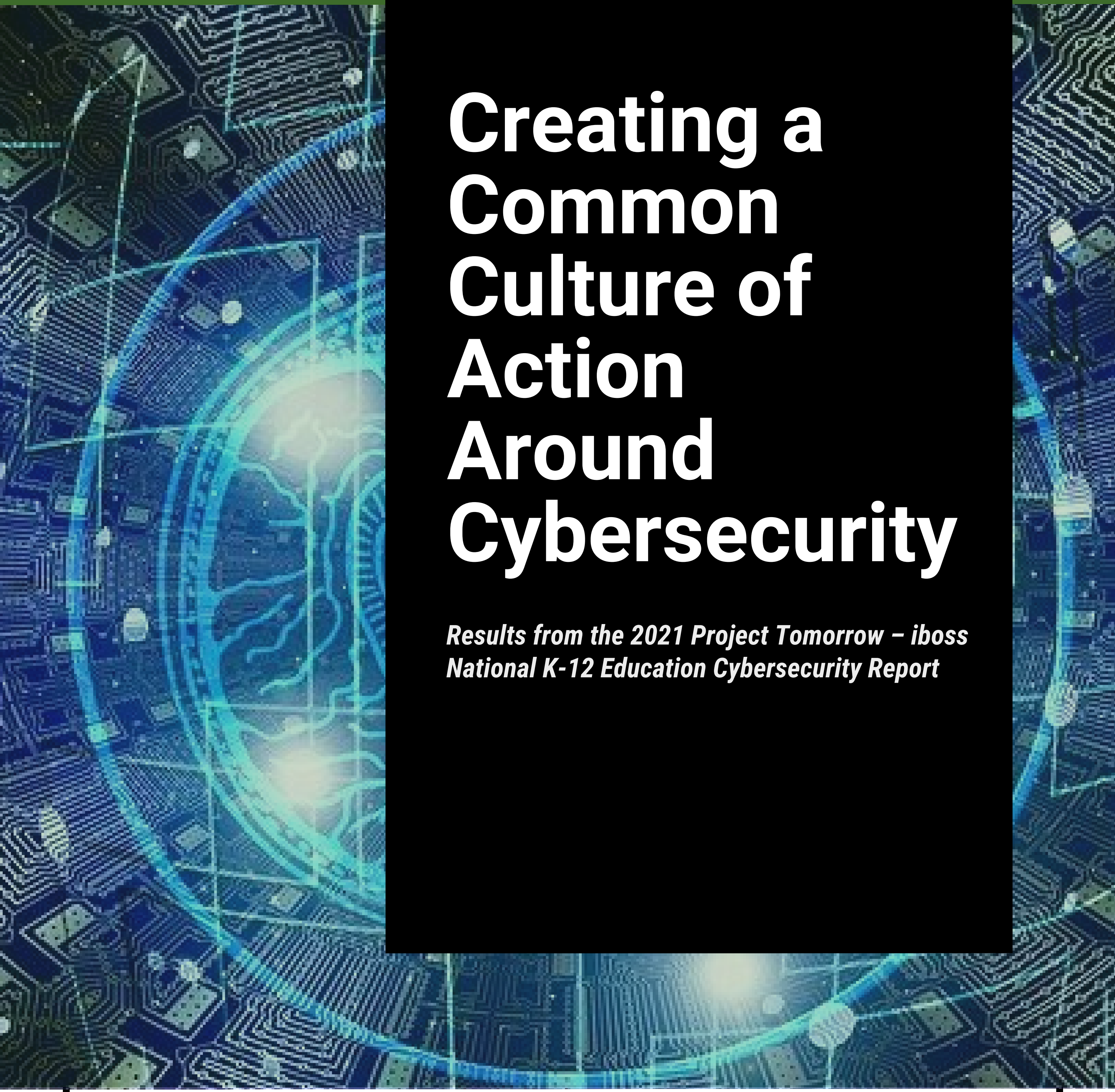


# Creating a Common Culture of Action Around Cybersecurity

*Results from the 2021 Project Tomorrow – iboss National K-12 Education Cybersecurity Report*

project tomorrow SpeakUp

iboss™

# Introduction

*Increasing the security posture within a school district necessitates deliberate education of executive leadership so that a common cultural understanding about the importance of cybersecurity is adopted across the organization.*

*-District Technology Leader*

Executive leaders across all sectors have a fiduciary responsibility to protect the tangible and intangible assets of their organization. Increasingly, those assets include mission-critical data and information systems. The same is true for K-12 education enterprises with the additional imperative, unique to education, to ensure that technology resources are readily available and safe to use to support the educational mission of the school district. At the heart of this obligation for comprehensive asset protection is the need for a shared value system and accountability around cybersecurity across the entire organization. To that end, today is very much different than yesterday in K-12 education.

