Who can CISOs trust? Sharing information is both essential and a professional hazard

Chad Thunberg
February 3, 2022 6 minute read

President Biden's recent executive order on cybersecurity calls on the public sector to work with private companies to create more secure environments and emphasizes the importance of sharing information as a best practice. Many of us may see "information sharing" as a synonym for risk or liability as information sharing requires a lot of caution. Handled incorrectly, you may increase the exposure of a vulnerability.

At Yubico, we approach information sharing as a necessity that must be done judiciously. We work with highly sensitive information on a regular basis, and carry responsibilities for the security and risk management practices of corporations. That corporate structure carries a fiduciary responsibility to shareholders, and any information sharing has to be considered against the risk of violating that responsibility.

Tackling this topic as it relates to the public and private sectors will require much more debate. Instead, I'd like to start by sharing how I think about risks related to information sharing and how I've approached mitigating these concerns on a personal level.

Losing control

When information is shared, the responsibility to protect that information is extended or distributed. Like a password accidentally shared in a Tweet, once information is out there, it's no longer under your control. Each individual with access to information must be trusted to keep it in confidence, even when they might be at their worst.

There’s a well-known bar in Seattle where many security professionals meet weekly to unwind and swap stories. Seattle is a Mecca for security professionals, including those focused on the discovery of software and hardware vulnerabilities in new products. It’s a combination made for leaks: free-flowing alcohol and people with highly sensitive information in their heads!

Inevitably, someone has too much to drink. The alcohol, in turn, loosens the tongues of those who were already prone to tell stories they shouldn’t. Why tell those stories? Often it was the need to be admired, the need to be seen as the “big fish” in the pond, or some other personal self-doubt or insecurity. The result could have been a mishandled remote code execution bug and a termination of a contract, if not something more impactful.

If you’ve ever witnessed something like this, it serves as a lesson learned: Keep your cards close to the vest unless you want someone else’s loose lips sharing them with others who might gain advantage from them.

So we all know there’s plenty of risk when you share, but what’s the risk of not sharing?

The downside is that when we build moats, we make our organizations into islands. The reluctance to connect with peers to seek guidance or to compare notes — and then missing some important information that catches up to you later — could be just as damaging as sharing too much with the outside world.

Who do you trust?

When a breach happens, there’s a tendency to want to raise the drawbridge. However, it could be helpful to reach out to peers to see whether they’ve seen a problem, contained one, or are responding to one. Having this additional information early on can significantly help your organization’s response to a breach, which corrects potentially damaging missteps.

This is a calculated risk not to be taken lightly. Who can you trust with a two-way sharing of information? Here are a few best practices I’ve found that have helped me through the decades:

- **Start with a pre-established set of relationships** — an inner circle of trusted people — who you’ve known for years and have had time to observe their behavior in previous information-sharing scenarios. I regularly meet with security leaders that I’ve known since the start of my career. The long history and shared experience allows for comfortable and relatively safe bi-directional conversations.

- **Be familiar with the consortiums or associations that facilitate security information sharing**, like the Information Sharing and Analysis Center (ISAC) set up for particular industries. Infraguard is also a good resource, especially for individuals and companies involved with the local and federal government.

- **Find secure messaging systems that help you start one-to-one or group conversations with your inner circle.** I use Signal and Keybase (now acquired by Zoom) for the more sensitive conversations. Slack and your favorite video conferencing solution are used for staying in touch.

- **Learn from your mistakes and those disclosures you now regret.** I have made some disclosure mistakes over my career. In one particular instance, it was with an impressive interview candidate. The risk did not pay off and the mistake almost led to a public disclosure that would have been disruptive to my career.

- **Get executive buy-in internally before sharing and problems happen.** As a representative of the company with sensitive information, it just makes sense to let the appropriate executives know what you're doing and get sign-off to operate freely. It doesn't hurt to inform the legal team so they can provide any legal or regulatory guidelines for what you can and can't share. If some mistake is made down the road, you're more likely to have support from the company's leaders rather than get thrown under the bus. Make sure to establish these internal relationships and lines of communication early.

Don't let fear rule the day

Even aging is a risk in this business. As you get older, you naturally get more cautious because of all those valuable "lessons learned." CISOs need to form a network of friends who understand the technology and that they can also trust, which can take years. You can augment this process with some associations that help with information circulation, but in the end, you really need friends with whom you can discuss the details with.

The agile CISO has to somehow get past being overly cautious and act strategically on information sharing. That freedom to talk can make the difference between smart preemptive action that prevents the next crisis and catastrophe.