ethikos Volume 34, Number 6. June 01, 2020

Cybersecurity and compliance in a pandemic

By Mac McMillan

Mac McMillan (mac@cynergistek.com) is CEO Emeritus at CynergisTek in Austin, TX.

Security has always had a love-hate relationship with compliance. The guiding principle of compliance is balance, and it, at some point, has a minimum—meaning sometimes even no security is acceptable if the mission is at risk, and when that mission is life or death, if necessary, no security is acceptable. That doesn't mean it is desirable or appropriate to ignore protections or not important to seek compensatory measures. But when everyone is moving as fast as they can and still falling behind and even simple tasks become difficult or nearly impossible, everything that isn't critical to the core mission becomes secondary—and rightfully so. It is at these times that security and privacy officials and their compliance counterparts have to shift their approach. The mission is still the same—to protect the organization and the patient—but it should be done without interfering with care or adding more stress to an already chaotic environment. The mission is to be truly essential.

Things are going to happen fast, decisions are going to be made without the normal afforded consideration. Moves are going to happen, people are going to be repurposed to fill critical shortages. New people are going to be introduced constantly; new systems and methods of treatment are going to be tried and implemented without the testing or structured implementations normally followed. People and processes are going to be relocated, the world as we know it is going to be turned inside out and move faster than ever. On top of all of that, the staff is going to be stretched thin, facing longer hours under increased stress. Over time, they will experience rest deprivation and countless highs and lows as patients suffer and recover—not to mention facing their own risks head-on every time they report for duty. All of this makes for an incredibly volatile environment where risks will be higher. Add to this the unfortunate reality that the criminal element will see this as an opportune time to exploit organizations, and you have the makings of real drama for security and compliance. That is exactly what needs to be quickly eliminated if security and compliance professionals are going to be successful and be an asset to the organization during this time.

Leadership

Security can't support what the leadership wants to accomplish without understanding something called "the commander's intent." The way to achieve that understanding is by being close enough to the leader as decisions are being made to hear and understand what the leader wants to accomplish. During crisis situations, the hospital will stand up its emergency operations command center, and the chief information security officer (CISO) should be in or have access to that command center. The CISO should be there to listen and gain an appreciation for where the hospital is heading so they can anticipate security challenges and direct security efforts to support appropriately. Compliance should press to make sure security is present so that their input is considered and that the risk decisions made and measures taken can be adequately documented. During crisis, there isn't time for relaying information through multiple layers. It should flow from the leadership to the CISO to their team so they know what and how to support more effectively. Compliance can assist leadership during crisis by supporting organizational command and control that facilitates effective communication of critical information to and from them.