The pandemic and resulting disruptions in traditional school modalities created a new stress-test for the technology infrastructure in many school districts. To support the continuity of learning, a core component of a school district's mission, new technology plans and rollouts were quickly implemented that significantly increased the digital footprint and reach within many districts. For example, an unprecedented number of digital learning devices and mobile hotspots were distributed to students from kindergarten through high school. Learning management systems were not only adopted but their usage was mandated alongside new online curriculum products supporting both core and supplemental instruction. This resulted in record levels of online activity and product usage by students, teachers and staff. Online tools to support communications from school to home as well as internal operational interactions have become essential resources. And adoption plans for new cloud-based applications including for finance and human resources were re-prioritized on a faster timeline. For the most part, these changes in our education enterprises, most notably around the increased usage of technology within both the instructional and operational aspects of a district, are permanent changes. Despite nostalgic pulls for a pre-pandemic school model, it is simply not possible to turn the clock back to February 2020 and unravel the increased dependency we have today on technology within our education systems.

While many reports and media stories have documented the physical or behavioral impact of these changes on the way students access learning content or how a teacher records their professional development time, there are other ramifications of this new environment that may be less obvious but certainly not less important. Heading that list is the increased risk and vulnerability of K-12 education data and information systems to a cyberattack. With increased dependence on technology and a wider online network, especially beyond the traditional school physical footprint, comes the inevitable amplified exposure to new potential threats to mission-critical information systems. The fallout from a cyber or ransomware attack on a school district's infrastructure can have a long tail of impact beyond disruptions to the education delivery system including financial, public relations and community trust repercussions. And while there is much to be learned from how other sectors, including those in transportation, finance, retail and manufacturing have addressed their cyber threats and/or events, the readiness of K-12 districts today to deal with these new realities appears to be lagging despite the increased vulnerabilities and documented upticks in such threats and attacks.

Project Tomorrow's® annual Speak Up Research Project has documented the evolution of technology use, both from an instructional and operational perspective, within K-12 education since 2003. Since 2017, the Speak Up results have also included a focus on K-12 districts' cybersecurity preparations.  However, as noted above, today is very much different than yesterday especially relative to cybersecurity preparation. The combination of the expansion of technology resources within the K-12 education enterprise and the increase in cyber threats to school districts has mandated that we conduct a more comprehensive review of the state of cybersecurity within K-12 education. In partnership with iboss, a new Speak Up Research effort was initiated in spring 2021 to understand the views and values held by school district leaders on their overall readiness to address these unprecedented cybersecurity challenges. Nearly 600 district administrators and technology leaders from a representative cross section of school districts nationwide responded to the call for input on this urgent topic by completing an online survey between January and May 2021. Our analysis of the resulting data from the first annual **2021 Project Tomorrow – iboss National K-12 Education Cybersecurity Research Study** and collection of first hand insights from district leaders nationwide underscores the imperative for a new national call for greater awareness and action on K-12 cybersecurity.

It is our hope that this new executive report will be a clarion call that resonates from the classroom to the school board meeting for every district to implement a cross organizational strategy to combat the present and future threats to the security of their district technology assets. To support that work, this report identifies and discusses three specific K-12 Cybersecurity Insights from the Speak Up research that can provide district leaders with a starting point for developing a new cross organizational approach for their district's cybersecurity preparation.

# K-12 Cybersecurity Insights

1 **An effective cybersecurity plan must be rooted in a shared and realistic sense of concern, responsibility, and accountability within the district.**

2 **The new technology dependence in K-12 education demands that district leaders re-assess their approach to the management of their technology assets, both human and digital. This has huge implications for cybersecurity readiness and preparations.**

3 **Cybersecurity preparation begins with an understanding of the need to walk the talk with increased funding to support both readiness and mitigation efforts.**

These insights and the supporting research data are discussed in detail in this new report. It should be noted that the data findings reveal serious gaps in our current approaches, notably around the awareness levels of key leaders to the current cyber threats. Thus, in our concluding section, we are issuing a call to action for the nation's K-12 districts and supporting educational organizations, associations and companies to rally together to increase awareness on the urgency for more comprehensive K-12 cybersecurity information across all levels of leadership within a school district, the development of a new common culture that is dedicated to action on cybersecurity and the identification of best practices for effective data systems protection.

