SOPHOS

The Impact Of Compromised Backups On Ransomware Outcomes

Insights from 2,974 organizations that were hit by ransomware in the past year

A Sophos Whitepaper. March 2024

Introduction

There are two main ways to recover encrypted data in a ransomware attack: restoring from backups and paying the ransom. Compromising an organization's backups enables ransomware actors to restrict their victim's ability to recover encrypted data and in doing so dials up the pressure to pay.

This report provides deep-dive analysis of the impact that backup compromise has on ransomware outcomes. It also shines light on the frequency of backup compromise in ransomware attacks.

Research overview

The findings are based on a vendor-agnostic survey commissioned by Sophos of 2,974 IT/cybersecurity professionals across 14 countries whose organizations had been hit by ransomware in the last year. Conducted by independent research agency Vanson Bourne in January and February 2024, the survey reflects respondents' experiences over the previous 12 months. For further details of the respondents, see the appendix at the end of the report.

Executive summary

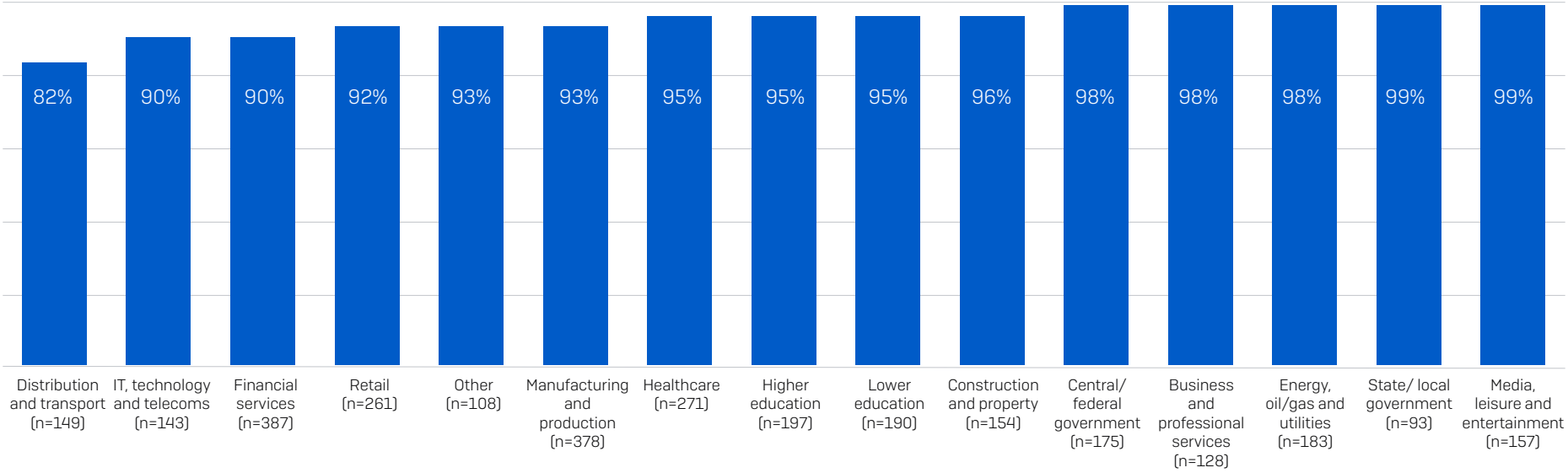
The financial and operational implications of having backups compromised in a ransomware attack are immense. When attackers succeed in compromising backups, an organization is almost twice as likely to pay the ransom and incurs an overall recovery bill that is eight times higher than for those whose backups are not impacted.

Detecting and stopping malicious actors before your backups are compromised enables you to reduce considerably the impact of a ransomware attack on your organization. Investing in preventing backup compromise both elevates your ransomware resilience while also lowering the overall Total Cost of Ownership (TCO) of cybersecurity.

