Mobile, Cloud, and Outsourcing Trends Pose IT Security Risks to Higher Education and Not-for-Profit Sectors

By Lucas Morris, CISSP, Cynthia A. Pierce, CPA, and Christopher P. Reffkin, CISSP

Higher education institutions and not-for-profit organizations face many of the same IT security risks that businesses do, including risks from the growing use of mobile devices, cloud computing, and outsourcing of important functions to third parties. But how many colleges, membership associations, and other not-for-profit organizations follow the same rigorous practices that businesses use to protect themselves, their employees, and their information from unauthorized access by hackers, identity thieves, and other technology-savvy criminals?

The answer? Probably fewer than should.

Like commercial enterprises, higher education institutions and not-for-profit organizations need to follow the rules of “CIA” when protecting information:

- **Confidentiality.** Information should be accessible only to those who are authorized to view it.
- **Integrity.** Organizations should provide a high level of confidence that information viewed by authorized users is accurate and free from tampering.
- **Availability.** Information should be available on demand.

Bad things can happen to good organizations when they do not follow the rules of CIA. For example:

- In 2011, hackers broke into a server at a major East Coast university and stole names, Social Security numbers, and other personal information of more than 175,000 current and former students, faculty members, and staff members.
- A year later, a student at a major Midwestern university infiltrated the student information system. Although there was no evidence of any personal information being downloaded, more than 600,000 records were breached.

Administrators and IT professionals at higher education institutions and not-for-profit organizations can protect their valuable digital assets by understanding the potential risks involving mobile devices, cloud computing, and outsourcing to third-party vendors.
Mobile Devices: The Consumerization of IT

Perhaps no piece of technology is more popular today than the smartphone and its larger cousin, the tablet. Being able to communicate with friends and family by tapping a few keystokes on a small screen has revolutionized social communication – and whole industries that thrive on people’s desire to stay in touch with one another.

When people go to work, they want to have the same convenient technology at their fingertips so they can share files and be more productive. However, workplace technology sometimes lags consumer technology, so employees use their personal devices – with or without employers’ permission – to accomplish what they want. This trend is known as the consumerization of IT.

Though not without benefits to employers, the consumerization of IT also presents security risks. Mobile devices are lost or stolen easily; if smartphones and tablets are not password-protected, people who find or steal them might have access to employers’ files.

Higher education institutions and not-for-profit organizations need to decide what policy they will follow when it comes to using mobile devices at work. Should colleges and other organizations allow employees to use their own devices, thus avoiding a major investment in mobile computing? Or should employees’ use of personal devices be forbidden in favor of employer-owned smartphones and tablets?

Whatever the decision, administrators and IT professionals should make sure that all employees using mobile devices for work use strong passwords (random letters in both uppercase and lowercase, numerals, and special characters such as asterisks), limit Internet access, and make no unauthorized modifications. The last thing any employer wants is for an employee to inadvertently download a Trojan horse virus disguised as a game that can steal valuable data from a mobile device.

Rogue Use of Cloud Computing

Just as employees use their personal mobile devices to access work files without permission, many of them also use their personal cloud computing accounts to transfer and share work files. Such rogue interaction with these hard drives in the sky is more widespread than employers would like to admit.

According to a survey by computer security software company Symantec Corp., 69 percent of employees admit to unauthorized use of cloud-based email/communications at work, and 38 percent say they have used cloud-based storage/applications at work without their employers’ permission.1

When employees put work files on personal cloud storage accounts, the information in those files might not be as secure as it is behind their workplace firewalls. Moreover, employers lose control of the information in those files when they are stored in personal cloud accounts.

Because employees will continue to use these eminently convenient cloud storage services unless employers provide sanctioned alternatives, higher education institutions and not-for-profit organizations should integrate cloud computing into their strategic IT plans and make sure that no employer information is residing in personal cloud computing accounts.
Outsourcing can pose an IT security risk if organizations do not know the controls their vendors have over client data.

Outsourcing to Third Parties

The use of third-party vendors to provide additional IT capacity and functionality has been a boon to many industries. Third parties that host specialized “software as a service” applications for payroll, fundraising, and other functions can help higher education institutions and not-for-profit organizations manage their IT programs without having to make major investments in specialized in-house resources.

At the same time, outsourcing can pose an IT security risk if organizations do not know the controls their vendors have over client data. Administrators and IT professionals can find out how their data is protected by vendors by creating a comprehensive list of vendors they pay and sending a short security questionnaire to the vendors.

If the list is extensive, organizations will want to consider conducting a risk-based analysis to identify the vendors that handle the most sensitive data and then interview or even visit them to see what safeguards they have in place. Ask how often they conduct penetration testing and if they conduct an annual or more frequent IT security assessment. Perhaps more simply: Do they even have an information security policy? Vendors that cannot provide evidence of such basic measures are a source of serious information security risk.

Mitigation of IT Security Risks

Given the legal and financial liability that organizations face when IT security breaches occur, higher education institutions and not-for-profit organizations cannot place too great an emphasis on understanding the risks that mobile devices, cloud computing, and outsourcing to third-party vendors present.

Administrators and IT professionals would do well to assess the potential risks that mobile devices, cloud computing, and outsourcing could present to organizations and develop appropriate strategies for mitigating those risks going forward.

Contact Information

Lucas Morris is with Crowe Horwath LLP in the Chicago office. He can be reached at 630.574.1850 or lucas.morris@crowehorwath.com.

Cynthia Pierce is the managing partner of Crowe higher education/not-for-profit services. Based in the Chicago office, she can be reached at 312.899.7019 or cynthia.pierce@crowehorwath.com.

Chris Reffkin is with Crowe in the Indianapolis office. He can be reached at 317.208.2547 or chris.reffkin@crowehorwath.com.