

The Hidden Costs of Ransomware

Businesses pay the price for partial protection.



CARBONITE® + WEBROOT®


Backup ◊ Train ◊ Block ◊ Protect ◊ Restore

opentext Business Solutions

┌

The true cost of ransomware infections includes more than just the ransomware payment.

We spoke with business leaders and IT professionals to find out how their organizations were affected by ransomware, beyond losing access to their data and paying a ransom.



Hidden costs can be just as significant as the ransom payment.

Even with security measures in place, defensive layers must be implemented to reduce the threat surface area.

←

Key findings

50%

of ransomware demands were more than \$50k

45%

were ransomware victims in both their business and personal lives

40%

of ransomware attacks consumed 8 or more man-hours of work

50%

of victims were deceived by a malicious website email link or attachment

46%

of businesses said their clients were also impacted by the attack

45%

of victims were unaware of the infection for more than 24 hours

38%

of businesses said the attack harmed their brand or reputation

17%

of victims were unable to recover their data, even after paying the ransom

Signs pointing to a decline in ransomware are no cause for celebration. Webroot's 2021 Threat report gleaned from our BrightCloud Threat Intelligence service reveals that attacks are declining but only because ransomware has become more targeted, better implemented, and much more ruthless, with criminals specifically targeting higher value and weaker targets.

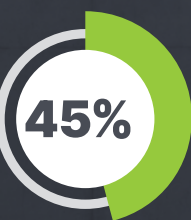
Businesses have become preferred targets because they can and will pay more to get their data back.

Although some businesses partially follow cybersecurity best practices, gaps in security exist because the threat surface area is so large, and because cyberthieves are so good at exploiting the gaps.

Operational Costs

Once inside the environment, ransomware replicates and spreads, causing more damage as it propagates. Some businesses are fortunate enough to spot the infection right away and immediately begin remediation. But for many businesses, the infection doesn't reveal itself for 24 hours or more after the initial infection.