Learning 1: Ransomware actors almost always attempt to compromise your backups

94% of organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack. This rose to 99% in both state and local government, and the media, leisure and entertainment sector. The lowest rate of attempted compromise was reported by distribution and transport, however even here more than eight in ten (82%) organizations hit by ransomware said the attackers tried to access their backups.

Percentage of ransomware attacks where attackers attempted to compromise backups



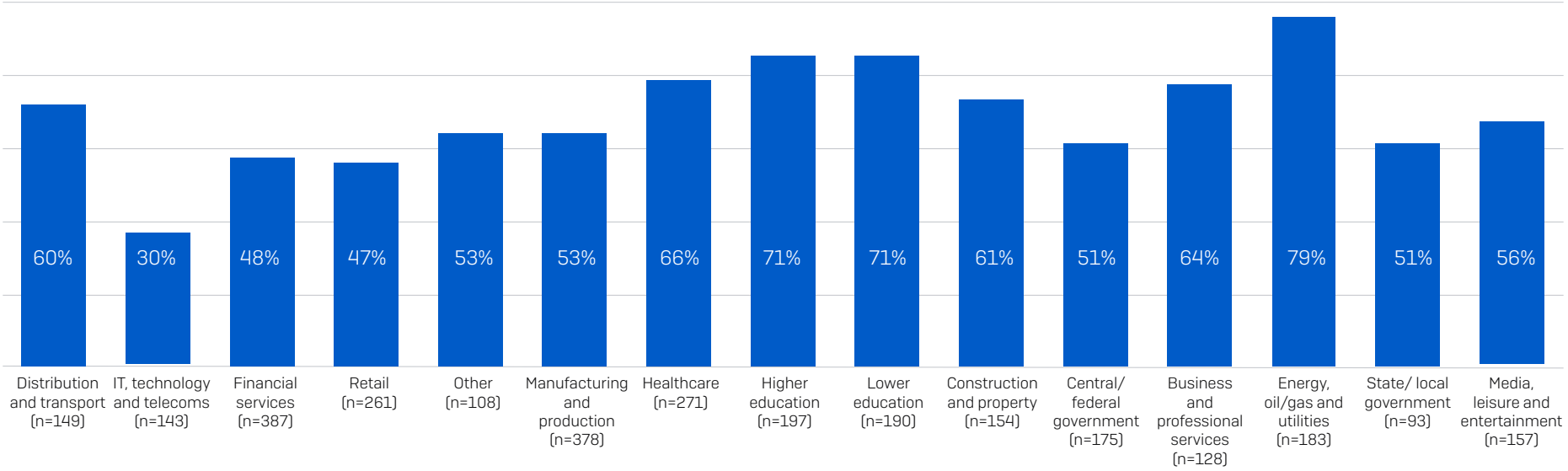
Learning 2: Compromise success rate varies greatly by industry

Across all sectors, 57% of backup compromise attempts were successful, meaning that adversaries were able to impact the ransomware recovery operations of over half of their victims. Interestingly, the analysis revealed considerable variation in adversary success rate by sector:

- Attackers were most likely to successfully compromise their victims' backups in the energy, oil/gas, and utilities (79% success rate) and education (71% success rate) sectors
- Conversely, IT, technology and telecoms (30% success rate) and retail (47% success rate) reported the lowest rates of successful backup compromise

There are several possible reasons behind the differing success rates. It may be that IT, telecoms and technology had stronger backup protection in place to start with so was better able to resist the attack. They may also be more effective at detecting and stopping attempted compromise before the attackers could succeed. Conversely, the energy, oil/gas and utilities sector may have experienced a higher percentage of very advanced attacks. Whatever the cause, the impact can be considerable.

Success rate of backup compromise attempts



Learning 3: Ransom demands and payments double when backups are compromised

Data encryption

Organizations whose backups were compromised were 63% more likely to have data encrypted than those that didn't: 85% of organizations with compromised backups said that the attackers were able to encrypt their data compared with 52% of those whose backups were not impacted. The higher encryption rate may be indicative of weaker overall cyber resilience which leaves organizations less able to defend against all stages of the ransomware attack.

