Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Higher Education: Open and Secure?

Copyright SANS Institute
Author Retains Full Rights
An open, diverse environment is a standard requirement in higher education. Institutions include four-year colleges/universities, two-year community colleges and junior colleges, some of which are private and many of which are public. While their networks must be open to students, faculty and parents, higher education institutions must also protect their business assets from the same threats that affect the commercial and government sectors.

Unfortunately, under most circumstances, higher education institutions are strapped for resources to manage the balance between openness and security against malware and sensitive data exfiltration, according to nearly 300 higher education IT professionals who took a SANS survey conducted in February and March 2014. In the survey participants confirmed the historical difficulties of making their environments secure while also providing the openness institutions need for their students, staff, parents and benefactors. As one write-in response stated, "University culture often conflicts heavily with the need for robust security: Adjusting the culture would allow more emphasis on security controls."

Changing institutional culture is only part of the problem respondents face in getting the resources needed to secure their environments while meeting needs for openness. They also face the challenges of securing the buy-in of upper management, skills shortages and difficulties meeting multiple requirements for the safety of the personally identifiable information (PII) hosted and processed on their networks.

These and other results are discussed in further detail in the following pages, along with advice on how organizations can improve their risk posture while working within their institutional limitations.

**Key Findings**

- **Lacking risk assessment policies.** Only 45% of organizations represented in the survey have formal risk assessment and remediation policies in place, and the situation is worse in institutions with fewer than 2,000 employees, where only 31% have such policies.

- **Sensitive systems of concern.** The biggest concerns are administrative systems (selected by 70% of respondents in our multiple-choice question). Faculty and staff computers, tied with web applications, were the second biggest concerns (selected by 64% of respondents), and faculty and staff mobile devices (selected by 60% of respondents) were the third area of concern.

- **Sensitive data at risk.** Personally identifiable information (PII) receives special attention, with 76% having institutional policies restricting access to PII and 71% avoiding storage of PII.

- **Encryption lacking.** Much PII is not encrypted. Only 54% encrypt PII in transit, while just 48% encrypt PII at rest.

- **Unclassified and unmanaged data.** Only 57% classify their sensitive data and provide guidelines, and even fewer (55%) define appropriate owner, user and administrative roles.

- **Understaffed and under budget.** While 64% believe they need 1–5 full-time equivalents (FTEs) of additional staff, 43% believe they cannot pay premium rates for premium skills. Lack of budget, selected by 73% of respondents, is deemed a cause of not being able to maintain or increase IT staffing.
Most survey respondents are actively involved in the provisioning, management or oversight of cybersecurity information, data privacy or compliance programs at higher education institutions. In the survey 48% of the respondents work for public universities, 19% work at private universities, 10% work at private colleges and 7% work at two-year public/community college institutions. The remaining participants work at military academies, online-only colleges or universities, or public colleges, as shown in Figure 1.

![Figure 1. Type of Higher Education Organization](image)

Although the majority of respondents (87%) work at institutions located in the United States, the survey did attract some international response. Five percent work at European institutions, 3% work in Canadian institutions and the remaining 5% work at institutions in New Zealand, the Middle East, Latin America or other areas. Still, results are based predominately on US institutions.
Security Job Roles

The survey participants were primarily security administrators or security analysts (31%), followed by senior-level management professionals (security managers/security directors/CSO/CISO combined made up 24% of respondents), network operations/system administration (14%), IT manager/IT director/CIO (10%) and other IT roles (developers, compliance officers, hardware experts, ops managers and so on made up 9%). Educators (professors, teachers and departmental staff) make up an additional 9% of the sample, as illustrated in Figure 2.

Respondents represent a good blend of security management and technical security roles, suggesting that the institutions represented are devoting human resources at the upper management level as well as at technical levels and that our survey base provides a good perspective on security in higher education.
Mostly Large Organizations

The survey determined size of the institution by the size of the workforce, including faculty, staff and consultants. The largest percentage of respondents (19%) reported having between 2,000 and 5,000 employees, and 17% reported having over 15,000 members in their workforce. Another 14% reported having up to 500 total workforce members (see Figure 3).

