January 24, 2023

The High Price of Business Interruption Requires New Response Modalities

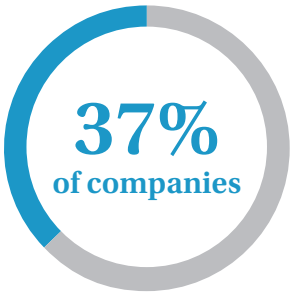
Restoration Is the Most Critical Factor in Reducing Incident Costs

FENIX 24®

A CONVERSANT GROUP COMPANY

In the minutes and hours after a catastrophic cyberattack, incident responders engage in a series of actions in a standardized order, including engaging a breach counselor, selecting a forensics vendor, deploying forensics capture tools, answering "whodunnit and how," and, finally, restoring systems to operational. Aside from the law enforcement objectives of digital forensics science, all these activities are, at their root, about one primary goal: getting the business operational again while staying in compliance. They are done as quickly and efficiently as possible to minimize the significant financial, legal, and brand impacts business interruption can have on the organization and the customers that rely on it.

Why, then, is restoration—the discipline of restoring systems to operational—so often chronologically and ideologically last in the incident response (IR) process? Why, too, is restoration so often left to less experienced IT teams, rather than bringing in focused experts when the stakes are so indisputably high?



37% of companies self-reported being hit by ransomware in 2021, with an average incident cost of $1.85M.

Today, most public- and private-sector organizations have Incident Response and Disaster Recovery Plans (IRPs and DRPs) in place to help prepare them for when the inevitable occurs. The frenetic activity post-breach typically begins with a breach counselor (a legal expert focused on cyber incidents) assembling an external team of experts to make very rapid and key decisions and determinations, including which systems have been infected, whether to pay ransoms, if backups are viable, and how to approach restoration ("greenfield" vs. from backups). Since restoration experts are last to be hired—if, indeed, they are hired at all—fundamental decisions that dramatically affect the time to restore (TTR) have often already been made by people less experienced, less capable of reducing downtime and risk, and thus of reducing the total cost of the incident. With restoration trailing in the chronological flow and perceived importance, clients suffer far longer business interruption than necessary.

Perhaps this process flow once made a lot more sense. Formalized cyber disaster planning appears to have gone more mainstream ~10 years ago, when the scale and scope of cyberattacks such as ransomware were at far lesser scale. Attacks were often limited to a small subset of servers (leaving much of the business operational). Downtime was not a top five expense, and attackers were using less destructive methodologies while demanding lower ransoms; remediation was easier to manage by IT teams who had the skills to address it. It made sense for the IR process to be designed to address organizational gaps of the time: legal assistance, ransom negotiation, compliance, forensics, crisis communications and the like. In this environment, cyber insurance carriers were content to allow or encourage organizations to attend to recovery on their own.

> "The best way to serve clients, then, is to ensure our response model is designed to address the highest cost, most destructive factor in the attack: Business disruption."

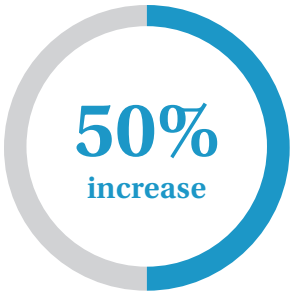
Today's threats proliferate, buoyed by ransomware as a service (RaaS) that arms even simple hackers with sophisticated tools, many of which are designed to take down entire global organizations while destroying defensive measures such as backups. They use these devastating consequences as leverage to extract payment from their victims. The costs of downtime are becoming impossible to ignore by both organizations and cyber insurance carriers, and restoration has become too complex for internal teams to handle efficiently. The best way to serve clients, then, is to ensure our response model is designed to address the highest cost, most destructive factor in the attack: Business disruption.

