TATA CONSULTANCY SERVICES

Building on belief

Cybersecurity: A Proactive Leadership Strategy for Future-Focused Educational Institutions

Point of View

By Debasis Behura

Overview

Escalating cybersecurity threats in education

The cybersecurity threat landscape has become more dynamic in a post-COVID, hyper-connected world—including in the education arena. However, for many stakeholders in this sector, including administrators, educators, students and at the boardroom level, phishing, ransomware and denial-of-service attacks are not top of mind. Recent data suggests they should be. For example, according to the Cybersecurity in Higher Education 2021[1] report, $3.9 million USD is the average total cost of a data breach in education institutions.

Without a proactive cybersecurity strategy to protect identity and network and application access, there is more at stake than financials. Reputation and trust built over the course of decades or even centuries can vanish in an instant, costing not only irreparable damage to the brand but also in tangible terms of downtime, legal action, and intellectual property loss. These and other types of cyberattacks are successful in their intent because most educational organizations lack an effective security posture. And with many higher education institutes conducting leading-edge research in cybersecurity, any incident exposing their weakness in this area can raise credibility issues regarding the gap between theory, research and practice.

Proof point

$3.9 million USD is the average total cost of a data breach in education institutions. 80% of those breaches involve Personally Identifiable Information.[1]

[1] Cybersecurity in Higher Education 2021:
https://www.bluevoyant.com/resources/cybersecurity-in-higher-education/

Impact of cyberattacks and other information security incidents

With the quick shift to remote "emergency education" and boundary-less workspaces, the traditional classroom perimeter has dissolved. With an expanded attack surface, a new class of cyberthreats has emerged based on identity and access management risks that magnify the impact of other cyber incidents. In the higher education segment, students, educators, faculty and intellectual property (such as research data) are increasingly vulnerable to cyber-threats from **supply chain packages (including the IT supply chain)**, ransomware, phishing, and distributed denial-of- service (DDOS) attacks.

Did you know?*

- In 2020, there were 8.5 billion records compromised – that's more than 4 times the number of records breached in 2019.
- 23% of all attacks were related to ransomware, which was the #1 threat type in 2020.
- In 2020, cybercrime cost the world $8 trillion, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history and is more profitable than the global trade of all major illegal drugs combined.
- 33% of all attacks involved compromises via phishing emails, emphasizing the lack of security awareness culture in organizations which continues to be a big risk. Phishing is the #1 delivery method for ransomware and malware.
- In the education industry, it takes an average of 212 days to identify a breach and another 71 days to contain a breach, for a total of 283 days.

* From the 2020 report "Getting Ahead of Cybersecurity Risk Within Canadian K-12 Schools"

Proof point

Ransomware attacks alone have increased by 100% between 2019 and 2020.[2]
The average cost of a ransomware attack in higher education in 2020 was $447,000.[3]

[2] Threats Impacting Education Cybersecurity
https://www.fortinet.com/blog/industry-trends/threats-impacting-education-cybersecurity

[3] Cybersecurity in Higher Education 2021:
https://www.bluevoyant.com/resources/cybersecurity-in-higher-education/

In K-12, the biggest challenges typically come from data breaches involving student and staff personal information due to inadequate security practices of school vendors and partners providing administrative services. The rise in cybersecurity incidents in K-12 education is bringing about an increased awareness of the risks and creating a sense of urgency for implementing countermeasures among policymakers, school districts, vendors and students.

Proof point

In 2020, 377 school districts (and other K-12 education organizations) across 40 states experienced a record-setting 408 publicly disclosed cybersecurity incidents.[4]

Recognizing risk factors

COVID-19 exposed the lack of business continuity planning within all industry sectors, including education. With an "emergency education" scenario where classroom activities suddenly needed to be delivered via remote network connections, the lack of (or very weak) information security policy across the education sector became apparent. In addition, education has unique scenarios that have exposed it to higher risk for cybersecurity-related incidents.

