for qualifying assistance organizations	Priced from the wage table below

The Microsoft 365 licensing line. Microsoft cancelled the donated Business Premium grant of 10 free licenses at each organization’s first renewal on or after July 1, 2025. What remains is up to 300 free Business Basic licenses and discounts of up to 75 percent on many offers ([Microsoft Learn](#)).

	Business Basic (nonprofit grant)	Business Premium (nonprofit price)
Price	Free for up to 300 users (Microsoft)	\$5.50 per user per month, paid yearly, 1 to 300 users (Microsoft)
Identity	Entra ID Free with security defaults (Microsoft Learn)	Adds Entra ID P1 with Conditional Access (Microsoft Learn)
Devices	Basic Mobility and Security, a limited subset of Intune with no macOS support or mobile app management (Microsoft Learn)	Intune Plan 1 (Microsoft Learn)
Endpoint	Defender for Business sold separately (Microsoft Learn)	Defender for Business included (Microsoft Learn)
Email threat protection	URL time-of-click protection (Microsoft)	Defender for Office 365 Plan 1 (Microsoft Learn)

For 25 staff at the published prices, checked September 23, 2026, the Basic grant costs \$0 a year and Premium \$1,650 (25 × \$5.50 × 12), against \$6,600 at the [commercial price](#). An organization that kept Premium only for the 10 people who had donated licenses pays \$660. Basic with security defaults is a defensible start for an organization with no managed laptops and no high-risk work. Move to Premium once the organization manages laptops, moves large payments, holds health or client records, sends staff to policy events, or fits CISA’s high-risk civil society profile, because Conditional Access is what lets it require phishing-resistant sign-in for the people who matter most. Headcount does not set the risk.

Baseline controls at every size:

- **Phishing-resistant MFA as the goal.** CISA calls it the gold standard and names FIDO/WebAuthn as the only widely available form ([CISA](#)). Start with administrators, payment approvers, and executives, and keep two cloud-only emergency access accounts ([Microsoft Learn](#)). Until then, CISA ranks app one-time codes or push with number matching as the best interim options and SMS or voice as a last resort.

- **Legacy authentication blocked**, through security defaults or [SCuBA MS.AAD.1.1v1](#). Security defaults are on by default only in tenants created on or after October 22, 2019 ([Microsoft Learn](#)).
- **The domain authenticated**. SPF, DKIM, and DMARC moving to reject, and automatic external forwarding off ([SCuBA Exchange Online baseline](#)).
- **Payment changes verified out of band**, as set out in Part 1.
- **Backups that survive the attack**: automatic, encrypted, and with one copy offline ([Cyber Essentials](#)), with restores tested ([CISA](#)).
- **Card donations through a processor-hosted page or redirect**, validated with SAQ A as the acquirer requires ([PCI SSC](#)).
- **A named account for every employee and volunteer** ([Texas DIR](#)), with admin accounts kept out of daily work ([CISA civil society guide](#)).
- **A written, exercised incident plan** with the Texas deadlines, kept in hard copy. [DIR's 2024 breach guide](#) states deadlines that do not reflect the 30-day Attorney General rule SB 768 set in 2023, so use the statute.

Appendix A turns these into a checklist, with the frameworks and the points where official guidance disagrees.

What it costs

The public evidence does not support one correct number for security spending. In the [2024 NTEN and Heller Consulting survey](#) of over 300 nonprofits, 45 percent said they spend too little on technology and 20 percent reported a technology budget below \$10,000.

The Center for Internet Security offers a planning rule. [The Cost of Cyber Defense, version 1.1](#) concludes that implementing CIS Controls IG1 should cost less than an IT budget of 5 percent of revenue and/or a cybersecurity budget of 20 percent of that IT budget, which combined is 1 percent of revenue. Both percentages are CIS modeling assumptions, not measured nonprofit spending, and CIS leaves out labor, training, and consulting.

CIS IG1 annual cost estimate	Tier 1 (1 to 10 employees)	Tier 2 (10 to 100 employees)	Tier 3
On-premises tools, tools only	\$5,906 to \$38,124	\$35,088 to \$176,961	\$220,760 to \$1,446,187
MSP services	\$23,000 to \$41,000	\$44,000 to \$200,000	\$208,000 to \$1,800,000
CSP services	\$23,000 to \$255,000	Not in the evidence reviewed	Not in the evidence reviewed

Source: [CIS, The Cost of Cyber Defense v1.1](#), Table 4 and Table 5. The on-premises figures are vendor quotes carried over from v1.0 (August 2023), and CIS says Tier 1 MSP offerings meet most, not all, IG1 Safeguards.

Illustration using the CIS planning rule, not a quote.

Annual revenue	IT budget at 5% of revenue	Cybersecurity budget at 20% of IT	Against the CIS ranges
\$200,000	$\$200,000 \times 0.05 = \$10,000$	$\$10,000 \times 0.20 = \$2,000$	Below the Tier 1 on-premises low end (\$5,906); the Basic grant with security defaults, staff time, and the Part 1 payment controls carry the program
\$750,000	$\$750,000 \times 0.05 = \$37,500$	$\$37,500 \times 0.20 = \$7,500$	Above the Tier 1 on-premises low end (\$5,906); below the Tier 1 MSP low end (\$23,000)
\$5,000,000	$\$5,000,000 \times 0.05 = \$250,000$	$\$250,000 \times 0.20 = \$50,000$	Covers the full Tier 1 MSP range and the Tier 2 MSP low end (\$44,000)
\$25,000,000	$\$25,000,000 \times 0.05 = \$1,250,000$	$\$1,250,000 \times 0.20 = \$250,000$	Above the Tier 2 MSP high end (\$200,000)

Against the CIS Tier 2 managed service range, which starts at \$44,000, a 25-person organization's \$1,650 Premium license is the small line. Price licensing at nonprofit rates; price labor and monitoring from wage data or real quotes.

Program	What it offers	Eligibility limits
Microsoft 365 Business Basic grant	Free for up to 300 users	Eligible nonprofits; lacks the Premium security features above
Google Workspace for Nonprofits	\$0 per user per month; discounts on paid editions	Eligible nonprofits
Okta for Good	50 free Workforce Identity licenses with single sign-on and adaptive MFA	Eligible 501(c)(3)s; excludes hospitals, healthcare, schools, and government entities
Cloudflare Project Galileo	Free protection, including Business plan features	At-risk organizations in human rights, civil society, journalism, or democracy, brought or approved by a Cloudflare trusted partner
CISA Cyber Hygiene Services	Free services, including vulnerability scanning	U.S. governments and public and private sector critical infrastructure organizations; nonprofits are not named as a general eligible class

Federal grants. FEMA's Nonprofit Security Grant Program funds physical and cybersecurity enhancements at nonprofits at high risk of terrorist or extremist attack, and its FY 2026 Authorized Equipment List includes encryption software, anti-malware, firewalls, and intrusion detection. A nonprofit may request up to \$200,000 per site. FY 2026 allocated \$17,533,563 to Texas streams (this study's sum; detail in Appendix C). Texas nonprofits apply through the Office of the Governor's Public Safety Office, whose eGrants notice opened January 12 and closed March 12, 2026. FEMA later extended the state agencies' deadline from July 24 to July 31, 2026. FY 2027 is the next opportunity.

Insurance. The [NAIC](#) counted 28,555 cyber claims closed without payment in 2024 against 9,941 with payment at U.S.-domiciled insurers, excluding alien surplus lines; excess policies drive much of the gap (10,802 unpaid against 514 paid), while primary policies run about 1.9 to 1. It gives no reasons, so this is not a denial rate, but it is a reason to read coverage terms before an incident. The [CIAB](#) reported cyber premiums down 3.2 percent in the second quarter of 2026, the ninth straight quarterly decrease. Applications ask about controls; Travelers' [MFA supplement](#) asks whether MFA is required for all employees using web-based or cloud email. Bring evidence to renewal: MFA on email, endpoint protection, and a dated restore test, and get written confirmation of what covers payment diversion.