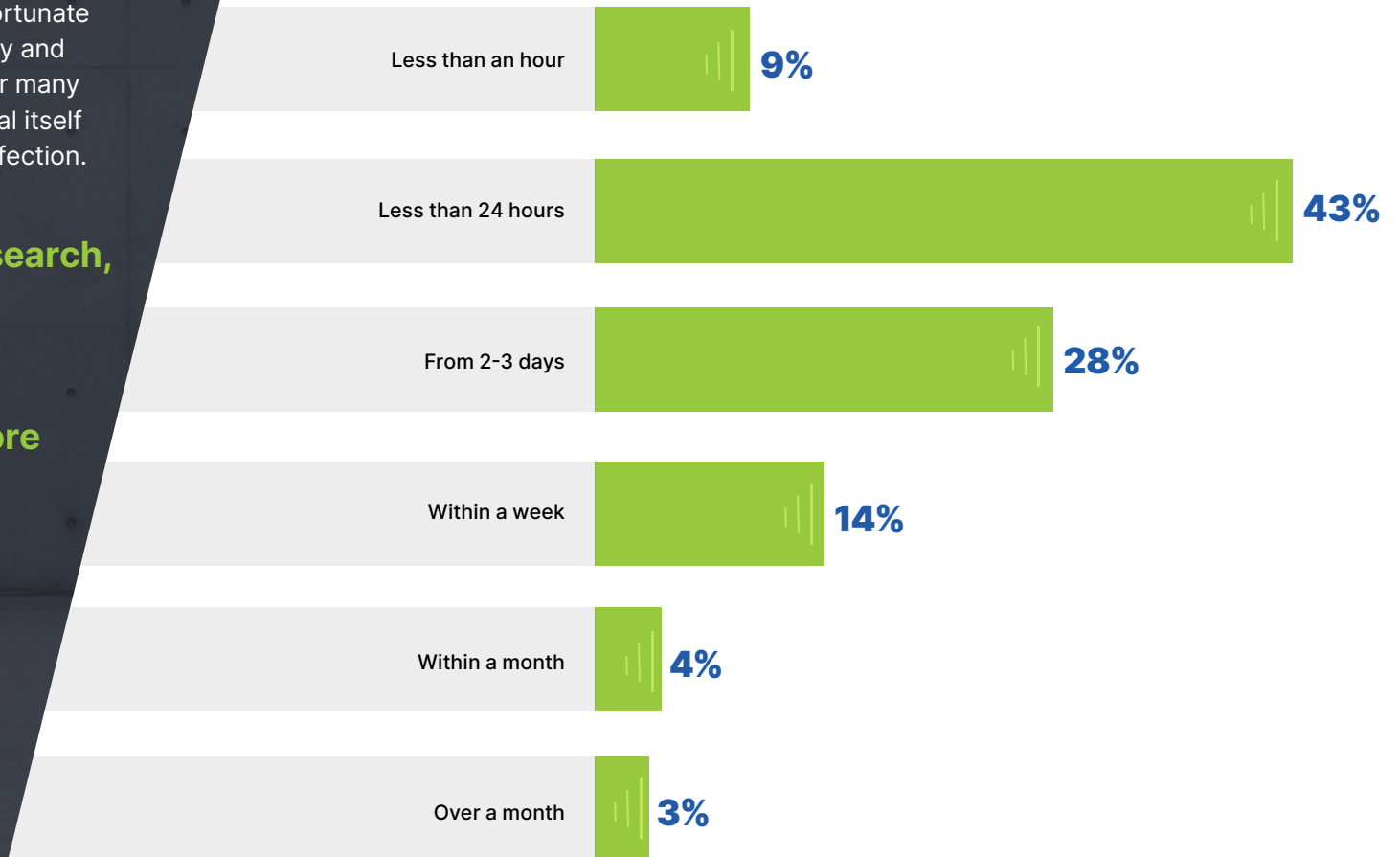
According to our latest research,



of ransomware victims were unaware of the infection for more than 24 hours.

Ransomware Time-To-Discover

This graph shows how long it took for ransomware to reveal itself after an initial infection.

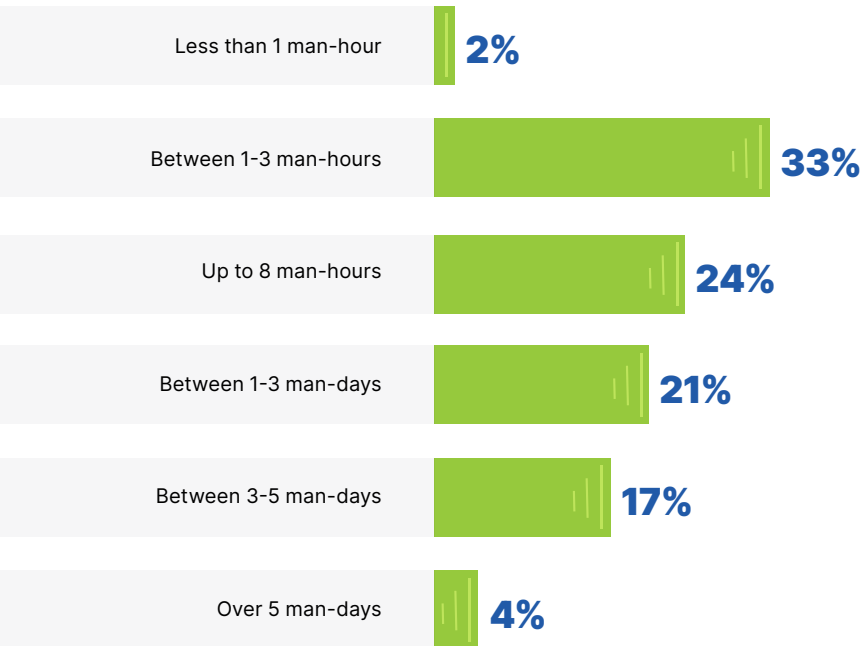


The further ransomware spreads, the longer it takes to mitigate. Every infected device requires additional man-hours. Sent emails and attachments with malicious content multiply the work involved exponentially. In best-case scenarios, a ransomware infection that is caught early may only require a few man-hours to remediate. In our study, while one-third of victims required three man-hours or less to remediate ransomware...



Ransomware Remediation Work-Hours

This graph shows how long it took to clear the system of ransomware and restore operations to normal.



