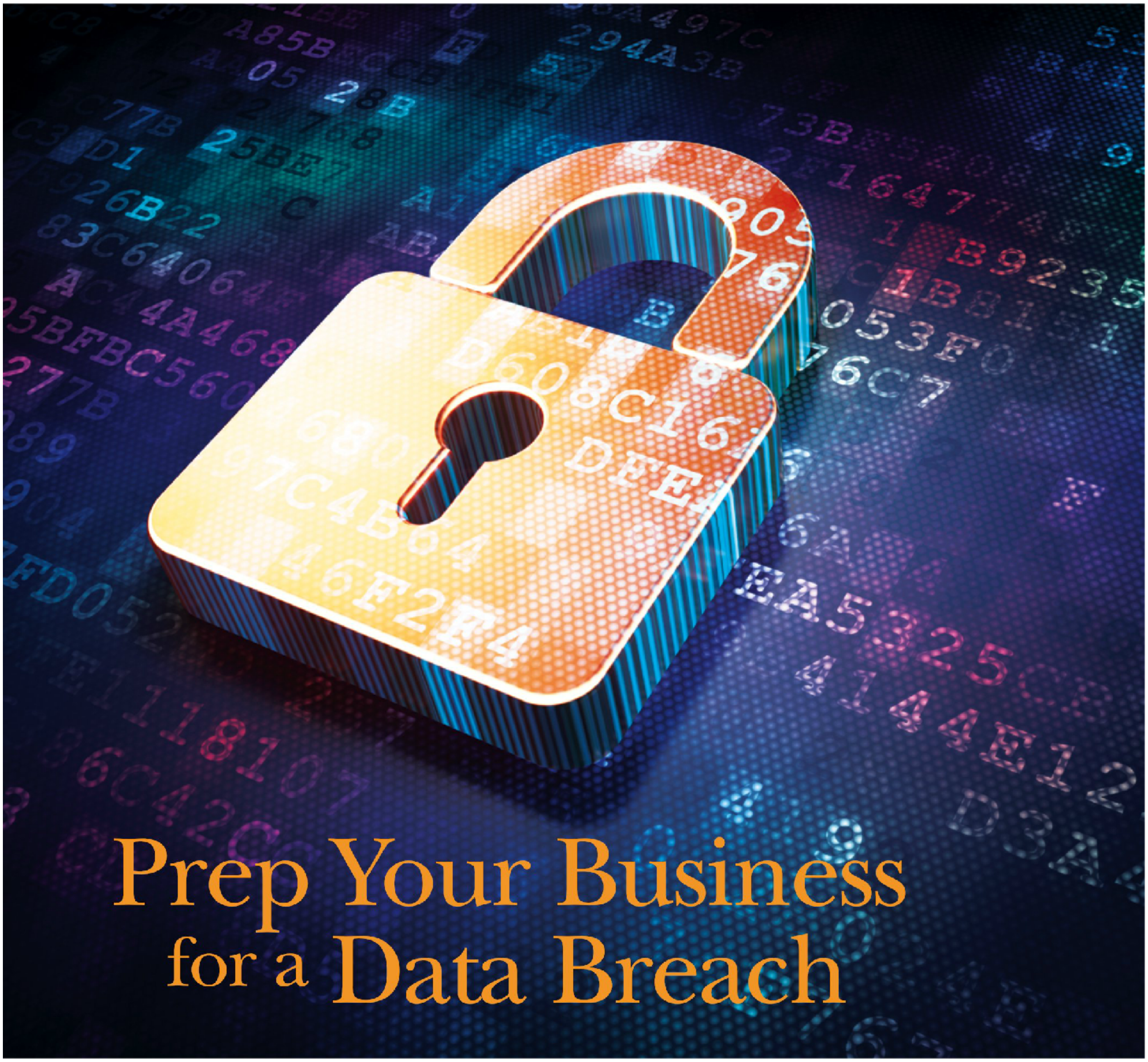


Prep Your Business for a Data Breach

By Pamela A. Keene

How vulnerable is your business to a computer data breach? Chances are you're not dealing with thousands of files containing Social Security numbers, protected health information or financial information belonging to other people. However, as the owner of a small- to medium-sized business, don't stop reading yet. You may not be safe from cybercrime.

What are the risks? Who or what poses the greatest threats? What protections are the most effective?

"Data breaches are much more common than most people think and at one time or another; between 40 and 70 percent of businesses will experience some kind of breach," says Steve

‘Data breaches are much more common than most people think and at one time or another, between 40 and 70 percent of businesses will experience some kind of breach.’
– Steve Vicinanza, Cirrity

Vicinanza, CEO and founder of Cirrity, a channel-only secure cloud solutions provider. “However, attacks come from a number of places, not just from overseas hackers or organized crime.”

It stands to reason that some industries require more protection than others. For instance, those that deal with health information, online commerce where credit cards are accepted, banking and financial services rank near the top of hacker targets. It’s becoming more common to hear about insurance companies, retailers and health institutions falling victim to massive breaches where identifying information is compromised or financial data is accessed.

“Typically the big breaches come from organized adversaries who are looking for personal information about customers, credit card data of business clients or banking information about the business itself,” says Andy Green, lecturer of information security and assurance in the Coles College of Business at Kennesaw State University. “The options are much more understandable for business owners today, and many software applications include protections such as encryption to help companies shield their data.”

