The General Counsel's Playbook for Working with Cybersecurity Consultants

By Sam Rubin, VP of GTM Strategy, Unit 42

When you are hit with a data breach, knowing who does what will help you respond expeditiously, effectively, and in a manner that minimizes risk to the enterprise. For that your company needs to have an incident response strategy in place. The General Counsel is critical to this process.

Introduction

In today's business and legal environment, corporate counsel plays a critical role when their company experiences a data security incident. General Counsels (GC) can no longer profess ignorance on "tech stuff" and pass the buck to Information Technology (IT). The frequency, sophistication, and severity of cybercrimes continues to increase. Every enterprise possesses sensitive information. When that information is compromised the door opens to a range of liability issues.

"There are only two types of companies: those that have been hacked and those that will be." Yet many in-house counsel remain unprepared.

Note I wrote "when" and not "if." Former FBI Director Mueller famously said that, "there are only two types of companies: those that have been hacked and those that will be." Yet many in-house counsel remain unprepared. Like a Little Leaguer stuck deep in right field, counsel knows they must catch the next data security incident that comes their way, but hope nothing happens.

The best advice? Don't fret about having to make the big play; prepare and plan your response ahead of time for when the ball comes your way. No one expects a GC to take over the IT department, collect forensic images, extract malware samples from memory, or solve the cyber crime. You will, however, be expected to know the proper steps to take in the event of a compromise, how to find the best help possible, and what pitfalls to avoid.

This paper offers practical strategies to better prepare in-house counsel for a data security incident.

Know When You Need Outside Help

To achieve readiness to respond to a data security incident, take stock of your organization's internal capabilities. Under what circumstances can your internal IT team adequately respond and at what point will they be in over their heads?

One tech company I worked with has its own dedicated information security team staffed with seasoned digital forensic experts who can respond to nation-state threat actors with confidence. On the other hand, I also worked with a publicly traded company that relied on a two-person outsourced IT team and a "datacenter" that consisted of two desktop computers in a broom closet. Your organization falls between these extremes. Assess whether you are more like company A or company B.

To find out, talk to your IT team. Ask who in the organization is responsible for information security. Speak to those people about the types of incidents they have handled in the past—how they investigated, how they contained the incident, and how they remediated any security gaps.

Seek out IT or security-based process around incident handling—including policies, procedures, and guidelines. Ask how the team might handle a hypothetical incident that involves access to and exposure of your sensitive data. Is data preservation, collection, and investigation part of the answer? Your discoveries will shape your sense of how long you should wait before calling for outside help.

An important part of this process is establishing an incident escalation protocol. This protocol should be a component of a broader incident response plan and should define escalation and internal notification procedures in the event of a data security incident. A well-developed protocol shared by IT, security, and legal teams ensures that stakeholders have a process for assessing an incident's potential impact. The protocol should identify an explicit point at which to alert counsel and senior management and at which to call in outside help. Find the sweet spot between keeping false alarms to a minimum and ensuring that genuine risks receive immediate attention and the appropriate response.

Who You Gonna Call?

If you already have a relationship with an incident response (IR) consultant, that's great. If not, start looking now—not in the midst of a crisis. Begin with your current set of trusted advisors. Your outside counsel's firm may offer a referral. Many national law firms have a privacy and/or data security practice that works regularly with cybersecurity consulting entities. Your insurance broker or agent can be a helpful resource too.

Many national law firms have a privacy and/or data security practice that works regularly with cybersecurity consulting entities. Your insurance broker or agent can be a helpful resource too.

Talk to these recommended providers to understand how they operate, how much they typically charge, and their relative areas of strength and weakness in terms of service delivery. As with any top-notch professional services firm, seek demonstrated subject matter expertise, responsiveness, and an organization that listens to and understands your needs. The firm you select should have direct experience in your industry and in responding to the types of cyber risks you face.

Consider entering into a contract with the IR consultant now, in advance of need or crisis. Many firms offer "IR Retainers" that run from a low upfront cost to hundreds of thousands of dollars. Typically, higher-dollar retainers include lower per-hour fees, pre-incident assessment services, and contractual service-level agreements guaranteeing response times. Find the mix that's right for you.

Assessing the Scope of the Incident

When an incident occurs, your IR consultants will first need to assess its scope. Through one or more initial meetings or calls, they will take time to understand your network infrastructure. If you've planned ahead and already have your IR team on retainer, the consultants may have already gained this requisite understanding during an initial assessment. Either way, they will determine what is known about the extent of the incident, identify technical competencies required for the investigation, decide how many consultants should be assigned, and create an overall project budget. The more transparency you provide—the more efficient the knowledge transfer—the better the prospects for a positive outcome.