The cost of ransomware remediation includes the work-hours required (which can be calculated) as well as the opportunity cost of diverting IT resources away from other strategic priorities (harder to quantify). The hourly cost for IT resources varies widely. At the high end, rates are around \$250 per hour, while conservative estimates are closer to \$100 per hour. Using these as benchmarks, it's possible to estimate the cost in IT resources for remediating ransomware at the high and low ends of the spectrum.

HIGH-END COST ESTIMATE	LOW-END COST ESTIMATE
\$250/hr. x 3 hrs. = \$750	\$100/hr. x 3 hrs. = \$300
\$250/hr. x 8 hrs. = \$2,000	\$100/hr. x 8 hrs. = \$800
\$250/hr. x 24 hrs. (3 work days) = \$6,000	\$100/hr. x 24 hrs. (3 work days) = \$2,400
\$250/hr. x 40 hrs. (5 work days) = \$10,000	\$100/hr. x 40 hrs. (5 work days) = \$4,000

As for the cost of downtime, the range of estimates is even wider, depending on the size and nature of the business, risk tolerance and vertical. Estimates for small and midsize businesses start around \$10,000 an hour while for enterprises, the average cost can be around \$300,000 an hour. In our study,

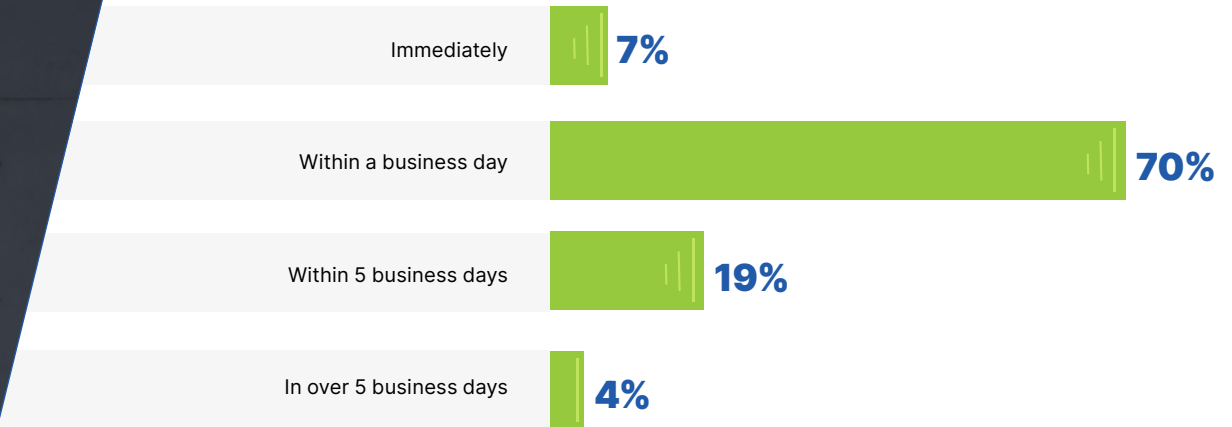
70 percent of businesses that refused to pay a ransom were able to recover their data within a day after ransomware was discovered,

and 18 percent we able to recover in up to five days. Out of businesses that did pay a ransom, 38 percent had their data decrypted immediately versus 46 percent that had it decrypted within a business day.

These recovery and decryption times may or may not fall within the risk tolerances for the business. Recovery time objectives (RTO) will vary based on the type of data that needs to be recovered or decrypted. For non-critical data and applications, a 24-hour recovery time may fall within the RTO for those systems. For mission-critical data, a 24-hour recovery may exceed the tolerable limit and help drive the cost of downtime higher than the cost of the ransomware payment itself.

