

DataSure24's January Brainbytes: They Don't Teach This in School

DataSure24 is your cybersecurity partner, working to help meet your company's specific security needs. Each month, we'll offer bytes of information about emerging risks, news, and protective measures to help keep your data safe and your network secure.

New Year's resolutions come in all shapes and sizes: Get in shape. Budget your money better. Reduce stress. Spend more time with loved ones.

Better cybersecurity programming doesn't usually doesn't make the cut.

But less than three weeks into 2023, large-scale cyberattacks have quickly filled cybersecurity news feeds. **Last week the Des Moines School District, the largest in Iowa, was the victim of a ransomware attack.** The district closed schools for two days following the attack, so technicians could work to restore the computer system and protect data.

A week prior, the Swansea Public School District in Massachusetts closed schools for a day after it was struck by a ransomware attack.

Verizon's [2022 Data Breach Report](#) (DBIR) found **ransomware attacks accounted for more than 30% of breaches in the education sector. In 2022, 26 U.S. school districts - including the Los Angeles Unified School District (LAUSD), one of the largest school districts in the U.S. - had been hit by ransomware.** The LAUSD breach was deemed the largest educational breach in recent years by government officials.

Government officials warn that **malware attacks are on the rise, and that school districts are attractive targets. But why?**

- **School districts (specifically public school districts) work with limited budgets and often lack the resources or personnel to detect or respond to attacks quickly or adequately.**
- **Local school districts may be behind the curve when it comes to technology.** In fact, this past November, the Government Accountability Office warned the U.S. Department of Education that its plan for addressing risks in school is **YEARS** out of date and needs to be updated to include current cyberthreats and more specific guidance around cybersecurity.
- **School networks can be accessed by a large number of devices, some of which go home with students or are used for remote learning.**

The true cause for these data breaches may never be identified, so it's difficult to postulate specific solutions to prevent future breaches. Looking at the reasons *why* educational institutions are targeted, however, may provide some insight into **cost-effective changes to cybersecurity programming that will help keep data more secure:**

- **Implement Multi-factor Authentication**
- **Test and Protect Your Backups**
- **Prioritize Patch Management**
- **Global Admin Rights**
- **Know What Your Network Looks Like**

These changes, as part of a larger, **comprehensive cybersecurity program is the best way for businesses to help identify potential cyberthreats and prevent, or mitigate the effects of, an attack. This includes:**

- **Security Assessments**
- **Risk Assessments**
- **Chief Information Security Officer (CISO)**
- **Employee Awareness**
- **Incident Response Plan**

You can't protect your organization if you don't know where you are weak, where you are strong, where your security gaps are, and where you need help. With limited internal resources, **having an external party, such as DataSure24, serving as your CISO may be the smartest, cost-effective solution for your business.** A dedicated person overseeing, and focused on, the larger security program **will help ensure that your business makes the newsreel due to its successes rather than a cyberattack.**

At the end of the day, it all comes back to good cybersecurity.

*Cybersecurity should always be a business priority. **Unprepared organizations will become easy targets for cyberattacks.** Now is the time to learn the potential cybersecurity risks for your business, and build a complete cybersecurity plan.*

For more info on the benefits of CISOs, check out our latest blog: [Time to Do Your Homework on CISOs](#)

If you would like to speak more about how DataSure24 might help your company meet its security needs, contact us by clicking below, or call (716) 600-3724. We look forward to hearing from you!

[Email Us!](#)