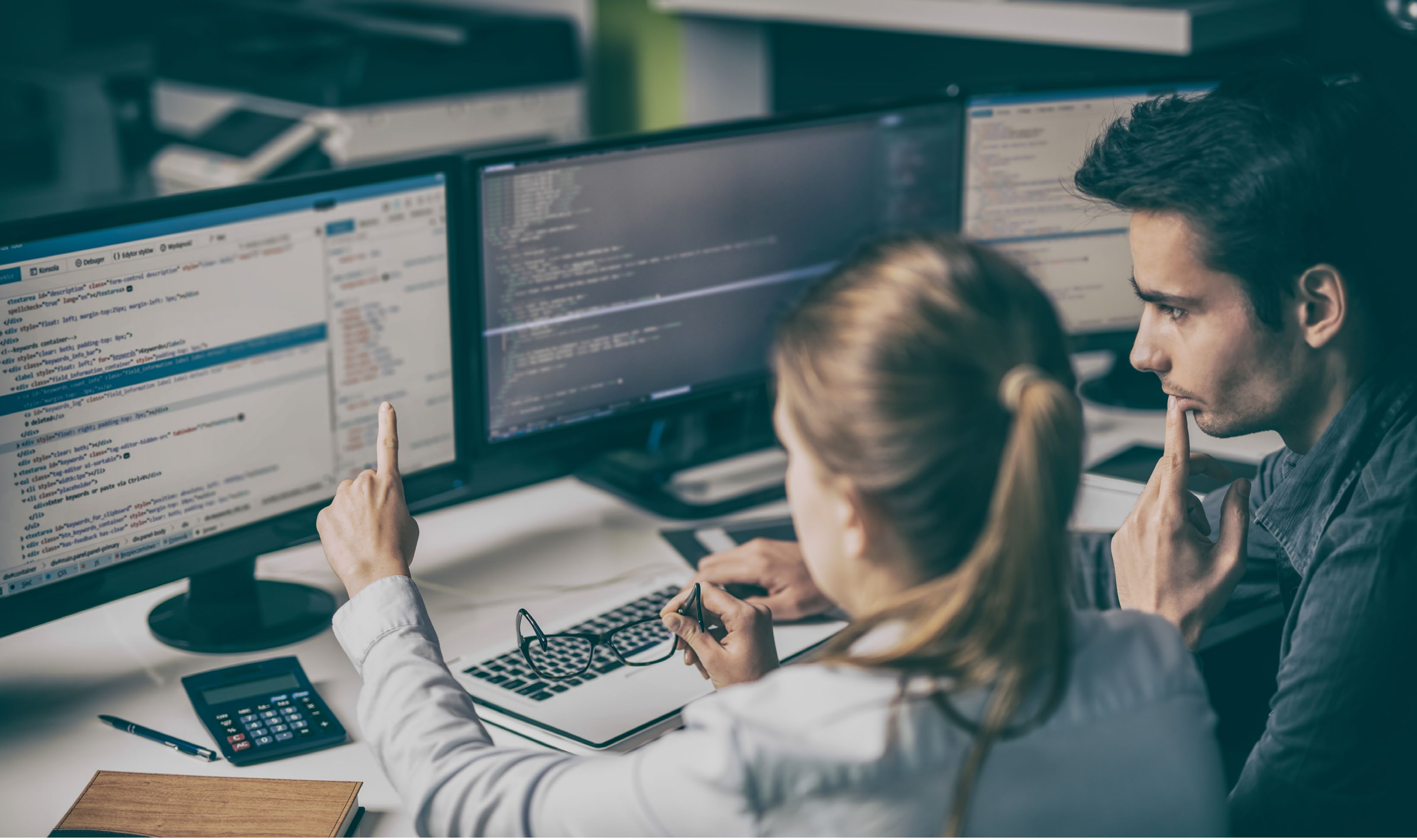


Responding to Cyberattacks

Omnipresent Problem Puts Most Organizations at
Risk of Complete Shutdown

VIPRE®

Responding to Cyberattacks

Omnipresent Problem Puts Most Organizations at Risk of Complete Shutdown

Introduction

New research by VIPRE Security reveals some serious gaps in the ability of organizations to defend against and respond to cyberattacks. The gaps threaten their survival in some cases, causing most IT managers (66%) to live in fear that a cyberattack would cause their business to shut down temporarily (44%) or even permanently (22%).

