
Survey

# Ransomware threats and cyber insurance

Huntsman®
Defence-Grade Cyber Security

> At two separate events that Huntsman Security attended and sponsored, we surveyed delegates to garner their views on how ransomware was changing their operational activities

# Ransomware threats and cyber insurance

Much has been written about the challenge businesses face in relation to ransomware, it is "everyware" – as Huntsman Security discussed in our **May 2022 webinar**.

But for all the news stories about ransomware cases – whether major organisations that provide services leading to huge disruption for millions, as in the case of Colonial Pipeline, or more localised and less critical businesses like KP peanuts – it is not always clear what effects these threats have had on the behaviours and approaches of security professionals, CISOs, technical teams and – critically – businesses.

The other aspect of the ransomware scourge is the effect on the cyber insurance market. How are cyber insurers responding to the risk their policy holders face? And what does that mean for your upcoming cyber insurance renewal?

At two separate events that Huntsman Security attended and sponsored, we surveyed delegates to garner their views on how ransomware was changing their operational activities.

The majority of respondents were highly experienced and skilled members of the security profession. One event comprised security professionals, managers and consultants together with internal and external auditors, and was organised jointly by two professional bodies (ISACA – the West Midlands chapter and the IIA). The other, was a membership organisation for major enterprises and security teams at some larger organisations – and was attended senior managers, security leaders and risk owners

## The Survey

The survey was short, multiple choice, and provided some space for respondents to elaborate on any actions the business had taken in response to the ransomware epidemic; some of those actions were as interesting as the answers to the questionnaire itself. During the events we received views from almost 50 senior security and audit professionals across all sectors.

The results are presented on the following pages.

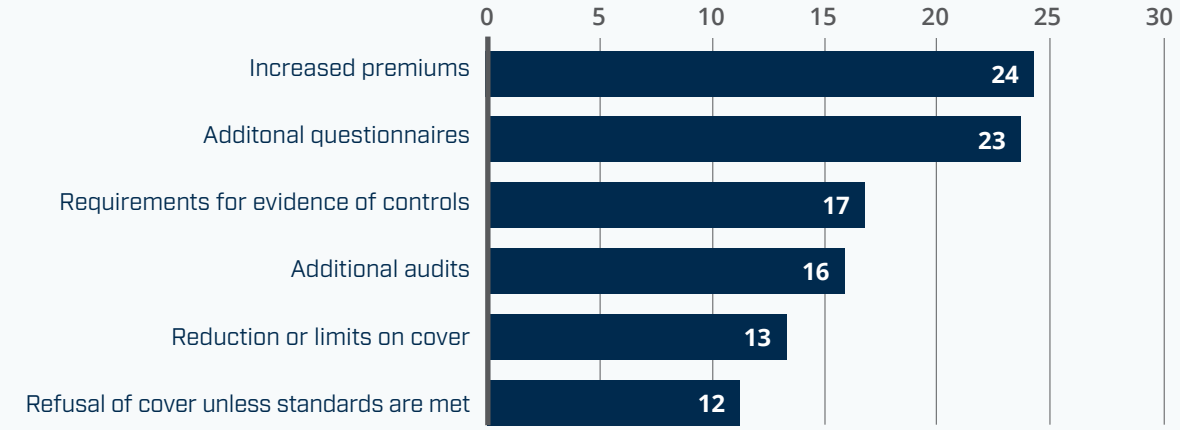
## Impacts on Cyber Insurance

We asked what changes respondents had observed in cyber insurance, particularly in terms of additional steps, costs or overheads required for cyber insurance renewal, as part of the overall risk management strategy.

The list of possible impacts we provided was not comprehensive or exclusive – so someone could easily have observed both increased costs and increased oversight (i.e. multiple answers were recorded). In fact, 30 respondents (64%) reported more than one impact being evident.

Have you seen changes in cyber insurance requirements?

