Why DFIR Is Needed in Partnership With Cyber Insurance

Cyber insurance is critical for organizations as cybercrime continues to accelerate in severity and costs

Too often, cybercrime victims have learned what kind of applicable coverage they have only after a security incident has occurred. As a result, policyholders and insurance providers alike have become much more proactive about specific inclusions and exclusions in policies, including cybersecurity policy riders.

Insurance is necessary to mitigate scores of financial, regulatory, reputational, and other costs that cyberattacks inflict on organizations. However, our firsthand experience across industry sectors shows recurring patterns across threats and incidents that policyholders and insurance providers are contending with. In this whitepaper, we will review patterns of attack, the need for digital forensics and incident response (DFIR), and the importance of reporting as it relates to insurance claims.

PATTERNS OF ATTACK

Ransomware is the primary threat concern in cybersecurity. Ransomware is a simple, accessible cybercrime enterprise for bad actors to launch and operate, and it's highly adaptive. For example, the bad actors behind ransomware variants, such as ClOp and LockBit, show lucrative sophistication in how they ratchet up extortion while offering to "settle the matter" of ransom payment in terms and tone usually seen in business negotiations. In 2022, the FBI's Internet Crime Complaint Center (IC3), which collects reports of internet crime and assists victims in freezing money involved in cybercrime, reported a total of 2,385 ransomware victims.[1] The large number of reports primarily came from the healthcare, critical manufacturing, and government facilities industries.

Adding to the stress of ransomware's business impact is its attackers' inherently lingering, real-time nature. Unlike attacks that steal or expose sensitive data before vanishing and leaving those files intact, ransomware attacks thrust organizations into a stressful race against the clock. Administrators and incident responders must rapidly determine how many affected systems are ransomed, what type of malicious program is being used to hold files hostage, and if a company's backup and recovery capabilities are able to quietly restore files and operations. DFIR underpins everything in a ransomware attack.

Business email compromise (BEC) ranks second as a threat concern, close behind ransomware. In a BEC attack, bad actors often send emails impersonating a legitimate source, such as a CEO, requesting information that ultimately leads to the bad actor conducting fraudulent money transfers. BEC attacks rely heavily on social engineering scams and phishing emails to trick unsuspecting employees. In 2022, the IC3 received a total of 21,832 BEC complaints, amounting to adjusted losses over $2.7 million.[1]

When DFIR professionals respond to cybersecurity incidents such as ransomware or BEC, they shape the outcome by determining what happened, assessing the extent of damage, triaging what is known, and setting the pace for recovery.

> Ransomware and BEC are the two leading causes of loss. They accounted for nearly 50% of claims in 2020 and 2021.[2]
>
> — NetDiligence 2022 Cyber Claims Study

WHY YOU NEED DFIR

A DFIR provider partners with clients to swiftly contain incidents and conclusively restore systems after an attack. These experts will be familiar with your organization and have an understanding of your network in the case of a cyber incident.

DFIR services exist to prevent a hall of mirrors from needlessly impeding response actions, execution of incident response plans, and support of crucial processes that affect insurance claims and other dependencies. Whether at the first subtle signs of suspicious network activity or during the rapid physical disruption of commerce, transportation, and healthcare, DFIR teams deploy at a moment's notice to intercept attacks, save precious electronic evidence, perform damage control, and determine what is necessary for secure restoration. Importantly, the teams may have to do these steps simultaneously or in a very specific order to best serve a victim whose industry has norms on calling in law enforcement, notifying regulators, proving compliance to insurance, or sharing intelligence with peers.

Forensics accounted for 53% of the average total crisis services costs of a cyber incident from 2017-21[2]

It is no surprise that DFIR roles and relationships determine cyber insurance's current stakes and foreseeable future. After all, forensics accounted for 53% of the average total crisis services costs of a cyber incident during the period from 2017-21, according to the NetDiligence 2022 Cyber Claims Study.[2] If a policyholder does not have sufficient DFIR experts and resources in place before an incident happens, it can easily end up paying more for remediation in the end — without the advantages these experts could have delivered along the way.

Between incidents, and particularly when insurance policies are being acquired and updated, Pondurance combines veteran DFIR insights with advisers' eyes to proactively examine the postures and preparedness of clients.

