

**RANSOMWARE UPDATE**





# The fight against ransomware

The data shows that only 59% of companies who paid a ransom successfully recovered all their data.



**Gareth Wharton**  
Cyber CEO, Hiscox

Sadly, cyber criminals and companies defending themselves have been engaged in an expensive and risky game of cat and mouse for the last decade. In 2019, however, we saw a significant shift in the criminal's favour. Ransomware attacks increased significantly, with a number of groups: -REvil, LockBit and others coming to the fore. Norsk Hydro<sup>1</sup> and the city of Baltimore<sup>2</sup> attacks being two of the most high-profile. During 2020, cyber insurers started to make increased cyber security demands of their customers. At this point in time ransomware was all about the encryption of data, so insurers mandated off-site backups to mitigate the risk of criminals using ransomware to encrypt their critical data. To a certain extent this levelled the field, forcing ransomware gangs to pivot their techniques.

Since 2020 two key trends evolved. First, the use of so-called double extortion techniques, whereby criminals are both encrypting and exfiltrating (stealing) data. Why did this change the game? Even if customers had created frequent off-site backups, criminals could still extort them over the release of the stolen sensitive data. Secondly, the proliferation of ransomware as a service (RaaS) lowered the barrier to entry for even the most unsophisticated cyber criminals. Similar to software as a service (SaaS) whereby customers rent a range of services like email or collaboration servers, RaaS allows criminals with no cyber knowledge to run ransomware campaigns for a modest monthly fee.

These two factors have driven insurers to demand new and better IT security controls. For example, not running insecure remote access services, ensuring remote services are properly protected by multi-factor authentication (MFA) and requiring enterprise-wide patching of critical services within a set

number of days after the vendor releases the patch. Now, companies not only have a higher bar to complete a cyber insurance proposal form, but to qualify for a quote there is often a need to enhance security controls or processes. This is all in an effort to make the company a more difficult target for ransomware gangs.

Of course, such security controls are not the only tools available to fight ransomware. Key vendors and governments have an interest in defending against the ransomware threat. For example, one of the most common techniques of ransomware gangs is phishing emails using Microsoft Office attachments that contain macros to download the first stage of a ransomware attack. Just this year, Microsoft announced it will be blocking Office macros by default. Though it is a positive step forward, we are already seeing the ransomware gangs pivot to different types of files such as .lnk or .iso files. This shows how quickly the game of cat and mouse moves.

Governments also play a pivotal role in fighting ransomware through more offensive operations. In the last 18 months, both US and European governments have targeted ransomware gangs. For example, the Interpol action against Clo<sup>3</sup>, the USA action against the Darkside gang<sup>4</sup> and Interpol's takedown of the notorious Emotet botnet<sup>5</sup>. Additionally, governments are trying to limit criminals' ability to 'cash-out' cryptocurrency. This is forcing ransomware gangs to either move to different type of attacks or shift their focus away from US/EU entities. Finally, government agencies, notably CISA in the USA and NCSC in the UK, have been much more proactive on raising alerts of potential attacks like the Log4j vulnerability in December 2021.

So, given the evolution of ransomware in the last few years, what is the current state of ransomware? Using the data from the **Hiscox Cyber Readiness Report 2022**, we can better understand what customers are really facing. The report is based on survey findings of more than 5,000 companies across eight countries and a range of sizes and industries.

The data shows that only 59% of companies who paid a ransom successfully recovered their data. It's important to understand that paying for a decryption key doesn't mean that you will get all your data back. In nearly all cases we see, the criminals do provide a working decryption key, as it is a business transaction to them after all. There are two things, however, that can limit the effectiveness of even a working decryption key. The first is speed, since it often takes weeks to fully decrypt data. Secondly, as the malicious encryption

<sup>1</sup> <https://www.bbc.co.uk/news/business-48661152>

<sup>2</sup> [https://en.wikipedia.org/wiki/2019\\_Baltimore\\_ransomware\\_attack](https://en.wikipedia.org/wiki/2019_Baltimore_ransomware_attack)

<sup>3</sup> <https://www.bleepingcomputer.com/news/security/operation-cyclone-deals-blow-to-clop-ransomware-operation/>

<sup>4</sup> <https://www.bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-operation-shuts-down/>

<sup>5</sup> <https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>

# The fight against ransomware

## continued

routine runs, it does so on live transactional systems. This is like pulling the power cord out of a live, running database server, and it is likely the ransomware process may damage the integrity of the data. In other words, the fact the ransomware has occurred, regardless of a decryption key means all data can't be fully recovered and needs to be rebuilt. Forty-three percent of those respondents who paid a ransom said they received the recovery key but still had to rebuild systems. Equally alarmingly, 36% who paid a ransom sustained another attack.

