

# INCIDENT RESPONSE

Peace of mind means knowing you're not alone when it matters most. That's why our incident response process is built into your policy — and ready to act the moment you need it.

## Our Response

These are the moments that test your team, your systems, and your strategy. But you're not in it alone.

We've streamlined that process with Trend Micro and our incident response experts to ensure your business operations are back up and running in no time — with as minimal disruption to the systems you rely on.

A full guide to our process is included in this document. We recommend integrating it with your cyber incident response plans.

## Onboarding

A cyber-attack can be one of the most stressful and confusing moments you'll face. That's why all Invision insureds are offered onboarding calls with our incident response coordinators and with one of our cyber privacy counsel law firms.

It's a chance to meet them, walk through the IR process, and get practical advice on how to prepare. So if the worst happens, you'll already know exactly what to do—and who's got your back.

## Trend Vision One™

Trend Vision One™ isn't just a security platform—it's globally recognized for excellence in incident response and digital forensics. By combining advanced Network Detection and Response (NDR) with cross-layer XDR it offers comprehensive threat visibility for rapid action.

Our DFIR partners are experienced in using the whole breadth of the Trend Vision One™ platform to offer ground breaking response processes for our customers. These are designed to contain and remove threats faster than ever before.



## Arrange Your Incident Response Onboarding Session

Go to [www.invisioncyber.com/contact/onboarding](https://www.invisioncyber.com/contact/onboarding)

# IR PANEL PARTNERS - US

## Digital Forensics Incident Response

Our DFIR partners were chosen for their deep expertise in Trend Vision One™. Together, they bring experience from thousands of incident response engagements.



## Recovery

We've partnered with recovery firms who've helped organisations bounce back from some of the most complex cyber events in recent history. They know what it takes to restore systems, stabilise operations, and support your team.



## Privacy Counsel

Handpicked for their unwavering focus on the customer and deep cyber legal expertise. They understand Trend Micro's technology, systems, and customers inside and out. With full attorney-client privilege, they're here to protect your interests.



## Alternative Vendors

Our panel of vendors has been carefully selected to act as a high-performing, coordinated team—bringing together the specialist expertise needed to manage incidents swiftly and effectively. However, we know you may already work with providers you trust. If you'd prefer to use your own vendor, we'll do our best to accommodate — provided we can complete the necessary due diligence.

To discuss adding an alternative provider to your panel, contact us or your broker as early as possible.

**We recommend you always contact our incident response team before engaging any vendor during an incident.**

This panel is not exhaustive, and in some cases, it may be appropriate—based on the specific nature of the incident—for the cyber services team to engage an alternative vendor.

# INCIDENT RESPONSE

## IR FAQs

---

### **What should I do if I suspect a cyber incident?**

Act quickly. Notify your insurer immediately via your policy's emergency contact process. Time is critical — early response can help contain damage and streamline the claims process.

### **Do I need to wait for forensic evidence before reporting an incident?**

No. You should notify us as soon as you have reasonable suspicion of a cyber incident or compromise. We'll help guide next steps, including engaging forensic experts if needed.

### **What kinds of incidents are typically covered under cyber insurance?**

Coverage varies, but policies often include ransomware attacks, business email compromise, data breaches, denial of service, and legal or regulatory costs related to privacy violations. Always check your policy wording and consult your broker for help.

### **How long does it take to resolve a claim?**

It depends on the complexity of the incident. But the more prepared and communicative you are, the faster we can assess and settle your claim. We aim to make the process transparent and timely.

### **What documentation will I need to submit a claim?**

Typically, an incident report, logs or evidence (where available), and a breakdown of losses incurred. Our team will walk you through the details — you won't have to figure it out alone.

## Myths and Misconceptions

---

### **"It's best to try to solve the incident myself so I don't use my insurance"**

It's always best to contact our IR team early. If there is nothing for them to do straight away, they will simply keep in contact and make sure everything's ok. It doesn't cost anything to speak to our teams and it doesn't count as a notification of claim.

### **"Cyber claims are slow and bureaucratic."**

Not with the right partner. Our approach is responsive, structured, and people-first. Some claims are more complex than others but we intend to process the claim as quickly as possible.

### **"I'll be blamed for the breach."**

Cyber risk is a business reality, not a personal failure. Threat actors are sadly common in cyber space, whilst we also know that sometimes mistakes just happen. What matters is how you respond — transparency and speed make a difference, and we're on your side.

