CARLTON FIELDS

Here Are Seven Phrases That Can Help Your Business Avert Cybersecurity Attacks

January 31, 2020

It starts inconspicuously enough with an email. You're busy, so without thinking, you quickly open it and view the attachment. You may have just compromised the security of your entire company and the privacy of every client.

The headlines speak for themselves. According to Risk Based Security research, 4.1 billion records were breached in the first six months of 2019 alone. Florida has not escaped the trend. More than half a dozen Florida municipalities fell victim to cyberattacks last year, including ransomware attacks that brought government operations to a screeching halt and resulted in hefty ransom payments. When ransomware took down Lake City government's servers, phones, and email, the city agreed to pay a $460,000 ransom. Within weeks, Riviera Beach agreed to pay $590,000. Verizon reports that such attacks are one of the most common types of attacks, and McAfee LLC found that ransomware attacks more than doubled in 2019.

As large ransom payouts continue, we can only expect more of the same. A handful of simple steps, however, can go a long way in preventing and mitigating the consequences of these types of attacks:

▪ **Know thyself:** Cybersecurity is not a one-size-fits-all issue. It needs a customized approach tailored to the organization. So, step one: know your business. Think about what information you have, where it's stored, and the potential impact a breach could have on your business's activities. Would the biggest impact be to your supply chain, your trade secrets, the resulting breaches of contract? Once you know your greatest vulnerability, you know where to start. Cybersecurity is a business risk like any other. Evaluate your risks and your risk mitigation options. Prioritize mitigating whatever risks would have the biggest impact on your business. Document your efforts. If a breach happens and litigation ensues, you'll need to show you acted reasonably. Prepare now. Know your industry and the most common threats targeting it.

▪ **It takes a village: Get more people involved.** Different organizational roles within your business will have different ideas about the cyber risks most relevant to your business, as well as what resources they'd need in place to mitigate those consequences and recover from an attack. They know the information they need, where it is kept, and what problems would arise without it.

▪ **People are your greatest asset, and weakness: Train your employees.** Human error remains one of the leading causes of breaches and training one of the most cost-effective aids. Once they're trained, test them. Send fake phishing emails to make sure people are following through. The only thing worse than not having a policy is having one you don't follow.

▪ **Keep it simple: Don't let your cybersecurity discussions get stuck in technical jargon.** You do not necessarily need to be tech savvy to be cybersecurity-smart. IT security is important, but it is only one part of cybersecurity. Make sure your non-IT and information security staff understand the key concepts so that they can help identify and mitigate risks.

▪ **Keep up with the times:** Time and again we see massive breaches resulting from known vulnerabilities. Make sure you're timely applying any necessary patches, implementing security updates, and taking other measures to strengthen your systems.

▪ **Prepare for the worst: Make yourself as low-risk as possible:** Don't collect or hold onto data you don't need, protect the data you have, and back up your data regularly. Backup systems give you options. And Buy cyber insurance. You may never need it, or it may prove critical to helping your company recover from a breach. If nothing else, the policy likely provides access to experienced breach counsel and forensic firms, whose expertise may prove indispensable when responding to a breach.

▪ **Practice makes perfect:** You must have and rehearse an incident response plan, which is the organization's playbook in the event of an incident. The plan identifies the team, how to reach them (including after hours), contact information for external resources (such as insurance professionals, counsel, and forensic firms), and how to investigate and respond to an incident. The plan should be tailored to your organization and tested. According to the Ponemon Institute, companies that have and extensively test their incident response plans save more than $1 million in costs after a breach.

As ransomware continues to evolve, these steps become only more important. The better we meet the threat, the less ransomware we'll see.

Reprinted with permission from the *Miami Herald*.

Authored By

Patricia M. Carreiro

Related Practices

Cybersecurity and Privacy