The size of the workforce is important because it may point to the robustness of the security program for that institution. The larger institutions store more data in more places, which could result in larger overall exposure. Those institutions likely have more individuals to devote to security tasks.

How many people work at your institution, either as employees, contractors or consultants?

The larger institutions store more data in more places, which could result in larger overall exposure. Those institutions likely have more individuals to devote to security tasks.
Higher educational institutions typically have three main business functions that distinguish their network security requirements: administrative, academic/instructional and research functions. These functions usually run over separate networks with different IT security requirements. For example:

- The administrative business function supports the business of running the institution.
- The academic/instructional business function supports the educational component and houses student records that may contain sensitive information.
- The research business function typically generates large amounts of income to support the university, making the research data valuable to attacks seeking intellectual property.

**What Keeps Them Up at Night**

Historically, academic networks have worked under the assumption that students and faculty, using their own devices or IT-managed devices, are accessing their records, course materials, assignments and more. As such, higher education institutions are early adopters of BYOD (bring your own device) and have become models of managing the risk around these devices.

Most institutions today require their students to purchase their own computers and are challenged to create a network infrastructure that can support multiple personally owned devices. Not only are they dealing with multiple student-owned devices connecting into the network (tablets, smartphones, laptops), but faculty and other staff members are also using personal devices. All of those devices present a sizeable challenge when added together. For example, a population of 46,000 individuals on the network each having five devices (some personal, some institution issued) creates 230,000 potential breach points, each of which could be a point of compromise.

In our survey faculty-used mobile devices and faculty computers were among the top concerns in our survey—but not the top concern. In a multiple-choice question, 70% of respondents were most concerned about administrative systems that handle student and financial records, while 64% were concerned with faculty and staff computers, both laptops and desktops. As one respondent wrote in response to another question, “… We frequently don’t know about faculty/staff connecting BYOD devices to sources of sensitive information until after they have done it, when they cry for help.”
Respondents are equally concerned with their web applications that deal with student financial records, with 64% also selecting that choice. And 60% are concerned about faculty or staff use of mobile devices. Far fewer (less than 30%) are concerned with student-owned devices, indicating confidence in their student networking technologies; or it could mean respondents have some naiveté about their vulnerabilities. See Figure 4 for a complete breakdown of the systems institutions are concerned about.
The lesser concern over student-owned devices makes sense. Faculty and staff handle large amounts of sensitive data (for example, student records, health benefits, and financial and research information), whereas students typically handle only their own or family PII, and on occasion PII of fellow classmates. It was specifically the exposure of this type of protected data that landed Iowa State University in hot water in April 2014, when it was discovered that nearly 30,000 records for enrollees between 1995 and 2012 were exposed on five departmental servers.\(^1\) While the servers were taken over by attackers wanting the computing power to create BitCoins, the fact remains that privacy-protected data subject to regulatory compliance was inadvertently exposed on those servers.

An interesting finding was that 26% of respondents are concerned about “things” that aren’t traditionally thought of as computers—devices such as printers, copiers, scanners, laboratory data acquisition devices, surveillance cameras, door access controllers, vending machines and HVAC systems. Attacks have been documented involving these types of “things” connected to university networks. For example, networked printers have been documented as being vulnerable to breaches that can result in data exfiltration.\(^2\) It’s encouraging to see the level of awareness—with 26% of respondents reporting that they were concerned about the security of such “things;” however, that number should be higher given the amount of interconnected devices that they are probably hosting in their enterprises.

**What Needs Protection**

As you can see from the previous results, respondents are more concerned with their internal, PII-heavy storage systems than their endpoints, and particularly less worried about those endpoints on their student academic networks. This is also reflected in what systems they feel require protection. In order, respondents say they are most concerned with protecting against:

1. Exploits against internal database systems and servers
2. Malware delivered to staff endpoints via a variety of vectors
3. Exploits against websites or servers
4. Phishing attacks

---

1. [www.news.iastate.edu/news/2014/04/22/serverbreach](http://www.news.iastate.edu/news/2014/04/22/serverbreach); This breach made the “top breaches in April” list for SCMagazine.
Looking at their answers as a whole, respondents indicate endpoints are strategically important to their protection programs. Malware can be delivered to endpoints via web drive-bys, phishing attacks and software vulnerabilities. Results also show that exploits via student-owned applications don’t raise the same protection concerns as employee devices, as shown in Figure 5.

