VIEW POINT

# IMPLEMENTING CYBERSECURITY FOR K-12 REMOTE LEARNING AMIDST THE PANDEMIC

Infosys®
Navigate your next


## Abstract

With the ever-increasing threat landscape and hackers targeting all industries and services, cybersecurity incidents are on the rise for education sector as well. This is solely because the security controls are usually not as stringent in this sector and attackers can extract valuable data of students, teachers and parents and misuse it. The number of students in K-12 sector as well as in the higher education sector using online channels and mobile devices have increased multi-fold in the last couple of years. The second quarter of 2020 saw a huge surge in online education due to the Covid-19 situation. Teachers are motivated, but neither equipped nor trained to handle cybersecurity incidents, and the same is true for students who are very tech savvy but lack understanding of online safety. While it's paramount to raise cybersecurity awareness among the many actors of education sector, security controls also need to be implemented based on the "secure by design" principle. Through this paper, Infosys proposes a multi-layered cybersecurity approach to strengthen K-12 education's (kindergarten to 12th grade) security posture.

## Need for Cybersecurity in the Education Sector

In the new normal, online studies are of life. With 70% of educational institutions having very basic cybersecurity governance and more than 50% facing security incidents, the risk is at a critical stage. With data being shared at fast speed and being available from anywhere, at any point and from any device, a holistic approach to cybersecurity is need of the hour.

## Key Actors of K12 - Education Sector

Following are the common actors of K12-Education Sector".

**Core Users**: Students and teachers make most of education sector's users. Teachers publish and utilize online content, while it's part of day to day activities for students. The access for this core group doesn't just rely on school provided endpoints (servers, laptops / desktops); it is mostly through personal devices (laptops / tablet / mobile devices) and security for these devices fall into a no man's land at times. Parents, school administrators and coaches also form the core users' section. Parents usually need to access progress of students and provide required information to school administration. Administrators require access for admin and housekeeping purpose as well as to understand larger needs of students and teachers. Coaches require access to schedule sessions and track the progress of students. Often some of these users have access to PII (personally identifiable information) data of students. Also, health records such as vaccination records, medicines are also maintained at school levels, and so securing PHI (protected health information) data is very critical.

**Partial Users**: Prospective students, students from other schools, users from social services agencies and guests come under this category, which may require limited access to school premises, general information and in some cases, data about students.

**Vendors**: Vendors / staff for food, cleaning, school supplies may require limited access to data and apps, but they are integral part of education eco-system. The IT vendors / system providers are the core backend users, thus their being cybersecurity aware and access to them should be provided based on least privilege principle only.

## Key Systems involved in the K12 - Education Sector

Following are the systems that different K12-sector actors require access from / to.

**Primary Channels:** This includes devices, users explicitly use such as laptops / desktops, mobile devices, tablets. In these devices, users use web browsers, web/ mobile apps, backend channels (such as APIs / commands), social media accounts. Many of these apps are internet facing and can be accessed from anywhere. Schools usually provide very limited devices and so the BYOD (bring your own device) concept is common for students. This poses a significant challenge of securing such devices as the their control is not completely with the school.In addition, productivity applications such as Microsoft (office) 365, G suite are used daily and any access to them and usage also require proper security controls.

**Other Channels:** With cloud and IoT being an integral part of our everyday life, there are some channels, that are gaining time share in daily usage. Students and teachers often use devices such as Google Home, Amazon Alexa to obtain information on the fly. Smart routers also are used extensively. If these channels are not secured robustly, there can be devasting repercussions with regards to cyber breach. In fact, last year 70%+ IoT cybersecurity attacks were targeted on smart routers and smart cams.

**Backend:** These systems are used implicit, but provide the core functionality. They include backend servers (on-premise or in cloud), database, cloud hosted applications / APIs, SaaS applications, Big data, Artificial Intelligence (AI) services. With students being tech-savvy, the landscape is huge involving poly-cloud (provided from different cloud services providers), development and productivity platforms, tools, online education data and material, etc. Securing these backend services becomes critical for the K-12 education sector.