(number of responses, multiple answers allowed)



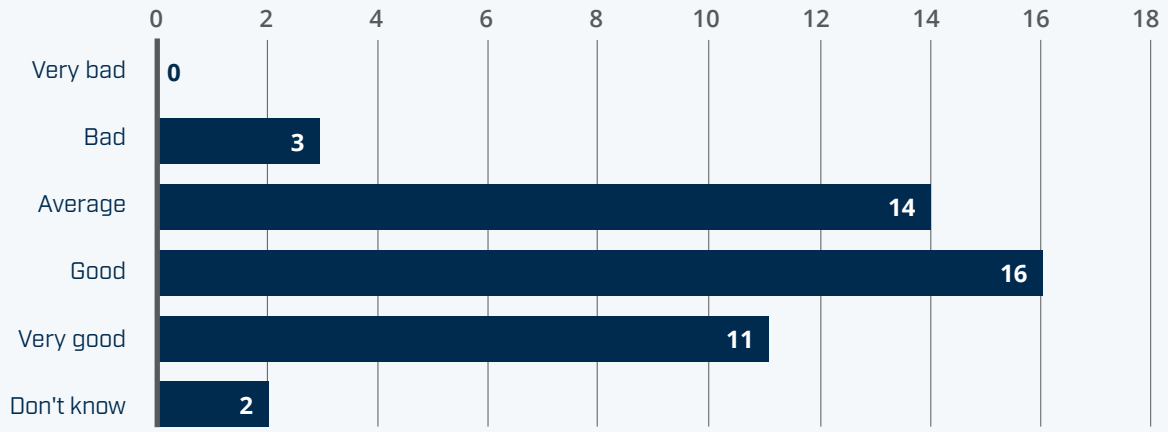

> “The results show that the commonest impact was financial, over half of the respondents cited an increase in the cost of premiums.”

The results show that the commonest impact was financial, over half of the respondents cited an increase in the cost of premiums. But the survey also brought out the increased underwriting rigour across the sector, with 23 people reporting additional questionnaires, 17 who were asked to provide evidence of their controls and 16 who had to undergo additional audits.

Finally, we saw limits on cover or refusal of policies being a challenge for almost 25% of those we surveyed. This suggests that for some businesses the risk of under-insurance or no insurance at all were very real prospects.

## The visibility of security risks

How good is your visibility of the risks your organisation faces from ransomware? (number of responses)




> This leaves a significant proportion (30%) with only average visibility of a risk that is well publicised, hugely damaging and difficult to insure against.

We then asked about the visibility of ransomware risks within the respective organisations represented. On such a question it is worth remembering that the answer could be "how visible" to the business in general, or specifically to the individual filling in the survey.

Given the audience was security and audit team stakeholders, however, it is safe to assume that if risks were not particularly visible to them, it is probable that they were not visible and hence understood by the rest of the business either.

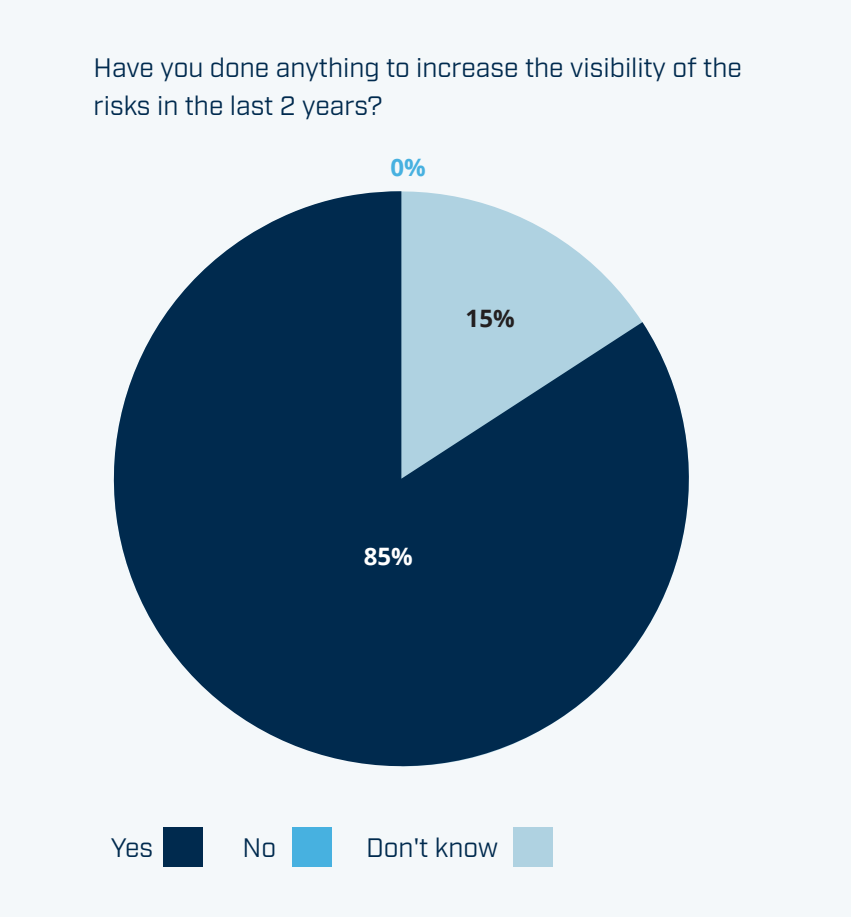
Most of the respondents (27 in total, almost 60%) responded that they had either "very good" or "good" visibility. This leaves a significant proportion (30%) with only average visibility of a risk that is well publicised, hugely damaging and difficult to insure against. Interestingly, most of the roles of those reporting this uncertainty were in audit or control assurance, rather than in security management or operations.