BE PROACTIVE WITH A DFIR PARTNER

With a DFIR partner in place, organizations demonstrate to insurance providers that they are taking proactive, responsible steps to pursue comprehensive defense strategies. In turn, they greatly lower their risk profiles and reduce premiums.

It is important to not only be ready to react to threats but also have the reporting tools to show insurance providers that security protocols were in place when the breach happened. Should a compromise occur, a DFIR partner will serve as a trusted representative of its client in working with the provider to deal with the recovery process including providing specific reports that the insurance provider needs to file claims. This approach leads to far better results than "starting from scratch" in the heat of a breach and makes for an easier process to file claims with any provider.

KNOW WHAT'S COVERED — AND WHAT ISN'T

Knowing your insurance policy coverage and limits before a cyber incident happens is crucial. Uncertainty can cost a great deal in response time and financial losses. While digital risks apply to nearly every facet of business today, insurance sold to cover common business risk does not always cover the cyber equivalents.

It is common for an organization to call in our team for urgent incident response. But because there may be confusion about coverage, the organization may not know until halfway through the engagement if its policy actually contains applicable cyber coverage. This is a classic example of why it is important for every organization's cross-functional crisis response team with members representing the C-suite, operations, risk, legal, IT, and other departments to have a clear understanding of current insurance coverage before an incident occurs.

HAVE A SECURITY ADVISER AND ADVOCATE BEFORE, DURING, AND BETWEEN CRISES

Navigating cyber insurance's higher stakes is a daunting proposition for even the largest Fortune 500 organizations. Buyers seeking new or updated insurance policies need an objective, outside set of eyes to help scope and tailor coverage, while providing ongoing risk management advice.

Pondurance performs this role across a host of industry sectors, bringing years of insight from monitoring client networks, responding to incidents, tracking evolving threats, and distilling data necessary for risk-based decision-making.

When finalizing cyber insurance policies, policyholders benefit from specifying their designated go-to response firm for incidents. Specifying your own response firm, particularly one already familiar with your operations and insurance situation, is a pivotal step underpinning the total value of a policy.

Pondurance takes the data-first philosophy into every security consultation, insurance assessment, and advisory conversation anytime clients launch mergers and acquisitions, modernization, pandemic response, and other initiatives. Following the data is essential for dispelling assumptions and a false sense of security. Policyholders cannot afford to wait until a crisis happens to discover whether an incident is covered.

A policyholder should designate upfront which incident response firm it will work with. Otherwise, the policyholder will have to work with one of the insurance provider's default incident response partners that will focus first and foremost on meeting the insurance provider's interests.

In cyber insurance matters, Pondurance works as the policyholder's advocate and ally, using knowledge of our clients' security architecture and wider industries to conclusively determine what happened, from the root cause of an incident through downstream consequences. In incident response work, Pondurance helps clients execute plans and facilitate crucial time-sensitive processes, from preserving evidence and IT operations to supporting insurance claims and independently verifying when affected systems are fully restored. In a tornado analogy, this goes beyond measuring holes and taking pictures of debris. Pondurance helps clients with the IT equivalents of getting utility services restored, inventorying possessions in a new, secure space, and assessing how recovery construction can improve ruggedness and resiliency in the end.

> “We thought we had been making the right security investments. Then we had an incident and brought in Pondurance. They immediately proved their value and earned our trust due to their immense expertise and guidance throughout the entire process. **We simply wouldn‘t have been successful without them**.“
>
> — Steve Long, CEO Hancock Health

CONCLUSION

Cyber insurance is among the most important technology, legal, risk, and reputational decisions a cross-functional team of senior leaders can make. Above all, leaders need advocates and partners making sure they have proper coverage in place and are ready to respond at the first sign of trouble. Pondurance is that advocate and strategist for a wide set of clients in many different industries but specializing in healthcare, manufacturing, education, retail, and government.

Whether you plan to acquire cyber insurance in the coming months, are looking for advice on competing policies, or are due for renewing coverage, contact us to arrange a conversation about your objectives. Our team has the experience, data, and skills necessary to maximize cyber insurance's advantages.

ABOUT PONDURANCE

Pondurance delivers world-class managed detection and response services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce.

By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, DFIR professionals, and compliance and security strategists who provide always-on services to clients seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Sources:
1. *Federal Bureau of Investigation Internet Crime Report 2022,* Internet Crime Complaint Center, 2022.
2. 2022 Cyber Claims Study, NetDiligence, Oct. 2022.