CORVUS

Incident Response Done Right

When it comes to incident response, there's an abundance of widely circulated horror stories. This organization paid how much in ransom? And it took how long for them to get back up and running? The unimaginable: they didn't even have an incident response plan?

We've got goosebumps already.

Because of the "if it bleeds, it leads" nature of the media, it can seem like the world is brimming with successful cybercriminals and fumbling, unprepared victims. But that's not the case. For just one example, only about a quarter of Corvus ransomware claims result in paying a ransom — and that ratio has been trending down, not up, thanks to improving preparation and response practices.

Since the spotlight so rarely lands on those who do everything right, we figured we'd cover (from start to finish) an example of how incident response can go well using a real example of a ransomware attack. No jump scares — just the story of an organization that took the time to prepare for a potential ransomware attack, and lived to tell the tale when the fateful day came.

Don’t Go Chasing Waterfalls

Before we dive into the details, it’s important to highlight the concept of **parallel work streams** and how it can make incident response much more efficient. Through our story, we’ll showcase exactly how this approach can keep your organization on track, but first, let’s run through a quick explanation.

When organizations begin the incident response process, they often deal with the fracture of different work streams through a “waterfall approach.” This relies on a linear timeline, where each step leads to the next. The downside here is that it can cause slower results, with even more complications along the way. Important tasks that could be getting checked off are placed behind other tasks that may seem important or vital but in reality have limited impact on subsequent tasks.

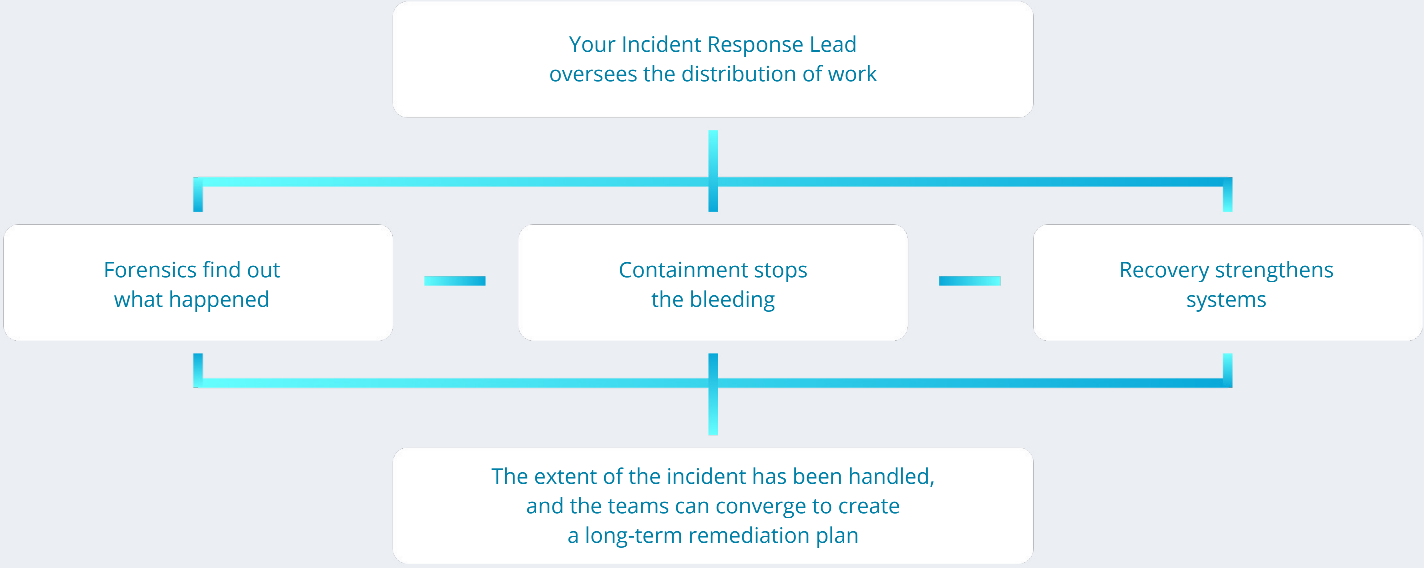
What we like to see, instead, are different work streams occurring simultaneously (“in parallel”) that spawn from one central figure who is overseeing the entire process. The work streams are carried out by sub-teams and focus on specific components necessary to recover from the incident.

If you visualize a diamond, you can picture how this plays out. On the top, where it’s narrow, we have the command center responsible for overseeing the distribution of work amongst sub-teams, who in turn, are working to find solutions for concerns revealed as the initial investigation continues to uncover essential information. As more action items are distributed, we see the sides of the diamond expand out. Eventually, the broad part of the diamond will converge again, as sub-teams complete their tasks and work towards the common goal of resolving the incident.