We sought to compare this set of answers to the previous ones. Is there any correlation between increasing insurance premiums and having good visibility of risks (and by implication good controls in place to provide that visibility)?

Of the 27 people answering "very good" or "good" 14 still saw increased premiums (52%). In the remaining 19 surveys we found 9 were also seeing an increase – roughly the same. So, it would appear that visibility and understanding of risks won't necessarily lead to premium reductions in isolation – there is likely to still be a need to provide further information and clarity to insurers. It seems clear that insurers are looking at the controls in place as a means to manage their own risks, as well as those of the insured organisation.

> “Ransomware has really spurred security and audit teams into action as regards controls assurance as a way to achieve better visibility of risk.”

## Improving controls and risk visibility




Given the broadly positive view above, one might expect the answer to this question to be different: Have businesses done anything to improve visibility? Why bother if visibility is already “good”?

Here we see that ransomware has really spurred security and audit teams into action as regards controls assurance as a way to achieve better visibility of risk.

85% have been bolstering security oversight and operational visibility of security in the last two years (since the highest profile ransomware attacks have been reported). Perhaps this explains why the quarter of companies now have very good visibility, either way, it does show that the need to improve is almost universally recognised.

Hence the tracking and management of additional controls, the embedding of new processes and behaviours, and the need to report on the progress of uplift projects and deliver operational KPIs to improve their risk management efforts.

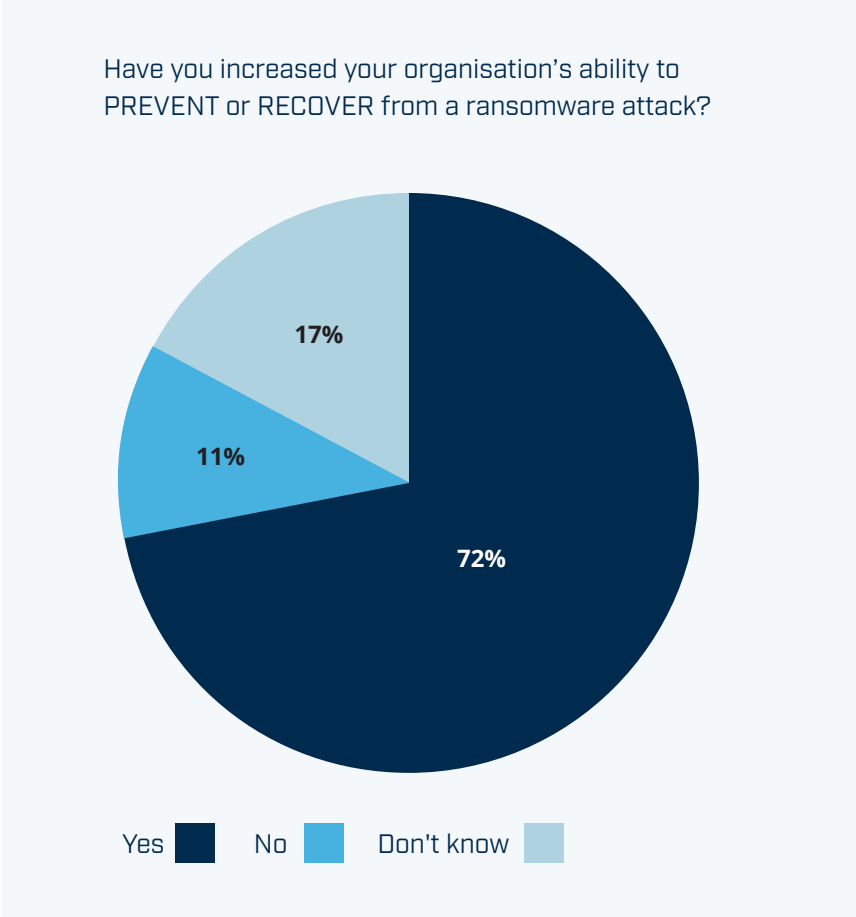
Notably, no survey respondents said that they had NOT done anything in this regard.