Budget line	How to price it	Source in this study
Microsoft 365 licensing	Users × \$5.50 × 12 for Premium; \$0 for the Basic grant	Microsoft nonprofit price
Managed IT and monitoring	Written quotes, checked against the CIS ranges	CIS Cost of Cyber Defense v1.1
Phishing-resistant keys	One primary and one spare for each administrator, payment approver, and executive, at the vendor's current price	Not priced in this study
Password manager	Users × the vendor's nonprofit price	Not priced in this study
Offline backup and a timed restore	Storage cost plus staff hours	Not priced in this study
Cyber and crime insurance	Broker quote, with written confirmation of social engineering and funds transfer coverage	NAIC; Nonprofits Insurance Alliance
Breach counsel and forensics	Terms agreed in advance	Part 2
Security Program Manager time	Hours × loaded rate (salary × 1.40)	BLS ECEC

Add the lines and compare the total with the 1 percent check.

Who does the work

Deciding who owns security comes before deciding whom to hire. CISA's [Cyber Guidance for Small Businesses](#) calls leaving security to the IT team alone a common mistake. It tells the chief executive to select a Security Program Manager, who need not be a security expert or even an IT professional, and who reports progress and roadblocks at least monthly. The role can sit with an operations or finance lead. A design judgment built on that guidance:

Duty	Cadence	Record it produces
Report progress and roadblocks to the executive director	Monthly	One-page report
Review the payment-change callback log with finance	Monthly	Signed log review
Keep the list of the organization's domain, DMARC setting, giving page, payment-app accounts, and handles	Quarterly	Dated list
Keep the vendor inventory and receive provider reports	Quarterly	Inventory and reports on file

Duty	Cadence	Record it produces
Run the tabletop and the timed restore	At least annually	Dated results
Bring results to the board	Each board meeting	Board minutes

The technical work can come from several places, and most Texas nonprofits will combine more than one. The table is this study's design judgment.

Model	Usually fits	What it covers well	What to settle in advance
Volunteer or board member with IT background	Fewer than 10 staff, little or no technology budget	Advice, vendor selection, reading provider reports, asking the board's technical questions	Keep oversight separate from hands-on administration; do not let one volunteer hold the only administrator credentials; if the person is paid for IT work, see the volunteer-status and conflict-of-interest points in the board section and Appendix E
IT generalist with security duties	Roughly 10 to 100 staff with devices and an office to support	Daily administration, device setup, joiner and leaver accounts	Security competes with every other ticket; pair the role with a monitoring service and a named program owner
Managed service provider (MSP)	Most organizations without internal IT, through Tier 2	Help desk, patching, backups, licensing, baseline security	A shared-responsibility map; see the provider contract list below
MSSP or outsourced security operations center	Any organization that cannot watch its own systems around the clock	Monitoring, alert triage, response support	Monitoring scope and authority; see the provider contract list below
Fractional or virtual CISO	Organizations that need program ownership, board reporting, policy, and insurance and contract answers, but not a full-time executive	Strategy, risk register, board and auditor reporting, vendor oversight	Separate assessment from operation where budget allows, or disclose the overlap to the board
In-house security lead	Larger organizations, health systems, and contractors holding sensitive government data	Continuous ownership, internal authority, faster decisions	One person is a single point of failure; the role still needs monitoring coverage and a backup

What the people cost. BLS's [May 2025 wage estimates](#), released May 15, 2026, give these [Texas medians](#); metro figures are in Appendix D. Benefits add about 40 percent: BLS [Employer Costs for Employee Compensation](#) puts private-industry benefits at 28.7 percent of total compensation in the West South Central division (June 2026, all occupations, not IT or nonprofit rates), so multiply a salary by roughly 1.40.

Role (SOC code)	Texas employment	Texas median wage	Approximate loaded cost (median × 1.40, this study's arithmetic)
Computer user support specialist (15-1232)	72,030	\$59,490	About \$83,000
Network and computer systems administrator (15-1244)	34,840	\$101,240	About \$142,000
Information security analyst (15-1212)	16,130	\$129,890	About \$182,000
Computer and information systems manager (11-3021)	73,060	\$171,530	About \$240,000

One information security analyst at the Texas median costs more than the entire security budget the CIS rule gives a \$5 million organization. The market is tight as well: CyberSeek counted [42,559 cybersecurity job postings in Texas](#) from May 2024 through April 2025, and in the global [ISC2 2025 workforce study](#) 33 percent of respondents said their organizations lack the resources to adequately staff their teams.

What to put in a provider contract. A provider relationship works best when both sides know who owns what:

- **MFA on every provider account** used to reach the organization's systems, as a joint [CISA advisory](#) says contracts should require.
- **Security vetting before access**, as the [National Council of Nonprofits](#) advises.
- **Proportionate controls with periodic evidence**, the model [Government Code 2054.138](#) applies to state agency vendors, scaled down.
- **A shared-responsibility map** of which IG1 Safeguards the provider owns and which stay with the nonprofit.
- **Monitoring scope in writing**: what is watched, during which hours, and who may disable an account or isolate a device.
- **Incident notice that leaves room inside the Texas deadlines.**
- **Accurate insurance answers**, so the organization's MFA attestation matches the real configuration.
- **Exit terms**: return of administrator credentials, documentation, and data.

Buy outcomes, not headcount

For most Texas nonprofits, a security hire is the wrong first step. The wage table above shows why, and one person is a single point of failure.

What an organization needs is outcomes it can verify: the measures in the quarterly board report below. Those outcomes can come from a managed service provider, a monitoring service, a fractional security leader, a capable IT generalist, or a mix. The contract is where they get written down.

Two things stay inside: ownership, meaning a named person who receives the reports and makes the call, and the board’s judgment about risk. Managed service providers are partners in this work, and the strongest partnerships are the ones where both sides can point to the same list of who owns which control.

Donte Wong, CISSP, Founder and CEO, Mount Xion Technologies

What the board should ask

The 2026 [NACD and Internet Security Alliance Director’s Handbook on Cyber-Risk Oversight](#) states that its principles apply to nonprofit boards. The [Nonprofit Risk Management Center](#) warns that an annual insurance briefing is not, by itself, risk oversight.

Texas law gives directors four practical points (detail in Appendix E): meet the ordinary care standard and document it ([BOC 22.221](#)); rely on management and outside experts only while no red flag is known ([BOC 3.102](#)); check whether the certificate of formation limits liability for directors and, since 2025, officers ([BOC 7.001](#)); and note that [chapter 521](#) places breach notice duties on the organization; whether any personal exposure follows for a director is a question for counsel.

Questions for the board:

1. Who in management is accountable for cyber risk, and how does the board hold them to it? ([CSF 2.0 GV.RR](#))
2. What is our approved cyber risk appetite? ([GV.RM-02](#))
3. Are security resources adequate for the strategy, and what results do we see each quarter? ([GV.RR-03](#), [GV.OV](#))
4. Where do we get independent cyber expertise, and whose reports are we relying on? ([NACD Principle Three](#))
5. Who decides on a ransom payment, and when does that decision come to the board? ([NACD Tool A](#))
6. What stops a fraudulent payment or a changed bank account? ([BoardSource](#))
7. Can we meet the Texas notice deadlines: individuals within 60 days, the Attorney General within 30 days for 250 or more Texans? ([Bus. and Com. Code 521.053](#))
8. Does our program follow a recognized framework sized to our headcount? ([chapter 542](#))
9. Are our D&O, cyber, and crime coverages adequate, and does our certificate of formation limit director and officer liability? ([BOC 8.151](#); [BOC 7.001](#))
10. Would a diversion cross the Form 990 line 5 threshold, and how would we disclose it? ([IRS](#))
11. Does our conflict of interest policy reach IT vendors connected to insiders? ([Form 990 line 12](#))
12. Have we built a relationship with our local FBI field office? ([NACD Tool O](#))

A quarterly board report can answer most of these on one page:

Measure	Where the study grounds it
Share of administrators, payment approvers, and executives on phishing-resistant MFA	Part 4, baseline controls
Payment and bank changes received, and how many were verified by callback	Part 1

Measure	Where the study grounds it
Date and length of the last timed restore from the offline copy	Part 2
Time to remove access for departing staff and former vendors	Part 4, who does the work
Vendor contracts still missing breach notice or certified deletion terms	Part 2
Risks accepted, each with an owner and a review date	CSF 2.0 GV.RM-02

The first 90 days are laid out in Appendix B.

