TAG CYBER

USING BALBIX TO SECURE HIGHER EDUCATION FROM RANSOMWARE THREATS

DR. EDWARD AMOROSO, TAG CYBER
DR. GAURAV BANGA, BALBIX

Balbix®

TAG CYBER

USING BALBIX TO SECURE HIGHER EDUCATION FROM RANSOMWARE THREATS

DR. EDWARD AMOROSO
DR. GAURAV BANGA

Higher educational institutions are particularly prone to cybersecurity threats due to ransomware. We offer guidance for how schools can reduce the associated cyber risk using the commercial Balbix cybersecurity platform.

INTRODUCTION

The university campus network was once well-defined and secure behind a perimeter firewall. Like all organizational information technology (IT) infrastructure, however, this setup has shifted toward a virtual architecture, consistent with zero trust principles. Accordingly, university workloads have shifted from premise data centers to the cloud and software-as-a-service (SaaS).

A consistent backdrop that IT security teams at universities have always had to accept is the general culture of open access and free sharing so indicative of a learning environment. As such, it has never been easy for security teams to impose policies that restrict access—and this has remained true for modern zero trust-based university networks.

As a result, universities are now excellent targets for ransomware attacks, given the open nature of their infrastructure, their open culture of sharing and their surprisingly significant resources. Consider that universities manage endowments that can reach billions of dollars. Donors' personally identifiable information is high-value data that must be protected. Hackers and criminals view universities as great ransomware targets.

In this report, we explain how the university network has evolved and how this specifically makes them vulnerable to the types of attacks commonly found in ransomware campaigns. We then show how attack surface management from commercial security vendor Balbix offers an effective means to reduce this cyber risk.

HIGHER EDUCATION COMPUTING ENVIRONMENTS

The modern higher educational institution faces a series of cybersecurity challenges that combine conventional enterprise risk with the unique characteristics of higher learning environments. In particular, colleges and universities must find means to address cybersecurity problems such as the following:

- *Protecting Important Research* – Protecting research and results from adversarial eyes has grown in significance with increased nation-state-sponsored cyberthreats.
- *Managing Endowment Risk* – The size of many university endowments has increased the risk of ransomware demands from an adversary.
- *Balancing Privacy and Openness* – The challenge arises that student privacy must be balanced with the competing need to maintain an open sharing environment.

These risks are complemented by the full range of common enterprise cybersecurity challenges that face any organization of non-trivial size. Accordingly, larger colleges and universities will tend to be at higher risk, if only because the value of their targeted resources (e.g., endowments) is also high.

RANSOMWARE RISKS FOR HIGHER EDUCATION

A common attack strategy against universities involves the use of ransomware to make demands of the school's leadership. In March 2021, for example, the FBI issued a warning for U.S.-based higher education regarding the growing incidence of ransomware targeting the sector.

Universities, specifically, must contend with several challenges related to the growing ransomware risk. One issue they must deal is with sub-optimal budgets as few universities have established a culture and tradition of heavy cybersecurity spending. This creates a disadvantage for most higher education settings to implement the best controls.

In addition, reporting relationships for CISOs in higher education have been poorly defined. After a major breach incident at Penn State, for example, the university reevaluated the role of its CISO and decided to elevate the position, providing that role with greater responsibility and authority to take suitable security preventive or responsive action.

Perhaps the greatest challenge is that many universities have not been aggressive enough in deploying the best possible cybersecurity platforms to their infrastructure. Oftentimes, they have used free software, open-source tools or freemium versions of protection. This trend must shift in favor of the best available protection platforms.

HOW BALBIX CAN HELP HIGHER EDUCATION REDUCE RANSOMWARE RISK

The Balbix Security Cloud offers an excellent commercial option for higher education CISOs and their security teams to effectively reduce their risk, especially for the growing ransomware campaigns targeting colleges and universities. Balbix has great experience and expertise in this sector and understands the challenges facing higher education CISOs.

The Balbix Security Cloud supports cybersecurity posture automation with consequences expressed in a way that is actionable and that connects with CISOs and their teams. The solution was created to complement existing vulnerability management and related security posture capabilities used in the enterprise, while also addressing the major challenges and shortcomings that such functions have typically exhibited for most security teams. Some higher education teams will find that Balbix can replace their existing posture tools.

