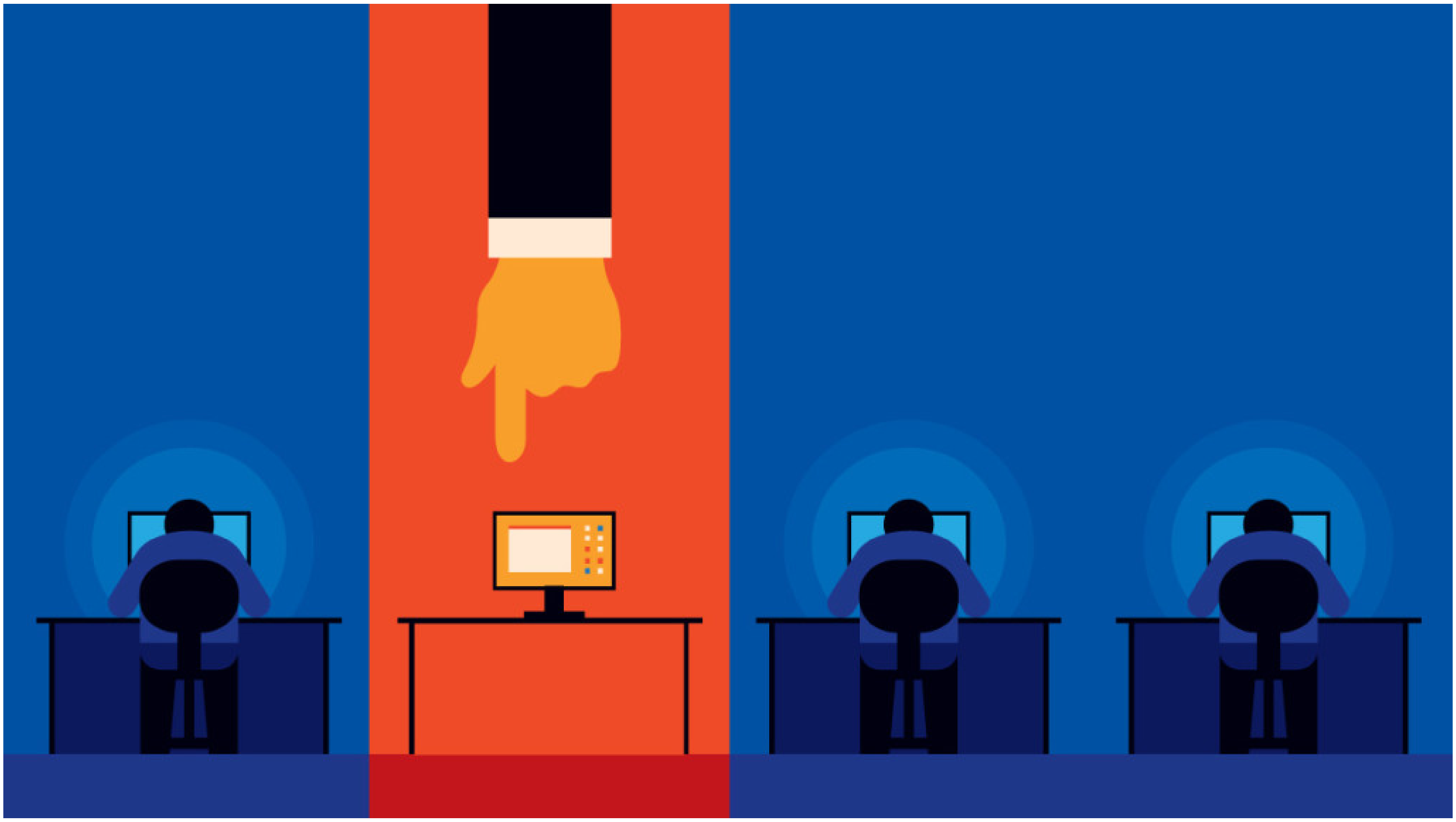
Harvard
Business
Review

SECURITY & PRIVACY

Which of Your Employees Are Most Likely to Expose Your Company to a Cyberattack?

by Kon Leong

DECEMBER 05, 2017



HARRY HAYSOM/GETTY IMAGES

When poet Alexander Pope first said “to err is human,” he probably didn’t realize how prescient those words were in capturing the world of cybersecurity. Yes, the root cause of most security breaches can be traced to human actions, or lack thereof. However, the bigger mistake is to believe that cybersecurity can be attained simply by correcting bad behavior.

Today, cybersecurity has expanded far beyond its traditional domain of external threats, typified by external hackers attacking network vulnerabilities. It now includes insider threats, which are much more complex and difficult to manage, as evidenced by some very serious recent insider breaches, such as those involving Edward Snowden and Chelsea Manning. The nature of insider threats can be categorized into malicious, accidental, or negligent, and account for a combined 39% of all data breaches according to recent research.

With employee behavior playing an ever larger role in the state of your organization's cybersecurity, here then are some general insights into the human side of cybersecurity that can help shape the right approach for your company:

Rethink employee training.

