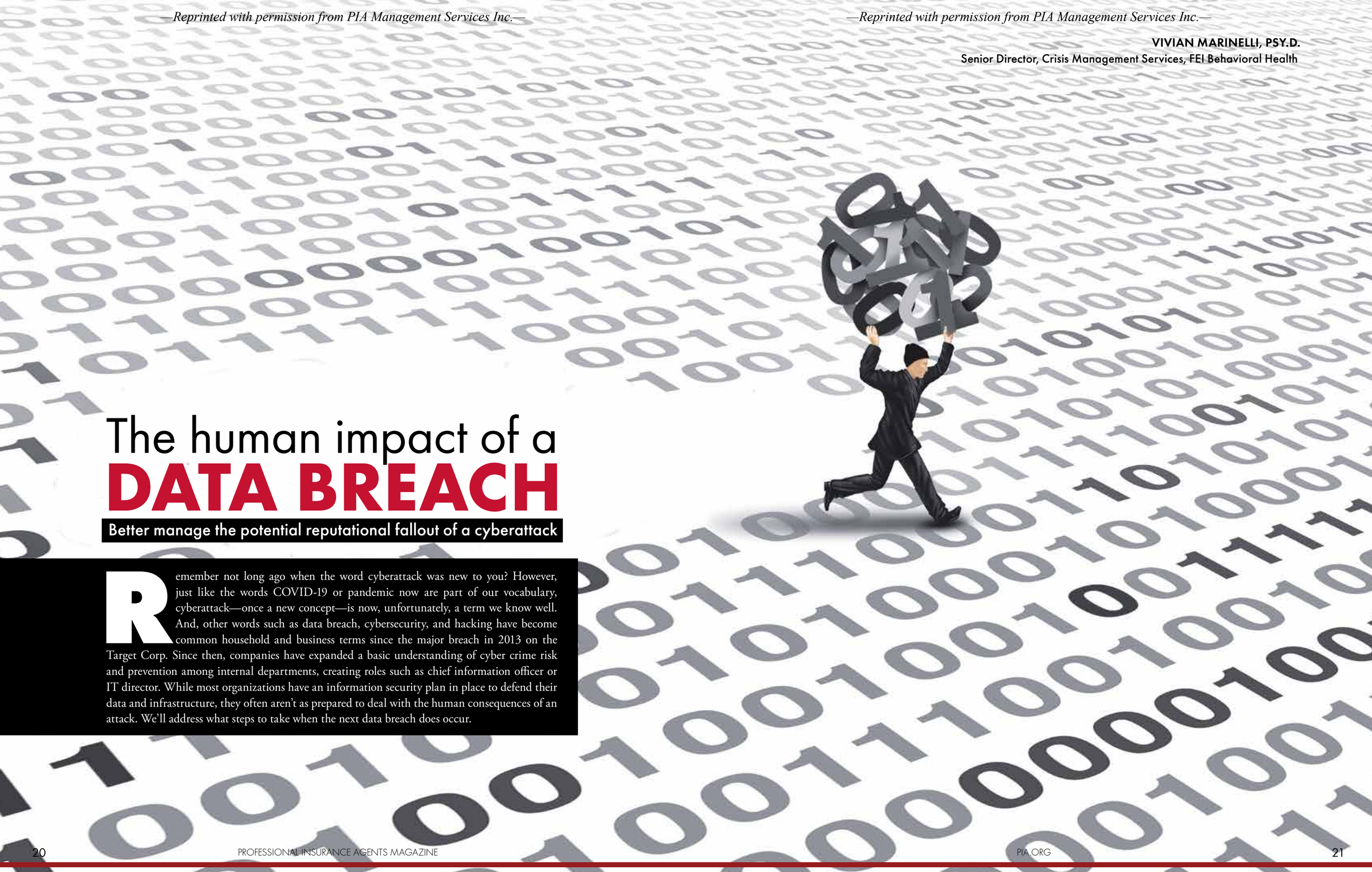
—Reprinted with permission from PIA Management Services Inc.—

—Reprinted with permission from PIA Management Services Inc.—

VIVIAN MARINELLI, PSY.D.
Senior Director, Crisis Management Services, FEI Behavioral Health



