I Left My Security in the Office

For many people, information technology has changed the very meaning of work. The classic locus of work is the office, a place where people gathered to perform a variety of tasks with a common purpose. Office workers saw their colleagues more than they saw their spouses; they dressed well; they came and went at relatively regular times so they could catch their trains or avoid the traffic.

Mobile Work

Now I, and many people like me, do not *go* to work. We have laptop computers, cell phones, a printer and Internet connectivity at our homes. Our "office" is where we live. We are in touch with many of our colleagues on a daily basis, but see them only rarely. We are mobile workers, able to do our jobs anywhere as long as we have the technical tools of our trade.

I submit that changing the definition of work necessitates a corresponding redefinition of security over the information with which we work.

I can hear a serious objection to my premise here: Many people do not work in an office, but in a factory, a hospital, a laboratory, a store. Their work is tied to a place and they cannot work anywhere else. True, no one can make steel at home. Among the many manifestations of the changes technology has wrought is that we have created two classes of workers: information workers, whose world is broad, without boundaries or clocks, and place-bound workers who are far more limited in their freedom of movement or in alternatives for getting through disruptions such as heavy snowfalls. This bifurcation has already had major economic, social and political consequences that I will not go into here. This is, after all, the *ISACA® Journal*, not *The New Republic*. Here I will address just the implications for information security.

Physical Security

One of the tenets of information security has been the physical protection of data centers, defined as "where data are." The prevention of unauthorized physical access, damage and interference to the organization's information and information processing facilities is one of the key objectives stated in ISO 27002.[1] However, with worker mobility, even if data reside in a room with limited access and other preventive controls, they are accessible everywhere. This raises the stakes for the physical security of information resources; a data center cannot be stolen, but a laptop computer certainly can be.

Consider just a few of the headings in the relevant chapter of ISO/IEC 27002:

- Physical security *perimeter*
- Physical *entry* controls
- Securing *offices, rooms and facilities*
- Protecting against *external* and environmental threats
- Working in secure *areas*[2]

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2Jdm75x

Steven J. Ross, CISA, CISSP, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal's* most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

The entire reference for physical security is place. Keeping in mind that the ISO/IEC 27002 standard, definitive in the information security field, was published in 2013, we can see how rapidly the environment in which information is used has changed.[3] I would rest easier if hard-drive encryption and two-factor authentication were universally implemented, but that is not the case. Perhaps a later version of the standard will recognize that data are not where the servers are, but where the users are.

Data Leakage Prevention

Not that long ago, somebody[4] wrote:

> *There is no single answer to the problem of data leakage…. [I]f personnel are issued laptop computers and virtual private network (VPN) access capabilities, it may be assumed that they are expected to be mobile, work remotely and take their data with them. So at what point are data considered to be leaked? Are they leaked when they leave an organization's premises?*

The statement is still relevant, but with more immediacy today. For many information workers, issuance of laptop computers with VPN capabilities need not be preceded with "if." The conditional has become assumptive. Information is not "leaked" when a worker is off-premises. The person may rarely, if ever, work *on*-premises. If the frontier between contained and leaked is not the office building, is it the organization-issued personal computer? What then of that person's smartphone or the flash drive on which he or she stores backups?

There is an implicit, but unwarranted, expectation that an authorized user will not betray the trust placed in him or her, either intentionally or inadvertently. Even if that were a reliable control, what meaning does trust have in an era in which data sharing is promoted as an ideal? The boundaries of trust must be encoded in policy that, it is hoped, will lead to behavior. Maybe so, if the definition of "trust" is clear. Clarity of the policy will (or, perhaps, may) motivate staff to follow the rules.[5] But trust parameters are a weak substitute for secure perimeters.

Business Continuity Management

The effect of workers' mobility on business continuity management is so extreme that the plans written even a few years ago may no longer make sense. Most business continuity plans written in the past 25 years have consisted of a search for and transition to designated alternate workplaces. Hence, there is a commercial industry of office space for contingent use (aka hot sites) and many organizations maintain empty, but well-equipped, office space, just in case.

"THE EFFECT OF WORKERS' MOBILITY ON BUSINESS CONTINUITY MANAGEMENT IS SO EXTREME THAT THE PLANS WRITTEN EVEN A FEW YEARS AGO MAY NO LONGER MAKE SENSE."

These provisions make little sense when the extent of a business interruption is the length of time it takes workers to get home—or even less time if people work at their homes on a routine basis. For those few transactions for which minutes are of the essence, coffee shops beckon. If an organization has migrated its data center away—far away—from the building where its work is done, then having workers toil at home is possibly a benefit—at worst, an inconvenience—and not a disaster at all.

Data Center Recovery

The same consideration, but in reverse, applies to data center recovery planning.[6] The ability for people to work remotely is entirely dependent on the availability of information systems centrally. Information workers enter data into systems, manipulate the data and use them for various purposes. That is their job. So, no systems, no jobs, neither in the office nor at home. Increasingly, IT managers recognize this and maintain two or more

data centers sufficiently far from each other so that the same event cannot incapacitate both.

There is another, perhaps deeper, implication of the technical enablement of worker mobility (and here I may stray into sociology after all). It is hardly an original observation that information technology is changing society, its cultures and mores, and is doing so at a dizzying and dislocating pace. For this discussion, it has changed the nature of work, of the office, of colleagues and of management. Why should information security be immune from the forces technology has unleashed in our workaday lives? We have to embrace these societal changes because there is no other alternative. We security professionals need only remember how different things were a decade ago to get some idea of how different they will be five years hence.

Endnotes

1 International Organization for Standardization/ International Electrotechnical Commission, ISO/IEC 27002:2013 *Information technology—Security techniques—Code of practice for information security controls*, p. 30, *https://www.iso.org/standard/54533.html*
2 *Ibid*., p. 31-33, author's italicization
3 Yes, "Security of equipment and assets off-premises" is addressed, deep in the chapter and almost as an afterthought. The "premises," evidently, are where the data center resides.
4 Oh, right, that was me in 2009. Ross, S.; "Data Plumbing?" *ISACA® Journal*, vol. 6, 2009.
5 *Ibid*.
6 Aka IT disaster recovery planning