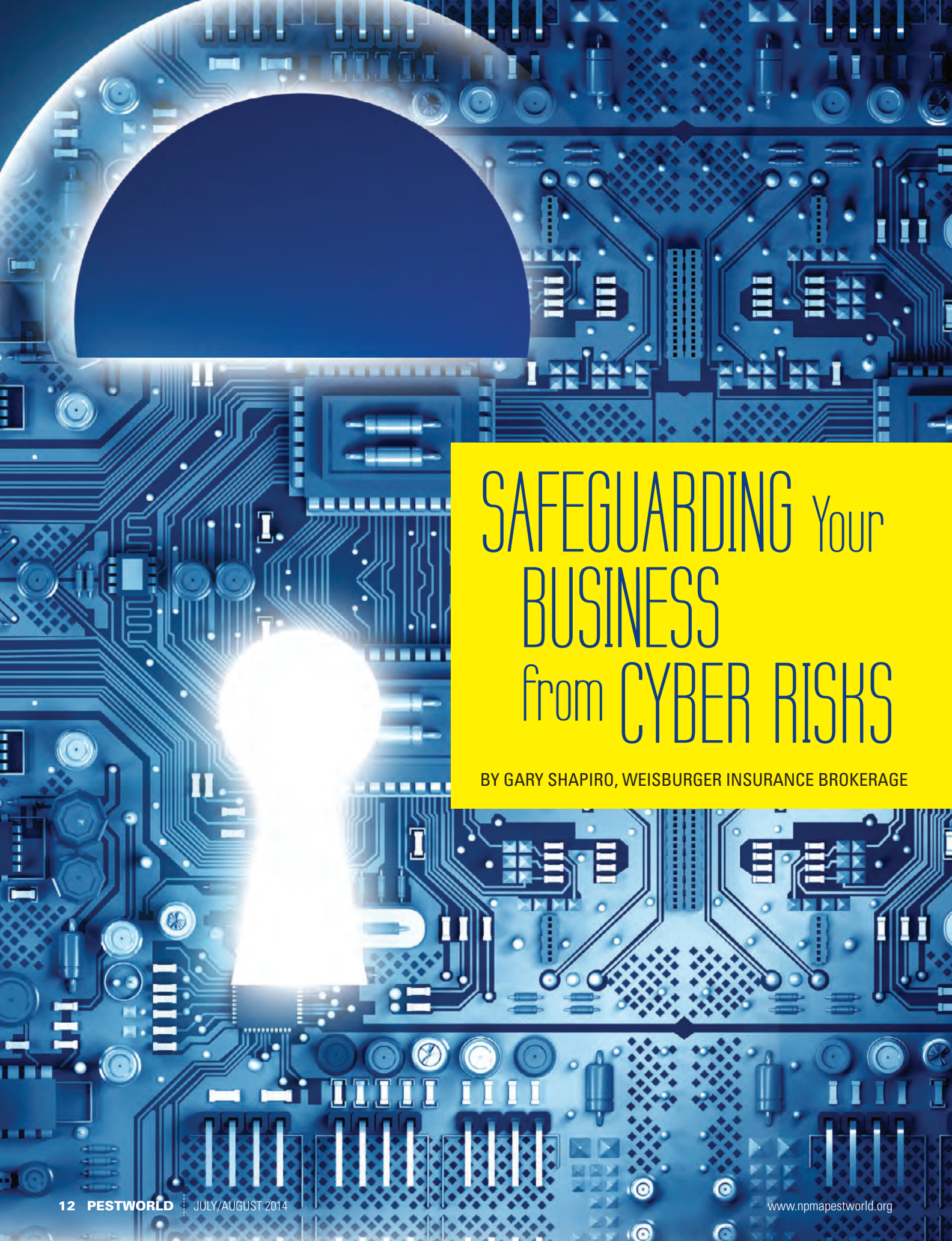

SAFEGUARDING Your BUSINESS from CYBER RISKS

BY GARY SHAPIRO, WEISBURGER INSURANCE BROKERAGE

CYBER sales are a critical and growing source of annual revenue for many businesses. With every "click" of the purchase button, shoppers put themselves at risk of having their personal information stolen—a risk that is typically absorbed by the businesses from which they are buying.

To protect a business against cybercrime, it is essential to take a proactive approach and have the right kind of insurance coverage. Every business has its own unique needs and risks, but there are some general guidelines outlined below that can help manage that risk and protect the business both in store and online:

IDENTIFY **the critical information a business has, needs and stores**

- Analyze the threat to that critical information. Questions to ask include:
- Does your business have an online sales/advertising component? If so, are you protected against the increasing threat of cyber risks?
- Is sensitive customer information stored on site?
- Do you have adequate protection if your site or online sales/advertising tools are compromised?

EVALUATE **the vulnerabilities to your business that would allow a cyber-attack on that data, and assess the impact of the attack.**

- Develop countermeasures to prevent and mitigate damage in the event of a cyber-attack by having sound response strategies in place. Such measures include:
- Evaluating the security settings on software, browser and email programs.
- Using one computer for online banking needs and using SecureID protection.
- Monitoring use of mobile devices and public Wi-Fi access for employees.
- Storing critical information through a remote server.

DEVELOP **the plan, implement it and communicate it to leadership and employees so they know their role and responsibility. Test the plan periodically and revise as necessary.**

While it is important to develop and implement safeguards against cyber criminals, these plans are most effective when combined with the proper insurance coverage designed to address cyber risks. Coverage typically includes liability protection for when customers or others who have been affected hold a company responsible for information stolen during data breaches or other network intrusions. A cyber policy also can include coverage for forensic investigation, litigation and remediation expenses associated with the breach as well as regulatory defense coverage, crisis management or public relations expenses, business interruption and cyber extortion.

Cyber risk is a very real issue that can impact a business and have a lingering effect on the business' ability to operate. Taking the proper risk management steps, as well as obtaining the proper insurance coverage, will help ensure that the business' bottom line is protected. «

One of the largest retail data breaches in US history occurred at Target Corporation during the 2013 holiday shopping season, exposing the personal financial information of 40 million shoppers. As this event demonstrates, your business is vulnerable to data breaches, even if you follow strict data security protocols. The following article underscores the need for cyber insurance.