—Reprinted with permission from PIA Management Services Inc.—

—Reprinted with permission from PIA Management Services Inc.—

RALPH LABARTA
Chief technology officer, Engage PEO

A great defense

Plan now to maximize your agency's value

Like companies across business sectors, insurance agencies have seen improvements in efficiency, client engagement and overall profitability through technology. Whether it is something as simple as enhanced communications and marketing through web-based channels, or as comprehensive as agency management programs and comparative raters, digital initiatives have changed the way that agencies—and individual agents—do business. Clients have greater access to information about unique insurance products, and those that provide insurance have a greater ability to demonstrate how their offerings meet the specific needs of customers. On the business insurance side, technology has also sparked new partnerships that have brought the mission of human resources and insurance closer together.

With these rewards come obvious challenges. Agency owners and managers must not only be experts in the products they offer and in general business management tactics, they must be tech-savvy too—or find the right partners to help them. Above all, they must learn about, and defend against, ever-changing cybersecurity threats.

The fact is that companies of all sizes, including small- and mid-sized organizations, are at risk of a cyberattack—one that could cause financial devastation. While many high-profile data breaches have focused on large global enterprises, such as Equifax, smaller organizations are, in some ways, in a more precarious position. This is because they often lack the resources or awareness to implement safeguards; and their networks can be used as gateways to the larger organizations that they may serve.

According to a 2017 research report by the Ponemon Institute, 61 percent of small- and mid-sized businesses experienced a cyberattack in 2017—up 6 percent from the previous year. Another report from the Better Business Bureau, the *2017 State of Cybersecurity Among Small Businesses in North America,* surveyed more than 1,100 companies about their understanding of and experience with cybersecurity. While a smaller number (about 20 percent) reported having been victim of a breach, of those more than 35 percent suffered a significant financial loss.

For insurance agencies, a primary concern is the protection of personal information relating to individual clients and business customers. But, agencies also must understand the need to safeguard their own financial information, assets and employee data. While cybersecurity threats are changing constantly, here are several key areas that should demand your attention today, along with strategies to keep your data, and your agency, safe.

Targeted phishing attacks

While phishing has been around for a while, and warnings about the practice are plentiful, it still ranks as one of the greatest threats to your agency. Emails with malicious content targeted at specific individuals in your organization will continue to be a grave threat, and the practice is becoming more specialized. For instance, spear phishing is a targeted attack when a malicious email appears to come from someone who you may know well; this email is specially sent to you, and perhaps a small group of your colleagues. The goal is to trick you or a member of your organization into providing valuable information, via false weblinks for instance. This information may include account numbers and passwords that can give an intruder access to your agency's network, customer data and bank information.

How can your agency combat phishing attacks? First, it is important to use an outsourced (cloud-based) email service provider such as Microsoft Office 365. These cloud-based programs provide advanced and constantly updated tools to block malicious links and phishing attacks, and they offer additional security options, such as mobile security. Since your in-house IT team may be small, and the bulk of your focus needs to be on your business, outsourcing is the best solution, offering teams of hundreds of engineers working to address email-based cyberattacks as they occur and evolve every day.

Second, make sure everyone in your agency receives ongoing technology training and support. Phishing works by targeting one of the most vulnerable links in an organization's technology structure—its people. By making sure your employees know to spot and avoid malicious emails, you provide a final layer of defense beyond your email provider.

IoT in the office

A common practice is to support wireless network access in office shared workspaces and to support employee devices and guests. This creates exposure to resources on the corporate network where the computers and servers are connected and confidential data is stored.

The vulnerability has expanded in recent years, as the Internet of Things has made its way into the office environment via smart TVs, connected appliances, alarm systems and other connected devices. The presence of IoT devices on secure networks introduces easily exploitable vulnerabilities that can be leveraged to gain access to secure resources. Hackers attempt to locate IoT devices within an office environment, access the devices and install malware.

To protect your agency, it is essential to make sure your wireless networks are segregated from the secure "corporate" network that stores your critical data. A separate internet connection should serve these segments, a task that can be achieved economically via broadband service providers that offer cable and internet services. All devices that present a security vulnerability, but contain no corporate data should use the "guest" network for internet connectivity. Then the corporate network can be dedicated to only allow secure wired connections to devices that have been approved or meet a minimum threshold of security compliance.

Remote-access attacks

The ability to work from anywhere is a convenience that often is characterized as a must-have for business management and executives. No doubt, your agency allows remote access to your network and/or email for employees to work from home or the field. Over the years, many vendor solutions have come to market to address the demand; however, the majority of solutions introduce security vulnerabilities that far outweigh the perceived benefits. Traditionally, remote access implies you are opening an access method to your secure network. When the front door to your house represents a possible opening to individuals in your immediate neighborhood, remote access represents a front door accessible to anyone in the world at any time.

The concept that employees need remote access to their office-based computers or server is outdated and represents a large security risk relative to the specific need, which is most likely, a specific file, email or customer record. Businesses should close outdated remote access points, and move to web-based file sharing, email and application suites that support multifactor authentication. As an example, instead of supporting remote access to an employee's office desktop, utilize a file sharing service such as OneDrive or Egnyte to which only specific shared file libraries are synchronized. When remote access to these files is needed, secure login with multifactor authentication can be used from any browser without exposing other data resources unnecessarily.

Home/public network breach

As phishing attacks become more specialized, attackers will focus on specific targets and the technology resources they utilize. An attacker will seek to identify the laptop of an individual with elevated rights or access to financial authorization. Tools that exist today can be used to monitor a laptop as it connects to the internet from the employee office, public Wi-Fi or home network. Network weaknesses or compromised devices on the same network can present an opportunity that can be detected automatically and trigger an attacker's bot to strike.

Your organization can take steps to combat the threat, beginning with the implementation of clear rules for employees to follow. When remote access is needed, employees should utilize cellphone hotspots to avoid shared Wi-Fi connections. Business laptops should be equipped with effective real-time virus and malware detection software including "DNS" filters that only allows access to a filtered list of internet sites. Home networks, particularly for employees with elevated rights, should be segregated to provide a secure connection that is not exposed to the employee's smart refrigerator, the gaming console or the smart thermostat. Business management and executives should consider employing the services of an IT services firm to assist in elevating the security of key employee home networks.

Preventing cyberattacks is critical not just for your agency's immediate financial security, but also for your reputation as a trusted and skilled adviser to your clients, and therefore your long-term performance. Remember that your business customers also are potential targets of hacking and malware, and so as you advise them on how to protect their assets and employees with the right insurance products, you should remind them of the importance of cybersecurity as well.

Today, some insurance agents work to provide their clients with value-added services, from IT support to employee communication. Many are doing this by working with professional employment organizations. While the idea of agents partnering with PEOs used to be met with a healthy dose of skepticism, the trend is changing direction.

Partnerships between insurance agents and the right PEO—one that offers attractive commissions to agents and high-caliber services to clients—are becoming more important. PEOs drive best practices, administrative efficiencies and savings through aggregation. The mission of PEOs extends beyond the administration of health insurance and related compliance—the industry leaders also offer payroll and tax administration; safety and risk management; worker's compensation administration; human resources and regulatory compliance support; and technology administration.

As agents move to take advantage of the many benefits that technology has to offer, they would be wise to guard against the dangers and to advise their clients to do the same.

In his role as Engage PEO's chief technology officer, Labarta oversees the company's technology and process innovation, including all customer-facing technology services. He has led technology operations and strategy and major product development initiatives for a national PEO as well as for leading companies in the chemical and energy industries. For more information, see engagepeo.com.