FORRESTER®

SpearTip Incident Response Services Are Valued By Both Cyber Insurers And Organizations With Active Breaches

The cybersecurity threat landscape has never been more treacherous. The frequency and sophistication of attacks is on the rise, leading to increased frequency of costly breaches. The resulting cost of a breach can be significantly reduced based upon the timeliness and effectiveness of the data breach investigation and remediation.

SpearTip Incident Response (IR) service supports organizations facing an active breach through rapid engagement, identification, isolation, and remediation. With advanced cybersecurity expertise and specialized resources available 24/7/365, SpearTip is a trusted partner to cyber insurance providers that can engage quickly with insured clients. SpearTip utilizes its own proprietary tools to identify, contain, and recover from breaches. The company supports direct clients, insurers, and brokers by providing professional communications at every stage of the process, so all appropriate parties are kept aware of actions being taken, progress toward mitigation, and any valuable insights as they are discovered.

To better understand the benefits, costs, and risks associated with both SpearTip's managed security and incident response services, SpearTip commissioned Forrester to conduct a Total Economic Impact™ (TEI) study for its managed security services solution, ShadowSpear.[1]

In addition, SpearTip commissioned Forrester to conduct a Spotlight study of its incident response services.[2] This Spotlight study provides highlights of the TEI study, which included interviewing four decision-makers using SpearTip, two of whom started working with SpearTip to deal with an active breach. Two cybersecurity insurers were interviewed specifically for this Spotlight study. Highlights of the TEI study are included on page 6 due to the commonality of tools and skills utilized in security managed services, such as investigations and recovery activities, and the role that SpearTip's services have in significantly reducing the probability of breaches.

Less than 1 hour to engage incident response team

Global, 24/7/365 incident response team availability

INCIDENT RESPONSE SERVICE REQUIREMENTS

The interviewees' organizations searched for an incident response service that could provide:

- **Availability to quickly engage an incident response team on an active breach.** The interviewees from the two companies that engaged with SpearTip during a breach, as well those from the cybersecurity insurers, considered the availability of an incident response team to engage almost immediately to be essential to getting help resolving data breaches.
- **Global, 24/7/365 availability for incident response.** The cyber insurance interviewees

said that their firms require that IR partners have teams available for global assistance on a 24/7/365 basis.

- **Specialized expertise and tools leading to effective and efficient incident response.** The cyber insurance interviewees expect their IR partners to have teams with the necessary skills and tools to quickly and effectively investigate, contain, and remediate client breaches.
- **Professional and soft skills ensuring all appropriate parties are properly informed of progress and findings.** Every stage of the incident response process is stressful for and important to the breached organization, as well as the cybersecurity insurer, requiring empathetic communications.
- **Claim process completion that is both thorough and timely.** The cyber insurance interviewees require that their IR partners have knowledge and focus to provide completed claims documents in a timely manner.
- **Strategy risk advisory for cybersecurity insurers.** Per the cyber insurance interviewees, the reputation of insurers depends upon their ability to provide cybersecurity risk advice to clients, and they expect IR partners to be able to assist them in this activity.
- **Ability to increase clients' operational resilience.** Interviewees from the breached organizations and cyber insurance companies sought IR partners that would provide support beyond active incident response activities to offer education on preventative measures and incident response preparation.

USE CASES: CYBERSECURITY INSURANCE

For this study, Forrester interviewed two cybersecurity insurers that SpearTip obtains referrals from, or gets engaged by, when clients experience data breaches and for advisory services.

- The breach response services unit of a cyber insurance company has utilized SpearTip as a forensic vendor for more than two and a half years. The interviewee is the co-chair of the firm's forensic vendor panel, which evaluates and selects vendors for client incident referrals.
- A cyber insurance broker works directly with IR experts like SpearTip in support of corporate clients. The broker also provides advice and consultation on mitigating risk, financing it, and designing insurance coverage that effectively addresses key operational risks. In addition to IR referrals, SpearTip may be engaged to discuss IR preparation and its relationship to a client's insurance policy.

