ProCircular
SECURITY. PRIVACY. TRUST.

“They Click Too Much”

Revisiting User-Centered Cybersecurity in 2021

By Aaron R. Warner, CEO
ProCircular, Inc.

Human Stressors 101

Your business depends on people. Humans drive it with strengths and weaknesses, emotions, and motivations. They're both rational and irrational, often both at the same time. Research indicates that people actively seek out individuals who are similar to themselves, and they are more comfortable when they feel appreciated. A recent study published in the Journal of Social and Personal Relationships (Adam J. Hampton, 2018) claims "certainty of being liked to be the strongest mediator point to a live interaction."

Reciprocally, perceiving stress can have a negative impact on emotional wellbeing and social interaction. Research shows that perceived stressors, such as repeated, negative interactions with others, can impact our bodies and minds very much like actual stressors. This tendency comes from necessity. Our bodies have evolved to sense and respond quickly to danger. Unfortunately, our bodies are not great at differentiating between real and perceived threats well. (Smitha Bhandari, 2020). That's why a user submitting a complaint to a helpdesk will trigger the same physiological response as a person who threatens with a weapon.

"A user submitting a complaint to a helpdesk will trigger the same physiological response as a person who threatens with a weapon."

Technical professionals are no different, feeling safer around other technical people. There is a dominating and unfortunate tendency to view anyone outside of that circle as an idiot. A fascinating paper published in 1986 says, "The notion that the developers of information technology have power that they can use in their dealings with users is intuitively appealing." More disconcerting, the study also finds that "It seems likely that gatekeepers of information technology would be able, if they chose, to extract rewards from those individuals or groups who depend upon it." (Markus, 1986)

I.T. and cybersecurity professionals are given a great deal of trust, influence, and responsibility. They can see a users' every action, prevent them from accessing information, and shape how they perform their work. The perceived disparity or conflict between I.T. professionals and their users could create barriers to these job functions.

Technical teams tend to inadvertently create situations in which a small group is invested with significant control over another. That disenfranchised group of users becomes otherized, and they are seen as inherently different from the I.T. or cyber professional. That means that their concerns, suggestions, and challenges to the status quo tend to be dismissed by IT professionals who intrinsically see them as the "idiot."

When there is no IT or security emphasis built into the corporate culture, these teams feel compelled to exclude "non-security" or "non-technical" people from the decision-making and implementation processes. Isolated security is doubly harmful because it fails to incorporate users' needs into your security controls and fails to instill cybersecurity awareness in your users.

Paging Dr. Dumbass

Healthcare organizations provide a helpful example. The demands placed on technical professionals are extraordinarily high, and with human lives on the line, the stakes couldn't be any higher. Within this high-tension environment, when a user clicks the wrong email or intentionally visits a questionable website, the response is often swift and negative. That dismissive professional probably sees those users as threats to the status quo, idiots, adversaries, or guilty of creating unnecessary risk. However, blaming users for the issues they face is a tidy way of ignoring the actual problem. Users are not idiots. If an organization is serving hundreds or thousands of clients, customers, or patients, it's safe to assume that competent individuals support it. Users are motivated to complete their job functions. If hyper-restrictive cybersecurity controls are keeping them from their duties, their priority is to find a workaround.

ProCircular
SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

Insecure workarounds can include password sharing, tunneling, or the use of home systems if company-provided systems prove too restrictive. In the case of healthcare, many of the worst 'offenders' are highly trained and deeply educated individuals with an I.Q. that far exceeds most of their peers. Users are savvy and motivated enough to break down or work around barriers to their job functions. Failing to incorporate your users' necessary functionality into your security program will inevitably turn your workforce against your security program. In 2021, users present the most significant opportunity for insight into developing a customized cybersecurity program.

Cybersecurity helps ensure the confidentiality, integrity, and availability of that data, but you want to make sure these controls don't inhibit your users. Incorporating those users and their feedback into your security development efforts will ensure your controls' effectiveness and encourage a security-aware internal culture.

Shadow I.T. Is Your Friend

Security-aware users can be your primary source of intelligence. "Shadow I.T." refers to users who find technological workarounds to problems that prevent them from doing their jobs. For instance, imagine an I.T. department with a highly restrictive policy for purchasing applications. This policy alone doesn't eliminate the users' need to get their jobs done, and diligent employees will always find a way. When that conflict arises, a user asks themselves, "Should I follow their rules, or should I do what I'm being paid to do?"

