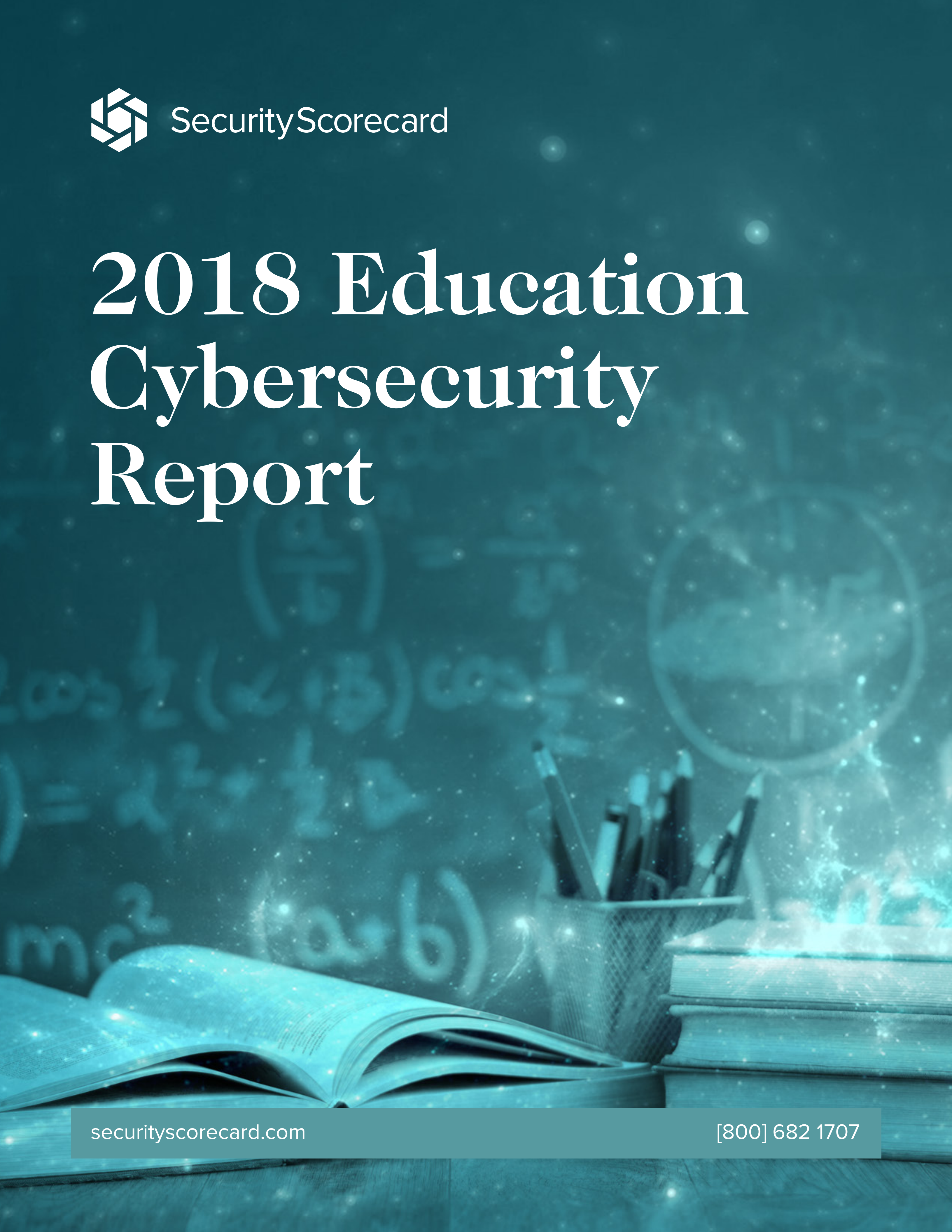


SecurityScorecard

2018 Education Cybersecurity Report

securityscorecard.com [800] 682 1707

Introduction

Data collection is a vital resource for schools across the world. These records, which can include a student's personal information (name, address, social security number, e.g.) to test scores and behavioral assessments, are highly sensitive in nature.

Though some schools continue to collect student data on paper, stashing it away in filing cabinets or off-site facilities, many more are now collecting and storing this information digitally—on local networks or cloud systems. This shift mirrors what's happening inside the classroom, as many schools have adopted new technology and learning systems into their curricula.