Open questions and update triggers

This edition will be updated when any of the following occurs:

- the Texas Attorney General announces an outcome in the [Center Point investigation](#) or the [July 2025 GoFundMe warning letter](#);
- the church-affiliated ministry’s next return (its 2025 return was not yet in the IRS e-file index as of September 16, 2026) shows any further recovery;
- a follow-on pass verifies Goodwill North Central Texas’s primary breach notice, how long its stores stayed closed, and how many there are, which would make it a candidate opening for a public cut;
- the Ascension class action settles or reaches its [March 13, 2028 trial date](#), or a source explains why the OCR count is lower than the figure reported to Maine;
- the University of St. Thomas settlement reaches its [October 5, 2026 final approval hearing](#), or final approval of the Our Lady of the Lake University settlement is verified;
- a court, the Attorney General, or the Legislature settles whether a nonprofit is a “business entity” under [chapter 542](#);
- CISA issues the [CIRCI final rule](#), HHS finalizes the [HIPAA Security Rule update](#), or OMB finalizes the May 29, 2026 proposed revision to [2 CFR 200.303](#);
- FEMA announces [FY 2026 Nonprofit Security Grant Program awards](#) or publishes the FY 2027 notice;
- the [Texas Cyber Command](#) states whether private nonprofits are eligible for the TX-ISAQ;
- Microsoft changes commercial Business Premium pricing, which moves the nonprofit price under its [75 percent nonprofit discount](#);
- new Attorney General listings or OCR revisions change this study’s nonprofit breach counts, since [listings roll off after a year](#); or
- this edition is revised, which requires a fresh evidence cutoff, legal review, and link validation.

Appendix A: control checklist

Identity

- ☐ MFA is enforced for every user through security defaults or Conditional Access.
- ☐ Administrators, payment approvers, and executives use FIDO2 security keys or passkeys; SMS and voice are a temporary last resort.
- ☐ Legacy authentication is blocked.
- ☐ Two cloud-only emergency access accounts exist; Global Administrators number two to eight, ideally fewer than five.
- ☐ Each employee and volunteer has a named account; admin accounts are not used for daily work; departing users are disabled promptly.
- ☐ Passwords: 15 characters where used alone, 8 minimum behind MFA, no composition rules, password manager provided.
- ☐ Systems that cannot support MFA are reported to leadership.

Email and payments

- ☐ SPF, DKIM, and DMARC are published, moving toward p=reject.
- ☐ External auto-forwarding is off except for approved domains.
- ☐ Payment and bank changes are confirmed by calling an independently sourced number; releases require a second person.
- ☐ Check positive pay is on where checks are issued.
- ☐ Bank recall steps are written down; staff type www.ic3.gov directly.
- ☐ The broker has stated what covers voluntarily transferred funds.

Devices and data

- ☐ Updates are automatic; unsupported systems are replaced; Known Exploited Vulnerabilities are patched first (CISA).
- ☐ Devices are managed; at 20 or more employees, endpoints run detection and response.
- ☐ Payments run on a computer not used for browsing, as DIR advises.
- ☐ Backups are encrypted, one copy is offline, and restores are tested.
- ☐ Donations use a processor-hosted page or redirect, with SAQ A completed as the acquirer requires.
- ☐ Sensitive identifiers stay out of donor free-text fields; the board has adopted a retention and deletion schedule.

Vendors

- ☐ Every vendor with access is inventoried: IT provider, donation processor, web administrator, payroll, bookkeeping.

- ❑ Contracts require MFA on provider accounts, breach notice, and data destruction at exit.
- ❑ The donation processor's PCI DSS compliance is checked annually.

Response

- ❑ A written plan names a champion, current contacts (bank, insurer, counsel, forensics), and the Texas deadlines, with a printed copy offline.
- ❑ A tabletop runs at least annually.
- ❑ Staff can forward phishing to phishing@txcc.texas.gov, a Texas Cyber Command path open to anyone (TXCC).

Frameworks that fit

Framework	Issuer and scope	Where it fits
CISA Cyber Essentials	Written for leaders of small businesses and small and local government agencies. CISA does not name nonprofits; this study applies it to nonprofits of similar size (CISA).	Leader duties at every size
Guidance for Civil Society (May 2024)	Joint guide treating nonprofit, advocacy, and faith-based groups that defend human rights and democracy as high-risk communities (CISA)	Advocacy, policy, faith-based, and diaspora-serving nonprofits
NIST CSF 2.0 Small Business Quick-Start Guide (SP 1300)	NIST says it can assist nonprofits, government agencies, and schools (NIST). SB 2610 lists the NIST Cybersecurity Framework among qualifying frameworks (SB 2610).	Starting guide under 20 employees, where the program must still conform to CSF 2.0 or another listed framework; full CSF 2.0 at 100 and up
CIS Controls IG1	56 safeguards that CIS calls essential cyber hygiene, aimed at small to mid-size organizations with limited IT and security expertise (CIS)	Named benchmark for 20 to 99 employees
CISA SCuBA baselines	Secure configuration baselines that all organizations can use; CISA's ScubaGear checks a Microsoft 365 tenant against them at no cost (CISA)	Technical target for Microsoft 365 tenants
CISA Cross-Sector Performance Goals 2.0	December 11, 2025 revision aligned to NIST CSF 2.0; the civil society guide still cites the superseded v1.0.1 numbers (CISA)	Goal set for 100 to 249 employees

Where official guidance disagrees

Password length. Texas DIR's 2024 tip sheet says at least 8 characters of mixed-case letters, numbers, and symbols (DIR). The FTC says at least 12. NIST SP 800-63B-4, final in July 2025,

requires at least 15 characters for a password used alone, allows at least 8 for a password used only within MFA, and bars composition rules. This study's resolution: enforce MFA wherever available, set 15 characters as the floor wherever a password stands alone, accept 8 only behind enforced MFA, drop composition rules, and provide a password manager.

Backups. DIR advises backing up automatically, or at least weekly, to offsite or cloud storage. The [#StopRansomware Guide](#) warns that automated cloud backups may not suffice, because locally encrypted files can sync to the cloud and overwrite good copies. This study's resolution: a cloud copy counts as one copy, but at least one copy must be offline or out of reach of a compromised device, and restores must be tested.

Appendix B: 30/60/90-day action plan

First 30 days: close the cheapest paths

1. Name a Security Program Manager with a monthly report to the executive director.
2. Confirm security defaults or Conditional Access equivalents, confirm legacy authentication is blocked, and create two emergency access accounts.
3. Issue security keys or passkeys to administrators and payment approvers.
4. Adopt the call-back rule for payment changes; ask the bank about positive pay and record its recall contact.
5. Publish SPF, DKIM, and DMARC at p=none; turn off external auto-forwarding.
6. Make one offline backup copy and test a restore.
7. Report systems without MFA to the board.

By 60 days: set the program's shape

1. Choose the licensing line and budget it at list price.
2. Remove unused accounts and separate admin accounts.
3. Move online giving to a processor-hosted page or redirect and confirm SAQ A with the acquirer.
4. Adopt the password policy and deploy a password manager.
5. Train staff and volunteers, with role-based sessions for finance and leadership.
6. Review vendor contracts for MFA, breach notice, and data destruction.
7. Print a one-page incident plan with the Texas deadlines.

By 90 days: test and document

1. Run two tabletops: a bank-change request from a compromised vendor mailbox, and a restore from the offline copy.
2. Move DMARC toward p=reject after reviewing reports.
3. At 20 or more employees, run ScubaGear and record the results.

4. Adopt a retention schedule and purge sensitive identifiers from donor systems.
5. Review cyber and crime coverage with the broker.
6. Map the program to NIST CSF 2.0 or CIS IG1 and date the record; chapter 542, where it applies, looks at the program in place at the time of the breach ([Sec. 542.003](#)).
7. If the organization faces high risk of terrorist or extremist attack, prepare for the FY 2027 Nonprofit Security Grant Program; the FY 2026 notice lists adopting CISA's performance goals as an example project ([FEMA NOFO](#)).
8. Report to the board: MFA coverage, the restore result, payment changes verified, and open risks.

Appendix C: Texas resources

Every resource below was verified in this study's evidence. Eligibility and contact details can change; confirm them before relying on them.