## Applicable Security Standards and Security Frameworks

The industry standards and frameworks relevant to the education sector are as follows:

**NIST**

- NIST 800-53
- NIST 800-171
- NIST 800-88
- ISO 27000
- ISO 27001
- ISO 27002:2013
- ISO 31000 (Risk Management)

**Other key controls:**

- HIPPA - health records of students
- PCI-DSS (for contractual obligations)
- SOX
- OWASP Top 10 / SANS Top 25
- CSA CCI (CCM - cloud control matrix)
- Security Assessment:
- HECVAT - only for 3rd party risk assessment
- SIG (shared assessment)

# Cybersecurity based on NIST View for K12-Sector

Following are the key activities that can be undertaken to implement a cybersecurity program by leveraging the NIST framework for K12-sector,


## IDENTIFY

- User list (core users, partial users, vendors) and associated accounts – verify if readily available in a directory
- Create roles matrix for all users
- Identity end-to-end user life cycle management process (on-boarding, offboarding, termination, providing access based on privileges / roles)
- Inventory of all hardware, systems and software and mapping of who has access and in what capacity
- Current state assessment to find gaps, address them and edge towards a standard cybersecurity reference architecture
- Risk assessment to identify existing critical vulnerabilities
- Identify data privacy requirements
- Create target cybersecurity architecture and roadmap
- Identify requirements for security awareness program and training
- Review and update relevant school board policies for security governance and risk management

## PROTECT

- Build a zero trust strategy encompassing all facets of cybersecurity and focus on user, devices and network first (access, authorization, multi-factor authentication, network micro-segmentation)
- Protect network – network segmentation based on tiers, track traffic and log related information
- Protect endpoints – encrypt laptops, implement endpoint detection and response (EDR) solutions
- Protect data – encrypt sensitive data at rest, in transit, backup data, data archival and purge policies and automation, implement data loss prevention (DLP) solution for network, endpoints and emails
- Protect workloads (services, APIs, applications) – enable API security and security for backend services with proper authorization and protect against atop vulnerabilities (OWASP top 10 and SANS 25)
- Protect devices – use modern device management techniques to authorize devices and restrict access from registered devices for critical information
- Protect users – create unique identities for all users and leverage multi-factor authentication
- Centralized SOC solution (SIEM) – collect security related logs in one place
- Secure by Design – cybersecurity embedded in each step from product envisioning to market release
- Periodic patch management
- All RFPs should involve cybersecurity requirements or/and compliance to already existing one
- Run security awareness programs and campaigns periodically

## DETECT

- Monitor the infrastructure and web/mobile usage
- Leverage data loss prevention (DLP) tools for monitoring at endpoint, network and email level especially for protected, confidential and PII data
- Utilize SIEM (security incident and event monitoring) solution to log, create alerts for any unusual activities on the network or by the staff.
- Track user behavior through analytics for unusual activities
- Enable visibility into cloud workloads (Infrastructure, Data, Applications, SaaS services, Office 365, etc.)

