ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

You've Been Breached During the Holidays: Now What?

Technology, Privacy, and eCommerce

Editor's note: ACC Docket *is republishing this holiday-themed article, as it is timely and helpful for general counsel to mitigate cybersecurity risks. Although this was published pre-COVID and the suggestion for leadership to reconvene in the office during lockdowns is unlikely, this critical message*

still applies: General counsel must be on high alert for breaches during the holidays. Read more to see if your cybersecurity team is prepared this holiday season.

It was the start of the Thanksgiving holiday when the GC of a large retail company got an urgent call from her CEO. “We’re under attack. I just got off the phone with IT and we have been hacked. Ransomware and a DDOS. Call whoever you need to call, notify whoever you need to notify, and get this fixed.”

A crippling attack on a retailer and its website right before Black Friday, and on a day in which few people work, is not a coincidence. Hackers often time their attacks for maximum effect. This fact, which extends to all industries, leads to the critical question: What do you do when it happens to you?

One way to start thinking about the answer is to take a step back and ask: Why is the CEO calling the GC? Isn’t this an IT problem?

To be absolutely clear, cybersecurity is far more than just an IT problem. Companies that have been the subject of high-profile breaches have found this out the hard way, as CEOs and GCs have lost their jobs as a result.

In fact, there is a reason why these leaders are often fired after a hack, because the worst-case scenario is not the attack, as bad as that may be, but the litigation, regulatory enforcement, and reputational damage that can follow. Long after IT has remediated the problem, the aftermath of a successful attack can stay with the company, draining precious resources and lingering in the minds of consumers, clients, and the public. Conversely, sound planning and sufficient senior-level attention to cybersecurity, including the GC, significantly mitigate the fallout and allow the company to bounce back from a breach more quickly and fully.

Ultimately, the key is to have a written, proactive, holistic, risk-based, and well-practiced incident response plan — one that reasons backwards from that worst-case scenario. A critical element of the plan is knowing, in advance, whom to call, even on Thanksgiving. As a breach scenario can lead to litigation, it is important for lawyers to help lead the response and enlist any outside counsel, cyber forensic consultants, or crisis communicators.

Crises often beget panic. Without a clear plan, different employees will go off on their own or all do the same thing, much like little kids playing soccer. Knowing the right people to call, and having relationships with them in advance, can severely cut down on that debilitating phenomenon.

The GC or her designated cyber counsel should have the 24-hour contact information and those trusted relationships in advance, or at least have the relationship with outside counsel who can bring in others and help lead the response. That contact information should not be kept only electronically, especially as firm IT resources can be disabled during a cyber event.

[Related: ACC 2020 State of Cybersecurity Report]

Furthermore, a company stands a far greater chance of protecting the forensic reports after breaches or the drafts of required notifications to regulators when they have been prepared under the direction of counsel. Those firms that have their IT departments call in forensic consultants directly, however, often find their reports not only lacking in privilege, but drafted in a way that could favor the plaintiffs.

As state and global jurisdictions have significantly varying notification requirements and timelines, the

lawyers can help ensure that those regulatory obligations are met. Equally important, what a company says in those notifications is as crucial as when and if they say it.

Crafting the regulatory notifications and public statements in the right way is essential, especially as facts often change during a crisis, and these notifications can be used against the company in subsequent litigation, enforcement actions, or even before Congress. Having skillful lawyers involved from the beginning, and having a plan that explicitly requires all regulatory and public statements to have a legal review, can greatly diminish the risk of litigation, regulatory enforcement action, and lasting reputational damage.

GCs also play a key role in whether to call in law enforcement to assist during and after a breach. There are many advantages to partnering with law enforcement, as they often have the latest intelligence and may even be able to provide classified briefings to select company officials. They can also help consolidate investigations during a company-wide breach. However, there are risks to calling in the feds, so in-house or outside counsel should be involved in this decision and they should have the direct lines of key FBI cyber personnel and Assistant US Attorneys at the ready.

Once the GC gets back to the office — which, if she knows whom to call, may not have to be until after the Thanksgiving meal — the GC or her designated cyber counsel will likely be called upon to help lead the internal investigation or coordinate those efforts by outside counsel and cyber forensic companies. That is not the time for the GC or her trusted designee to “learn cyber.”

Rather, they should have the trusted internal relationships, the trusted external relationships, as well as a facility with the technology. Oftentimes, it will be the lawyer who must translate “tech” to senior leadership, and it is often up to the lawyer to challenge technical decisions to make sure they are reasonable, defensible, and grounded in a solid risk assessment.

Thanksgiving should be a happy time, and time spent with family, or at least away from the office. However, the less convenient a time it is for you, the more convenient a time it is for the hackers. That is why having a proactive, holistic, risk-based and well-practiced plan is so important, which not only helps prevent successful attacks but also allows you to know what to do and whom to call when that call comes.

Erez Liebermann

Chief Counsel on Cybersecurity and Privacy Matters

Prudential Financial

Liebermann also serves a point of contact to regulators and law enforcement on cybersecurity matters. Prior to joining Prudential Financial, Erez spent 10 years as a federal prosecutor.

Michael Bahar

Co-Leader of the Global Cybersecurity and Privacy Team

Eversheds Sutherland

He was previously general counsel and staff director to the US House Intelligence Committee, and

former deputy legal adviser to the National Security Council at the White House.