The shift to modern data collection, while integral to a student's growth and even a school's standing, also invites incredible risk considering the sheer amount of personal data that's being aggregated on networks. Taken as a whole, a student's school file can offer someone malicious actors a stereoscopic view of a child's life, including the location of their home and personal health data, to increasingly personalized academic records like attendance, teacher assessments and observations, learning outcomes, and test scores.

Alarmingly, out of 17 industries in the U.S., Education comes last in terms of total cybersecurity. This should be a cause for serious concern among students, parents, school boards, and the education industry as a whole. And yet, despite the ubiquity of data collection and the ever-increasing number of schools nationwide storing data digitally, the Education industry is not doing its part to protect its students (and, essentially, itself) from such risks.

Key Insights

SecurityScorecard analyzed 2393 companies with a footprint of 100 IP addresses or more in the education industry, from April 2018 to October 2018. We found the following:

- The Education Industry was the lowest performer in terms of cybersecurity compared to all other major industries.
- The Education Industry performed poorly in patching cadence, application security, and network security.
- There are several regulatory requirements for cybersecurity performance to improve in the education industry.

The results show that although hackers have become increasingly deft at stealing school and student data, the education industry is no better prepared to deal with these malicious threats.

What Information Is At Risk?

According to a 2017 report from the U.S. Department of Education[1], internet-based data collection, learning, and management platforms have not only become more ubiquitous but also the target of more precise, dangerous hacks. And it's happening more and more often. Despite this, the study notes that many schools continue to underestimate the need to responsibly monitor and protect network infrastructure.

Securing these networks and protecting this information is essential. There is a growing concern because schools collect an incredible—and vastly increasing—amount of personal data about students, to varying degrees.

As schools incorporate new testing and teaching methodologies based on technology and its ability to compile massive amounts of data, the information stored increases exponentially. Not long ago, teachers mentally recorded their observations and strategies for working with students. Assessment information, learning tool data, educator observations, attendance data, instructor feedback, and summative evaluations are now aggregated electronically, providing easier access to educators, but subsequently also to malicious actors.

[1] United States, U.S. Department of Education , Office of Educational Technology. (2017, January). National Educational Technology Plan. Retrieved from https://tech.ed.gov/netp/

The rise of Computer-Based Assessments for Learning (CBAfL) offers additional resources for educators, but also poses extra privacy and cybersecurity concerns. While CBAfLs provide real-time snapshots of students' academic strengths and weaknesses, they also collect identifying information, so educators can differentiate between individual students. As much as teachers need access to these metrics, they also need better security awareness to protect today's youth.

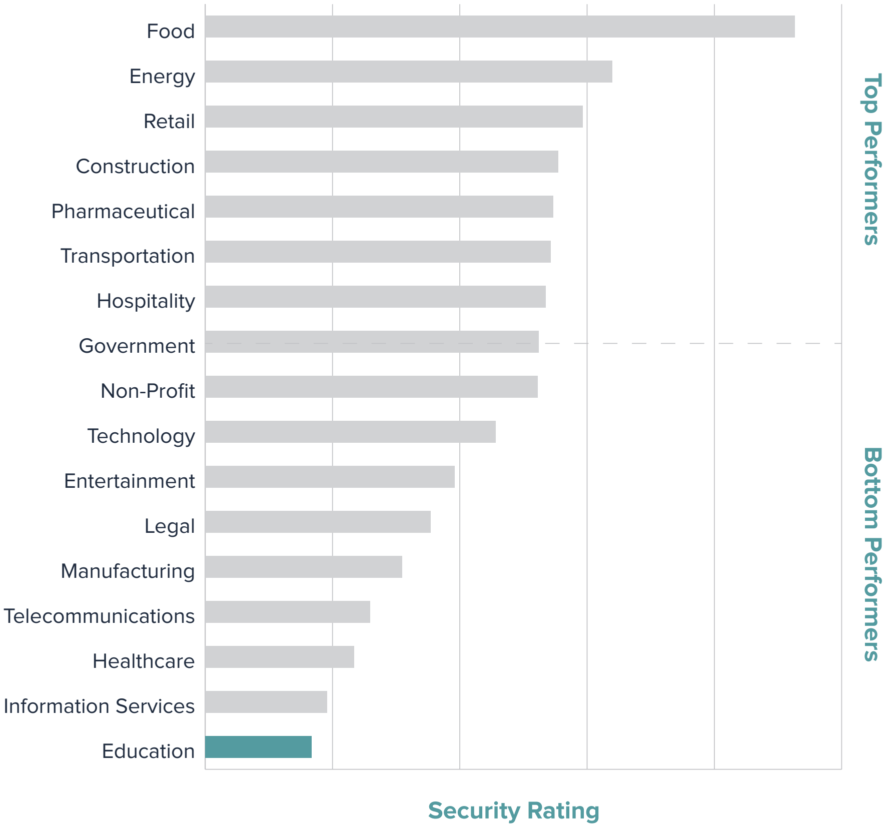
Where Do Schools Store Information?

