EDUCAUSE
CENTER FOR APPLIED RESEARCH

IT Security in the Bring-Your-Own Everything (BYOE) Era

Research Report February 26, 2013

Eden Dahlstrom, EDUCAUSE

Stephen diFilipo, Cecil College

> There are risks and costs to action. But they are far less than the long-range risks of comfortable inaction.
>
> — *John F. Kennedy*

We are living in the era where affordable, easy-to-use, and readily accessible technologies facilitate a bring-your-own everything (BYOE) standard in the workplace and in the learning environment. Bringing your own technology has been and continues to be the norm for students, and it is becoming the norm for faculty and staff.[1] This "consumerization of technology" is setting a new standard in which various populations across an institution bring their own devices, software, apps, and cloud-based technology to create a personal computing environment. The consumerization of technology understandably raises questions and concerns about IT infrastructure, planning and governance, security practices, support strategies, teaching and learning, and fiscal considerations (see Figure 1). This ECAR report focuses on the specific issues around security practices as it pertains to BYOE—and offers solutions for minimizing security breaches and maximizing compliance with institutional standards.

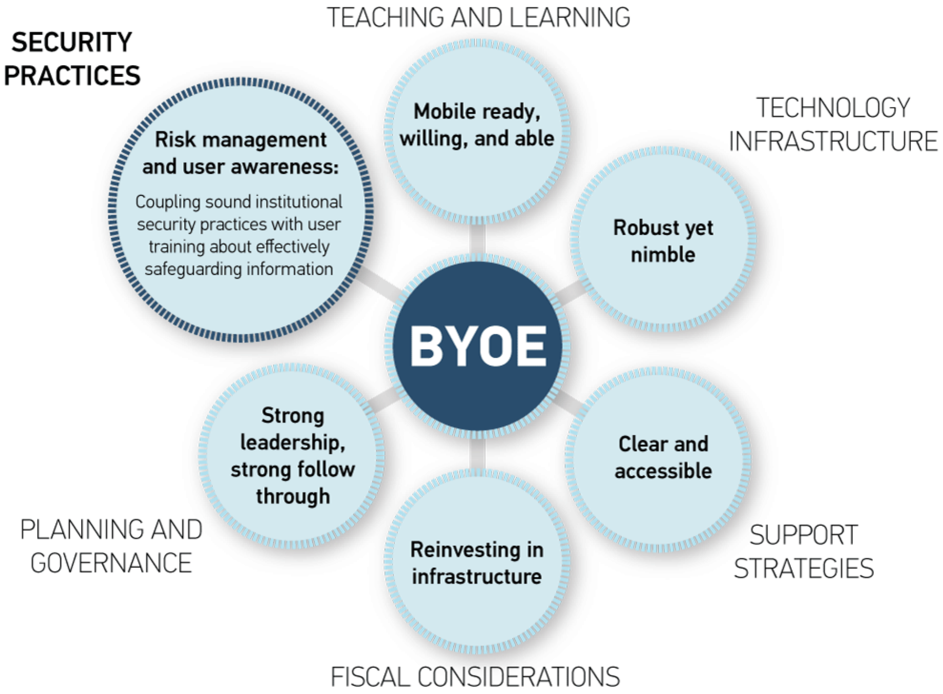
SECURITY PRACTICES
Risk management and user awareness:
Coupling sound institutional security practices with user training about effectively safeguarding information
TEACHING AND LEARNING
Mobile ready, willing, and able
TECHNOLOGY INFRASTRUCTURE
Robust yet nimble
BYOE
Strong leadership, strong follow through
PLANNING AND GOVERNANCE
Clear and accessible
SUPPORT STRATEGIES
Reinvesting in infrastructure
FISCAL CONSIDERATIONS

Figure 1. ECAR Framework for Studying BYOE

ECAR is addressing these issues by conducting research on how the consumerization of technology has opened the doors to a bring-your-own-computing-environment culture and the subsequent impact on and opportunities for higher education. A full ECAR report will explore each of the content areas depicted in Figure 1 in greater detail. This mini report provides a synopsis of the current BYOE computing environment issues that relate to IT security practices in higher education. This is not a roadmap for establishing measures to maximize security practices for those who "BYO"; rather, this report offers a way to think about security and if and how BYO affects security decisions by considering the following:

- What are the ***most important*** IT security practices for higher education institutions?
- What are some ***exemplary practices*** to handle or manage IT security practices?
- What ***strategic innovations*** are here now and on the horizon for IT security practices due to the consumerization of IT?