> “Most businesses have responded to the threat of ransomware with additional controls.”

## The ability to PREVENT and RECOVER from ransomware attacks

These next two questions asked whether specific control improvements had been made, and indeed (in free text), what those improvements were.

The first question was about prevention and recovery.




The responses to this question show that most businesses have responded to the threat of ransomware with additional controls (technology, controls or processes). 72% said “yes” and only 11% said “no”. While multiple answers to this question were possible, the proportion of “don’t know” answers is perhaps higher than would be expected given the responses to the previous questions.

In reality, the “don’t know” answers could fall into either camp – so if we were to allocate them equally between the “Yes” and “No” groups, we would see 80% of businesses reporting improvements and 20% not.

> “The descriptions of what control improvements had been made provides interesting reading.”

The descriptions of what control improvements had been made provides interesting reading. We took the answers and grouped them where possible, counting up similar tactics and also splitting out compound responses where several countermeasures have been deployed or initiatives pursued. The overall tally for the improvements is as follows:

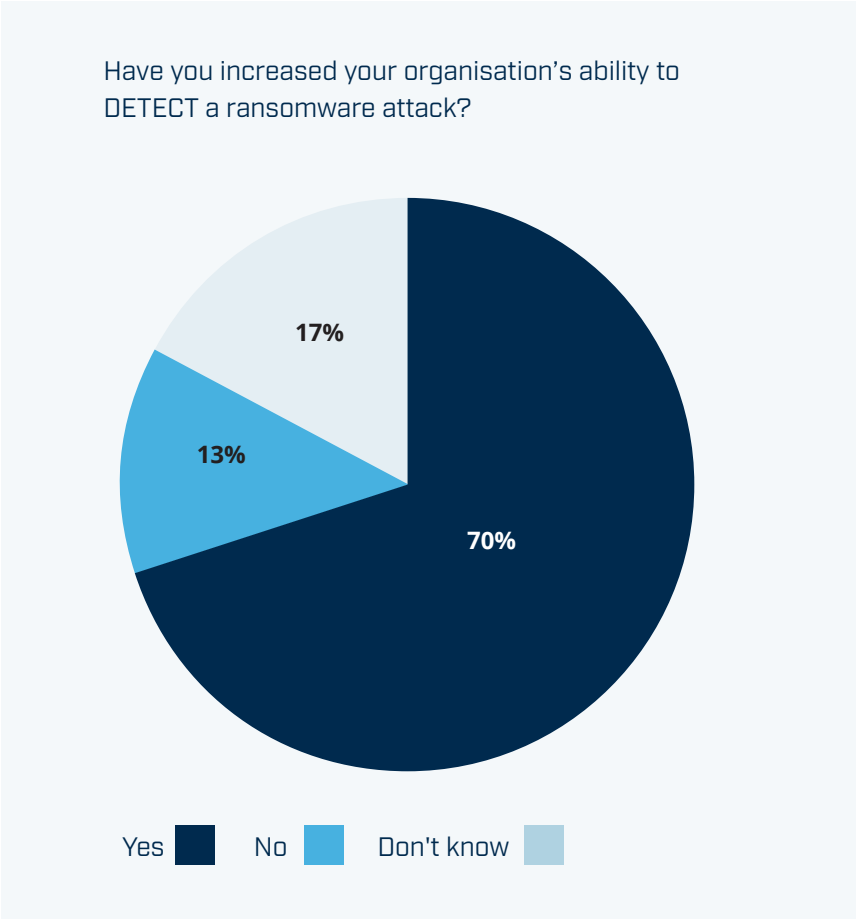
| Area of improvement | Tally |
|---|---|
| Focus on key controls/systems/tools | 14 |
| Monitoring/Intrusion detection/EDR | 7 |
| Incident management/BC planning | 6 |
| Reporting/visibility | 6 |
| Patching/vulnerability management | 4 |
| Awareness/Education/Training | 3 |
| Backups | 3 |
| Configuration Management | 2 |
| Ransomware table-top/desktop exercise/simulation | 2 |
| SOC team/technology | 2 |
| 3rd party risk management | 1 |
| Focus on defence | 1 |
| Phishing tests | 1 |
| Privileged account management | 1 |
| Single sign on | 1 |
| VPN remote access | 1 |

There is nothing in the list to argue with, and it is unsurprising to see that a focus on key controls, systems and tools is rated highest – the guidance from government on ransomware risks almost universally focusses on a shortlist of specific and high value defences.

