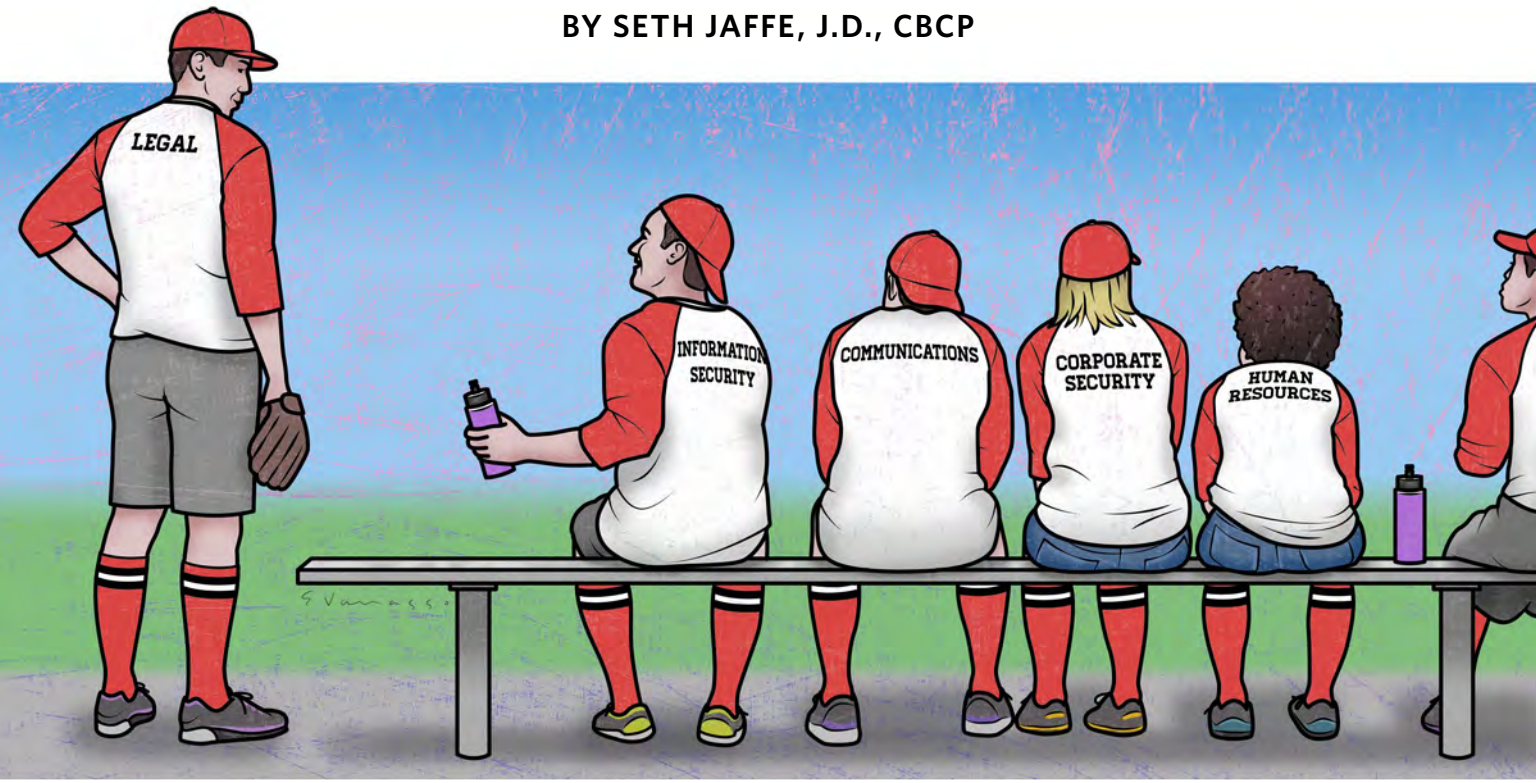
IMPROVE YOUR INCIDENT RESPONSE

Ways to leverage your legal team and others prior to a cyber event

BY SETH JAFFE, J.D., CBCP



MOST INCIDENT RESPONSE PLANS arise within the information security or information technology departments, but in-house counsel certainly has a dog in the fight. When cyber events rise to the enterprise level, it's all-hands-on-deck to respond efficiently and effectively, and counsel is on the front line.

All too often, though, the legal department is left out of an incident response until late in the game, oftentimes leading to inflated damages from subsequent data breach litigation. That doesn't need to happen, so let's explore opportunities for cybersecurity and legal to work together.

ILLUSTRATION BY ENRICO VARRASSO

ESTABLISH A CYBERSECURITY COMMITTEE

In the face of lackluster cybersecurity policies, members of a company's board of directors may find themselves personally liable for a data breach.[1] As a result, numerous authorities recommend including on the board a member with cybersecurity knowledge.

That's not always feasible, so a second option is to create a cybersecurity committee tasked with briefing the board at regular intervals. A cybersecurity committee should include, among others, representatives from information security and legal, both of whom are instrumental in assisting the board with enforcing policies sufficient to satisfy the directors' duties of care and loyalty.

EXPECTATIONS FOR ATTORNEY-CLIENT PRIVILEGE

Information security personnel, in their desire to bring a cyber incident under control, all too often jump the gun by engaging forensic vendors without involving a legal team member. The communications and reports from that engagement can come back to haunt the company in post-breach litigation.

Known as "attorney-client privilege," communications to and from legal representation for the purpose of obtaining legal advice are, for the most part, protected from disclosure. Early involvement of legal provides the opportunity to bring third-party vendors under the privilege, which in turn allows for better communication during a stressful and time-crunched period.