These findings will be supplemented in the final ECAR report with the results of a recent ECAR survey about BYOE practices in higher education. The survey data will provide an understanding about the current state of policies, practices, and experiences of BYOE in higher education and will also provide insight about the future plans for, and implications of, BYOE.

Findings

> Security is a chain; it's only as secure as the weakest link.
> — *Bruce Schneier,* Secrets and Lies: Digital Security in a Networked World

The volume of information published about user-provisioned technologies and security can be suffocating. A Google search on "byod + security" returns more than 8 million results in 0.23 seconds—too much information to be useful. Many of the top hits are commercial products and services that offer to address mobile IT and BYOE-related security needs. Your institution may well benefit from security hardware or software upgrades, services, and systems, but before investing in infrastructure or technology to mitigate security risks, consider what IT leaders in higher education told ECAR about BYOE and IT security with regard to the most important issues, exemplary practices, and forthcoming innovations.

ECAR conducted interviews, focus groups, and a survey of higher education IT leaders about BYOE security practices, and the results can be distilled into two broad categories: risk management and user awareness (see Figure 2). These two categories cover a spectrum from technology to people, and this report explores these issues to cover what matters most, what works well, and what may be on the horizon to make BYOE security practices easier to manage in the future.

Risk Management
User Awareness

- ✓ Securing Data
- ✓ Managing Access
- ✓ Securing Systems and Networks
- ✓ Managing Identity and Authentication

- ✓ Raising User Awareness
- ✓ Educating Users
- ✓ Enforcing Compliance

Figure 2. What Matters Most for BYOE Security Practices

The proliferation of user-provisioned technologies does not change the basic best practices around security very much—a solid security presence and plan on campus can adjust to most BYOE challenges. The fears of BYOE being the cause of a virus spreading throughout a campus network or of sensitive data being stolen, corrupted, or lost are often misplaced—the real cause is likely a straight-up security vulnerability that transcends BYO technologies. If institutional security practices are already porous, BYOE issues won't necessarily make things worse.

There is no silver bullet for ensuring IT security—there will always be risk to manage, and there will always be new user-awareness issues. Even the most vigilant CIOs can only aspire to do due diligence to minimize and/or mitigate security breaches. In what follows, ECAR prompts readers with questions (see italic text) to help assess current practices and offers suggestions or examples of exemplary practices.

Risk Management

> What I used to love about being CIO was getting the chance to be directly involved in small, cool projects led by faculty; now, I find myself spending most of my time talking with security auditors and those involved in regulatory compliance.
>
> —*A higher education CIO, quoted in* The Evolution of the CIO: An EDUCAUSE Issues Brief

User-provisioned technologies don't so much cause new or more security issues beyond what IT units already take responsibility for; rather, the recent explosion of BYOE draws attention to security issues and brings them into sharper focus. The security practices that are most important to higher education IT can be decoupled from BYO and pursued as stand-alone exemplary security practices. In fact, if sound security practices are in place, user-provisioned technology becomes a whole lot less scary.

As noted in the January 2013 ECAR report on IT infrastructure for BYOE, a perfunctory approach to BYOE security issues is neither recommended nor prudent, yet security practices should not be so Draconian that they limit access to what is arguably the single greatest invention of the 20th century—the Internet. ECAR approaches BYOE security issues from the perspective that data are the paramount institutional asset and are therefore the most important consideration when discussing BYOE security issues. From this standpoint, the most important risk-management issues for BYOE are securing data, carefully managing access to systems and services, using secure networks for enterprise-based activities, and authenticating identities. Dollars are better spent on these activities than on unique security concerns for user-provisioned devices and other technologies.

