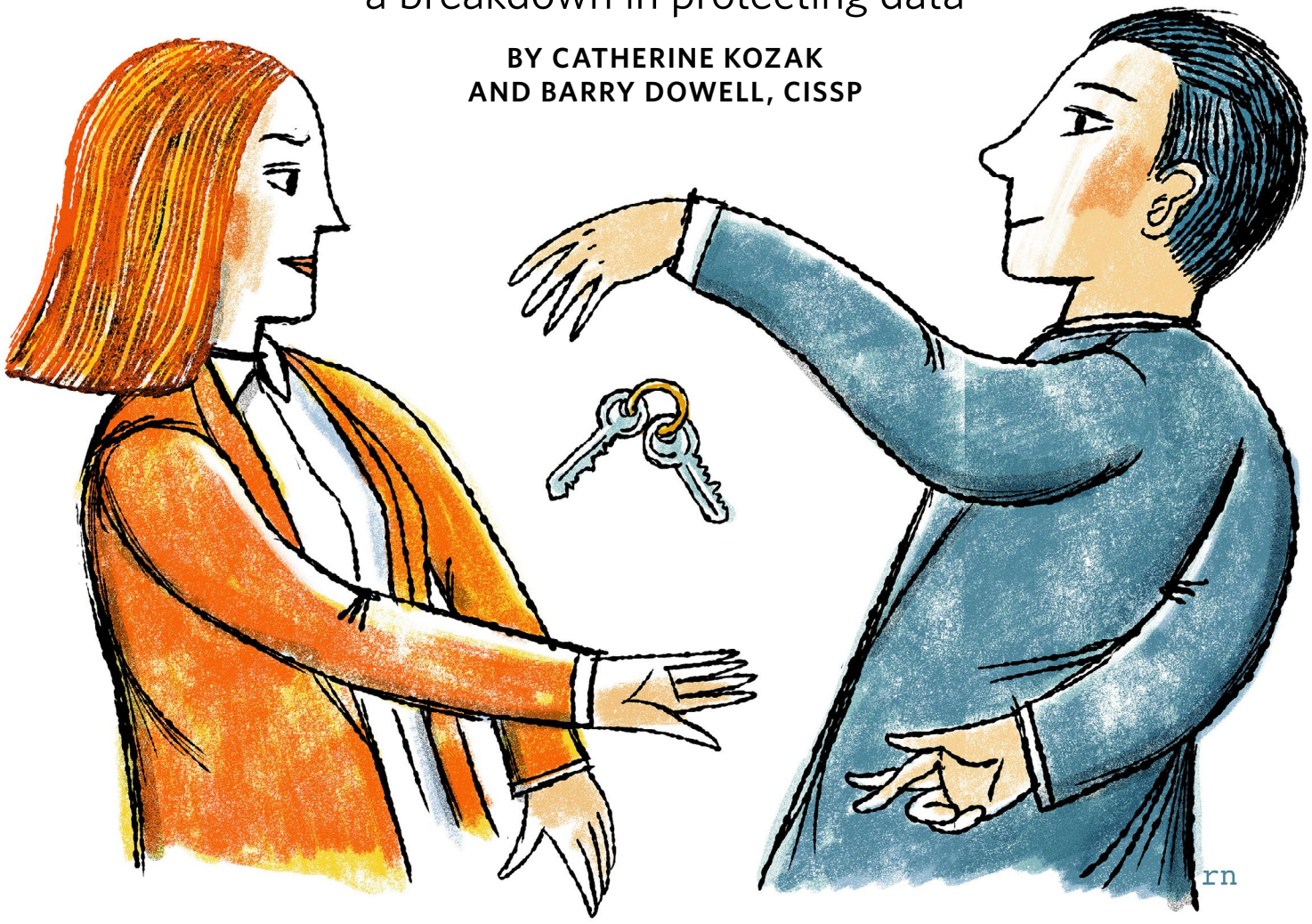
DO TELL

Fuzzy ethical guidelines can lead to a breakdown in protecting data

BY CATHERINE KOZAK
AND BARRY DOWELL, CISSP



IT WAS A ROUTINE CHANGING OF THE GUARD: a new contractor for IT services taking the reins. As expected, authorizations to access technical equipment and company systems were updated. And as is typical in such transitions, most lower-level staff, especially technicians, were retained at the customer worksite and managers and upper-level supervisors were relocated to other positions within the company. Some moved on to new roles elsewhere.