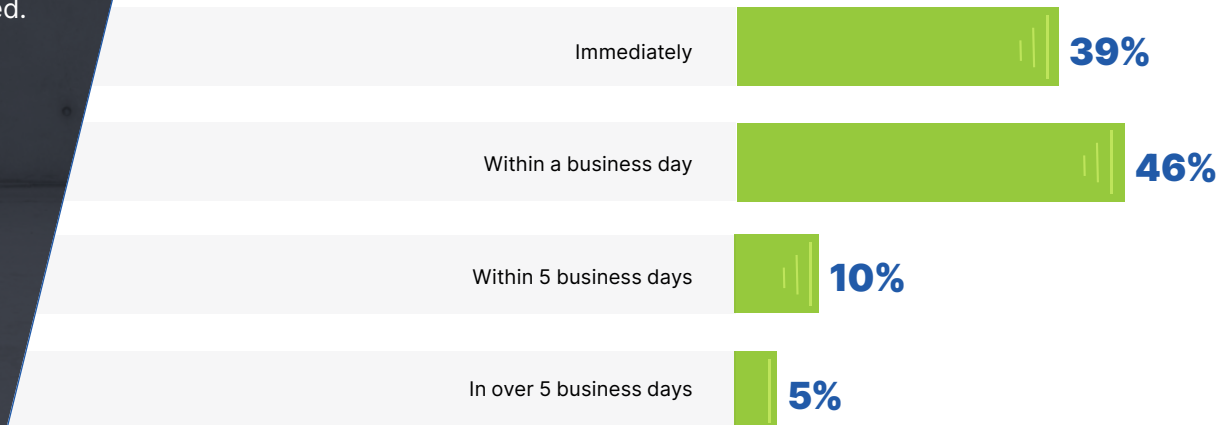
Data Recovery Time (No ransom paid)

For companies that were able to recover without paying a ransom, this graph shows how long it took to recover.



Data Encryption (Ransom paid)

For companies that paid a ransom, this graph shows how long it took to decrypt the data.



Brand and Reputation

Like ransomware, downtime also entails hidden costs. If either extends to external customers, the reputational harm and diminished brand equity can exceed both the ransomware payment and the operational costs associated with an attack.

Customer loyalty is increasingly fickle. According to one study, 61 percent of consumers switched some or all of their business from one brand to another in the last year, and 77 percent admitted they now retract their loyalty more quickly than they did three years ago.¹

Customer Loyalty is Fickle



61%

Consumers who switched some or all of their business to another brand in the last year



77%

Consumers who admit they now retract loyalty faster than they did three years ago

Brand and Reputational Harm



46%

Businesses that experienced ransomware whose clients were also impacted



38%

Businesses whose brand or reputation were harmed as a result of a ransomware attack

Brand valuation is an inexact science. Some methodologies combine the financial performance of the underlying products or services, the role the brand plays in purchase decisions, and the brand's competitive strength. Other methodologies focus on brand equity among the target customers, how much extra a buyer is willing to pay because of the brand, or how much additional market share it allows a brand to capture.²

In our study, 46 percent of businesses that experienced ransomware said their clients were also impacted, and 38 percent said the attack harmed their brand or reputation.

Considering the equity businesses have worked for and invested in for their brands, a one-in-three chance that ransomware further impacts their customers and, in turn, their reputation is a significant and potentially costly risk.

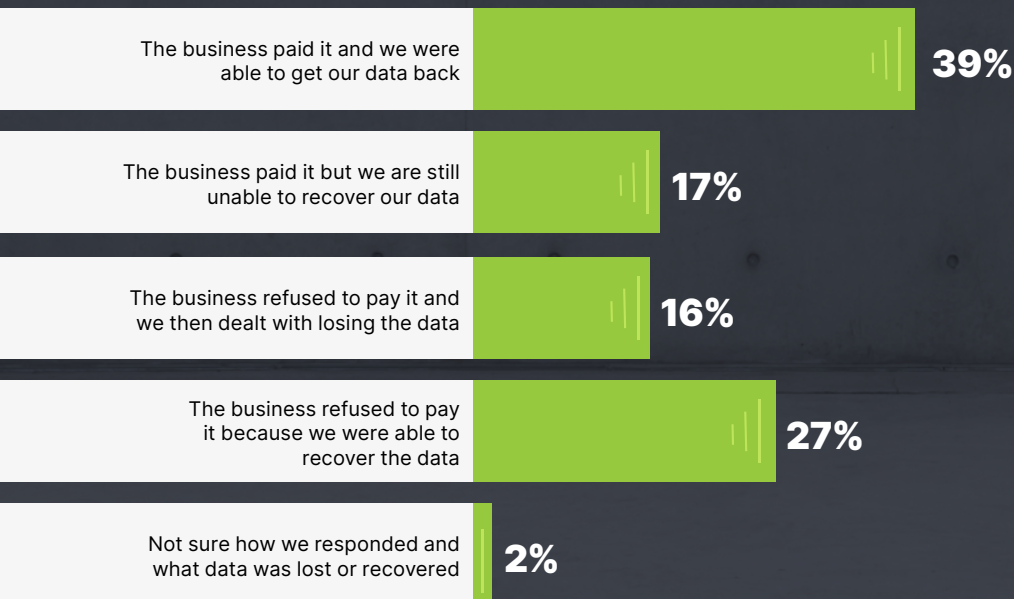
Regardless of their valuation, businesses spend a significant portion (in the neighborhood of seven to eight percent³) of their revenue on sales and marketing to raise awareness of their brands and be top-of-mind for their audience. An attack, or the resultant downtime, that extends to a customer or partner could undermine any equity a business has accumulated through ad spend, social media buys and other advertising and marketing channels.