The research shows IT managers understand the importance of effective cybersecurity but responding to an attack is a problem, with 54% of IT managers relying on manual processes for remediation. Even worse, 55% do not have an incident response plan (IRT), which would hinder their ability to react in the first place. On any given day, fewer than half (41%) have access to a web-based s ecurity dashboard, which means 59% lack anytime/anywhere access to security solutions. Add to that the fact that only a quarter of study participants apply software patches on at least a weekly basis, and you have the makings of a potential disaster should an attack occur.

It isn't all negative, though. VIPRE Security's "Managing Cyberattacks" survey found that IT managers feel they are well-served with their endpoint security. And in what is unquestionably an encouraging sign, a full 80% said their organizations offer security training to employees at least quarterly.

MSPs Share Shutdown Fears

A separate, parallel study of 250 U.S.-based MSPs found that MSPs, by and large, are better prepared than IT managers to handle cyberattacks, which comes as no surprise. They can react faster to an attack, thanks to greater remote access to security tools, and they patch systems more frequently. And while only 45% of IT managers have a documented IRT, 75% of MSPs have one.

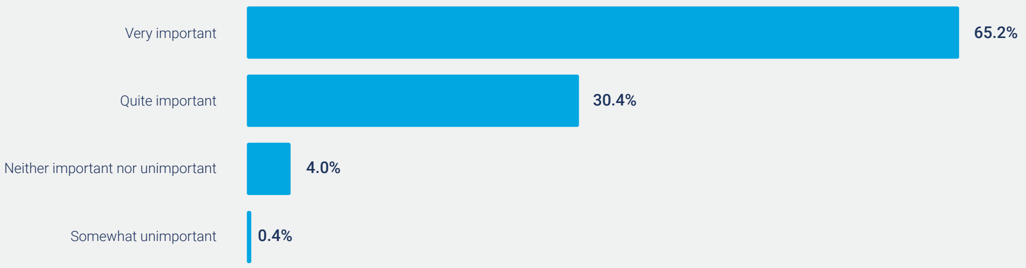
Nevertheless, they fear a business shutdown as a result of malware attacks almost as much as their in-house counterparts. Almost two thirds (62%) said a malware attack that compromises their clients' systems and data would force a shutdown of their business. Of those, 44% estimated the shutdown would last a day but 18% said it would be permanent. On the bright side, 33% said an incident would not impact their business.

Key Findings

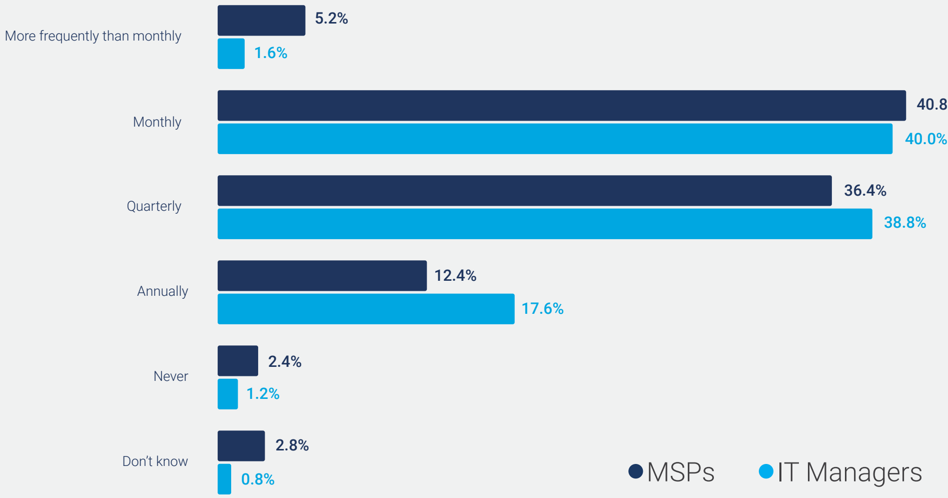
The "Managing Cyberattacks" survey polled 250 managers at U.S. firms of 50 to 1,500 employees between August 31, 2017 to September 15, 2017. Here are the key findings from the study:

- 96% of IT managers understand the importance of protecting their businesses from the latest threats.
- 66% said their business could close following an attack.
    - 44% said it would close for a day.
    - 22% said it would go out of business.
- 45% don't have a documented Incident Response Plan (IRT).
- Only 25% of companies apply patches on at least a weekly basis.
- 55% rely on manual processes to respond to an attack.
- Only 41% have access to an online security dashboard.
- 80% conduct cybersecurity training at least quarterly.
- 73% have high confidence in their defenses.

