PONDURANCE

Why DFIR Is Needed in Partnership With Cyber Insurance

Cyber insurance is becoming critical for more organizations with cybercrime accelerating in both severity and costs.

Cybercrime victims too often are learning what kind of applicable coverage they have only after a security incident has occurred. Insurance purchasers and providers alike have become much more specific about inclusions and exclusions in policies, including specific cybersecurity policy riders.

Insurance is necessary to mitigate scores of financial, regulatory, reputational, and other costs that cyber risks inflict on companies. However, our firsthand experience across industry sectors shows recurring patterns of threats and incidents that organizations 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 paying out insurance claims.

PATTERNS OF ATTACK

Business email compromise (BEC) scams alone are staggeringly common and effective. Between January 2014 and October 2019, the FBI's Internet Crime Complaint Center received complaints totaling more than $2.1 billion in BEC losses.[1] The ability to hijack an authentic executive email account or create a fake message close enough to trick a distracted employee makes anyone a well-armed robber with the means to pull off a heist and sow confusion in the wake because BEC scams blur the lines between traditional, digital break-ins, and fraud.

It's one thing for an attacker to evade layers of defenses intruding into your perimeter, but what if the attacker just impersonates the boss via email or social media instead? How much are companies' policies, security controls, and insurance designed for the former scenario versus the latter? This is an example of an urgent area we help customers study to keep claims and coverage from resting on dated thinking or assumptions.

Another massive cyber insurance catalyst that is hard to overstate is ransomware. Ransomware is a simple, accessible cybercrime enterprise for individuals to launch and operate and is highly adaptive. For example, adversaries behind ransomware variants like Ryuk, Sodinokibi, and Maze 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. Maze pioneered the extortion tactic of releasing ransomed files to the public, just one example of a data breach threat if ransoms are not paid.

While many ransomware campaigns can have the feel of scale and opportunism over strategy — targeting masses of people with one exploit and seeing what detonates — other schemes are more targeted. Pondurance Chief Information Security Officer and Vice President of Services Dustin Hutchison described patterns of attacks against healthcare businesses in a Data Breach Today article, "A threat actor may view the compromise of one entity holding so much data as much more attractive than targeting each client organization, based on the effort versus reward."[2]

Adding to the stress of ransomware's business impact is its attackers' inherently lingering, real-time nature. Unlike attacks that might steal or expose sensitive data before vanishing and leaving those files intact, ransomware thrusts companies in 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 whether a company's backup and recovery capabilities are able to quietly restore files and operations. DFIR underpins everything.

These situations prove that DFIR capabilities and professionals responding to a cybersecurity incident shape the outcome of everything: determining what happened, the extent of damage, triaging what is known, and setting the pace for recovery.

WHY YOU NEED DFIR

A DFIR firm partners with customers to swiftly contain incidents and conclusively restore systems after an attack. A DFIR firm 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, executing incident response plans, and supporting crucial processes that affect insurance claims and other dependencies. Whether at the first subtle signs of suspicious network activity or the rapid physical disruption of commerce, transportation, and healthcare – as in the case of the NotPetya ransomware – 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, they may have to do these steps simultaneously or in very specific order to best serve the victim whose industry might also have norms about calling in law enforcement, notifying regulators, proving compliance to insurance, or sharing intelligence with peers.

It is no surprise that DFIR roles and relationships determine cyber insurance's current stakes and foreseeable future. Did you know that according to Society Insurance, 51% of cyber claim costs were associated with IT forensics in 2018?[3] If an organization does not have sufficient DFIR experts and resources in place before an incident happens, they can easily end up paying more for remediation in the end – without the advantages these experts and experience 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 customers' posture and preparedness.

> **51% of cyber claim costs** were associated with IT forensics in 2018.[3]
>
> — Society Insurance

BE PROACTIVE WITH A DFIR PARTNER

With a DFIR partner in place, companies demonstrate to insurers 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 customer in working with the provider to deal with the recovery process including providing specific reports that the insurance carriers need to file claims. This leads to far better results than starting from scratch in the heat of a breach and makes an easier process to file claims with any carrier.

KNOW WHAT'S COVERED ... AND WHAT ISN'T

Knowing your insurance policies' 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.

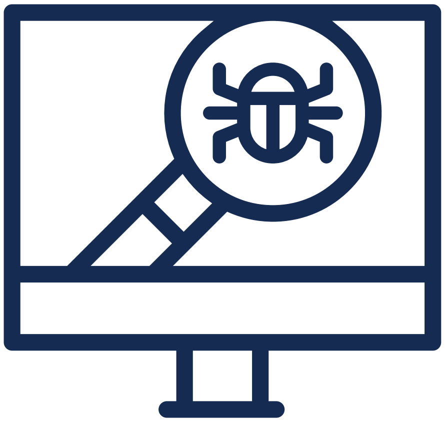
As a 2020 report from the Organisation for Economic Co-operation and Development (OECD) notes, "Much of the variation in coverage results from differences in definitions, conditions and exclusions as policies have evolved very quickly, hindering the emergence of standardised language." [4]

It is common for a company to call in our team for urgent Incident Response and not realize until halfway through the engagement whether they actually have applicable cyber coverage due to confusion about what different corporate policies cover. This is a classic example of why it is important for every company'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 beforehand.

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 customer networks, responding to incidents, tracking evolving threats, and distilling data necessary for more risk-based decision-making.



When finalizing cyber insurance policies, policyholders benefit from writing in, or 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 any time customers launch merger and acquisition, modernization, pandemic response, and other initiatives. Following the data is essential for dispelling assumptions and a false sense of security. Companies cannot afford to wait until a crisis happens to discover whether an incident is covered.

A policyholder not establishing a designated firm will have to work with one of the insurance carrier's default incident response partners that focus on meeting the carrier's interests, first and foremost.

This means trying to minimize insurance liability. To use a property insurance analogy, this is comparable to insurance inspectors arriving in a neighborhood battered by tornadoes, verifying that, yes, your home's roof was destroyed and there is now a fallen tree in your living room. The inspector photographs the damage, verifies the property is your address, makes you sign forms limiting further claims, and cuts you a check for an amount deemed acceptable in the carrier's eyes.

In cyber insurance matters, Pondurance works as the policyholder's advocate and ally, using knowledge of our customers' 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 customers execute plans and facilitates crucial time-sensitive processes, from helping preserve 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.

Specifying your own response firm, particularly one already familiar with your operations, and an insurance situation is a pivotal step underpinning the total value of a policy.

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 an advocate and strategist for a wide set of customers in many different industries but specializing in healthcare, manufacturing, 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.

> “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

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 customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations. Visit www.pondurance.com for more information.

Sources:
1. FBI, Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion, Apr 2020.
2. Data Breach Today, Victim Count in Magellan Ransomware Incident Soars, Jun 2020.
3. Society Insurance, Cyber Claims Digest for 2020 Planning, 2018.
4. OECD, Encouraging Clarity in Cyber Insurance Coverage, 2020.