Building Cyber Resiliency: Preparing for the Cyber Incident *Before* it Happens

Client Alert
11.20.2024

Cybersecurity articles and webinars are quick to advise on what to do when the cyber incident happens. While this advice is extremely helpful—and I certainly have authored and presented many of these post cyber-event focused articles and webinars—my recent focus has been to advocate the steps one can take in advance of the cyber incident. In other words, short of implementing the typical cyber defenses, what else should companies do? My simple response is this: prepare for the event as if it will happen and don't assume your defenses are perfect.

Building Resiliency

So, how does a company build that resiliency? There are three basic steps: create the Incident Response Plan (IRP), recruit the Incident Response (IR) team, and implement robust and comprehensive training that includes full-scale tabletop exercises. In my experience, it is the rare client who appears with its IRP in hand and IR team in the wings. Most clients need immediate help and advice, and hours, if not days, can be wasted in the immediate aftermath of a cyber incident with the client wondering if its insurance policy will cover the event, and if so, what will it cover, whether its policy requires paneled experts (and if not, where does one find those experts), what laws apply, who needs notification, and more. When properly prepared and used, IRPs are well worth the time and energy it takes to prepare them because most of these questions will be answered as the IRP is drafted. IRPs become valuable roadmaps for navigating the early chaotic hours of a cyber incident. In addition and as noted above, they are extremely useful tools during the *process* of their preparation, for as the initial IR team drafts the IRP, they must identify, connect with, and gain buy-in from their internal and external IR teams and familiarize themselves with the function and interconnection of the entity's basic digital

Related People

Claudia Rast
Shareholder

Related Services

Cybersecurity and Privacy Specialty Team infrastructure. The IRP and IR team are critical to the entity's successful response and recovery from a cyber incident. The real trick is to ensure that the IRP does not languish on the company server, and the internal IR team does not forget its training. The IRP should be printed out and tucked into the laptop case or backpack of every internal IR team member, and training that includes tabletop drills should be an annual exercise.

Retain External IR Experts

Whether your IT staff is internal or external, unless their day job involves digital forensics and cybersecurity, you should engage specialized and experienced third parties to assist with incident response. Experts in forensics, law, and public relations are the main external partners of the IR team, and their skill and experience are invaluable. Cyber insurance policies will generally list paneled legal and forensic teams, but it is the rare insurer that will refuse qualified experts as long as they agree to the insurer's panel rates. Once vetted and engaged, these external IR team members can conduct periodic vulnerability assessments and be active participants in your tabletop exercises with internal IR members. Contact your insurance broker to confirm pre-approval of these external IR team members.

CISA also offers a wide variety of tabletop exercise packages for download: Click here to preview.

The FBI is another helpful partner when the cyber incident occurs. The Office of Private Sector oversees the Bureau's effort to increase collaboration and information sharing with the private sector. Check out this link describing how the FBI works with businesses. Building relationships with the FBI and/or CISA agents in advance of an event allows sufficient familiarity for all to be ready, willing, and able to work together when the inevitable incident happens.

Final Thoughts

Perhaps the most important message is the realization that you are never "all set;" the measures you implement, the tools you deploy, and the training you roll out must be subjected to continuous scrutiny and updating. Everyone from the C-Suite to the storeroom must participate in—successfully—cyber scenario training. ***Every person in your company represents a potential pathway for threat actors to find and exploit***. In sum, draft your IRP, recruit and assemble internal and external IR members, and conduct periodic tabletop exercises. These measures create the resilience needed to survive a cyber-attack. Entities that actively prepare and train for cyber incidents are those that recover faster, better, and with far less economic loss than those who do not.

Please feel free to contact the author of this Client Alert or your Butzel attorney for more information.

Claudia Rast
734.213.3431
rast@butzel.com