Today, schools formally use electronic databases to collect information and provide smoother student transitions from grade to grade. Cloud-based dashboards provide a single location for storing and sharing information. Educational Software-as-a-Service (SaaS) delivers teachers and school administrators visual data representations that provide at-a-glance insights to help track individual and group metrics which helps advance opportunities and close achievement gaps. Despite their value in helping at-risk students, dashboards pose data security risks because of the increased number of individuals with access to data, particularly in larger districts.

Only some schools integrate data with state information systems. The variability of resources available within schools, districts, and states create another problem for data storage. An individual school may store information related to daily work, while the district stores aggregated information in its databases, and the state collects data from standardized testing. In areas where funding restricts data sharing opportunities, student personal data may be at risk.

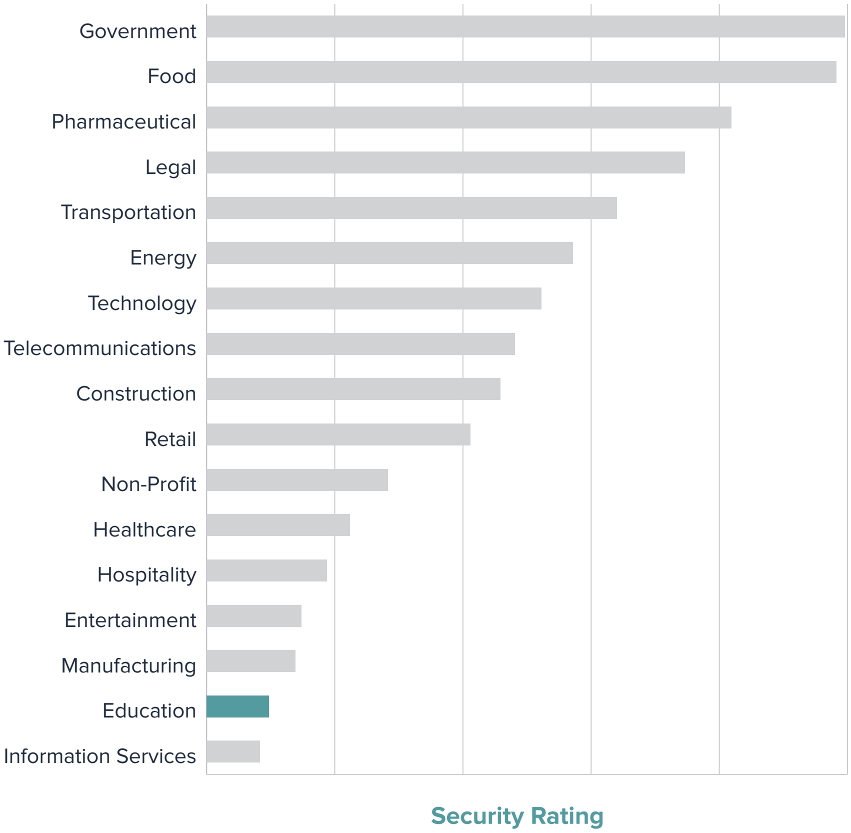
As education continues to move toward the future, local institutions will need to safely share information with state and federal level stakeholders.

Overview: The State of Cybersecurity in the Education Industry



Education struggles with application security, endpoint security, patching cadence, and network security. These four cybersecurity weaknesses put youth at risk, in spite of schools' efforts to protect children and prepare them for the future. As a result of these cybersecurity weaknesses, education comes in last in terms of total cybersecurity safety, out of 17 industries.