Some essential work streams you can expect to see throughout this process include:

- **Forensics:** Answering the questions of what happened.
- **Containment:** Determining how to stop the initial “bleeding” while getting a plan in place.
- **Recovery:** Taking the right steps to strengthen your systems for the future.

While those are the core three work streams you’ll see when responding to an incident, there are usually also components that involve legal advisory, as well as internal and external communications. Ultimately, you can have an infinite number of streams but they’ll need to be parallel with each other so one project doesn’t end up preventing progress somewhere else.



Preparation Must-Haves

Our scenario is drawn from the real experience of a Corvus policyholder, and relayed by the members of the Corvus team who worked directly on the incident response with the policyholder. Some minor details have been changed to ensure total privacy. Our subject is a professional services company with around 200 employees. Let's call them **Raven Corp**.

The IT manager wakes up on a Saturday morning to an alert that a user was unable to access files on the main file server; a quick examination showed that it had been encrypted. While this is never the news anyone wants to hear, particularly on the weekend, this organization had an advantage. They've prepared accordingly for the worst case scenario. Here's a brief checklist of everything they did well to prepare, with the majority completed before experiencing an attack:

- They had created an **incident response plan (IRP)**, which detailed exactly who to call first: their insurance carrier. We recommend having your carrier's contact information on your incident response plan, as they can be a valuable resource for providing introductions to the vendors you'll need to get out on the other side. In this case, they were able to get in touch with a breach coach, and a forensics and recovery team.
- They had developed an **asset inventory**, which accounted for all of their systems and the different associated applications. Knowing what you have is half the battle. This enabled them to be in a great place for recovery. It outlined their Tier 1 infrastructure, which is what they needed to have up and running first (to be able to get anything up and running). Everything was documented, and there was a clear order of operations.
- **Backups**. Our organization was in a better position due to their backups being properly maintained and protected which prevented the threat actor from gaining access to them. With strong security controls, as well as backup strategies and solutions, you'll be more likely to have systems up and running quicker. In this case, their backups were disconnected from the Windows domain, had different credentials, and were protected by MFA. Just for good measure, they had an immutable backup on-site with immutable backups stored in the cloud - defense in depth at its finest.
- They knew to ask for help! This may seem obvious, but there are no individual superheroes in incident response. This organization immediately reached out to experts and utilized the resources available to them.

The first 48 hours of an incident response process can dictate the outcome of a response effort. By having each of these points covered in their prior preparation and team-wide mindset going into the incident, the Raven team were set off on the right track, avoiding some of the classic mistakes that can come early on in the incident's timeline and cause delays.

Forensics

When done properly, the first phase of the response effort is likely to be a forensic examination of the IT system performed by a third party that specializes in investigative work.

While working with a forensics team, there's one crucial thing to understand about the partnership: **they're data consumption experts**. In their effort to paint a picture of exactly what happened within your environment, they will want to gather any and all data that's available, even if seemingly insignificant or unrelated. We want to emphasize the partnership aspect, as they'll need help from the impacted organization to get access to everything they need to depict the attack.

What we saw happen here — another example of incident response done right — is how the organization worked with their forensics team. They had specific employees working as knowledge experts, who were able to supply the forensics team with every resource they requested within hours. Without the delays of waiting for access to files and various logs, the analysis time can be cut down by days or weeks.

The leadership of the team made it clear to everyone at Raven Corp that the forensics provider was here to do the investigation - they were an ally - and that the internal employees were here to play a supporting role to facilitate the quickest outcome. This prevented a common mistake made by organizations dealing with a cyber incident, where some employees might try to tackle aspects of the investigation themselves, either before or during the vendor's investigation. This duplicates efforts and takes internal employees away from activities that require internal knowledge of the systems. Everyone plays to their strengths.

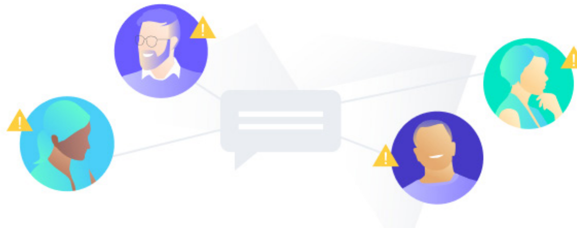
Giving the experts the room to work, while clearly communicating and providing necessary resources, can make it a much more seamless process. After all, everyone wants the same thing — business back as usual.