Education risk factors include:

- **A culture of open collaboration.** The culture of academia itself, based on a foundation of openness, sharing and collaboration combined with a lack of cybersecurity awareness and preparedness, makes cyberattacks and other malicious cyber incidents more insidious. In addition, social learning (in online groups or on videoconference calls, for example) can allow accidental leaks where personal data is shared in chats or onscreen. This type of risk can also be seen on other social media channels like Instagram, Facebook and Twitter.
- **Proliferation of student accounts, unsecured remote desktop ports and IoT devices.** The challenges to information security have increased further as the classroom and network environment has rapidly expanded to include a proliferation of student accounts. In fact, student account and log-in data is among the most voluminous and highly compromised personal identity information (PII) data on the web. Students increasingly use university accounts to log in to a wider range of services, including administrative portals, remote video tools, university and student

[4] The State of K-12 Cybersecurity: 2020 Year in Review: https://k12cybersecure.com/year-in-review/

web applications and remote learning tools. This proliferation of accounts creates higher risk of data breaches and threats targeting vulnerable websites. Remote learning has also introduced the addition of many new, personal devices connecting from unsecured networks, introducing greater risk to malicious threat actors. These student accounts, all accessed by a variety of applications and devices, require strong identity and access controls.

- **Weak or nonexistent remote network security.** Attackers often exploit the less-than-enterprise-grade security inherent in IoT devices used in remote and home networks. The explosive growth in online learning has also created large numbers of short-term students, creating further burden on the infrastructure (including processes like background checks). The proliferation of such student accounts, often used well past graduation, compound the probability of data breaches over the long term.
- **Lack of basic email security.** Over half of all analyzed universities and colleges lack all basic email security configurations[5] such as DNS-based email security protocols to authenticate emails between users and protect against phishing attacks. Ad hoc data transfer processes, such as excel spreadsheet attachments, multiplied by increasing number of student accounts, further increase the likelihood of information security incidents.
- **Content management systems and unsecured network.** Vulnerable learning content management systems can also make soft targets for easy access into enterprise environments by threat actors.
- **Legacy infrastructure with no centralized control.** Many educational institutions are dealing with multiple, disparate departments using fragmented legacy technology and infrastructure that lacks central control and oversight.
- **Lack of adequate data protection and data recovery,** which allows ransomware to compromise backups.

Proof point

66% of universities lack basic email security configurations to authenticate emails between users and protect against phishing attacks.[6]

[5] Threats Impacting Education Cybersecurity:
https://www.fortinet.com/blog/industry-trends/threats-impacting-education-cybersecurity

[6] Cybersecurity in Higher Education 2021:
https://www.bluevoyant.com/resources/cybersecurity-in-higher-education/

When connecting from unsecured networks, these risk factors create exposed vulnerabilities to:

- **Phishing attacks.** Malware that injects code or redirects users to malicious sites
- **Ransomware.** Demands made by cyber criminals who threaten to disclose sensitive student data
- **Malware.** Common systems, applications and even web browsers used by students and educators infected with malicious code

Proof point

According to the Threats Impacting Education Cybersecurity report, 9 of the top 10 cybersecurity incidents target Internet of Things (IoT) devices and content management systems (CMS). The same study reveals that over one-fifth of all analyzed universities and colleges had open or unsecured remote desktop ports, which is the number two threat vector, behind phishing, for ransomware gangs.[7]

According to a recent CNN article[8]*, a ransomware attack occurred in January of 2022, impacting websites of about 5,000 schools (most in the US), disrupting their web presence and remote learning activities.*

[7] Threats Impacting Education Cybersecurity:
https://www.fortinet.com/blog/industry-trends/threats-impacting-education-cybersecurity

[8] CNN article "Ransomware attack affected websites of 5,000 schools" Jan 7, 2021:
https://amp.cnn.com/cnn/2022/01/07/politics/ransomware-schools-website/index.html

Understanding cybersecurity best practices

The research data shows there is a need for institutions to focus on risk in these areas and create a robust and resilient information security strategy to avoid financial loss as well as negative impact to trust and reputation. For example, many educational institutions, especially technology institutions, often publish information security research articles yet fail to have a solid cybersecurity strategy in place.

Essential elements of an effective cybersecurity strategy

Build a cross-function cybersecurity framework

Cybersecurity initiatives must encompass all functions, beyond just IT, within an educational institution to get buy-in and collaboration. According to the report, "A Systematic Review of Cybersecurity Risks in Higher Education," the following recommendations are essential for a proactive approach.