Application Security

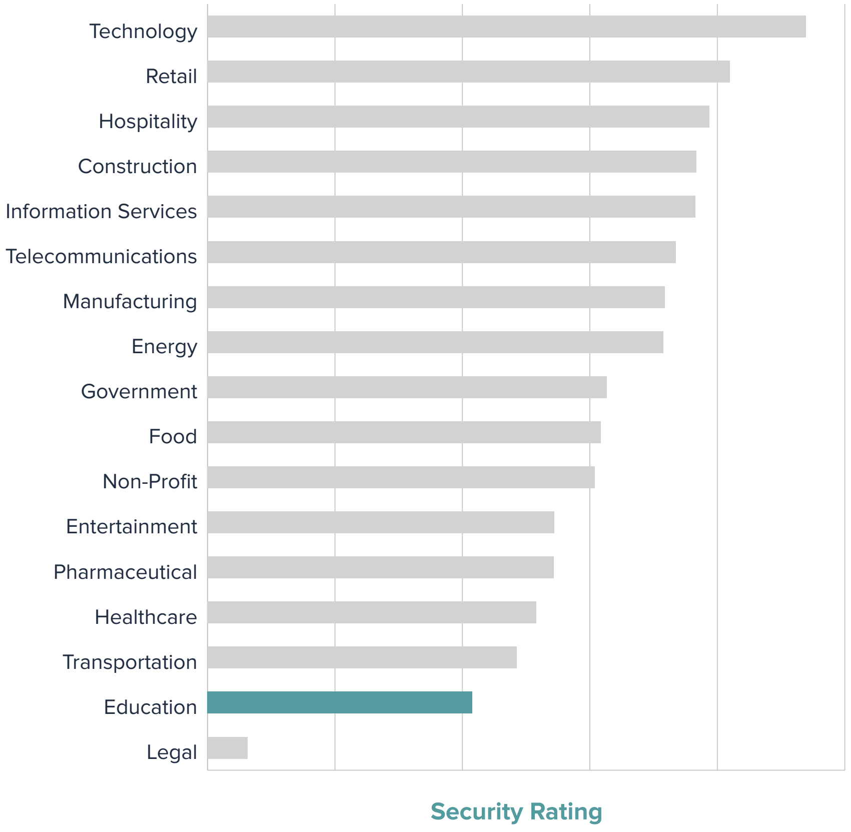


Application security implies removing vulnerabilities that allow malicious actors to breach software. As more schools rely on educational technology and software solutions for testing and metrics, substantial risks come into view. The "Cyber-Security in Today's K-12 Environment" study notes that application software vulnerabilities represent a top target for hackers, and educators' reliance on these technologies is one of the most significant data breach risks.[2]

School districts, both large and small, incorporate a wide variety of stakeholders. Unfortunately, the sophistication of their in-house technology varies and the physical locations of those involved make consistent staff training a challenging task. While the Great Schools report suggests implementing a life-cycle strategy to incorporate application security as part of system development, schools mid-integration cannot engage in this cost-saving technique.

[2] “Cyber-Security in Today’s K-12 Environment.”Council of Great City Schools (Fall 2017)."

