COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 12. December 09, 2021 'Don't Say Breach in an Email': Tips for Security Incident Response Plans

By Theresa Defino

Minneapolis-area attorney Brad Hammer recalled an instance where a client's chief information security officer (CISO) emailed him and the privacy officer, and said, "We've had a breach incident; we need to get on the phone."

Eh, not the best way to start off responding to a security incident or breach, he said.

"First, don't say breach in an email," said Hammer, a privacy and security expert and founder of the Vakaris Group. In this case the CISO was "brand-new," hired perhaps only two weeks prior, and she had a brand-new second-in-command.

"The first question that the privacy officer and I asked is, 'Are you deploying the incident response plan?' And they said, 'We have an incident response plan?'"

Hammer was stunned by this response and told the privacy officer later that it was "concerning on so many levels, because, one, you would think that would be something that they would discuss in transition" because the old CISO was still around. "It wasn't as if [the previous CISO] had left in shame. Arguably there should have been some meetings there where they talked about handing things over."

Secondly, "I have concerns about the new CISO that [she] never asked if there was an incident response plan, especially as an incident was occurring. Maybe she hadn't had a chance to dust it off yet, but she and the second-in-command were acting on any number of items" following a possible breach without the benefit of reviewing the incident response plan, Hammer said.

First Call? Not the Lawyer

Hammer talked about incident response plans during the recent Compliance & Ethics Institute, sponsored by the Society of Corporate Compliance and Ethics, co-publisher of *RPP*.[1] He also discussed overall HIPAA compliance, stressing the importance of building relationships with information technology (IT) and other members of a compliance team.[2]

Frequently Hammer works with human resources (HR), IT and marketing employees of his clients, "especially where I am sort of supporting the privacy officer role, serving as pseudo privacy officer." He recalled an incident when an HR manager called at 7 p.m. on a Friday evening saying, "We had a breach; this is what happened."

In response, Hammer said, "'Well, did you call IT/security?' He said, 'No, I called you.'"

Hammer said he explained that the lawyer should not be the first call. After a breach, "the function within the organization [in the lead] needs to be IT," he said.

When a covered entity (CE) or business associate (BA) is in the thick of a breach, "the first step is you need to stop whatever...it is that is going on. Lawyers don't know how to do that," Hammer said. "I'm fully willing to admit

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

there's a lot I don't know how to do, and that's one of them. Involve us, certainly, because you want things under [attorney-client] privilege. But don't call me to stop the breach, because I don't even know where to start."

So, who's on the team? Who's running the show after a breach? As Hammer mentioned, he believes, particularly in an ongoing breach, that IT staff should be at or near the top. The individuals who need to play key roles in an incident response plan, in Hammer's view, are:

- IT, IT security, and security (maybe the same, possibly different roles).
- Legal or compliance.
- HR.
- C-suite, executives, boards of directors.
- Customer relations, communications and/or public relations.
- Audit.
- Shareholder management.
- Business development or marketing.
- Union leadership.
- Finance.

This document is only available to subscribers. Please log in or purchase access.

Purchase Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.