**What are the primary attack vectors you are most concerned with protecting against?**

![Figure 5. Attack Vectors Most in Need of Protecting](image)

Of the 11 attack vectors listed in our survey, six are related to the capability of the institution to patch its internal systems’ external-facing applications: exploits against internal database systems and servers, malware delivered to staff endpoints, exploits against websites or servers, exploits against other critical applications, DNS server exploits and malware delivered to student endpoints. As a result, patching and vulnerability management are critical to protecting against these types of risks. The other five vectors not deemed by respondents as critical for protecting are initiated by the user and could be addressed with a security awareness program and policies for supporting, allowing or denying specific forms of student traffic.
How They Prioritize

Respondents use a variety of factors in establishing their incident response and mitigation priorities. Not surprisingly, asset criticality ranked highest, followed by business impact and the severity of the threat, as these three factors are closely linked, as shown in Figure 6.

What are the primary attack vectors you are most concerned with protecting against?

Assets can range from business processes to IT services used by those business processes, to software components that comprise the IT services, to hardware needed to run the software components, to the staff needed to make the whole thing work.

Security personnel should complete an asset prioritization at each appropriate level, ultimately identifying the most critical business process and associated data. Sensitive data, as defined by law or regulation, should certainly be classified at a higher level than publicly available data. Data classification policies and standards are key components to defining institutionally sensitive data.

The criticality of an asset together with the severity of a threat or threat families targeting this type of asset are key aspects that affect how vulnerabilities are treated in the traditional risk equation (risk = threat x vulnerability). A student endpoint may not be as much of a priority because it is not accessing sensitive databases with other information of use to attackers. So, the student endpoint’s ranking may be lower than, say, an internal database hosting sensitive data (for example, student, alumni or faculty PII), whose assets should be ranked as more important to protect (through vulnerability management and patching).
When comparing Figure 6 with Figure 7, impact on business appears to go hand-in-hand with the criticality of the asset.

![Image of a bar chart showing the prioritization of asset criticality and other factors.]

**How do you prioritize incident response and mitigation? Select the top three that apply.**

In the figure a rating of 1 indicates it was the top priority for a respondent. A rating of 2 indicates a second priority, and 3 indicates the third priority. What you see in the figure is a compilation average of each answer. By averaging, we can see that survey respondents were most concerned about asset criticality and less concerned with threat isolation.

Should a critical asset be compromised and data exposed, the impact takes away resources (time and money) from the business to apply to managing the auditors, press and impacted individuals involved in the incident. Such expenses can be daunting, costing the average reporting organization $3.5 million in US dollars—a 15% rise over that cost last year, according to Ponemon's latest Cost of a Data Breach report.\(^3\) As a very small example of one cost involved, say you needed to provide a year’s worth of free credit monitoring services for 10,000 people. At $15 per person, that's $150,000 just for that service.

---

Assessing Risk

Because assessing asset criticality and business impact are so important, it is surprising that only 45% of respondents have a formal assessment and remediation policy in place. Even more concerning, 37% report that they have no formal policy and 18% don’t know if they have such a policy, leaving 55% without a formal policy for assessing and remediating risks through staff and technology resources (see Figure 8).

The survey responses also indicate that smaller institutions with 2,000 or fewer employees (that make up 44% of our sample) generally report that they do not have a formal risk assessment and remediation policy. In our survey 69% of organizations of 2,000 employees or fewer do not have such a policy or are unaware of one.

Of those with more than 2,000 employees, 56% report that they have such a policy. While this represents a higher percentage compared to smaller organizations, this number is still low—another 44% don’t have policies.
As they develop and improve their risk management programs, IT directors should keep an eye toward processes and technologies that can reduce the administration of overlapping mandates and simplify reporting.