The privilege plays out within a company itself as well, allowing the incident response team members to freely discuss what may have been the cause of the incident without fear that said communications will become evidence of culpability in a subsequent jury trial.

Even without the privilege, the legal team member should brief the incident response team early about communication best practices. As an example, team members should avoid conjecture, instead focusing on the facts and limiting communication only to what is required.

In addition, team members should limit communications to those with a need to know, and they should make clear that those communications are confidential and, if applicable, attorney-client privileged.

NEGOTIATING CYBERSECURITY INSURANCE

Enterprise-wide cybersecurity events generally come with dollar signs attached, the cost of which can be difficult to stomach.

Many companies choose to take out cybersecurity policies to offset that cost, but like any insurance, there are exceptions and exclusions. In recent cases now working through the courts, insurance carriers have denied claims on numerous bases. Failure to comply with minimum required procedures and risk controls, for example, has been the cause of a denial.

In one example, restauranteur P.F. Chang's found its claim denied because the carrier argued that the restaurant was not injured by the cyber breach, but rather its customers were injured. Sony got a taste of the "incorrect party" denial as well when its carrier refused to pay a violation of privacy claim because, as Zurich Insurance argued, it was the hackers who published the material, not Sony. And lately, carriers are denying claims citing the "act of war" exclusion, arguing that attacks facilitated by nation-state actors are outside the cyber insurance policy.

For data breaches originating with a third-party vendor, claims are often dictated by contractual obligations written years before in applicable master services agreements.

What's clear, in light of the aforementioned claim denials, is that legal and information security should work together during procurement and negotiation of cyber insurance policies—not only to minimize exceptions and exclusions, but also to understand them as applied to ongoing policies and procedures.

And the legal implications of cost shifting do not stop at insurance claims. For data breaches originating with a third-party vendor, claims are often dictated by contractual obligations written years before in applicable master services agreements. Here again, legal must work with information security to settle on cybersecurity provisions correctly tailored for each vendor in view of the types of data processed by the third party.

FULFILLING NOTIFICATION OBLIGATIONS

At present, all 50 U.S. states have data breach notification laws on the books, obligating a company to disclose certain facts of the breach to either the affected data subjects, a state authority like the attorney general, or both. Notification obligations, however, differ by jurisdiction.

It is the job of the legal team member, and outside counsel, to assess whether a cyber incident has risen to the level of a breach, thereby triggering obligations within the law. Notification obligations, however, do not live solely in state data breach laws, but also are found at the national level, internationally, through associations and contractually.

In carrying out required notifications, the legal team members assume a number of roles. They work with the communications department to craft the language of the notification letter, ensuring it meets state requirements. Where data breach notification vendors are needed, legal engages and manages them to ensure compliance with law. And early participation in the incident response process better prepares legal to field inquiries from regulators.

DATA BREACH LITIGATION

Class action suits stemming from data breaches are on the rise. As a result, companies victimized by cyberattacks find themselves having to relive the breach in a courtroom.

Certain measures can be put in place prior to a cyber event that will situate a company on more favorable footing when plaintiff attorneys come knocking. Standing to bring suit, for example, is a major issue in data breach litigation and can offer a strong defense in protection of a victimized company. Plaintiffs must show an injury in fact, a causal connection between the claimed injury and the defendant's acts, and that the alleged injury would be redressed by a favorable decision in the lawsuit.

Working together, information security and legal can put in place policies and procedures that lessen the chance for the plaintiffs to get past the second prong—causality.

Working together, information security and legal can put in place policies and procedures that lessen the chance for the plaintiffs to get past the second prong—causality.

Attorneys often play the long game; during an incident, legal members of the incident response team will be preparing for litigation by quarterbacking litigation hold notices, overseeing electronic discovery, memorializing facts that may prove useful at trial, and organizing the theory of the case.

UPDATING THE INCIDENT RESPONSE PLAN

Many cybersecurity laws already mandate regular updates to a data security program;[2] regardless, it is just good practice.

Updates should occur in numerous instances, including upon major changes in infrastructure, as a result of organizational change, due to new programs that affect the privacy of data subjects, and at least annually in view of changing laws and regulations.

For obvious reasons, the legal team member, in conjunction with information security, should lead this initiative. Failure to do so may well paint a target on the back of the company, leading to regulatory oversight, fines, public relations nightmares and litigation.

DATA SECURITY IS A TEAM EFFORT

In a few short years cybersecurity has moved from relative obscurity to the forefront of compliance and risk mitigation. Consequently, data security is a team effort involving nearly every department related to compliance. Yet many information security departments are still going it alone.

Now is the time to establish ongoing relationships with other participants of the incident response team, whether they be the communications department, corporate security, human resources or especially legal.

In-house and outside counsel can be an invaluable partner to information security teams in lowering risk and protecting the company from damages associated with cyber incidents. Information security professionals would do well to take their own advice—don't wait until you're in the midst of a breach to make your move. Bridge the gap in your institution today. ■

SETH JAFFE, *J.D., CBCP, is vice president of incident response and general counsel for LEO Cyber Security.*

FOOTNOTES:

[1] The directors of Home Depot, Wyndham Hotels and Target faced shareholder derivative suits following their respective data breach events.

[2] As an example, the Alabama Data Breach Notification Act ("adjustment of security measures to account for changes in circumstances"); FTC Red Flags Rule ("Ensure the Program is updated periodically"); HIPAA Security Rule ("update as needed"); Massachusetts CMR 17.03 ("Reviewing the scope of the security measures at least annually"); NYDFS Section 500 ("assessed and updated as necessary by the CISO").