RADWARE SOLUTIONS FOR EDUCATION

EDUCATION CONCERNS AND CHALLENGES

Educational institutions require applications to streamline processes, provide content and cut costs. The growth in online services and web-based content introduces new challenges to school districts and universities that need to address issues such as 24x7 access to online services and protect student records.

Radware's *2018–2019 Global Application and Network Security Report* provides insight into the cybersecurity threats and challenges specific to the education vertical. The report summarizes perspectives from educational security professionals, including business concerns, the types of attacks experienced and their impact, and trends in attack landscape and threats. Educational business concerns include availability/staying open for business, protecting sensitive data and lack of expertise and resources to manage cybersecurity protection.

Staying Open for Business

Educational institutions depend on their websites and online services. Networks and applications must be available 24x7 to allow students and faculty to access resources, especially during admissions, exams and other critical time periods. Education respondents to the aforementioned survey reported that malware and bots, distributed denial of service (DDoS) and social engineering attacks were the most frequently experienced types of attacks.

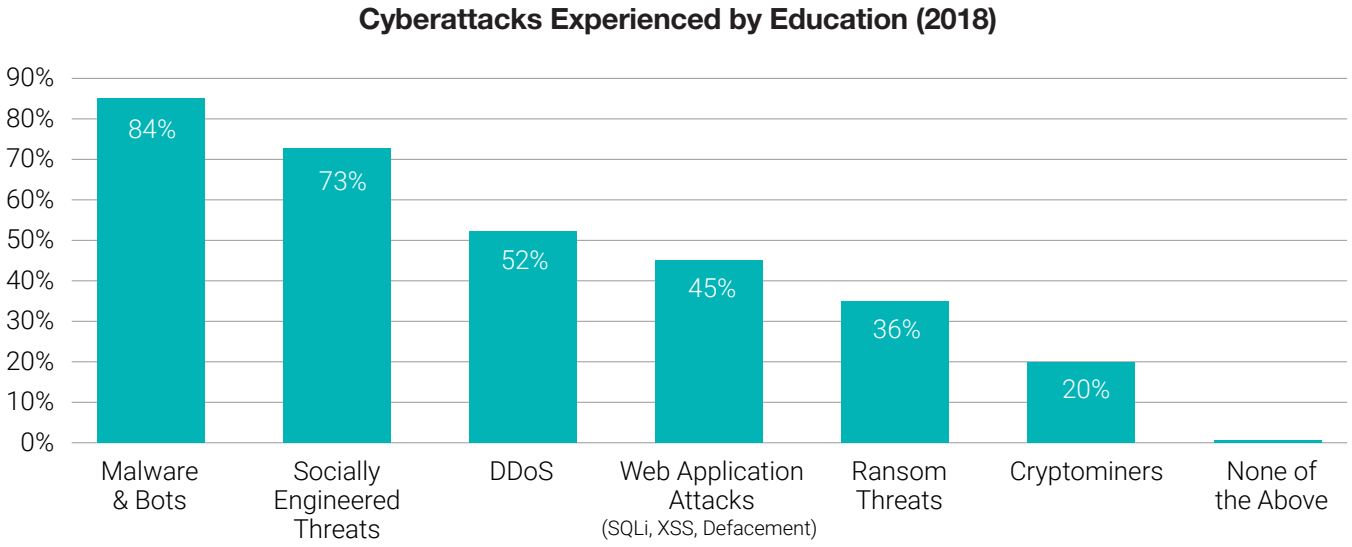

Figure 1: Types of attacks experienced (2018)