As in any discipline or science, models and processes mature and evolve alongside the macroenvironment they serve. We are at the cusp of a needed evolution: one where restoration does not lag other incident processes, but rather, is being conducted immediately in the initial hours of attack. One where restoration and Digital Forensics and Incident Response (DFIR) partners work collaboratively, synergistically, in an orchestrated fashion, enabling each other to be more effective and cost efficient on behalf of the client.

This paper will contemplate the need to prioritize disaster recovery within the IR team's chronological flow and hierarchy, elevate its perceived criticality within the cyber insurance industry, and prioritize the establishment of oversight and standards for restoration provider quality.

The Scale of Attacks and Costs of Downtime Continue to Grow

In a 2014 Forrester report evaluating enterprises' reasons for purchasing a next-generation firewall, only 44% of companies reported suffering a breach in the preceding year. By contrast, a recent survey published by Sophos revealed 37% of companies self-reported being hit by ransomware in 2021, with an average incident cost of $1.85M. Ransomware is only one attack modality in an attacker's arsenal; this statistic does not even include such threat actor favorites as malware, business email compromise (BEC), insider threats, and others that can also impact business operations. In the total calendar year of 2021, researchers saw a 50% increase in cyberattacks on corporate networks compared to 2020; in part attributable to the Log4J vulnerability, but also a part of an overall, long-term growth trend of attackers working to exploit weaknesses in corporate defenses. While initial indicators are that ransomware attacks have abated slightly in the first half of 2022, which has been believed to be attributable to numerous factors including the crash of cryptocurrency, the disappearance of notable ransomware groups, and the war in the Ukraine, few experts expect the downward trend to continue over the long term.



In the total calendar year of 2021, researchers saw a 50% increase in cyberattacks on corporate networks compared to 2020.

Unsurprisingly, attack complexity and destruction have increased as well. Enterprise IT architectures have become significantly more complex, globally distributed, decentralized, and connected. Attackers are preying on this complexity, finding security gaps in this vast estate of controls and configurations where patching and orchestration is suboptimal; areas where compliance and frameworks cannot shield the organization due to their lack of timely specificity. Not only has the attack surface

Ransomware as a Service (RaaS) has exploded, putting more sophisticated ransomware modalities into the hands of everyday hackers. According to our internal estimates, where a few years ago only nation state actors and/or less than 5-10% of attacks were sophisticated, today we are seeing over 80% of attacks leveraging advanced tools.

expanded, but threat actors are wielding variants and tools that propagate virtually instantly across global systems. And the attacks just keep on coming. Ransomware is every hacker's tool: RaaS has exploded, putting more sophisticated ransomware modalities into the hands of everyday hackers. According to our internal estimates, where a few years ago only nation state actors and/or less than 5-10% of attacks were sophisticated, today we are seeing over 80% of attacks leveraging advanced tools. Companies erroneously assume their backups are their defense, but in 2021, backups were targeted in 94% of attacks and at least some repositories were affected in 68%.

While no one is immune to attack, enterprises that can least afford downtime are among the most likely to be targeted as they have the greatest incentive to pay. These include healthcare (where downtime can cost lives), financial services, retail, and manufacturing (where loss of transactions can cost up to millions per minute), and legal, insurance, education/research, government, and other sectors where secrecy and sensitivity are paramount.

Incidents like municipal ransomware attacks provide a cautionary tale on the ripple effects of organizational disruption. Last year, a Ryuk ransomware attack on Belgium's third largest city, Liege, left civil status and population services at a standstill, causing the widespread cancellation of burials, weddings, birth registrations, and other municipal services. Hackers attacking East London's Hackney council disrupted homebuyers' ability to process land search requests, creating a collapse in property purchases. This year, Costa Rica made history as the first country to declare a state of emergency following a ransomware attack by the Conti group, which affected government services, took healthcare services offline, and affected private-sector companies involved in the import/export of goods. And on a smaller scale, an attack on Bernalillo County in New Mexico forced the closure of municipal buildings and the 24-hour-a-day lockdown of inmates in an affected detention center, as surveillance cameras and automated door locks were rendered inoperable. While it's clear that disruption hits the fiscal health of the organization, it is equally true that, for many industries, downstream effects on customers, patients, and nations are potentially massive in scale.