*We experienced a cyber event almost 2 years ago that shut us down. As a district we all went through the process of recovery together. We have full support of our Cabinet and Superintendent when it comes to keeping our network and student data safe.*

*-District Technology Leader*

**K-12 Cybersecurity Insight #1**

**An effective cybersecurity plan must be rooted in a shared and realistic sense of concern, responsibility, and accountability within the entire district team.**

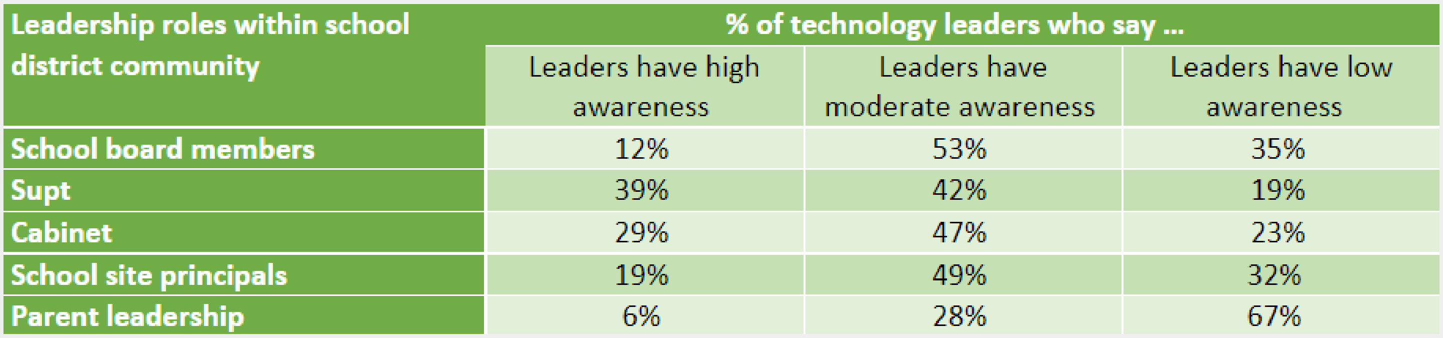
The protection of district assets including digital infrastructure and data should be a primary responsibility for every district leader. Cybersecurity is not just the job of the technology department. When that inevitable cyber-attack happens, it will impact every aspect of a school district's operations with implications for finance, human resources, student assessments, parent communications, teachers' instructional practices and community trust. Therefore, it is imperative that a cross-organizational approach to cybersecurity includes a focus on educating the key leaders on cybersecurity issues including the District Superintendent, school board members, chief academic officers, public relations directors, business and finance leaders as well as the chief technology or information officers.

The readiness of a district team to implement effective methods for thwarting or mitigating a ransomware attack or hack to district systems depends first upon leadership team buy-in regarding their district's vulnerabilities for a cyber event. Included in developing that buy-in must be an assessment of the overall knowledge or awareness of the team regarding risks and potential vulnerabilities to cyberattacks. Technology leaders in this year's National K-12 Education Cybersecurity research facilitated by

Project Tomorrow report a mixed bag of awareness within their district community on those potential risks and vulnerabilities. As documented in Table 1, only 39% of technology leaders say that their Superintendent has a high degree of awareness regarding cybersecurity issues. On average, the technology leaders believe that the members of their district leadership team have a moderate level of awareness about these mission-critical issues, but not necessarily a high level of familiarity or knowledge about cybersecurity. **For example, 53% of technology leaders say their local school board members are moderately aware or informed on cybersecurity issues; only 12% of the technology leaders agree that their school board members are highly aware.**

As districts create new plans and approaches for protecting their data and information systems, the awareness levels of parents about cybersecurity should be a top discussion as well. As noted in Table 1, two-thirds of technology leaders (67%) say that awareness level of parent leaders (such as those serving on district advisory councils or parent-teacher association leadership teams) is low. More work obviously needs to be done to ensure that parents are more familiar with the risks associated with a district breech or ransomware attack as they may be the ones who need to clean up a child's credit report or data records for years to come after the attack. **Additionally, given the impact of a cyberattack on community trust, transparency regarding how the district is protecting their assets including student data is an important new consideration for district communications.**

**Table 1: Awareness levels of various district leadership positions regarding cybersecurity – an assessment of the district technology leaders**



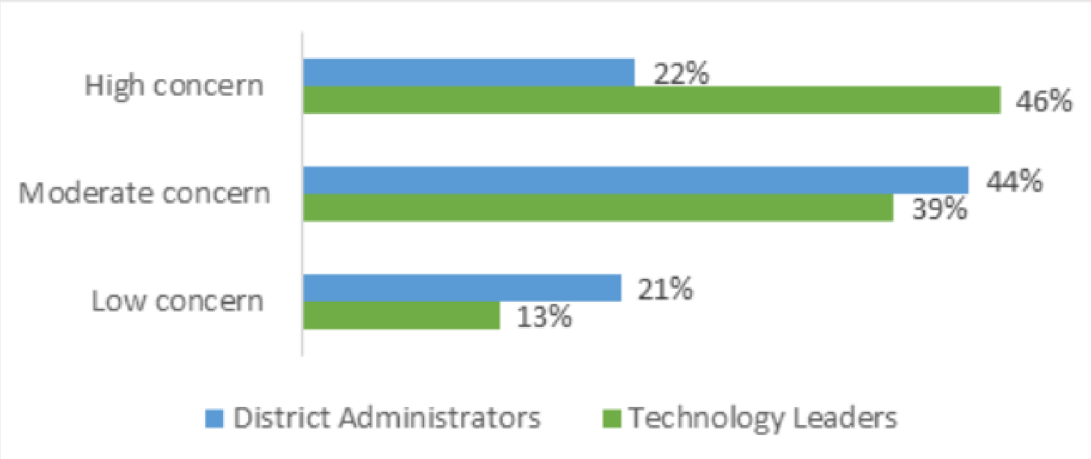
| Leadership roles within school district community | % of technology leaders who say ... | | |
|---|---|---|---|
| | Leaders have high awareness | Leaders have moderate awareness | Leaders have low awareness |
| School board members | 12% | 53% | 35% |
| Supt | 39% | 42% | 19% |
| Cabinet | 29% | 47% | 23% |
| School site principals | 19% | 49% | 32% |
| Parent leadership | 6% | 28% | 67% |

