

FREE for qualified industry professionals. Subscribe Now



CURRENT ISSUE

SUBSCRIBE

ARCHIVE SUBMISSIONS

ABOUT

MEDIA KIT

CONTACT

JULY/AUG/SEPT 2014



Should IT Security Be on My Radar?

With the growing importance of information systems in the modern enterprise, Sam Segran explains why senior executives need to have a pulse on cyber risks As told to Matt Alderton

Cyber security is definitely not a problem just for IT. A hiccup in computer security can impact any part of the business. Leaders from all areas-finance, marketing, HR-really need to be cognizant of the fact that a secure environment is a prerequisite for them to be able to do what they need to do for the business.

If you're doing it right, security is something you don't even notice. But if you're not doing it right, it's the one thing that can torpedo everything. If people gain access to your systems, they can destabilize your operations very quickly and derail whatever core mission you're working toward, whether that's doing business, building a brand, or protecting data.

If you're a business leader, you should ask yourself, "Do I know what security measures are in place in this organization? Have I received any information on how to be secure? Have I received information that tells me what to look out for?" If the answer is no, communication may need to happen between the CIO and institutional leaders. There has to be constant communication between IT leaders, other business leaders, and with end users. Everyone should be part of that information sharing mechanism.

Wi-Fi has increased. Mobile devices have increased. People are using a huge number of apps. The issue of cyber security is not going away. People need to constantly keep an eye out for new information and threats, and they need to share that information with each other. The power of social networking, after all, comes when people share good information, and one piece of good information is a warning about the dangers that exist out there. We should be helping each other instead of depending on the IT organization alone to keep us safe.

"If you're doing it right, security is something you don't even notice. But if you're not doing it right, it's the one thing that can torpedo everything you're doing." —Sam Segran

In the old days, the threat could be something as simple as a virus or a worm, or someone hacking into your system. Now we're seeing a combination of approaches. You have smart hackers, for instance, who have figured out new ways of injecting malware, such as getting people to click on something or sending an e-mail getting them to download something. One current method [involves them] calling to say, "We notice your computer has a problem; we can help you if you download this fix." It may appear like it's coming from Microsoft or another reputable company. People have a tendency to be conned by someone calling them like that directly, and once you get a payload on your system, it inherently takes over. It doesn't matter what kind of firewall protections you have at that point; it can cause a huge amount of damage.

Another concern is social media. We have a large community of people—33,000 students, plus faculty and staff-who are active social-network users. All that activity has an impact on the security posture of the university. It could be something simple. For instance, somebody sets up a password and a password recovery question, but the answer to the recovery question is posted on a social network, like where you went to high school.

Because of these risks, we spend a lot of time educating the community. New students, faculty, and staff attend an orientation session where we give them basic information to raise their awareness. We provide them with a safe computing website link and other information to protect themselves. We also tell them what kind of tools the university provides; in our case, we use Symantec software, which is provided free to all faculty, staff, and users.

It's not just within the institution, either; it's also how employees work outside it. Do they secure their systems at home, for instance? Do they know how to secure their home network? We provide information that increases their knowledge base so they can secure their home environment, as well. It's a huge challenge, and addressing it requires leadership at all different levels and in all different areas of the institution.

IT/TECHNOLOGY