The human impact of a DATA BREACH

Better manage the potential reputational fallout of a cyberattack

Remember not long ago when the word cyberattack was new to you? However, just like the words COVID-19 or pandemic now are part of our vocabulary, cyberattack—once a new concept—is now, unfortunately, a term we know well. And, other words such as data breach, cybersecurity, and hacking have become common household and business terms since the major breach in 2013 on the Target Corp. Since then, companies have expanded a basic understanding of cyber crime risk and prevention among internal departments, creating roles such as chief information officer or IT director. While most organizations have an information security plan in place to defend their data and infrastructure, they often aren't as prepared to deal with the human consequences of an attack. We'll address what steps to take when the next data breach does occur.

Last year provided plenty of stress and uncertainty for all of us, including your clients. If you (or a bank or a credit card company) have to make a call to tell your clients that their personal information has been compromised, you can imagine how quickly the stress level will intensify. Cyberattacks can be stressful for victims, especially without advanced warning or time to prepare. It can affect victims at three levels:

Corporations. When an agency's sensitive information has been hacked, it ends up facing a lot of scrutiny. How could you let this happen? How does this impact the clients' information? What are you going to do to fix this? The perception of the agency's image will take a negative hit, especially in the media or with your customers.

Employees. Employees, too, are affected on a personal level as the first line of response for customers after an attack. Updating your staff about the planned response and support that will be communicated to customers is imperative for your agency to regain trust, create a unified message and build a positive image. Keep in mind your employees' personal information may have been breached as well.

Customers. Often the hardest hit during an incident. Their sensitive information has been stolen, usually under circumstances completely beyond their control or knowledge. It can be a traumatic and fear-inducing experience.

That means your agency must be ready to respond to and support each of the audiences in the days, weeks and months after a cyberattack. How to do that? It starts with a solid business continuity/disaster response plan. In a data breach situation, it will be your disaster response portion of the plan. The first step is identification of the breach. Once you have identified that an attack has occurred, you can begin to stop additional damages from happening. This involves a basic three-step approach for responding to a cybercrime:

1. Report the crime
2. Repair the damage
3. Prepare for re-victimization

Report the crime

Reporting the crime is complicated. It not only involves notification to authorities but also, notification to customers. That is also when the human impact will start. This is when the most fear, anxiety and need of support will occur. Depending on the size of your organization, the need to activate a call center may be necessary to notify the various stakeholders of the organization. Having the information about how the breach was identified and reported to authorities might help lower anxiety and fear.

Specifically, a good plan will outline a process for quickly assessing the scope of an attack's potential personal impact. It also will detail how the company will assist its customers and employees through elements like:

Set up a call center to assist customers. This might include an on- or off-site call center staffed by a crisis management provider, staff counselors, critical incident responders, and/or the human resource department. Many independent insurance agencies do not have the resources internally to support every victim of a cyberattack. Establishing relationships with outside vendors for support beforehand is vital, especially for the onslaught of calls that will occur within the first 48 hours after news of the data breach goes public.

Repair the damage

It is not uncommon for victims to run the gauntlet of anger, guilt, anxiety and fear of vulnerability after a data breach. These responses are understandable. An employee or customer whose data is stolen can spend years enduring the consequences. Remember, victims of cybercrime do not just lose a credit card or account passwords; they lose the sense of privacy and control over multiple aspects of their lives—from medical histories to Social Security numbers and identities—for an unknowable duration. Many times, a data security program will be offered to the victims for several years as a way to ensure no additional breaches occur. To help them, you should provide virtual or on-site counseling and support.

An organization must act as an advocate for the victims. Remember, this is not their fault. Affected organizations should:

Listen. You may be the first person to listen to what the victim is experiencing and feeling.

Provide information. You need to be able to provide details on what information was breached, what you are doing to ensure their data is safeguarded going forward and, how you are supporting them at this time.

Keep an open mind. Yes, the client or customer initially will blame the agency, but being proactive in reaching out and

being as transparent as possible will be most helpful during this difficult time.

Normalize your customer's feelings. Provide specific ways to help them decrease their sense of violation now and security in the future.