The Cost of Ransom Payments

After the cost of remediation, downtime, lost opportunity and reputational harm are considered, what's left is the ransom payment itself. It's important to note that **the FBI does not support paying a ransom to cybercriminals**. According to the FBI, "Paying a ransom emboldens the adversary to target other organizations for profit, and provides for a lucrative environment for other criminals to become involved."⁴ The FBI goes on to say that paying a ransom does not guarantee an organization will regain access to their data. According to our research, **nearly 17 percent of businesses paid the ransom but were still not able to decrypt their data**.

Ransomware Victim Responses

This graph shows whether or not businesses paid the ransom and what the results were.



Average Cost of Data Loss

\$18K - \$35K

Average cost of
small-scale data loss
(about 100 data records)



\$5M - \$15.5M

Average cost of
large-scale data loss
(about 100M+ data records)

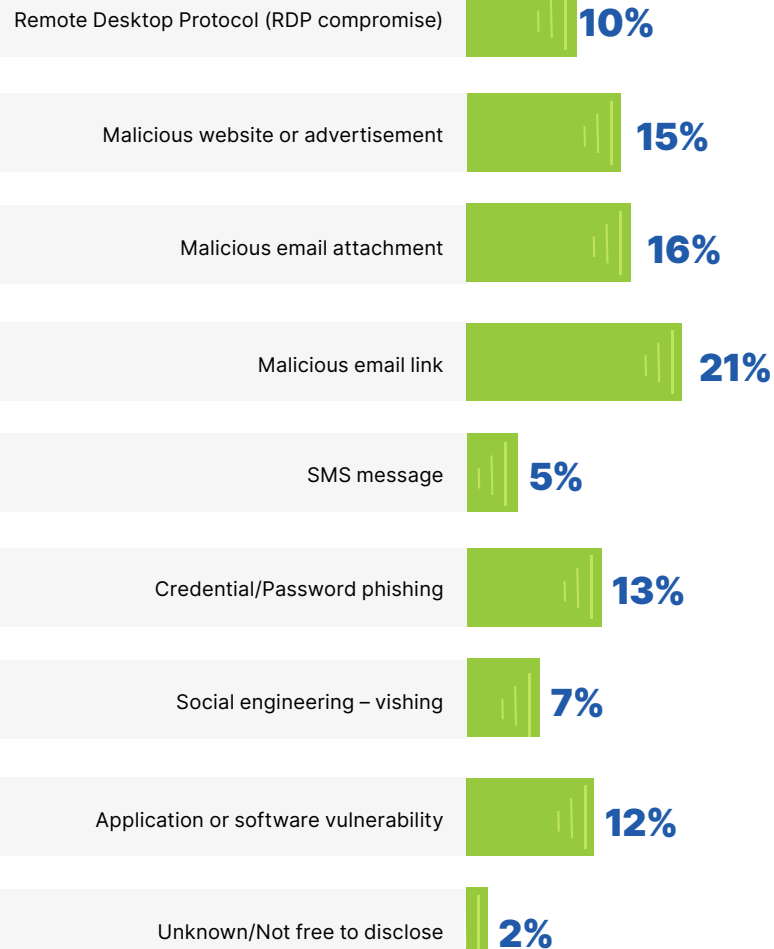


Another 16 percent refused to pay the ransom and accepted the consequences, presumably begrudgingly. Depending on the cost of the ransom payment, that may have been the preferred option. Ransom demands vary widely. About a quarter of businesses in our survey were asked to pay between \$11,000 and \$50,000, and almost 35 percent were asked to pay between \$51,000 and \$100,000. According to the Verizon Data Breach Investigations Report, small-scale data loss incidents (comprising about 100 data records) costs businesses between \$18,120 and \$35,730, while large-scale data loss (comprising 100 million or more data records) can cost between \$5 million and \$15.6 million.⁵