Containment

Imagine driving in a blizzard, in the middle of the night, with no headlights. Occasionally, a passing car or a street lamp will shed some clarity, but the majority of your journey home is trusting that you've memorized the route and your car stays on the road. Containment can be similarly unclear and dangerous. The main objective is to prevent further access or damage, but you can't always have enough information to know where the threat actor is in the environment or what they have done to maintain access. That's what the forensics team is working on. In the meantime — remember, parallel work streams — we saw Raven Corp tackle some basics to protect their environment and create a starting moat to defend from. They changed the passwords to administrative accounts (assuming that the threat actor had access to them), and disconnected the environment from the internet as a precautionary measure to ensure the threat actor couldn't access the environment.

Once they start gaining insights from the forensic team, they are able to pinpoint certain systems that need specific attention. With more context to what happened in the attack, they can take the adequate measures with an internal team to respond to the updates and decrease the risk to their organization. As the investigation progresses, the requests from the forensic team will slow and become more specific, until the environment has been completely contained. This incremental approach allows for business operations to resume in a staggered approach - when your business is down, some functionality is better than no functionality at all.

CORVUS



Recovery

Once the investigation reaches a certain point, the Incident Response Lead will assign sub-teams to begin the recovery effort: repairing damage, replacing hardware, restoring data, and generally getting back on-line.

We saw Raven Corp truly shine at this point in the incident response process. Recovery efforts can often be complicated and overwhelming when there are too many unclear spreadsheets floating around. This creates confusion over what has been updated, and what still needs to be. To avoid this, the internal team can coordinate with the vendor — ideally working together efficiently enough that there's hardly a distinction between the two.

In this case, we saw the organization work from one single document that contained the status of all of their systems. A huge perk, however, was that our organization had an asset inventory from even before the breach. This allows everyone — from various teams and departments — to follow the tracker and update on the same set of procedures. Then the metrics populate on one single source, and we avoid questions like: "How long until we get the Tier 1 systems running?" Everyone, across work streams, is on the same page.

Communication

It is possible to have too *much* communication. A positive we saw from this organization was that they weren't overwhelmed with the demand to make unnecessary, constant updates to a stressed executive team. In fact, they stopped and asked the experts: "How should we most efficiently communicate?"

Instead of wasting too much of the team's energy on too many spontaneous, time-consuming meetings, they decided that in the first few days of the incident response they'd have a morning update and an evening update. If something arises in between, they'll flag it and everyone can jump on a call. They let the technical teams work. This is where the shared tracking mechanism (that we mentioned in Recovery) can become incredibly useful. It decreases the need for constant interruptions when everyone can check in and see the exact status of all of the systems.

Expectations were set clearly throughout all of the teams, and as work streams started to converge, there was a natural rhythm that occurred through collaboration. Once things had settled, they were able to switch up the conversations to: "What can we do in the future to prevent this from happening again?"

CORVUS

It's a Marathon, Not a Sprint

After 2 weeks, The Raven team was able to finally take a deep breath and see that they'd handled the extent of the breach. What had been a stressful journey, was one that had been cut in almost half of the typical response time for an organization of similar size and industry due to their preparation and trust in the process. Retroactively, they had a better, comprehensive understanding of what happened. This was an opportunity to use their vendors as guides to create a long-term remediation plan. At the end of it all, some noteworthy successes:

- Even after having one of the most efficient incident response processes we've ever seen, this organization still took the time to open up a dialogue of "how can we get better?" and "what did we learn?"
- When speaking to vendors, they listened, asked good questions, and strategically determined what cybersecurity controls they needed to improve on, and what could wait for later down the line.
- They didn't rush their remediation plan. It's an exhausting procedure to recover from a ransomware attack, and they took their time to reflect on every step of their response.

Key Takeaways

- Raven Corp was prepared for the worst, before the worst happened. Take the time to set your organization up for success with an incident response plan, an asset inventory, and a robust backup strategy.
- You can streamline the response process by using an Incident Response Lead who oversees response operations and delegates out tasks to experts.
- There are no individual heroes in incident response. The best results come from listening to the response experts and trusting the process.

CORVUS

About 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.

Founded in 2017 by a team of veteran entrepreneurs from the insurance and technology industries, Corvus is backed by Insight Partners, Bain Capital Ventures, .406 Ventures, Hudson Structured Capital Management, Aquiline Technology Growth, FinTLV, Telstra Ventures, Obvious Ventures, and MTech Capital. The company is headquartered in Boston, Massachusetts, and has offices across the U.S.