In most of the articles that make the press, the reason they are report-worthy is that either the company is high profile or the ransom demand is noteworthy (e.g., multi-million Dollar). However, our research shows the median ransom paid was under \$10,000. This shows that ransomware is not just large, complex attacks on big business by notorious ransomware gangs, but is now a commodity attack used by far less sophisticated attackers. The key point to note is that SMEs are absolutely not safe from this sort of attack.

We also find that there's a discrepancy in which certain industries are more likely to pay a ransom. When we look at the percentage of respondents who paid by industry, this suggests which company sectors are the most and least prepared.

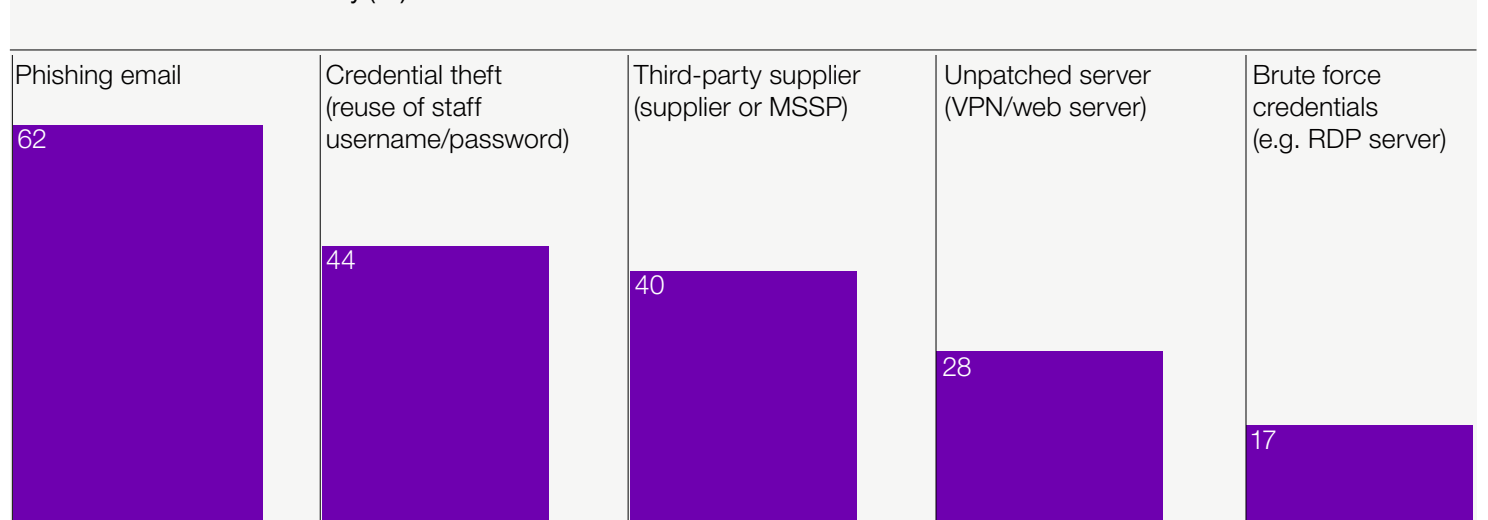
The most and least prepared sectors (%)



This largely tallies with our own experience. Both professional services and financial services often have the funding for more thorough security programs and are thus better protected with the ability to respond to an attack if one takes place. Additionally, the least prepared are also those industries with the some of the tightest supply chain windows and least required regulation on security. If an attack occurs, these companies can't be offline for long and paying the ransom often feels like the only option.

When we look at the data on how attackers got into respondents' systems, the results are similar year over year. There are five key entry methods, and from our internal data we see all of these being used. Though these attack vectors may be tried and tested by the ransomware gangs, they are not impossible to defend against.