When users cannot gain access to the resources they need, they'll often create the solution themselves. If a group cannot purchase the software they need in a timely fashion, they will create something from scratch. Their homemade software could function well enough to meet their own goals, but it won't have even the most basic cybersecurity controls built into it. These types of shadow I.T. departments can threaten the security and integrity of the entire organization.

"Should I follow their rules, or should I do what I'm being paid to do?"

An alternative approach would be the more user-centric cybersecurity program. Taking a more inclusive and less combative approach to cybersecurity can lead to a more effective program. Rather than taking away additional permissions and access, educate users on the rationale for those controls and provide them with the education necessary to avoid basic cybersecurity risks. Simple guidelines, such as "Don't hard code credentials," can save an organization from weeks of downtime and millions paid in ransom.

The Enemy of My Enemy

Users are not your adversaries. Just as your customers are not your adversaries, your organization needs end-users to survive. If they are properly equipped, your users can become your best line of defense against hackers. Users who are trained to identify threats are likely to spot an attacker's presence before a technological solution could indicate a compromise.

ProCircular recently responded to a client's incident in which employees reported indicators of compromise almost a full year before their monitoring technology detected and alerted of the breach. In this case, employees in the order entry department claimed that their computers were "Just….slow. Not broken, but….slow." According to the tickets, the helpdesk ignored these reports, and in some cases, the reporting staff was made to feel foolish for even making the call.

The situation eventually culminated in a significant security breach that cost tens of thousands of dollars to resolve. ProCircular's I.R. team found that foreign actors had been siphoning off 10-15% of thousands of servers' resources to mine bitcoin. Had the hackers used the entire infrastructure at 100%, it would have been immediately apparent. Remember, the hackers aren't idiots either. They strategically chose to bleed just enough from the VMWare infrastructure to support their efforts for months at a time.

ProCircular
SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

Had the I.T. group taken a more user-centric approach to their security, the organization could have avoided the significant financial and reputational damage caused by the breach. In placing immediate blame on the user, they essentially remove blame from the real adversaries, the bitcoin miners. Giving users the "benefit of the doubt" can be the first step to opening productive lines of communication.

The Actual Target: Money

Users are not the target. For the hacker, they're simply a means to an end. Attackers aim for financial gain, and they see a minimal profit in someone's identity or personal wealth. Attackers use individuals as a proxy to access organizational data.

In this sense, you can view your users as organizational assets that must be protected. The user is a victim, and their actions aren't personal. Too often, victimized users are held out as pariahs, and the consequence for these perceived slights is a loss of access, resulting in the inability to do their jobs. The state of cybersecurity education is an entirely separate article. Still, it's safe to assume that most of the content is produced by the same brilliant creative minds that brought you "Ladder Training" and "TPS Memos 101." The punishment doesn't fit the crime, and it drives these same people even further underground.

"The user is a victim, and their actions aren't personal."

Rather than denouncing users that have interactions with security threats, celebrate them as defenders of the organization. Take the time to explain the correct course of action, and when they follow your guidance, make sure that everyone hears about it.

The academic literature supports this approach as well:

> *"The results suggest that priming users to cybersecurity risks reduces their risk-taking behavior associated with cybersecurity whereas negative framing of messages associated with cybersecurity has no significant effect on users' behavior. The results also suggest that users who had taken a risk adverse cybersecurity action exhibited greater confidence associated with their action, perceived greater severity associated with cybersecurity risks, perceived lower susceptibility of their computer to cybersecurity risks, and perceived lower trust in the download link they had encountered in the experiment. This research suggests that priming is an effective way to reduce cybersecurity risks faced by users."* (SHARMA, 2017)

It's not your fault, Will.

Users are not at fault. The malicious actors behind cyberattacks work against the best interests of the users and the organization. Blaming a user is no different from pointing the finger at a family for having their house burgled. Although that family may have left their front door open, it's unlikely that they intended to have their possessions stolen. The same is true of an A.P. clerk who mistakenly wires money to a thief. As mentioned above, there's no malicious intent, and describing the user as being "at fault" actually works against the organization's goals. In summary, victim shaming reinforces bad behaviors and lowers the users appreciation for the seriousness of their mistakes.

They Can't Be Trusted

These issues are amplified in geographically dispersed organizations. Picture the bank with twenty branch locations, the healthcare system with ten critical care locations, or the manufacturer with overseas production. These organizations must customize their security controls to be effective in the place they will be used.

