Draft risk management plan

Business, Risk Management

The top three security threats that Aim Higher College faces are the following: * Mobile devices connecting to the network * Social Medal * Compromised routers intercepting sensitive information These threats are the most common that any college faces. The threats have remained at the top of the list every year for a variety of reasons. This list of threats Is also unique to college campuses. I will discuss each of the threats in this report.

Students, especially college students, are consistently on some type ofsocial mediatie or on a mobile device that gains them that type of access. There are many varieties of devices such as tablets, smartness, laptops, and now even checkmates. Devices such as these are connecting to wireless networks whether it's from a service provider or campus. With these connections many aren't just using them for social media, but also for checking grades, schedules, or relevant news. The devices depend on connecting to networks but also need to do so in a secure fashion.

Each device has to be checked for viruses, spare, and other types of mallard while still maintaining the GIG-A triad. A balance must be found between usability and security. Each time a remote device is connected to the network there is a possibility that the network can be compromised by one these devices. Every device should be authenticated, scanned, and identified. Many are unaware of the risks that can come from connecting to networks, especially wireless access. The use of social media has increased in recent years and according to this chart we can see according to age groups how many are connecting to social media.

Students and teachers both use things like Faceable, Misplace, Linked, Mainstream and many ore. These applications have the potential to transmit mallard every time they are used on the campus network. Mallard can be embedded in everything from videos to comments. Any time a student orteacherclicks on a video viruses, keystroke loggers, or worms can be installed and start destroying or intercepting data. The Infected devices must be Identified quickly and the mallard removed while still allowing others to access the websites.

Another challenge unique to social media is the fact that not only Is there a potential network impact, but students may be caught or violations to campus policy on their own time. Social media Is being scrutinized on a massive scale and students and teachers both must watch the types of posts they posting on these sites. Posting personal beliefs that could be construed as hate or Ignorance. Posts against faculty or staff could cause a person to be expelled or fired depending on the situation. People posting pictures or videos of themselves in lewd or mischievous acts could be reprimanded for their actions.

Most believe these toy 2 making it public especially when sharing with others. The last threat in the list is a improvised router intercepting sensitive information. As the core routing system for the Internet, BGP defines the most efficient route for Internet data to be transmitted around the world, deciding which " links" carry Internet data. Think of it as the Internet's navigation system, providing turn-by-turn directions for all Internet connections. By hijacking the BGP translations, attackers can drive

unsuspecting surfers and/or students, faculty and staff attempting to access the university network to malicious sites.