Higher education institutions strike a delicate balance between safeguarding personal data and intellectual property, while also encouraging academic freedom, openness, and collaboration. But doing so is challenging, especially with new threats and threat types arising each year.

In the Cisco 2018 Security Capabilities Benchmark Study, 60% of higher education institutions reported at least one public security breach (for all industries, this number was 55%).

The Internet of Things (IoT) and Bring Your Own Device (BYOD) on campus are the most challenging areas to defend. 71% of respondents say IoT and BYOD pose a high or moderate risk for their campus. 36% say they expect a cyberattack in Operational Technology (OT) in the next year. OT includes IoT devices like HVAC systems; washers and dryers; vending machines; and security cameras.

The personnel gap — a top obstacle to security in education

Colleges and universities say they would expand cloud security, mobility security, network forensics, and data-loss-prevention capabilities, if only they had the security personnel. Today, 31% of college and university respondents say their current workload is too heavy to take on any new responsibilities.

The bright side...

The cost of attacks

Of respondents that say that their systems were down for nine hours or more as a result of a recent security breach.

49% Of respondents say that more than half of their systems were impacted.

32% Number of attacks that resulted in financial damages of more than $500,000.

51% Number of attacks that resulted in losses of between $100,000-$499,000.

23%