July 2019

Security Awareness News

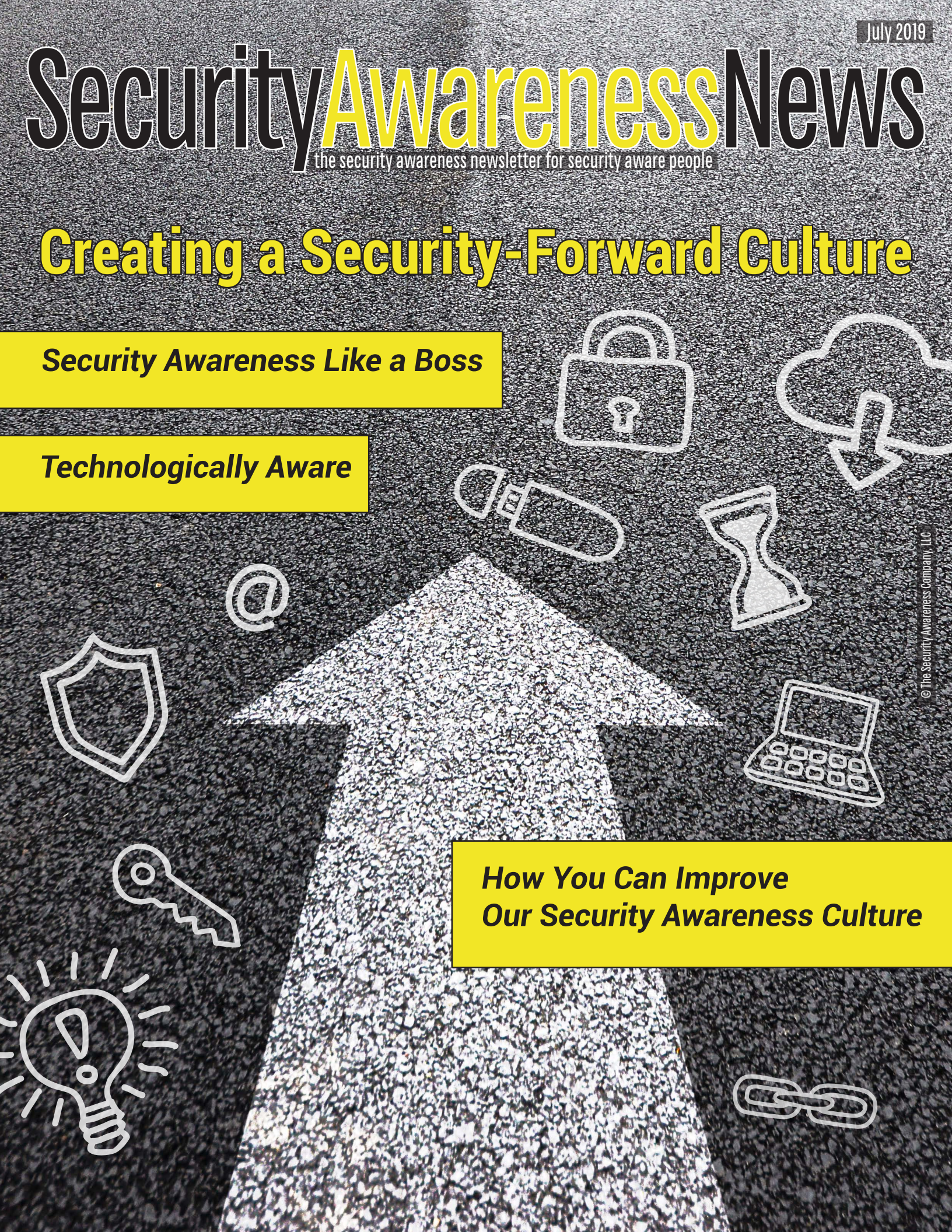
the security awareness newsletter for security aware people

Creating a Security-Forward Culture

Security Awareness Like a Boss

Technologically Aware

How You Can Improve Our Security Awareness Culture



Security Awareness Like A Boss

The success of most organizations heavily depends upon management. Good management yields a healthy business. Similarly, good security awareness from management improves an organization's overall security culture. That's why it's imperative that owners, CEOs, and all upper-level employees develop proper security habits and set the tone of awareness for their organization.

3 Habits of Secure Senior Employees

1. **Participating in the organization's awareness training program.**
   When executives participate in training, they positively reinforce the importance of the organization's security and how it applies to everyone from the front desk to the CEO. They also keep their awareness skills honed, which bears added importance considering that upper-level employees are top targets for cybercriminals.

2. **Following organizational policies.**
   There may be managers who feel that certain policies don't apply to them. Perhaps that's true in some cases. But not only does following the same policies required of all employees set a great example, it also aids in eliminating unnecessary risks.

3. **Holding all employees to the same security standards.**
   It's important to ensure that every employee in your organization is held to the organization's security standards. Allowing certain employees or departments to circumvent policy (in order to complete a project on time, for example) sets a dangerous precedent.

Four Eyes and Avoiding CEO Fraud

CEO fraud, or business email compromise (BEC), occurs when a cybercriminal spoofs the email address of an executive and uses it to email employees specific requests for wire transfers of money.

