VIPRE® AntivirusBusiness

Network Security Report: The State of Network Security in Schools

Managing tight budgets. Complying with regulatory requirements. Supporting Internet-based learning technologies. There are many challenges facing schools when it comes to managing their networks to ensure they deliver required performance yet remain secure and protected. But while these factors change the way K-12 schools operate, malware continues to be a significant risk and securing the school network continues to be a challenge.

Contents

Introduction

ThreatTrack Security, the developer of VIPRE Business Premium, conducted a survey to gain a better understanding of the specific network security challenges IT administrators in K-12 schools are facing today. The survey found that, by and large, schools have been able to achieve a relatively good level of network security on school-owned and school-managed systems – that is, on elements over which network and security administrators have a degree of control. But changing dynamics are shifting schools' network security concerns. Today's challenges are a result of two key factors:

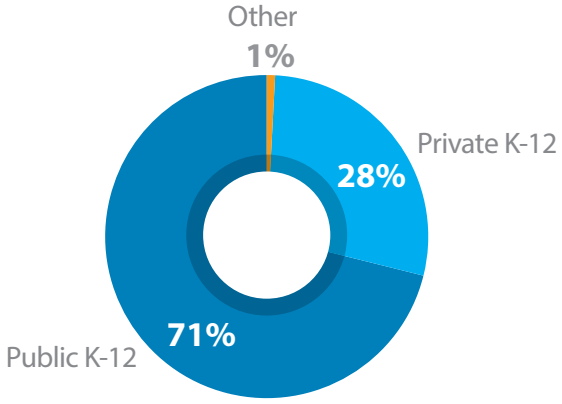
- **The explosion in personal, storage and mobile devices that students, faculty and employees use to access the school network.** Many of these devices do not have adequate – or any – antivirus software installed on them, opening up vulnerabilities on the schools' systems when they access the network.
- **The behavior of students, faculty and employees on the network.** As users continue to click, download and connect their way to malware infections, they continue to represent a significant risk to network security.

Methodology

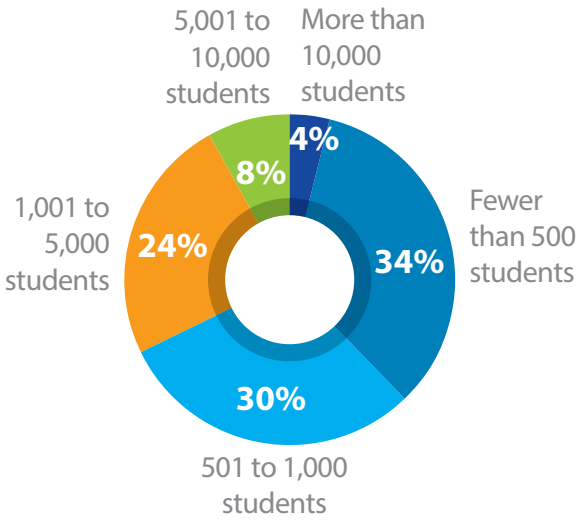
ThreatTrack Security conducted a web-based survey to understand the network security landscape in K-12 schools in the United States. This survey targeted individuals responsible for IT and network security at public and private K-12 schools. Respondents who did not fit these criteria were excluded. The survey gathered 202 qualified responses.

Respondent demographics

According to the U.S. Census Bureau, 75 percent of K-12 schools in the U.S. are public. The survey respondents mirror this with 71 percent coming from public schools and 28 percent from private schools. The remaining 1 percent of respondents did not indicate whether their institutions were public or private.



Qualified respondents by institution type



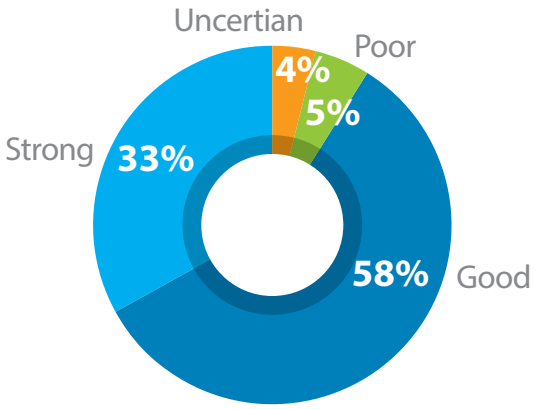
Qualified respondents by student body size

Respondents were relatively evenly distributed based on student body size with, not surprisingly, the fewest number of respondents representing very large schools (more than 10,000 students).

