From the Sponsor EXECUTIVE FORUM **CYBER SECURITY**

Vampires and Cybersecurity

As Halloween approaches, our thoughts tend to veer to things that go bump in the night. One of the most popular frightening characters of lore are vampires, the un-dead creatures that suck the lifeblood out of their victims. Besides being scary, vampires are usually charming and attractive, at least until they sink their fangs into you! The protections against vampires are well known: wolfsbane flowers, garlands of garlic and sunlight will all keep a vampire at bay, and a stake driven through his heart will put him permanently out of commission. But, vampires have two advantages that they put to very good use. First, many people don't believe in them, they're not taken seriously so their victims don't watch out for them or take the necessary precautions. Second, with their handsome charm, they are able to convince their victims to throw away their garlic and approach them unprotected. In fact, folklore suggests that vampires cannot enter a house unless they are specifically invited in! Picture Dracula saying, in his best Bela Lugosi accent, "Come here!"

What does this have to do with cybersecurity? Everything, except that cyber threats are scary all year round!

Cyber threats include hackers trying to break into your computer systems, smartphones and databases, ransomware delivered through email phishing attacks, customer data or other sensitive information breached as the result of poor controls, or just plain old employee mistakes. Any or all of these can cause business interruption, fines, lawsuits and reputational damage that suck the lifeblood out of your business. Very scary indeed! And, just like with vampires, we're all familiar with the protections that can ward off these threats.

William M. Prohn

Managing Director, Dopkins Systems Consultants; Director of Information Technology

Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Having a well configured firewall and end-point (anti-virus) software are the wolfsbane and garlic of cybersecurity. As long as someone doesn't remove them they can be effective in preventing many attacks. Training and regular practice for users in identifying suspicious emails and websites can keep criminal hackers at bay. Strong passwords, kept secret, with multi-factor authentication (such as a separate key sent to your phone) help to ensure that only authorized people are accessing your systems and data. Well documented user permissions with limited access to data and files limit the damage that can be done if someone does manage to impersonate a valid user and login. Having a current, complete off-site and off-line backup can be a life-saving response when ransomware hits. Encrypting data stored in databases, and being transmitted via email is the ultimate protection for your confidential data, just like a stake through a vampire's heart.

Unfortunately, the comparison doesn't end there. The cyber threats have the same advantages as the vampires: some people don't believe, and others can be tricked into surrendering. Many business owners and their employees feel that there are definitely scary threats, but they simply don't apply to them. "I don't have anything a hacker would want to steal" or "We're too small to be a target" are common ways the threats are waved off. Hackers, like vampires, aren't that particular: any blood or any data will do to prolong their evil activities for another day. Large companies may offer a bigger payday, and might have more and potentially stronger controls, but the greater reward justifies a hacker targeting them. Smaller companies may result in a lesser haul, but without basic protections in place, they are "low hanging fruit" and susceptible to random hacks and ransomware.

Companies who have added technical protections (firewalls, passwords, permissions) can still be thwarted by the attractive allure of phishing emails and entertaining websites who beckon their users to "Come here!" Almost any employee can circumvent many of the protections that are in place by simply opening an attachment or following a suspicious link. Users must be taught and reminded that cyber threats are not myths, they are real risks to their personal data, their employer's success and their jobs. Business owners and managers should separate myth from reality for their employees and other users, identifying the threats and risks that the business faces and educating them on safe computing behaviors and other essential protections.

A modern-day vampire hunters kit for cybersecurity should include a complete inventory of technology (hardware, software and data), a periodic risk assessment to prioritize where to best deploy protections, an Incident Response Plan to guide the organization through the scary times of an attack or breach; and policies, training and practice for users to identify and react to threats. If you're still unsure about the scary monsters you face and what protections are best to ward them off, contact us. We'll be your Dr. Van Helsing.