Just how expensive is downtime? It varies widely by business and industry, but according to Uptime Institute's 2022 Outage Analysis Report, over 60% of outages cost over $100k; 15% of outages cost over $1M. Looking at data in Figure 1 below, which is presented in NetDiligence's 2022 Ransomware Spotlight Report drawn from a database of cyber insurance claims of 1,400 ransomware incidents between 2017 and 2020, we see that, while average total incident costs were $279k, business interruption costs (where applicable) alone averaged $375k.

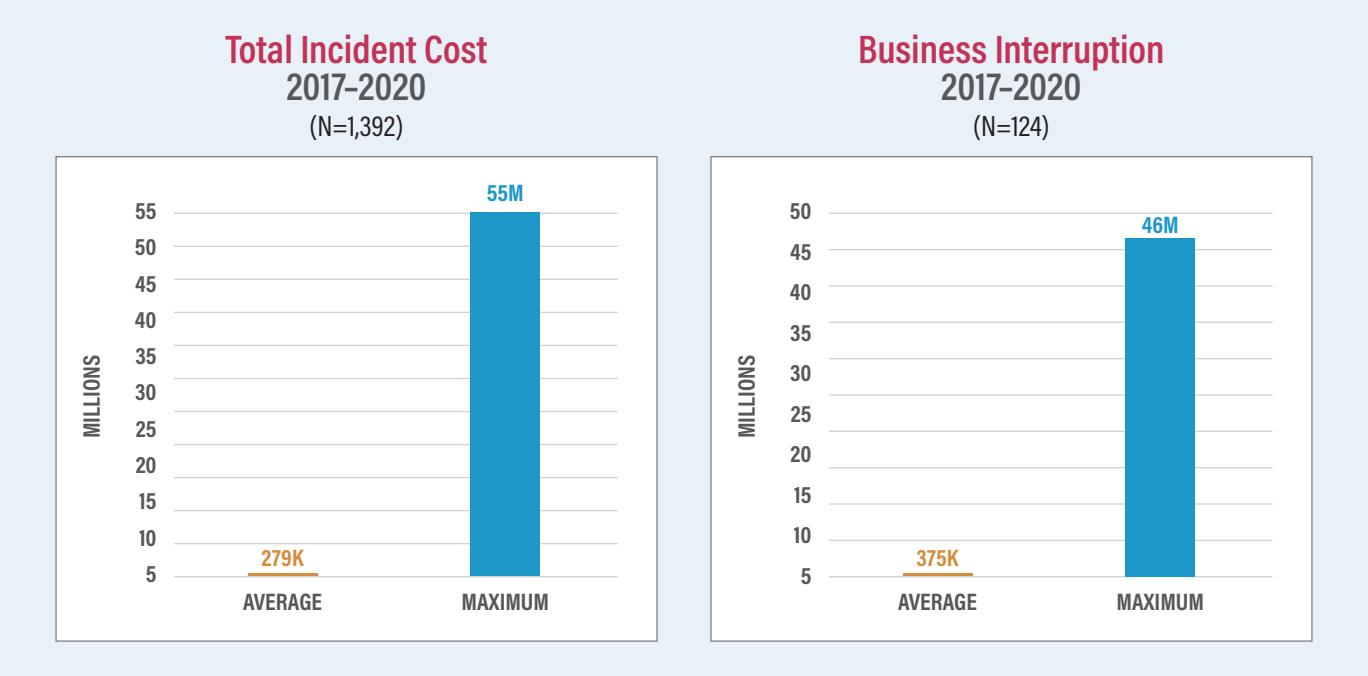


Figure 1: Incident costs of ransomware incidents, 2017-2020, from insurance claims database. Source: NetDiligence's 2022 Ransomware Spotlight Report.

