Role of IT in Educational Institutes

IT Landscape in Education

Information Technology (IT) today is no longer just a field or vertical that people study or work for. It has penetrated all other verticals like Banking and Finance, Entertainment, Healthcare, Construction, Manufacturing and Education. The use of IT in all these sectors is so prominent that now, no one would even dream of working without use of it. The adaptation of IT into Education is particularly noteworthy as, here, IT is not only taught to the younger generation, it is also used as a medium through which education is imparted.

Schools and higher education institutions strive to build adaptive and cost-effective network infrastructures to support today’s sophisticated styles of teaching and learning. Use of technology and Internet access has become an essential part of a student’s curriculum to encourage comprehensive learning. IT is no longer used as a mere research tool, but most of an institution’s processes have gone online: whether we consider attendance, examinations, creating and submitting assignments, declaring results, and other various tasks. Use of laptops and tablets for classroom assignments has become the need of the day.
With the GOOD comes the BAD…

Educational institutes are a hot target for hackers who seek student’s personal information or simply to tamper with results or grades. Networks of educational institutes are particularly vulnerable because they tend to be more “open” or less secured as compared to other verticals. Lesser experienced IT staff and undervalued IT budgets are some of the main factors contributing to this gap.

Educational networks also face challenges relating to unproductive, inappropriate use of the Internet; managing traffic from a myriad of BYOD devices; managing different Internet requirements for different users at different time schedules. Some of the most common scenarios relating to IT related issues in Educational Institutes are given in the section below.

It is very important to balance the useful utilization of this technology to its full potential for academic purpose and avoid misuse. It can neither be wise to block the resource entirely for fear of harm, nor can it be made fully available. In all of this, the trick is to find the correct balance: Balance between users’ exposure to the technology, and restrictions for required amount of protection.
Institutes are Hot Targets for Attackers

Hackers today have grown to be very sophisticated. The lone-wolf hacker creating nuisance viruses in a basement has been replaced by sophisticated foreign governments and organized crime rings as the top cybersecurity threat to colleges and universities. Among the education cyberattacks that have occurred recently are crime rings stealing vast amounts of credit card numbers; governments trying to infiltrate nuclear research databases; and students hacking the registrar’s office to change grades.

Typical Scenarios in Institutes

Cyberoam safeguards from intrusions and other attacks

Cyberoam’s Firewall acts as armor around the network periphery, shielding it from any hostility from outside. The Intrusion Prevention System (IPS) acts as a second layer of defense. Cyberoam’s DoS and DDoS Attack Prevention mechanism adds further to the safety.
Students access unproductive/harmful web content and applications
Institutions need to control student’s Internet surfing so that they do not spend their precious time in unproductive web activities like social networking, gaming, sports, chatting, etc. which would take a toll on their academic performance. Furthermore, students need to be protected from inappropriate or harmful content on the Internet at all times: especially from content related to pornography, violence, criminal activities, profanity, alcohol, drugs or illegal activities.

Cyberoam productively focuses web access
Cyberoam’s Web and Application Filter allows administrators to block all harmful and unproductive content on the web. Millions of websites and applications are categorized into Cyberoam’s in-built Web Categories like Social Networking, CrimeAndSuicide, Gambling, Entertainment; and Application Categories like P2P, Social Networking, Instant Messenger which can be used to create appropriate policies.

Also, Cyberoam allows you to design Custom Denied Messages which allows administration to communicate effectively with the students as to why they are not allowed access to these websites and, in turn, develop healthy surfing habits among pupils.
Untimely use of Internet during lectures
With the introduction of computers, laptops and tablets in classrooms, teachers face the challenge of retaining their pupil’s attention during lectures. While the classes are on, they have to make sure that students access only the required course material while they teach and not go wandering into cyberspace wherever they please. Furthermore, some course work may require access to certain websites or applications that are otherwise banned.