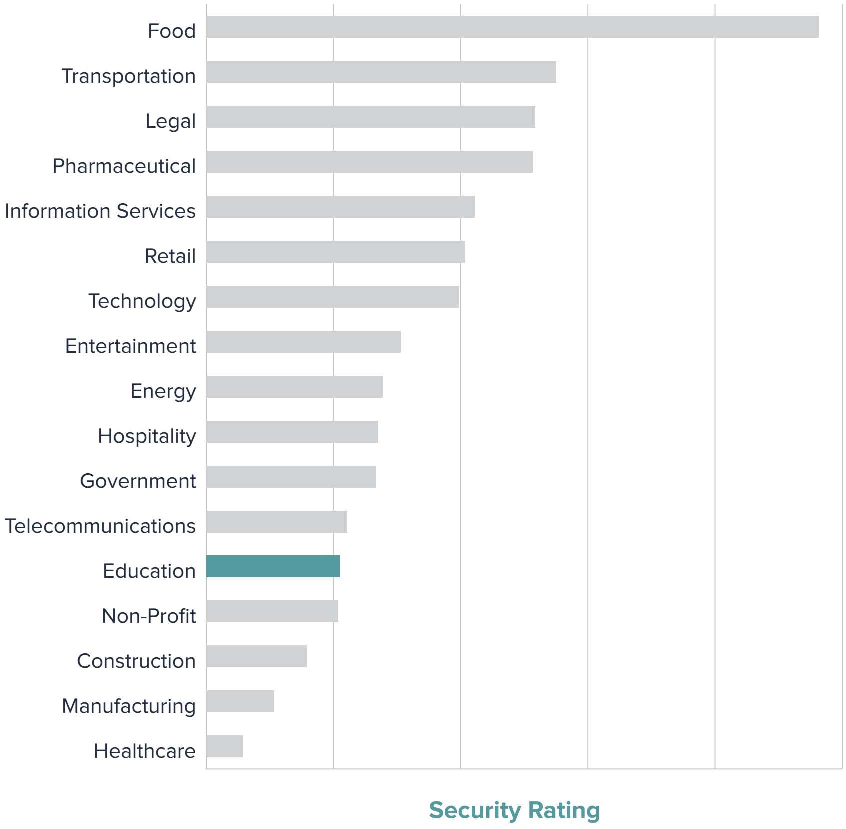
Endpoint Security



Traditionally, endpoint security focuses on protecting devices from unauthorized software users, including hackers. The increase in classroom devices places education at a higher risk if its endpoint security systems fail.

As students increasingly commute with devices, they put educational resources at risk by connecting to their home networks. The younger the students, the higher the risk. Schools need to secure sensitive data stored on district devices and find more efficient ways to report lost or stolen ones.

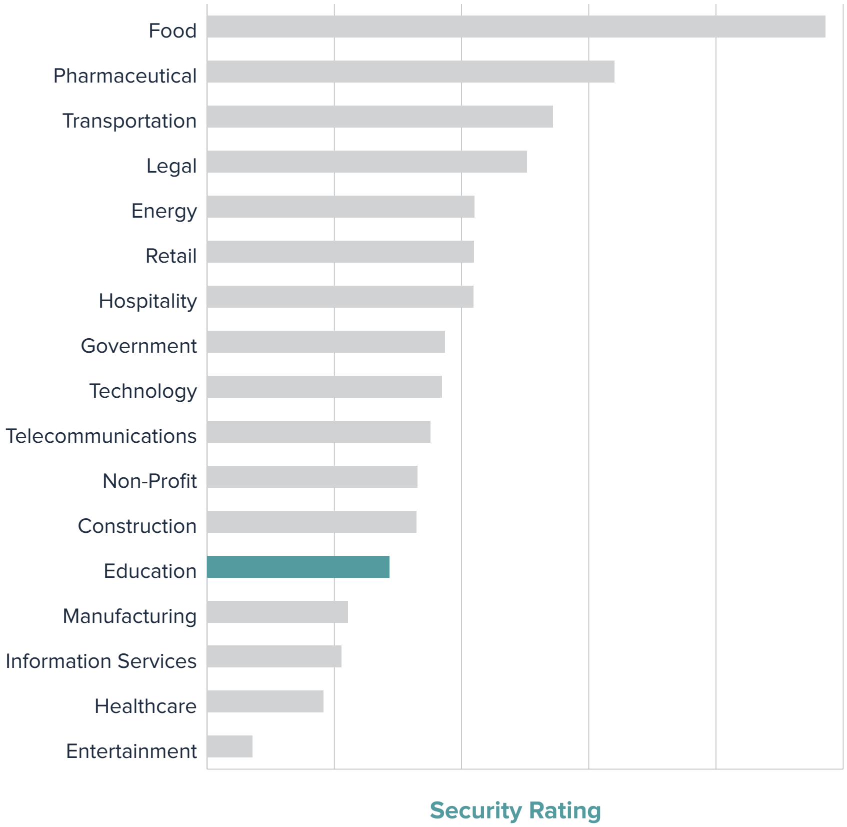
Patching Cadence



Updating software to eliminate security vulnerabilities requires time and resources. However, the continuous access and use of electronic devices makes software updates an essential security practice.

Despite IT departments recognizing the importance of a rapid patching cadence, updates are often scheduled when systems are inactive. A slow patching cadence or late patch installation, open systems up to unauthorized users.

Network Security



Networks are indispensable to access classroom materials and resources as they incorporate more laptops and tablets than curricular tools. As more students use cloud services to connect work between the home and the classroom, the education sector needs to focus on business continuityof network security.

59% of service providers experienced distributed denial of service (DDoS) attacks in 2017, a 2018 SC Magazine article shows.[3]

Despite the low number of attacks on education systems, the rise in DDoS attacks exposes the education system to malicious actors actively seeking weaknesses to exploit. Network security issues plague the education industry as it stands on the brink of becoming the next major attack target.

[3] Mayne, M. (2018). The complexity of DDoS attacks is rising says a new report. Retrieved from https://www.scmagazineuk.com/complexity-of-ddos-attacks-is-rising-says-new-report/article/738739/

Keep It Private: What The Regulations Say

Schools must follow a litany of privacy regulations to protect student information. Navigating them can be overwhelming, but we need to understand the rules as well as their intersections.