Defensive Measures

Ransomware Attack Vectors

This graph shows how ransomware was able to penetrate the system.



The best prepared businesses in our survey were the ones that refused to pay the ransom because they were able to recover their data. Over one-quarter of our respondents fell into this category, and nearly 80 percent of them were able to recover their data in a day or less.

The best way to be able to recover data is to back it up.

But deploying backup isn't the only defensive measure businesses should consider.

Gaps in protection must be closed to ensure the resilience of the entire system.

In our survey, the businesses that experienced ransomware had initiated several cybersecurity improvements to fortify the entire attack surface area and present a unified defense against cyberattacks. It starts by looking at the attack vectors that lead to a ransomware infection in the first place.

In our survey, the most common threat vectors were the employees themselves,

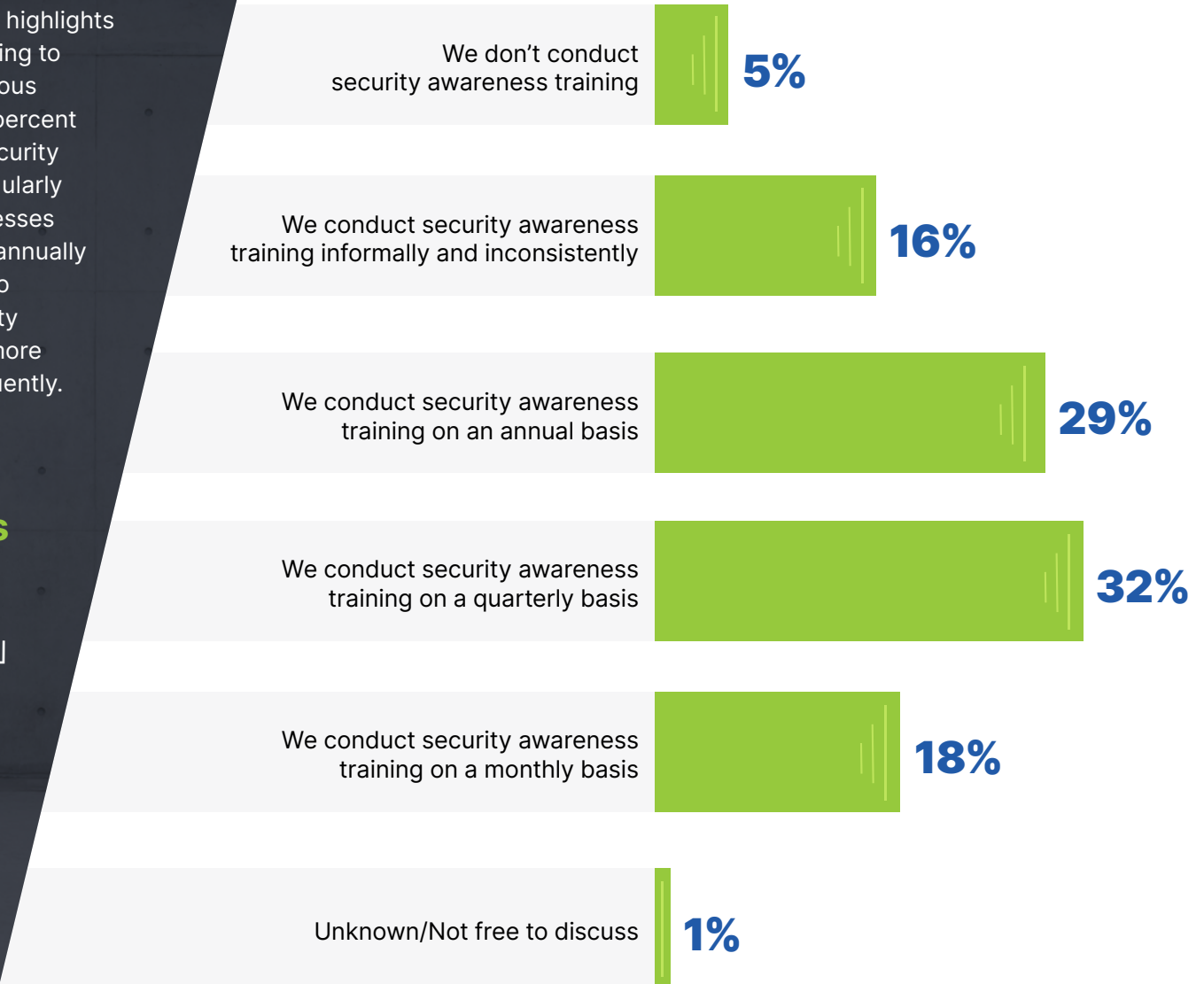
who had inadvertently visited malicious websites, clicked on malicious email links or attachments, or disclosed their login credentials. The other most common exploits were Remote Desktop Protocol (RDP) and software vulnerabilities.