© Project Tomorrow 2021

Overall, the relatively low levels of awareness of key stakeholders in cybersecurity preparation is sobering. As more media attention is placed both on cyber incidents in education as well as commercial environments, awareness levels may rise. Fortunately, the K-12 Cybersecurity Resource Center provides a comprehensive reporting of publicly disclosed cyber-attacks within K-12 districts. Per their latest report, *The State of K-12 Cybersecurity: 2020 Year in Review*, the number of publicly disclosed school incidents (including student and staff data breaches, ransomware and other malware outbreaks, phishing attacks and other social engineering scams and denial-of-service attacks) increased 18% over 2019 reporting.[i] Correspondingly, the US Government Accountability Office (GAO) has also recently acknowledged both the increased vulnerability of K-12 institutions to attacks like these and the need for more updated resources to help school districts protect their digital assets.[ii] However, despite this enhanced spotlight on the threats within K-12 education, this year's data from the Project Tomorrow research indicates that there is a significant disconnect within many school districts, not just on familiarity with cybersecurity issues, but also on the seriousness of protecting data assets and a sense of urgency around ensuring adequate protections are in place. **When asked their level of concern regarding the security of their district technology infrastructure and networks against a malicious cyber-attack, only 22% of district administrators identified their current concern level as high** (Chart A). While over twice as many technology leaders (46%) said they have a high concern level, that percentage still feels low considering the prevalence and virality of recent K-12 ransomware attacks.

[i] https://k12cybersecure.com/year-in-review/
[ii] https://www.gao.gov/products/gao-22-105024

**Chart A: Level of concern regarding a cyberattack on your district technology infrastructure and network**



© Project Tomorrow 2021

**Key takeaway:** To develop a shared culture within your district around cybersecurity, start with a comprehensive education process so that all stakeholders and decision-makers gain a realistic understanding of the risks and vulnerabilities, accept their roles and responsibilities as active participants, and buy into a new district culture that prioritizes protecting district assets. Without that common cybersecurity preparation culture in place, it is highly challenging to expect all district administrators to be engaged in actively and purposefully addressing these challenges.

*I regularly spell out our cybersecurity vulnerabilities and needs to address such. In 2019-20 I took a hard approach to educate staff and cabinet regarding such vulnerabilities, we then put a plan in place to begin making these changes along with a communication plan. We also sent out a monthly newsletter with basic information regarding internet safety best practices. It is important to regularly communicate concerns and new cybersecurity threats to staff. These communications keep the threat and importance of cybersecurity at the forefront.*

*-District Technology Leader*

*This is what has worked in our district. Educate: Build awareness in users of their role in managing risks. Mitigate: Implement robust systems to protect data and networks. Investigate: Provide tools to monitor and determine system breaches.*

