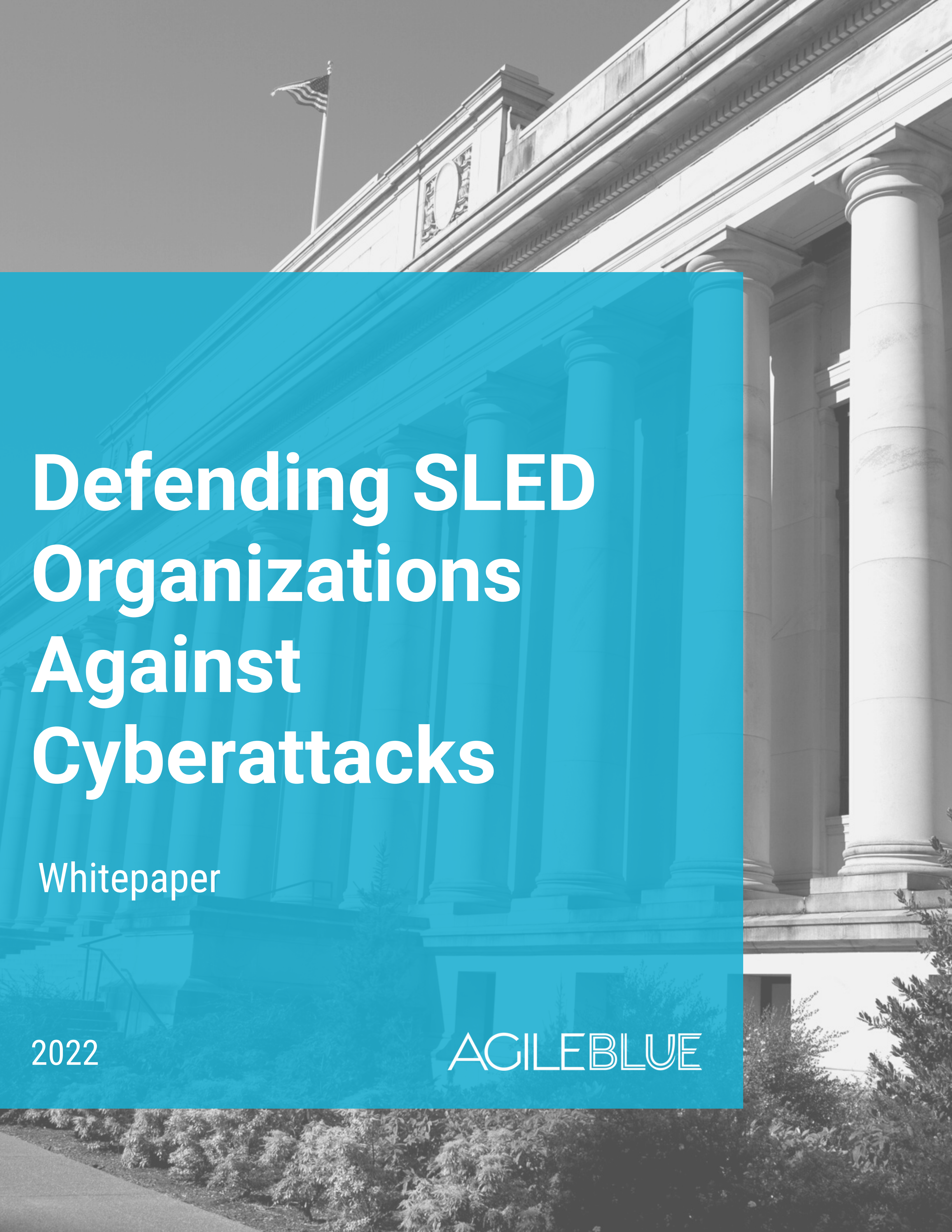


Defending SLED Organizations Against Cyberattacks

Whitepaper

2022

AGILEBLUE

If you're a state, local, or education (SLED) organization, you're likely familiar with the need for a robust, secure, and resilient IT infrastructure due to the industry being at high risk of cyber-attacks. State and local government agencies and educational institutions are high-profile targets with confidential and sensitive data and typically very limited cybersecurity resources.

SLED ORGANIZATIONS: HIGHLY TARGETED CYBER VICTIMS

In most cases, state and local government agencies, as well as educational institutes haven't kept up with the digital transformation over the last several years. While some have moved toward digital systems for business, most local governments in the U.S. operate in an analog fashion such as accepting tax checks in person, asking residents to fill out paperwork in person, and holding plenty of in-person meetings. Since the pandemic, local government and schools scrambled to set up remote work and learning without having the necessary cybersecurity infrastructure in place causing major gaps within their infrastructure.

