Defending Networks at Higher Learning Institutions—Heroes Needed

An International Survey of Network Professional and Users
Introduction

A total of 678 international participants from higher learning institutions completed a survey on campus network and security. Participants included students, faculty and staff as well as IT professionals with networking responsibilities. The survey was administered in the United States, United Kingdom and Germany, primarily focusing on the network environment, security and threats specifically occurring at higher education institutions.

Executive Summary

This research finds that higher education campus networks are unlike any other enterprise class network. Their average user has 4 or more devices connected to the network, and more than one quarter of those devices are already infected with a virus or malware before they gain access to the network. In addition, each year twenty-five percent or more of their users change, generating massive churn. It is no surprise that 8 out 10 higher education IT professionals say securing their network is harder now than ever before.

Most IT professionals stated the greatest threats to their security actually come from within their own campus, and 1 in 3 students know of fellow students performing malicious acts. These professionals also share that most users are not taking reasonable security measures to protect their own sensitive data, failing to adopt new security measures and trusting questionable networks.

Vast numbers of users with a tremendous variety of devices wielded by uneducated users pose a huge set of challenges. Yet this research also finds that less than half of higher education institutions have a comprehensive networking solution to help manage their networks and secure the information that flows through for both the students and the institution.

Key Findings

Uncontrollable Network

- 81% of IT professionals state securing campus networks is becoming more challenging
- 89% indicate substantial increase in number of connected devices

The Enemy Within

- 25% or more of personal devices are already infected, said most IT professionals
- 59% of IT pros indicate the greatest security risk is within the campus
- 1 in 3 students know of other students performing malicious acts
- Only 61% of IT pros think users take sufficient steps to protect their sensitive data

Defending the Network with Pitchforks

- IT professionals reveal 48% of campuses lack comprehensive network management capabilities

Detailed Findings

Securing Campus’ Networks is Growing More Difficult

This research sought to determine the state of the network at higher learning institutions, where IT pros must manage and protect the network with thousands of users and, in larger universities, tens of thousands of users. The bottom line is 81% of IT professionals at those institutions state securing the network is more challenging than ever. The findings in this report identify the technical challenges and user habits that make securing these networks so daunting.
Device Proliferation Adds Network Demand and Complexity

Earlier we discussed the huge number of users on school networks but today most users have more than one device resulting in even more connections to the network. This research finds that 60% of users have 4 or more devices connecting to the school’s network. This means that smaller campuses will likely have 40,000+ devices on their network and over 200,000+ devices are connected on larger university’s networks. This trend appears to be accelerating as nearly 9 in 10 IT professionals stated the number of devices connecting to the networks are increasing.
IOT Devices Growing

The survey then asked participants what types of devices are connecting to the network. While the top 4 items - smart phones, laptops, computers and tablets - were expected, the number of newer internet enabled devices was surprising. On average, 1 in 3 users have either a webcam, smart watch or a personal assistant on campus. Companies like Apple, Amazon and Google are running huge marketing campaigns for these devices, driving the trend. The number and variety of devices connecting to higher learning institutions networks is only expected to increase.
Vast Numbers of Devices Are Infected and Connecting to the Network

While the sheer number of devices is a problem enough, IT professionals shared that many of those devices are showing up already infected with malware. In fact, more than half of IT pros stated 25% or more of connected devices are already infected before they join the school network for the first time. For IT and security professionals this is serious problem. They must ascertain the nature of the malware to determine if the device should be allowed on the network and then provide constant vigilance on those devices while on the network to ensure they do not spread their malware to other users and devices. IT must have network tools capable of monitoring and managing this threat at a scale that most enterprises never experience.

IT Voicing Concerns About the Volume of Connected Devices

Staff and faculty often have direct interactions with the IT staff and were more likely to hear about concerns and frustrations from colleagues. As such, this research asked faculty and staff if IT has ever voiced concerns about the number of devices connecting to the school network. 35% revealed that IT has shared concerns about the volume of devices connecting to the network. This provides additional insight that this a growing problem for IT and something beyond normal network challenges.
Massive User and Device Churn Every Year

This research has found the number of users and volume of devices is extremely large for higher learning institutions. And to make matters even more challenging, IT professionals share that 25% or more of the users change each and every year. This does make logical sense as new students join the school and many existing students graduate. This is creating tremendous churn for the IT and not just because of the new users themselves, but the huge number of devices that change each and every year. For IT this means new devices to detect, scan and manage, knowing that many of them are already infected.

More Than Half of IT Pros State More Than 25% of Network Users Change Every Year

On average, what percent of network users (students and staff) change each year?
Challenges Lead to Service Interruptions

While IT has stated that managing the network is increasingly difficult, this research finds that these challenges are resulting in end-user impact. 71% of the faculty and staff who use the network daily reported they experience network issues at least once a month. In fact, 40% are experience problems several times a month or more. The findings indicate that users and institution are losing productivity from increasing network challenges.

71% Faculty and Staff Share School Networks Suffer Performance Issues Once a Month or More

The Hackers are Already Inside

This research then asked all participants where the greatest security risk comes from. A majority of IT professionals (59%) stated that the largest risk is already within the campus and likely on the network, a concern perhaps based on the massive number of infected devices.

Interestingly, we asked this same question to students, faculty and staff. Students believed most threats (55%) would come from outside the campus. Faculty and staff joined in that perception with 63% of them thinking threats were outside the school.