A close examination of attack vectors highlights the need for security awareness training to educate users on how to spot suspicious activity. Our research shows that 20 percent of companies either don't conduct security awareness training or only do so irregularly or informally. More than half of businesses conduct security awareness training annually or quarterly, and only 17 percent do so monthly. Our results show that security training with phishing simulations is more effective when conducted more frequently.

After 12 sessions, click rates on malicious links and attachments dropped 50 percent.⁶

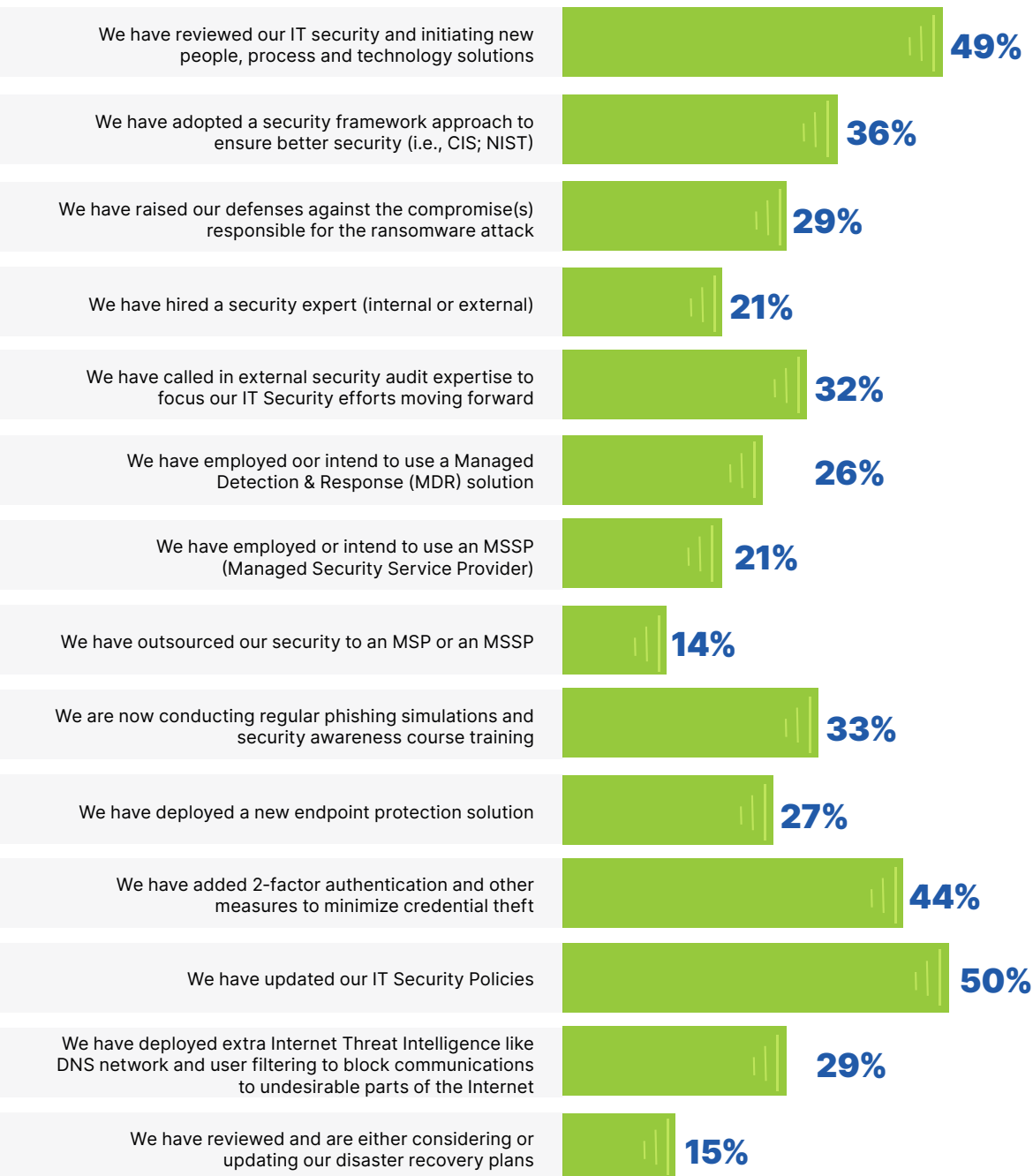
Security Awareness Training Practices

This graph shows whether businesses implement security awareness training and, if so, how often.



Post-Infection Security Practices

This graph shows changes that resulted from a successful ransomware attack.



Security awareness training is the most effective way to address the common threat vectors that lead to successful ransomware attacks.

But there are several other defensive measures businesses should consider, and it shouldn't take a ransomware attack to trigger their implementation. Some of the most important defensive measures businesses should consider include:

- Adopt a security framework such as the Center for Internet Security (CIS) or the National Institute of Standards and Technology (NIST)
- Enlist an expert to undertake an external security audit focusing on IT security
- Implement two-factor or multi-factor authentication (2FA, MFA) to minimize credential theft
- Deploy internet threat intelligence and DNS filtering to block malicious sites

After experiencing a ransomware infection, many of the businesses in our survey committed to these and other best practices to increase their defenses against future attacks.

Lessons Learned

Our research included businesses with annual revenues ranging from \$100,000 to \$1 billion, with most falling between \$1 million to \$500 million. Company size ranged from 1 to 10 employees up to more than 10,000.

