The CLO's Role in Smart Computing

Learning leaders have to prepare to handle cyberthreats • BY ELLIOTT MASIE

Elliott Masie is the chairman and CLO of The Masie Center's Learning Consortium and CEO of The Masie Center, an international think tank focused on learning and workplace productivity. To comment, email editor@CLOmedia.com.

In discussions about major challenges or changes the learning field will need to face in the next 24 months, I always start with a surprising topic: cyberwarfare.

Witness the news reports about the Sony Corp. intrusion, the hacking of government databases or cyberattacks on Facebook and other major social networks. Corporations and their distributed workforces must be supported to address, respond to, defend and accept threats from cyberintrusion, cybersecurity and cyberwarfare.

There are several realities in 2015 that are shaping the cyber issues that will affect and play a role in learning organizations:

BYOD, open computing and cyber: More workers are using their own devices in a BYOD, or bring your own device, context. They will increasingly demand access to corporate servers and knowledge from a device that is neither purchased nor configured by the company's IT department. BYOD users will be given better access, but there will be a greater need for them to be aware and compute more safely.

Cyberwarfare: Many major countries, including the United States, have been building up cyberwarfare and cyberdefense capacities. For many years, these capacities have been working in the background off the news screens, but they are now out and public. Workers have to be ready to deal with intellectual property and communication security, especially when traveling globally.

Nonphysical cyberthreats: Workers could be in an airport lounge awaiting a flight while participating in a webinar from their tablets or laptops. Wearing a headset, it is easy to listen to and talk about a key topic. But who is sitting nearby listening? Cyberthreats also happen in the coffee shop: One of my colleagues had his passwords hacked while sitting in a coffee shop using wireless. Someone used a program to "sniff" the air for wireless communication and snagged his passwords, which were then passed along to third parties that committed commercial intrusion.

Cyberpolicy and onboarding: We will need to add cyber policies, realities, warnings and corporate approaches to onboarding processes for our new employees. We should make cyber issues part of orientation, promotions and manager development.

In a nutshell, learning organizations will have to step up and support the organization's cyberculture transformation. This new role will require:

- Subject-matter experts with cybersecurity competencies.
- Instructional design for knowledge domains on corporate cyberpolicies.
- Creating on-the-job assets, e-learning, MOOCs and performance support tools for cybersecurity readiness.
- Metrics to assess and measure cybersecurity readiness.
- Building case studies and role models for cyber issues.

Several realities in 2015 are shaping cyber issues that will affect learning organizations.

In the early days of PC training in the 1980s and early 1990s, we regularly trained our workers on IT security issues. I remember leading sessions about how and where to place data and what to do with floppy disks that had backups. Today, IT and learning leaders will need to shape cybersecurity culture efforts by doing an organizational assessment:

- What are the current knowledge assumptions about cybersecurity in the workforce?
- What are the biggest threat forces?
- Currently, what learning resources security is available and used for cyber?
- What prompts exist in the workplace to remind people about cyber smartness?

Finally, we must collect stories that can be used in future programs. Once, before traveling to a foreign country, I was advised by our government not to take a laptop. So, I purchased a new tablet and brought it with me empty. I did not access my corporate email server for the duration of my stay. Even so, the tablet was somehow "bugged" so that all data I would add in the future would secretly be sent back to that country. I only learned of the bug when I returned home and had the tablet checked, then wiped. Lesson learned. It was a personal and teachable aha moment.

Cyberthreats are real, and they are growing. We cannot and should not stop computing because of these new realities, but as learning professionals, we need to help our organizations shift to smart computing. CLO