How important is the ability to quickly assess that devices are connecting, updating and working as expected so that your business is protected at all times against the latest threats?



Typically, how frequently do you conduct cyber threat awareness training for your clients?

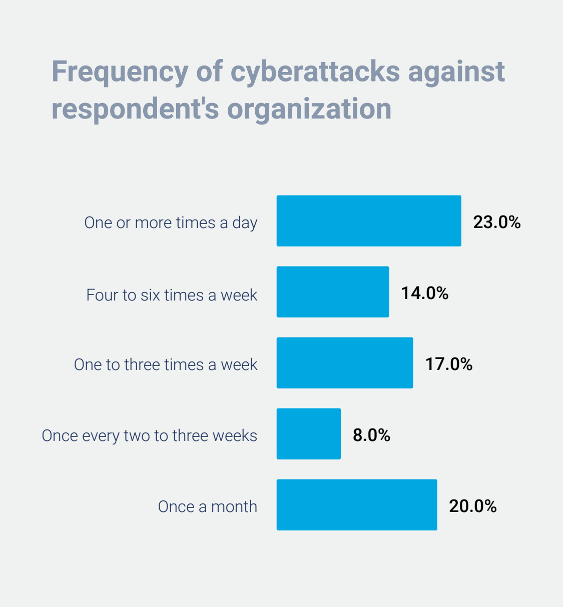


Awareness and Remediation

If true recognition is the first step to solving a problem, IT managers at least have gotten that far. When asked about the level of importance in their ability to quickly assess that devices are connecting, updating and working as expected to protect their businesses against the latest threats, 96% described it as either "very" or "quite" important. So, clearly, IT managers recognize the need to be ready and responsive.

Another positive finding centered on the frequency of cyberattacks against their organizations. Here is a partial breakdown:

On the surface, this looks like a lot, but that's the reality of doing business in an increasingly connected world. More important is the fact that IT managers know they are being targeted and keeping track of the frequency of attempts. The more information you have about threats, and the risks they pose to your business, the better you can prepare to deal with them.


Frequency of cyberattacks against respondent's organization

Most respondents expressed confidence in their ability "to see the scope, impact and pattern of a specific threat," with only 16% saying they have difficulties in that area. More than half (57%) said it was "fairly" or "very" easy, while 26% said it was neither easy nor difficult.

When it comes to remediation, most respondents revealed no major problems with the ability of their IT resources to report on attack remediation when it comes to detection, quarantine, cleaning and deletion. Here's a breakdown of combined "fairly" and "very" difficult answers:

Detection	15%
Quarantine	15%
Cleaning	14%
Deletion	16%

There is room for improvement, of course, though a comfortable majority is happy with their resources in these areas.

Management Focus

Another encouraging finding about threat awareness came in a response to a question about how frequently top executives ask IT managers about protection from cyberattacks. Compared to a year ago, business owners, presidents and top executives are asking about defenses more frequently:

The uptick in daily inquiries, as well as the overall increased frequency, denotes a keener focus on cyber threats. Most likely, the massive WannaCry and Petya ransomware attacks in the spring of 2017 sharpened their interest. The Equifax breach, potentially affecting 143 million Americans, was disclosed after the survey was conducted, so it had no impact on these results, though it's reasonable to conclude it likely would have.

Today	1 Year ago
14% daily	9% daily
24% weekly	23% weekly
32% monthly	33% monthly
19% quarterly	21% quarterly
10% annually or less	12% annually or less

User Training

Asked about security training, most IT managers indicated it is happening with some frequency. A mere 1% said they don't do it while another 18% said training is conducted annually. But 40% said they do training monthly and 39% quarterly.