Most common method of entry (%)



# The fight against ransomware

## continued



This summer, Hiscox conducted further analysis on the phishing threat. Per a recent test across five companies, we see that a generic phishing testing is not enough to stop ransomware.

We ran two tests against these five companies. Simulation one was using a well-known phishing test provider and standard phishing lures (i.e. Amazon package, LinkedIn alert, etc.). The overall click rate for mass emails in simulation one was 9%. Most interestingly, the most effective of the five lures was an Office 365 themed email around resetting a password. Though it's unsurprising with such a large Office 365 install base, the fact it was clicked four times as often as the other lures is alarming.

In simulation two, we used a targeted email, designed uniquely and specifically for each individual company, but with limited social engineering effort. We also targeted senior managers, rather than the general employee population. In this scenario, the click-through rate jumped four-fold to 36%. What this shows is that while phishing training is a critical part of any company's security requirements, targeted training for senior managers should also form part of additional support for senior staff.

Since there's no perfect result once a company has been attacked with ransomware, the ideal situation is to mitigate the risk as much as possible.

### Steps to prevent a ransomware attack include:

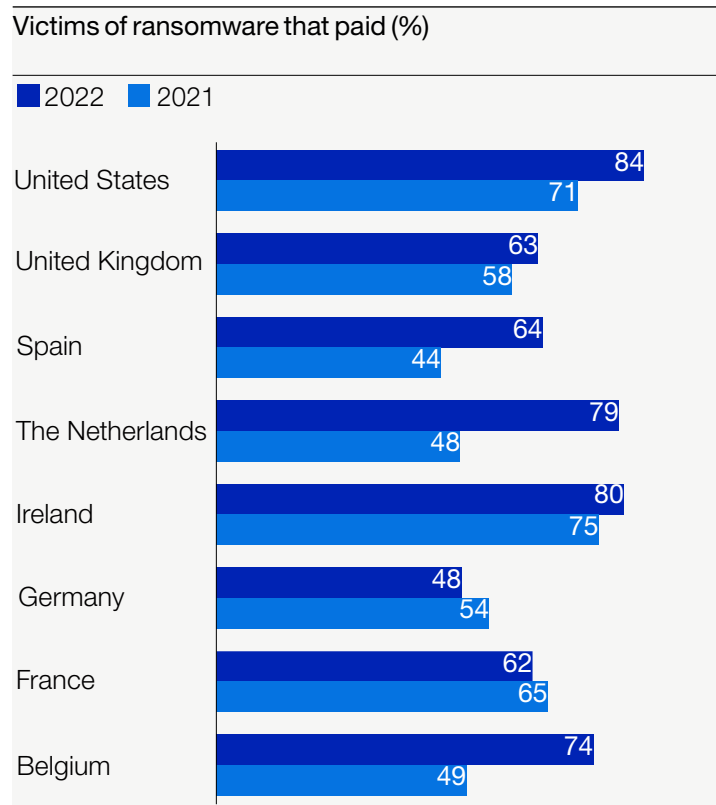
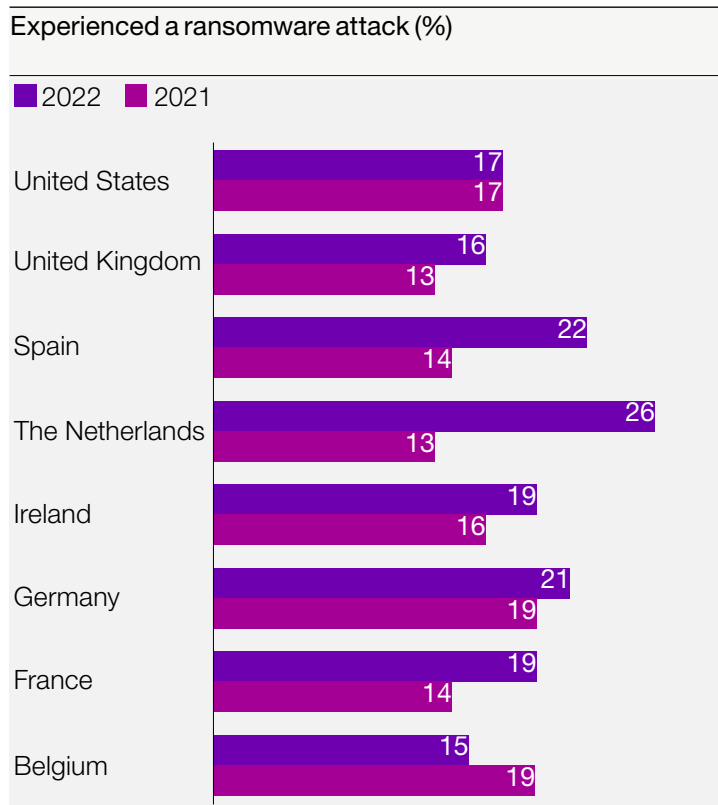
 <b>Attackers route in</b>	 <b>Mitigations</b>
Phishing email	General and custom staff training, strong email security
Credential theft (reuse of staff username/password)	Staff training on use of unique passwords, multi-factor authentication (MFA)
Third party (supplier or MSSP)	Understanding supply chains, regular audits
Unpatched server (VPN/web server)	Software bill of materials (SBoM) to know what is in your estate, regular patching
Unpatched server (VPN/web brute force server credentials e.g. RDP server)	Staff training on use of unique passwords, MFA, 'just in time' control of internet-facing ports

