Published on *The National Law Review* https://natlawreview.com

Media Query Call on Line 1: Do’s and Don’ts from an Information Security Officer

Article By:

Privacy & Security Practice Group at Mintz Levin

Putting your organization’s name in the paper can be a boon to both your business and your career. The ego stroke isn’t bad either; it can be quite a jolt to see your name in a trade or general news publication for the first time. Speaking with the press on information security, however, has unique pitfalls for you and your company if you are not prepared.

The Information Security field is all about mitigating risk, and this brief post will help you mitigate risk before you have that phone call with the Metropolis Business Journal.

Consult with your CISO, Counsel and PR Director (or equivalent)

Your Chief Information Security Officer (or closest equivalent) is going to have their fingers on the pulse of the latest security news – that’s part of their job. If your interview might cover the latest breach in the news, your CISO may have greater insight into what happened and how it impacts your organization. You should also ensure that you are both on precisely the same page in terms of security priorities and projects (and what you are comfortable sharing about them).

Counsel will help you navigate the close relationship between data security and the law; make sure that you understand how statutes and regulations impact your firm before speaking about them in public. This is all the more important if your business covers multiple states or nations.

PR, your CMO or whomever speaks with the press regularly for your organization should be a close ally no matter the topic. They know the lay of the journalistic land and know the professionals as compared to those that will mangle your quotes and misrepresent you to the world. Even if you’ve had regular experience speaking to the media, make sure that you are in line with the PR policies and culture of your organization.

Do’s and Don’ts on Information Security Interviews

Do convey professionalism and try to stick to business-like language at all times. Say “Keeping all of our systems tracked and patched” sounds better than “Find all our stuff and patch it.”. It may be difficult to avoid using more casual language over the course of a long conversation, but when hitting your major points do speak as if there are hundreds or more listening (because there are).

Do convey that you understand the risks to your business. Whether it's competition that wants your intellectual property or concerns about a malicious insider, you want your customers and business partners to know that you are on the case. Avoid deemphasizing risks, as this may make you appear disinterested in the topic and ignoring a potential hole in your security program. Recently a CIO was quoted in an article saying that mobile device security was not a concern. Perhaps that CIO had a solid mobile device management program and could track every bit coming and going from their iPhones, but the article did not read that way.

Don't portray yourself as invincible. This is a given; do not throw down the gauntlet and dare those who would otherwise ignore you from trying to knock down your web site (or worse).

***Don't expose your weaknesses*. ** Are you a company of over 1,000 people and you lack a dedicated full time person to the protection of your electronic information? If so, a) you're asking for trouble and may already have it and b) you really don't want to let the world know it. Don't publicly share critical pieces of your security infrastructure without serious thought about how that information might be used against you. If there are entire elements of your security program that haven't even been implemented (e.g. password policies, mobile device management, security awareness, vulnerability management, etc) do not discuss them on the record with a journalist.

Don't help perpetuate myths and stereotypes about information security. Improving security doesn't always mean spending the most (or any) money, or making things more difficult to get the job done. Security documentation never needs to be endless tomes of legal and technical jargon. We need to let our management know that we can be effective and judicious in our use of time, money and resources. We are there to partner with and protect the organization, not (as was recently conveyed in an article by someone in a security role) to just encrypt everything we can and put extra passwords on our computers.

We're all in this together

What you say may be used against you by putting not just your organization but your entire industry in a bad light. While partnering with your industry peers is a topic for another article, know that you are being watched with Google Alerts and news services every time you appear in a blog or newspaper. When you speak, make sure that you have a clear, concise and accurate message about information security being a top priority.

William Kyrouz is Mintz Levin's Chief Information Security Officer and our guest blogger. His "views from the CISO" will be posted from time to time.

National Law Review, Volume V, Number 272

Source URL:https://natlawreview.com/article/media-query-call-line-1-do-s-and-don-ts-information-security-officer