Securing Data

What does it mean to focus on securing data, not devices? Because devices are more commonly mobile and more commonly provisioned by users than ever before, it is neither feasible nor sufficient to rely on device security to safeguard data. Data should reside on secure servers, be encrypted at rest and in transit, and only be accessed through secure applications or https. These are exemplary practices, regardless of BYO or institutional provisioning, and, when coupled with user awareness about keeping data secure when they are accessed and viewed on "my screen," they can mitigate most data security risks. The forthcoming ECAR BYOE report will include benchmarking metrics about the extent to which higher education focuses on managing access (securing data) and managing assets (securing devices). The former is more commonplace than the latter, and the majority of institutions say that implementing or improving security for data is a high or essential priority. Also planned for the final BYOE report is information about the implementation of mobile device management (MDM) and data loss prevention (DLP) systems—deployment of these was surprisingly uncommon.

Managing Access

How sophisticated and reliable is your process for designating and managing roles and permissions? Though the assignment of roles and permissions is not the sole responsibility of IT, as the stewards of enterprise systems, services, and data, IT is a major stakeholder in ensuring the accuracy of access designations. The gold standard for effectively managing access includes both well-defined role-based access and multifaceted institutional oversight authorizing personnel to access secure data and mission-critical systems. To meet this standard, institutions must have a well-defined process in which access to systems and data is contingent on assignments—or roles—rather than on individuals. Role-based access allows an institution to define what a person can and cannot see and do based on that individual's current role(s) in the organization. If an individual's role changes, access should seamlessly and immediately change accordingly. Institutions should also have a functional system in place to edit, update, and audit roles and permissions as personnel change. De-provisioning access rights when roles change is not always easy because of the challenges of tracking people in decentralized campus systems; however, developing this ability is a wise investment of time and money because of the major security risks associated with role-based activities.

Securing Systems and Networks

How effectively do you secure data-center access? If you have a local data center, key/keycard access should be based on role, and the facility should be secured by de jure measures (i.e., access is limited and monitored—the facility is locked regardless of human action/inaction). Off-site or cloud-based data should reside in a secure commercial data center with N+1 redundancy. If data are secured (because they are encrypted at rest and in transit), and if systems that use these data are secured, then most risk of data loss, corruption, or hijack is mitigated. However, a potential vulnerability also can be found in network security.

How often and aggressively do you perform network security audits to proactively detect technical and personnel-based security vulnerabilities? The key characteristics of an exemplary security audit are that it is routine, frequent, systematic, and comprehensive. Additional system and log monitoring outside formal audits is also an exemplary practice.

Open Wi-Fi Connections

Providing a free, open Wi-Fi connection outside the institutional firewall enabling access to Internet resources only and leveraging browser-based solutions for all student, faculty, staff, and public resources (portal, website, LMS, library, blogs, social networks, etc.) for non-enterprise activities is both exemplary and innovative.

How often do you perform network penetration tests to detect malicious outsiders; are server and system logs monitored, and are notifications generated when thresholds are exceeded; are notification thresholds set at appropriate levels? Other system and network considerations include assessing the efficacy of your intrusion-detection system and the user-authentication protocol (discussed in the next section).

Managing Identity and Authentication

Is the institutional capacity to manage identities and authentication in line with the institutional priority to do so? In the ECAR study *Identity Management in Higher Education, 2011*, findings showed that institutional priority (measured via an importance scale) was out of sync with the capacity to effectively manage identities, yielding a capability gap.[2] Though these capability gaps were not as pronounced as previously measured in the 2006 version of this ECAR study,[3] they were universal for each of the identity management benefits measured. Lessons learned from these studies about the importance of user authentication, role-based authorization, and federated identities still apply today.