Regardless of company size or annual revenue, the lessons learned after experiencing ransomware were universally shared,

as they are for any business that relies on data. In their own words, here's what business leaders and IT pros had to say about the costs and consequences of ransomware:

“ Cybercriminals are always adapting. Eventually, they'll find a way. Have everything backed up – cloud, hard drive – just routinely back stuff up. ”

“ Hire more people because the cost is totally worth it. ”

“ It is a nightmare. Do all you can to prevent ransomware. ”

“ We've learned a great deal from our ransomware incident and have taken steps to assure that it does not happen again. ”

“ It is crucial to develop an incident-response plan and use up-to-date antivirus and endpoint detection and response. ”

“ Weigh out options. Paying the ransom is not guaranteed to bring back data. Weigh out options. Paying the ransom is not guaranteed to bring back data. ”

More Information

Carbonite and Webroot offer a comprehensive portfolio of cyber resilience solutions to help businesses present a unified defensive front against ransomware attacks. From threat detection and remediation to disaster recovery and high availability, we provide all the tools necessary to prevent attacks, recover from adverse events and ensure high levels of uptime for almost any environment or business.

carbonite.com

webroot.com

¹ Accenture, Seeing Beyond the Loyalty Illusion, 2017

² Forbes, What Is A Brand Really Worth?, 2017

³ Small Business Administration, How to Set a Marketing Budget that Fits your Business Goals and Provides a High Return on Investment, 2013

⁴ Federal Bureau of Investigation, Ransomware, accessed March 2021

⁵ Verizon, Data Breach Investigations Report, 2019

⁶ Webroot Customer Campaigns, June 2020

CARBONITE® + WEBROOT®

Backup ◊ Train ◊ Block ◊ Protect ◊ Restore

opentext Business Solutions