Automated Asset Discovery and Inventory

The first goal of the Balbix platform is to address the ongoing challenge of inaccurate and incomplete asset inventories, which is common in colleges and universities. Without having clarity around the specific devices, apps, endpoints and other resources in use across the campus network, as well as across the cloud and SaaS, it becomes impossible to have a complete measure of the security posture. This challenge is further driven by the consistent change that occurs for even those assets with an established inventory.

Balbix addresses this requirement through automated, continuous monitoring of the campus network posture, including traffic flows, to discover assets. The types of assets that emerge from this task include premise and cloud-based devices, applications, systems and services—including managed and unmanaged assets. Fixed and mobile systems, including internet of things (IoT) devices, are also included in the asset discovery capability.

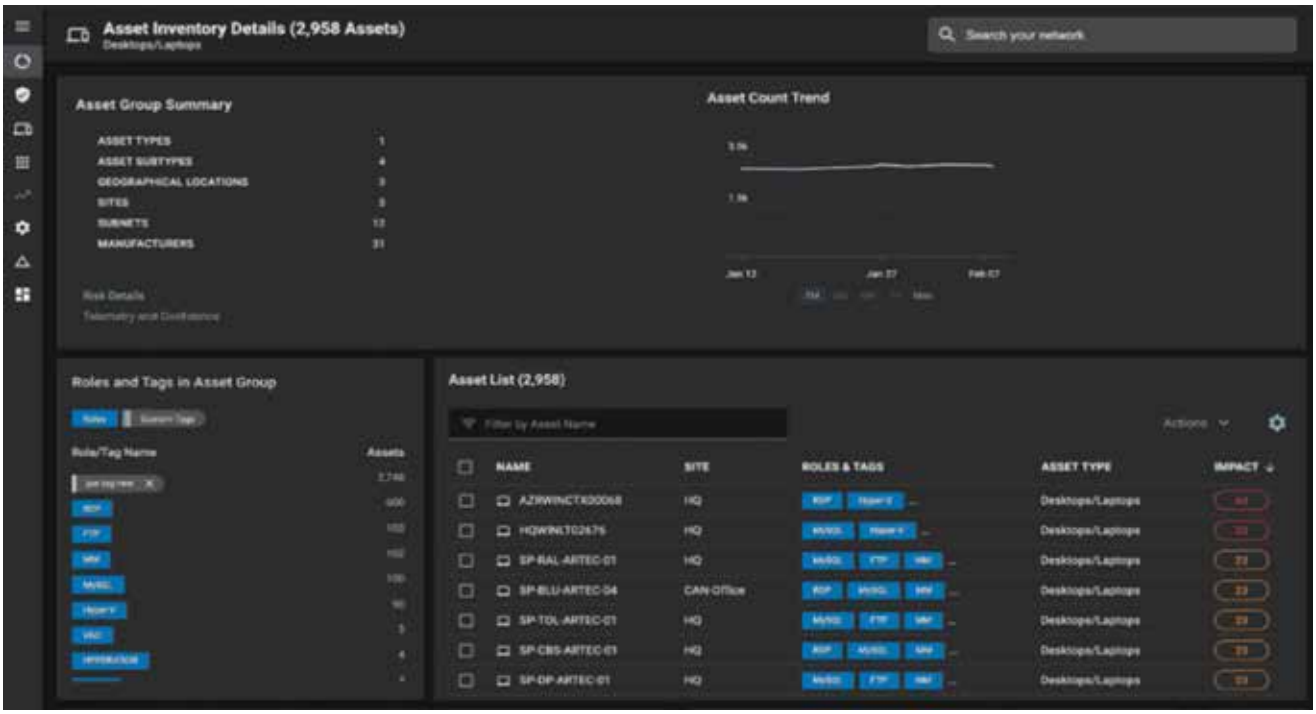

Figure 1. Balbix Platform. Discovered Asset Details.

The output data discovered in the Balbix platform, using its library of API-based connectors, includes identification of access to SaaS-based and on-premise tools and systems. Balbix performs the heavy lifting of unifying data from different tools, deduplicating, correlating and performing machine-learning-based inferencing. The solution takes advantage of scheduled exports for end-to-end automation, resulting in a near real-time analysis. It also presents risk quantifications (see below) in financial terms so higher education officials and staff can better understand the consequences of exposures.

Figure 2. Balbix Security Cloud. Risk Quantifications.

Continuous Cybersecurity Asset Management
Once a complete view of the security posture has been created for the entire attack surface, the obligation emerges to manage and maintain the asset inventory and associated context in a unified and maximally automated manner. The Balbix platform includes support for vulnerability and risk management workflows to ensure that assets are managed continuously to provide accurate security posture even as the attack surface evolves.