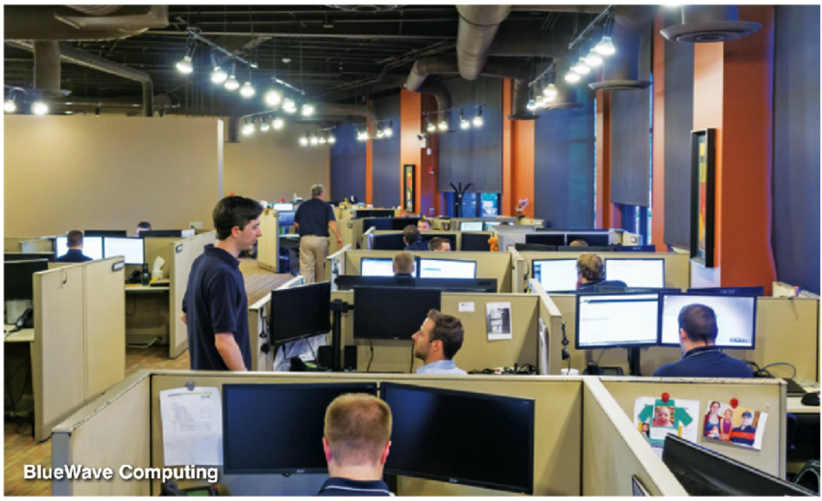
Different industries may need different levels of security. “If your industry is regulated, you need to protect your data specific to compliance regulations, which are stringent,” says Greg Chevalier, vice president of the information security group of BlueWave Computing, a Smyrna firm that provides information technology planning and support for small businesses. “Unregulated businesses must be sensitive to the security of their data as well, but they typically face a different type of risk — the one of losing business or damaging their reputation, but without the legal consequences. In either case, data security is an important and timely issue that everyone in business needs to recognize.”

Hossain Shahriar, assistant professor of information technology in KSU’s College of Computing and Software Engineering, teaches an “ethical” hacking course to help students find and identify system threats. “Once they know the system’s weaknesses, they’re better prepared to detect possible breaches,” Shahriar says. “They learn how to scan networks and discover what’s there, even if it’s not readily obvious.”

Shahriar pointed out that a large number of corporate breaches in recent months occurred long before they were detected. “Some were only found through routine data audits, after the damage was done.”

Times Have Changed

Steve Ryerse, president of Eclipse Networks Inc., has been in the IT business since 1989. “There was a time when we had to convince companies that they needed a network to effectively do business. No one connected to the Internet because it didn’t even exist and the only security issue you had was in transferring data between company offices through a telephone line,” he says. By the end of the 1990s, more people started to use email and surf the Internet, and that has led to greater risks.



BlueWave Computing

Photo by Karlis Robinson

Eclipse Networks Inc.

“Companies began to install firewalls to address possible intrusions from the outside and now almost everyone has them. In fact, I won’t let any of my customers do business without a firewall.”

Firewalls are just one way to protect company data. Firms now offer intrusion detection that will alert the firm when a threat has been detected. “We recommend a layered approach to our clients,” Chevalier says. “This includes annual risk assessments and penetration tests, plus ongoing content filtering and blocking. Attack methods are becoming more sophisticated and complex and companies’ networks have more possible entry points than ever before, including mobile devices.”

Installing firewalls, using internal servers and company-specific networks can help reduce the risk of a company’s data being hacked by outsiders. These tactics can also address the proliferation of viruses and malware that can shut down a company just because someone has downloaded an executable file that’s come in through an email or because an employee is browsing the Internet.

“Your IT person can also set up your company’s network to limit the number of people who have administrative rights,” says Jimmy Chum, lead instructor of information security at Chattahoochee Technical College’s Marietta campus. “It’s fairly easy to do and the employees who only have user-level rights can do just about everything on their computers except download or install software.”

Unintentional Breaches from Within

A user’s ability to install software holds the potential for extensive damage to computers and networks. Viruses and malware can be attached to emails and once opened, it infiltrates the system and does anything from corrupting data to shutting down the operating system. Sometimes it runs in the background of your computer and is difficult to detect.

“One of the newest threats is the crypto virus, sometimes called ‘ransomware,’” Ryerse says. “Once it’s released into your system, your data is hijacked and encrypted so that you can’t access it until you pay a ransom. And what’s to say that once you’ve been attacked that you won’t be again?”

Shahriar estimates that approximately 20 percent of data breaches originate from within the company, most unknowingly. “Employees being given more access than is necessary can create security issues,” he says. “Create and implement an access-control policy and define each employee’s role to add protections. Regularly audit access logs to monitor for possible unauthorized activity.”

Developing a written policy regarding data security is an invaluable first step to protecting sensitive files and data. It should cover such things as personal use of company computers and equipment, Internet browsing and the frequency of changing passwords. “One of your most robust defenses against data breaches is regular training of your employees,” Shahriar says. “It’s a people issue.”

Green goes one step further: “Where many organizations run into problems is not because of the technology. It’s because of the culture of the organization. Develop a strong and clear policy, keep employees informed and put controls into place with checks and balances. It’s not a matter of if you’ll have a data breach; it’s a matter of when. You need to be prepared.” ■

‘It’s not a matter of if you’ll have a data breach; it’s a matter of when. You need to be prepared.’

– Andy Green, KSU Coles College of Business