

Case Study:

Flash to HTML5 Migration



Flash Conversion for a Leading University's Cybersecurity Programs

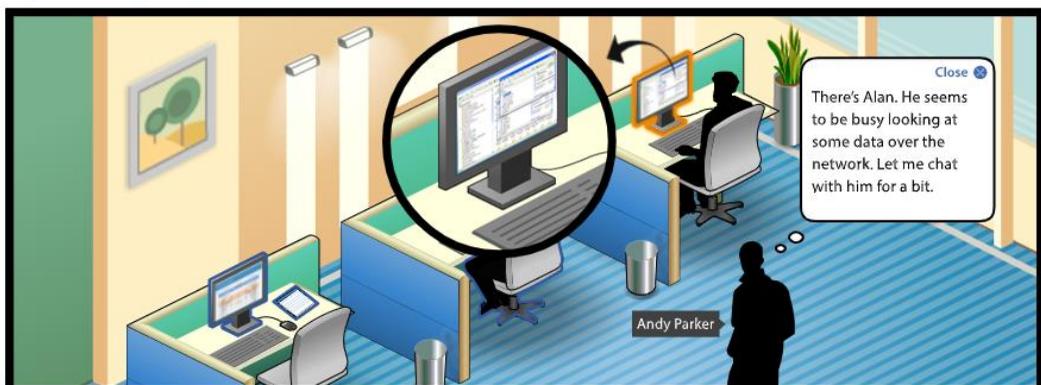
Client Description: The client is an online state university that was founded more than 70 years ago to serve working adults and service members. It offers undergraduate and graduate programs in fast-growing and in-demand fields.

Business Need: The client was seeking to prolong the shelf-life of their popular Flash-based online Cybersecurity program. With a large number of students accessing the courses from tablets and desktops, Flash was a deterrent. Moreover, there were questions with regard to its support by Adobe and compatibility with common browsers in the long run. In the process, they also wanted to update some content and package courses into plug and play modules.

Solution: MPSi migrated the Masters in Cybersecurity program from Flash to HTML5 for the client in a very short timespan. The program comprised 9 Cybersecurity courses that included 9 web-based tutorials, 4 interactive case study simulations and 4 Day-in-the-life simulations that were developed in Flash. MPSi used the combination of HTML5, XML, CSS3, Javascript, and JQuery to migrate approximately 2000 screens with multiple sub-screens and layers of content into the HTML5 framework, replicating the original functionality and look-and-feel, and designing and implementing workarounds wherever required. The information about the course structure, i.e. number of modules, number of topics in each module, and the information about the course directory structure was stored into an XML file. The solution enabled the courses to be deployed on Windows/Mac desktops, Apple iOS devices (iPad) and Android tablets. MPSi ensured that the components are optimized for network usage by compressing the assets for size reduction. The course complied with SCORM 2004 specifications and was hosted on the client's Blackboard LMS.

Scenario

To learn more about the IT security lapses at the Dallas office, select each highlighted element on the screen. Begin with the notepad kept on the first desk.



[Skip to the Module](#)

Flash Conversion for a large business conglomerate's Cybersecurity Programs

Vulnerabilities of LANs, WANs, and MANs

Revisit the Cypher X scenario. Which of the following could be security vulnerabilities in an office setup similar to Cypher X's Dallas setup?

Select each option to learn about Andy's observations.

Unattended Computers

Printers

Access to Gaming Web Sites

Discarded

[Submit](#)

This could pose a serious threat to the LAN, as any material downloaded from the Internet can contain viruses or worms. Access to online games, movies, and songs should be restricted. All files that are downloaded from the Internet should be scanned for malware prior to being downloaded. Note that today many anti-virus products have web browser plug-ins which will analyze links in search results and indicate if the link is good / trusted, suspicious or known problems, or of unknown trust / certainty. This can help in users clicking on known problem website links which could compromise the user's computer to phishing or waterhole attacks.

Intranets

An intranet is a collection of private networks that enable the secure sharing of information within an organization, which in turn helps users to build communication and improve productivity across the organization. An organizational intranet allows for intranet access.

The use of intranets can help to isolate business workgroups, to reduce network traffic, and to contain proprietary or business intelligence.

[Click here to learn more about how Andy uses the intranet at work.](#)

Corporate Communication

This section is used by our management team for sharing the vision and mission statements, corporate code of conduct, branding guidelines, and staff newsletters. In fact, when we have new recruits at Cypher X, we ask them to get started with this section. It gives them an idea of the corporate culture and how things are done here. I also find that the staff newsletters make me feel connected to the company.

Vulnerabilities of WLANs

Like their wired LAN counterparts, WLANs are prone to security vulnerabilities. In fact, a WLAN is more susceptible to attacks because it includes both the organization's internal network and the general public network segments. An open WLAN, which does not require users to

Traffic Analysis

Traffic analysis helps determine the load on a wireless network. This type of analysis gathers information about the frequency and timing of network packets in transit. The attacker can identify the Web sites being visited and read messages that are sent on the

WHA?P
SO WHAT?P
HOW WHAT?P

Reflect

Business Impact: The migrated courses were well received by the students. The migration gave the students more flexibility to access them anywhere-anytime. The chunking into micro-units gave flexibility to the faculty to mix-and-match existing content assets to easily create SCORM-compliant learning modules.

MPS Interactive also updated content in collaboration with the client's SMEs. The courses were packaged into micro-units. We developed an interface that allowed UMUC administrators and faculty to select one or more micro-units and package them into a SCORM-compliant module with the click of a button. MPSi also packaged the modules for compliance to xAPI to make the courses more learner-centric and future-ready.

About MPS Interactive

MPS Interactive is a global pioneer of eLearning solutions with extensive experience and a strong global presence. Our offerings feature diversified, innovative learning and technology solutions, such as simulations, serious games, augmented & virtual reality, 3D virtual worlds, web portals, and LMS.

MPS Interactive serves corporations, universities, schools, publishers, and government institutions alike and counts over 70 Fortune 500 companies among its clients.

To know more, feel free to write to us at marketing@mpsinteractive.com.