### **"Insurers will do everything to avoid paying"**

We hear this one a lot. In reality it is completely wrong, as long as the circumstance is covered by the policy, it is in the insurers best interest to pay.

### **"Reporting an incident affects my future premiums?"**

Not necessarily. We look at how incidents are managed, not just the fact they happened. Being transparent and proactive can actually help reduce future risk — and show insurers you're a responsible risk partner.

## Final Message

---

**We understand that reaching out to your insurer during trouble can feel daunting—and that trust isn't easily earned. But we want to change that.**

**Our team has real-world experience managing cyber incidents of all sizes. We know that even with strong controls in place, things can go wrong, mistakes happen and threats evolve.**

**We're here to support you—every step of the way.**



## GET IN TOUCH

 [enquiries@invisioncyber.com](mailto:enquiries@invisioncyber.com)

 [www.invisioncyber.com](http://www.invisioncyber.com)

71 Fenchurch St,  
London,  
EC3M 4BS





All applicable terms and conditions are outlined in your policy.

If you choose to use a provider not included on our panel, you must notify Invision in advance and obtain written approval from our claims department before incurring any related expenses. This can be arranged through your broker or by using the contact information provided in your policy documents.

All service providers operate as independent contractors. They are not agents or employees of Invision, and Invision is not a party to any agreement between you and your chosen provider.

Invision assumes no liability for the services rendered by any provider. Likewise, Invision is not subject to any obligations or liabilities related to those agreements. You are not required to follow a service provider's recommendations, nor are you obligated to contract with any approved provider—unless otherwise stated in your policy.

Invision Cyber is a trading style of Acies Management Holdings Limited, a company authorised and regulated by the Financial Conduct Authority no. 830581. Registered in England no. 11136744 at 71 Fenchurch St, London, EC3M 4BS. Invision Cyber underwrites on behalf of various Lloyd's of London Syndicates. Invision Cyber conducts business in the UK in respect of business received from USA domiciled and licensed Excess and Surplus lines brokers and as such USA domiciled Insureds must rely solely upon the advice of a licensed broker. Invision Cyber is a strategic insurance partner of Trend Micro, operating independently with no formal affiliation or financial relationship with Trend Micro.

# RESPONSE PROTOCOL - US

In the event of an incident, email:

[incident-response@invisioncyber.com](mailto:incident-response@invisioncyber.com)

Write your policy number here for quick reference:

## What to include in your email

Contact us as soon as possible with:

- Your name
- Your contact details (both phone and email)
- Your business name
- Your policy number
- A brief description of the incident
- Other information you feel can help

**NOTE:**

Avoid referring to the word "Breach"  
It's a legally-defined term that may trigger individual and regulatory notice obligations.

## Useful Information

- You can arrange an onboarding session on our website and speak to our Cyber Services Managers (CSM) team to learn more about this process.
- Keep your broker in the loop from the start – they'll be a great point of contact for you.
- Reach out often and early – If you feel there is any potential compromise to your systems or data.
- You can talk to a CSM about any event, **contacting us does not mean you're making a claim.**

All Invision incidents are handled by cyber services managers at Beazley—one of the world's leading providers of cyber insurance.

Beazley has a long-standing reputation for excellence in incident response management and handles around 4000 calls a years.



### Contact Incident Response

Either fill out our dedicated incident contact form or email [incident-response@invisioncyber.com](mailto:incident-response@invisioncyber.com). This email is monitored 24/7 and on receipt the case will be passed to one of our Cyber Services Managers (CSM).

You can also call the hotline: **866-567-8570 (US)**



### CSM Triage Call

Your dedicated CSM will reach out to you (phone or email) shortly to establish details of the incident and develop a response plan. They will help to assign any appropriate vendors (DFIR, Recovery etc), get SOWs signed.



### Privacy Counsel

Privacy counsel is typically the first service brought in during a cyber incident. They determine breach notification obligations, assert attorney-client privilege over the investigation, guide comms, and ensure proper notice to individuals and regulators.



### Remediation & Recovery

Industry-leading forensic firms, experienced with Trend Vision One™, will help remediate the incident, whilst our recovery partners will help return to full operations. All work seamlessly with your internal teams, CSM, and privacy counsel to ensure a coordinated response.



### Other Services

Your CSM will also help arrange:

- Crisis Communications
- Ransomware Negotiators/Facilitators
- Notification and Credit Monitoring
- Call center services

You should notify us as soon as possible of any potential or confirmed cyber incidents that result in a reasonable suspicion of impact to your network and/or sensitive information, such as personally identifiable information ("PII").