Risk to assets and asset criticality are also driven by regulations governing PII. According to the survey results, institutions must follow a variety of regulations and federal laws, including the Family Educational Rights and Privacy Act (FERPA), which deals with the protection of student records and was selected by 75% of respondents. PCI DSS was the second most required regulation, with 71% selecting this option, which indicates that their payment systems are critically interlinked with their PII assets. Not far behind, 69% selected HIPAA/HITECH, which could represent medical schools, student health centers and/or employee insurance data (see Figure 9).

What privacy-related regulations must your organization adhere to for the personally identifiable information (PII) it manages? Select all that apply.

[Figure 9. Key Privacy-Related Regulations]

The fourth item, selected by 62% of respondents, is the state data breach notification laws.

This range of compliance regulations strains the resources of institutions already constrained by budget, resources and staff. As they develop and improve their risk management programs, IT directors should keep an eye toward processes and technologies that can reduce the administration of overlapping mandates and simplify reporting.
PCI DSS is the one standard that is “forcing” network segmentation in the case of credit card payment devices, such as dining hall cash registers, bookstore credit card payment systems, university-based hotel/conference centers, vending machines or web-based payment systems (tuition payment, athletic ticket office or alumni donation websites). It is a challenge to comply with PCI DSS, and many institutions try to run such money collection systems over separate secure networks.

The “Other” responses were mostly attributed to the 6% overall of international respondents, who indicate they have their own compliance issues, just as US institutions do. Their write-in responses provide a good list of the privacy laws in their countries, including the European Union (EU) Safe Harbor framework, the EU data protection directives and the Freedom of Information and Protection of Privacy Act in Canada. They also pointed to the emphasis on encryption requirements in their respective countries.

**Strategies for Managing Risk**

According to our survey, respondents use a variety of techniques to protect PII: Roughly 76% of respondents have institutional policies that restrict PII access, while 71% avoid storage of such information. The next two most widely used policies are classifying data and providing guidelines (57%) and defining the data owner, user and administrative roles (55%). Figure 10 illustrates the various policies at respondent institutions.

**Examples of PII**

There may be some slight variations in definition between states, dependent on the state data breach notification law definitions, but PII generally includes the following:

- Social Security numbers (SSN)
- Credit card numbers (CCN)
- Driver’s license numbers (DMV)
- Passport numbers or bank/debit account numbers

**What do your current policies around the protection of your organization’s PII include? Select all that apply.**

![Figure 10. Current Policies to Protect PII](image)
In most cases (38%), the IT security officer was directly responsible for managing the risk assessment program, followed by the CIO (23%).

**Budgetary Impact on Strategy**

When we look at the budget situation of the participants, we can conclude that implementing an effective PII data protection strategy is challenging. Inadequate budgets for tools and staff can create a significant gap in an institution’s PII defense capabilities.

Most respondents (45%) didn’t know what percentage of their IT budget is spent on security, which is not surprising, given that only 34% of respondents are at the management level. However, 37% of respondents reported their institution spends between 1–6% of their overall IT budget on IT security, in line with the results of other SANS surveys. See Figure 11 for a detailed look at how much of the IT budget institutions earmark for security.

The results may be a bit deceptive because, at many institutions, the IT security budgets are not limited to the IT Security Office budget. For example, equipment may be funded by the CIO’s administration budget, resulting in the IT security dollars being spread across a number of IT “budgets” within a department or college.
Budget-related issues are vital to the security efforts in academic institutions. Smaller IT security budgets can negatively impact the capability of an institution to justify acquiring commercial IT security hardware and software, which comes with long-term expenses related to maintenance, licensing and renewal. Instead, many may opt for freeware or open source products, which present new risks and maintenance overhead (requiring specialized skills) that a commercial vendor might have covered in its contracts.

**Staffing**

Staffing and employee retention is problematic because most higher education institutions can’t match industry salaries for experienced IT security analysts and cannot compete with industry for experienced security analysts.

Survey respondents report a wide range of staffing situations, the majority (54%) stating they have between one and five IT security-focused FTE staff members, with 18% maintaining staffs between 6 and 10 FTEs. Another 8% (presumably very small institutions) report having no dedicated security staff, another 8% report less than one FTE, and 4% (presumably very large organizations) have 21–50 FTEs. Just 2% reported more than 50 FTEs devoted to security, as illustrated in Figure 12.