> **"SpearTip helps us on our mission to be a strategic risk advisor to clients."**
>
> *Cyber product leader, risk advisor, and insurance broker*

USE CASES: CLIENTS WITH BREACH

For this study, Forrester interviewed two companies that were experiencing a data breach and engaged SpearTip.

- A managed IT service provider had an incident progress to become a ransomware attack. The company's insurer engaged SpearTip Incident Response services to recover from the breach. SpearTip worked efficiently and communicated openly, which prevented significant downtime and helped establish a trusted partnership. Prior to this incident, recovery efforts threatened to overwhelm the resources of the managed IT service provider's security team, but the firm paid no ransom with the help of SpearTip.
- An IT service provider initially utilized Incident Response services from SpearTip to recover from an accidental inside attack. Malware, hidden in an acquired business' server, was awakened

through a simple adjustment by an IT technician. The attack quickly spread across the data center, and the IT service provider feared it could expand to other data centers and take down the entire company. Despite the attack occurring at 3 a.m., SpearTip began remediation within an hour of being contacted due to its 24/7/365 availability.

KEY FINDINGS: CYBERSECURITY INSURANCE

- **Rapid incident response globally, 24/7/365.** The insurance industry interviewees noted that they need broad coverage because threat actors frequently attack during off-hours when more limited monitoring and reduced remediation resource staffing were likely. SpearTip provides that full coverage.

  Both interviewees were satisfied that SpearTip's turnaround time from initial contact to action is less than 1 hour.

  The interviewees were impressed that SpearTip has both a global 24/7/365 incident response service and a security operations center (SOC).

"I refer clients to SpearTip because of their SOC with 24/7 monitoring capability, the incident response service, and the ShadowSpear tool — having all those capabilities makes them stand out."

Breach response services manager, specialist insurer

- **Specialized expertise and effective professional skills.** The insurance industry interviewees were both aware that SpearTip's team had cybersecurity experience from a blend of demanding organizations, including the US military, Secret Service, FBI, and cyberespionage companies. They noted that their technical expertise and historical experience provide valuable discipline for effective incident response, including an ability to frequently outmaneuver an adversary.

"They were one of the first forensic investigative firms I met that has drawn together such a strong forensic background and skill set."

Cyber product leader, risk advisor, and insurance broker

Both insurance industry interviewees valued the clear and thorough communications that SpearTip's team provided to clients through the incident response process. The interviewees said that the quality of information provided and speed at which it was delivered minimized the impact of cybersecurity events and made the SpearTip vendor relationship a valuable resource for their clients.

"Our insured [companies] that we're servicing — they're having a really bad day because they're in the middle of a cybersecurity incident. Their whole business and livelihood could be on the line. So the soft skills needed to empathize with an organization are just as important as their expertise. SpearTip does a good job with that."

Breach response services manager, specialist insurer

The cyber insurance industry interviewees valued SpearTip's process flexibility and the professional and considerate interactions of SpearTip technicians with clients during an attack recovery.

"SpearTip completely saved that investment for me and my partners. I'm going the distance with ShadowSpear."

Cofounder, IT service provider

- **Quality support through the entire incident and claims lifecycle.** Both insurance industry interviewees noted that the SpearTip team is a partner to their clients by sharing expertise outside of incident response events. They said that recommendations from SpearTip helped improve their clients' security posture by proactively addressing key operational risk areas.

  The insurance industry interviewees said that after concluding an investigation, SpearTip rapidly finalized reports, sent them to insurers, and shared information with attorneys so claims could be adjusted swiftly. They appreciated the flexibility of SpearTip in working with their billing processes, the accuracy of their reports, and the speed with which invoices were filed.

KEY FINDINGS: CLIENTS WITH BREACH

- **Rapid incidence response.** Both interviewees were pleased that SpearTip's turnaround time from initial contact to action is less than an hour.