Resource	What it offers	Notes
Texas Attorney General, Consumer Protection Division	Complaints about charity impersonation and flood-related scams at 1-800-621-0508 or through the online complaint form named in its July 2026 consumer alert	The office represents the public interest in charity .
Texas Attorney General, data breach reporting	The reporting page for breaches affecting 250 or more Texans, and the public listing of notices	Notice is due within 30 days under 521.053(i) .
Texas Cyber Command reporting paths	Phishing forwarding to phishing@txcc.texas.gov and TX-ISA0 threat reporting, open to anyone	Its formal incident reporting channels are for state agencies, higher education, and local governments.
TX-ISA0	Threat intelligence and a portal for sharing indicators; DIR's page says it is open to any entity in Texas, including the private sector	The Command describes sharing with governmental entities, federal agencies, and covered entities, so confirm eligibility first.
DIR cooperative contracts	Purchasing through DIR contracts for qualifying assistance organizations	Includes nonprofits providing educational, health, or human services, food banks, and approved legal aid providers.
FBI Internet Crime Complaint Center (IC3)	Complaints about fraud and cyber incidents, filed regardless of the amount; IC3 advises requesting a bank recall immediately	Type www.ic3.gov directly; criminals impersonate IC3.
FBI field offices in Texas named in this study	San Antonio and El Paso , both of which have issued charity-fraud warnings	The NACD handbook suggests boards build a relationship with the local field office .
IRS Form 990 instructions, Part VI, line 5	The definition of a significant diversion of assets , including theft by outsiders, and the reporting threshold	The board section sets out the threshold.

FY 2026 Nonprofit Security Grant Program allocations for Texas

FY 2026 NSGP stream	Total allocation	Actual allocation	Management and administration
Texas state (NSGP-S), outside the four urban areas	\$5,475,000	\$5,201,250	\$273,750
Houston Area	\$5,226,302	\$4,964,987	\$261,315
Dallas/Fort Worth/Arlington Area	\$5,010,308	\$4,759,793	\$250,515
San Antonio Area	\$996,995	\$947,145	\$49,850
Austin Area	\$824,958	\$783,710	\$41,248
Texas total (this study's sum)	\$17,533,563	\$16,656,885	\$876,678

These are allocations, not awards. FEMA [expected FY 2026 awards by September 30, 2026](#).

Appendix D: method, counts, evidence labels, and timeline

This appendix holds the counts and method behind the study's Texas figures.

How many Texas nonprofits and foundations

On September 23, 2026, this study counted the Texas file of the [IRS Exempt Organizations Business Master File extract posted September 8, 2026](#). The IRS assigns each record to a state by filing address and refreshes the extract monthly. The file holds 154,539 exempt organization records. Of those, 133,046 are 501(c)(3) organizations, of which, by the [IRS foundation codes](#), 10,735 are private foundations, 10,076 of them non-operating. Other published counts measure different things:

Measure	Figure	Date	Source
Texas EO BMF records (this study's count)	154,539	Posted Sept. 8, 2026	IRS EO BMF
501(c)(3) records in that file	133,046	Posted Sept. 8, 2026	IRS EO BMF
501(c)(3) private foundations in that file	10,735	Posted Sept. 8, 2026	IRS information sheet
Exempt organization returns and forms filed from Texas	170,266 (of 1,798,413 nationally)	Fiscal year 2025	IRS Data Book 2025, Table 1-3
Nonprofits in Texas	More than 130,000; about 1 in 20 Texas workers employed by a nonprofit	February 2025	Texas Senate Resolution 163
Private foundations in Texas	6,379, with 105,898 public charities and 21,873 other 501(c) organizations	Slide undated; deck trend data run through 2022	OneStar Foundation and North Texas Nonprofit Institute

This study uses the IRS file because it is current and dated.

How often Texas nonprofits report breaches

On September 23, 2026, this study matched filers in the [Texas Attorney General's Data Security Breach Reports](#) listing and the [HHS Office for Civil Rights breach portal](#) to Texas records in the [IRS EO BMF](#) by name and city, checking every match and near miss by hand. These are this study's computed statistics.

Dataset	Texas 501(c)(3) filers	People affected
Texas AG listing , all 633 entries	30 entries (4.74 percent) from 27 organizations; 29 distinct incidents	513,836 of 49,582,156 Texans (1.04 percent); 512,048 distinct
Texas AG listing , 262 entries with a Texas address	30 entries (11.45 percent); 37 (14.12 percent) from any exempt organization	513,836 of 7,475,106 Texans (6.87 percent)
HHS OCR, State TX, 2024	9 of 60 reports (15.0 percent); privately organized nonprofits 5 of 60 (8.3 percent)	2,510,683 matched; 442,155 at privately organized nonprofits
HHS OCR, State TX, 2025	12 of 57 (21.1 percent); privately organized 7 of 57 (12.3 percent)	273,094 matched; 72,064 at privately organized nonprofits
HHS OCR, State TX, Jan. 2 to Sept. 4, 2026	6 of 53 (11.3 percent); privately organized 5 of 53 (9.4 percent)	66,173 at privately organized nonprofits

Texas charities filed roughly one [AG entry](#) in twenty. Some matched filers are government: five AG entries (77,353 Texans) come from four community MHMR centers that hold 501(c)(3) status but are units of local government under [Health and Safety Code 534.001\(c\)](#), and such centers plus the Lubbock County Hospital District hold most matched individuals in the 2024 and 2025 [OCR data](#), so the table separates privately organized nonprofits.

NTEE group	AG entries	Texans affected
Health (E)	9	332,008
Education (B)	5	62,307
Human services (P)	3	2,403
Religion (X)	3	5,668
Other	10	111,450

Health carries most of the exposure, and one entry drives it: the [AG record for Lone Star Community Health Center](#) in Conroe reports 250,130 Texans, nearly half the nonprofit total. Its breach window, December 2 to 18, 2025, matches a [notice from Aesto Health](#), a health data archiving vendor that says its AWS environment was accessed then, and Lone Star's homepage links that notice, though Aesto's non-exhaustive client list does not name it. This reads as a vendor incident, not a direct attack.

The AG's own type field tags only [9 entries](#) as Nonprofit Organization, so counts that rely on it understate the rate.

Method limits:

- [Section 521.053\(j\)](#) removes AG notices after a year unless the entity files again, so the listing is a rolling snapshot: 630 of 633 entries were published September 26, 2025 to September 21, 2026.

- Only breaches of 250 or more Texans reach the AG (521.053(i)), and the OCR portal lists only breaches of 500 or more, one State per report.
- AG totals count people notified by several entities more than once, and out-of-state nonprofits were not matched, so the charity count is a floor.
- Name matching errs: an exact match paired Frost Bank's AG entry with an unrelated private foundation of the same name, which was rejected.

Nationally, the Identity Theft Resource Center counted 146 Non-Profit/NGO compromises in 2024, later restated as 145, and 139 in 2025, revised to 138 in its H1 2026 report. ITRC assigns sectors by SIC code, so the category excludes nonprofit hospitals, universities, and social services organizations.

Fraud reported to the FBI from Texas

Texas ranked second among states in the FBI IC3 2025 Internet Crime Report for complaints (97,912, behind California) and losses (\$1,825,636,181). IC3's 2025 Texas report counts 2,253 business email compromise (BEC) victims and \$304,318,015 in BEC losses, second only to investment fraud and about one dollar in six of Texas losses. Nationally, BEC losses reached \$3,046,598,558 on 24,768 complaints. These figures cover all complainants, not nonprofits alone.

What sector data shows

Community IT Innovators, an employee-owned managed IT provider serving US nonprofits with 15 to 300 staff, reports on its own clients, not the sector. Its 2025 report found that all three 2024 wire fraud incidents also involved an internal compromised account, and its 2026 report found the same in 2025's single case. Suspected account compromises rose to 648 in 2025 while confirmed ones held at 32, which the firm partly attributes to better alerting. It recorded zero ransomware incidents each year from 2022 through 2025.

The Verizon 2025 DBIR Small and Medium-Sized Business Snapshot found ransomware in 88 percent of breaches at organizations under 1,000 employees, against 39 percent at larger ones; the DBIR has no nonprofit category. Community IT's zero and Verizon's 88 percent describe different populations, and neither is a Texas nonprofit sample. For health nonprofits, HHS OCR reports that hacking and IT incidents were 81 percent of 2024 breaches of unsecured PHI affecting 500 or more people. None of these sources measures Texas nonprofits; the Texas cases in this study are its evidence.

What the searches did not find

Incidents at large Texas United Ways, YMCAs, Habitat for Humanity affiliates, Salvation Army units, dioceses, museums, zoos, or symphonies were not found in a bounded public-source search. That is not evidence that none occurred: the Attorney General's listing covers only breaches of 250 or more Texans and drops entries after a year. No CISA, NIST, BoardSource, National Council of Nonprofits, or NACD guidance on fractional CISOs or IT-skilled volunteers by name was found in a bounded public-source search.