It would be interesting to investigate how some of the institutions managed to get that many FTEs dedicated to IT security. For example, are the 21–50 FTEs part of the central IT organization or are they distributed across the departments? Such questions, though, are outside of the scope of this survey.
It does, however, make sense that smaller institutions don’t have large security staffs and vice versa, which is born out when we correlated size of organization against number of IT staff, as shown in Table 1.

<table>
<thead>
<tr>
<th>Number of FTEs</th>
<th>Fewer than 100</th>
<th>101-500</th>
<th>501-1,000</th>
<th>1,001-2,000</th>
<th>2,001-5,000</th>
<th>5,001-10,000</th>
<th>10,001-15,000</th>
<th>More than 15,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>1%</td>
<td>3%</td>
<td>2%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>&lt;1</td>
<td>0%</td>
<td>3%</td>
<td>4%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>1-2</td>
<td>1%</td>
<td>1%</td>
<td>7%</td>
<td>8%</td>
<td>7%</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>3-5</td>
<td>1%</td>
<td>1%</td>
<td>3%</td>
<td>4%</td>
<td>5%</td>
<td>6%</td>
<td>3%</td>
<td>4%</td>
</tr>
<tr>
<td>6-10</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
<td>1%</td>
<td>4%</td>
<td>5%</td>
<td>3%</td>
<td>4%</td>
</tr>
<tr>
<td>11-20</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
<td>1%</td>
<td>4%</td>
</tr>
<tr>
<td>21-50</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>3%</td>
</tr>
<tr>
<td>51-100</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>&gt;100</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

In the smaller institutions, the norm is usually one person responsible for multiple roles in IT, with security being just one of those roles. Small IT departments have to trade off the tasks of completing security tasks to ensuring the infrastructure works. These actually both work together, so these resources may not be as stretched as they seem.

**Security Teams Understaffed**

However, most respondents feel that their staffing numbers fall short of their needs. The majority of respondents (64%) believe their institution should increase its IT security staff size by 1–5 FTEs, as shown in Figure 13.
Budget Impact

As suspected, budget is the dominant factor for not hiring more employees. In our survey 73% of respondents cite lack of budget as their inhibitors in maintaining or increasing the IT security staff. More importantly, 43% reported not being able to compete for skilled IT security workers—most likely against higher paying organizations (see Figure 14).

What is the reason your organization is short on staff and/or resources? Select all that apply.

![Figure 14. Reasons for Staffing Shortfalls](image-url)
Losing the competitive edge plays out in many forms. It’s hard to keep qualified employees with current certifications when private companies offer two to three times the salary they were receiving at the university. A lack of budget prevents the institution from making any type of meaningful counteroffer. Thus, higher education institutions, particularly public institutions, find themselves in the cycle of hiring inexperienced analysts, training them and then losing them to higher paying jobs.

It can also be said that lack of funds breeds creativity. Even without the resources of their other industry counterparts, IT security personnel in higher education have pioneered the notion of supporting anytime, anywhere computing for students. And, based on their write-in comments, they are also creatively using and building technologies to support their scarce resources. As one respondent wrote, “We’ve built incident mgmt (sic) tools to help us remain efficient.”
When it comes to protections, institutions of higher education are using a variety of tactics and technologies, starting with network segmentation and following up—to some degree, but not enough—with data protections such as encryption.

**Network Segmentation**

As leaders in supporting BYOD, particularly for student networks, higher education institutions use network segmentation as a common practice for both security and performance reasons. At the same time, federal regulations such as HIPAA and PCI DSS are forcing institutions to segment or outsource health or credit card services, which are both strong risk areas for any organization.

Of those respondents whose institutions segregated their networks to protect specific systems from external attack, 73% segment their administrative network from the rest of the university network, as shown in Figure 15.

![Figure 15. Variations of Network Segmentation in Higher Education](image)

Somewhat fewer (43%) segment the student dormitory/recreation center network from the university network. PCI DSS requirements are forcing institutions to investigate segmenting the business functions of their institutions that deal with credit card payments, such as dining facilities, recreational facilities, tuition payment and athletics payments facilities.
Technologies They Use

To segment networks, respondents still rely primarily on firewalls, with 84% reporting that they are satisfied or very satisfied with this technology area.