*-District Technology Leader*

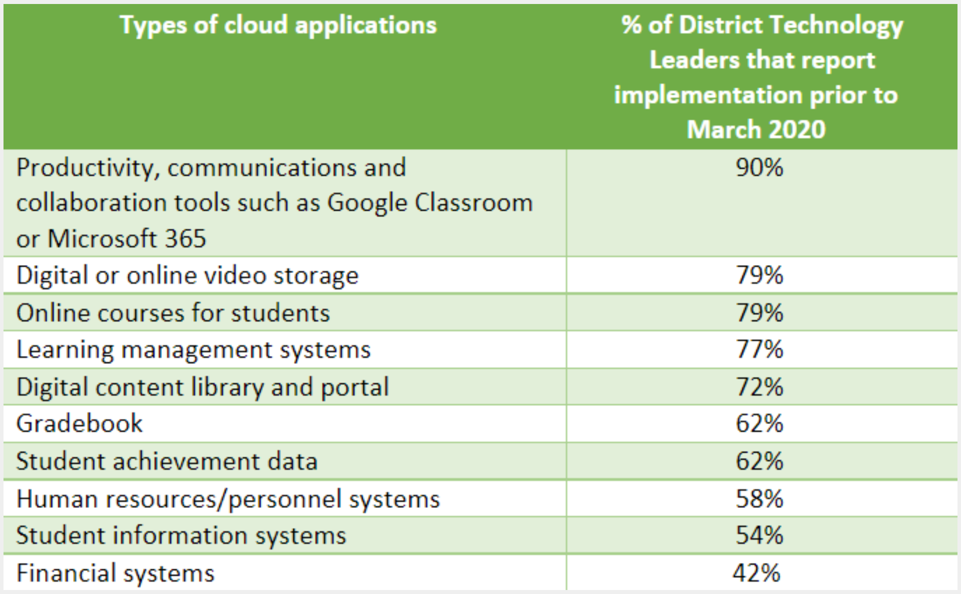
## K-12 Cybersecurity Insight #2

**The new technology dependence in K-12 education demands that district leaders re-assess their approach to the management of their technology assets, both human and digital. This has huge implications for cybersecurity readiness and preparations.**

It is widely acknowledged that the environment in K-12 education schools and districts is very different today than before the pandemic. Further evidence is noted by the technology leaders regarding their staffing challenges. Technology leaders identify that one of their biggest challenges right now is increased workload on their IT staff (72%) to provide heightened levels of customer service and support to students and families on an almost 24/7 basis. This is naturally precipitated by the greater implementation since March 2020 of one-to-one programs where every student is assigned a school-owned digital learning device (tablet, laptop, Chromebook) to use in school and at home.

However, while increased workloads may be a current reality, recent Speak Up research also indicates that in many districts outdated assumptions particularly around support models are still driving planning and decisions. This is particularly true relative to the structure of many district information technology departments and divisions. This need to re-evaluate the work and priorities of district IT departments is not a byproduct of the pandemic, however. The

**Table 2: Cloud applications in place in K-12 districts prior to March 2020**



| Types of cloud applications | % of District Technology Leaders that report implementation prior to March 2020 |
|---|---|
| Productivity, communications and collaboration tools such as Google Classroom or Microsoft 365 | 90% |
| Digital or online video storage | 79% |
| Online courses for students | 79% |
| Learning management systems | 77% |
| Digital content library and portal | 72% |
| Gradebook | 62% |
| Student achievement data | 62% |
| Human resources/personnel systems | 58% |
| Student information systems | 54% |
| Financial systems | 42% |

© Project Tomorrow 2021

process of re-engineering support models, staffing and aligning IT department priorities and plans to better reflect current district needs is long overdue, with early evidence of this need pre-dating the pandemic. The timeline for widespread district adoption of cloud-based services provides valuable insights here. In 2012, 46% of technology leaders nationwide reported that they were already strategically migrating certain applications and services, previously managed internally on district hardware, to the cloud. Four years later in 2016, over two-thirds of technology leaders said their districts' student information systems, learning management systems, gradebooks and content libraries were all in the cloud now. Given that rapidly escalating trend line, it was not surprising therefore that districts reported extensive use of cloud-based applications in place prior to the pandemic for both student and teacher tools as well as operational activities (Table 2). For example, prior to March 2020, 90% of districts already had in place Google Classroom or Microsoft 365 to support student, teacher and staff productivity.

Technology leaders report many benefits to moving to more cloud applications in the future. Those benefits include:

1. Greater reliability and flexibility within the IT infrastructure with cloud applications
2. Less concerns about storage constraints
3. Increased student access to applications outside of school
4. Greater integration of technology within teaching and learning activities
5. Increased overall efficiencies in operations

It would be expected that the district’s decisions to move from on premises services to cloud applications should stimulate a top to bottom evaluation of IT department staffing responsibilities. Tasks and roles formerly needed to support local infrastructure and hardware dependent services should be strategically abandoned with the move to cloud. Correspondingly, new responsibilities aligned with a greater dependence on technology and online connectivity would replace those no longer needed activities.

Given the steady migration to cloud services over the past 9 years and the increased district dependence on technology and online resources caused by the pandemic, building internal capacity to address cybersecurity should at the top of that list of new responsibilities. From the recent Speak Up research, however, that does not appear to be the case. **Nearly 6 in 10 technology leaders say that their current staffing for cybersecurity is not adequate to meet the needs of their district to protect information assets and resources.** In addition to the external threats to cybersecurity, this new finding indicates that there is also an internal threat; the lack of an appropriate investment in district cybersecurity expertise seriously undermines any potential readiness to protect district assets. This failure to support cybersecurity preparation with adequate staffing also explains why only 21% of technology leaders say that their district strictly requires cybersecurity vendors to complete a risk assessment to determine if they maintain third party validation and cloud compliance certificates. There is simply not enough staff to monitor this relatively easy to implement compliance requirement.

This failure to appropriately staff for cybersecurity is further evidence of the challenges districts face creating a system wide leadership culture that can adequately and appropriately support cyber readiness and preparation. When asked to identify the obstacles to creating an effective district culture for protecting network and data assets, technology leaders again cited inherent disconnects within their environment.