> “Here we see similar results, slightly fewer answered “yes” and slightly more answered “no” but the overall shape of the data points is the same.”

## The ability to DETECT ransomware attacks

The second question was about detection of ransomware at the point of initial intrusion or as it takes holds and spreads. Ransomware is by its very nature an obvious attack once the attacker triggers the encryption and demands the ransom.




Here we see similar results, slightly fewer answered “yes” and slightly more answered “no” but the overall shape of the data points is the same. The number of “don’t know” answers is once again of interest for being higher than one might expect.

Some of the control improvements above relate to detection (and response of course), so the results of consolidating the free text answers again show a predictable distribution.

| Area of improvement | Tally |
|---|---|
| SIEM and log, monitoring and analysis | 8 |
| Extend/change SOC coverage/scope/provider | 7 |
| Endpoint detection/EDR/XDR | 6 |
| Deployed detection mechanisms/tools | 5 |
| Better/more proactive monitoring and improved controls | 5 |
| Penetration/external testing/validation | 2 |
| Patching/vulnerability management | 2 |
| Security Orchestration/Automation/Response | 1 |
| Increased resources (people) and focus | 1 |
| Focus on key controls/systems/tools | 1 |
| Establish emerging risk function | 1 |
| Enhanced Firewalling | 1 |
| Awareness/Education/Training | 1 |

The pattern is clear in the top 5 rows of the table of summarised responses. The degree of "infrastructure monitoring" covering SIEM technology and the role/use of a SOC take the first two positions in our list, then beneath those are three categories that relate to "endpoint monitoring" in some form or another. If we extract those and total the results, we get this table:

| Consolidated top 5 responses | Consolidated Tally |
|---|---|
| **Infrastructure** Monitoring (SIEM, Logging, SOC provision) | 15 |
| **Endpoint** Monitoring (EDR, XDR, endpoint detection) | 16 |

As such, both approaches carry a high degree of favour. From a sample of 47, almost a third have adopted one of these two well recognised detection approaches as part of their ransomware risk management (some have pursued both and so appear in both categories).

## Summary and conclusions

The results of the survey were interesting for the degree of agreement between the various security professionals, the audit community and conference participants. Ransomware awareness is high.

We can say with a high degree of certainty that ransomware is a widely recognised risk that most organisations have sought to in some way manage. The results also confirm a common view of the types of controls they have adopted to prevent, detect and recover from ransomware attacks.

We've also observed, however, that the cost of cyber insurance is significant and has been increasing. And this has historically been the case even for businesses that have improved their visibility of risk, and the controls they have for prevention, detection and recovery.

Perhaps once the reduced risk environment delivered by these tighter controls has had an impact on attack prevalence and severity these costs will start to reduce.

Given this, the reliance on better controls for more accurate risk pricing in this way directly implies our other clear finding: That insurers and enterprises alike are paying more attention to the reporting and assurance on the state of controls, the better visibility of risk and the efficacy of security operations processes.

## Want to find out more?

For more information on Huntsman Security's ransomware solutions for end users, consultants and insurers and how they can bring timeliness, reliability and consistency to cyber security posture management processes:

**Click here**

# About Huntsman Security

Since 1999, Huntsman Security has been on the cutting-edge of cyber security software development, serving some of the most sensitive and secure intelligence, defence and criminal justice environments in the world.


**HUNTSMAN | TIER-3 PTY LTD**

**ASIA PACIFIC**

t: **+61 2 9419 3200**

e: **info@huntsmansecurity.com**

Level 2,
11 Help Street
Chatswood NSW 2067

**EMEA**

t: **+44 845 222 2010**

e: **ukinfo@huntsmansecurity.com**

7-10 Adam Street,
Strand
London WC2N 6AA

**NORTH ASIA**

t: **+81 3 5953 8430**

e: **info@huntsmansecurity.com**

GINZA EAST SQUARE 4F
3-12-7 Kyobashi Chuoku, Tokyo
Japan 104-003

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman