CORVUS

How to Work with your Cyber Insurer on Incident Response

5 Tips to Maximize your Partnership

Your cyber insurance provider can be your greatest advocate in responding to a cyber incident. But it's important to know how to leverage their resources for maximum impact and avoid common mistakes that can derail the incident response process. Here are 5 tips for working with your cyber insurer on every stage of incident response.

Setting the scene

It's eight o'clock Wednesday morning and you've just sat down at your desk, coffee in hand, ready to start your day. Just as you're about to begin answering emails and reviewing your calendar, your phone buzzes with an alert from your COO.

There's been a **suspected breach** at your company, and you've been advised to be wary of any incoming emails. Some employees are unable to access their devices, so **normal operations at the company are on hold.**

Upon booting up your computer, all you see is a black screen with red text: *"if you see this text, your files are encrypted..."*

These are just some of the questions that will be swirling in the heads of any leader when a ransomware attack begins.

- Who is your first phone call?
- What's step one?
- Where will you be by the end of the day?
- After all is said and done, what will it all cost your business?
- And are those costs covered by insurance?

The good news is if you have a solid cyber insurance policy, you won't have to scramble for answers.

That's because modern cyber insurance is a bit different than most other types of insurance.

For example, at the first sign of smoke in your home, you'd call the fire department before you even consider reaching out to your insurer. It's not till after the emergency has been handled that they'd come to assess the damage.

When it comes to cyber, you should call your insurer the moment you get a whiff of an incident. *Don't even grab the metaphorical fire extinguisher.*

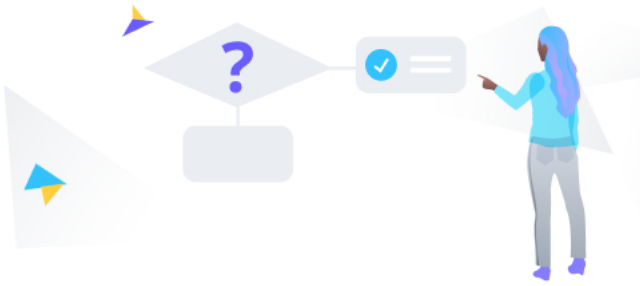
Your insurer will step into the crisis management role, making the call to the right people to help resolve your incident, as well as arranging with other vendors and contractors for the cleanup and remediation efforts.

In this whitepaper we'll explain why it's so important to understand the specifics of how you'll work with your insurer during an incident, go through those specifics in detail, and offer tips to maximize the partnership with your insurer.

> Your carrier is an ally throughout the entire incident response process, and we want to showcase exactly how you can leverage their expertise.

CORVUS

1. Before the Incident: Add Your Cyber Insurer to your IRP



Let's rewind. Before you're staring down that ominous black screen on your desktop, ideally some preparation has taken place to prepare your team for this scenario.

An incident response plan (IRP), in the form of a written document, means your organization has a system in place before there's a breach, so you can respond quickly and with intent. An IRP is also crucial to have on hand to showcase after an incident, **to prove to regulators and others involved: We had a system in place to limit risk.**

If you don't have an IRP in place yet — that's where to start. The SANS Institute, a provider for security training and certification, published a **handbook on a structured 6-step plan** for incident response which includes details on developing an IRP and practicing a *"fire drill"*.

Assuming you do have an IRP, you can move onto **integrating your cyber carrier into the documented plan**, and communicating that change to all relevant stakeholders.

Your IRP should outline when and how you'll communicate with your carrier in response to an incident, and who will be the one to do it.

"Who" is up to you; just make sure there's a clear chain of command. "How" should be communicated very clearly in accordance with contact information provided by your insurer. We recommend you put this contact information directly into your IRP to avoid confusion. (More on this with respect to Corvus specifically in the next section).

In terms of the "when" question, we'll share a couple of rules of thumb we share with our Corvus policyholders:

- If you plan on **involving outside vendors**, it's time to notify your insurer.
- If you **suspect ransomware is in any way involved**, it's time to notify your insurer.
- At the end of the day, **the sooner you notify your carrier, the smoother the process will be.**

We emphasize this point because as a cyber insurer we work with incident response vendors on a daily basis and know the best vendors very well. So not only can we help speed up the process by recommending forensics teams and legal counsel *(and any other vendors needed)*, we can view the scope of work and determine coverage to avoid surprises of unforeseen costs when the dust settles. We're here to work with policyholders every step of the way, and that includes walking them through your various vendor options.

Once the updates to your IRP are complete, be sure that anyone who may need to take action in the event of an incident **has the updated versions, knows the changes that have been made, and has offline access to the information** in case their work devices are inaccessible for any reason during an incident.

Lastly, ask for help: if you have any questions, most good cyber insurers will be happy to work with you on adapting your IRP to fit their recommended process.

Stage 1 best practices summary:

Document the who, when, and how of contacting your insurer directly within your IRP; ask for help from your insurer if needed!

Socialize the IRP among any staff that will need to take action in any situations planned for in the IRP and train them on response — even conducting drills.

CORVUS

2. Discovery of an Incident: When to Notify your Insurer

If there's a reason for concern at your organization — *perhaps indications of a breach identified by your IT team, or an employee falls for a phishing campaign* — you should inform your carrier as quickly as possible.

If you've followed Stage 1 of this guide, your Incident Response Plan will identify exactly who within your organization should notify your carrier, and that person will have offline access to the information about how to do so.

Even if the incident seems minor, don't hesitate to contact your carrier. Dealing with incidents almost daily, we've seen situations escalate quickly; much like a fire starting, dealing with a low flame is a lot more manageable than a three-alarm inferno. And if we stick with the fire analogy, we can spend time with your team plotting out fire escape routes, drilling *"stop, drop and roll,"* and the overall effort made to educate the masses on fire safety.

Stage 2 tips summary:

Follow the instructions in your IRP regarding who will contact your carrier, and how — but do so with safety in mind.

Don't be afraid to break the glass. We'd rather respond to a false alarm than arrive at an inferno.

Corvus Policyholders

In the event of an incident, Corvus policyholders can reach us either through email or our hotline.

These are available in our **Guide to Risk + Response services**, which we recommend you print and keep handy in case your systems and devices are not usable. If you misplace the Guide or aren't in your normal place of work at the time of an incident, you can find the contact details on the **Policyholder Dashboard** or **through your broker**.

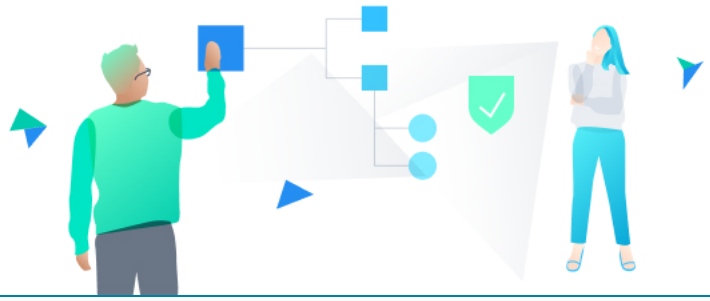
To save you time in the future, we recommend putting this contact information directly into your IRP.

Our response speed is the same either through phone or email, so use whichever method you prefer. **What matters most to us is that you're using the choice that feels most secure.**

If you believe that your email may have been compromised in the incident, we'd recommend that you use the hotline — or email us off the compromised network through a personal account. *Just make sure to let us know that you're looking to keep communications outside of your corporate email.*

If you're concerned that your desktop or laptop is infected, use another device or a mobile browser to reach us through email.

3. Work with Your Insurer's Team and Connect with Vendors



Once in contact, your carrier will want to know all the information that's available to start forming the picture of what kind of incident you're dealing with. However, it's not advised that your team start performing their own forensics investigation in order to get more clarity as it could overwrite forensics data or impede future analysis. Just provide what information is known and have the team stand by.

Hanging up from the initial call with your carrier, you'll have an idea of the roadmap for how they'll work with you through the process, as well as actionable steps to take next.

You should also come away from the initial call with guidance on lining up a **suite of vendors that fit the needs of your specific situation. This could involve privacy counsel, a digital forensics firm, and others.**

The introduction of these vendors will be necessary for moving forward — they'll learn the ins-and-outs of the situation and use their highly specific expertise to navigate different aspects of your situation.

Legal Counsel

In particular, involving counsel is critical for protecting the investigation and moving it forward. You'll work with a legal team that acts as a **"breach coach."** These specialists are well-versed in the subject matter of data breaches and privacy laws, so they'll provide **actionable advice on how your organization can face the current challenges in the context of complicated and location-specific privacy laws.**

At this step of the process, your legal team will probably work with you on two things:

- **Reviewing your internal and external communications.** Your legal counsel should be involved in any conversations where legal advice may be sought with the intent to **protect confidentiality and attorney-client privilege**, according to Beckage, a technologically-focused law firm. Attorney-client privilege is essential for reducing risk and limiting exposure.
- Your legal counsel will also **encourage you to collect information about the incident and thoroughly document all your steps.**

Forensics Firm

The addition of the **forensics firm** is necessary for not only containing and resolving the intrusion if it is still ongoing, but also to answer an array of technical questions regarding the incident.

Before services can be safely restored, your carrier needs to determine key components, such as:

- How did the threat actors gain access?
- What did the threat actors do?
- What malware or vulnerabilities are left in your system?

With those questions answered, there's a greater understanding of the full picture.

CORVUS

3. Work with Your Insurer's Team and Connect with Vendors

(Cont.)

What to expect when working with vendors:

Following initial calls with your vendors, they will provide scopes of work detailing what they plan to do, at the carrier discounted rate, with an overall estimate of cost.

This helps your organization and the insurer better understand the scope and potential cost of the claim, and allows your carrier to flag any work that may not fall within the policy's coverage.

Also, while your forensics firm will be working with you as soon as possible to contain the incident, some threat actors are more sophisticated than others. In the example scenario to the right, the incident was complex and time-consuming.

So while you can expect to have your initial forensics findings within a week or two, some more complicated investigations can take up to two months to be completed.

Stage 3 best practices summary:

Tell your insurer what you know, but refrain from starting your own internal investigation

Leverage the experience of your insurer's claims team to choose vendors.

Be forthcoming with vendors - the more information they have, the better they can serve your organization

Let's examine a hypothetical situation of a ransomware attack so we can delve deeper into the role that the forensics firm plays to get an organization up and running.

We're looking at a relatively **large organization** with its own **in-house security team,** and **ransomware has infected nearly all of the machines throughout their network.**

The forensics team needs to perform an **initial analysis** of the situation to answer the pressing questions:

How did the malware work, and why did it spread?

What were the digital footprints, or Indicators of Compromise (IOC) left by the attackers?

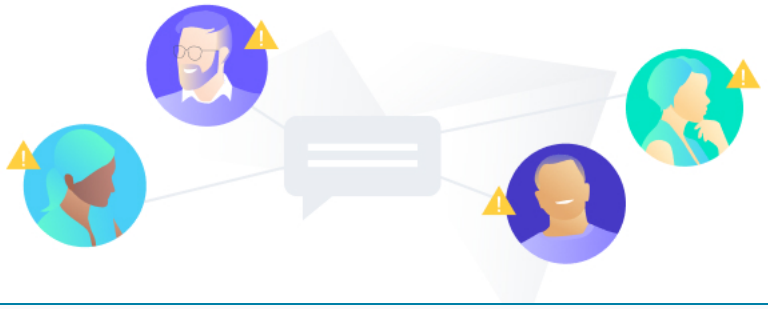
What other partners or vendors did they need to loop into communications to prevent further attacks?

The forensics team will also be able to determine **how long the threat actors had access to the company systems.** If it's long enough, the ransomware may be sophisticated and tailored to target their specific networks.

In this case, the company is large — and the ransom demand is a massive multi-million dollar request to match. If they find themselves in a situation where they need to pay the ransom, the forensics team and your carrier will be able to **help navigate the complexities of communicating with the threat actor and work with cryptocurrencies.**

Your forensics team, as well as our **Risk + Response team** *(if you're insured by Corvus)* will want to work with you in the aftermath to come up with an effective and individualized security roadmap to protect your organization in the future.

4. Work with Counsel and Notify Individuals via Vendors



As you move past the investigation, you'll need to determine your organization's notification requirements.

Legal counsel will help your organization determine your obligations under laws and regulatory regimes. If there are impacted individuals from the breach, we will line up necessary vendors such as notification and call center services vendors or credit monitoring vendors to help notify individuals if necessary.

Depending on the severity of the breach, you may only need to contact affected individuals directly — however, **depending on the scale, you may need to involve regulatory agencies.** *We'll cover that in the next step.*

Working with legal counsel will provide you with the resources to tackle the world of **varying state-by-state data and privacy laws.** With experience in the realm of notifying individuals *(and regulatory bodies)* of data breaches, they will walk you through how to execute the necessary communications.

They'll assist you in organizing several draft letter documents, depending on the states and local statutes *(and if any impacted individuals are minors)*. Their legal expertise allows you to have the confidence that you are meeting the complicated and varying local requirements for notification.

To get a sense for the level of complexity in notification, see this United States map that details **each state's regulations** for data breach laws that displays the variants across the country. Some states require, for example, that private companies disclose the breach to their state attorney general at the same time that they notify impacted individuals.

Another set of vendors that may be necessary in this step are **notification and call center specialists**. Your counsel will help you draft a FAQ script to provide and they'll be responsible for handling calls with impacted individuals as well as coordinating the mailing of notification letters.

Depending on the circumstances of the breach, you may need to also offer **credit monitoring services** to impacted individuals — which is when your carrier may involve a credit monitoring services vendor.

Stage 4 best practices summary:

Be ready to act quickly on the advice of your counsel to ensure you comply with notification laws and avoid additional fines that would increase the cost of the incident

5. Aftermath: Notify Your Carrier of any Lawsuits or Regulatory Investigations, And Reflect

After you complete the notification process, you've hopefully returned to business as usual *(or close to it)* and have your systems up and running. You may be moving on to discussions with your team about the lessons learned from the incident.

Did we follow our guide to responding to an incident?

What could we have done better to prevent the incident?

What can we do in the future to restore business operations quicker?

These are important conversations to have, and it's worthwhile to consider amending your IRP to reflect any gaps that were revealed by its real-life implementation. It can also be valuable to take the time to implement a **security roadmap that ties enhancements for security and IT resilience based on those identified gaps**.

Forensics providers should provide stock recommendations for the incident, but a more thorough analysis by the company should be done to understand any additional gaps that weren't identified during the incident. *It doesn't need to be about opening your pocketbook post-incident, but a thoughtful approach should be taken to mitigate future risk.*

You may have one last step to deal with in the aftermath: **depending on the scale of the attack and data accessed, there may be a regulatory investigation.**

The total number of records compromised in 2020 exceeded 37 billion, which is a 141% increase compared to 2019 — and the most records exposed in a single year since RiskBased Security began reporting on data breaches. So it makes sense that regulators are getting more serious about investigating — *and potentially levying fines against* — organizations that fail to protect their consumer's data. Evolving regulatory bodies, like the **General Data Protection Regulation (GDPR)** in the EU and the **California Consumer Privacy Act (CCPA)** encompass hundreds of pages of new requirements pertaining to data privacy and security law.

The details will be specific to your industry, but in general this is where we'll see your careful documentation become incredibly useful.

You'll want to show regulators that you had adequate guidelines in place beforehand to prepare you for an incident, especially to prove you've been compliant with applicable laws and did everything in your power to protect the data of your clients or consumers.

Another potential situation is that impacted individuals may come back with a lawsuit or — if there are enough affected individuals — a class action lawsuit. Your policy will have potential for coverage for all the steps we've mentioned prior, as well as for defense counsel to aid in lawsuits or regulatory investigations.

Stage 5 best practices summary:

Have an honest post-mortem to **understand what your team did well in responding to the incident, and where planning was insufficient.** Unlike lightning striking twice, unfortunately attacks can (and do) happen again to victims, and you can be even better prepared in the future.

Be ready to show investigators the extent of your preparations and the ways in which your team acted in accordance with those preparations.

Resources:

Incident Handler's Handbook (SANS Institute)
Breach Response Checklist (Beckage)
US Data Breach Laws (Beckage)
2020 Year End Report (RiskBased Security)

CORVUS

Corvus is reimagining commercial insurance for a digital world by making insurance smarter, companies safer, and brokers more successful. Corvus empowers brokers and policyholders with actionable insights to mitigate complex risks and reduce losses through the CrowBar digital platform, smart insurance products, and premier risk management services. Corvus is the world's largest specialty commercial InsurTech company.