The Cybersecurity Costs of Employee Stress

Clay Posey
BYU

Clay Posey is an Associate Professor of Information Systems in the Marriott School of Business at Brigham Young University and Chief Research Scientist at Beyond Layer 7, LLC. His research focuses on the human element in organizational cybersecurity by understanding how employees can both inhibit and promote the protection of their employers' sensitive assets.

Mindy Shoss
University of Central Florida

Mindy Shoss is an Associate Professor of Psychology at University of Central Florida and an Honorary Professor at Australian Catholic University. Her research focuses on counterproductive work behavior, workplace stress, and the future of work.

Last summer, Colonial Pipeline paid a ransom of almost $5 million after a cyberattack created widespread panic over the availability of gasoline across the Southeastern U.S. Just a few weeks later, the world's largest meat processing company agreed to pay an $11 million ransom in response to a cyberattack that suspended operations at plants across the U.S., Canada, and Australia. Attacks like these have been growing more common for years, and the Covid-19 pandemic has only made matters worse, with the FBI reporting a 400% increase in cyberattacks over the past two years.

In response, investment into cybersecurity has skyrocketed — but unfortunately, these efforts haven't always addressed the underlying factors that actually create vulnerabilities. While IT specialists toil away to create better, smarter, and safer technical systems, there is one risk they can't program away: humans. Especially as remote work becomes more prevalent and thus access to secure systems becomes more distributed, one wrong click by an employee can often be enough to threaten an entire digital ecosystem.

Furthermore, while some organizations have begun to complement tech-focused efforts with cybersecurity initiatives targeting employees as potential attack vectors, these programs generally assume that employees break security protocols out of either ignorance or malicious intent. Our recent research, however, suggests that much of the time, failures to comply may

actually be the result of intentional yet non-malicious violations, largely driven by employee stress.

Many Policy Violations Are Driven by Stress, Not Desire to Harm

We asked more than 330 remote employees from a wide range of industries to self-report on both their daily stress levels and their adherence to cybersecurity policies over the course of two weeks. In addition, we conducted a series of in-depth interviews with 36 professionals who were forced to work remotely due to the Covid-19 pandemic, in order to get a better understanding for how the transition to work-from-home has impacted cybersecurity.

We found that across our sample, adherence to security conventions was intermittent. During the 10 workdays we studied, 67% of the participants reported failing to fully adhere to cybersecurity policies at least once, with an average failure-to-comply rate of once out of every 20 job tasks.

But what led to those breaches in protocol? When asked why they failed to follow security policies, our participants' top three responses were, "to better accomplish tasks for my job," "to get something I needed," and "to help others get their work done." These three responses accounted for 85% of the cases in which employees knowingly broke the rules. In contrast, employees reported a malicious desire to cause harm in only 3% of policy breaches — making non-malicious breaches (i.e., those motivated purely by the need to get work done) 28 times more common than retaliatory ones.

We also found that people were substantially more likely to knowingly break security protocols on days when they reported experiencing more stress, suggesting that being more stressed out reduced their tolerance for following rules that got in the way of doing their jobs. Common sources of stress included family demands that conflicted with work, job security fears, and ironically, the demands of the cybersecurity policies themselves: People were more likely to violate procedures when they worried that following them would hinder productivity, require extra time or energy, mean doing their jobs in a different way, or make them feel like they were constantly being monitored.

Of course, since our data was self-reported, we were unable to measure breaches that employees were unaware of committing. As such, our research is less conclusive when it comes to the prevalence of security issues borne of ignorance or human error. But our findings do suggest that despite considerable media focus on the "insider threat" posed by malicious employees, there are a lot of well-intentioned reasons that an employee might knowingly fail to fully follow the rules. Based on this, we've developed three key takeaways for managers:

There's a Middle Ground Between Ignorance and Malice

Many leaders assume that employee security violations are either malicious or unintentional, and then design security policies based on that assumption. However, our research illustrates that there's a sizeable middle ground between ignorance and malice, and so managers would be wise to adapt their training programs and policies accordingly.