**The top obstacles include:**

**68%** Balancing the needs for access to education resources with concerns about security

**50%** Lack of technology expertise among teachers and administrators thus limiting their familiarity with basic security practices

**46%** Current internal culture is more reactive than proactive regarding security

**41%** School and district leadership not understanding the risks and/or potential impacts of a cyber-attack

All of these obstacles point to the need for greater awareness and education about cybersecurity across all aspects of our education ecosystems. But they also indicate the need for district IT teams to look in the mirror and evaluate if they are structured appropriately to support not only their current functions but also the ability to effectively advocate for cybersecurity and provide the internal leadership required. This is important as more and more districts evaluate and purchase security products and solutions. A good reference to support effective procurement is the National Institute of Standards and Technology (NIST) within the US Department of Commerce.[iii] The NIST guidelines are designed to enhance the security posture of all public sector entities and can be used by procurement departments within K-12 districts to ensure third party certifications and compliance. Examples include having vendors demonstrate that their certifications are up to date, data in the cloud can be isolated to meet state data privacy regulations, and the availability of third-party lab reports that validate the efficacy of the cybersecurity threat defense. Critical to the entire process of protecting district assets is the comprehensive understanding by district administrators and technology leaders on best practices for cybersecurity planning and the real unfortunate costs to the district of not doing that sµccessfully.

[iii] https://www.nist.gov/cybersecurity

🔑 **Key takeaway:** The education of key stakeholders around the urgency for more advanced and sophisticated cybersecurity protections is paramount to close the disconnect between district administrators and technology leaders on this important topic. But to ensure sustainability of these efforts, it is equally critical for district information technology departments and leadership to re-engineer their approaches to the current challenges in K-12 technology use, including support models and staffing priorities. As appropriate, district technology leaders need to strategically abandon older models that no longer serve the current environment. The current environment is typified now by increased access across the district enterprise and that requires a new 2.0 model for an IT department structure that both supports safe and secure access for all while also prioritizing the protection of those mission-critical district assets.

*I have three recommendations for improving cyber readiness. First, educate our user base to arm them with the knowledge needed to help protect from common attack vectors. Second, have dedicated staffing with a focus on cybersecurity as well as an understanding of the needs of the classroom. Three, have an appropriate suite of tools to help with protecting schools.*

*-District Technology Leader*

*To address these issues, we need sustainability in the funding for cybersecurity. When budgets are squeezed, operational costs like cybersecurity are the first to be hit. Additionally, district leaders need to enthusiastically embrace and model good cybersecurity habits and support the technology leaders in setting expectations for staff. It cannot just be the technology departments' problem.*

*-District Technology Leader*

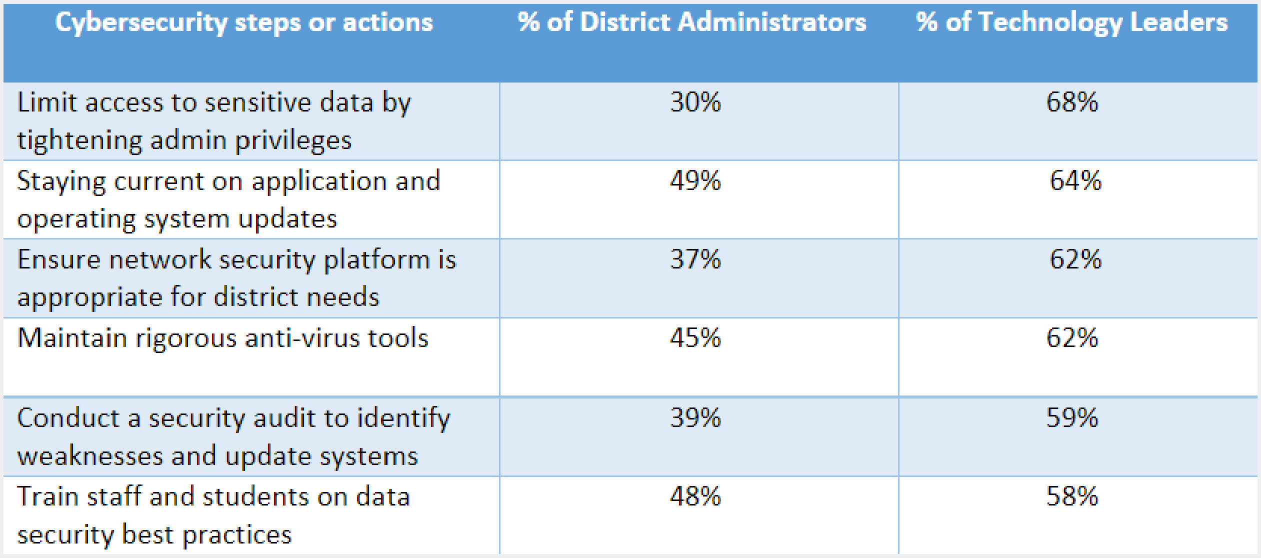
## K-12 Cybersecurity Insight #3

**Cybersecurity preparation begins with an understanding of the need to walk the talk with increased funding to support both readiness and mitigation efforts.**

Threats to the security of K-12 district data and networks is not a new phenomenon. However, K-12 districts are more vulnerable today due to their higher dependence on technology across their enterprises and an increase in the frequency and virality of the threats and attacks. This increased vulnerability means that we cannot continue doing the same things, or even doing the same things differently, rather we need to do different things within our districts to adequately and appropriately protect district data and network assets.

