Deloitte.

Who are you? The computer wants to know.

Convincing the machine you are who you claim to be is at the heart of network security. For the vast majority of us—those committed to safeguarding bank accounts, personal data, corporate patents, and inside information—success hinges on establishing our identity in a way that no one, man or machine, can replicate.

You might think that the risks are rising. After all, global workers are venturing far outside old corporate firewalls. From the ballpark to the beach, they're using their own smartphones and tablets to copy and forward proprietary documents and spreadsheets. And much of this data is stored on cloud computers belonging to other companies. Add it all up, and it may appear as though corporations have utterly lost control of their secrets.

Security companies stress these risks in their marketing. "But we're not simply at the mercy of the attackers," says Michael Wyatt, managing director, Deloitte & Touche LLP, and identity management solution leader in Deloitte Advisory's Cyber Risk Services. In the end, Wyatt says, smartphones in the hands of mobile workers may prove to be more secure than the old cubicle PC equipped and vetted by the tech department. "The developments that people associate with increased security risks also create opportunities for new solutions."

"The developments that people associate with increased security risks also create opportunities for new solutions."

Michael Wyatt
Managing Director
Deloitte & Touche LLP
Identity Management Solution Leader
Deloitte Advisory's Cyber Risk Services

Organizations that view the business landscape through this lens can continue to reap the benefits generated by technology and digital by consciously taking on and managing risk when it creates value for their businesses. It's this perspective—that risk can be used to power performance and isn't only something to be feared or avoided—that creates enhanced opportunity.

One such potential is in the area of identification. The old status quo features a corporation with firewalls ringing it like an electronic moat. Even within such a fortress, users must establish their identities for the machines. The systems, after all, can't verify users' identities the way a colleague might, by looking at them or hearing them speak. Instead, they demand strings of numbers and letters—passwords—to sign into virtual private networks and intranets.

This creates vulnerability, most of it stemming from the inconvenience these defenses pose. People struggle to remember passwords, so they stick them on Post-it notes to their monitors. They recycle old passwords or use ones that any hacker could guess. Currently, the two most common, according to security firm Splashdata, are "123456" and "password." "The weakest link in our security models, and a significant source of breaches, has always been the user," says Jeff Margolies, principal, Deloitte & Touche LLP.

While the PC in the cubicle recognizes users only by strings of symbols, security features in mobile devices can zero in on a person's identity in new ways. But the world is slowly moving beyond passwords. As recently as a decade ago, says Margolies, surveys showed that many users were wary of biometric filters, viewing them as intrusive and creepy. But their combination of convenience and security is hard to beat.

Already, many smartphones and tablets demand a fingerprint—which is far more precise than a password. A slew of other biometric filters, including face scans, voice recognition, and heartbeat signature, can add certainty.

And this is only the beginning. Mobile networks, increasingly, are able to identify people by the patterns of their lives—their movements, social networks, Internet searches, the apps they use, even the music they listen to. This data informs machine-learning systems that not only recommend itineraries or songs but can also vouch for a user's identity. The upshot? Even when a device is lost or stolen, network security can detect unusual patterns and shut off access.

"The weakest link in our security models, and a significant source of breaches, has always been the user."

Jeff Margolies, principal, Deloitte & Touche LLP

Reliance on others

With mobile workers operating their own devices, companies cede a certain amount of control and must rely more on the phone and Internet providers. This can be unsettling. But corporate crown jewels might end up being safer in some other company's cloud than in the old refrigerated data center in the headquarters' basement.

Even a decade ago, many companies resisted entrusting their most valuable data to outside providers. They understood the efficiencies of outsourcing the expensive, exacting, and labor-intensive work of running data centers. But if a company's secrets and intellectual property are in the form of digital data, can they afford to trust anyone else to handle it?

In a word, yes. A well-chosen cloud provider maintains security at a high level because its business is on the line if it doesn't. Due diligence is necessary, of course, to manage the risks properly. But even government intelligence agencies, holding some of the most sensitive data imaginable, have been turning to third-party cloud storage providers.

The result is a drastic shift for technology departments in companies around the world. They used to provide, maintain, and protect technology, end to end, within their digital fortresses. Now they're relinquishing much of this control. And that's not necessarily a bad thing.

But the vulnerable link in the system remains, as it always has been, the users. They control or generate the lion's share of the data. A primary challenge for corporate security is to make sure the users understand the data's transcendent value and to make smart decisions when producing, sharing, or storing the intimate details of the enterprise.

And here's the bonus: When corporations manage data intelligently, they not only avoid the nightmare scenarios we hear so much about, they also enhance their reputations and power performance. Consider all those hours squandered hunting down old passwords or creating new ones. In modern systems, employees can use that time instead to solve business problems and serve customers.

Contacts

US

Mike Wyatt
Director | Deloitte Advisory Cyber Risk Services
Deloitte & Touche LLP
miwyatt@deloitte.com

Jeff Margolies
Principal | Deloitte Advisory Cyber Risk Services
Deloitte & Touche LLP
jmargolies@deloitte.com

Luxembourg

Stéphane Hurtaud
Partner ¦ Information & Technology Risk
+352 45145 4434
shurtaud@deloitte.lu

Laurent de la Vaissière
Directeur ¦ Information & Technology Risk
+352 45145 2010
ldelavaissiere@deloitte.lu

To learn more about Deloitte Advisory's Cyber Security solutions, visit:
http://www2.deloitte.com/global/en/pages/risk/topics/cybersecurity.html