DIGITAL DEFENSE DIGEST

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

WHAT'S NEW

- The Nonprofit & Government Sector Security Initiative officially opens for enrollment, with free introductory workshops running through October and November.
- Congress is weighing the PILLAR Act, which would reauthorize and extend the federal State and Local Cybersecurity Grant Program (SLCGP) through 2033 after its funding phase was set to wind down in FY2026 – a program many of our government and school-district clients rely on.
- ShinyHunters' string of EdTech and Salesforce-linked breaches (Infinite Campus, Canvas/Instructure, and others) continues to grow, underscoring the risk lean IT teams carry with SaaS platforms that hold student and donor data.

This monthly publication is provided by Black Belt Secure

BLACK BELT SECURE

OUR MISSION:

To empower businesses of all sizes with the knowledge and tools they need to thrive in today's increasingly complex cyber threat landscape. We are dedicated to providing cutting-edge cybersecurity solutions and expert guidance to help our clients

CYBERSECURITY FOR THE SECTORS THAT CAN'T AFFORD TO FAIL: LAUNCHING OUR NONPROFIT & GOVERNMENT SECURITY INITIATIVE

Back in July, we teased something "coming this fall." It's here. This month, Black Belt Secure formally launches our Nonprofit & Government Sector Security Initiative — a dedicated program of workshops, right-sized assessments, and grant-readiness support built specifically for churches, nonprofits, school districts, and local government offices that operate with lean budgets and leaner IT teams. The timing isn't accidental. Over the past several months, the education and research sectors have absorbed a brutal string of headline breaches. The extortion group ShinyHunters compromised a Salesforce account tied to Infinite Campus, the student information system used by more than 3,200 K-12 districts and roughly 11 million students nationwide, eventually leaking contact records for over 137,000 school staff.

Weeks later, the same group hit Instructure, the company behind the Canvas learning management system, in an attack researchers say may have touched hundreds of millions of student and teacher accounts across thousands of institutions. And this summer, Google's Threat Intelligence Group disclosed a year-long, China-linked espionage campaign against internet-exposed REDCap research servers used by medical schools, universities, and hospital systems — a reminder that even niche academic tools are firmly in nation-state crosshairs. None of the organizations behind these headlines set out to be careless. They simply didn't have the security budget, staff, or vendor oversight of a Fortune 500 company — and neither do most of our nonprofit, education, and local government clients. That gap is exactly what this Initiative exists to close.

continued on page 2...

WHY LEAN-BUDGET ORGANIZATIONS ARE PRIME TARGETS

Attackers aren't picking on nonprofits, schools, and small government offices because the data is more valuable — they're picking on them because the data is easier to reach. These organizations typically share three characteristics that make them attractive: sensitive data at scale (student records, donor and beneficiary information, constituent PII), a patchwork of SaaS vendors that no one person fully owns or monitors, and IT staffing that is stretched across every technology problem the organization has, cybersecurity being just one of them.

The Infinite Campus and Canvas incidents illustrate the pattern precisely: the initial foothold in both cases traced back to a vendor's Salesforce environment, not a failure inside the school or district itself. Your organization can do everything right internally and still be exposed through a platform you don't directly control — which is exactly why vendor risk management and incident response planning have to be part of any right-sized security program, not optional extras.

Sector	2026 Wake-Up Call	Common Weak Point	Grant Lever
K-12 Schools	Infinite Campus / ShinyHunters (137K+ records)	Vendor SaaS access controls; MFA gaps	State ed-tech & E-Rate security funds
Higher Ed	Canvas/Instructure breach; REDCap espionage campaign	Unpatched research servers; shadow IT	NIST 800-171 / federal research grants
Nonprofits / Churches	Rising BEC & donor-data phishing tied to thin oversight	No dedicated IT/security staff; volunteer admin access	Foundation & insurer risk-reduction credits
Local Government	SLCGP funding uncertainty amid reauthorization debate	Legacy systems; no formal incident response plan	SLCGP / PILLAR Act, state homeland security grants

137K+
Records exposed in the Infinite Campus breach

3,200
School districts using the affected student system

2033
Reauthorization target under the proposed PILLAR Act

30%
Reported rise in nonprofit cyberattacks in recent years

FREE WHITEPAPER:

Cyber Resilience on a Public-Sector Budget

Cyber Resilience on a Public-Sector Budget is our new companion guide to this Initiative — covering the threat landscape for under-resourced organizations, grant eligibility requirements, a right-sized NIST 800-171/CMMC roadmap, and how to build an incident response plan without a full-time security hire.