Cyberoam provides Flexible, Schedule-based Traffic Filtering
While Cyberoam’s Web and Application Filtering can be used to block access to all unwanted content on the Internet, Schedules can be configured to allocate time period during the day or week when these policies are to be applied. Furthermore, administrator can tweak policies as and how the teachers require without any hassles. For example, you can schedule strict policies which allow only course-related content between 11 AM and 5 PM while a more lenient policy, allowing social networking and gaming, can be scheduled for after school hours.

Students taking undue advantage of YouTube Access
YouTube is a vast repository of videos relating a myriad of topics which schools nowadays like to use to provide an enhanced learning experience to the students. But, opening up YouTube for students spells trouble for the teachers. Students tend to stream songs, promos or other entertainment videos during lectures, resulting in distraction and strain on the bandwidth.

Cyberoam’s YouTube Education Filter does the trick
Cyberoam allows access to YouTube videos deemed as ‘educational’ via a special portal ‘YouTube EDU’ while being within a school network.

YouTube EDU consists of two sections, “YouTube.com/Teachers” and “YouTube for Schools”.

“YouTube.com/Teachers” educates teachers on how to make optimum use of YouTube within the classroom. On the other hand, “YouTube for Schools” is a network setting, which redirects the video traffic, making it possible for schools that block YouTube to unblock and allow access to YouTube EDU (Youtube.com/education). The teachers and Administrators decide what videos must be made available to the students, making a safe and a controlled environment for students.
Identifying users in a shared or dynamic environment

In a shared or dynamic environment, one of the major challenges faced by the administrator is to identify students who violate healthy surfing policies. For example, the administrator detects that an IP address in the network, say 172.16.16.57, has downloaded more content than allowed. But, the computer with IP 172.16.16.57 had been used by 4 different students. In such a case, how to find out who is the culprit? OR In an environment where devices are assigned dynamic IP address, how to pinpoint which particular device?

Cyberoam pinpoints exact user in a shared or dynamic environment

Cyberoam’s Identity-based control necessitates each student to authenticate before using Internet, whether it is a shared resource or a personal device. Logs and reports are recorded with the username rather than IP addresses. Hence, in case of breach or violation, administrator can find out exactly Who is doing What in the network.

Use of Proxies and Tunneling applications to bypass web controls

Students tend to use proxies or other tunneling applications like ultrasurf, tor, gtunnel to bypass the Internet controls imposed by the administration.

Cyberoam blocks proxy and tunneling applications

Cyberoam’s IPS and Application Filter can be used to block any such proxy and tunneling feature to discourage students from violating Internet use policies.

Bandwidth Choking

Unhindered social networking, upload and download of music and videos, and gaming choke the available bandwidth leaving very little for critical applications and key users.

Cyberoam keeps firm control over bandwidth usage

Cyberoam’s Quality of Service (QoS) allows custom allocation of bandwidth such that the most critical applications are given priority while reducing bandwidth-availability to a minimum to unproductive ones. Also, if institution has more than one ISP links, Cyberoam’s Multi-Link Management allows harnessing the bandwidth of all links simultaneously by distributing traffic over multiple links. Automatic Link Failover ensures Zero Downtime by providing failover to any working link when the primary link goes down.
Risk of Virus, Spyware, Adware, Spam infecting the network
Students may unknowingly download viruses or spyware into the network which may result in loss of data, corrupt documents or slow network. This could possibly open up the school network to botnets which would install bots in the school computers and use them for broadcasting viruses, Spam. Entry of adware into the network may result in embarrassing pop-ups and inappropriate advertisements.

Cyberoam blocks all kinds of Malware and Spam at the Gateway
Cyberoam's Gateway Anti Virus protects the network against entry of any virus, Trojan, worms, etc at the gateway itself. The Gateway Anti Spam has a Spam detection rate of 99.5% with a false positive rate of 1 in 1.5 million. Its unique IP Reputation and Recurrent Pattern Detection (RPD) technology blocks all types of spam including excel, pdf, multi-lingual spam etc.