### If the worst happens, how do you mitigate a ransomware attack?

- Make sure you have reliable, frequent and tested offline backups – for small companies, this could be as simple as taking back-up drives home or storing them offsite.
- Prepare for the worst – make sure you have a ransomware response plan and test it frequently. Who would you call, how would you communicate with staff, customers, stakeholders, media etc.?
- Get help from your IT supplier help – do you need to retain a specialist incident response (IR) firm?
- Cyber insurance – use the benefit of a response firm through your insurance provider to manage the incident and get you back up and running.
- Don't panic – take time to assess the situation and the options you have before taking action

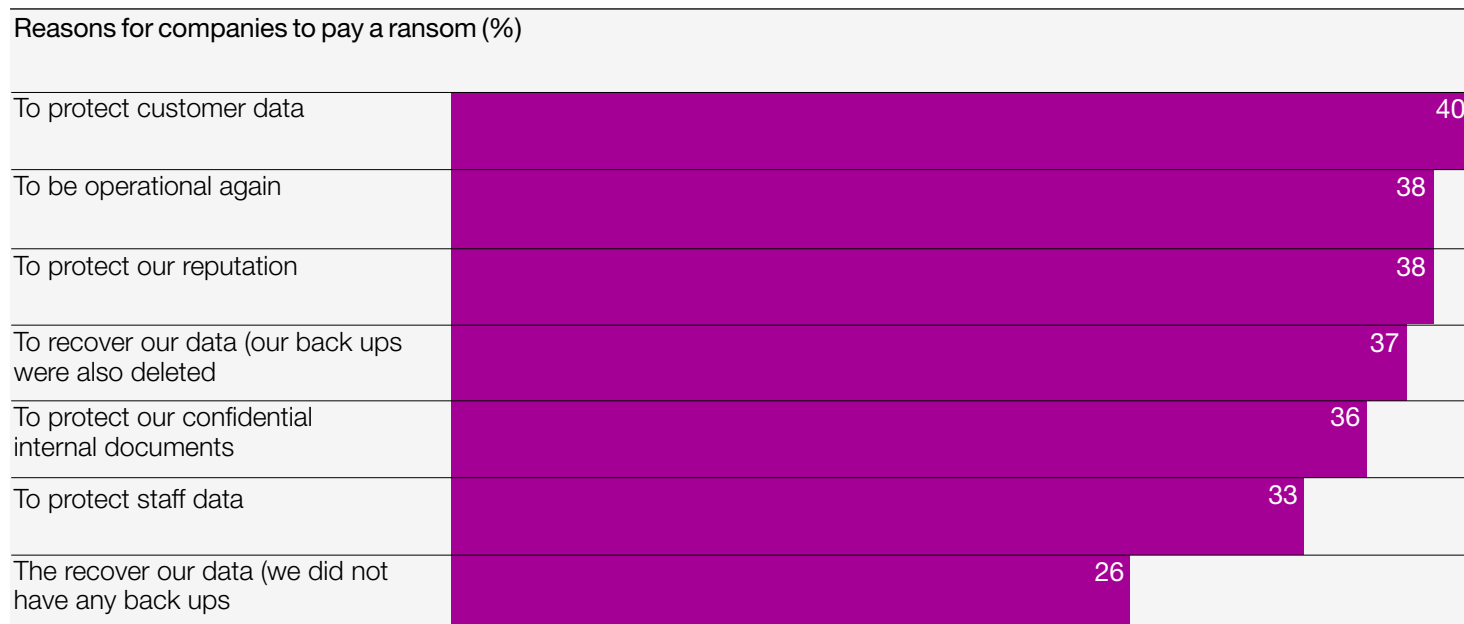
Ransomware is a threat to all businesses regardless of size, industry or location. It needs to be taken seriously by all parties, customers, insurers and governments. Co-ordinated action has shown to be effective, but there is much more to do. It's a threat you can and should protect yourself from, since as we've explained, once you've been attacked, there's no easy way to get back to business as usual. Most businesses are a target of commodity ransomware, not high-profile state actors, so companies should focus on making themselves difficult to be attacked. However, equally important is to have a plan if the worst happens – have a tested plan in place and good back-ups. A useful starting point is the NCSC '**Exercise in a box**' which is an online tool to allow businesses to practice their response to cyber-attacks (<https://www.ncsc.gov.uk/information/exercise-in-a-box>).