User authentication is the starting point for effective identity management, and recent evolutions in authentication practices attempt to balance rigorous security standards with user (in)conveniences. Two-factor authentication to verify user identity to sensitive data, mission-critical systems, and secure client applications seems to be increasingly common in higher education for “its most privileged users” (e.g., system administrators logging in remotely), but this evidence is still emergent and is anecdotal at best.[4] Not to be confused with two-step authentication, which is commonly just a username and user-generated password, two-factor identification typically includes a username plus two user credentials. Typically, credentials include something you *know* (a password or PIN), something you *have* (mobile device, token, smartcard), or something you *are* (biometrics or other personal attribute).[5]

A few institutions that have implemented two-factor authentication for “privileged users” are James Madison University, University of Fraser Valley (Canada), Carleton College, and University of California at Davis. The University of Georgia is "…piloting two-factor authentication with a token to ensure that faculty and staff with access to sensitive information have an additional layer of security to protect that data."[6] Technology available today to improve user-authentication security and simplify user experiences includes products and services from companies such as Duo Security, which lets users use their mobile phones as an authentication factor credential, and YubiKey, a fob that when partnered with a password manager program generates a one-time, 44-character encrypted passcode. It is not a great stretch to predict that two-factor or multifactor (two or more factors) authentication and single-use passcodes will replace simple two-step authentication in the near future. There is room to welcome procedures like these that attempt to balance security with simplicity and that are not too expensive to deploy or maintain. There is also room to welcome the next generation of user-authentication innovations that go beyond two-factor authentication, such as Jumio's Netverify Mobile product, which allows app publishers to authenticate customer identities by "seeing" a driver's license or ID card with a mobile device camera.[7] Though this technology is not presently ready to apply to authenticate users to mission-critical systems and services in higher education, optical recognition of user credentials could very well be a best practice for user authentication in the future.

User Awareness

> A common mistake that people make when trying to design something completely foolproof is to underestimate the ingenuity of complete fools.
>
> —*Douglas Adams,* Mostly Harmless

IT leaders have more direct influence over risk-management issues, such as securing data and managing access (discussed above), than they have over user awareness and behavior. User behavior is a real wild card for BYOE, as even the most intelligent and thoughtful students, faculty, and staff can inadvertently compromise institutional security if they are not aware of the potential risks and threat vectors. In ECAR-sponsored focus groups and interviews, the conversation about security generally started with, and circled back to, user-behavior issues. The importance of raising user awareness, being an active stakeholder in educating users, and advocating for enforcement of compliance with security policies was a key finding from this research.

Raising User Awareness

To what extent are users aware of sound security practices, and to what extent do they comply? Ideally, all users would have an appropriate understanding about safeguarding the information—especially confidential records—applicable to their jobs. Users would also recognize that as they move between roles (e.g., a student who is also on staff, a staff person who is also an adjunct faculty member, etc.), the use of computing resources may need to change. In this same ideal world, users would recognize that in some circumstances, their use of certain devices to access institutional networks, systems, or data might incur greater exposure to particular kinds of security risks. They would also respect security measures such as PIN- or password-protected devices and would adhere to security procedures. Having well-written, easily understood, and widely accessible policies on security for BYOE is a good practice, but it is important to understand that good policy does not translate into good security. This is especially true if compliance with policies is neither trackable nor enforceable. The forthcoming ECAR report on BYOE will provide benchmarking metrics on the extent to which various types of BYOE policies are currently in place. Acceptable use policies, policies addressing employee privacy expectations, and policies on security requirements for data were among the most common, but only about half of the policies we asked about existed at most institutions.

