WHAT IS CONSUMERIZATION OF IT? THE STATE OF CONSUMERIZATION OF IT

In 2005, Gartner pronounced consumerization "the most significant trend affecting IT in the next 10 years." Here we are over 10 years later, and while the buzz about the consumerization of IT may have since died down, the effects of it have not.

Although the concept of consumerization may not be discussed everyday, it is something that is literally surrounding us constantly in the workforce, at home, and in transit. For something so all-encompassing, why does it hardly receive any notice? We have renewed the research on the topic and have put together some of our findings on the state of consumerization of IT.

What is Consumerization of IT?

Consumerization of IT is the cycle of technology emerging first in the consumer market and then spreading to business and government organizations. This phrase is favored largely because employees are first selecting popular devices and technologies as consumers, then introducing them to the workplace, as opposed to a few decades ago when new technology began at the enterprise level and slowly trickled down to the general consumer market.

This consumerization not only refers to the use of personal electronics at work, like smartphones, tablets, and laptops, but it also covers the use of online services, such as online data storage, social media, and web-based email services as well as personal applications downloaded onto work

devices. Consumerization of IT has also come to encompass user experiences and user interfaces that mimic consumer UX and UI – bringing context-aware experiences to IT users.

While the idea of employees using personal devices at work and company devices at home was prevalent in 2005 when Gartner first defined it, the consumerization of IT is even more widespread in 2018 due to all of the factors that drive it. A consumer-ized IT experience is often a key factor in establishing a broader digital workplace.

Drivers of consumerization of IT

The biggest driver of the consumerization of IT is employees who act as well-informed consumers that spend a lot of time doing their homework. Typically without the organization giving permission or even being aware that this is happening, these employees may:

- Buy their own devices
- Install their preferred applications
- Download personal online service accounts on the corporate network with the device

Another driver of this trend is that our modern workforce is growing increasingly remote, making the monitoring of devices and security protocols all the more complex. Employees working from home like the option of being able to use their personal devices for business, especially if they have a preference of one platform over the other. Also, as consumers, we usually stay up-to-date with the latest and greatest when it comes to technologies, while organizations don't have the ability to purchase new devices every year.

Some of the other drivers of the consumerization of IT include:

- The BYOD movement
- The use of social media
- Adoption of cloud applications
- User preferences for consumer-like interface

Let's look at each.

The BYOD movement

One of the biggest phenomenons of the moment is the Bring Your Own Device (BYOD) movement. BYOD describes the digital business evolution in which employees bring their own personal phones, laptops, and tablets to work or use them for work purposes.

The BYOD movement has many benefits:

- Saves employers money
- Decreases the daily burden on IT departments
- Increases user adoption

However, the amount of security threats it puts the organization at risk for can quickly outweigh these advantages.

In order to reap all of the positives from BYOD, it is vital that companies have frequent trainings to ensure compliance with security measures. It is also important that strong policies be put into place to protect the network and sensitive company data from hackers and cyber threats.

The use of social media

Along with employees wanting to use their own devices in the workplace, many of them also want to be able to access their various social media accounts. Even if employees only use these accounts during their lunch hour or during breaks, they may not be aware of how easily their actions could compromise organizational security and expose the network to malware.

This is another situation in which organizations must take proactive measures. Organizations must thoroughly educate employees about how a downloaded application or even a quick click on an infected link can compromise the entire network. They should also ensure employees don't share any confidential business information online, no matter how well-meaning they may be.

Cloud adoption

As more and more companies migrate to the cloud, being able to collaborate with team members across the office, or even the world, has never been more simple. However, with this ability to share documents, files, and data comes the added risk of that sensitive data becoming intercepted by cyber criminals.

To negate the risk of security threats, and fully embrace the benefits that adoption of the cloud has to offer, companies must use effective communication to employees regarding the correct ways to share confidential information and choose a secure password. Going one step further, IT departments must be confident in the network's encryption methods as well as the security of any type of sensitive data, whether it be in storage or in transit.

Consumer-like user interfaces

Users of IT services are people too – and have come to expect the same speed, accuracy, and power of their favorite consumer services like Google, Netflix, and Amazon Prime. Today's business users find real value in experiences that "just work".

Consumerization of IT in 2018 & beyond

In today's workforce, most businesses have some, if not all, of their employees working remotely and the consumerization of IT is being pushed by a generation that grew up with the internet. Due to the familiarity of always having devices available, these workers are more likely to blur the lines between personal and work devices, especially if they prefer a different platform than what their organization offers (Mac vs PC).

While the blending of devices is typically a benefit for employees, it is usually a huge headache for IT departments as well as security professionals. IT departments are forced to keep track of a much higher number of very mobile technologies that are being shuttled all over. They are also usually the first line of defense when these said devices get attacked with malware.

The amount of data that is accessed at every second from laptops, desktops, mobile phones, and even Internet of Things devices requires a team dedicated solely to cyber security and ensuring all sensitive information is protected. However, if employees are highly educated and trained on how to properly use and access their devices, the consumerization of IT in 2018 will be better than ever before.

Related reading

- BMC Business of IT Blog
- BMC Security & Compliance Blog
- Introduction To Enterprise Mobility
- Shadow IT Explained: Risks & Opportunities