Downtime costs and TTR are increasing in part because ransomware threat actors are ensuring it—by effectively targeting backups but also by ensuring their tools are as devastating as possible.

In 2021, backups were targeted in 94% of attacks and at least some repositories were affected in 68%.

Bringing Restoration into the Initial Response to Improve Results

In our gap analysis, client needs and typical response flows are no longer aligned. Because of the scale and complexity of today's attacks and massive impact of downtime to clients, restoration teams should be engaged in the immediate aftermath of the breach. We propose an evolution where restoration teams take the lead in deploying tools and capturing forensics data, rather than relying on in-house IT teams who are rarely as skilled in this area, while at the same time beginning the work that will lead to more timely resumption of operations. This work must be done before forensics can do their job; it makes far more sense that it be conducted by highly trained, qualified professionals immediately, rather than putting the onus on IT teams who have more generalized training and are under considerable pressure. The most effective way to minimize downtime is to forge a new model where DFIR, recovery teams, and internal IT/security teams work collaboratively at the outset, supported by trusted orchestration and collaboration tools.

The reasons are multifold:

- Restoration science is evolving: Restoration professionals, such as those at Fenix24, are already working in this model, quickly establishing remote access, and using advanced Endpoint Detection and Response (EDR) tools from companies like CrowdStrike and Palo Alto Networks to identify key systems, lock down access, detect infected files, applications, and systems, and collect the forensic data that DFIR teams need before they can begin their investigations.
- By initiating this process early, restoration teams can ensure no essential enterprise data is wiped. Because of higher levels of data encryption in today's environments, restoration teams are highly qualified to take the lead in forensics data capture.
- Restoration teams are in the best position to evaluate the recovery strategy. Greenfield (starting to rebuild from scratch) or backup-based recoveries are not the only options; restoration experts can evaluate middle ground options when employed early to find the fastest, most cost-effective path to normal operations.
- This proposed process flow has shown up to 50% improvements in TTR in our engagements.
- Restoration is increasingly an area of specialization requiring training; by consistently leveraging experts in this critical area, key decisions can be made much more rapidly, shaving down restoration times and business disruption costs for both the organization and cyber insurance carrier.
- Today's breach coaches are more technical and understand the complex challenges inherent in this era's cyberattacks. They are more engaged in the overall process and are beginning to understand that qualified vendors across the entire process are needed to reduce overall incident costs.
- Better communications and collaborations tools now exist from companies like Cygnvs that enable all partners and carriers to be in real-time, safe, and secure communication with each other and clients throughout the attack and recovery lifecycle. Where once collaboration among partners was awkward and atypical, we are finding that forging strong alliances and process flows together is creating better efficiencies for all parties. Cygnvs also enables third-party providers to conduct simulations within their platform to ensure that, when the stakes are high and speed matters, workflows, communications needs, and processes have been vetted and can be met at speed.

> **Attackers are preying on this complexity, finding security gaps in this vast estate of controls and configurations where patching and orchestration is suboptimal; areas where compliance and frameworks cannot shield the organization due to their lack of timely specificity.**

