INCIDENT RESPONSE SERVICES FAQ

GODFREY & KAHN TREND MICRO

Why Godfrey & Kahn (G&K)?

We are an Authorized Breach Coach® by NetDiligence, an honor we obtained by combining the thought leadership of a nationally-leading firm with the one-on-one attention and cost-effectiveness of a Midwest firm. G&K has deep experience working with all industries and all sizes of companies across the United States on incident response matters. We routinely work with small and mid-sized companies who may not have cyber liability insurance, and we understand the need to get your company back to business after an incident. Our team members carry certifications from the International Association of Privacy Professionals, including the CIPP/US, CIPP/E, and CIPM designations, and specific security certifications, such as CompTIA Security+ and ISC2 (CC).

G&K Attorney Certifications:

What is a Breach Coach and why do we need one?

A Breach Coach is invaluable to an organization's cybersecurity preparedness. While any cyber incident will require a knowledgeable expert to triage responses and guide a review of regulatory obligations, a dedicated Breach Coach can seamlessly step into this role already knowing your business, its priorities, and its stakeholders. That saves a lot of time—a scarce resource in the event of a cyber incident. With Godfrey & Kahn as your Breach Coach, we capitalize on that saved time by working with Trend Micro to contain and remediate any unauthorized access issues. That gets you back to work sooner rather than later, which saves you money.

What does a Breach Coach do if there's no emergency to address?

Outside of an emergency cyber scenario, your Breach Coach will focus on proactive ways to best position your organization in the event of an incident in the future. G&K can speak to your stakeholders and/or employees about technology and cybersecurity best practices, and we regularly give specialized presentations to our clients called "Tabletop Exercises," or hypothetical data breach scenarios that allow your stakeholders to practice how they'd respond in the event of a data incident. Additionally, we can assist in customizing your Incident Response Plan so that your company has easily-accessible resources on how to best respond, when to contact certain third-parties, and other steps designed to best shield against any regulatory or other third-party follow-up request or audit. Please see below for more information on Incident Response Plans, and please contact us if you would like to discuss our various service offerings further.

How does the relationship between G&K and Trend Micro work?

Trend Micro provides the digital forensic and cybersecurity acumen necessary to quickly identify, contain, and resolve instances of unauthorized system access, while Godfrey & Kahn analyzes the legal, regulatory, and contractual obligations and notification requirements for any applicable states or territories. As Breach Coach, Godfrey & Kahn will direct Trend Micro's efforts and keep you informed of all progress made.

GODFREY & KAHN

TREND MICRO™

Will G&K's relationship with Trend Micro affect its ability to keep communications under privilege?

When you sign up with G&K and Trend Micro, we will execute a tri-party agreement that states any incident response services, including any communications between G&K and Trend Micro, will be covered by attorney-client privilege. Protecting this information is important in the event that a security incident gives way to litigation, and invaluable to consider on the front-end of an incident.

Why is an Incident Response Plan (IRP) important?

When a security incident hits, every minute matters. An IRP is meant to guide your Incident Response Team through the steps that need to be taken immediately during an incident, in what order, and by which individuals, such that your company can resume operations as quickly as possible. Without an IRP, it's left to memory (fallible in a high-stress situation) and chance (something no one wants to rely on in a cyber incident). G&K regularly advises its clients on customizing an IRP, and we know the task does not call for a "one-size-fits-all" approach. We can help focus your IRP with the steps and processes most appropriate for your Incident Response Team and your company; addressing any risk areas while being mindful and cost-efficient in our final deliverables.

Who should be on my organization's Incident Response Team?

While there is no single answer for who best to include in your Incident Response Team, typically we see major stakeholders from departments including IT, HR, Accounting, and Marketing, as well as any C-Suite Executives responsible for day-to-day operations. If your organization maintains a large inventory of vendor agreements, you may want to include a representative from Procurement that has knowledge of customer and vendor relationships. Smaller organizations may want to include their entire IT team. Discussing how to best to staff and assemble your Incident Response Team is a common and important part of our work with clients.

What kind of cyber matters does G&K normally handle?

We regularly assist clients with both reactive and proactive cybersecurity initiatives. Our firm serves as Breach Coach for clients in nearly every industry including healthcare, financial services, insurance, manufacturing, education, trucking and transportation, technology, data providers, and governmental entities. We work with clients on their breach response plan, conduct tabletop exercises with their incident response team, and further advise on steps to take in connection with maximizing the likelihood of protecting communications under attorney client privilege.

The Godfrey & Kahn team has advised on hundreds of security breaches, incidents, investigations, or other similar cyber-related inquiries from its clients. In this capacity, the team has assisted clients in responding to regulatory inquiries from nearly every Attorney General office in the United States. The team also has coordinated investigations with federal law enforcement agencies including the Federal Bureau of Investigations and the White House Secret Service cybercrimes unit.

How long will it take to get on a call if an incident occurs?

We maintain two regularly-monitored methods for alerting us of a cybersecurity incident. Typically, any calls to our hotline (833-DATALOSS or 833-328-2567) or emails to our dedicated intake email address (incidentresponse@gklaw.com) are addressed immediately, and initial phone calls can usually be held the same day.

If you are the victim of a cyber incident, contact us at
incidentresponse@gklaw.com or **1-833-DATA-LOSS**