These initial scoping calls are a two-way street. The consultant assesses your needs and the level of effort required. At the same time, you and your IT and security team assess the consultant's competence and fit for your needs.

For example, did the consultants take the time to listen and fully understand the problem? Were they responsive? Do they seem resourceful and sufficiently flexible to fit their services or delivery methods to your needs and environment? Do they demonstrate expertise in and knowledge of the type of incident you face? Do they have the capacity to support you at this time? If the answers to any of these questions give you pause, don't hesitate to reach out to another firm.

Structuring the Engagement

Be mindful of these important strategic considerations in how you structure your company's engagement with your IR consultant.

Given the sensitive nature of the investigation and potential downstream legal and regulatory risks, consider a three-party engagement letter. In this structure, your outside counsel retains the IR consultant on your behalf. This is the preferred method of protecting privilege in an investigation—the IR consultant works at the direction of outside counsel.

Prepare for the eventuality that while the investigation itself may remain privileged, the facts uncovered may require disclosure.

This arrangement is not bulletproof, however. Prepare for the eventuality that while the investigation itself may remain privileged, the facts uncovered may require disclosure.

Make sure you are comfortable with the confidentiality provisions in your engagement letter. IR consultants are often incented to share "war stories" about their more compelling engagements. These make for potent marketing materials or for presentations at industry conferences. Your contracts must prohibit this behavior.

Consider the budget. Incident response investigations can be expensive. But you needn't fork over a blank check. Your consultant's contracts should provide transparency about investigation pricing. These documents should clarify expectations on duration, hours, and deliverables. If you sign an engagement letter providing only a rate schedule, your next month's invoice will likely deliver a healthy dose of sticker shock.

Containment

You face a serious data security incident. It has escalated to a point beyond which you can manage it internally, and you have a trusted IR provider on board who has quickly assessed the situation.

Typically, when we are called upon to respond to an incident, our client's most immediate need is containment—to "make it stop." Containment refers to the immediate steps that must be taken to stanch the bleeding, limit the damage caused by the incident, and prevent further damage.

Whether you need to shut down remote access, remove a server from your network, or block a particular network port on the firewall, your IR consultant should be ready with practical advice. Typically, the IR consultant will make containment recommendations, but your IT team will be responsible for implementing the suggested changes to your network.

Stay mindful that containment steps can destroy digital evidence that might be relevant to the investigation. Weigh the benefits of containment against any detrimental effects containment actions might have on the integrity or availability of digital evidence. For example, completely wiping a server because the IT team suspects it is compromised may contain the incident, but it also destroys all evidence that might support an investigation into the incident. That's throwing the baby out with the bathwater.

Evidence Preservation and Collection

Your consultants will move quickly from containment to forensic investigation. Investigative objectives will vary depending on the incident. They include determining the initial vector of the compromise, what the attackers did in the environment, and what, if anything, they took.

Accordingly, the investigation will commence with the identification, preservation, and collection of relevant evidence. The environment and the specifics of the incident will define the scope of the collection. Your IR consultants may collect

"triage" forensic artifacts from live servers, images of RAM memory, historical firewall logs, or even create full-disk forensic images.

The need for speed must be balanced by the need to preserve and collect information in a forensically defensible manner.

Collection strategies must, by design, scale across thousands of endpoints. Speed is paramount. Regardless of the targets of collection, the overarching strategy in incident response investigations is to move fast. This need for speed must be balanced, however, by the need to preserve and collect information in a forensically defensible manner should the need later arise to defend or authenticate the findings.

A nimble and resourceful incident response practitioner will leverage the software tools and data sources already available in the enterprise. These might include firewall logging or a previously deployed endpoint detection, or security information and event management application.

Counsel's most effective role at this juncture is to act as project manager. Help ensure that the necessary resources from your company—both human and technical—remain available to the consulting team. As long as information flows easily between your IT people and your consultants, trust that the technical experts on both teams understand the variables and can chose the best path forward.

Let the Investigation Play Out

After the initial scramble to contain the compromise and collect relevant data, your IR consultants need time to perform their investigation. The consultants will parse log files, extract relevant digital artifacts, and create a timeline of relevant activity. They will search for indicators of compromise—traces left by the accounts, malware, and other software tools the attacker deployed. This iterative process often leads the team to new data sources and new systems as they follow the attackers' digital trail.