Educating Users

For whom is security awareness training mandated, and what is covered in this training? Faculty, staff, and students cannot reasonably be expected to comply with security standards of which they are not aware. Though ignorance is not a defensible excuse, educating users by raising their awareness that certain BYO practices can increase or decrease security risk could bolster compliance with institutional policies. As the stewards for data and the systems in which these data are housed, IT leaders are in a strategic position—or may perhaps be obligated by position—to make a case for educating users about the risks and benefits of using their own technology. In its BYOE research, ECAR found that mandated security awareness training is common but not universal for knowledge workers in higher education. Benchmarking metrics about security training practices will be shared in the forthcoming report. Also in this report will be what IT leaders believe are the most important education and training areas for BYOE security needs in higher education.

Enforcing Compliance

Can you monitor compliance, can you detect noncompliance, and can you act to enforce consequences for noncompliance? Enforcement is by far the biggest problem with compliance for BYOE. According to ECAR focus groups and interviews, enforcement of formal policies and practices is a luxury rather than common practice; however, there was general consensus that IT units could shut down infrastructure or block users from networks when a security threat or breach is detected. Most institutions rely on policy—and on user compliance with policies—but admit that enforcing compliance with policies is not always possible because IT may not have the power, authority, or inclination to do so. In most institutions there is a gray area where policy violations that are technically enforceable are not enforced because doing so would disrupt business continuity for the users. For example, if you see a faculty member hand his iPad to his child in a restaurant, subway, or community meeting on Sunday night, and you know that the iPad has the institutional e-mail application installed (because you helped set it up), do you disable that faculty member's account on Monday morning because you witnessed him violating the policy that "no one shall be permitted to use this device if you use it to access your institutional e-mail account"? Probably not. But do you use this as a prompt to send a reminder out (to all BYO users) about this policy? Maybe so. The best practices for IT professionals when it comes to BYOE security are to emphasize user awareness that includes information about potential consequences and enforcement, use good judgment when enforcing policies (or rewrite policies so they are enforceable), and strive to have effective training about users' personal responsibilities when using their own technologies to conduct college or university business.

Recommendations

Sound security practices are sound security practices, and these apply equally to institutionally provisioned and user-provisioned resources and technologies. Exemplary practices (for institutionally provisioned technology and BYOE) can only be attained with a clear understanding of who needs or wants access to what and—based on those access needs and wants—of the types of security measures that should be in place to protect sensitive data and the systems on which the data live. The ECAR recommendations that follow reiterate sound IT security practices, with an emphasis on what matters most for BYOE.

Focus on securing data, not devices.

Data should reside on secure servers, be encrypted at rest and in transit, and only be accessed through secure applications or https.

Be an active stakeholder in managing access to enterprise-level systems, services, and data.

Role-based access and multifaceted institutional oversight authorizing personnel to access secure data and mission-critical systems should be well defined, understood, and followed. A functional system should be in place to edit, update, and audit roles and permissions as personnel change.

System and network audits and oversight are methodical.

Local data centers should be secured via key/keycard, access is permitted based on roles, and security of data centers is formally monitored. Cloud-based or off-site commercial data centers should have robust security and redundancy. Security audits should be routine, frequent, systematic, and comprehensive. Additional system and log monitoring outside formal audits is also an exemplary practice.

Identity management efforts are multifaceted.

Institutional priorities for identity management standards should be in sync with the capacity to effectively manage identities. Two-factor authentication to verify user identity access to sensitive data, mission-critical systems, and secure client applications is becoming common in higher education but is not universal. Mobile device authentication should be required if and when access to mission-critical enterprise-level services, systems, and data is essential and authorized from a user-provisioned device.

Be an advocate for educating users about BYOE security concerns.

As stewards of systems and data, IT shops are obligated to make a case for educating users about the risks and benefits of using their own technology. Motivate the adoption of smart security practices by addressing personal security issues simultaneously with institutional security issues.

Engage in activities that raise user awareness of security issues.

Have well-written, easily understood, and widely accessed policies on security for BYOE, but accept that good policy does not translate into good security.

Compliance can be monitored, and policies are enforceable.