The collected data used to help categorize and manage assets based on their visible attributes includes IP addresses, DNS information, inventory data and other signals that can be used to identify entities. Balbix uses a technique called host enumeration logic (HEL) to normalize the accurate asset inventory view to support stateful, intelligent deduplication, sanitization and other data clean-up tasks.

Such tasks must be performed at all levels of the technology stack, each of which will provide a different type of asset-related information. Layer 7 analysis, for example, extracts application-level information about assets, whereas layer 3 and 4 analysis extracts information about packet headers and protocol behaviors. The goal is to combine this collection into a unified view of the discovered asset. The Balbix unified data model extends to 450+ attributes of assets. The data model includes coverage for laptops, traditional VMs and physical servers, IoT, network equipment and SaaS assets, plus cloud-hosted Kubernetes clusters, AWS S3 buckets, AWS EC2 instances, as well as their equivalents in GCP and Azure environments.

Risk-Based Vulnerability Management
A major problem reported by college and university security teams is the large volume of alerts collected by typical vulnerability management and scanning tools. It is common for the number of alerts to become so high that security teams cannot maintain proper risk categorization, handling and mitigation. This situation is ironic because the success of vulnerability management programs is often measured based on the number of alerts generated.

The Balbix platform handles volumes that result from vulnerability management processes by ingesting and analyzing data from a large number of security-, IT- and business-related data sources. These sources include vulnerability assessment tools, security scanning platforms, threat and vulnerability feeds, breach and attack simulation tools, SAST and DAST tools, penetration testing results, crowdsourced security test output, endpoint controls, CMDBs, ticketing systems, GRC tools and more.

Enterprise Vulnerability Prioritization
Prioritizing vulnerabilities requires attention to relevant factors, most of which will vary in intensity between academic environments. The Balbix approach involves establishing several major categories of factors so that higher education teams can organize the best mitigation strategies. Such mitigation can start with those vulnerabilities that can have the greatest negative impact on critical assets. The factors address vulnerability severity and threat level, as well as asset exposure, criticality and security controls.

Ultimately, the goal is to perform a continuous breach likelihood calculation, which is a computed summation of the individual attack vector computations. Such analysis is complemented by probabilistic graph models which estimate the vulnerability levels associated with the various risk scenarios. Collectively, these computations and values provide a college or university with an accurate understanding of their cybersecurity posture.

Cyber Risk Quantification
The goal of accurately establishing a quantitative measure of security posture for the organizational attack surface requires the use of a risk formula that makes sense to the local domain. To avoid multiple equations, formulas and other metrics, the Balbix platform defines a consistent cyber risk equation that can be used across all assets and over all aspects of the school to perform continuous cyber risk assessments.

The Balbix platform automates risk quantification. While this is certainly not a new strategy in enterprise cybersecurity, the specialized artificial intelligence models integrated into the platform support the calculation of risk trending, breach likelihood, breach impact scoring, breach likelihood by inventory and more. These are presented in a visual display that is easy to share with both IT security staff and higher education officials.

In addition, Balbix higher education customers benefit from the financial impacts that can be traced back to conditions of underlying assets and vulnerabilities for easy remediation. Expressing risk in business contexts has become a common approach for enterprise security teams hoping to illustrate the consequences of cyber risk to management and executive staff while supporting operational and strategic decision-making based on business risk.

Board-level Cyber Risk Visibility and Reporting
The final goal of the Balbix platform is to ensure that campus IT security teams have the best available tools for reporting and explaining vulnerability and risk posture to the organization. This must include reports for school officials, including trustees, as well as colleagues with a more detailed understanding of security programs. Such reporting must cover the entire attack surface and must account for ongoing change.

Most college and university officials will tend to focus on the reputational impact of potential breaches because this represents the most direct consequence of cyber risks such as ransomware. Balbix supports detailed impact modeling that uses estimates based on factors such as prior information, contextual impact modeling based on business tags, usage, volumes and interactions, and impact modeling based on inferences from prior and contextual data.

ENTERPRISE ACTION PLAN

It is recommended that higher education security teams and college or university officials act immediately to review, address and improve their cybersecurity posture assessment. This is best done using an automated platform that can unify existing posture-related tools such as scanning and security testing. As suggested above, the Balbix platform provides excellent support in this regard and should be included in source selection plans.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and nonclients alike—all from a former practitioner's perspective.