For external threats, there is the usual battery of defenses against viruses, malware, phishing, and network attacks. However, many of these defenses are often compromised by errant or lax human behavior, which makes employee training even more critical. In this area, company-wide training on best practices for handling the latest security threat is a common approach; unfortunately these guidelines are often skimmed, overlooked, or disregarded entirely. Furthermore, the standard memo on security often fails to capture the nuances presented by more dynamic security threats, which are often internal. For instance:

- How does an employee differentiate a bona fide email conversation versus phishing bait?
- When should an employee speak up about a coworker's suspicious activity?
- What types of information can and cannot be shared, and with whom?

In order to make a meaningful and lasting impact on employee behavior, organizations should instead consider frequent and interactive training sessions. Recent research by the Ponemon Institute indicates that employee training is tied as the third-most-effective method of decreasing the per capita cost of a breach, right after extensive use of encryption and assignment of an incident response team.

INSIGHT CENTER

The Human Element of Cybersecurity

For the more resistant users, one can employ a variety of creative training techniques that involve employee interaction, feedback, and discussion. For instance, take the method of gamification: one could supplement a cybersecurity presentation with a game of spotting suspicious activity, which compels employees to develop responsive skills. Moreover, engaging employees in hands-on training encourages buy-in and accountability.

It should be noted that in all cases of cybersecurity training, it's a case of train, retrain, and repeat. Too often, organizations hold a single seminar and then expect that to suffice. Given the constant influx of new employees in any organization and the constant change in security threats, periodic training should be mandatory.

Identify high-risk users and intervene.

Basic human behavior is very hard to reprogram. Therefore, training should be augmented by constantly updating technology, which has now evolved to detect errant behavior. The advancement of technology has only just begun to solve what seemed to be intractable issues in security and governance, and these new capabilities such as predictive analytics and artificial intelligence are expected to better monitor and influence human behavior. By employing a modern breed of analytics that enables organizations to analyze documents for sensitive content, review user actions, and track the flow of data across the enterprise, cybersecurity stakeholders can now identify many common indicators of negligent or malicious activity, including:

- Accessing, moving, or deleting large volumes of sensitive content
- Inappropriately creating, storing, or sending sensitive content
- Extreme negative sentiment towards the organization in messages

Then, of course, there is always the tried and true method of simulation, such as sending out mock-phishing emails and seeing who clicks. By identifying signs of risky behavior, organizations can stage strategic intervention with high-risk users, or potentially even catch the next "Snowden" in progress. In leveraging such technologies, however, organizations should give due consideration to the issue of privacy, which plays an ever more complex and changing role in today's regulatory environment.

Shape the solution to the human user and not vice versa.

It should be noted that the perfectly secure system is often perfectly unusable. We've seen many instances where the best intentions in security resulted in limited adoption. For example, PKI encryption using individual certificates, an encryption method potentially applied to messages and other transactions that authenticates the recipient using a digital "key," can offer excellent granular security. However, because it requires more steps from the end-user and administrator, it never really became widely adopted. If security involves extra effort from the end-user, it becomes harder to get participation.

Companies need to engage with the end-users to find out how far out of their way they're realistically willing to go in their everyday activity to support cybersecurity efforts. In other words, avoid protocols that rely on them doing any more than they actually will.

Constantly adapt to changing threats.

As the threat focus shifts from external hackers and network vulnerabilities to internal staff and content repositories (think email, file shares, and SharePoint sites), the security picture becomes a lot more complex.

Fortunately, the rapid advancement in content technologies makes it easier to secure these data repositories and also apply advanced governance and analytics to enable detection and remediation of risky behavior. The advent of these technologies also happens to address other critical issues, such as applying discipline to what is currently unbridled data access by data analytics, and satisfying new privacy regulations such as the General Data Protection Regulation (GDPR), a new data regulation that globally mandates greater privacy requirements for organizations handling EU resident data.

It's true that to err is human, and humans will keep erring. But increasingly, technology and improved practices can help you identify those employees who are most at risk of exposing your company to a cyberattack — before it becomes a major problem.

Kon Leong is co-founder and CEO of ZL Technologies, Inc., a software and cloud vendor to large enterprises for information governance and analytics solutions. Previously, he was co-founder in several high tech startups.

This article is about SECURITY & PRIVACY

⊕ **FOLLOW** THIS TOPIC

Related Topics: RISK MANAGEMENT

Comments

Leave a Comment

POST

1 COMMENTS

Michael Mazzotta 8 months ago

What I have a real hard time understanding is why companies (especially healthcare) allow employees to use the company internet as their own by shopping, on-line games… in addditiion to employees plugging in their own devises like cell phones and thumb drives.
This, I believe is the "low hanging fruit" that really should be addressed first. After this, we can move on to additional security such as two-step verification.

REPLY 0 👍 0 👎

JOIN THE CONVERSATION

POSTING GUIDELINES

We hope the conversations that take place on HBR.org will be energetic, constructive, and thought-provoking. To comment, readers must sign in or register. And to ensure the quality of the discussion, our moderating team will review all comments and may edit them for clarity, length, and relevance. Comments that are overly promotional, mean-spirited, or off-topic may be deleted per the moderators' judgment. All postings become the property of Harvard Business Publishing.