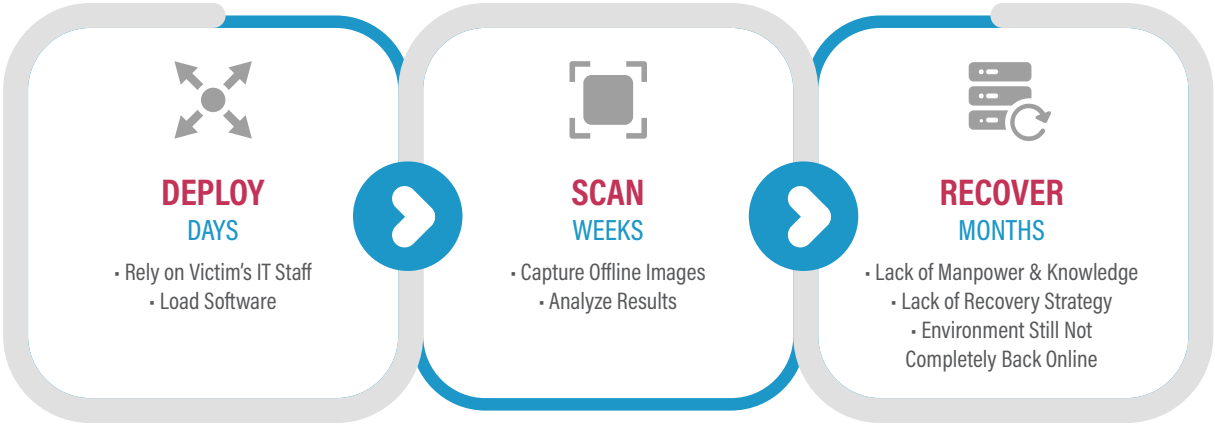


Figure 2: Historical Incident Response Process (No Restoration Partner)

A Shift in Process Paradigm Can Reduce Downtime Up to 50%

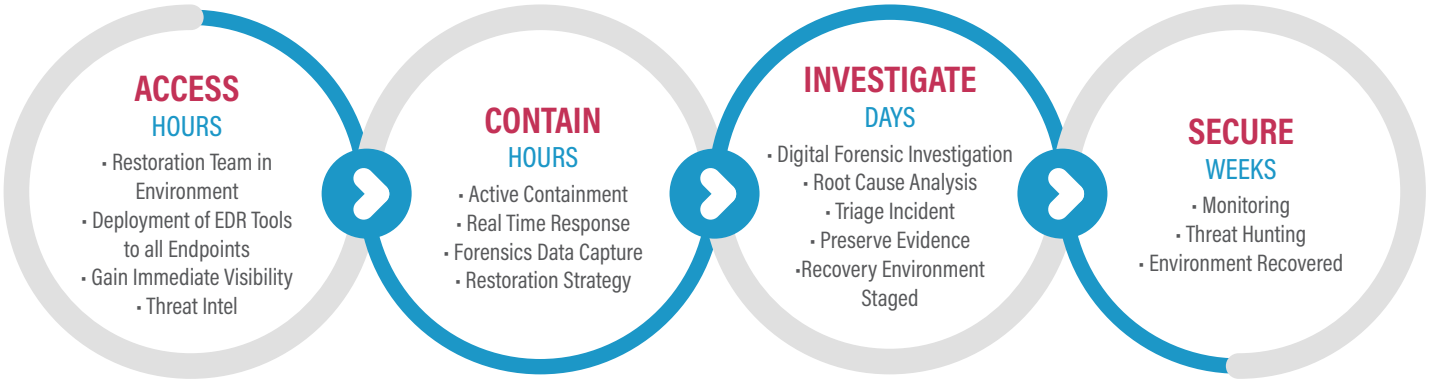


Figure 3: Proposed Incident Response Process (Restoration Partner Involved at the Outset)

- Accelerate incident response
- Minimize downtime
- Reduce business interruption (65% of cost of a cyber incident)
- Greater visibility for better decision making
- Lower overall incident response costs
- Reduced adversary impact

The typical referral flow is as follows: the enterprise hires a legal team (a breach coach), who then selects a DFIR firm. The DFIR firm and/or breach coach may, or may not, refer the company to a restoration partner. What we most often see is that breach coaches hesitate to recommend restoration partners to the victim organization given the lack of explicit carrier panels (lists of preferred, qualified restoration partners), leading to the perception by some in claims that restoration is an "extra" expense instead of the key to reducing business interruption costs. However, since everyone should be working together to reduce the costs of incidents, an orchestrated, more collaborative flow should be more broadly implemented to achieve these aims.

Overcoming Barriers to a Better Model

It often takes a fair amount of "pain" before we are willing to break an old, trusted model or process.