Texas wages by metro area

Annual median wage, all industries, May 2025 (BLS OEWS):

Occupation	Dallas-Fort Worth-Arlington	Houston-Pasadena-The Woodlands	San Antonio-New Braunfels	Austin-Round Rock-San Marcos
Information security analysts	\$133,610	\$126,370	\$122,560	\$134,100 (low precision)
Network and computer systems administrators	\$103,260	\$101,430	\$96,770	\$104,520
Computer user support specialists	\$60,710	\$59,250	\$57,400	\$61,990
Computer and information systems managers	\$173,810	\$172,160	\$163,490	\$176,990

Evidence labels

Label	Meaning in this study
Confirmed fact	Stated by the affected organization in its own notice or filing, including Form 990, or by a government authority, a court record, or a vendor with direct incident visibility.
Corroborated observation	Reported by a named news organization or researcher and consistent with other evidence, but not confirmed by the affected organization. The text names the reporter.
Attacker claim	A ransomware or extortion group's leak-site listing or statement. It is written as a claim and does not establish scope, data volume, or attribution.
Statistic	A count from a named survey, dataset, or report, with its year. Counts this study computed from the IRS, Texas Attorney General, and HHS OCR data are identified as this study's own.
Guidance	A recommendation from a named issuing body, such as CISA, NIST, the FBI, the FTC, Texas DIR, or Microsoft.
Law or regulation	Statute, rule, or contract text, summarized as general information (see the legal section).
Open theory	A plausible explanation that the public record cannot select or reject.
Founder's Perspective	Donte Wong's professional position or recommendation, intentionally distinguished from a finding about a named organization. Each is a draft pending his approval.

A lead that could not be verified is written as “not found in a bounded public-source search.” That means the search did not find it, not that it did not happen. When an organization disclosed a loss in its own Form 990, the study credits the disclosure as transparency.

Texas organizations that fit the civil society profile

NTEE group	Texas 501(c)(3) records
Q, International, Foreign Affairs and National Security	1,569
R, Civil Rights, Social Action and Advocacy	664
P84, Ethnic and Immigrant Centers	169
Total	2,402

International relief (Q33) is the largest single code at 835 records; refugee issues (Q71) has 25. Read 2,402 as an approximation, not a floor. The code mapping is this study's, not CISA's. It includes relief groups that may do no human rights work, and it leaves out faith, cultural, and academic groups and the 25,766 Texas 501(c)(3) records with no NTEE code. The IRS assigns state by filing address, which represents headquarters.

Timeline: Texas incidents and turning points, 2018-2026

Period	Event	Defensive lesson
2019	Mailed checks stolen from Covenant United Methodist Church in Austin and nine members, more than \$10,000	Paper checks and open mailboxes are part of the attack surface.
July 2018 to June 2020	A federal indictment alleges taskings against a Texas-based human rights and religious freedom organization: its email accounts (July 2018), its website (December 2019), and the organization again (June 2020); unsealed March 2025	Advocacy groups are espionage targets.
April 2020	An Episcopal diocese in North Texas warned of emails impersonating its bishop and clergy	Leader impersonation is verified through a known channel.
July to October 2020	Blackbaud ransomware reaches Texas donors, patients, and universities	What the nonprofit stored on the platform set the size of its notice.
April to October 2022	CHRISTUS Spohn, OakBend, and CHI St. Luke's incidents take Texas nonprofit hospitals offline or expose patient data	Attackers stayed for days to weeks; segmentation and transfer alerts turn that time into a detection window.
May 2022	Attorney General warns of charity scams three days after the Uvalde shooting	Impersonation follows Texas tragedies; publish giving channels before one.
August 2022 to March 2023	Our Lady of the Lake University intrusion and notice, about seven months apart, with an AvosLocker claim in between	Leak-site claims can precede notices; a current data map shortens file review.
Late 2022	A Texas private school discovers a loss in the \$500,000 to \$1 million band to vendor impersonation, disclosed in its own IRS return	Bank changes need a callback on a number already on file.

Period	Event	Defensive lesson
March to October 2023	SEC order, multistate settlement, and Texas Assurance of Voluntary Compliance against Blackbaud	Vendor contracts should set notice roles, retention, and deletion.
May to June 2023	MOVEit exploitation reaches Texas universities through the National Student Clearinghouse	A vendor's vendors also hold the organization's data.
September 1, 2023	SB 768 cuts the Attorney General notice deadline to 30 days	Incident plans must carry current Texas deadlines.
2023 to 2024	Four more Texas nonprofits, a faith-based social services nonprofit, a youth organization, a church-affiliated ministry, and a nonprofit service provider, disclose payment losses between \$250,000 and \$1 million in their IRS returns	Payment procedures need controls that survive one mistake.
February 2024	Change Healthcare breach affects 11,331,028 Texans; Legacy Community Health extends a bank line of credit	Vendor concentration is a cash-flow risk.
May 2024	Ascension ransomware; some Texas ERs set up a diversion process; records back June 4	One laptop led to privileged accounts; identity controls limit what one mistake reaches.
October 1, 2024	2 CFR 200.303(e) adds cybersecurity to federal award safeguards	Security duties arrive with federal money.
November 10, 2024	Goodwill North Central Texas closes all stores; Rhysida later claims the attack	Plan to run revenue and client services offline.
May to July 2025	Microsoft announces, then begins cancelling at renewals from July 1, the donated Business Premium grant	The free tier lacks Conditional Access and endpoint detection; decide the licensing line deliberately.
July 2025	Hill Country floods; Center Point impersonation investigation; fake fundraiser in a flood victim's family's name	An organization's name and giving channels need an owner before a disaster.
September 1, 2025	Chapter 542 safe harbor and the Texas Cyber Command take effect	A framework-sized program is the Texas sizing device, though nonprofit coverage is unsettled.
December 2025	A vendor incident at Aesto Health matches the window of Lone Star Community Health Center's entry, 250,130 Texans	One vendor entry can dominate a sector's breach count.
January to September 2026	Texas leads all states in large health breach reports: 53, affecting 6,099,627 people	Texas health data is breached at scale; 6 of the 53 reports came from Texas 501(c)(3)s (this study's match).

Period	Event	Defensive lesson
January to July 2026	FY 2026 Nonprofit Security Grant Program allocates \$17,533,563 to Texas streams (this study's sum). Texas applications closed March 12, and FEMA's state-agency deadline, extended once, closed July 31	Security grants exist for nonprofits at high risk of attack; FY 2027 is next.
July 2026	Texas floods and a new Attorney General scam alert ; Microsoft reports Midnight Blizzard captive-portal lures , some redirecting to device code sign-in	The patterns repeat; close the device code path.
September 2026	Texas Annual Conference of the United Methodist Church warns of calls spoofing churches' own banks	Caller ID is a claim; call the number on the card.

Appendix E: legal and board reference

Obligations at a glance

Obligation	Who it reaches	Deadline or duty	Source
Individual breach notice	Any person doing business in Texas that owns or licenses computerized sensitive personal information	Without unreasonable delay, no later than 60 days after determining a breach	Bus. and Com. Code 521.053(b)
Attorney General notice	Same, when 250 or more Texans are involved	30 days, by online form; public listing for up to one year	Bus. and Com. Code 521.053(i), (j)
Notice penalties	Same	\$2,000 to \$50,000 per violation; up to \$100 per individual per day of late notice; capped at \$250,000 per breach	Bus. and Com. Code 521.151
TDPSA	Does not apply to nonprofits as defined in 541.001(18)	None directly; may arrive by contract	Bus. and Com. Code 541.002(b)
Chapter 542 safe harbor	Business entities under 250 employees; nonprofit coverage unsettled	Voluntary: exemplary damages are barred if the entity demonstrates that a framework-conformant program was implemented and maintained at the time of the breach	Bus. and Com. Code 542.002 to 542.004
Texas medical privacy	Anyone handling PHI, including on a nonprofit basis, subject to exemptions	Staff training within 90 days of hire, records kept six years; penalties up to \$1.5 million a year	Health and Safety Code 181.001, 181.101, 181.201