All policies for BYOE security issues should be enforceable and enforced; IT has the authority and ability to shut down infrastructure or block users from networks when a security threat or breach is detected. If policy compliance can neither be tracked nor enforced, then repackaging the “policy” information as “guidelines” or “suggested use/behavior” or the like (to more accurately communicate the level of expectation for compliance) may be prudent.

Seeking out strategic innovations for security as it applies to BYOE is a collective and ongoing responsibility.

Innovations are happening daily, and instead of including innovations of today in this report that may not be applicable tomorrow, the *most* strategic innovation recommendations are to pay attention to what is happening today and to be forward-thinking about evolving and emerging technologies and how they will be adapted and used tomorrow.

The ECAR Queue

This consumerization of information technology/BYOE research preview on IT security provides a sneak preview of the work ECAR is undertaking to understand how the consumerization of IT is affecting higher education. In 2013, ECAR will produce a series of publications on this topic, and we are experimenting with opportunities to provide content throughout this research effort by releasing aspects of the study monthly. This report is the third in the series and was preceded by a summative research preview and an IT infrastructure report. The complete report and supporting materials will be released at the end of quarter one in late March. The project research hub (http://www.educause.edu/library/resources/byod-and-consumerization-it-higher-education-research-2013) will be updated as information about this project emerges:

- Full ECAR report on higher education BYOE
- Infographic, slide deck, and support materials

This suite of resources will provide actionable recommendations, which can be useful in developing or refining those elements of a comprehensive BYOE strategy that are within the purview of IT leadership, as well as perspectives about BYOE issues for which IT may not be directly responsible but that IT leaders will benefit from understanding.

About the Authors

Eden Dahlstrom (edahlstrom@educause.edu) is a Senior Research Analyst with EDUCAUSE. Stephen diFilipo (sdifilipo@gmail.com) is Vice President and Chief Information Officer at Cecil College.

Citation for This Work

Dahlstrom, Eden, and Stephen diFilipo. "IT Security in the Bring-Your-Own-Everything (BYOE) Era." Research Preview. Louisville, CO: EDUCAUSE Center for Applied Research, February 26, 2013, available from http://www.educause.edu/ecar.

Notes

[1] Eden Dahlstrom, with foreword by Charles Dziuban and J.D. Walker, *ECAR Study of Undergraduate Students and Information Technology, 2012*, Research Report (Louisville, CO: EDUCAUSE Center for Applied Research, September 2012), available from http://www.educause.edu/ecar, and Eden Dahlstrom and Stephen diFilipo, *IT Issues in the Bring-Your-Own-Everything (BYOE) Era,* Research Report (Louisville, CO: EDUCAUSE Center for Applied Research, forthcoming).

[2] Mark Sheehan et al., *Identity Management in Higher Education, 2011*, Research Report (Boulder, CO: EDUCAUSE Center for Applied Research, 2011), available from http://www.educause.edu/ecar.

[3] Ron Yanosky and Gail Salaway, *Identity Management in Higher Education: A Baseline Study,* Research Report (Boulder, CO: EDUCAUSE Center for Applied Research, 2006), available from http://www.educause.edu/ecar.

[4] EDUCAUSE Constituent Group for Security listserv “quick poll,” http://www.educause.edu/discuss/discussion-groups-related-educause-programs/security-discussion-group/two-factor-authentication-quick-poll.

[5] Two-Factor Authentication, Internet2 Dashboard, available from https://wiki.internet2.edu/confluence/display/itsg2/Two-Factor+Authentication.

[6] EDUCAUSE Constituent Group for Communicators listserv “deploying two-factor authentication tokens,” http://www.educause.edu/discuss/constituent-groups-about-information-technology-management-and-leadership/it-communications-constituent-group/deployi.

[7] Sarah Perez, “Jumio Brings Identity Verification to Mobile Apps—Just Hold Up Your ID to the Camera,” TechCrunch, February 21, 2013, http://techcrunch.com/2013/02/21/jumio-brings-identity-verification-to-mobile-apps-just-hold-up-your-id-to-the-camera/.