Cybersecurity budget is one of the main pain points for SLED organizations. Carving out a cybersecurity budget within state and local governments can prove to be difficult with elected officials and budget-conscious residents given that much of the government's funding comes from taxes. The lack of knowledge or understanding of cybersecurity causes cuts within the budget.

In a report from Deloitte, the top obstacles to cybersecurity in state government are due to having insufficient cybersecurity budgets or lack of a dedicated cybersecurity budget all together. Unfortunately, the pace of cyberattacks have been accelerating with 44% of SLED agencies indicating that they experience cyberattacks at least daily according to iland.

SLED CYBERATTACKS OF NOTE

Reports of cyber-attacks against government and educational targets occur weekly in the U.S. In a report from TechTarget, it was stated that there has been at least one instance of a town, county, or state government falling victim to a ransomware attack every month in 2022.

1 Quincy, Illinois Attack

Mayor Mike Troup held a press conference on May 24, 2022, announcing the city was hit with a ransomware attack. While some departments like police and fire had email and phone systems down, no personal information appeared to have been stolen. The city put more than $600,000 to stem the attack.

2 Texas Government Attacks

In 2019, threat actors coordinated attacks that took 23 different small Texas towns offline at the same time. The state of Texas declined to name the towns affected and claim no ransom was paid, however the attacks demonstrate the impact these attacks have on local governments and its citizens.

3 Baltimore Ransomware Attack

In 2019, Baltimore, Maryland, was hit with a ransomware attack that brought the entire city to a screeching halt. The city refused to pay the $80,000 ransom demand. Unfortunately, restoring data and recovering their systems cost the city taxpayers more than $18 million from new hardware, remediation, and lost revenue.

4 MacEwan University Phishing Attack

MacEwan University in Edmonton, Canada was scammed out of $11.8 million due to a staff member falling victim to a phishing attack. The attack came from an email impersonating a vendor that was sent to the victim requesting a change in banking information.

5 Lincoln College Forced to Close

The college located in Lincoln, Illinois, was founded in 1865. Tragically, the school suffered a ransomware attack in late 2021 and was forced to permanently close in 2022. The school was hit by the COVID-19 pandemic, however the ransomware attack blocked access to critical systems and data thus preventing the school from being able to recruit and enroll students and continue their fundraising efforts.

> “Lincoln College has been serving students from across the globe for more than 157 years. The loss of history, careers, and a community of students and alumni is immense."
>
> *- David Gerlach, President*

DEFENDING AGAINST CYBERATTACKS

Employee Training and Awareness

An employee accessing their email on a smartphone while using a public Wi-Fi network, for example, can cause a lot of problems. A breach is considerably less likely to occur if everyone in an organization follows the same security procedures. Making the entire staff aware of the various threats that exist – from data breaches to ransomware – will prevent them from making basic errors that could jeopardize a company's security.

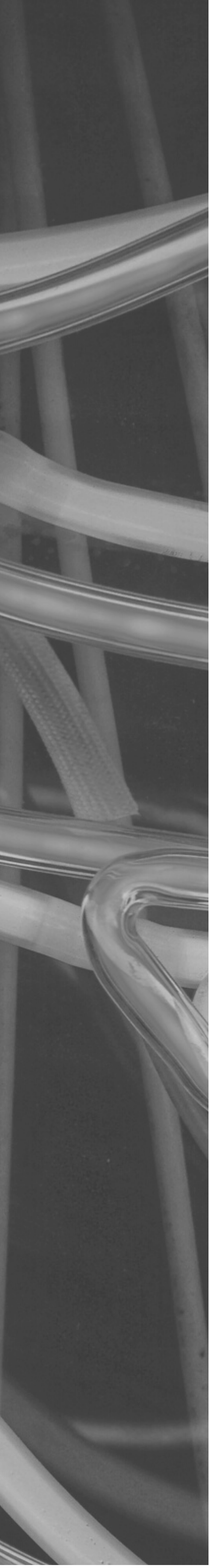
Moving to the Cloud

At this point, most SLED organizations should have a cloud migration strategy in place if they haven't already made the transition. Hosting on-premises is expensive. SLED organizations with smaller IT teams and small budget for hardware backup and on-premises maintenance can greatly benefit by moving to a cloud solution. When moving data to a large cloud provider, it means that data and transactions are safeguarded by industry-leading protocols and software that keep organizations more secure. Moving to the cloud also allows SLED organizations the flexibility of allowing their employees and students to use any combination of locations and technology that suits their workstyle.

A total revamp of outdated systems will help to engage next-generation security solutions that are capable of providing state-of-the-art solutions, including XDR and MDR.

