Organizational Doxing

schneier.com/blog/archives/2015/07/organizational_.html

Recently, WikiLeaks began publishing over half a million previously secret cables and other documents from the Foreign Ministry of Saudi Arabia. It's a huge trove, and already reporters are writing stories about the highly secretive government.

What Saudi Arabia is experiencing isn't common but part of a growing trend.

Just last week, unknown hackers broke into the network of the cyber-weapons arms manufacturer Hacking Team and published 400 gigabytes of internal data, describing, among other things, its sale of Internet surveillance software to totalitarian regimes around the world.

Last year, hundreds of gigabytes of Sony's sensitive data was published on the Internet, including executive salaries, corporate emails and contract negotiations. The attacker in this case was the government of North Korea, which was punishing Sony for producing a movie that made fun of its leader. In 2010, the U.S. cyberweapons arms manufacturer HBGary Federal was a victim, and its attackers were members of a loose hacker collective called LulzSec.

Edward Snowden stole a still-unknown number of documents from the National Security Agency in 2013 and gave them to reporters to publish. Chelsea Manning stole three-quarters of a million documents from the U.S. State Department and gave them to WikiLeaks to publish. The person who stole the Saudi Arabian documents might also be a whistleblower and insider but is more likely a hacker who wanted to punish the kingdom.

Organizations are increasingly getting hacked, and not by criminals wanting to steal credit card numbers or account information in order to commit fraud, but by people intent on stealing as much data as they can and publishing it. Law professor and privacy expert Peter Swire refers to "the declining half-life of secrets." Secrets are simply harder to keep in the information age. This is bad news for all of us who value our privacy, but there's a hidden benefit when it comes to organizations.

The decline of secrecy means the rise of transparency. Organizational transparency is vital to any open and free society.

Open government laws and freedom of information laws let citizens know what the government is doing, and enable them to carry out their democratic duty to oversee its activities. Corporate disclosure laws perform similar functions in the private sphere. Of course, both corporations and governments have some need for secrecy, but the more they can be open, the more we can knowledgeably decide whether to trust them.

This makes the debate more complicated than simple personal privacy. Publishing someone's private writings and communications is bad, because in a free and diverse society people should have private space to think and act in ways that would embarrass them if public.

But organizations are not people and, while there are legitimate trade secrets, their information should otherwise be transparent. Holding government and corporate private behavior to public scrutiny is good.

Most organizational secrets are only valuable for a short term: negotiations, new product designs, earnings numbers before they're released, patents before filing, and so on.

Forever secrets, like the formula for Coca-Cola, are few and far between. The one exception is embarrassments. If an organization had to assume that anything it did would become public in a few

years, people within that organization would behave differently.

The NSA would have had to weigh its collection programs against the possibility of public scrutiny. Sony would have had to think about how it would look to the world if it paid its female executives significantly less than its male executives. HBGary would have thought twice before launching an intimidation campaign against a journalist it didn't like, and Hacking Team wouldn't have lied to the UN about selling surveillance software to Sudan. Even the government of Saudi Arabia would have behaved differently. Such embarrassment might be the first significant downside of hiring a psychopath as CEO.

I don't want to imply that this forced transparency is a good thing, though. The threat of disclosure chills all speech, not just illegal, embarrassing, or objectionable speech. There will be less honest and candid discourse. People in organizations need the freedom to write and say things that they wouldn't want to be made public.

State Department officials need to be able to describe foreign leaders, even if their descriptions are unflattering. Movie executives need to be able to say unkind things about their movie stars. If they can't, their organizations will suffer.

With few exceptions, our secrets are stored on computers and networks vulnerable to hacking. It's much easier to break into networks than it is to secure them, and large organizational networks are very complicated and full of security holes. Bottom line: If someone sufficiently skilled, funded and motivated wants to steal an organization's secrets, they will succeed. This includes hacktivists (HBGary Federal, Hacking Team), foreign governments (Sony), and trusted insiders (State Department and NSA).

It's not likely that your organization's secrets will be posted on the Internet for everyone to see, but it's always a possibility.

Dumping an organization's secret information is going to become increasingly common as individuals realize its effectiveness for whistleblowing and revenge. While some hackers will use journalists to separate the news stories from mere personal information, not all will.

Both governments and corporations need to assume that their secrets are more likely to be exposed, and exposed sooner, than ever. They should do all they can to protect their data and networks, but have to realize that their best defense might be to refrain from doing things that don't look good on the front pages of the world's newspapers.

This essay previously appeared on CNN.com. I didn't use the term "organizational doxing," though, because it would be too unfamiliar to that audience.

Posted on July 10, 2015 at 4:32 AM • 43 Comments