However, based upon the recent Speak Up research on cybersecurity preparation in K-12 school districts, technology leaders and district administrators are not on the same page even conceptually regarding the types of steps or actions that should be taken to reduce their district's vulnerabilities for a cyberattack (Table 3). **While 68% of technology leaders endorse limiting access to sensitive data by tightening administrative privileges to that data, only 3 in 10 district administrators hold the same view.** The deep disconnects between the views of this disparate leadership groups within a district present a real challenge for school districts who want to implement more rigorous security

### Table 3: What steps a school district should take to reduce cyberattack vulnerabilities

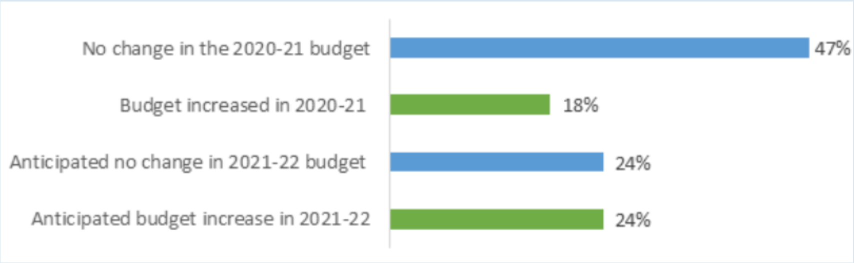


| Cybersecurity steps or actions | % of District Administrators | % of Technology Leaders |
|---|---|---|
| Limit access to sensitive data by tightening admin privileges | 30% | 68% |
| Staying current on application and operating system updates | 49% | 64% |
| Ensure network security platform is appropriate for district needs | 37% | 62% |
| Maintain rigorous anti-virus tools | 45% | 62% |
| Conduct a security audit to identify weaknesses and update systems | 39% | 59% |
| Train staff and students on data security best practices | 48% | 58% |

© Project Tomorrow 2021

measures. Given that the high value accounts for hackers will be the district leadership, implementing a system for two factor authentications for example will inherently require that district administrators see the value and importance of such steps.

In addition to the disconnect on which steps to implement, the divergence in the views of technology leaders and district administrators also speaks to the challenges around sustainable funding to support cybersecurity. If district administrators do not see the importance of certain protection measures, they are not likely to support budget line items or increases for cybersecurity. The new Speak Up research underscores this point despite the fact that the pandemic resulted in greater dependence on technology and increased exposure and vulnerability. **Only 18% of technology leaders reported an increase in their IT department budget to specifically address cybersecurity; 47% said that there was no change in their budget for cybersecurity from 2019-20 to 2020-21** (Chart B). Technology leaders were most likely working on their 2021-22 budgets at the



© Project Tomorrow 2021

**Chart B: State of district IT budgets for cybersecurity per district technology leaders – 2020-21 vs. 2021-22**

time they completed the Speak Up survey on cybersecurity in K-12 districts. At the time they were creating their budgets, only one-quarter of the technology leaders (24%) anticipated any kind of budget increase for the 2021-22 school year.

It is hard to “walk the talk” on cybersecurity if the funding is not there to support those efforts. While federal pandemic funding (CARES, ESSER) has dramatically increased the coffers of most school districts, it appears that much of the focus from IT departments has been on using those types of funds to support short term continuity of learning efforts such as buying digital learning devices  and mobile hotspots.

This discussion around budgeting for cybersecurity however also echoes back to our Cybersecurity Insight #2 about the need to rethink our IT department structure, functions and priorities. This same concept applies to IT budgeting as well. A dedicated line item in the district budget must be designated for cybersecurity. But to get to that point, district administrators and technology leaders must be on the same page regarding not only the important and urgent need to protect district assets but share a common culture about how to best address this district wide imperative of cybersecurity.

**Key takeaway:** New initiatives and imperatives come and go in K-12 education. But the most important and impactful ones are those efforts that are funded appropriately and sustainably. To truly walk the talk of cybersecurity in our K-12 districts, dedicated funding is needed to support awareness building activities and to address the current and future threats to our district’s data and information systems. As noted earlier, the ability of a school district to execute on its mission depends upon the availability of technology resources to support teaching and learning, the core of the educational imperative of a school district. That does not happen without appropriate levels of funding.

