COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 11. November 11, 2021 Compliance Refresher: Get Cozy With IT Folks, Review Insurance, Fine-Tune Policies, Training

By Theresa Defino

Attorney Brad Hammer doesn't always don a suit and tie, or what he calls his "lawyer's uniform." A privacy and security expert and founder of the Vakaris Group based in the Minneapolis area, Hammer found that dressing to match the folks he meets goes a long way toward eliciting the vital information he needs to help craft security policies or review ones already in place.

As he discussed during a wide-ranging talk at the recent Compliance & Ethics Institute, sponsored by the Society of Corporate Compliance and Ethics, co-publisher of *RPP,* security or information technology (IT) departments at HIPAA covered entities and business associates often have good policies and procedures in place—but there are limits.[1]

Security officials are "really good at writing policies about acceptable use and password requirements and any number of things related to security or protecting data," Hammer said. But, adding he meant "no offense" to security officials, these individuals "are really, really bad…at communicating those policies. No one in the organization knows [the policies] exist."

The answer, he said, is to "take the people who are good at communicating policies, the compliance people, [and have them] go talk to the information technology and security people." The goal is to "share with everybody how awesome the policies are and help with the protection of the data," he said.

Hammer prefaced his remarks by sharing a sobering July report by IBM and the Ponemon Institute,[2] which quantified the costs of data breaches from 2020. The cost of mitigating a health care breach was estimated at $9.23 million, slightly more than a general U.S. data breach but more than twice the cost ($4.24 million) of a breach globally, based on data from firms in 17 countries.

Hammer said the cost is important to know as it could help organizations fight for more funds to prevent and safeguard against these breaches; most, he said, likely need more resources and personnel.

Looking again at the cost of a global breach, of the $4.24 million, lost business accounted for $1.59 million or 38% of the total; "detection and escalation" accounted for $1.24 million or 29%. Post-breach response was estimated at $1.14 million, or 27%, with notification costs estimated at $270,000, or 6% of the total.

Common Vectors Include Phishing

The report showed that even a relatively small breach of 500 records can be costly to manage—the range was $80,000 to $120,000. According to Hammer, the previous year's report noted that the cost of a single breached record in the United States was $242, "so small data breaches do cost a lot of money"—and generally more than elsewhere in the world.

The new report also showed that organizations that employed both incident response teams and incident response planning faced lower breach costs—$3.25 million versus $5.71 million.

According to the report, "the most frequent initial attack vectors were (1) compromised credentials, 20% of breaches (2) phishing, 17% (3) cloud misconfiguration, 15%. Business email compromise was responsible for only 4% of breaches but had the highest average total cost at $5.01 million. The second costliest initial attack vector was phishing ($4.65 million), followed by malicious insiders ($4.61 million), social engineering ($4.47 million), and compromised credentials ($4.37 million)."

As Hammer put it, "your employees and their access to your systems are, continually, the most critical vector in terms of the cause of the breach." This means "getting policies in place" and providing training "is as important as any encryption, firewall" and other technical tools that an organization can implement.

As an aside, Hammer said he actually doesn't like to use the word "hacker," saying it "implies that you didn't do anything wrong." Maybe a breach could have been prevented, but in all cases, "there's probably some lessons to be learned about either improving security or improving policies," he said.

The new report also showed that the average cost of a "mega breach" affecting 50 to 65 million records was $401 million, at the top end, while a breach of 1 to 10 million records cost $52 million.

It is critical to be aware of lost revenue and customers, which result from "business disruption, revenue loss, system downtime, cost of loss customers [and] reputation harm," said Hammer, who called the final item "really important."

Ironically, the two areas where organizations spend the most amount of time negotiating in their contracts—breach notification and post-breach response—"are going to be your smallest areas of costs," said Hammer. These include call centers, providing credit services and reporting the breach to authorities.