# Who's being attacked? Who's paying?



## Why did companies pay a ransom?

In many attacks, it appears ransomware gangs are deliberately targeting backups, reinforcing the need for segregated back-ups to be operational again. Companies need to protect customer data when data exfiltration occurs and criminals threaten to publish the data.

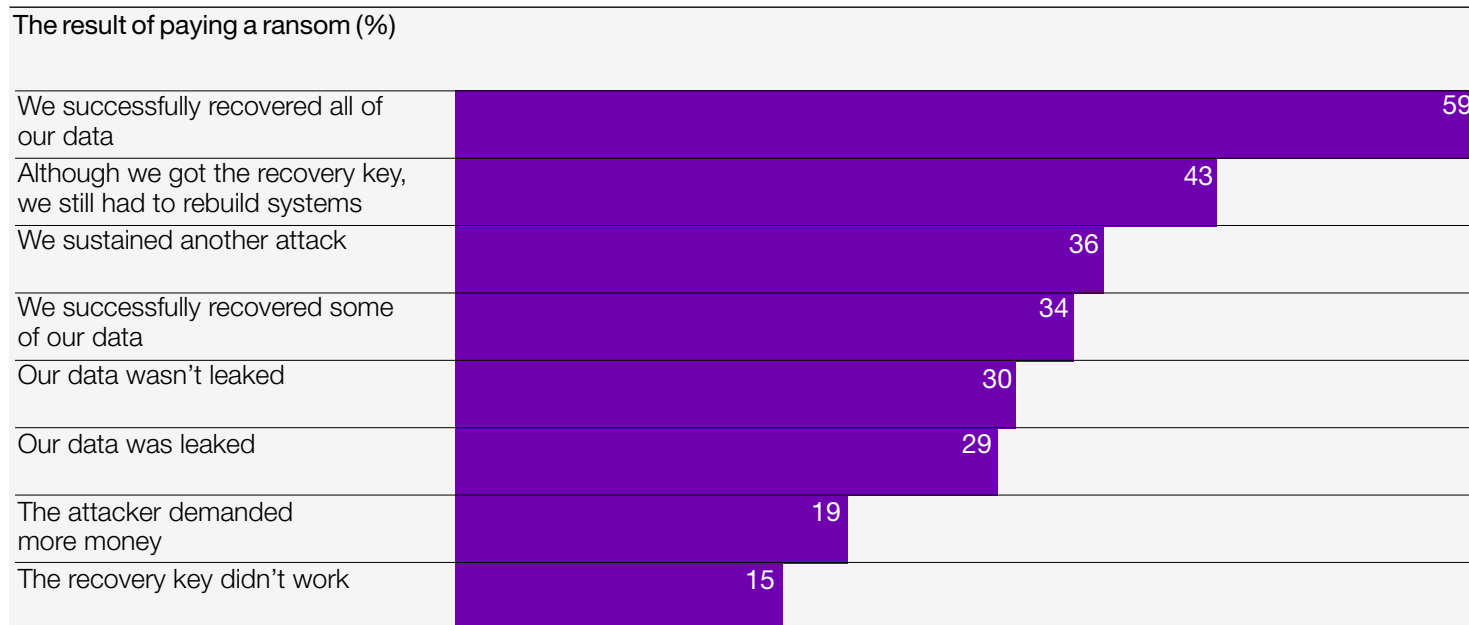


## Did paying a ransom work?

Only **59%** fully recover their data because in many cases not all data can be recovered.

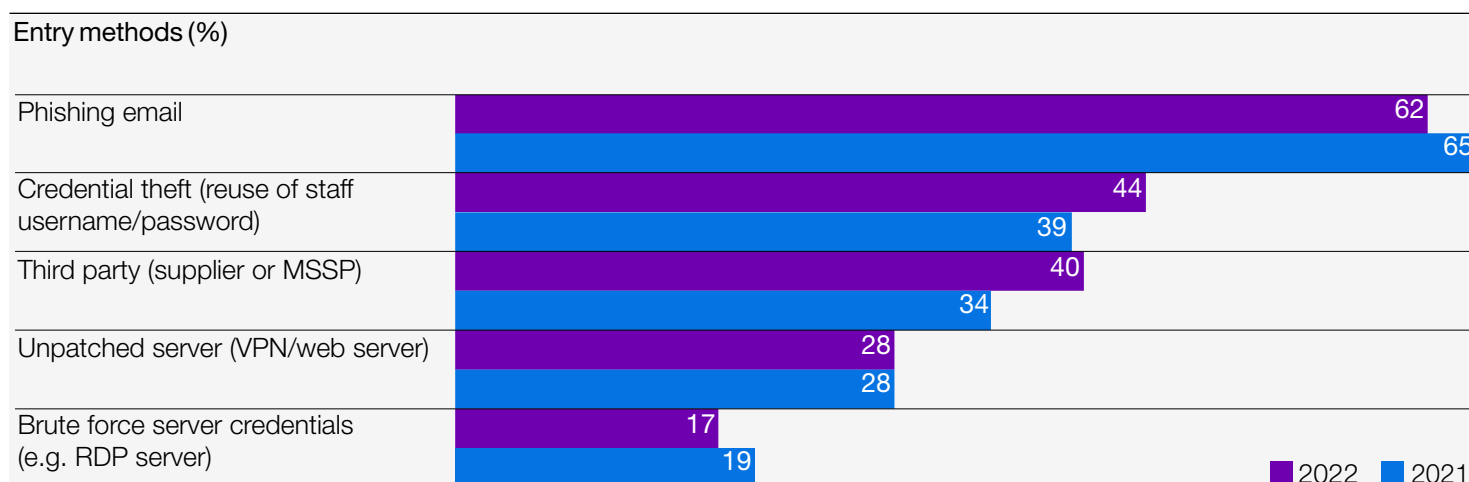
This is a commercial transaction, so there's no benefit for ransomware gangs to not give working decryption keys. That doesn't mean, however, that it will be easy to get back to business right away with the key.

For 36% of those who paid a ransom, the initial ransomware still led to further attacks.



## How are attackers getting in?

**Five key entry methods are being used.** These are tried and tested by ransomware gangs, but they're not impossible to defend against.



Per a recent small test by Hiscox across five companies, a generic phishing testing is not enough to stop ransomware.

Per Beauceron Security, click-rate average reports from global phishing vendors range from 3.4% to 12%. The overall click-rate for mass emails in a generic phishing test was 9%. In a more targeted approach to senior managers, they clicked 36% of the time. This is more than double the average and among a more high-profile group of people. Targeted training for senior managers is especially important.

**Hiscox Ltd**

Chesney House  
96 Pitts Bay Road  
Pembroke HM 08  
Bermuda

+1 441 278 8300

[enquiries@hiscox.com](mailto:enquiries@hiscox.com)

[hiscoxgroup.com/cyber-readiness](https://hiscoxgroup.com/cyber-readiness)