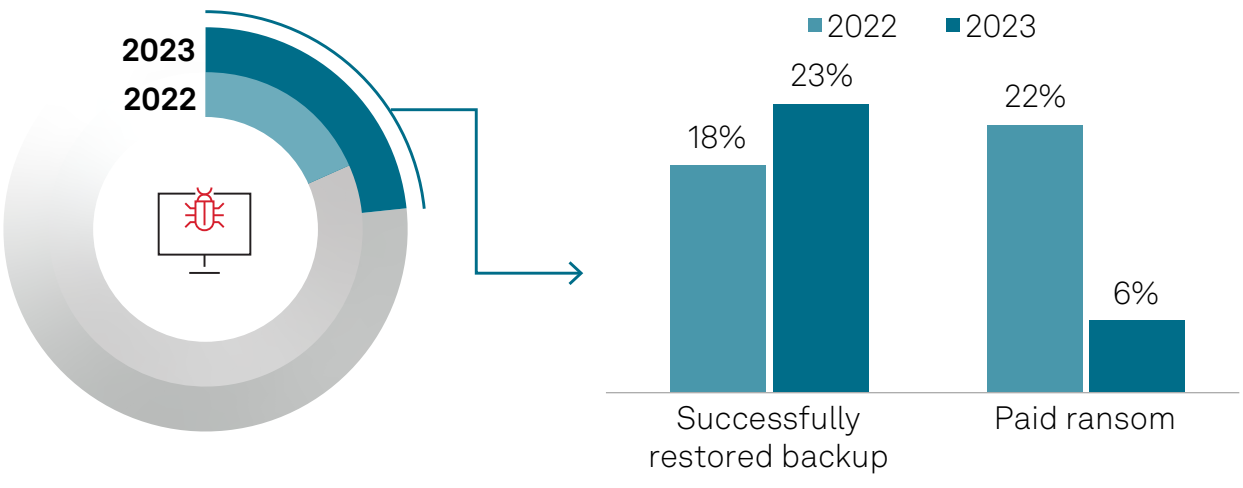
S&P Global
Market Intelligence

Filling critical incident response skills shortages with highly experienced service providers

The quantity, business impact and complexity of cyberattacks continue to **increase every year**

For example, a 451 Research study showed that **23% of respondents were victims of ransomware**, up from 18% of respondents in last year's study.



Q: Has your organization been the victim of ransomware in the past 12 months?
Q: How did your organization handle the ransomware event?
Source: 451 Research Voice of the Enterprise: Information Security, Endpoint Security studies, 2022 and 2023

The shortage of qualified security professionals continues to plague organizations

37%
of respondents in a 451 Research study indicating that they will be **adding managed security services** to augment staff or handle event-based responses

46%
of respondents indicated their organization plans to add managed services **to augment specific expertise** needed by their security team

Q. Is your organization currently changing, or planning to change, the layout of your information security team? Please select all that apply.
Q. What is the main reason your organization is adding managed services?
Source: 451 Research Voice of the Enterprise: Information Security, Organizational Behavior 2023

More than one-third (35%) of respondents said that current information security **staffing levels are inadequate** to address the challenges faced by their organization.

Respondents also indicated **difficulties with recruiting** and retaining information security professionals.

Acquiring and securing **legally defensible forensic data** after an attack is a key pain point for organizations.

31%
of respondents in 451 Research's Voice of the Enterprise: Information Security, Endpoint Security 2023 study felt that their endpoint security solution was **least effective at conducting after-the-fact investigations**.

Conclusions

It has become clear that employing a modernized incident response approach that leverages the capabilities of open **extended detection and response (XDR)** platforms plus a **security analytics platform (SIEM)** to feed the XDR with high-quality data is more effective and efficient .

This combination can enable organizations to return to a stable operating state **much faster** than traditional incident response approaches. Further, employing digital forensics best practices at scale, particularly for gathering data from endpoints, can be key not only in preserving evidentiary data, but also in speeding mean time to remediate for critical incidents.

Further, engaging an external **critical incident response team** can be an important tool in the fight against cyberattacks. These teams can provide both proactive and incident response capabilities, filling in talent gaps with highly specialized and experienced professionals that leverage best-of-breed tools.

wipro cybersecurity
by cybersecurists

To learn more about how Wipro's Critical Incident Response Team can secure your digital frontier, please contact us at: wipro.com/cybersecurity/contact/