Frequent user training is a critical component of any security strategy, considering most security incidents result from user actions. Phishing, which preys on user curiosity and fear, is especially effective and accounts for least 90 percent of ransomware attacks.

Response Readiness

Tempering the survey's results regarding threat awareness are some troubling findings regarding businesses' level of readiness for a malware attack. In some areas, it is far from ideal. Consider that more than half of respondents (55%) said they have a documented IRT. If they suffer an attack – an increasingly probable occurrence – they could be scrambling to figure out what steps to take and in what sequence.

That alone is problematic because you can't afford to be indecisive while a malware infection is spreading across your network. But the lack of preparedness doesn't stop there for many businesses: 55% of IT managers rely on manual processes to address an attack. That means fewer than half can access their security solutions remotely. That slows your ability to react, especially if you're away from the office when it occurs.

MSPs Not Always Remote

Interestingly, remote access to security solutions is only available to 67% of respondents in the MSP survey. That the number is higher than for IT managers makes sense – after all, remote management is what MSPs do. But it should be higher. If MSPs are to maximize their security response readiness, they should have anytime/anywhere access to security solutions to best protect their clients.

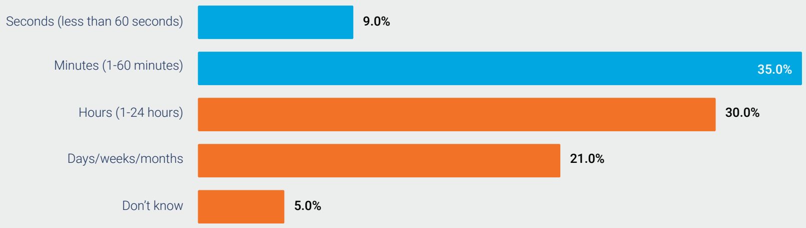
Speed Limits

When it comes to addressing an attack, there's clearly plenty of room for improvement. Just getting information on identifying threats, remediation and potential business impact of cyberattacks is slower than it should be:

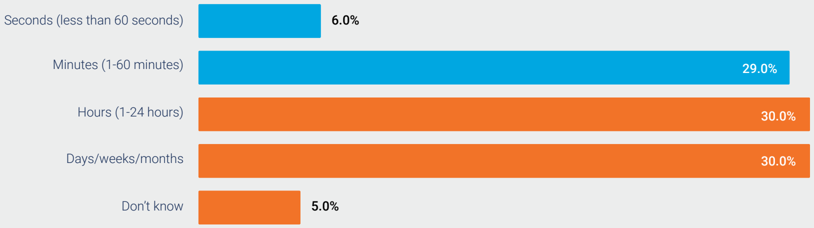
More than half of respondents would need multiple hours or days to compile reports on remediation and the business impact of an attack. This is too slow at a time when it takes mere seconds for some types of malware to spread across networks and hours to jump borders, affecting hundreds of thousands of users in multiple countries. Such was the case with WannaCry.

Even demonstrating protection from cyberattacks is in place is a complicated task for most IT managers. If asked by upper management for information about security, fewer than half (41%) have the option of showing them an online dashboard. Even for those with access to one, it isn't a straightforward task since 68% said they would need to "generate several security reports." The situation is even more onerous for the 47% who said they have to manually collect information from various systems to run reports.

