ellucian

WHITE PAPER SERIES

On the defense:

How higher education institutions can significantly reduce data breaches with the SANS 20

On the defense:

How higher education institutions can significantly reduce data breaches with the SANS 20

Introduction 3

Invest in prevention, not recovery 4

Developing an in-depth data defense strategy 5

Summary 8

About Ellucian 8

Introduction

No industry is immune to IT security breaches, including higher education institutions. In fact, data breaches at colleges and universities are increasing epidemically and currently account for 17 percent of all reported data breaches—making higher education second only to the medical industry.[1] Approximately one-third of colleges and universities have experienced more than one data breach. As a result, many institutions are conducting external data security audits not only to evaluate their vulnerability status, but also to significantly increase their data security controls.

In an effort to assist with the audit process, the System Administration, Networking, and Security (SANS) Institute, a trusted security resource committed to effective cyber defense, has developed a 20-point checklist of critical security controls. Considered the gold standard for implementing a comprehensive data security approach, this checklist provides guidelines for security controls, processes, and services, enabling institutions to identify and address gaps in accordance with industry best practices.

If the best defense is a good offense, the SANS Institute's 20 security controls have become proactive tools for assessing opportunities to hedge risks within your organisation and then leveraging technology to continually monitor and control those risks. This white paper details important measures you can take to improve institutional data security before a significant breach occurs by ensuring that systems are mapping back to the standards defined by the SANS Institute.

1. Privacy Rights Clearinghouse, Chronology of Data Breaches, Security Breaches 2005 to Present

Invest in prevention, not recovery

Most media information surrounding data security breaches emphasises the harmful consequences to individuals. However, less often publicised are the debilitating effects breaches can have on an entire organisation. The transparency of aggregated information between your institution's campuses, administrative departments, and online and mobile portals means the damages sustained by a seemingly isolated breach can become an enterprise-wide experience—a painful reminder of the cost of doing too little, too late.

Unfortunately, when an institution experiences a data security breach, the breach is typically large in scale. From possible fines, legal fees, and expenses associated with the responsibility of notifying all affected individuals, financial damages can be substantial. Moreover, your institution's good reputation is on the line and can be severely tarnished by a breach, resulting in shaky consumer confidence, lower enrollment numbers, and a possible decline in alumni contributions.

You can better defend against data attacks by first identifying susceptible areas within your institution. In keeping with the SANS Institute's 20 security controls, take the necessary steps to monitor systems and remove and reduce outdated or unauthorised access to protect against future breaches.

Developing an in-depth data defense strategy

The SANS Institute's 20 security controls derive from existing and emerging threats that have been identified as significant risks to networks and the information generated, transmitted, and stored on them.

And while all 20 security controls sanctioned by the SANS Institute are equally important, we have identified nine that can improve the protection capabilities of your institution's auditing and monitoring tools and contribute to an enhanced, enterprise-wide data security strategy.

Control 4: Continuous Vulnerability Assessment and Remediation

The management of potential data breaches is an ongoing effort. Today, systems must be able to perform continual, automated vulnerability assessments and management scanning to identify vulnerabilities and minimise opportunities for hackers.

Be sure your controls include a policy-based system with advanced reporting capabilities. This allows you to use audit and monitoring information as part of your vulnerability scanning exercises to better detect suspicious or unauthorised access and activity patterns. In addition, you can monitor privileged user activity and sensitive data access or changes. Equally important is to establish a policy by which all your audit and monitoring logs are stored in a data warehouse that is separate from your institution's database and application network.

Control 6: Application Software Security

Web-based and application software are highly susceptible to hackers. Ensure that communications between your databases are kept secure by proactively identifying, correcting, and preventing deficiencies.

Leverage the monitoring capabilities of your security controls to automatically patch and update systems with the latest releases and versions. This includes encryption capabilities to protect sensitive data that is not only present in your database but also transmitted over the network to application tiers and end users.

Control 8: Data Recovery Capability

When breaches occur, all systems can be compromised—including backup files and archives. Even after a data recovery, evidence of polluted data can remain. Processes must properly encrypt all critical information to ensure a rapid and safe recovery.

As part of your data recovery process, encrypt all backup files—regardless of where the files end up (e.g., on campus, in a remote location, or in cloud storage). Encryption implementation is a critical part of a well-integrated data security process, and your system should include all database files, export files, and redo/archive log files that are generated as part of your regular data backup.

Control 12: Controlled Use of Administrative Privileges

The credentials given to someone with higher or "root" administrative privileges are highly sought after by hackers. Ensure that all standard and administrative user accounts are properly managed with tools that can track, control, prevent, and correct the unauthorised use of administrative privileges on computers, networks, and applications.

Include in your data defense strategy privileged user and application entitlement alerts and reporting capabilities. Examples include privileged user access controls, role and class elevation, and unauthorised user access and activities. These types of monitoring capabilities can prevent direct access to administrative or privileged database and application accounts based on characteristics such as network location, application signature, and time stamping.