These steps take time.

If the incident affects only one or two systems, the investigation might take a few days. In larger compromises—such as Equifax, U.S. Office of Personnel Management, or Home Depot—investigations can take months. As the investigation unfolds, in-house counsel's main task will be assuring the availability of human and technical resources to the consulting team.

Patience

It can be difficult to stay patient when company stakeholders demand more information about the incident and insist something be done. Beware the danger in revealing early information or acting too quickly in response to it. Initial conclusions about the scope of a compromise seldom align with what becomes known when the dust settles. Equifax, for example, is still updating how many user accounts were compromised 10 months after its breach. Months after its initial disclosure, Facebook disclosed that an additional 37 million user accounts were improperly accessed by Cambridge Analytica.

Update Calls

Find a cadence for investigation updates that satisfies company stakeholders and works for the consultant team. Give the team all the time and space you can. Pressure for frequent updates always accompanies a serious incident response. But daily update meetings can hamper the IR team and increase costs. This proves especially true given the effort required to organize and prepare for update calls. Add to that effort the time and resources diverted from the investigation itself. In my experience, even in rapidly evolving situations, two or three update calls per week strikes the right balance.

When the regulators and plaintiffs' attorneys come calling, a comprehensive forensic report is your best record regarding the incident, the state of the information security environment at the time of the compromise, and your response.

The Forensic Report

Most data security incident investigations require a forensic report. Ideally, the report should address: how and when the intrusion occurred; whether the attacker accessed or acquired sensitive or regulated data; the controls put in place to address the compromise; and how your company remediated any exploited vulnerabilities.

When the regulators and plaintiffs' attorneys come calling, a comprehensive forensic report is your best record regarding the incident, the state of the information security environment at the time of the compromise, and your response. Be prepared to come forth with the facts you intend to litigate. A thorough forensic report often serves as critical evidence. It demonstrates that your company had "reasonable" security safeguards in place and that you acted appropriately in a timely manner to notify regulators and affected customers.

As counsel, you will play a significant role in drafting the forensic report. Under privilege, work with the consultants on drafts to make sure you can understand what it says and that it properly addresses the issues. The forensic team's understanding of the legal risks of particular language will not match your understanding. Watch out for words loaded with legal meaning, such as "personal information" or "breach."

Until the time is right, hold the report close. Its disclosure should be undertaken as a highly strategic decision. The same information that might otherwise serve as your shield can be twisted and wielded as a sword by plaintiff's attorneys to expand claims against the company.

That said, the consequences of not having a report can be far worse. The efficacy of your incident response will prove crucial in demonstrating reasonable security safeguards. As you oversee preparation of the report, your overriding goal should be to demonstrate that the company undertook a comprehensive and appropriate response to the incident.

Moving Forward

Your IR consultant's forensic report will often contain recommended actions to further remediate the IT environment. This could mean re-imaging systems, adding additional security controls, or making configuration changes to your company network. These necessary steps are only a beginning. In the wake of a serious incident, your company should consider an enterprise-wide assessment or review of your information security program.

In the wake of a serious incident, your company should consider an enterprise-wide assessment or review of your information security program.

You should pursue two strategic objectives:

- In the short term, take affirmative steps to improve your information security program to help defend against any pending litigation or regulatory inquiry. Demonstrate to regulators that you take the incident seriously. This helps tip the balance toward a decision not to pursue an investigation.
- In the longer term, a severe compromise offers an opportunity to drive real change. In-house counsel is uniquely positioned to mature your company's overall security program. A data security incident can inspire the company to improve its information security program and lower its risk profile.

Barely a week goes by without headlines of another major company or organization losing sensitive information to hackers. Sooner or later, this challenge will land on your desk. Be prepared and always have a plan in place.

About the Author

Sam Rubin is the Unit 42 Vice President of GTM Strategy. He maintains an active docket of cases and often serves as an expert witness in digital forensics. Sam has deep expertise in matters involving theft of intellectual property, incident response, e-forgery, leaks of confidential information, and information security best practices. He has provided technical advice and expert opinions in a number of highstakes cases, including a landmark victory in a trade secret misappropriation case, a federal criminal securities fraud case, and civil litigation stemming from a $1.2 billion Ponzi scheme. Sam is co-author of "What Every Lawyer Should Know About Digital Forensics," published in *The Pennsylvania Lawyer*, and is a frequent presenter and lecturer on computer forensics, insider threats to proprietary data, and other cyber-related topics.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com