They are also using IDS/IPS closely followed by endpoint security for employees and email protection, yet satisfaction rates for these technologies are quite a bit lower, as shown in Table 2.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Very Satisfied or Satisfied</th>
<th>Disappointed</th>
<th>Not Using</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls</td>
<td>84%</td>
<td>11%</td>
<td>2%</td>
</tr>
<tr>
<td>IDS/IPS</td>
<td>68%</td>
<td>13%</td>
<td>10%</td>
</tr>
<tr>
<td>Endpoint security for employees</td>
<td>65%</td>
<td>21%</td>
<td>7%</td>
</tr>
<tr>
<td>Email protections</td>
<td>63%</td>
<td>18%</td>
<td>14%</td>
</tr>
<tr>
<td>All-in-one edge security appliance</td>
<td>58%</td>
<td>9%</td>
<td>25%</td>
</tr>
<tr>
<td>Encryption</td>
<td>56%</td>
<td>14%</td>
<td>21%</td>
</tr>
<tr>
<td>Endpoint security for students</td>
<td>44%</td>
<td>15%</td>
<td>32%</td>
</tr>
<tr>
<td>Continuous monitoring</td>
<td>44%</td>
<td>11%</td>
<td>32%</td>
</tr>
<tr>
<td>NAC/Other access controls</td>
<td>39%</td>
<td>17%</td>
<td>32%</td>
</tr>
<tr>
<td>SIEM for incident response</td>
<td>34%</td>
<td>16%</td>
<td>39%</td>
</tr>
<tr>
<td>Analytics and intelligence for incident response</td>
<td>30%</td>
<td>13%</td>
<td>43%</td>
</tr>
<tr>
<td>DLP</td>
<td>26%</td>
<td>11%</td>
<td>50%</td>
</tr>
</tbody>
</table>

The 18% disappointed rating with email protections is interesting, because protections are very dependent on the email technologies used by the institution. Many institutions previously used homegrown email systems, but have now migrated to cloud-based email solutions, such as Gmail or Microsoft Live. These cloud services tend to include their own email protections, although one downside of this is that the institution is subject to the whim of the email provider when it comes to the provider changing/updating its spam filters. For example, a number of institutions went “email dark” when Google changed its filters and didn’t notify its customers.
Looking for Something New

Only 56% of respondents are satisfied or very satisfied with current encryption technology, even though encryption is a mainstay security control that is required by regulations and policies. This could be one underlying factor as to why only 54% encrypt PII, which we discussed earlier in this paper. Finding an encryption solution that works in the three major OS platforms (Windows, Mac OS and UNIX/Linux) within the institution can be expensive. Most commercial encryption solutions charge per-seat fees, which can result in expenditures of hundreds of thousands of dollars.

The same encryption solution must work at the peer-to-peer level. Suppose someone at institution A is sending information to a colleague at institution B in an encrypted file. Both institutions must support the same encryption scheme, and so, encryption key management between institutions is a critical requirement that is difficult to manage.

In addition, the same encryption requirements extend to state and federal government reporting agencies that require the institutions to send them reports.

Network access controls (NAC) are traditionally a primary means to segment network traffic into safe zones while providing a way to track who is on the network. From our responses, 68% are using NAC, yet only 39% are pleased with their results. It appears respondents are relying more on and are happier with networking technology like firewalls (98% use; 84% satisfaction) to segment their traffic. This is likely because NAC tools tend to be expensive and difficult to deploy in large networks.