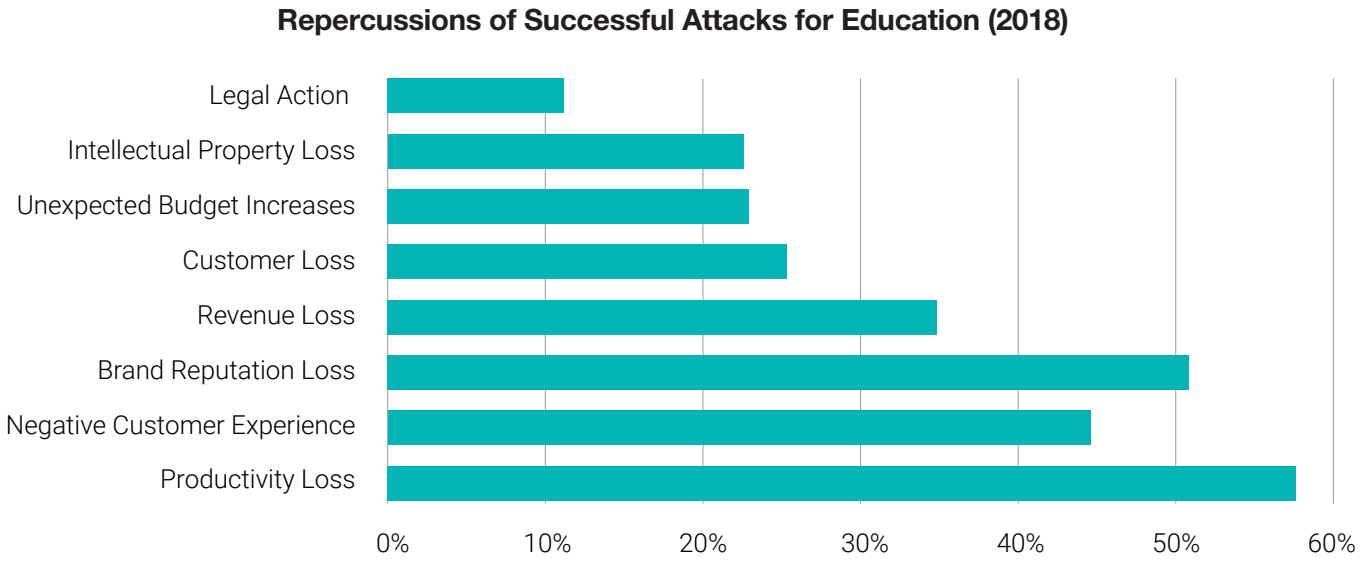

Figure 2: Repercussions of successful attacks (2018)

Because educational institutions are dependent on their applications, it comes as no surprise that application vulnerabilities were identified as the top threat (34%) that education IT managers were concerned about for 2019. Students and faculty require ease of use and security of their applications/online services to be on par with standards set by Google, Amazon and Netflix.