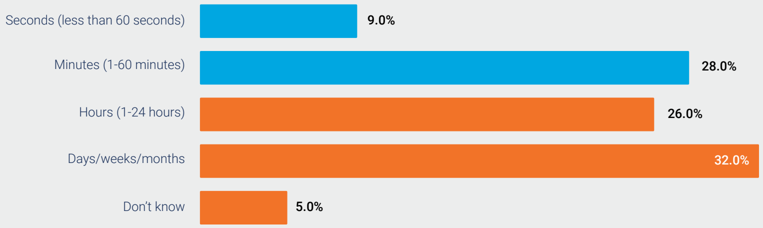
Speed Limits – Identifying Threats



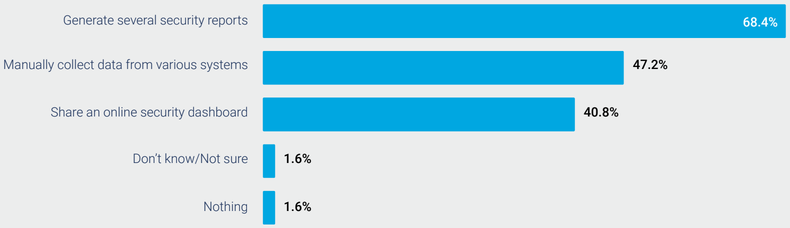
Speed Limits – Remediation



Speed Limits – Business Impact



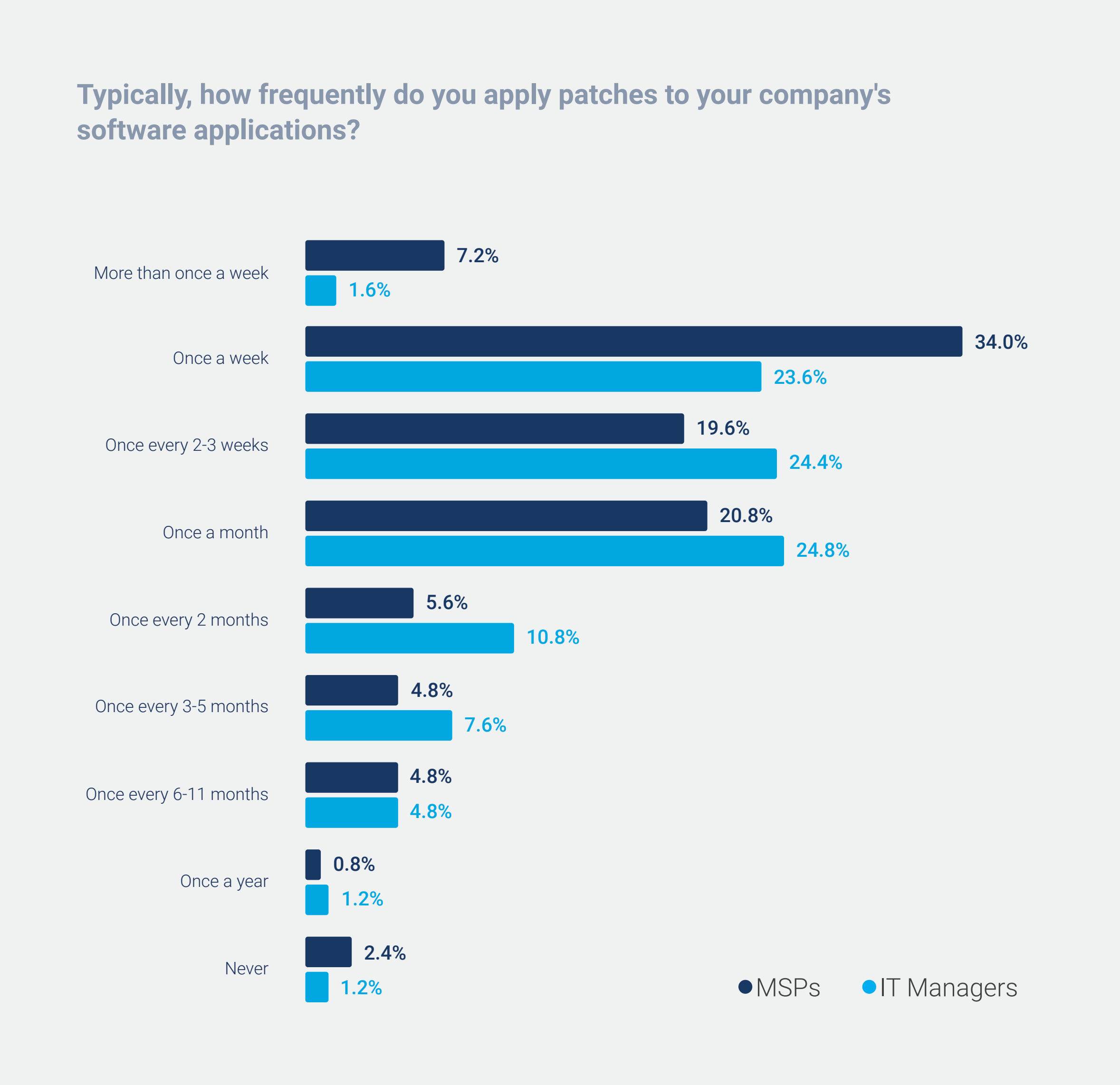
What do you/your team do to show upper management/owner/ president that the company is protected from cyberattacks/threats?



