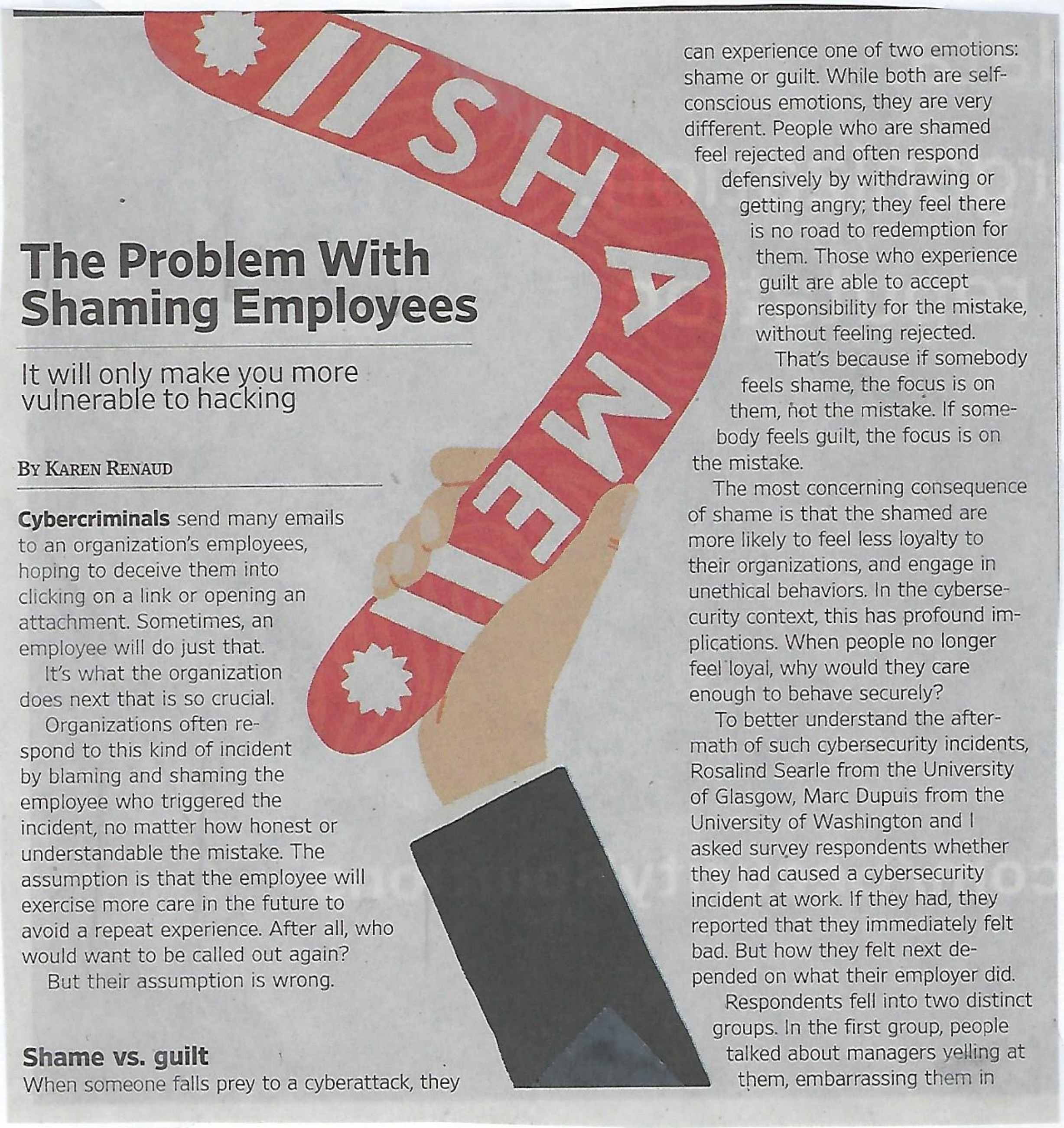
The Wall Street Journal   **December 8, 2021**

"Journal Report: CYBERSECURITY"

****

"The Problem with Shaming Employees"

It will only make you MORE vulnerable to hacking.   **by Karen Renaud**



The Problem With Shaming Employees

It will only make you more vulnerable to hacking

By Karen Renaud

Cybercriminals send many emails to an organization's employees, hoping to deceive them into clicking on a link or opening an attachment. Sometimes, an employee will do just that.

It's what the organization does next that is so crucial.

Organizations often respond to this kind of incident by blaming and shaming the employee who triggered the incident, no matter how honest or understandable the mistake. The assumption is that the employee will exercise more care in the future to avoid a repeat experience. After all, who would want to be called out again?

But their assumption is wrong.

Shame vs. guilt

When someone falls prey to a cyberattack, they can experience one of two emotions: shame or guilt. While both are self-conscious emotions, they are very different. People who are shamed feel rejected and often respond defensively by withdrawing or getting angry; they feel there is no road to redemption for them. Those who experience guilt are able to accept responsibility for the mistake, without feeling rejected.

That's because if somebody feels shame, the focus is on them, not the mistake. If somebody feels guilt, the focus is on the mistake.

The most concerning consequence of shame is that the shamed are more likely to feel less loyalty to their organizations, and engage in unethical behaviors. In the cybersecurity context, this has profound implications. When people no longer feel loyal, why would they care enough to behave securely?

To better understand the aftermath of such cybersecurity incidents, Rosalind Searle from the University of Glasgow, Marc Dupuis from the University of Washington and I asked survey respondents whether they had caused a cybersecurity incident at work. If they had, they reported that they immediately felt bad. But how they felt next depended on what their employer did.

Respondents fell into two distinct groups. In the first group, people talked about managers yelling at them, embarrassing them in

15%

of U.K. employers name and shame employees for cybersecurity incidents

33%

decrease access privileges

63%

inform the employee's line manager

17%

lock them out of their computer until they complete remedial training

Source: John M. Blythe et al., "Human Cyber Risk Management by Security Awareness Professionals," 2020, based on Qualtrics survey of 45 cybersecurity professionals

front of their peers and not trusting them after the incident.

It was clear from their comments that these employees felt shame and rejection, and that the employer-employee relationship was damaged, perhaps irretrievably.

Those in the second group said that their mistake had been met with understanding and support. They were told how to repair the situation. The consequence, in contrast to the other group, was a much stronger relationship between the employer and employee after the incident, and a desire to do better in the future.

Boomerang

What does this mean for organizations? The destructiveness of shame, when used as a behavioral-modification tool to bring employees into line, leads to a situation where no one wins. This doesn't mean that employees aren't held accountable for their mistakes. What it does mean is that the focus should be on helping the person to correct their mistake and do better in the future.

The implications of our survey were clear: Shame is similar to a boomerang that will come back to hurt the organization, as well as harming the employee. Managers should deal with the mistake, but *not* reject the employee. If employees feel that their personhood is being attacked, they will respond defensively. Shaming results in a lose-lose outcome.

Employees can be an organization's greatest asset when it comes to defeating the efforts of cybercriminals. Using shame as a behavior modification tool squanders that potential. And that's the real shame.

Dr. Renaud is a chancellor's fellow at the University of Strathclyde in Glasgow, Scotland. She can be reached at ***reports@wsj.com.***

FROM TOP: JAVIER JAÉN; MICHAEL PARKIN