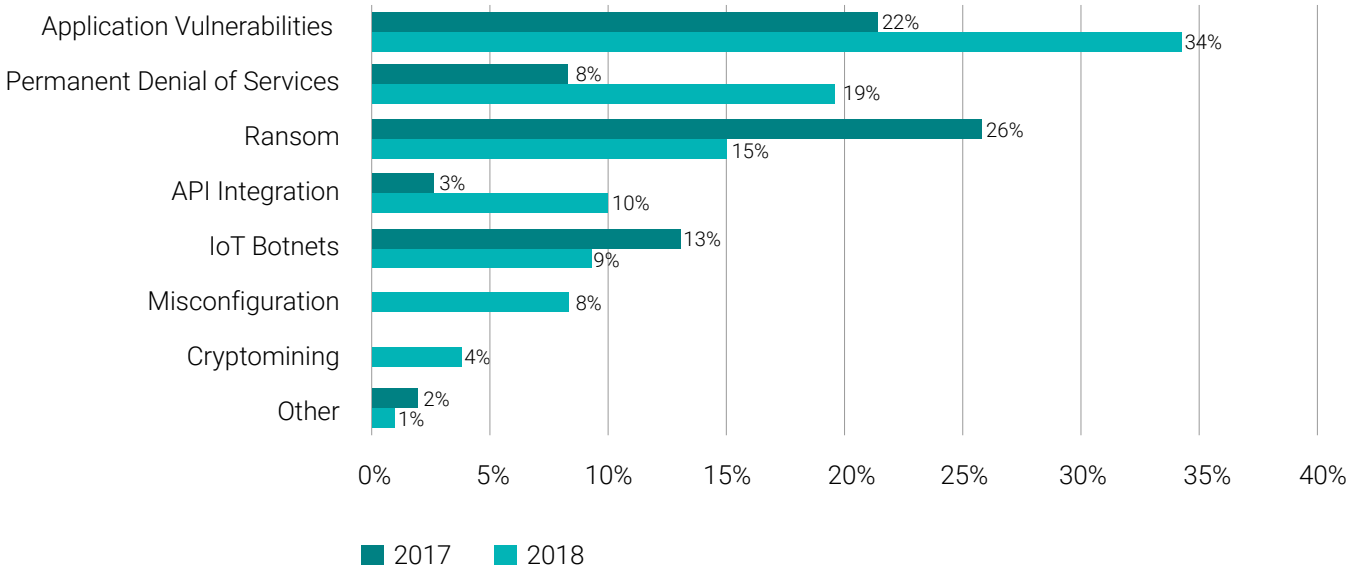

Figure 3. Perception of the biggest threats for 2019

Protecting Sensitive Data

Schools and universities process and store a large amount of personal information. According to the aforementioned report, data leakage is the top concern of education professionals when faced with a cyberattack, followed by service outages, reputation damage and revenue loss.

This is consistent with findings from a 2019 survey by the Consortium for School Networking and the Education Week Research Center of 300+ education leaders.[1] Sixty-eight percent of school district leaders believe that student-data privacy and security is a more important priority in 2019 compared to 2018, and over half of the school districts have formal password and security policies that are widely followed.

Educational institutions continue to move applications and data to the public cloud to transform infrastructure operations, improve the user experience and reduce costs, but they have less control and visibility to manage and secure these applications in cloud environments. Seventy-two percent rely on their public cloud provider to secure their cloud applications. One-third of respondents reported credential threats as the top cloud environment issue followed by web and application intrusion.

Top Security Threats to Cloud Environment for Education

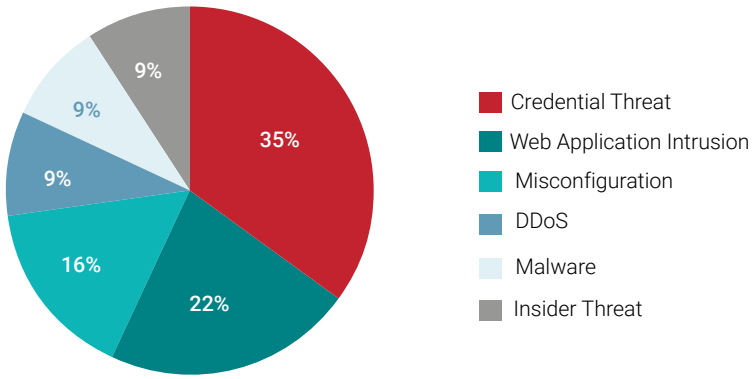

Figure 4. Top security threats to Education cloud environment

Schools and higher education institutions have to comply with evolving regulations and standards, such as PCI and General Data Protection Regulation (GDPR). Encryption protocols are required to secure student transactions, but attacks using encryption are also a concern, growing 13% in 2018 according to Radware's *2018–2019 Global Application and Network Security Report*.

Lack of Expertise and Resources to Handle Complex Threats

Although keeping websites, data and the network secure is critical, it is becoming increasingly difficult given the cybersecurity skills shortage and the increasing array of attack vectors. Based on Radware's *2018–2019 Global Application and Network Security Report*, 63% of security teams were exhausted after a 24-hour attack. According to Keith Krueger, chief executive officer of the Consortium for School Networking, if the largest school districts are scrambling to keep up, "one can only imagine the challenge for small school systems with no technical staff."