The Family Education Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

This US federal law grants parents a right to inspect and review student records until their children are 18. They can also ask for changes to the data and allow the disclosure of certain amounts of information. Once children turn 18, or attend post-secondary institutions, these rights revert to the child.

In terms of information technology, educational institutions need to meet FERPA requirements when engaging in online or connected services. Therefore, schools must inform parents and students to obtain appropriate consent.

The Protection of Pupil Rights Amendment (PPRA) (20 U.S.C. § 1232h; 34 CFR Part 98)

When schools attempt to collect survey, analysis, and evaluation information, PPRA governs the use and consent rights. This US federal regulation set forth by the U.S. Department of Education requires written consent in 8t protected areas. Data concerning behavior and attitude feed classroom analytics technology.

As more schools incorporate applications collecting personal information, they need to ensure not only its safety but prepare the appropriate consent and notifications.

The Children's Online Privacy Protection Act (COPPA) (15 U.S.C. § 6501–6505)

COPPA focuses on children aged 13 and under, and states that schools need to ensure that information comes with verifiable parental consent. For example, any elementary and middle-school web-based application that uses student information for logins, such as Google Classroom or tablet -earning applications, must also include a written parental consent form.

COPPA only applies to information that travels across the Internet. However, since many applications involve wireless connections for access and use, schools must review the data collected to ensure compliance.

The Children's Internet Protection Act (CIPA) (47 U.S.C. § 254)

Under CIPA, educational institutions who receive educator discounts for Internet access must certify the existence of an Internet safety policy and show proof of technology protection measures. Moreover, these protections must include blocking and filtering Internet access to images or content defined in the regulation as obscene, pornographic or harmful to minors, while also ensuring constant online monitoring of minors' activities. Finally, CIPA also requires that schools provide education about appropriate online behavior for chatrooms and social networking, as well as cyberbullying awareness.

While this legislation does not govern data protection, it incorporates firewalls and Internet monitoring that coincide with other information security and cybersecurity requirements.

General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

In May 2018, educational institutions will need to follow GDPR consent requirements. Articles 12, 13, and 14 discuss consent. The GDPR seeks to ensure fair and transparent permission for collecting data. Additionally, the GDPR requires data subjects have ongoing review access and revocation opportunities.

While not a US regulation, many US schools may need to engage in GDPR compliance. The GDPR's definition of EU citizen includes any foreigner living in the EU, as well as individuals holding EU citizenship, living abroad. School systems should review their student population to ensure compliance with GDPR requirements for children and families who fit the GDPR's definition.

Societal expectations bombard educators and school IT departments. Parents read about applications to help children learn and then request that schools use them. Parents, however, do not understand the ongoing work that monitoring student data requires.

The 2016 National Educational Technology Plan provides some direction for educational institutions throughout its 107-page report.[4]

The Lesson on Cybersecurity

All educational institutions should have a cybersecurity plan that takes into account technical aspects such as monitoring and managing networks, maintaining and upgrading equipment, estimating network capacity, protection with firewalls and anti-virus/anti-malware software, filtering content and security, and paying for insurance and licensing fees. Additionally, schools should incorporate network redundancy and backup recovery plans. A cybersecurity plan should reflect a holistic approach to student data protection. By incorporating technology and people, a robust program mitigates risks, while also ensuring ongoing education instills good security habits into employees, students, and their parents.

[4] United States, U.S. Department of Education, Office of Educational Technology. (2017, January). National Educational Technology Plan. Retrieved from https://tech.ed.gov/netp/

About SecurityScorecard

SecurityScorecard helps enterprises gain operational command of their security posture and the security posture of their third-parties through continuous, non-intrusive monitoring. The company's approach to security focuses on identifying vulnerabilities from an outside perspective, the same way a hacker would. SecurityScorecard's proprietary SaaS platform offers an unmatched breadth and depth of critical data points including a broad range of risk categories such as Application Security, Malware, Patching Cadence, Network Security, Hacker Chatter, Social Engineering, and Leaked Information.

To receive an email with your company's current score,
please visit instant.securityscorecard.com.

www.securityscorecard.com
1 (800) 682-1707
info@securityscorecard.com
@security_score

SecurityScorecard HQ
214 West 29th St
5th Floor
New York City, NY 10001