## RESPOND

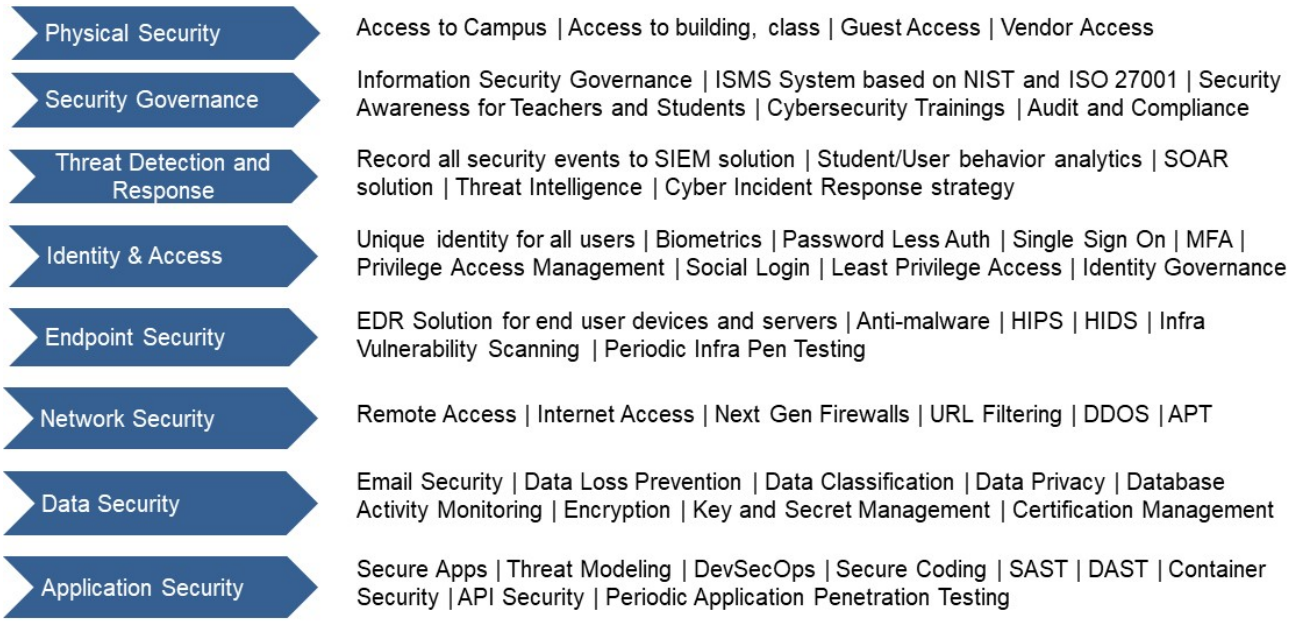
- Build a process for responding to a cybersecurity incident
- Ensure timely notification to stakeholders whose information/data may be at risk
- Build a process to manage communications with parents, community and the press
- Create a business continuity / disaster recovery plan
- Leverage cloud for additional backup
- Build a process for reporting the attack to the authorities
- Define processes for investigation and response (and simulation exercises)

## RECOVER

- Build a process across the organization to repair and restore the affected components
- Create RACI matrix and involve teams from infrastructure, network, applications to remediate
- Keep stakeholders updated about recovery progress
- Work with cybersecurity vendors (for third party tools) for any updates required in tools and their implementation

## "Secure by Design" based Security Framework for K-12 education

Infosys recommends the implementation of "Defense in Depth" and "Secure by Design" based cybersecurity framework for K12-sector. The below diagram depicts key security capabilities required across security tracks.




## Mapping Cybersecurity Controls with Actors

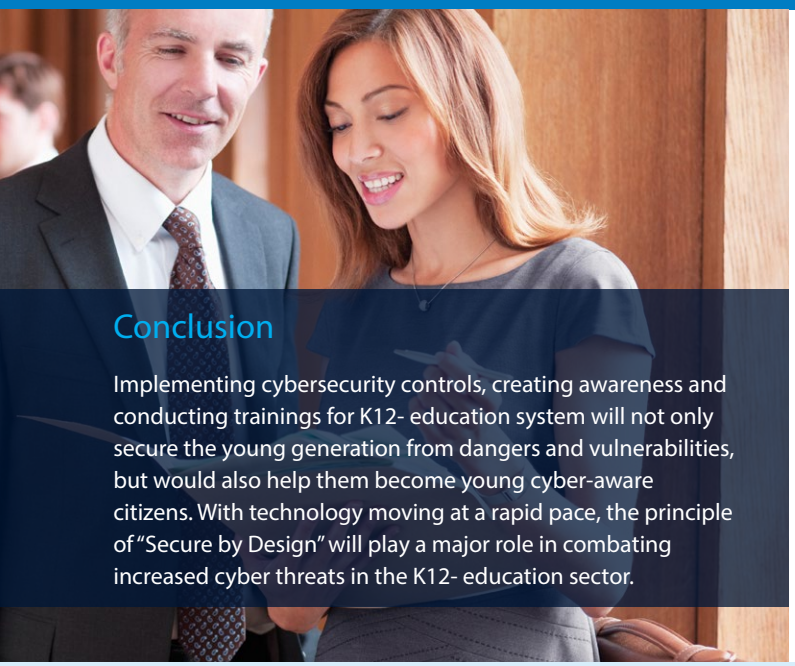
In case of major gaps between current cybersecurity posture and target security framework, security controls need to be prioritized. Given below is a table that provides quick reference to map security controls and K-12 actors. This table will require revisions based on school district's / K12-sectors current cybersecurity posture, target reference architecture and roadmap.