Ransom demand

Victims whose backups were compromised received ransom demands that were, on average, more than double that of those whose backups weren't impacted, with the median ransom demands coming in at $2.3M (backups compromised) and $1M (backups not compromised) respectively. It is likely that adversaries feel that they are in a stronger position if they compromise backups and so are able to demand a higher payment.

Ransom payment rate

Organizations whose backups were compromised were almost twice as likely to pay the ransom to recover encrypted data than those whose backups were not impacted (67% vs. 36%).

Ransom payment amount

The median ransom payment by organizations whose backups were compromised was $2M, almost double that of those whose backups remained intact ($1.062M). They were also less able to negotiate down the ransom payment, with those whose backups were compromised paying, on average, 98% of the sum demanded. Those whose backups weren't compromised were able to reduce the payment to 82% of the demand.

Rate of Data Encryption

89% when backups are compromised

52% when backups are **not** compromised

Ransom Demand (Median)

$2.3M when backups are compromised

$1M when backups are **not** compromised

Paid Ransom to Recover Data

67% when backups are compromised

36% when backups are **not** compromised

Ransom Payment (Median)

$2.3M when backups are compromised

$1.062M when backups are **not** compromised

Learning 4: Overall ransomware recovery costs are 8X higher when backups are compromised

Not all ransomware attacks result in a ransom being paid. Even when they do, ransom payments are just part of the overall recovery costs when dealing with a ransomware attack. Ransomware-led outages frequently have a considerable impact on day-to-day business transactions while the task of restoring IT systems is often complex and expensive.

The median overall ransomware recovery costs for organizations whose backups were compromised ($3M) came in eight times higher than that of organizations whose backups were not impacted ($375K). There are likely multiple reasons behind this difference, not least the additional work that is typically needed to restore from decrypted data rather than well-prepared backups. It may also be that weaker backup protection is indicative of less robust defenses and greater resulting rebuilding work needed.

Those whose backups were compromised also experienced considerably longer recovery time with just 26% fully recovered within a week compared with 46% of those whose backups were not impacted.

Overall Ransomware Recovery Costs (Median)

$3M	when backups are compromised
$0.375M	when backups are **not** compromised

Recommendations

Backups are a key part of a holistic cyber risk reduction strategy. If your backups are accessible online, you should assume that adversaries will find them. Organizations would be wise to:

- Take regular backups and store in multiple locations. Be sure to add MFA (multi-factor authentication) to your cloud backup accounts to help prevent attackers from gaining access.
- Practice recovering from backups. The more fluent you are in the restoration process, the quicker and easier it will be to recover from an attack.
- Secure your backups. Monitor for and respond to suspicious activity around your backups as it may be an indicator that adversaries are attempting to compromise them.

How Sophos can help

Sophos MDR: Our experts defend your backups

Sophos MDR is a 24/7 expert-led managed detection and response service that specializes in stopping advanced attacks that technology alone cannot prevent. The service extends your IT/security team with over 500 specialists who monitor your environment, detecting, investigating, and responding to suspicious activities and alerts.

Sophos MDR analysts leverage telemetry from your backup and recovery solution to detect and stop attempted backup compromise, neutralizing ransomware actors before major damage is done. They also take signals from the security tools you already use, including your endpoint, email and firewall solutions, to detect ransomware and breaches. With an average threat response time of just 38 minutes, Sophos MDR works faster than your next threat.

Sophos XDR: Giving IT teams the visibility and tools to stop attackers

In-house teams can use Sophos XDR to get the visibility, insights, and tools they need to detect, investigate, and respond to multi-stage threats, across all key attack vectors, in the shortest time. With Sophos XDR you can leverage telemetry from your backup and recovery solution, as well as your wider security stack, to quickly see and respond to attacks.

Appendix

The survey was conducted in small and mid-sized organizations with 100-5,000 employees across 14 countries: Australia, Austria, Brazil, France, Germany, India, Italy, Japan, Singapore, South Africa, Spain, Switzerland, United Kingdom, United States.

2024-03-18 (WP-NP)

SOPHOS