Claim Your FREE Copy Today At: blackbeltsecure.com/reports

INTRODUCING THE NONPROFIT & GOVERNMENT SECTOR SECURITY INITIATIVE

The Initiative is built around three simple commitments, designed to meet lean-budget organizations exactly where they are:

Free introductory workshops — live, plain-language sessions on the threats your organization actually faces and the handful of controls that matter most, run monthly through the fall.

Right-sized Compliance Gap Assessments — a scaled-down version of our standard assessment, priced and scoped for annual budgets measured in the tens, not millions, of thousands.

Grant readiness support — documentation, control mapping, and posture evidence formatted to match what state and federal cybersecurity grant applications actually ask for.

GRANT READINESS SPOTLIGHT: THE SLCGP & THE PILLAR ACT

The federal State and Local Cybersecurity Grant Program (SLCGP) has distributed roughly $1 billion to state, local, and tribal governments since 2022 to fund exactly the kind of planning, assessment, and workforce projects our Initiative supports. The program's active funding phase was on track to wind down in FY2026, but the House has already passed the PILLAR Act, which would extend SLCGP authorization through 2033. The bill now awaits Senate action.

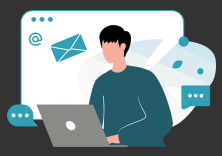
What this means for local government and school-district clients: cybersecurity spending tied to an approved State Cybersecurity Plan remains one of the most reliable ways to fund the exact projects — gap assessments, MFA rollouts, incident response planning — that our Initiative is built to deliver. We're tracking the reauthorization closely and will flag application windows as state administrative agencies open them.

BLACK BELT SECURE
Defend Today, Thrive Tomorrow.

FIVE LOW-COST MOVES EVERY LEAN IT TEAM SHOULD MAKE THIS MONTH

- **Turn on phishing-resistant MFA** for every admin account tied to a SaaS platform holding student, donor, or constituent data — this is the single control most breaches this year would have stopped.
- **Inventory your vendor logins -** list every SaaS platform (Salesforce, your SIS, your LMS, your donor CRM) and confirm who at your organization, not the vendor, owns access review.
- **Patch internet-facing research and data tools** like REDCap on a defined schedule — the recent espionage campaign succeeded largely against outdated, internet-exposed versions.
- **Write down your incident response plan** — even one page naming who calls whom, in what order, is worth more than no plan at all.
- **Talk to a vCISO before you talk to a grant officer** — grant applications score higher when they cite a documented assessment and roadmap rather than good intentions.

Questions? Email info@blackbeltsecure.com or visit blackbeltsecure.com for a free assessment.



CALL TO ACTION & CONTACT SECURE YOUR BUSINESS BEFORE THE NEXT WAVE HITS

Beyond protecting networks, Black Belt Secure is committed to strengthening the organizations that strengthen our communities. This fall's Initiative workshops kick off in October alongside Cybersecurity Awareness Month, with sessions tailored for church and ministry administrators, school-district technology directors, and city/county IT staff across North Texas and beyond. Ask your account team for the workshop calendar, or reach out directly to reserve a seat — space in each session is limited to keep the conversation practical and specific to your organization.

SCHEDULE A FREE ASSESSMENT

Not sure where your organization stands? Our no-obligation Compliance Gap Assessment — now available in a right-sized format for nonprofits, schools, and government offices — delivers a prioritized, plain-language finding report within 5 business days.

blackbeltsecure.com/audit

(469) 557-2007