Thomas Kuhn, famous historian and philosopher of science, argued in "The Structure of Scientific Revolutions" that shifting paradigms are provoked by old models failing to fit new data—new, proposed models are met with harsh resistance, then acceptance, then rapid discipline change. We argue that IR methods and associated costs are now at the breaking point. Insurance carriers are aware they can no longer sit on the sidelines, uninvolved in the "how" and "who" conducts restoration. It is simply becoming too costly and commanding too great a share of the overall incident cost. And customers, of course, are looking to security professionals for efficient solutions. So, what are the barriers to adopting the proposed model and methods to overcome them?

According to Uptime Institute's 2022 Outage Analysis Report, **over 60% of outages** cost over $100k; **15% of outages** cost over $1M.

Addressing Knowledge Gaps: Educate, Educate, Educate

It's essential to continue educating the insurance carrier community about the true source of rising incident costs—the growing scale, scope, and impact of today's breaches, and the cost breakdowns of the activities within IR. Carriers assemble significant data, to be certain; but much of IR work is done under privilege, so carriers don't necessarily get the benefit of full transparency. The industry, including associations like NetDiligence, can assist by continuing to share amalgamated, anonymized data that demonstrates the high costs of downtime and the very high return on investment of expert restoration services.

It's also important to educate breach coaches that restoration must be viewed comparably to forensics: a specialty requiring outside expertise, by professionals focused on these esoteric challenges to ensure the job is done correctly, expediently, and comprehensively. It's time to shift the paradigm: we can no longer see restoration as something that IT or security generalists can or should do in an environment where breaches are so damaging, technologically advanced, and causing such financial and systemic damage. We believe many breach coaches already understand this; we can help others who lack sufficient access to data.

It's also necessary to educate clients that most restoration work can be done remotely, resulting in significantly faster progress. Restoration work can move in unanticipated directions, requiring the addition and shifting of specialized staff resources. Through remote access and work, restoration partners can be continuously agile in the allocated teams and eliminate travel expenses and associated delays, greatly reducing time and costs (by up to 50%) without compromising quality.

Encourage Carrier Panels for Restoration Experts

Insurance carriers have lists of qualified DFIR partners (or "carrier panels" mentioned above) their insureds must leverage in the event of cyberattack. Because they don't maintain panels for restoration partners, some breach coaches are hesitant to recommend restoration services, or may recommend companies they know without conducting exhaustive due diligence for quality. By encouraging the development of carefully vetted carrier panels that list reputable restoration partners, breach coaches and insureds will feel more confident that restoration partners listed are focused on consistency and can demonstrate quality standards and metrics, making restoration a more standard part of incident response processes.

In NetDiligence's 2022 Ransomware Spotlight Report drawn from a database of cyber insurance claims of 1,400 ransomware incidents between 2017 and 2020, we see that, while average total incident costs were $279k, **business interruption costs** alone **averaged $375k.**

Forming a Collaborative Ecosystem Among Incident Response Providers

Recovery partners benefit from strong, collaborative relationships with DFIR counterparts (and vice versa); it can be uncomfortable for some to bring in other teams early, as many of these teams are not used to working across the aisle at speed. Fenix24 has built strong partnerships with Palo Alto Networks, CrowdStrike, and others, and we see the model working to great effect. It does require some adjustment; teams must learn some new process flows, but once established, the efficiencies are undeniable. Orchestration and communications tools facilitate the expediency required.