On Their Wish Lists

Although they may not be investing in security information and event management (SIEM), analytics, NAC and identity management controls now, such technologies are on respondents’ radars or wish lists as potential future investments. When asked what it is they’d like to invest in over the next 24 months, respondents selected SIEM, NAC-type controls, identity management, better logging and visibility across the organization, and endpoint and mobile device management—along with more buy-in from management, support for staffing and technologies, and resources to remediate findings of their security scanning.
In fact, more support from management, more staff and more resources appeared most frequently in the 118 open-ended responses provided. The most common items in the security wish list include the following, in no particular order:

- Increased IT security budget
- SIEM products
- Management support/cultural buy-in to security as part of the business process
- IDS/IPS products
- Monitoring/analytics capabilities
- Budget
- Increased staff
- Increased role-based training
  - Security awareness training
  - Technical training for IT staff
  - InfoSec primer training for upper management
  - Training for better monitoring and analysis capabilities
- Upper management support for IT Security initiatives
- Increased system and network log collection

Many included multiple requests per write-in answer, much of which points back to lack of resources and more support from top management and the environmental culture. As one respondent listed, he could use more “Awareness of staff. More buy-in from both exec-level and IT to abide by InfoSec’s policies and recommendations.”
Focus on the Data

As higher education institutions increase their network size, speed and access, providing adequate security monitoring and protections becomes more important in guarding the key asset of any institution—its data. Based on survey responses, higher education institutions need to address the following items:

- **Classify data.** Data classification defines the sensitivity of institutional data. In our survey 57% of respondents have data classification policies in place, and 76% have PII policies governing access. This seems to be backwards because PII policies should be a subset of the overall data classification policies.

- **Encrypt data.** Only 53% of respondents segment the networks in which PII is processed. And encryption is used sparingly for PII at rest (48%) and in transit (54%). These statistics must change if we are to protect our data.

- **Assess risk.** Only 45% of respondents said they have such policies. Risk assessment is a crucial step in the overall institutional security policy, enabling the institution to define critical assets. It also facilitates compliance with the various regulations and laws governing data access and dissemination.

- **Deploy data analytics for incident response.** Technologies such as SIEM, data loss prevention (DLP) and NAC can enable institutions to determine the extent of attacks against their critical assets and provide the necessary metrics for upper management.

- **Incrementally increase IT security budgets.** Increases in budget are likely required. Security management personnel can use the data collected while completing data classification, encryption, segmentation, risk assessment and data analytics to justify increases.
Despite their challenges, higher education institutions seem to be mostly successful at preventing attacks from infiltrating their environments. In our survey 67% of respondents indicated they had no successful breaches in the past 12 months that involved loss of sensitive information, research or institutional or system information such as passwords—at least none that they were aware of. This could mean that the respondents’ institutions had highly successful security policies in place, or it could mean that they were unable to identify the breach—which, given their lack of monitoring technologies like NAC (for endpoint visibility and access controls) and SIEM, makes some sense. Another 16% said they’ve had one successful breach, while another 14% have experienced two to five such breaches. The remaining respondents had six or more breaches.

Based on their wish lists, it is evident that IT security staff are all too aware of the shortcomings they face in terms of budget, staff and technologies to use in the battle against an increasingly advanced cyber enemy. These IT pros are achieving a great deal with a minimal budget and a culture that values openness over security. Survey respondents demonstrated a genuine effort and desire to focus on assurance (given the budget, staff and time) rather than mere compliance—which unfortunately does not always lead to a more secure environment.

To catch up with their more well-funded peers, these organizations need low-cost, easy-to-administer investments that will meet their needs for better visibility, data protections, and identity and access controls. Continued improvement in people, processes and technologies will be required of higher education institutions as threats and budgets continue to challenge them.
Randy Marchany is the chief information security officer of Virginia Tech University and the director of Virginia Tech’s IT Security Laboratory. He is a coauthor of the original SANS Top 10 Internet Threats, the SANS Top 20 Internet Threats, the SANS Consensus Roadmap for Defeating DDoS Attacks and the SANS Incident Response: Step-by-Step guides. Randy is currently a certified instructor for the SANS Institute. He is a member of the Center for Internet Security development team that produced and tested the CIS Solaris, HPUX, AIX, Linux and Windows2000/XP security benchmarks and scoring tools. He was a member of the White House Partnership for Critical Infrastructure Security working group that developed a Consensus Roadmap for responding to the DDoS attacks of 2000.

SANS would like to thank its sponsors:

ALIEN VAULT

tenable
network security

TREND MICRO
Securing Your Journey to the Cloud
### Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>OnlineTXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>