[1] https://www.edweek.org/ew/articles/technology/2019/03/20/rural-school-districts-lag-behind-in-cybersecurity.html

Industry respondents varied in their perceptions of cyberattack preparedness (see Figure 5). The education vertical consistently ranks itself lower than average for its confidence to mitigate all types of cyberattacks. Automation can help with the security response to continuously changing and complex multivector attacks.

	Vertical Markets							
Extremely/Very Well Prepared	Total	Financial Services	Service Providers/ Telco	Education	Government	Healthcare	Retail	High Tech
Malware & Bots (Worms, Viruses, Spam)	59%	63%	61%	53%	58%	55%	57%	65%
Distributed Denial of Service (DDoS)	53%	54%	63%	33%	52%	55%	61%	63%
Web Application Attacks (SQLi, XSS, Defacement)	49%	56%	50%	31%	47%	52%	43%	64%
Socially Engineered Threats (Phishing, Fraud)	49%	53%	50%	31%	44%	58%	57%	53%
Ransomware	48%	51%	50%	29%	50%	39%	57%	55%
Advanced Persistent Threat	41%	46%	46%	27%	38%	39%	35%	48%

Figure 5. Vertical markets preparedness to safeguard against specific cyberattacks

SOLUTION SUMMARY — WHAT YOU SHOULD CONSIDER

Educational institutions face many operational and security challenges. Radware has more than 20 years of experience leveraging cybersecurity research to provide solutions that solve business and technology challenges. Radware solutions have the industry's most expansive set of compliance certifications, including PCI, HIPAA, GDPR and advanced ISO regulations, to address data security in the cloud, including application and malware protection and encrypted traffic inspection.

For concerns with staying in business, Radware offers a behavioral-based attack mitigation service that combines on-premise detection and mitigation with cloud-based volumetric attack scrubbing, plus keyless SSL attack mitigation that defends against encrypted attacks without impacting legitimate traffic. Radware's application delivery controller (ADC) ensures availability and disaster recovery for local and globally dispersed applications while providing a scalable architecture and automation across multiple heterogeneous environments.

To protect sensitive data as well as mission-critical web applications and APIs, Radware's web application firewall (WAF) solution uses a positive security model and machine learning algorithms to provide adaptive defense against the OWASP Top 10 and other threats. Radware's WAF integrates with the hybrid attack mitigation solution and Radware's Bot Manager, which provides precise bot mitigation and management.

For security and control over assets in multiple public cloud environments, Radware's Cloud Workload Protection Service provides one solution to identify exposed assets and remove excessive permissions, detect misconfiguration issues and detect and defend against data breaches.

To assist with resources and expertise, Radware's attack mitigation and WAF solutions use machine learning, real-time signature creation and auto-policy generation to automate the attack protection life cycle to shorten time to mitigation by automatically mitigating attacks.

Radware's Emergency Response Team (ERT) offers a fully managed network and application security service 24x7, which includes immediate response, onboarding, consulting, remote management and reporting. The ERT offers threat intelligence subscriptions designed to provide actionable real-time data for immediate protection against active suspicious attacks and attackers.

CASE STUDY

This Midwest school system was experiencing DDoS attacks from students eight months out of its nine-month school year. It was losing federal education funding because it couldn't administer required testing. The school's one-person IT department was overwhelmed trying to handle these attacks, and its ISP provider could only *black hole* both good and bad traffic to stop the attacks.

The competition proposed a standard solution that didn't solve the school's problem: either always-on or on-demand DDoS protection.

Radware was chosen for offering an affordable, flexible solution of always-on cloud DDoS service for the school's critical eight-month testing period with on-demand protection for the remainder of the school year. The school solved its attack and budget problem and has been a positive reference for Radware's capabilities with other businesses and educational institutions.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.