To see it in action, check out this article that includes the entire email thread of a real-life BEC attack: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/here-is-an-email-thread-of-an-actual-ceo-fraud-attack/

Executives can prevent this from happening by:

1. **Empowering employees with awareness training so they can identify when they're being scammed.**
2. **Implementing a "four eyes" principle, which simply requires two people to authorize certain transactions.**
3. **Limiting the amount of personal info you make public in order to deter social media data mining.**
4. **Thinking before you click. Scammers use advanced phishing techniques that target high profile individuals.**

Technologically Aware

Four engineers get into a car. The car won't start.

The mechanical engineer says: "It's a broken starter."

The electrical engineer says: "Dead battery."

The chemical engineer says: "Impurities in the gasoline."

The IT engineer says: "Hey, I have an idea. How about we all get out of the car and get back in."

All jokes aside, security awareness isn't something we can just turn off and on again to fix a problem. It requires your full attention, both at work and at home, even for technologically-inclined members of our organization!

5 Action Items for the IT Crowd

ONE **KEEP SYSTEMS CURRENT** • Out-of-date devices and software are common attack vectors for cybercriminals. Those in charge of updating systems need to stay on top of recent security flaws and ensure our systems and devices receive the latest upgrades as soon as those upgrades become available.

TWO **AVOID SHARED ACCOUNTS** • Sharing accounts with multiple users limits your ability to manage and audit the account, or keep a track record of who made what changes and when. It also makes offboarding and credential updates more difficult, among the many other risks associated with shared accounts. Wherever possible, require individual accounts for every person and avoid using services that don't offer multiple accounts.

THREE **MANAGE PERMISSIONS** • The more people who can make high-level, high-impact changes, the higher the risk of something going wrong. To protect both yourself and the organization, allow the least amount of privilege needed to perform a function. For employees who are granted higher access, require them to always log in with limited privileges and to selectively elevate only when needed. This limits any potential security incidents to having a more localized effect, as opposed to a global impact.

FOUR **DON'T MAKE ASSUMPTIONS** • Never assume that your co-workers, your bosses, or your teammates know about a particular vulnerability or a security risk just because it seems obvious to you. Keep in mind that not every member of our organization is as tech savvy as you may be. So, use clear, timely communication to spread knowledge and help ensure that nothing gets missed.

FIVE **FOLLOW ORGANIZATIONAL POLICIES** • Even if you're the one to write and enforce policies for other end-users, it's also your responsibility to lead by example. Employees with a higher understanding of the technical operations of our organization should also understand the risks those policies are designed to eliminate, and therefore should know the importance of following those same policies.

How *YOU* Can Improve Our Security Awareness Culture

BY TAKING TRAINING SERIOUSLY

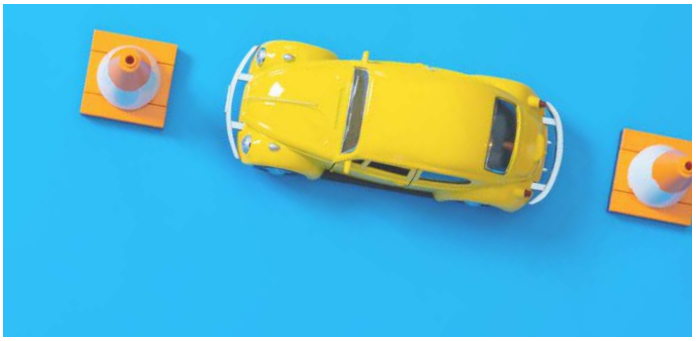
We know training sometimes feels unnecessary and can get in the way of actual job functions and schedules. But it is essential for maintaining a healthy, security aware culture. Without training, the likelihood of security incidents increases. Every incident could result in massive financial repercussions, as well as destroyed relationships with our clients, customers, and partners. They can even permanently tarnish our reputation.

BY TAKING TRAINING HOME

Security awareness doesn't end when you clock out. Your households and families deserve protection, too. That's why we encourage you to take what you learn about security here at work and apply it to your personal life. At a minimum, you should require strong password practices and enforce social media policies (share less!). Those of you with kids especially need to develop a security aware culture at home.

BY REPORTING INCIDENTS ASAP

Incidents happen. The only way we can mitigate the damage they cause is with swift action. If you find a random USB drive, for example, do you wait until after a meeting or after lunch to report that drive? Or do you turn it in immediately? The longer potential incidents go unreported, the longer we're exposed to vulnerabilities.



BY ALWAYS FOLLOWING POLICY

Our policies exist to reduce security incidents and increase the overall strength of our organization's security culture. No one is above those policies and circumventing them for any reason exacerbates our risk profile. If you want more information or clarification on our policies, please ask!

What do we mean by Security Awareness Culture?

Culture traditionally refers to the shared customs, arts, and other characteristics of specific groups of people. Similarly, the security awareness culture of an organization refers to the shared human effort of information security. Our primary goal is to spread awareness and empower individuals to know how to identify threats, know how to react to those threats, and know how to protect our organization and themselves.