The traditional approach to remote offices or operating companies is to wall them off and provide only the bare minimum capabilities. In any of the examples above, it's normal for the I.T. or cybersecurity team to view these outside users as nothing

ProCircular
SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

but a new risk and apply restrictive permissions. This situation inevitably leads to workarounds, such as password sharing and the use of unsecured personal devices. Imagine a lonely I.T. professional in a foreign country. Their regional Director demands that they disable corporate restrictions so their team can "just get the job done." In this case, security and productivity are contradicting one another, and the non-technical professionals are forced to prioritize one over the other.

In these situations, we can see that both 'sides' of the discussion have motivations, priorities, and constraints. An open and honest conversation about each of those factors can lead to a compromise that protects the I.T. person's job, the Director's production bonus, and the overall organization's bottom line.

Don't Blame I.T. Either

Lastly, this article may place more of the blame than necessary on the technical professional. Like users, they have an impact throughout the organization, but they're motivated by their own personal job responsibilities. These technology professionals are often trying to do their jobs despite a severe lack of funding and support from executive management. ProCircular's Risk Assessment work typically starts inside I.T., simply because they tend to know where the most significant risks lie. The helpdesk will know who is working shadow I.T. Indicators of risk can present themselves as helpdesk requests, like "How do I get access to invoice.db?" or "why can't I run PowerShell commands?". The helpdesk can provide insight into areas where security controls are misaligned with job functions. They'll also get calls from departments when a key employee leaves. Maybe they'll discover an organizational dependence on an application that was written by a long-gone intern.

"Indicators of risk can present themselves as helpdesk requests, like 'How do I get access to invoice.db?' or 'why can't I run PowerShell commands?'"

Cultural adoption must start at the top. It's up to the CEO or leader of the organization to ensure that the company culture supports a user-centric approach to security. If the cyber team is encouraged to see bad guys inside the organization, or if the helpdesk isn't staffed well enough to provide them training outside of the department (read: context), it's a management problem.

The Solution: User-Centric Security

What are your users trying to get done? Start there. When a security program fails to incorporate user-accessibility, it pits the user against the organization's goals. When your security resources and business resources are working in competition, you're not maximizing business output. A well-implemented user-centered security program will involve users in all aspects of the design. Security professionals will check their judgment at the door and build security around the larger organizational goals.

Incorporating a user-centered approach into your security program could be as simple as asking, or even begging, users to get involved. Make sure to keep your users in the security loop, planning implementation and reviewing controls in post-event meetings. A security program built around user context keeps it interesting, relevant, and free of blame or judgment. Ultimately this results in the success of all involved.

Your organization seeks to be a profitable, growing, effective company. Maybe you aim to serve your patients or deliver secure elections; regardless of your industry, a robust security program is simply a means to an end. Incorporating a user-centered approach in your cybersecurity program will ensure those means work as efficiently as possible.

Cybersecurity programs built around the humans in the organization will always be more effective than those who treat their users as fools by default.

For more information on measuring your risk and building a user-centric security program, please visit www.procircular.com.

ProCircular
SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

Bibliography

Adam J. Hampton, A. N. (2018). You're like me and I like you: Mediators of the similarity–liking link assessed before and after a getting-acquainted social interaction. Journal of Social and Personal Relationships, https://doi.org/10.1177/0265407518790411.

Deloitte. (2020). Cyber crime – the risks of working from home. Retrieved from www.deloitte.com: https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-cyber-crime-working-from-home.html

Markus, M. L.-A. (1986). "POWER OVER USERS: ITS EXERCISE BY SYSTEM PROFESSIONALS". ICIS 1986 Proceedings, https://aisel.aisnet.org/icis1986/28.

Nelson, N. a. (2017). "Studying the Tension Between Digital Innovation and Cybersecurity.". 3rd International Conference on Information Systems Security and Privacy (SIGSEC).

SHARMA, K. (2017). IMPACT OF FRAMING AND PRIMING ON USERS' BEHAVIOR IN CYBERSECURITY. MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY, https://scholarsmine.mst.edu/cgi/viewcontent.cgi?article=8660&context=masters_theses.

Smitha Bhandari, M. (2020, November 17). What Does Stress Do to the Body? Retrieved from WebMD: https://www.webmd.com/balance/stress-management/stress-and-the-body#1

ProCircular
SECURITY. PRIVACY. TRUST.

2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com

844-95-SECUR