SOCIAL JUSTICE | LEGAL AID | CYBERSECURITY

This Is What a Cyberattack Really Costs

The Kansas Cyberattack and the Client Who Could Not Get a Restraining Order

A Warning for Every U.S. Nonprofit Serving Vulnerable Clients

Most people think of a cyberattack as a technology problem. For one woman sheltering from a stalker in Kansas, it was something else entirely. It was the reason her restraining order could not be processed. It was the reason she could not go home.

What Happened

In October 2023, Jane Smith[1] was staying in a Kansas safe house, days away from getting the legal protection she needed. Her attorney had filed the paperwork, the case was moving, and for the first time in a long time, things were going in the right direction.

Then the Kansas Supreme Court sent an alert that the statewide court system was down.

Russian cybercriminals had hit the Kansas judicial network with ransomware. Their case management systems went dark and electronic filing stopped. Courts across the state were suddenly operating on paper, left scrambling to keep up with thousands of active cases.

For most people, that is an aggravating delay. For Jane, it meant staying in danger while the court system that was supposed to protect her sat offline. When she needed to check on her case status, she had to leave the safe house and go to the courthouse in person, putting herself at unnecessary risk. None of this would have happened if the system had been protected.

> Cyberattacks on nonprofits are not victimless crimes. Behind every breached database is a client who trusted an organization with something they could not afford to lose.

[1] For her protection, we are not using the client's real name.

What It Cost

Cleaning up after a cyberattack takes far longer than the attack itself. In this case, it took four months for court systems to fully recover.[2] Kansas courts had to request $2.6M in emergency funding just to get started with the recovery.[3]

Core systems came back online by December 2023, but full restoration stretched into early 2024, and every case filed, every hearing scheduled, and every order issued during those four months had to be manually reconciled once systems returned.

At Kansas Legal Services, attorneys lost access to court records and were unable to fully support their vulnerable clientele. The people they served had no choice but to wait.

And this isn't an isolated incident: Malware attacks on state and local governments rose 148% in 2023.[4]

148%	**$2.6M**	**4 Months**
rise in malware attacks on state and local governments in 2023	emergency funding requested by Kansas courts just to begin recovery	before court systems were fully restored and operational

> Kansas Legal Services clients did not get hacked, but they paid the price anyway. When an organization gets hit, there is nowhere to redirect the blame. The data exposed belongs to the people who trusted you with it. The question is not whether an attack could happen to you. It is whether you will be ready when an attack does happen.

The Lesson for Your Organization

The people who come to you are already carrying more than most people will ever understand.

They come with immigration cases that could determine whether they stay in this country. They come with eviction notices and custody battles and criminal records they are trying to put behind them. They are fleeing abuse, fighting for their children, and navigating proceedings that could change the course of their lives. They come to you because they need someone in their corner and they trust you to keep what they share safe.

Cybercriminals know exactly what you hold and exactly how little most nonprofits spend on protecting it. That gap between the your data's value and the resources protecting it is not a secret. It is an opportunity they are actively looking for.

Cybersecurity was probably not what you had in mind when you started this work. But the people sitting across from you every day are counting on you to get it right, even if they do not know enough to ask for it.

---

[2] *Government Technology*, "Amid Cyber Attack Recovery, Kansas Courts Advance IT Work"

[3] Kansas Legislative Research Department, *Kansas Cybersecurity Update*

[4] *StateScoop*, "Cyberattacks on state and local governments rose in 2023"

What We Built and Why

We at Techbridge have spent 25 years in the nonprofit community. We know what lean IT looks like. We know what tight budgets feel like. We know the pressure of doing work that matters with resources that never quite stretch far enough.

Our partner, Serket-Tech Security, specializes in protecting organizations that cannot afford to get it wrong. Their work covers endpoint protection, GRC compliance, security assessments, and staff training. They price their services for the reality of nonprofit budgets, not corporate ones.

Together we created Operation Safe Harbor because the nonprofit sector deserves the same level of protection as any other industry, and because the people nonprofits serve deserve nothing less. You should not have to choose between serving your clients and protecting them.

Sources

Kansas Legislative Research Department, *Kansas Cybersecurity Update* — Describes the October 2023 attack on the Kansas Judicial Branch as shutting down online access to the court system for several months.

https://klrd.gov/2024/12/18/kansas-cybersecurity-update/

Government Technology, "Amid Cyber Attack Recovery, Kansas Courts Advance IT Work" — Confirms the October 12, 2023 Russia-based ransomware attack on the state's judicial system, which necessitated that the office go offline and required months of recovery, according to the Kansas judicial branch's 2024 Annual Report. Also notes the OJA notified around 150,000 people in May 2024 that personal information was believed to have been exfiltrated.

https://www.govtech.com/security/amid-cyber-attack-recovery-kansas-courts-advance-it-work

AP / *SecurityWeek*, "Kansas Court System Down Nearly 2 Weeks in 'Security Incident' " (October 26, 2023) — Original reporting confirming the disruption left attorneys unable to search online records and forced them to file motions the old fashioned way — on paper.

https://www.securityweek.com/kansas-court-system-down-nearly-2-weeks-in-security-incident-that-has-hallmarks-of-ransomware/

StateScoop, "Cyberattacks on state and local governments rose in 2023" — Citing the Center for Internet Security, malware attacks increased by 148%, while ransomware incidents were 51% more prominent during the first eight months of 2023 than the same period a year earlier.

https://statescoop.com/ransomware-malware-cyberattacks-cis-report-2024/

Start protecting yourself now.

A free 20-minute conversation with our team is all it takes to find out where your organization stands and what it would take to protect it.

techbridge.org/safeharbor