Patchy Practices

Another area of security that needs improvement is patch management. Asked how frequently they apply software patches, barely 2% said they do it more than once a week. Only 24% of respondents said they do it weekly, while another 24% said every two to three weeks. Another 25% said they apply patches monthly.

Timely patch management is critical to protecting business data because hackers often exploit vulnerabilities in popular applications and systems. Diligent patch management minimizes exposure to ransomware and other types of malware.



High Confidence

Despite the gaps in security readiness and access to advanced tools, IT managers expressed a high degree of confidence in their cyber defenses. On a scale of 1 to 10, 73% rated their confidence 8 or higher. The number is down from 89% of IT managers who, in the spring of 2017, expressed confidence in their ability to defend against malware. It's a significant dip, possibly related to recent high-profile malware attacks, but most likely has to do with the fact that, in the spring, it was worded differently.

In any case, respondents indicated they are happy with their endpoint protection, with only 14% saying they find it difficult to protect against threats. Those who outsource security also expressed high levels of satisfaction with their vendors. Here's the breakdown for "fairly" and "very" satisfied responses:

Prevention	75%
Management	72%
Communication	74%

Working with MSPs

The above numbers are strong enough to make a case for outsourcing security to service providers, especially those with remote capabilities. Further proof is in the results from the parallel MSP survey, which showed MSPs have a better handle on security, overall, than in-house IT managers. Here are some critical areas in which MSPs scored higher:

MSPs also see a higher frequency of malware attacks on their clients (32% vs. 19%) multiple times a day. This likely is a result of access to better tools and being more attuned to what to look for. Taken together, all these numbers help explain why MSPs also scored higher in the confidence meter regarding cyber defenses (80% rated 8 or higher vs. 73% of IT managers).

Patch Management Timeliness	41% at least weekly vs. 26% of IT managers
Respond to an Attack Remotely	68% vs. 43%
Use Online Dashboard	56% vs. 41%
Documented Response Plan	74% vs. 45%

Conclusion

While IT managers have a handle on critical security aspects such as endpoint protection and user training, their overall ability to respond to threats is less than ideal. Even though IT managers understand compromise risks, it takes them too long to create security reports because they use manual processes. Patch management practices leave much to be desired, and the lack of a documented IRT at most organizations is troubling. These gaps slow down the ability to respond to threats and attacks, making organizations more vulnerable than they should be.

Recommendations

Based on the study's findings, here are five recommendations for IT managers:

- Develop and implement a strategy to apply patches as quickly as possible when issued.
- Make the case to management to invest in security platforms with anytime/anywhere access for quick response to attacks.
- Persuade management to invest in security tools with easy-to-use, web-based dashboards, automation and rapid report compilation.
- Develop, document and implement an Incident Response Plan.
- Consider outsourcing security to an MSP specializing in data and network protection.

About VIPRE

VIPRE is the highest-rated, award-winning internet security product for businesses and home users. It is powered by the world's most sophisticated security technologies, protecting millions of users from today's top online threats, including ransomware, zero-days and other malware that easily evades traditional antivirus. Backed by cutting-edge machine learning, one of the world's largest threat intelligence clouds and real-time behavior monitoring, VIPRE deploys in minutes to deliver unmatched protection without slowing down PCs. All VIPRE customers and partners receive free U.S.-based technical support.

To learn more, visit **www.VIPRE.com** and **try it FREE for 30 days**.

Top-Rated Endpoint Security

AV comparatives ADVANCED+ -REAL WORLD- PROTECTION TEST DEC 2016
vb 100 VIRUS virusbtn.com
ICSA labs CERTIFIED
Excellence in Information Security Testing Award
AV TEST av-test.org 06/2016 CERTIFIED WINDOWS
2015 Computing Security Awards
WINNER
Anti Malware Solution of the Year
SC MAGAZINE ¾