Non-compliance to Regulatory Requirements
Academic institutes need to abide by certain laws like Children's Internet Protection Act (CIPA) wherein they are to ensure that students are not exposed to inappropriate content over the Internet. They have to impose restrictions based on strict guidelines laid down by the Act.

Cyberoam provides “Easy Compliance”
Cyberoam helps institutes to comply with CIPA or other regulatory compliance. In fact, Cyberoam provides “Easy Compliance” wherein it required just a few mouse-clicks to enable CIPA-specific configuration.
Dealing with multitude of Wi-Fi and BYOD
Nowadays, since most institutions are Wi-Fi enabled, administrators have to deal with traffic from a multitude of BYOD. Students tend to carry more than 2 devices which include not only smartphones, but gaming systems, laptops, tablets, blu-ray players and many other connected devices. All these connect to the institute Wi-Fi resulting in strain to the network bandwidth. Also, Internet access from all these requires that added layer of monitoring and restrictive policies. These devices are at risk of eavesdropping, interception, modification of data in transit, spoofed email messages for social engineering and malware insertion attacks and service disruption.

Cyberoam provides high performance, integrated security over WLAN
Cyberoam wi and wiNG models have integrated Wireless Access Points that provide safety over a wireless network as efficient as that of a wired network. Additionally, Cyberoam allows administrators to allocate policies to users based on their location or MAC Addresses of their devices which help in controlling traffic. Identity-based controls ensure complete control over Internet traffic even when Dynamic IP addresses are allocated to these devices.

Providing protection in a Virtual Environment
Advancement in the current technology has made many institutes to make the shift from physical to Virtual Infrastructures. They have employed Server Virtualization and Desktop Virtualization technologies to facilitate faster and more efficient network.

Cyberoam offers Virtual Security
Cyberoam's range of Virtual Security appliances safeguards virtual virtual data-centers, “Security-in-a-Box” set-up, and “Office-in-a-Box” set-up. By offering comprehensive security features available in its hardware security appliances, in virtualized form, these virtual appliances offer Layer 8 Identity-based security on a single virtual appliance, which is as strong as security for the physical networks.

Monitoring the usage
It is of prime importance to keep a sharp eye on all network activities throughout the institution. It is necessary to check whether the policy you have implemented is correct and in tune with your requirements, and to keep track of newer trends that would influence future policy-making.

Cyberoam provides FREE, On-Appliance Reporting
Cyberoam records the information about the usage based on the actual surfing done. This information can be used to:
- Determine the heavy usage periods
- Spot Abusers
- Increase or decrease the surfing limit
- Reschedule the access
- Charge against students/staff for usage – if required
Cyberoam's On-Appliance Reporting provides easy-to-understand graphs and to check the impact of policies and monitor usage. You can especially use reports for:

- **Top Applications Used**

![Top Applications Graph]

- **Top Applications Users**

![Top Users Graph]
- **Top Web Users**

  ![Top Web Users Graph]

<table>
<thead>
<tr>
<th>User</th>
<th>User Group</th>
<th>Hits</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>N/A</td>
<td>2337744</td>
<td>1.06 TB</td>
</tr>
<tr>
<td><a href="mailto:administrator@secure_ad-ladap.com">administrator@secure_ad-ladap.com</a></td>
<td>Open Group</td>
<td>6527</td>
<td>562.24 KB</td>
</tr>
<tr>
<td><a href="mailto:administrator@ocmq.com">administrator@ocmq.com</a></td>
<td>Open Group</td>
<td>5209</td>
<td>32.71 MB</td>
</tr>
<tr>
<td>cyberoam</td>
<td>Open Group</td>
<td>1342</td>
<td>17.4 MB</td>
</tr>
<tr>
<td><a href="mailto:d1@ocmq.com">d1@ocmq.com</a></td>
<td>Open Group</td>
<td>967</td>
<td>29.08 MB</td>
</tr>
</tbody>
</table>

