K-12

Utah HB 44: A Cybersecurity Readiness Guide for School Districts

Current as of June 2026 · 9 min read

Utah's HB 44, the School Security Personnel Standards bill, did more than address physical safety. Folded into it is a new set of cybersecurity requirements for school systems (the provisions many districts first knew as HB 42). The law directs the state's Cybersecurity Commission to establish minimum cybersecurity standards for local education agencies and to phase them in over time, while expanding the Utah Cyber Center's and UETN's role in supporting districts directly.

For most district IT teams, the open question isn't *whether* to act. It's how to build real readiness while the specific standards are still being written. This guide walks through what HB 44 requires, what's still being decided, and the steps you can take now.

CONTENTS

What HB 44 requires (and where it lives)

HB 44 (2026 General Session, Chief Sponsor Rep. Ryan Wilcox; Senate Sponsor Sen. Ann Millner) is mostly a physical-security bill: armed school guardians, panic-alert devices, visitor management. The cybersecurity requirements are one part of it, and knowing exactly where they live matters when you are reading the law or briefing leadership.

The cybersecurity provisions are enacted at **Utah Code Title 53G, Chapter 8, Part 9 (LEA Cybersecurity Standards)**, Sections 53G-8-901 through 53G-8-903, with the standards-setting duty at **Section 63C-27-202(9)**. The bill was signed by Governor Cox and took effect **May 6, 2026**. In brief, Part 9 and the related Commission duty do four things:

- **Minimum standards, set by rule.** Each LEA must comply with minimum cybersecurity standards established by the state Cybersecurity Commission through administrative rulemaking (Section 53G-8-902), on a phased implementation timeline also established in rule.
- **Framework-aligned rules.** Section 63C-27-202(9) directs the Commission to align the standards with industry-recognized frameworks, specifically naming the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS), and to account for varying LEA resources, capacity, and needs.
- **State support for districts.** UETN, in consultation with the Utah Cyber Center and the state board, must develop implementation guidelines and technical resources, provide technical assistance, and coordinate cybersecurity services for LEAs. The three entities are also required to coordinate with each other so districts get consistent guidance without duplicated effort.
- **Breach reporting and a named contact.** Section 53G-8-903 adds data-breach reporting duties and requires each LEA to designate a primary cybersecurity point of contact (covered in detail below).

QUICK REFERENCE: WHERE THE CYBERSECURITY PROVISIONS LIVE

Citation	What it covers
Utah Code § 53G-8-901	Definitions for Part 9: the Utah Cyber Center, data breach, UETN
§ 53G-8-902	LEA compliance with the minimum standards on the phased timeline; UETN, Cyber Center, and state board support and coordination duties
§ 53G-8-903	Data-breach reporting, response cooperation, and the designated cybersecurity point of contact
§ 63C-27-202(9)	The Cybersecurity Commission's duty to set the standards by rule, aligned to NIST and CIS, with a phased implementation timeline
Effective date	May 6, 2026. The only date attached to the cybersecurity provisions

You can read the law yourself; the cybersecurity sections are short. The **enrolled HB 44 (PDF)** is hosted here for convenience, and the **Utah Legislature's HB 44 page** is the primary source.

Wait, is this HB 42 or HB 44?

Both, in a sense, and the confusion is understandable. The school cybersecurity requirements were drafted earlier in the 2026 session as **HB 42 (School Cybersecurity Amendments)**. During the session, those provisions were consolidated into **HB 44 (School Security Personnel Standards)** through a Senate substitute, and HB 44 is the bill that passed and was signed into law.

So if a vendor, a conference session, or a colleague refers to "HB 42 requirements," they almost certainly mean the same provisions; the current, correct citation is just HB 44, Utah Code 53G-8-901 through 903. HB 42 did not fail. Its cybersecurity provisions live on inside HB 44.

What it does NOT do (yet)

Just as important as what the law requires is what it leaves open. HB 44 does **not** contain a list of specific technical controls, and it does **not** set a single compliance deadline. Both are delegated to the Cybersecurity Commission, which writes the actual standards through administrative rulemaking, including a phased implementation timeline based on LEA size, existing cybersecurity infrastructure, and available resources.

> **No, there is no single "comply-by" date**
>
> The only date attached to the cybersecurity requirements is the law's effective date: May 6, 2026. HB 44 contains other dates, but they belong to its physical-security provisions, and none of them is a cybersecurity compliance deadline. The cyber timeline arrives with the Commission's rules, phased by district circumstances.