IT professionals who deal with the threats have a different view than that of users.
Students are the Threat

While IT has stated most attacks have come from within the campus, the research then asked students, which make up a vast majority of users, if they are knowledgeable about other students performing malicious acts. Shockingly, 33% of students have heard of fellow students hacking school networks or attempting to place malware on it. This does validate IT’s perspective that the major threats are already within the campus. These findings continue to describe a very challenging situation for IT and the tools that must defend the network from constant attack.

1 in 3 Students Know of Other Students Performing Malicious Acts

Have you ever heard that another student hacked or placed malware on the campus network?
Users are Part of the Problem

With so much threat and security risk today, the research then asked all participants what security measure they use on their connected devices. 80% of participants indicated they use a password to limit access, but only 61% of participants run any malware protection. Less than half of those surveyed use any of the newer security solutions, such as two-step authentication, fingerprint and facial recognition. While new security threats are constantly evolving, 60% of faculty and staff revealed they have not adopted any new security precautions over the last two years. Both of these findings appear to be risky given this report’s foregoing findings.
Users are Unaware Data Flowing into the Cloud

Nearly every business entity today utilizes cloud-based solutions whether for applications or data storage. This research sought to understand how aware users are of what types of services they are using. A large majority acknowledge their data is likely flowing through public cloud solutions, but a nearly 1 in 4 (24%) did not, showing either ignorance or lack of concern.

24% Lack Knowledge of Where Their Sensitive Data is Used or Stored

Users Lack Good Judgement

The research sought to determine if users changed their behaviour based on the types of information they were accessing or sharing. Most participants limited exposing personal information by using what they perceive as more secure networks, such as a home network, (79%), campus network (67%) and cellular network (62%). But more than a third (38%) report that they use questionable public networks over which they share private information.
Misplaced Confidence
A huge majority of participants (83%) do trust the learning institution network. This research, however, has revealed the number threats and attacks that campus networks are constantly defending their users from. This data continues to show that many users are either ignorant or careless about their decisions about securing their devices and or their persona data.

83% Trust Their Personal Information is Secure on the Campus Network
Campus IT Pros Besieged by Numerous Network Challenges

While the preceding findings in this report have exposed some of the issues of managing a campus network, the research sought to gather a comprehensive list of top network challenges from IT professionals. The first observation about the data is that there are not one or two big issues, but nearly 10 issues possessing very similar magnitudes indicating broad and systemic challenges. The sheer scale of the systems is a concern as noted by growing numbers of users, (48%) and their devices. The IT team faces security issues from several vectors; attacks from within (40%), infected devices (40%) and constant attacks (34%). But IT professionals are also dealing with user issues; poor user judgement (43%), user ignorance (39%) and their low security defences (37%). Also, near the top is visibility, as 40% have indicated there are unknown devices on network. This list provided represents a daunting task for IT professionals.

Distributed Networks with Shifting Workloads

Another challenge than can be unique to the higher learning institutions is the multitude of locations, requiring a highly distributed network. Furthermore, besides the administration buildings, the network cannot be designed around a static load distribution as significant numbers of students and faculty access the network in multiple locations each day.
IT Lacks the Networking Tools for Success

Perhaps the most surprising finding in the research is the tools that campus IT and networking teams have to manage and defend their networks. While at first glance the chart below looks rather good, as most participants appear to have the 5 key elements needed for enterprise class network management, in studying the data, the realization emerges that at best only 52% of schools have all 5 capabilities. Stated another way, nearly half (48%) of campuses lack comprehensive network management capabilities. Given the scale, massive security threats and questionable user decisions this looks to be a situation that will have repeated unfortunate outcomes.

IT Pros Reveal 48% of Campuses Lack Comprehensive Network Management Capabilities

Which of the following are you able to do with your current network management solutions?
Conclusion
There are few enterprises in the world that have as many users as an average higher learning institution. Even fewer enterprises have the massive number of devices connecting to their networks and with a larger percentage of them infected. Add in the fact that more than a quarter of those users and devices change each year, and it is no surprise that this changing landscape means it is difficult to establish a fixed security strategy and defence. Worse, the largest volume and highest risk security attacks are already within the campus and connected to the network, making the concept of a defensive perimetry elusive.

The learning institutions’ students, faculty, and staff don’t help the situation. They do not take reasonable security precautions and take extra risks. The data in this report shows it is a mix of ignorance and carelessness, which is always a bad combination.

The IT professionals revealed they have a long list of networking challenges centering in three key categories: scale, security and ignorance. But nearly half of all colleges surveyed showed they don’t have a comprehensive network management solution to help manage their network. Higher learning institution IT professionals are facing challenges that their peers in business enterprise rarely face and use inadequate tools in an attempt to protect their users and their schools. In an era where all entities must protect personal user data and intellectual property, learning institutions appear underprepared and to be taking unnecessary risks. They have some of the most challenging network scenarios in the world and need world-class tools to help them meet the mounting threats.

Survey Methodology
A total of 678 participants, having networking responsibilities or network users, completed the survey. Participants were from the United States, United Kingdom and Germany. The survey was administered electronically, and participants were offered a token compensation for their participation.
About Dimensional Research

Dimensional Research provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. For more information, visit www.dimensionalresearch.com.