Obligation	Who it reaches	Deadline or duty	Source
Federal award safeguards	Nonprofit and college recipients and subrecipients of federal awards	Reasonable cybersecurity measures for PII and sensitive information; HHS awards from Oct. 1, 2025	2 CFR 200.303(e)
State grant safeguards	Local government grantees; a nonprofit usually only when its grant agreement or a rule adopts TxGMS, or a statute such as Gov't Code 2105.008 extends it	Same duty as 200.303(e)	TxGMS v2.1
Texas HHS Data Use Agreement	Texas HHS contractors handling confidential information	Breach notice in 1 hour (federal system-of-records data) or 24 hours (other); written report by 5 p.m. on the third business day	DUA v8.5
Vendor security controls	Vendors holding state agency data	Risk-proportionate controls; periodic evidence	Gov't Code 2054.138
Contractor training	State agency contractors with access to state systems	Certified training; agency reports completion to the Cyber Command by Aug. 31	Gov't Code 2063.104
GLBA Safeguards Rule	Title IV colleges, through the Program Participation Agreement	Written program with MFA and encryption; FSA breach report within 24 hours	FSA, FSA on service providers, 16 CFR 314.4
CIRCI (proposed)	Would reach hospitals with 100 or more beds, critical access hospitals, Title IV colleges	None until a final rule; proposed 72 hours for incidents, 24 hours for ransom payments	CISA
HIPAA Security Rule update (proposed)	HIPAA covered entities and business associates	None until final; final action projected July 2027	Unified Agenda

NIST CSF 2.0 governance outcomes

Outcome (CSF 2.0)	What it calls for	Board use
GV.OC-03	Legal, regulatory, and contractual cybersecurity requirements, including privacy obligations, are understood and managed	Confirm management tracks breach notice, grant, and contract duties
GV.RM-02	Risk appetite and risk tolerance statements are established, communicated, and maintained	Approve the appetite statement
GV.RR (category)	Roles, responsibilities, and authorities are established and communicated to foster accountability	Know who owns the program

Outcome (CSF 2.0)	What it calls for	Board use
GV.RR-01	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a risk-aware culture	Set expectations for the chief executive
GV.RR-03	Adequate resources are allocated commensurate with the risk strategy, roles, and policies	Test the budget against the plan
GV.OV (category)	Results and performance of risk management are used to inform, improve, and adjust the strategy	Receive regular results and act on them

Texas director duties and protection

Provision	What the text says	Effect on directors
Bus. Orgs. Code (BOC) 22.221(a)	A nonprofit director acts in good faith, with ordinary care, and in a manner the director reasonably believes is in the corporation's best interest	Sets the standard
BOC 22.221(b)	A director who met the standard is not liable; the claimant must prove the director did not	Places the burden on the claimant
BOC 3.102(a)	A governing person may rely in good faith and with ordinary care on reports from officers, employees, counsel, a CPA, a person reasonably believed to have professional expertise, or a committee	Supports reliance on management and outside experts
BOC 3.102(b)	Reliance is not in good faith if the person knows of a matter that makes it unwarranted	Known red flags remove the protection
BOC 22.223	A director does not have the duties of a trustee, including for donor-restricted property	Keeps the corporate standard
BOC 7.001	The certificate of formation may eliminate or limit a managerial official's monetary liability, except for loyalty breaches, bad faith, improper benefit, and statutory liability	Protects only if the certificate says so
BOC 8.151	The organization may buy insurance or another arrangement to indemnify current and former governing persons, officers, employees, and agents	Legal basis for D&O coverage
Civ. Prac. and Rem. Code (CPRC) 84.003(2), 84.004(a)	A volunteer serving without compensation beyond expenses, including a director, officer, or trustee, is immune from civil liability for acts or omissions resulting in death, damage, or injury	Limits third-party claims against unpaid directors; paid directors are not volunteers

Provision	What the text says	Effect on directors
CPRC 84.007(a)	No protection for intentional, wilfully negligent, or consciously indifferent or reckless conduct	Carve-out
CPRC 84.007(b)	Chapter 84 does not limit directors' or officers' duties or liabilities to the organization or its members	Duties to the organization remain

[S.B. 2411](#) (effective September 1, 2025) changed “governing person” to “managerial official” in [BOC 7.001](#), so limits can now reach officers. A certificate drafted earlier that names only directors or governing persons does not protect officers until it is amended. Whether chapter 84 volunteer immunity reaches purely economic cyber loss is unresolved; a [2017 Houston Fourteenth Court of Appeals decision](#) applied it to unpaid directors in a property damage dispute. Form 990 lines 11a and 11b ask whether every governing body member [received the complete return](#) before filing.

Source library

Each source is listed once, under the part of the study that first cites it.

Opening and the short version

- [American Banker: Exclusive: Texas fire department battles Venmo flood scams](#)
- [Austin American-Statesman: Health records system restored after Ascension hospitals cyber attack in the Austin area](#)
- [Microsoft: Microsoft 365 Pricing for Business: Plans for Nonprofits](#)

Part 1: The money

- [E-filed IRS Form 990 and 990-EZ returns of seven Texas 501\(c\)\(3\) organizations, tax years 2021 through 2024: Schedule O disclosures under Part VI line 5, one Part IX line 24c expense entry, and one 990-EZ Schedule O entry. The filings are not linked here, because the organizations disclosed on their own and this edition does not name them.](#)
- [Internal Revenue Service: 2025 Instructions for Form 990](#)
- [ProPublica Nonprofit Explorer \(IRS e-file\): Project 4031 Inc, Form 990, tax year 2019](#)
- [U.S. Court of Appeals for the Fifth Circuit: published opinion, No. 21-40220](#)
- [U.S. Attorney’s Office, Eastern District of California: Nashville Man Pleads Guilty to Conspiracy to Defraud Fresno County](#)
- [U.S. Attorney’s Office, Eastern District of Kentucky: Texas woman sentenced to 80 months for money laundering and identity theft, January 4, 2024](#)
- [Eden Prairie Local News: Two women charged in \\$1 million grant fraud](#)
- [Texas Annual Conference of the United Methodist Church: Pause. Verify. Protect: Safeguarding Your Church from Financial Fraud](#)

- [An Episcopal diocese in North Texas: Scam alert! Phishing/whaling scammers trying again. Here's how to fight back](#)
- [Greater Houston Community Foundation: How to Avoid Impersonation Fraud: Donor Security Tips](#)
- [Houston Landing: Houston Library foundation cut checks to vendors, city employees that couldn't be cashed](#)
- [KSAT: San Antonio man fraudulently cashes \\$95K check meant as donation for church, police say](#)
- [FBI Cleveland: St. Ambrose Catholic Parish Was a Victim of a Business Email Compromise Scheme](#)
- [BleepingComputer: \\$1.75 Million Stolen by Crooks in Church BEC Attack](#)
- [San Francisco Chronicle: A nonprofit that helps the poor lost \\$650,000 to scammers. The boss had to go after them herself](#)
- [The Boston Globe: Hackers fooled Save the Children into sending \\$1 million to a phony account](#)
- [Community IT Innovators: Nonprofit Cybersecurity Incident Report, 7th Edition: 2025](#)
- [FBI: Business Email Compromise](#)
- [Federal Trade Commission: Cybersecurity for Small Business](#)
- [FBI IC3 and USPIS: Mail Theft-Related Check Fraud is on the Rise](#)
- [FBI Internet Crime Complaint Center: 2025 IC3 Annual Report](#)
- [FBI IC3: criminals impersonating IC3, public service announcement, 2025](#)
- [Nonprofits Insurance Alliance: scams targeting nonprofits](#)

Part 2: The records

- [Senator Ron Wyden: letter to the FTC on Kerberoasting and the Ascension ransomware attack, September 2025](#)
- [Michigan Public \(NPR station\): Ascension: employee mistake allowed ransomware attackers access](#)
- [Austin American-Statesman: Cyberattack still affecting Ascension Seton hospitals in Austin](#)
- [KWTX: Ascension hospitals experiencing delays after ransomware attack](#)
- [CNN: Ascension cyberattack and ambulance diversions, May 10, 2024](#)
- [SecurityWeek: 5.6 Million Impacted by Ransomware Attack on Healthcare Giant Ascension](#)
- [Houston Chronicle: St. Luke's Health record system is still offline 2 weeks after ransomware attack at parent company](#)
- [The Dallas Morning News: Dallas-based Christus Health experienced unauthorized activity on its computer network](#)
- [The HIPAA Journal: AvosLocker Claims Credit for Christus Health Ransomware Attack](#)
- [U.S. District Court, Northern District of Texas: class action complaint against CHRISTUS Health](#)