| Security Controls | Student | Teacher | Parent | Administration | Others |
|---|---|---|---|---|---|
| Physical Security | Yes | Yes | Yes | Yes | Yes |
| Security Governance | - | - | - | Yes | - |
| Security Awareness | Yes | Yes | Yes | Yes | Yes |
| Security Monitoring | Yes | Yes | - | Yes | - |
| User behavior analytics | Yes | Yes | - | Yes | - |
| IAM – Profile | Yes | Yes | Yes | Yes | - |
| IAM – Access / SSO | Yes | Yes | Yes | Yes | Yes |
| Endpoint Security – User Devices | School provided devices only | School provided devices only | - | School provided devices only | School provided devices only |
| Endpoint Security – Servers | Yes – only for applicable students | Yes – only for applicable teachers | - | - | Server / App administrators |
| Network Security | Yes - Implicit | Yes - Implicit | - | Yes – Implicit | Yes |
| Data Security | Yes | Yes | Yes | Yes | Yes |
| Data Privacy | Yes | Yes | Yes | Yes | Yes |
| App Security | - | - | - | - | App developers / admins |

## Recommended Initial Goals for a Roadmap

To implement the cybersecurity framework, Infosys recommends security tracks that can immediately tackle key risks and vulnerabilities. The important steps and priorities are stated below; the remaining security controls can be selected based on current maturity state and roadmap:

1. Define / update security governance and risk framework
2. Make cybersecurity top priority for every transformation program
3. Leverage cloud (such as AWS, Azure, GCP) for transformation and enable native cloud security controls to kick-start proceedings for quick wins
4. Security Governance controls – Create a security awareness program and conduct trainings for students and teachers
5. Threat detection and response – Enable a centralized SIEM (Security Information and Event Management) solution for security incidents and event monitoring
6. Identity and Access Management – Enable single sign-on and MFA; for administrative access enable privilege access management solution
7. Endpoint security – Enable EDR (endpoint detection and response) and MDM (modern device management) solutions
8. Network security – Enable journey toward network micro segmentation. Internet being the new intranet, ensure secured internet access
9. Data security – Encrypt data, enable DLP (data loss prevention) and email security solutions
10. Apps / APIs security – Automate security testing for applications and empower developers for secure coding



## Conclusion

Implementing cybersecurity controls, creating awareness and conducting trainings for K12- education system will not only secure the young generation from dangers and vulnerabilities, but would also help them become young cyber-aware citizens. With technology moving at a rapid pace, the principle of "Secure by Design" will play a major role in combating increased cyber threats in the K12- education sector.

## References:


1. https://www.nist.gov/cyberframework
2) https://www.nist.gov/itl/applied-cybersecurity/nice
3) https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit
4) https://k12cybersecure.com/blog/how-should-we-address-the-cybersecurity-threats-facing-k-12-schools/
5) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/checklist_data_breach_response_092012_0.pdf
6) https://privacy.a4l.org/geps/


## About the Author


**Neeraj Mathpal,** *Senior Technology Architect*

Neeraj possesses over 16 years of experience in Cybersecurity and offers next generation advisory and creative solutions for cybersecurity problems. He is passionate about helping enterprises and businesses to be cyber secure and has led large security transformation programs in US. He currently leads Infosys cybersecurity pre-sales technical practice for North America.

Neeraj_Mathpal@infosys.com


For more information, contact askus@infosys.com

Infosys®
Navigate your next