WHERE THINGS STAND

1. **In effect now: the law itself**

   Part 9 is law as of May 6, 2026, including the breach-reporting duties and the designated-contact requirement.

2. **In progress: Commission rulemaking**

   The Cybersecurity Commission is writing the minimum standards, aligned to NIST and CIS frameworks. Watch adminrules.utah.gov.

3. **Coming: phased compliance**

   Compliance dates arrive with the rules, phased by LEA size, existing cybersecurity infrastructure, and available resources.

That is not a reason to wait. The statute already tells you the shape of what's coming: the framework alignment and the topic areas the rules must address are written into the law. Districts that map their current posture against those areas now will be in a far better position when the phased timeline lands, and most of the work involved is worth doing regardless of any rule.

What "good" looks like

Section 63C-27-202(9)(d) lists the areas the minimum standards must address, as appropriate to each LEA's size, risk profile, and resources. This list is the closest thing to a published syllabus for the coming rules:

- Identity and access management
- Asset management and inventory of hardware, software, and data systems
- Data protection
- Security monitoring and logging capabilities
- Vulnerability management, including regular security assessments and patching procedures
- Incident response and recovery planning
- **Security awareness training requirements for staff and administrators**
- Third-party risk management for vendors with access to LEA systems or data
- Network security controls
- Backup and disaster recovery procedures
- Governance structures for cybersecurity oversight within an LEA

Two things stand out. First, this is a mainstream control set: if you have worked with the CIS Controls or the NIST Cybersecurity Framework, nothing here will surprise you, which is the point of the framework-alignment requirement. Second, the human layer is named in the law itself. Security awareness training for staff and administrators is an explicit statutory topic, not an optional extra. A district that treats training as a once-a-year video will likely find that posture hard to defend once standards are in rule.

The free baseline, and what sits above it

HB 44 deliberately expands what Utah provides to districts for free. UETN and the **Utah Cyber Center** are tasked with implementation guidelines, technical assistance, coordinated services, and information sharing, and the law requires them to coordinate with the state board specifically to avoid duplication and give LEAs consistent guidance. If you have not talked to UETN or the Cyber Center recently, that conversation is step one, before any purchasing decision. Use everything the state gives you.

The baseline is real, but it is shared infrastructure serving every LEA in the state. Where districts typically find they need a layer above it is in the depth and per-person granularity of the human-risk work the statute calls for:

THE BASELINE AND THE LAYER ABOVE, SIDE BY SIDE

	The free state baseline	The layer above
What it is	Shared statewide services available to every LEA	Per-person depth for your district's human-risk work
Who provides it	UETN and the Utah Cyber Center	Programs your district selects, with advisory help
What it includes	Implementation guidelines, technical assistance, coordinated services, threat information sharing	Per-user cyber risk scoring, adaptive phishing simulations, automated remedial training, Google Workspace and Microsoft Entra ID directory sync
First move	Use all of it. Talk to UETN and the Cyber Center before buying anything	Identify what you still cannot see or evidence after the baseline, then decide

None of that replaces the state-provided baseline. It sits on top of it, in the layer where the statute asks for "security awareness training requirements for staff and administrators" and where most districts have the least visibility today. The honest sequencing: take the free baseline first, identify what your district still cannot see or evidence, then decide what belongs above it.

A practical readiness checklist

Here is a working checklist you can use to take stock before the Commission's rules land. It is organized around the statute's own topic areas, so work you do now maps directly to whatever the final standards require. Check items off as you go, or use the Download PDF button at the top of this page to get a copy you can print or share with leadership.

Governance and coordination

- [ ] Designate a primary cybersecurity point of contact (or confirm a regional education service agency arrangement) to interface with the Utah Cyber Center, the state board, and UETN
- [ ] Assign an owner for tracking the Cybersecurity Commission rulemaking as standards and the phased timeline are published
- [ ] Brief your superintendent and board on what HB 44 requires and what is still being set by rule
- [ ] Document a governance structure for cybersecurity oversight, even a simple one

Free baseline services

- [ ] Contact UETN and the Utah Cyber Center to inventory the services and resources currently available to your LEA
- [ ] Join the cybersecurity information-sharing initiatives coordinated by the Utah Cyber Center
- [ ] Record which state-provided services you already use, so gaps above the baseline are visible