But unexpectedly, a morally questionable action transpired, setting up a potentially disastrous violation of standard ethical practices.

ILLUSTRATION BY ROBERT NEUBECKER

FOLLOWING ORDERS—OR BREAKING THE RULES?

When the system administrator for the original prime contractor was instructed by management to change passwords for all devices the contractor had managed, the former employees were properly cut off from accessing and administering the devices, protecting the security and privacy for the new contractor and its customers.

The former administrator should have provided the updated passwords to the new contractors and system administrators as soon as possible. But in this case, the new contractor was given the wrong passwords.

More alarming, it was not immediately clear if system administrators who had changed the passwords declined to provide the new, correct ones at the behest of their employer—or because they were trying to create havoc for their former customer and co-workers. (The former was later confirmed by the former administrator, though "off the record.")

While doubtless an example of a grave, unethical act, if true, it may be less obvious how a cybersecurity professional should confront such a violation, especially if the employer lacks an ethics officer, or even an ethics policy.

ESTABLISHING ETHICS IN A RELATIVELY NEW INDUSTRY

Now part of nearly every facet of life worldwide, cybersecurity and subsequent ethics have become "a huge, huge challenge," says Sean Brooks with the Center for Long-term Cybersecurity at the University of California, Berkeley. "I think one of the things that we're really dealing with now is there is not a good sense of—not just in the cybersecurity industry, but in the broader tech industry—appreciation among the rank and file and also among corporate and private institutions about ethical obligations."

Even a well-respected member association such as (ISC)^2, established in 1989 during the early days of the digital revolution, cannot dictate industrywide ethical behavior. But from its inception, the organization's founders saw the need to create standards, certifications and ethical guidelines for the cybersecurity industry. "This is something, if you want to become a member of (ISC)^2 and to obtain our certifications, besides [having] necessary experience, besides passing the exam and having the recommendations of your colleagues, you have to obey the Code of Ethics," says Biljana Cerin, CISSP, (ISC)^2 Board Ethics Committee chair.

Developed by "seasoned experts" in the field, Cerin explains that the (ISC)^2 Code of Ethics is based on four canons, with the first one being the most important:

- Protect society, the common good, necessary public trust and confidence and the infrastructure;
- Act honorably, honestly, justly, responsibly and legally;
- Provide diligent and competent service to principals;
- Advance and protect the profession.

The reinforcement of ethics in the profession, found in educational programs, conferences and online, is a large part of why an (ISC)^2 certification is considered the gold standard in the industry, Cerin asserts. Prominently displayed on the organization's website is its Code of Ethics: "The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior. Therefore, strict adherence to this Code is a condition of certification."

ESTABLISHING THE RULES

Ethical standards also require lawful behavior, a melding that can be difficult in a profession that operates worldwide. At its core, ethical behavior requires making principled judgment calls based on different circumstances, Cerin explains, whether or not allowed under law.

"We have more than 140,000 members and those members work in different legal environments," she says. "Maybe something that is legal in one country is not legal in another one. So, it always comes down to: 'What am I—a professional in the field having, for example, favored access to some information? Seeing things that maybe other people are not able to see? What can I do to make sure I act professionally?'"

Still, employees and contractors should have guidance on ethical codes and violations from the organizations themselves. "That's where I think all of us should start," Cerin states. "It's kind of amazing how many companies don't have internal regulations that actually explain to people … the security policy or acceptable use policy."

Too often, ethical dilemmas in the cybersecurity workspace leave people feeling confused or powerless.

For instance, in the opening scenario where the system administrators provided the wrong passwords, they claimed to be following an order from their contractor's management to change the passwords and not give the correct passwords to their customer. Assuming the administrator was telling the truth, the management was attempting to cause harm to the soon-to-be former customers, and their conduct would certainly be considered unethical.

The administrators were given what in the military would be termed "an unlawful order." In the best of circumstances, that order could have been ignored and the correct information passed on. Unfortunately, there are myriad rea-

sons for what appears to be an obvious response. Perhaps there is fear of retribution or losing one's job. Perhaps the company lacks proper whistleblower protection, or there is no protocol in place to address violations. Perhaps the administrator simply feels obligated to obey his or her superior or is incentivized with promises for future work.

> "I think we need a lot more conversations within industry groups and within the classes that train the people who will become the professionals."
>
> *—Irina Raicu, director of the internet ethics program at the Markkula Center for Applied Ethics, Santa Clara University*

THE CHALLENGE OF ENFORCEMENT

By nature, ethics are "nuanced and contextual" and reflect the "inherent complexity of human life and human interaction," explains Irina Raicu, director of the internet ethics program at the Markkula Center for Applied Ethics at Santa Clara University.