- **Top Web Categories**

  ![Top Web Categories Graph]

<table>
<thead>
<tr>
<th>Category</th>
<th>Category Type</th>
<th>Hits</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAddress</td>
<td>Neutral</td>
<td>1553895</td>
<td>756.45 GB</td>
</tr>
<tr>
<td>Uncat</td>
<td>Neutral</td>
<td>677229</td>
<td>323.46 GB</td>
</tr>
<tr>
<td>Uncategorized</td>
<td>Neutral</td>
<td>89929</td>
<td>234.1 MB</td>
</tr>
<tr>
<td>InformationTechnology</td>
<td>Neutral</td>
<td>9309</td>
<td>396.28 MB</td>
</tr>
<tr>
<td>Spyware</td>
<td>UnHealthy</td>
<td>4218</td>
<td>185.36 KB</td>
</tr>
</tbody>
</table>

  View All
Top Internet Users

Data-wise Usage Report

<table>
<thead>
<tr>
<th>Date</th>
<th>Client Type</th>
<th>Used Time</th>
<th>Data Transfer</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-11-22</td>
<td>Web Client</td>
<td>00:51:07</td>
<td>30.01 MB</td>
</tr>
<tr>
<td>2013-11-26</td>
<td>Web Client</td>
<td>-08:58:57</td>
<td>638.09 KB</td>
</tr>
<tr>
<td>2013-10-21</td>
<td>Web Client</td>
<td>00:02:43</td>
<td>17.41 KB</td>
</tr>
</tbody>
</table>
- **Top Denied Applications**

  ![Top Denied Applications Chart]

- **Data-wise Usage Report**

  ![Data-wise Usage Report Chart]

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Type</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-06-28 00:00:00</td>
<td>Web Usage</td>
<td>0</td>
</tr>
<tr>
<td>2013-06-30 00:00:00</td>
<td>Web Usage</td>
<td>0</td>
</tr>
<tr>
<td>2013-07-02 00:00:00</td>
<td>Web Usage</td>
<td>0</td>
</tr>
<tr>
<td>2013-07-04 00:00:00</td>
<td>Web Usage</td>
<td>0</td>
</tr>
<tr>
<td>2013-07-06 00:00:00</td>
<td>Web Usage</td>
<td>0</td>
</tr>
<tr>
<td>2013-07-08 00:00:00</td>
<td>Web Usage</td>
<td>65</td>
</tr>
<tr>
<td>2013-07-10 00:00:00</td>
<td>Web Usage</td>
<td>0</td>
</tr>
<tr>
<td>2013-07-12 00:00:00</td>
<td>Web Usage</td>
<td>0</td>
</tr>
<tr>
<td>2013-07-14 00:00:00</td>
<td>Web Usage</td>
<td>0</td>
</tr>
<tr>
<td>2013-07-16 00:00:00</td>
<td>Web Usage</td>
<td>1293</td>
</tr>
<tr>
<td>2013-07-18 00:00:00</td>
<td>Web Usage</td>
<td>202</td>
</tr>
</tbody>
</table>
Conclusion

In summary, there is no easy, single step solution to protecting an educational institute's network and managing the Internet access. The threats to an Academic Institutes are highly varied both in their nature and in the medium of exposure. Furthermore, the nature of these threats is constantly changing; a change driven by external forces and by the evolving nature of how students use information.

However, just like virus scanning, managing and protecting the network is an ongoing process. Although a strategy needs to be developed, it is essential that flexibility and adaptability remain the cornerstones.

How Cyberoam Can Help

Cyberoam presents an integrated approach to protecting and managing your Institute’s IT resources. Robust virus scanning, intrusion prevention, Internet scheduling, filtering and blocking allows you to protect your institute and maximize use of your assets. Cyberoam protects filters and monitors your institute’s entire Internet access using simple policies.