Specifically, rather than focusing on malicious attacks, security policies should acknowledge the fact that many employee-driven breaches stem from an attempt to balance security and productivity. This means educating employees and managers on the prevalence of non-malicious violations, and providing clear guidance on what to do if adherence to security practices seems to conflict with getting work done.

In addition, organizations should take steps to incorporate employees in the process of developing and user-testing security policies, and equip teams with the tools they'll need to actually follow these policies. Too often, IT departments develop protocols in a vacuum, with limited understanding of how these rules might interfere with people's workflows or create new sources of stress. Especially as the shift to remote work has transformed how many people work, IT leaders should be sure to involve the employees who will be affected by new security measures in their creation, evaluation, and implementation.

Job Design and Cybersecurity Are Intertwined

It's common to think of security as secondary to productivity. In normal times, that's not necessarily a problem, as employees are likely to have the resources to devote sufficient energy to both. But as the myriad stresses of the pandemic make it harder to maintain productivity, that means that security tends to take a backseat to the critical tasks that drive performance reviews, promotions, and bonuses.

To address this, managers must recognize that job design and cybersecurity are fundamentally intertwined. The reality is that compliance with cybersecurity policies can add to employees' workloads, and so it should be considered and incentivized alongside other performance metrics when workloads are determined.

In addition, managers should work to identify and reduce sources of stress for their teams, since working under more-stressful conditions can impact employees' consistency in following security protocols (not to mention their wellbeing and effectiveness across a slew of other metrics). In particular, especially as remote work becomes more common, managers should be cognizant of the psychological burden to employees of working under systems that monitor them. Surveillance systems that seemed reasonable in the office might feel intrusive at home — and even if there's no obvious, direct fallout, our research suggests that the added stress could indirectly make people more likely to break security protocols.

Hackers Take Advantage of Altruism

Most managers would say it's a good thing if their employees want to help one another. But unfortunately, altruism can come at a cost: In our study, around 18% of policy violations were motivated by a desire to help a coworker. The pandemic has only increased the challenges we all face every day, and thus has created even more opportunities for well-meaning employees to "help" their peers in ways that leave their organizations vulnerable. Hackers know this, and they will often intentionally use social engineering tactics that take advantage of employees' willingness to bend the rules if they think they're helping someone out.

To address this, managers must not only implement security policies specifically designed to protect against these sorts of attacks — they must also work to reduce the impact of these measures on employees' workflows, and clearly explain their rationale, in order to increase employee compliance.

For example, as the move to remote work has reduced in-person communication, business email compromise (BEC) scams have become even more prevalent. These are scams in which an attacker poses as a supervisor or close coworker and emails employees with an urgent request to transfer funds. The time pressure and desire to help a colleague can push employees to break protocol and make these transfers without properly verifying the requests. Protecting your organization from these sorts of attacks means not just instituting a verification policy for large transactions, but also both educating employees on why the policy matters and minimizing the extent to which it impedes daily work.

***

In the modern cybersecurity landscape, every employee is a potential threat vector. To keep their organizations safe, technical and business leaders alike must understand the factors that can make anyone susceptible to flouting policy and opening the door to attackers. While the idea of a resentful employee purposefully trying to harm their company may make for a compelling story, our research points to the major role of employee stress in motivating non-malicious (yet potentially catastrophic) security breaches. To address the mounting risk of cyberattacks — as well as the countless other risks associated with an increasingly stressed-out workforce — leaders must undertake targeted efforts to minimize the root causes of stress in the workplace and design healthier, more sustainable workloads for employees at every level.

This work was supported by National Science Foundation RAPID Award #2030845, Division of Social and Economic Sciences. The views expressed here are the authors' and do not reflect those of the National Science Foundation.