Shadow IT and BYOD—Conquering These Corporate Cousins

By Almi Dumi, Sr. IT Security Engineer / Team Lead, {e}Mazzanti Technologies

Keeping Up with Business Needs and Devices

Shadow IT is a dreaded aspect of cyber security. It is a world in which employees use services such as their private computer or, say, an iPad, to do their work without having obtained corporate approval. Standard Information Security protocols should apply to Shadow IT but because the devices are personal, enforcement is difficult. Shadow IT, when used across an enterprise, strongly illustrates that

- The company lacks up-to-date cyber resources;
- The company is unable to cope as requirements change for various departments;
- The IT infrastructure isn't flexible enough to cover evolving business needs.

Bring Your Own Device (BYOD) is a hugely popular and insidious piece of the IT puzzle, but unlike Shadow IT the practice is acceptable and approved by the company, which, in truth, has no choice because employees, consultants, and other remote users or third-party service providers use a variety of personal devices in their work.

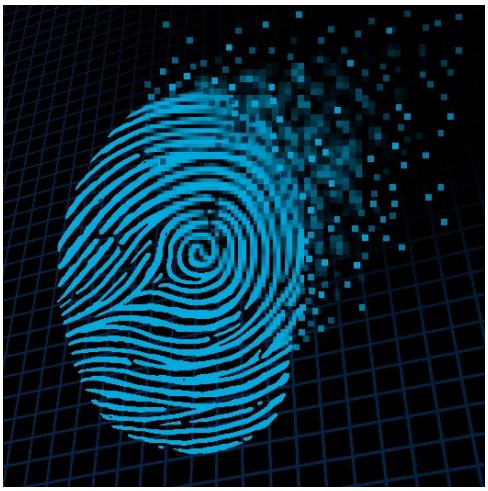
While BYOD may seem to be a practical solution for the modern workforce, and Shadow IT a natural consequence, both become an enormous challenge for information security, specifically with regards to safeguarding intellectual property. Protecting one's data is only truly feasible when the scope is within the logical boundaries of the company's network. It is therefore mandatory and well within the rights of IT security professionals to employ multiple layers of security to enforce a company's information security policies.

Security-first Mindset

IT staffers must be constantly trained, and often, as the cyber-threat landscape changes every day. Think of zero-day viruses and myriad threats the staff may be unaware of and vulnerabilities become readily apparent. The organization's security posture would be much improved with an educated and organized staff. Everyone—everyone— should be mindful of information security and operate with sensible, due diligence.

Information-security awareness programs and mandatory training must be implemented across the organization. It is vitally important to review and update these programs regularly to reflect today's threats and to elevate employees' awareness.

Multi-Factor Authentication



Organizations should use multi-factor authentication wherever possible**.** If there is a need to authenticate, there should be multiple authentication factors such as something one **knows** (a password) and something one **has** (a token), or perhaps an inherent biometric characteristic such as something one **is** (using a fingerprint, iris scan, voice recognition) or even something one **does** (perhaps a gesture).

Multi-factor authentication (MFA) is commonly used incorrectly as organizations end up using the same factor twice. Strong encryption and reliable intrusion detection and prevention mechanisms are basic requirements to protect data in transit and for BYOD users. Organizations should implement a defense in-depth strategy and constantly test defenses to ensure operation within established security standards.

Policies and Education Improve Security

There is something to be said about Acceptable Use Policies and appropriate controls when it comes to Shadow IT and BYOD. Security is the responsibility of everyone. Layered defense and a knowledgeable staff will reduce the risk of a security breach significantly and ensure prompt recovery.

Employees with access to information and third parties are most commonly targeted by social engineering attacks. Consequently, a company's staff is most vulnerable to being compromised, often unknowingly and unware, because they are an inside source with access to proprietary information. When asked why or how the typical reason starts with, "I didn't know..." Thus, the best advice for any organization to improve its security posture is to educate and protect its staff.