Embed cybersecurity awareness into the culture

- Start at the top. This means information security awareness must be part of strategic planning by leadership, including operational budgets.

- Create an assessment of what cybersecurity incidents and responses have cost – and could potentially cost – the organization.
- Provide ongoing training of human beings, often the weakest link, for password usage and to combat risking social engineering and phishing attacks.

Create strong governance, risk management and compliance focus with well-defined policies

- Develop a roadmap and incident response plan and define the owner.

Adopt a Zero Trust model

- Using defined access control policies, allow secure remote access privileges to only the network, endpoints, applications and services for which the user has been given explicit permission.

Implement ecosystem controls

- Build vendor risk management and IT supply risk management into the ecosystem.

Provide effective managed detection and response

- Use tested incident response and business continuity cyber drills.
- Conduct breach and attack simulation exercises.

Learn from others

- Observe and learn from peer institutions, including those that have been doing cybersecurity correctly and those who have not.

Use the partner/vendor network

- Create a proactive strategy leveraging partners to get insights into identified future security threats.

Edge networks with its distributed architecture should consider:

- Identity-driven controls like a secure web gateway for accessing internet and SaaS-based applications hosted by content providers.
- A cloud access security broker for cloud application access with threat detection/prevention and data protection capability.
- Zero Trust network access (ZTNA), for secure, VPN-less access to all endpoints, including a remote workforce to internal educational applications and systems hosted in the cloud or data center.
- Data leakage detection and prevention capability to detect and prevent any attempt of content leakage.

Data centers or content hosted in the cloud need to focus on:

- Network segmentation: All internet-facing applications should be segmented apart from the rest of the network to minimize any impact from potential breaches.
- Multi-factor authentication (MFA): This type of best practice authentication helps protect users from the likelihood of stolen credentials with additional authentication required during any attempted login.
- Web application security: Implementation of web application firewalls (WAFs) can help protect against phishing attacks and DDoS attacks that can cause a site outage.
- Browser security: Using a cloud-based security gateway helps protects against web-based malware attacks.
- Zero Trust Access (ZTA): This modern approach to access helps protect networks and applications using a zero-trust approach, providing only the necessary level of access privileges as needed.

Summary

The education sector around the globe is currently reeling and continuing to adapt to the disruption from the pandemic. Further disruptions caused by cybersecurity and data privacy incidents can be avoided. It is essential to be proactive, starting now, with the goal of making cybersecurity awareness education the first line of defense. In the end, a proactive approach to cybersecurity is a matter of trust: students, administrators, educators and other stakeholders in your organization expect and trust that you will protect their personal information from malicious attacks. Furthermore, educational institutions need every competitive advantage, so protecting the organization from cyber threats is imperative to protect your brand, your academic reputation and the future.

TATA CONSULTANCY SERVICES

Awards and accolades

#1 IN CUSTOMER SATISFACTION 2020/21 EUROPE Whitelane Research

top EMPLOYER NORTH AMERICA 2021 CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

top EMPLOYER GLOBAL 2020 CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

ASIA'S OUTSTANDING COMPANIES POLL 2020 ASIAMONEY

STEVIE AWARD 2020

CONGRATULATIONS CIO 100 WINNERS 2020

FinanceAsia ASIA'S BEST COMPANIES 2020

DIGITAL IMPACT AWARDS WINNER

CANADIAN HR AWARDS 2020

THE CIVIC 50 POINTS OF LIGHT

FTSE4Good

CDP DISCLOSURE INSIGHT ACTION

2020 Brand Finance® Awards

TOP 3 IT SERVICES BRAND

2020 Brand Finance® Awards

FASTEST GROWING IT SERVICES BRAND FOR THE DECADE 2010 - 2020

AWARDED Superbrands BRITAIN'S CHOICE 2020

AWARDED Superbrands AMERICA'S CHOICE 2020

Contact

To discover how to address today's most pressing challenges in education through the use of technology, visit https://www.tcs.com/education

Email: Education.Advisor@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world's largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 500,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit **www.tcs.com** and follow TCS news **@TCS_News.**