MICRO FOCUS

Flash Point Paper

Security

The Power of Trust between Businesses and Consumers

- *For your organization, what are the top threats to your digital consumer's trust?*

Security—Key Component of Trust

Consumer trust—it's important in today's world because it can literally make or break a business. Recently, security breaches, personal information abuse, and even something as seemingly benign as the user experience have brought about both public awareness and consumer disdain. We now live and work in an age where consumers decide how and with whom they want to do business largely through digital transactions. Businesses that serve their customers in a trustworthy fashion with the technology experience that consumers expect have the upper hand. Still, all it takes is one slip-up or wrong turn and this trust and, it's counterpart, loyalty, can recede if not go away over time.

Since the core purpose of any business is to acquire and keep customers, organizations of all sizes and industries must make the consumer experience a top priority. One of the key areas that can make or break the consumer experience involves how people interact with your digital systems. From logging in to logging out and everything in between, modern authentication enables this experience. An old security concept with a modern-day twist, system authentication mechanisms can serve as a critical factor for establishing in building the ongoing trust customers are looking for. It's something that I consider all the time, mainly because many businesses that I interact with make the process so difficult. I often experience things such as:

- Lack of multifactor authentication which can be one of the best ways to lock down accounts against
- Ridiculously low intruder lockout thresholds accompanied by painful password reset processes that often require a phone call into the business I'm dealing with
- Weak password policy requirements, i.e., when I try to set a strong password (or passphrase), the system tells me, of all things, that my password is too complex
- Login timeout values that are super short which then require me to jump through the old-school hoops of having to click to go back to the login screen, re-enter my username and password, and hope that I do it correctly so that I don't lock myself out

I have these experiences online more often than not and it's frustrating to say the least. I can't help but think that if the business can't even get this part of my user experience right, then what other gaps and risks are present behind the scenes? Are my login credentials stored securely and protected against common exploits? Will the business see when my account is compromised and stop the attacks? Will my mobile experience be more or less secure—or easier or more difficult to use—than my web experience?

Strong User Verification Foundational to Trust

If you are responsible for IT and/or security in your organization, I don't envy you. I see many people struggling to balance the demands of regulators and auditors with the demands of consumers. In today's business world with more tech-savvy consumers, you must focus on both. What I'm talking about here is two sides to the same coin. There are compliance mandates and security best practices on one side. On the other, it's about solving an array of business challenges—a big one of which is consumer trust and ongoing loyalty. If trust is to be built—and kept—over the long term, you must look at both sides of the equation. You have to factor in what the end user sees and does when interacting with your business. I believe that's largely what's missing.

Many businesses are simply going through the motions to meet this or that minimum security or compliance requirement without putting themselves in the shoes of the very people that they say they're trying to make (keep) happy. Looking at the overall authentication process involves various systems and people across local applications, mobile devices, and out to the cloud. When looking for opportunities to improve the authentication process, the following are considerations for maximizing the user experience while minimizing your security exposures:

- Two-factor or, ideally, multifactor authentication with the flexibility to choose which options can be used such as a biometric, voice, or geolocation
- The ability for new applications and systems to be recognized and analyzed to help determine risk scenarios and levels
- Controls such as risk-based authentication and re-authentication requirements to show that the system is looking out for the best interests of the consumer
- Self-service password resets that your users and helpdesk alike will appreciate
- Support for various authentication methods
- Visibility and oversight that allows for immediate control or prompt response to threat scenarios

Looking back at the positive interactions I've had with businesses, it comes down to how I felt during and after the interactions. If the business makes me jump through what I believe to be a bunch of unnecessary hoops, that left a bad taste in my mouth. Even when it's done in the interest of security or the greater good, when it's not well-thought-out or properly implemented, it makes me want to take my business elsewhere. Looking after-the-fact, I think about my experience with a web application or mobile app and whether it made me want to go back and use the system again. In other words, did it make me want to transact business with the organization again or was it a negative experience of reluctance and not wanting to have to do that again. It's about 50-50. I'm having more and more positive experiences with online services but there are still plenty that I'd rather not have to deal with. And much of it comes down to how I login, how I log out, and, essentially, how I'm treated as an end user of the system.

The Business Value of Trust

Perhaps the most important takeaway in the context of user interaction and experience that you and your executive management team needs to consider is: what happens when trust is lost? Is this something that you can measure? Will you know it when it happens? It's one thing for business to sustain losses when well-known data breach occurs. However, when it comes to trust, interaction, and lesser-known security events, there are many intangible factors at play. If systems and processes are not in place to support the measurement of the user experience, an impact to the business can occur both overnight or over time. Either way, when it's not being measured it certainly can't be fixed. This is certainly a function of business that goes beyond IT and security metrics. Yet, at the same time, it's information systems that can either a) help create positive experiences or b) serve as a barrier to business growth.

Some or all of this may seem overwhelming when trying to integrate robust authentication into your environment, but it really doesn't have to be. If you step back and look at the bigger picture there will be numerous opportunities

Micro Focus® takes an integrated approach to security, which leverages common components for a unified experience for both your digital consumers as well as your IT staff.

Contact us at:
www.microfocus.com

for improving both business processes and technical systems that can support a more positive user experience. One thing to keep in mind is that it's not just about the user experience or minimizing security risks. It's all about leveraging today's technologies as an opportunity to expand your business. Striking a balance between security, convenience, and long-term opportunities.

Given all the variables, there will never be perfection in computer systems. But there can—and should—be more positive experiences. With today's technologies, there's always no real reason that it can't be done eventually. I think it's safe to say that people are willing to pay a premium to companies they trust. The world is becoming more complex and consumers realize that. As long as the power of trust remains, you'll be on the right side of the equation. Inaction or action—stay where you are or move forward. It's a business decision that every IT and security professional has a part in. In this case, the decision is whether to make the user experience a better one that happens to be more resilient to attack or remain the same, if not go in reverse, in terms of risk and trust. It's ultimately a matter of choice and it can be more impactful to the business than is often assumed.

Written by Kevin Beaver, CISSP
Kevin Beaver is an independent information security consultant, writer, professional speaker, and expert witness with Atlanta-based Principle Logic, LLC. With over three decades of experience in the industry, Kevin specializes in performing independent security assessments and consulting to help his clients uncheck the boxes that keep creating a false sense of security. He has authored/co-authored 12 books on information security including the best-selling Hacking For Dummies and The Practical Guide to HIPAA Privacy and Security Compliance. In addition, he's the creator of the Security On Wheels information security audio books and blog providing security learning for IT professionals on the go. Kevin can be reached at through his website at **www.principlelogic.com** and you can follow him on Twitter at **@kevinbeaver**.

Learn More At
www.microfocus.com/digitalsafe