"We make ethical decisions all the time about what is the right thing to do in our interactions with other people, and about what kind of people we want to be when we take certain actions," Raicu says. "Laws, at their best, are codified ethics. They are things that we, as a society, have reached some decision that this is the right thing to do or this is the wrong thing to do. And the fact that it's difficult, and we may not agree on them, does not mean we don't have to make those decisions.

"And we make them according to our values and trying to help as many people as possible and hurt as few people as possible. So that's where ethics comes in—when there's no law that tells you exactly what to do or what not to do."

It can be helpful, advises Raicu, to look through different perspectives in making decisions that are aligned with one's values. The Markkula Center teaches a framework for ethical decision making that looks at it through five lenses: rights, justice, utilitarianism, common good, and virtue ethics. For a long time, she says, expectations in the industry were focused solely on skills with technology and protection of data.

But now there's greater understanding that ethical considerations are just as important for cybersecurity professionals, who often balance complex security situations under intense stress. "Those are the kinds of things that can't be addressed at the moment of crisis, when they discover a breach or something," Raicu warns. "I think we need a lot more conversations within industry groups and within the classes that train the people who will become the professionals."

Massive data breaches and hacking of public and private devices have become common, leading to more scrutiny of the ethical behavior of cybersecurity professionals. As a result, says UC Berkeley's Brooks, the culture of the industry is evolving to incorporate more ethical education and standards.

"But a lot of it is, these are companies, large institutions that have been built by folks who, by the nature of the career path, have never been forced to engage at an intellectual level with some of these more—I hate to use this term—'soft' issues around ethics and social responsibility and things like that," he says. "It's just not something that engineering educational programs have emphasized in the past, [and] there's no regulations to force the issues on companies."

If anything, the rapid-fire transformation to a data-driven, interconnected world has dramatically demonstrated that, absent ethical conduct by cybersecurity professionals, there's real potential, advises Brooks, "for truly bad things to happen."

One example he cites was the recent revelation that former U.S. government cybersecurity personnel had participated in hacking into accounts belonging to journalists and human rights advocates for the United Arab Emirates, and that some data from U.S. citizens had been swept up in the process. It's the kind of situation that should serve as a warning, "that there's now a fully formed class of professionals in the cybersecurity space."

CREATING A MORE ETHICS-ORIENTED CULTURE

From the earliest days of the tech fields, the career path for information security has been in the private sector, defense and intelligence communities, Brooks says. "That creates an institutional bias in the entire field around what is and what isn't permissible behavior. So, there's this whole class of professionals out there—some have built skills on the defensive side, some have built skills on the offensive side, some of whom have personal ethical frameworks, some of whom don't. You don't have strong industry standards about what is acceptable practice, and part of that is it's a rapidly changing space."

Even when there are professional associations like (ISC)^2 to support and certify cybersecurity professionals, Brooks says that the standards offered by the dozen or so groups for the industry tend to be uncoordinated and often competitive. Certifications have merit, he adds, but without enforcement and unified industry standards or a review board, they fall short of being the cyber industry's version of American Medical Association licenses.

Companies also have learned that best practices require multiple individuals who have appropriate access to systems and services to prevent the vulnerability of a single point of failure.

As the case of the systems administrator who mishandled password information illustrates, the possibility of a disgruntled employee or contractor can present an especially dangerous threat to company security. That's why it is common for terminated employees to immediately have their system access removed and be escorted from premises. Companies also have learned that best practices require multiple individuals who have appropriate access to systems and services to prevent the vulnerability of a single point of failure.

Ethical conduct is a critical workplace component in the cybersecurity industry, but it can still be overlooked, undervalued or unsupported. Still, that's no excuse to plead ignorance or not seek guidance, Brooks says.

"There are long-term issues around education, and ethics and professional standards, but I think for people who are in the field now, some of it is just really swallowing your pride and knowing how to ask for help from people who are outside your field. Because that's going to be critical to making you better at your job." ■

CATHERINE KOZAK *is a freelance writer and past magazine contributor who lives and works on the Outer Banks of North Carolina.*

BARRY DOWELL, *CISSP, is an information systems security official working as a contractor for a U.S. government agency. He has worked for that agency for more than 16 years, the majority of which were as a systems engineer and information systems security official.*