- [The Record from Recorded Future News: Texas hospital still bringing systems back online after Sept 1 ransomware attack](#)
- [TechTarget \(HealthITSecurity\): OakBend Medical Center Confirms Data Theft Following Ransomware Attack](#)
- [HIPAA Journal: ransomware attacks including Hendrick Health](#)
- [HHS Office for Civil Rights: breach portal, archive view](#)
- [The HIPAA Journal: CommonSpirit Health Issues Update Confirming 164 Facilities Affected by Ransomware Attack](#)
- [Office of the Texas Attorney General: Data Security Breach Reports](#)
- [Roll Call: Hack poses financial problems for community health centers](#)
- [CHRISTUS Health: Notice to Our Patients About a Cybersecurity Incident](#)
- [Comparitech: Ransomware gang says it hacked Goodwill, shut down stores in Texas](#)
- [ProPublica Nonprofit Explorer: USTA Texas Section](#)
- [Government Technology \(Tribune News Service / San Antonio Express-News\): Our Lady of the Lake University Notifies Data Breach Victims](#)
- [Breachsense: Our Lady of the Lake University breach tracker entry](#)
- [Office of the Vermont Attorney General \(consumer notice filed by the organization\): Evelyn Rubenstein Jewish Community Center of Houston Data Breach Notice to Consumers](#)
- [The Texas Access to Justice Foundation: The Texas Access to Justice Foundation, Notice of Data Event](#)
- [Texas Legislature: Business and Commerce Code Chapter 521](#)
- [Government Technology \(Tribune News Service\): Our Lady of the Lake University to Pay Millions Over Data Breach Lawsuit](#)
- [Government Technology \(Tribune News Service\): University of St. Thomas to Compensate Data Breach Victims](#)
- [University of St. Thomas data settlement website](#)
- [Texas Wesleyan University: cybersecurity updates, November 2023 \(archived\)](#)
- [Office of the Texas Attorney General: Attorney General Ken Paxton Obtains Settlement with Blackbaud Requiring Overhaul of its Data Security Privacy Practices](#)
- [Federal Trade Commission: In the Matter of Blackbaud, Inc., final consent package \(complaint and order\)](#)
- [U.S. Securities and Exchange Commission: Order Instituting Cease-and-Desist Proceedings, In the Matter of Blackbaud, Inc., Securities Act Release No. 11165](#)
- [Blackbaud: Blackbaud Reaches Agreement with the Federal Trade Commission Related to 2020 Security Incident](#)
- [Blackbaud: Blackbaud Resolves Multi-State Attorneys General Investigation of 2020 Security Incident](#)
- [Travis County District Court: Order approving the Texas Assurance of Voluntary Compliance with Blackbaud, Inc.](#)

- Federal Trade Commission: FTC Finalizes Order with Blackbaud Related to Allegations the Firm's Security Failures Led to Data Breach
- The Dallas Morning News, August 3, 2020: Texas institutions among hundreds hit in the Blackbaud ransomware attack
- The University of Texas at Austin (Giving to UT Austin): Blackbaud Data Security Incident
- The Dallas Morning News: Hackers may have accessed Social Security, bank info from Texas institutions, the data storage provider Blackbaud says
- KPRC 2 (Click2Houston): Texas Children Hospital notifies patients of data security incident
- British Deaf Association: Beacon CRM cyber-security incident
- Wordfence: \$4,998 Bounty Awarded and 100,000 WordPress Sites Protected Against Unauthenticated Remote Code Execution Vulnerability Patched in GiveWP WordPress Plugin
- The Register: Nearly a million non-profit donors' details left exposed in unsecured database
- CISA: #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability (AA23-158A)
- The Record from Recorded Future News: MOVEit fallout continues as National Student Clearinghouse says nearly 900 schools affected
- National Student Clearinghouse: list of affected organizations (California AG filing)
- Trinity University: National Data Security Incident
- NIST National Vulnerability Database: CVE-2024-8353 (GiveWP)
- The Baptist Paper: More than 1,000 nonprofits impacted by cybersecurity breach
- Federal Trade Commission: Joint Statement of Chair Lina M. Khan, Commissioner Rebecca Kelly Slaughter, and Commissioner Alvaro M. Bedoya In the Matter of Blackbaud, Inc.

Part 3: The name

- FBI San Antonio Field Office: FBI San Antonio Issues Warning About Disaster-Related Fraud Schemes
- Office of the Texas Attorney General: Attorney General Ken Paxton Announces Investigation into Fraudulent Charity Impersonation Scams After Tragic Flooding
- KPRC Click2Houston: 'Despicable': Florida woman arrested in connection to fake GoFundMe impersonating Hill Country flood victim's family
- KPRC Click2Houston: sentencing report on the fake GoFundMe for a Hill Country flood victim's family, July 17, 2026
- Office of the Texas Attorney General: Attorney General Ken Paxton Takes Action Against Unverified Flood-Related Fundraiser Potentially Scamming Texans
- News 4 San Antonio (WOAI/KABB): AI deepfakes are being used to target people donating to Hill Country flood victims
- Office of the Texas Attorney General: AG Paxton: Beware of Hurricane Harvey Charity Scams
- Federal Bureau of Investigation: Hurricane Harvey: Avoid Fraudulent Charitable Contribution Schemes

- [Office of the Texas Attorney General: CONSUMER ALERT: AG Paxton Advises Texans on Charitable Giving in the Wake of Uvalde Tragedy; Warns Against Potential Fraudsters](#)
- [Office of the Texas Attorney General: CONSUMER ALERT: Attorney General Ken Paxton Provides Guidance to Prevent Fraud and Support Charitable Giving Following Tragic Flooding in Texas](#)
- [Office of the Texas Attorney General: CONSUMER ALERT: Attorney General Ken Paxton Issues Guidance to Protect Texans from Flood-Related Scams and Price Gouging](#)
- [FEMA: major disaster declaration DR-4935](#)
- [FBI El Paso Field Office: FBI El Paso Tech Tuesday: Protecting Yourself From Charity Fraud](#)
- [Office of the Texas Attorney General: Registration and Filings](#)
- [Texas Legislature: Business and Commerce Code Chapter 17](#)
- [Texas Legislature: Penal Code Chapter 33](#)
- [GoFundMe: How You Can Help: Donate to Texas Flood Relief Fundraisers](#)
- [U.S. Department of Justice, USAO Western District of Texas: U.S. Attorney's Office Warns of Fraud Schemes Following Texas Floods](#)
- [U.S. Department of Justice \(court document posted by DOJ\): Sealed Indictment, 24 Cr. 687 \(S.D.N.Y.\)](#)
- [U.S. Department of Justice, Office of Public Affairs: Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns](#)
- [Microsoft: Digital Defense Report 2025](#)
- [CISA: Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society \(resource page\)](#)
- [Internal Revenue Service: Exempt Organizations Business Master File Extract \(EO BMF\)](#)
- [Microsoft Threat Intelligence: CaptiveCrunch: Midnight Blizzard targets travelers worldwide for malware delivery and credential theft](#)
- [Microsoft Learn: block authentication flows with Conditional Access](#)
- [FBI, U.S. Cyber Command CNMF, U.S. Treasury, UK NCSC: Iranian Cyber Actors Targeting Personal Accounts to Support Operations \(Product ID 20240927-001\)](#)
- [Microsoft Learn: Microsoft-managed Conditional Access policies](#)
- [Microsoft Learn: Configure Security Defaults for Microsoft Entra ID](#)
- [teiss: Nelson University suffers ransomware attack that may have exposed sensitive personal data](#)

Part 4: What to do about it

- [FBI IC3: device-code phishing public service announcement, May 21, 2026](#)
- [FBI IC3: OAuth consent phishing public service announcement, September 1, 2026](#)
- [Texas Legislature: Government Code Chapter 311 \(Code Construction Act\)](#)
- [Texas Legislature: Business and Commerce Code Chapter 541 \(Texas Data Privacy and Security Act\)](#)