Know your environment

- [ ] Build or refresh your asset inventory: hardware, software, and data systems
- [ ] Map where sensitive data lives: student records, staff data, finance systems
- [ ] List every vendor with access to your systems or data, and what they can reach

Core controls

- [ ] Measure MFA coverage across staff, administrators, and privileged accounts
- [ ] Review identity lifecycle: how accounts are created, changed, and removed when people leave
- [ ] Confirm a patching cadence and a way to find unpatched systems
- [ ] Check what security monitoring and logging you actually have, and who reviews it
- [ ] Review basic network segmentation between student, staff, and administrative systems

Resilience and response

- [ ] Verify backups exist for critical systems, including a copy an attacker on your network cannot delete
- [ ] Test a restore. A backup you have never restored from is a hope, not a control
- [ ] Write or update an incident response plan that includes the HB 44 reporting workflow: report to the Utah Cyber Center and notify the state board within 24 hours of discovering a data breach
- [ ] Run a tabletop exercise that walks through breach reporting and UETN coordination

The human layer

- [ ] Stand up security awareness training for staff and administrators; the statute names this area explicitly
- [ ] Measure phishing resilience, not just training completion
- [ ] Close the loop: route people who struggle into follow-up training instead of an annual reset

Data-breach reporting in brief

Section 53G-8-903 is the part of HB 44 most likely to matter on a bad day, so it is worth knowing cold. Here is the workflow the statute describes:

THE HB 44 BREACH-REPORTING WORKFLOW

1. **A data breach is discovered**

   Discovery starts the clock, so note the timestamp.

2. **Report the breach to the Utah Cyber Center**

   In accordance with Section 63A-19-405 and the procedures established in Commission rule.

3. **Notify the state board within 24 hours**

   The 24-hour window runs from discovery of the breach.

4. IF UETN-PROVIDED NETWORK INFRASTRUCTURE OR SERVICES ARE INVOLVED

   Coordinate with UETN

   Loop UETN in alongside the Cyber Center.

5. **Cooperate with the Cyber Center's investigation and response**

   In return, the Cyber Center provides response assistance to LEAs the same way it does for other governmental entities.

Separately, every LEA must **designate a primary point of contact for cybersecurity matters** who interfaces with the Cyber Center, the state board, and UETN. Smaller districts and charters should note that a regional education service agency may serve as the designated contact for multiple LEAs in its service area. If it does, the agency takes on coordination and documentation duties on behalf of the participating LEAs.

The practical takeaway: a 24-hour notification clock is short. The time to wire breach reporting into your incident response plan (who calls whom, with what information, verified against current contacts) is before an incident, ideally rehearsed in a tabletop exercise.

Where Harborcoat fits

Harborcoat is a Utah-based team of strategic security and IT advisors. We help districts take stock of where they stand against the areas HB 44 names, make sense of what the free state baseline covers, and decide, honestly, what, if anything, belongs above it. Where implementation work is needed, we coordinate it through vetted partner firms rather than performing deployments in-house, which keeps our advice independent of any one tool.

If procurement becomes part of the conversation, we help districts navigate cooperative purchasing and public-sector procurement vehicles. But most first conversations are simpler than that: a walk through the checklist above, what the Commission's rulemaking is likely to mean for a district your size, and what to do in which order. No pitch required.

Sources & further reading

HB 44, enrolled copy (PDF) (/documents/utah-hb44-enrolled-2026.pdf) · Hosted here for convenience; the cybersecurity provisions are Sections 18 through 22.

HB 44: School Security Personnel Standards (2026 General Session) (https://le.utah.gov/~2026/bills/static/HB0044.html) · Utah Legislature; primary source.

Utah Cyber Center (https://cybercenter.utah.gov/) · State services, breach reporting, and resources for public-sector entities.

UETN (Utah Education and Telehealth Network) (https://uetn.org/) · Network services and LEA technical support.

Utah Administrative Rules (https://adminrules.utah.gov/) · Where the Cybersecurity Commission's standards and phased timeline will be published. Still in progress as of June 2026; check here for the current status.

Talk through your district's readiness

A short conversation with a Harborcoat advisor can save weeks of guessing: where your district stands against the statute's areas, what the free baseline covers, and what to sequence first.

Harborcoat Technologies · (385) 999-2358 · info@harborcoattech.com · harborcoattech.com

Harborcoat Technologies · Strategic Security and IT Advisors · Current as of June 2026