*Yes, everyone in the district must be more aware of cybersecurity. However, funding for cybersecurity is what stands as the biggest threat for K-12 right now. We must get our local commissioner, finance director, and school admin to understand this great need. Otherwise, it will once again by the IT Staff basically sitting and watching an incident happen and then having to pick up the pieces.*

*-District Technology Leader*

# Next Steps

K-12 education thought leaders often talk about how challenging it is to get a school district to change direction or adopt new practices even in the face of impending threats or potential new opportunities. This may be the reality with cybersecurity as well. To get momentum around how to effectively address the current and projected cyber threats to K-12 school and districts assets, four essential conditions must be in place according to those experts:

1. A high concern or interest level by the stakeholders
2. An actionable plan that propels forward movement
3. Appropriate levels of funding to support that plan
4. The explicit and informed support of the executive leadership team

The findings from the first annual **2021 Project Tomorrow – iboss National K-12 Education Cybersecurity Research Study** as

documented in this report indicate that as a nation, we have more work to do on all four of those essential conditions relative to K-12 cybersecurity.  Given that, Project Tomorrow in partnership with iboss is initiating a yearlong national call for greater awareness and action on K-12 cybersecurity. This new initiative will focus on helping district administrators and technology leaders in 2022 develop a common language and shared culture within their districts around these three questions:

1. **Why should cybersecurity be a district wide imperative with a cross-organizational foundation of support?**
2. **How should a district leadership team build a new shared culture around cybersecurity?**
3. **What are the best practices for supporting a healthy cross-organizational culture within a district to protect mission-critical data and information systems?**

Over the next few months, the Project Tomorrow – iboss team will be sharing additional resources and opportunities to engage with district leaders on these three critical questions. We hope that you will join this effort with us, not only to improve the cyber positioning with your district but also to share your expertise and experiences with cyber threats and/or attacks. Please contact us at research@tomorrow.org for more information on how you can be engaged in this new national call to action with us.

# Appendix

## About the 2021 National K-12 Education Cybersecurity Report Research Study

Utilizing our 18-year legacy of effectively collecting and reporting on key trends in the use of technology within K-12 education, Project Tomorrow launched in January 2021 a new dedicated Speak Up Research Project to better understand the state of cybersecurity readiness and preparation in K-12 schools and districts. Two specific audiences were invited to submit feedback on their experiences and views on cybersecurity:  (1) district or central office administrators who did not have direct responsibility for technology infrastructure within their district such as Superintendents, Chief Academic Officers, Directors of Curriculum or Education Services and/or Chief Business and Finance Officers, and (2) district or central office administrators who do have direct responsibility for technology infrastructure such as Chief Information Officers, Chief Technology Officers and Directors of Technology.  Given the significant changes in the education system over the past two years due to the pandemic which have exacerbated the urgent need to better address cybersecurity, it was imperative that both of these audiences, district administrators and technology leaders, be included in the research to understand where differences in perspectives and values may exist.

From January to May 2021, 599 district leaders representing both audiences submitted an online Speak Up survey about cybersecurity. The overall respondent field was very highly experienced. For example, 51% of the technology leaders in the sampling have 16+ years of experience in K-12 technology leadership; 42% of the district administrators had the same level of district or central office management experience.

The resulting quantitative data analysis specifically examined the comparative data between the district administrators and the technology leaders. Descriptive statistics are included in this report to document both differences and similarities between the two leadership audiences. Open-ended narrative responses were coded as part of the trend analysis. A sampling of open-ended comments from district technology leaders included in this report are representative of those overall trends. The resulting data findings were reviewed by a panel of current and former district administrators and technology leaders who provided their additional insights and reflections on the importance of this report.

### About Project Tomorrow

Project Tomorrow's nonprofit mission is to support the effective implementation of research-based learning experiences for students in K-12 schools. Project Tomorrow is particularly interested in the role of digital tools, content, and resources in supporting students' development of college and career ready skills.  The organization's landmark research is the Speak Up Research Project which annually polls K-12 students, parents, educators, and community members about the impact of technology resources on learning experiences both in school and out of school, and represents the largest collection of authentic, unfiltered stakeholder voice on digital learning. Since 2003, almost 6 million K-12 students, parents, teachers, librarians, principals, technology leaders, district administrators and members of the community have shared their views and ideas through the Speak Up Project. Learn more at www.tomorrow.org.

### About iboss

iboss is a cloud security company that provides organizations and their employees fast and secure access to the Internet on any device, from any location, in the cloud. iboss has built the largest global containerized SASE cybersecurity cloud footprint. The iboss SASE cloud platform provides network security as a service, delivered in the cloud, as a complete SaaS offering. This eliminates the need for traditional network security appliances, such as firewalls and web gateway proxies, which are ineffective at protecting a cloud-first and mobile world. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking nearly 4 billion malware threats per day. More than 4,000 global enterprises trust the iboss SASE cloud platform to support their workforce, including a large number of Fortune 50 companies. To learn more, visit https://www.iboss.com/.