How NIST Enables Higher Ed to Ace Cybersecurity Challenges

SailPoint

How to Ace Its Cybersecurity Requirements

It's not just a matter of continually providing students with timely access to information. Higher education institutions must ensure access to applications and files is appropriate at all times to avoid breaches and regulatory non-compliance fines.

What and Why NIST?

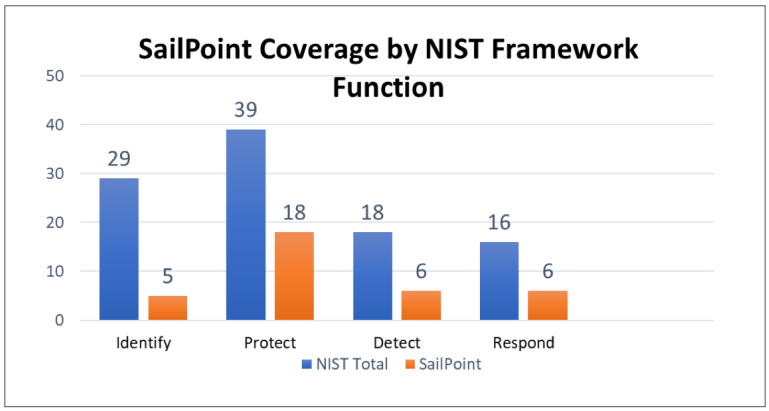
Recently hackers were able to access student data including grades, financial information and Social Security numbers through vulnerabilities in an enterprise resource planning system (ERP). The massive breach affected 62 colleges and universities. The ERP firm has published a patch that fixed the security flaw, but it serves as a reminder that security must be of utmost importance for higher education.

To mitigate such risk, the National Institute of Standards and Technology (NIST) has developed a cybersecurity and compliance framework consisting of standards, guidelines and best practices. NIST's approach is prioritized, flexible and cost-effective—thus ideal for higher education institutions.

Applying NIST in Higher Education

The NIST Cybersecurity Framework (CSF) is supported by various control frameworks such as ISO and NIST SP 800-171. As a whole, the CSF provides a list of things that all organizations, including higher education institutions, should be considering as part of security and compliance efforts. To reduce risk, NIST outlines a set of controls (referred to as 'subcategories' within its CSF) that institutions can consider deploying as part of a cybersecurity plan. Each control fits into five different recommended functions:

- **Identify** – Identify what needs to be managed
- **Protect** – Determining the appropriate controls to protect data
- **Detect** – Continuously monitoring and detecting anomalies, events and processes
- **Respond** – Establishing and continually improving response plans
- **Recover** – Ensuring resilience



Not all controls within each of the five functions apply to every institution. In fact, it's meant to be a pick list with some being more impactful than others depending on the use case requirements of the college or university. As such, higher education institutions can use identity governance to apply more than 35 controls across four of the five functions outlined by the NIST CSF.

Protecting Research Data in Schools

Institutions that are doing research (particularly government-based research) are required to develop 110 controls listed in NIST Special Publication (SP) 800-171. Some of these controls are required to make sure access is appropriate, managed and audited. In fact, detailed plans for workflow processes for control and access are required when applying or bidding on research grants/contracts. While some colleges and universities (particularly those with defense research funding in place) are already down the path of complying with NIST 800-171, many others are just beginning the process. For them, identity governance is critical to this journey.

Identity Governance Paves the Way for NIST Compliance

Some of the ways identity governance directly aligns with the NIST Framework[1] include:

- Access permissions and authorization are managed, incorporating the principles of least privilege access and separation of duties.
- Identities and credentials are issued, managed, verified, revoked and audited for authorized devices, users and processes.
- Personnel activity is monitored to detect potential cybersecurity events.

Furthermore, with the introduction of artificial intelligence and machine learning capabilities within an identity governance platform, institutions will see even greater alignment with core functions of the NIST Framework. Taking a predictive identity governance approach enables higher education institutions to leverage vast amounts of identity and event data. The advanced insights gathered through AI/ML reveals users and access that may pose risk. Moreover, colleges and universities can monitor the environment in real-time and anticipate how access and policies should change. This greatly enhances the ability to securely and efficiently control digital identities and their access rights to all applications and data, at all times.

[1] https://www.nist.gov/cyberframework

Key Takeaways

The NIST Framework requires more than one solution to meet all subcategories. In fact, a robust cybersecurity program effectively puts together multiple capabilities to gain maximum risk reduction across all areas. However, identity governance is a critical component for any organization trying to align with the NIST Framework. To learn more, **download the whitepaper.**

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.

EB1334-1909