What's Next? An Ounce of Prevention

Once the incident is finally resolved and all systems are up and running, we advise our customers not to be overconfident. The threat actor found their way through their defenses; and while this incident was diagnosed, resolved, and addressed, the enterprise has concrete evidence indicating they are due for an overall security posture assessment. Threat actors learn from their successes—companies whose defenses were penetrated, and particularly those companies who paid ransoms, are more prone to future attacks, or "reinfections." According to CyberReason's 2021 "Ransomware: The True Cost to Business" Report, 80% of companies that were affected by ransomware and paid ransoms experienced another attack. We advise our clients to be proactive, evaluating their security defenses for additional vulnerabilities. Many organizations believe that, since they are compliant with security or regulatory frameworks, they are secure. But attackers don't attack frameworks; they attack configurations and controls. Security controls are constantly changing, as are threat actor tactics. We recommend that organizations get a technical assessment based on control and configuration gaps (not policies) with assessment firms like Athena7, informed by current threat intelligence, to ensure they are prepared before another attack can strike.

Summary: In the End, Collaboration Is a "Win" for All Parties

The cybercrime problem is not improving; on the contrary, it continues to escalate despite some minor reprieves. Tensions between nations, a poor global economy, rising corporate IT complexity, are all poor indicators for malicious cyber activity. And threat actors are always evolving.

In this milieu, the costs continue to mount. Downtime is a bill that keeps growing higher for private- and public-sector organizations and the cyber insurers who are contracted to offset their rising risk exposure. While all are looking for solutions, we offer an innovative approach to incident response that can help greatly accelerate resolution times, shorten business interruption, arm teams to do their best and fastest work, and enable real-time agility during a fast-evolving crisis.

By collaborating as coordinated, dynamic incident response team that includes restoration partners, everyone wins: the business is up and running faster; costs are reduced for the organization and cyber insurer; forensics teams get the data they need to investigate with greater expediency; and "across-the-aisle" partnerships are formed to the betterment of the industry at large.

Changing paradigms is never easy, but we and our cyber insurance beneficiaries are seeing meaningful results. We invite others to join us.

References

- Yahoo Finance, "Forrester Technology Adoption Profile Survey Reveals Recent Security Breaches Among Top Purchasing Drivers for Next-Generation Firewalls (NGFW)," May 15, 2014.
- Sophos, "The State of Ransomware 2021," April 2021.
- Checkpoint Blog, "Check Point Research: Cyber Attacks Increased 50% Year over Year," Jan. 10, 2022.
- Abnormal Security, Abnormal Blog, "Q2 2022: Ransomware Landscape Continues Its Decline as Another Major Group Shuts Down," Aug. 15, 2022
- Veeam Software, "Veeam Data Protection Report, 2021," March 19, 2021.
- The Record, "City of Liege, Belgium hit by ransomware," June 22, 2021.
- Cyber Management Alliance, "5 Major Ransomware Attacks of 2022," June 15, 2022.
- State Scoop, "Months after ransomware attack, Bernalillo County, N.M., adopts cybersecurity policy," April 29, 2022
- Uptime Institute, "Outage Analysis Report," June 8, 2022
- NetDiligence, "2022 Ransomware Spotlight Report," v.1.1.
- Kuhn, Thomas S., "The Structure of Scientific Revolutions," 1962.
- CyberReason, "Ransomware: The True Cost to Business," June 2021.

> "The most effective way to minimize downtime is to forge a new model where DFIR, recovery teams, and internal IT/security teams work collaboratively at the outset, supported by trusted orchestration and collaboration tools."

AUTHORS:

Mark Grazman, *President of Conversant Group & Co-founder of Fenix24*

Heath Renfrow, *Co-founder of Fenix24*

Lindsay Smith, *Director of Content Marketing*

Fenix24, part of the Conversant Group family of companies, is a disaster recovery service provider that is raising the bar for post-incident response and restoration to significantly reduce the costs of downtime for its customers. Our battle-tested professionals are challenging old models, executing the most efficient and strategic recovery playbook in the industry for minimal costs and business interruption. Fenix24 is the army you need to push out the criminals that have compromised your environment and restore your company's IT operations.

Learn more at Fenix24.com.

FENIX24
A CONVERSANT GROUP COMPANY

fenix24.com

CONVERSANT GROUP

conversantgroup.com

1-855-FENIX24 | **Fenix24_dr**