Disaster Recovery Strategy

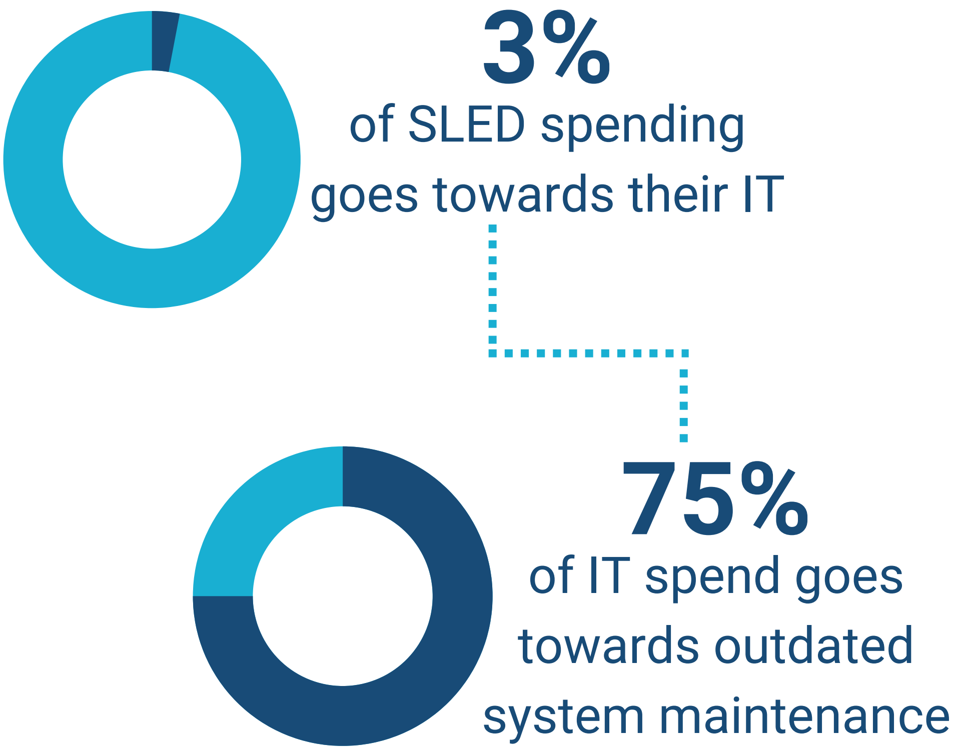
All organizations who experience a major data loss, security breach, or instance of system unavailability will be thrown into a catastrophic and costly event. The hope is that worst-case scenarios never happen, but the fact is they do. When they do, it's imperative to be ready to respond with the degree of speed and efficiency of business demands. Both cloud backup (BaaS) and disaster recovery (DRaaS) focus on minimizing data loss when a disaster hits and providing the business continuity that is needed for any SLED organization.



Budgeting for Cybersecurity

According to Barracuda, over 90% of cyber-attacks start with a phishing email with the intent to trick someone into installing or executing malware or disclosing sensitive information. SLED organizations are facing the reality of the need to detect, monitor, block, and recover from malicious cyber threats all while working with limited budget and IT resources. Only a shocking 3% of all SLED spending goes towards their IT. Additionally, about 75% of that small amount estimated by the Government Accountability Office (GAO) is spent on allocating to the operating and maintenance of legacy systems.

Because SLED organizations are funded by taxpayers and limited by fixed budgets, it is imperative that they find ways to get the best IT infrastructure for the right cost. Hiring a Chief Information Security Officer can cost and organization upwards of $200,000 a year. Outsourcing a third-party cybersecurity partner, such as a SOC|XDR platform, who can provide 24/7 monitoring, detection and response is a great way to keep SLED organizations protected for a fraction of the cost to hire a CISO at roughly $54,000 a year.



3%

of SLED spending goes towards their IT

75%

of IT spend goes towards outdated system maintenance

AGILEBLUE

AgileBlue helps you sleep at night by thinking about your cybersecurity 24/7, so you don't have to. With the perfect mix of people and technology, we work side by side as an extension of your team, providing our you with a SOC|XDR platform that is intuitive and adaptable at a fixed monthly cost.

Our platform is proven to detect cyber threats faster and more accurately across your entire digital infrastructure and cloud. We provide 24/7 monitoring, detection and response to identify cyber threats before a breach occurs.

Our tech is intelligent and automated, but we take a custom approach for every client we work with, analyzing and detecting exactly what you need it to. Our products are 100% cloud-based including advanced machine learning and user behavior analytics backed by our team of cyber experts who are always just a call away.

For more information, visit us at AgileBlue.com.

Ready to start protecting your company?

REQUEST A DEMO