Control 13: Boundary Defense

Today's extranet connectivity is vast. Between mobile, vendors, and internal and external network connections, the extension of your institution's data is at risk. Block hackers before they discover your weak spots.

Look for data security systems that include application- and database-specific monitoring and blocking capabilities. It is becoming increasingly difficult to sufficiently segregate or fence the database network tier in part because of the many application and user integrations. By utilising location and IP-based monitoring options, you can significantly reduce the risk of database-specific threats and gain additional insight into the daily traffic and activity of your infrastructure.

Control 14: Maintenance, Monitoring, and Analysis of Audit Logs

Hackers are counting on you to not notice the damage they've caused until it's too late. A centralised auditing tool will allow you to offload, store, and examine all database audit logs separate from your database environment, helping you stay a step ahead of hackers and improve damage control efforts.

A web-based, administrative front end can help define audit policies and establish alerts and notifications, as well as give you the ability to generate, schedule, and deliver audit reports and properly define retention policies for all audit logs and activity. It also serves as a method by which to apply standards for integration with other infrastructure-wide Security Information and Event Management (SIEM) tools for incident and event detection, and to receive specific alerts and notifications as part of the data integration.

Control 15: Controlled Access Based on the Need to Know

Your most critical data assets are your "crown" jewels. Make it a practice to isolate them from the crowd by parsing out sensitive data from the more public information on your internal networks. When classified appropriately, your most critical information can easily be identified and properly transmitted over only the most secure of channels.

In addition to properly defining and implementing access control procedures, sensitive data classification levels, and a segmented architecture, you can use specific system defense tools to assist in the enforcement and detection of these implementations. Just as important, be certain your defense strategy incorporates data protection capabilities to protect against all malicious activity—including both internal and external threats.

Control 16: Account Monitoring and Control

Hackers infiltrate systems primarily via default or dormant privileged accounts and easy-to-crack or expired passwords. Actively manage the lifecycle of privileged user accounts for systems and applications to prevent a motivated hacker from easily launching an attack.

In evaluating the audit-reporting capabilities as part of your data security system, be sure it includes the ability to:

- Provide a list of all database and application accounts that do not have password aging enabled or do not meet secure password requirements
- Provide a list of all accounts that have not been utilised or accessed in a defined period of time
- Report on all failed login attempts based on a defined threshold
- Establish a privileged database role and security class changes (additions or revocations)
- Alert to any abnormal database and application access based on login time, total access time, and location

For enhanced monitoring capabilities, systems should include the ability to:

- Limit privileged account or entitled privilege access based on location and/or time
- Monitor direct database and application access, separate from the application tier, for suspicious or malicious access
- Generate alerts and notifications when access or changes to sensitive areas occur

Control 17: Data Protection

Minimise your risk by encrypting all your data. With so much information moving across your networks, it's not always clear when sensitive data might be exposed. Encryption adds a critical layer of protection even if your data is compromised.

Critical to a comprehensive data security process is the encryption of data at rest, at the physical file level, and in transmission over the network between databases, applications, and end users. This documentation should include best practices for the creation, management, and protection of the database encryption keys.

To view the complete list of the SANS Institute's 20 critical security controls, please go to **http://www.sans.org/critical-security-controls.**

Banner® Data Defense

Recent data breaches have institutions looking for a well-vetted resource to assist in the mitigation of potential problems surrounding data security. And while most recognise the SANS Institute's critical controls as the premier guide for establishing a comprehensive data security process, many lack the financial or human resources to effectively integrate even some of these best practice controls into existing and expanding systems.

For institutions that run on Banner® by Ellucian, Banner® Data Defense offers a reliable, cost-effective data security option. This solution aligns to the SANS Institute recommendations by providing an Oracle®-developed data and network encryption package, firewall, and audit tool to offer a comprehensive security strategy that protects sensitive information. Moreover, it's specifically tailored to Banner—built by Banner experts for Banner customers for total system alignment.

The cost of doing nothing (or too little) is high—far outweighing the cost of implementing improved data security controls when a breach occurs. Today, the technology exists to automate data security efforts to create a formidable defense against attacks. Where applicable, network processes should strive to mirror the SANS 20 controls, essential guidelines for evaluating, supporting, and creating a data security strategy that can closely tie into all of your network and database activities.

About Ellucian

Ellucian helps education institutions thrive in an open and dynamic world. We deliver a broad portfolio of technology solutions, developed in collaboration with a global education community, and provide strategic guidance to help education institutions of all kinds navigate change, achieve greater transparency, and drive efficiencies. More than 2,400 institutions in 40 countries around the world look to Ellucian for the ideas and insights that will move education forward, helping people everywhere discover their futures through learning.

To learn more, please visit **www.ellucian.com**.

ellucian

Headquarters: 4375 Fair Lakes Ct, Fairfax, Virginia 22033, USA
Phone: +1 800.223.7036

www.ellucian.com