Cyber SOLUTIONS

## Hylant Risk Services

# CYBER CLAIM DO'S AND DON'TS

Not every cyber incident is a crisis. However, if you become the victim of a significant cyberattack, follow these recommendations to protect your organization's finances and reputation, and strengthen your insurance claim.

## DO'S

Implement the cyber risk response plan your organization created and frequently tested before the incident. In addition, do the following.

***1. Do engage your carrier(s) and insurance broker as soon as a cyber event is discovered.***
Obtain the carrier's input before incurring any costs, including charges from your regularly engaged service providers. Use your carrier's pre-approved panel vendors (i.e., service providers) unless directed otherwise. Secure a scope of work from each vendor and obtain written consent from the carrier.

***2. Do maintain an activity log.***
Record the decisions your organization makes, who makes them, the basis on which they were made, and the resulting activities. This information may be helpful when questions arise during the claim process. It also will be useful when you review the incident once it is over and may help you improve your response plan.

***3. Do store your cyber policy offline and communicate with the response team outside the regular business operating environment if the threat actor is still in the system.***
One organization discovered too late that the hacker had located their cyber insurance policy and knew how many millions of dollars the company was insured to pay as ransom.

***4. Do mitigate losses as much as possible.***
Your prepared response plan should contain steps such as changing passwords, securing the network if possible, contacting financial institutions to lock down accounts and watch for potential fraud, outsourcing work if your systems are down, etc.

***5. Do engage and listen to your breach counsel.***
Your breach counsel will let you know who (if anyone) must be notified and by when. Each state has its own requirements. Timely notification, if necessary, is critical to avoid fees and penalties.

***6. Do document all expenses.***
The insurer will need proof to pay your claim if a reimbursement policy or if a business interruption loss occurred. Remember to document all aspects of any business operation losses (e.g., downtime, outsourced work, salaries, missed contract deadlines, etc.).

## Hylant Risk Services

# CYBER CLAIM DO'S AND DON'TS

***7. Do conduct regular calls with stakeholders.***
Discuss what has been done and what is next. Make sure resources have been deployed where necessary. Address any questions or items that had not been anticipated.

***8. Do learn from the experience.***
Within a month of the cyberattack, conduct a debriefing session. Update your cyber risk response plan to incorporate any lessons learned. Conduct tabletop exercises to keep it current.

## DONT'S

While it's important to act quickly, it's also important to act purposefully. Follow your plan and remember the following.

***1. Don't delay telling your insurer about the attack.***
Once a problem is recognized, engage your broker or carrier and confirm the next steps. Your claims may be rejected if you incur costs without the carrier's input.

***2. Don't directly engage with the threat actor.***
You wouldn't talk to a bank robber, so don't talk to a hacker. The exchange won't go well and could result in costly fines and increased demands from the attacker. Let an experienced negotiator handle any necessary communications.

***3. Don't immediately reset your network or wipe it clean.***
By doing so, you could unnecessarily lose or corrupt data, resulting in added expense. Let the IT forensics team see what has and has not been impacted by the attack, identify the attack vector and determine whether anything can be salvaged.

***4. Don't share information with all employees.***
Only share information with those identified in your cyber risk response plan unless legal counsel advises otherwise. An information leak could cause significant financial and reputational harm to your organization.

***5. Don't release information publicly without consulting counsel and, if needed, engage a public relations firm.***
Vet all proposed communications through your legal counsel to protect your client-attorney privilege in the event of subsequent lawsuits. Releasing unnecessary communications could increase risks to your organization. Your legal counsel should also serve as the point person for your crisis communications team.

***6. Don't assume that insurance will pay for your employees' time to recover or restore your systems.***
Some insurance carriers may require you to hire an outside firm to do the work.

## ONE LAST "DO"

Do visit **hylant.com/CyberDo** to learn more about how we can help you understand your cyber risks and protect your business through cyber insurance coverage.