Prepare for re-victimization

As with any crisis scenario, potential challenges will likely arise in the moment. In the case of a cybercrime—especially one on a news-attention-grabbing scale—these might include the need to manage media leaks and press; the need to communicate relevant information in a timely manner, with limited or no use of technology; and the need to quickly address an influx of questions and concerns from customers and employees—both current and former, so it is important to update your continuity plan to maintain business operations.

Like any crisis plan, a cyberattack response plan is only as good as the training behind it. Most cyberattacks come from innocent-looking emails with attachments that get opened (i.e., phishing). These emails look like they are from someone you know, but actually are from hackers. Once a link is clicked, it opens the door for hackers to gain access to sensitive information. All employees should be educated on cyberthreats, so they increase their awareness and they can report anything that appears suspicious.

Protocols to assist your customers and employees. The follow-up in the aftermath of a cyberbreach can be overwhelming for the victim. It also can be overwhelming for company staff. An employer-sponsored

Employee Assistance Program can help employees in two ways. In the case of an internal breach, EAP counselors can connect staff to resources and guide them through the sense of loss and confusion by providing telephonic and face-to-face support. In an external or customer-facing breach, the employees themselves may need support after dealing with frustrated and frightened customers. An EAP can offer that extra in-person or telephonic group support in the form of a debriefing, which will allow employees to share their experience and concerns. It also will allow information to be shared from the organization on additional support and resources for the employees as they continue to work through the situation.

Continue to communicate and update. The last point—ongoing updates and communication—cannot be stressed enough. In a culture reliant on technology for a steady flow of information, separation from a business's network in a time of crisis can be disorienting and chaotic. It is difficult to send an all-customer email when the corporate email system is down or vulnerable. Instead, proactively establish communication protocols that rely on phone, text, social media (your Facebook page) or face-to-face interactions.

Helping new hires to avoid pitfalls. As part of the onboarding process (or as a refresher for all staff), new employees should be warned to:

- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known. Be particularly wary of compressed or ZIP file attachments.
- Avoid clicking directly on website links in emails. Instead, users should type the link directly in the browser's search bar or attempt to verify web addresses independently (e.g., contact the organization's help desk or search the internet for the main website of the organization or topic mentioned in the email).
- Log off or use a screen saver when not in front of a computer.
- Report any suspicious emails to your help desk or security office immediately.
- Avoid unsecure Wi-Fi hotspots. If employees currently are working remotely, make sure they have a secure log in. Any time an employee connects to public Wi-Fi, the data on a company's server is open for hacking. It goes without saying that airport and hotel Wi-Fi is another concern for employees who (used to) travel frequently.
- Be smart about peer-to-peer file sharing. Sharing files via flash drive is akin to a college student sharing a drinking cup. Instead of spreading germs, the drives potentially spread viruses.
- Avoid downloading software or apps from unknown sources.
- Maintain good password integrity, with the option to change passwords regularly.
- Be smart about laptops or mobile devices that float between systems and could, therefore, pick up viruses or compromise the system.

After reviewing technology protocols with new hires, you need to provide learning opportunities for identifying potential threats. Send a mock-questionable link to employees to see if they click on it, and implement consequences when an employee leaves the agency open for a cyberattack. Cyber security training is not a one-time event or something that only applies to the IT Department. It should be treated as an ongoing process and include employees across the agency's footprint.

Attacks against information technology infrastructure have a devastating impact for businesses of any size. The operational repercussions extend beyond the agency's walls to vendors, customers, partners and prospects. Following the above suggestions will help your agency stay resilient and better manage the potential reputational fallout a data breach can have on your organization.

FEI has a 40-year history in enhancing workforce resiliency by offering a full spectrum of solutions, from EAP and organizational development to workplace violence prevention and crisis management. For additional information, visit www.feinet.com. Marinelli provides consultation with customers on behavioral health as well as emergency preparedness, crisis response, and family assistance issues. She is experienced in the development of curriculum and training of FEI affiliates to serve as crisis support coordinators, and employees to act as peer support facilitators. She brings over 15 years of work in direct clinical services specializing in trauma and grief counseling to her position, which focuses on assisting individuals involved in critical incidents.