> **"Within an hour of me calling them, they were in my network and doing their thing."**
>
> *Cofounder, IT service provider*

- **Recovery with no ransom, major server rebuilds, or major outages.** Both companies had minimal damage due to the breach. The threats were contained and remediated without the need to pay a ransom, extensive server rebuilds, or a major end-user disruption.
- **Timely and effective communications to the security team through leadership.** These companies were in crisis mode, with attention given by the clients' security team, IT, legal, and leadership. SpearTip was able to balance working to resolve the breach while providing continuous feedback and direction, so all parties understood both the plan and current state. The cofounder of the managed IT provider said, "SpearTip worked hand in hand with my teammates and went right to work coaching us on how to put a stop to this whole thing."

> **"I was impressed with how [SpearTip] handled things and communicated while they were doing a client's attack recovery. They were very, very cooperative, and very willing to explain what their software was, what it did, how to work through the incident response plan, [and] what forensic data they actually needed. If helped keep everyone focused on resolution instead of our fears."**
>
> *VP of technology, managed IT service provider*

- **Recovery experience led to managed security with ShadowSpear for the company and its customers.** Both companies went from having SpearTip resolve a breach to utilizing ShadowSpear for security operations. The interviewees noted that they are now more confident with their security posture and that they had realized cost savings due to labor productivity, infrastructure reduction, and security software elimination. The cofounder of the managed IT service provider shared that the company's M&A activities have increased due to reduced cybersecurity concerns.

  One of the companies now provides a white-label cybersecurity service to its clients due to its complete confidence in SpearTip and ShadowSpear.
- **No breaches since utilizing ShadowSpear.** Neither of these clients, nor any of the other SpearTip clients interviewed for the TEI study, has had a data breach since implementing ShadowSpear. The composite organization within the ShadowSpear TEI study found that the data breach risk reduction due to utilizing ShadowSpear was valued at $1.1 million over three years.

TOTAL ECONOMIC IMPACT ANALYSIS OF SPEARTIP'S MANAGED SECURITY SERVICE, SHADOWSPEAR

For more information, download the full study: "The Total Economic Impact™ Of SpearTip ShadowSpear," a commissioned study conducted by Forrester Consulting on behalf of SpearTip, October 2021.

Payback period

<6 months

EXECUTIVE SUMMARY

The cybersecurity threat landscape has never been more treacherous. The frequency and sophistication of attacks is on the rise. Organizations are overwhelmed trying to keep pace, facing hiring challenges due to scarce and expensive skilled resources; recognizing 24/7/365 coverage is crucial; and trying to stay current with cybersecurity software capabilities. Adding the capabilities of a security operations-as-a-service platform like SpearTip's ShadowSpear could control costs while providing protection.

STUDY FINDINGS

Forrester interviewed four decision-makers at organizations with experience using the ShadowSpear and combined the results into a three-year composite organization financial analysis. Risk-adjusted present value (PV) quantified benefits include:

- **Data breach risk reduction valued at $1.1 million.** The interviewees described many ways that ShadowSpear improved their processes for preventing breaches. The shift to 24/7/365 coverage was considered essential due to attacks frequently occurring during off-hours and holidays.
- **Security team efficiency gain valued at nearly $706,000.** Deploying ShadowSpear offloaded most network-monitoring responsibilities, improving productivity for customers' security teams.
- **Reduction in on-premises labor, software, and infrastructure cost valued at more than $416,000.** The interviewees' organizations eliminated a significant portion of their security software licensing and supporting infrastructure costs.
- **Accelerated merger and acquisition activity due to confidence in cybersecurity protection valued at almost $424,000.** Some interviewees described an increase in confidence extending all the way to their C-suite, eliminating conflicts to move forward with M&A activities due to cybersecurity concerns.

> **"If I had to hire staff to do these same types of security initiatives, it would cost me two, three times as much as what I'm paying SpearTip. It gives me a little more freedom to use those dollars to repurpose and bring in other talent to do things that are going to help move the business forward financially."**
>
> ***Chief security officer, healthcare nonprofit***

https://speartip.com/forrester-report/

Appendix: Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

[2] Spotlight is a product within our TEI product suite that provides a focus on a component of a company's technology offering without producing separate ROI, benefits, and cost metrics.


FORRESTER®