FEAR NOT THE BREACH

Cybersecurity expert THERESA PAYTON says don’t wait until you’re in the middle of a breach to formulate plans. Write your cybersecurity playbook now.
Modern technology advances quickly. What’s innovative and fresh one day can be quickly outdated and short-lived in just a few months.

As smart devices get smarter, business and industry depend more heavily on them and the data they store, which makes fraud examinations more challenging and complex.

In college, I recall enduring one semester of BASIC language before I realized that there was nothing “basic” about it — at least for me. As CFEs, we don’t necessarily need to be computer scientists to operate in today’s tech society, but we do need to be aware of the current methods that fraudsters are using to steal from our companies and disrupt our lives.

Cybercriminals will keep changing tactics to bypass security measures and attack our systems. We must stay vigilant in our protection and detection efforts. Many cyberattacks are preventable through awareness, training and education. Even something as simple as updating software can make all the difference.

Teresa Payton, former White House chief information officer and keynote speaker at the 30th Annual ACFE Global Fraud Conference in Austin, delivers just such a message in the cover article.

“Cybercriminals change tactics daily,” Payton says. From sophisticated phishing schemes to ransomware attacks, these fraudsters exploit vulnerabilities within our information systems. Likewise, CFEs must also stay up to date on these nefarious trends if we want to fight fraud effectively and successfully in the 21st century.

But it’s not just a data or financial protection issue. The reputational risks we face from a cyberfraud attack impact our organizations tremendously. Not only must we be watchful for the attack, we also must have plans in place to remediate quickly should it happen.

“Awareness and education shouldn’t be one time a year and solely focused on compliance,” Payton says. Amen. Just as proactive data monitoring increases the ability to detect and prevent fraud, continuously updating your staff — all — your staff on these cyberfraud trends can be very effective. As we implement anti-fraud training and education more and more in our workplaces, the median life of a fraud declines. The ACFE Report to the Nations proves just that.

Payton warns us that we need a “[n]ew line of thinking” for our cyber training and to “practice a digital disaster before you have a breach.” We can’t hide from technology — it’s here to stay. But just as digital devices get smarter every year, so too must fraud examiners get smarter by staying on top of the latest schemes and the ways to combat them. — FM

Bruce Dorris, J.D., CFE, CPA, is president and CEO of the ACFE. Contact him at President@ACFE.com.
## Cover Story

### Fear not the breach! Write your cybersecurity playbook now

By Dick Carozza, CFE

Cybersecurity expert Theresa Payton says don’t wait until you’re in the middle of a breach to formulate plans. Develop a playbook so everybody knows their roles. Practice digital disasters. Line up your external helpers. Devise your communication strategy. Then, if you’re breached, cooler heads will prevail.

## Features

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>Global anti-fraud regulations</td>
<td>Mani Padmanabhan, CFE</td>
</tr>
<tr>
<td>32</td>
<td>Dark world of oil theft and fraud</td>
<td>Anastasia Nazarova, CFE</td>
</tr>
<tr>
<td>40</td>
<td>Bad leaders? Increased fraud</td>
<td>Donn LeVie Jr., CFE</td>
</tr>
<tr>
<td>44</td>
<td>Global fraud is the same — legal systems aren’t</td>
<td>Dr. Joseph T. Wells, CFE, CPA</td>
</tr>
</tbody>
</table>

Keep ahead of fluid global anti-fraud regulations

Bad leaders? Increased fraud
Hidden consequences of poor leadership

Global fraud is the same — legal systems aren’t