- [Texas Legislature: Business and Commerce Code Chapter 542](#)
- [eCFR: 2 CFR 200.303, internal controls](#)
- [Texas HHS: Data Use Agreement, version 8.5](#)
- [Texas Legislature: Health and Safety Code Chapter 181](#)
- [Texas Legislature: Government Code Chapter 2063 \(Texas Cyber Command\)](#)
- [NIST: SP 1300, CSF 2.0 Small Business Quick-Start Guide](#)
- [Center for Internet Security: CIS Critical Security Controls Implementation Group 1](#)
- [CISA: Cybersecurity Performance Goals 2.0](#)
- [Texas Department of Information Resources: Customer Eligibility](#)
- [Microsoft Learn: Microsoft for Nonprofits updates](#)
- [Microsoft Learn: Microsoft 365 for business security overview](#)
- [Microsoft Learn: Get Microsoft Defender for Business](#)
- [Microsoft 365 Business Premium commercial plan and price](#)
- [CISA: Implementing Phishing-Resistant MFA \(fact sheet\)](#)
- [Microsoft Learn: manage emergency access accounts](#)
- [CISA ScubaGear v1.8.0: Microsoft Entra ID baseline](#)
- [Microsoft Learn: Microsoft 365 for business security best practices](#)
- [CISA ScubaGear v1.8.0: Exchange Online baseline](#)
- [CISA: Cyber Essentials](#)
- [CISA: Cyber Guidance for Small Businesses](#)
- [PCI Security Standards Council: Does PCI DSS apply to merchants who outsource all payment processing operations and never store, process or transmit cardholder data?](#)
- [Texas Department of Information Resources, Office of the CISO: Cybersecurity Tips for Non-Profits and Small Businesses: Best Practices for Keeping Your Organization Secure](#)
- [Texas Department of Information Resources, Office of the CISO: I've been hacked! What now? Best Practices for Non-Profits and Small Businesses](#)
- [NTEN and Heller Consulting: 2024 Nonprofit Digital Investments Report](#)
- [Center for Internet Security \(CIS\): The Cost of Cyber Defense, Version 1.1: An Executive Guide for Implementation Group 1 \(IG1\) of the CIS Critical Security Controls](#)
- [Google for Nonprofits: Google Workspace: Nonprofit Resource Center](#)
- [Okta: Identity for Non-Profits](#)
- [Cloudflare: Project Galileo](#)
- [CISA: Cyber Hygiene Services](#)
- [FEMA: FY 2025 Nonprofit Security Grant Program Fact Sheet](#)
- [FEMA: FY 2026 Nonprofit Security Grant Program notice of funding opportunity](#)
- [FEMA: FY 2026 NSGP key changes](#)

- [National Association of Insurance Commissioners: Report on the Cybersecurity Insurance Market \(2025\)](#)
- [The Council of Insurance Agents & Brokers: Q2 2026 P&C Market Survey \(press release\)](#)
- [Travelers Casualty and Surety Company of America: Multi-Factor Authentication Supplement](#)
- [U.S. Bureau of Labor Statistics: Occupational Employment and Wages, May 2025](#)
- [U.S. Bureau of Labor Statistics: Occupational Employment and Wage Statistics Query System, Texas, May 2025](#)
- [U.S. Bureau of Labor Statistics: Table 7. Employer Costs for Employee Compensation for private industry workers by census region and division](#)
- [CyberSeek \(NICE, Lightcast, CompTIA\): Cybersecurity Supply/Demand Heat Map](#)
- [ISC2: ISC2 Study Finds Cybersecurity Budget Constraints Remain, But Do Not Worsen, While Skill Needs Grow](#)
- [CISA and international partners: Protecting Against Cyber Threats to Managed Service Providers and their Customers \(AA22-131A\)](#)
- [National Council of Nonprofits: Cybersecurity for Nonprofits](#)
- [Texas Legislature: Government Code Chapter 2054](#)
- [NACD and Internet Security Alliance: Director’s Handbook on Cyber-Risk Oversight, fifth edition \(accessible PDF\)](#)
- [Nonprofit Risk Management Center: The Garden of Risk Oversight: Positioning the Board to Cultivate Strategic Risk-Taking](#)
- [Texas Legislature: Business Organizations Code Chapter 22](#)
- [Texas Legislature: Business Organizations Code Chapter 3](#)
- [Texas Legislature: Business Organizations Code Chapter 7](#)
- [National Institute of Standards and Technology: The NIST Cybersecurity Framework \(CSF\) 2.0, NIST CSWP 29](#)
- [BoardSource: Nonprofit Fiduciary Duty + Responsibilities](#)
- [Texas Legislature: Business Organizations Code Chapter 8](#)
- [Internal Revenue Service: 2025 Form 990](#)

Update triggers and appendices

- [CourtListener: consolidated Ascension data breach class action docket](#)
- [CISA: Cyber Incident Reporting for Critical Infrastructure Act of 2022 \(CIRCIA\)](#)
- [Unified Agenda: HIPAA Security Rule, RIN 0945-AA22](#)
- [FEMA: Nonprofit Security Grant Program](#)
- [Texas Cyber Command: about](#)
- [Microsoft Nonprofits: Microsoft 365 Nonprofit Solutions](#)
- [Texas Cyber Command: Report an Incident](#)
- [Texas Legislature: S.B. No. 2610, 89th Legislature, Regular Session, enrolled version](#)

- CISA: Secure Cloud Business Applications (SCuBA) Project
- National Institute of Standards and Technology: NIST SP 800-63B-4 Digital Identity Guidelines: Authentication and Authenticator Management
- CISA: #StopRansomware Guide
- DHS/FEMA (NOFO copy hosted by California Governor's Office of Emergency Services): Fiscal Year 2026 Nonprofit Security Grant Program NOFO, DHS-26-GPD-008-00-99
- Office of the Texas Attorney General: Charitable Trusts
- Office of the Texas Attorney General: Data Breach Reporting
- Texas Department of Information Resources: Texas Information Sharing and Analysis Organization (TX-ISAO)
- Texas Legislature: Government Code Chapter 2175
- FBI Internet Crime Complaint Center (IC3): Business Email Compromise: The \$55 Billion Scam (PSA I-091124-PSA)
- Internal Revenue Service: EO BMF extract information sheet, including foundation codes (TE/GE copy)
- Internal Revenue Service: Data Book, 2025, Table 1-3
- Texas Senate: Senate Resolution No. 163
- Texas Demographic Center conference materials (OneStar Foundation, North Texas Nonprofit Institute): The State of the Texas Nonprofit Sector: Regional and Statewide Data Trends
- Texas Legislature: Health and Safety Code Chapter 534
- Internal Revenue Service: EO BMF extract information sheet, including NTEE codes (SOI copy)
- Aesto Health: notice of data security incident, December 2025
- Internal Revenue Service: EO BMF Texas extract (eo_tx.csv)
- Identity Theft Resource Center: 2024 Data Breach Report
- Identity Theft Resource Center: 2025 Data Breach Report
- Identity Theft Resource Center: H1 2026 Data Breach Report
- FBI IC3: 2025 Texas state report
- Community IT Innovators: 2026 Nonprofit Cybersecurity Incident Report
- Community IT Innovators: nonprofit cybersecurity incident report page
- Verizon: 2025 Data Breach Investigations Report: Small- and Medium-Sized Business Snapshot
- HHS OCR: 2024 report to Congress on breaches of unsecured PHI
- U.S. Bureau of Labor Statistics: OEWS Query System, Dallas-Fort Worth-Arlington, TX, May 2025
- U.S. Bureau of Labor Statistics: OEWS Query System, Houston-Pasadena-The Woodlands, TX, May 2025
- U.S. Bureau of Labor Statistics: OEWS Query System, San Antonio-New Braunfels, TX, May 2025

- U.S. Bureau of Labor Statistics: OEWS Query System, Austin-Round Rock-San Marcos, TX, May 2025
- KXAN: Austin Church and its congregation lose thousands in mail theft
- Texas Legislature: S.B. No. 768, Enrolled
- Texas Comptroller: Texas Grant Management Standards (TxGMS), version 2.1
- Federal Student Aid: updates to Gramm-Leach-Bliley Act cybersecurity requirements, February 9, 2023
- Federal Student Aid: service provider relationships and GLBA compliance, April 24, 2024
- eCFR: 16 CFR 314.4, Safeguards Rule elements
- Texas Legislature: Civil Practice and Remedies Code Chapter 84
- Texas Legislature: S.B. 2411, 89th Legislature, enrolled
- Texas Fourteenth Court of Appeals: No. 14-14-00981-CV (2017)

Document control

Edition: Full report, September 23, 2026. **Evidence cutoff:** September 23, 2026.

Basis: Public statements by affected organizations, government authorities, and responders with direct incident visibility, cited inline. This is a public analysis, not a forensic report, and it confers no certification. Recommendations are defensive design judgments, not findings that a named organization lacked a listed control.

Prepared by: Mount Xion Technologies, San Antonio, Texas. mountxiontechnologies.com