Key findings and analyses

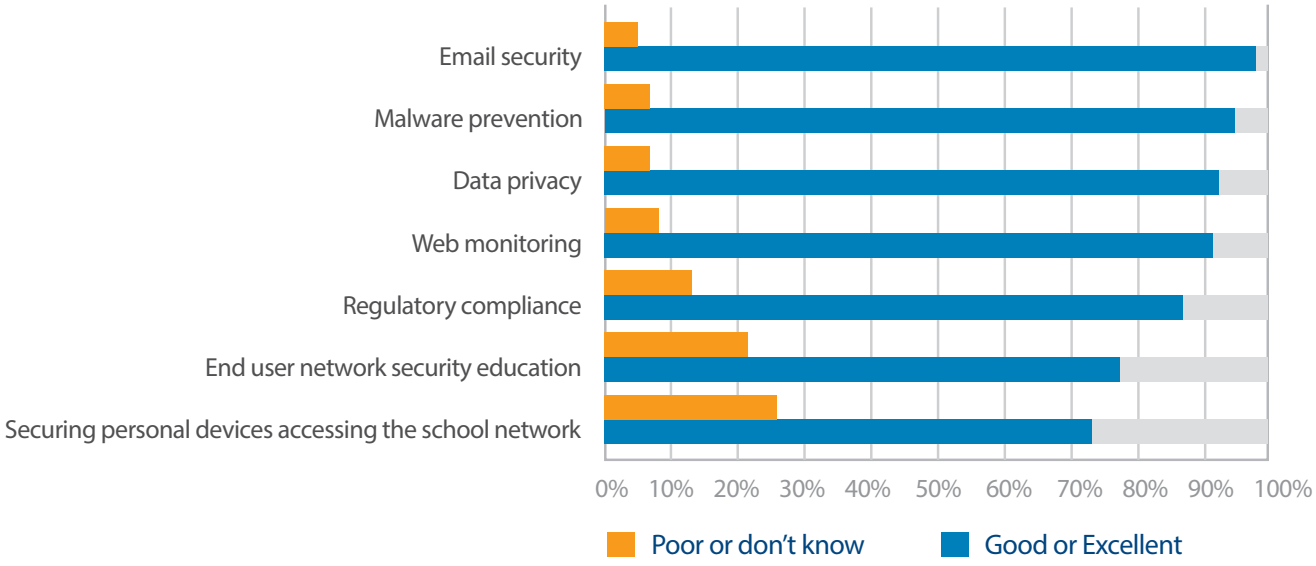
IT security readiness

In general, school network and security administrators are positive about their general IT security readiness. The vast majority of respondents – 91 percent – rate their IT security readiness as good ("we feel we have adequate security solutions and policies in place to defend against the most common threats such as malware and unauthorized network access") or strong ("we have a comprehensive strategy and policies in place to defend against common threats like malware and unauthorized network access, as well as more complex and advanced threats").



General security readiness rating

But a more detailed look by category shows that schools have higher confidence in their IT security readiness when it comes to those categories over which network administrators have the most control – and for which they have access to relatively mature technologies to manage. The four categories for which the vast majority of respondents rated their readiness as "good" or "excellent" are email security (96 percent), malware prevention (94 percent), data privacy (94 percent) and web monitoring (91 percent). The two categories with the highest ratings of "poor" or "don't know" were securing personal devices accessing the school network (27 percent) and end user network security education (21 percent). These two categories represent factors over which network and security administrators have less control; end user network security education is a challenge that cannot be adequately addressed by technology, and securing personal devices accessing the school network can be addressed by technology but that technology is often expensive and difficult to administer and manage.



IT and network security readiness by category

Changing security dynamics

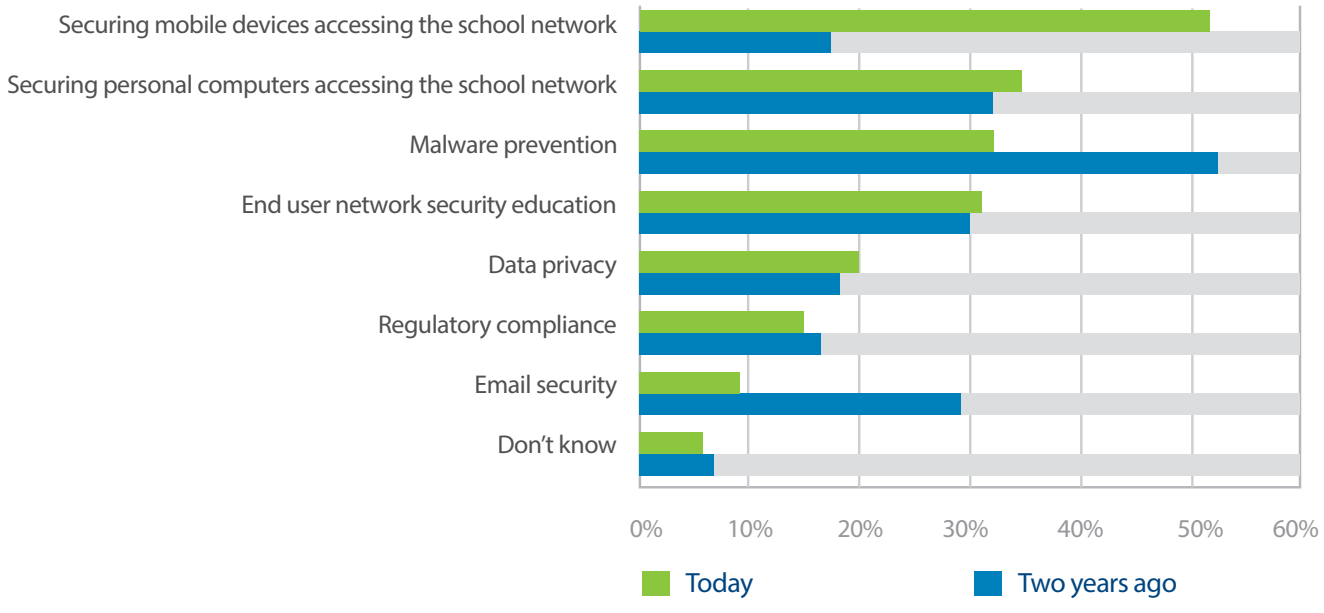
The survey looked at how network security has changed in schools over the past two years and, again, an overall pattern emerged that shows that the concerns and weaknesses that have seen the biggest decline over the past two years are areas that network and security administrators can manage with relatively mature technologies:

- Email security saw a 21 percent decline in the number of respondents citing it as a key concern.
- Malware prevention saw an 18 percent decline in the number of respondents citing it as a key concern.
- Inadequate virus protection (failed detections, false positives, management issues, etc.) saw a 21 percent decline in the number of respondents citing it as a key weakness.

Similarly, the concerns and weaknesses that are on the increase are those areas over which network and security administrators have less control:

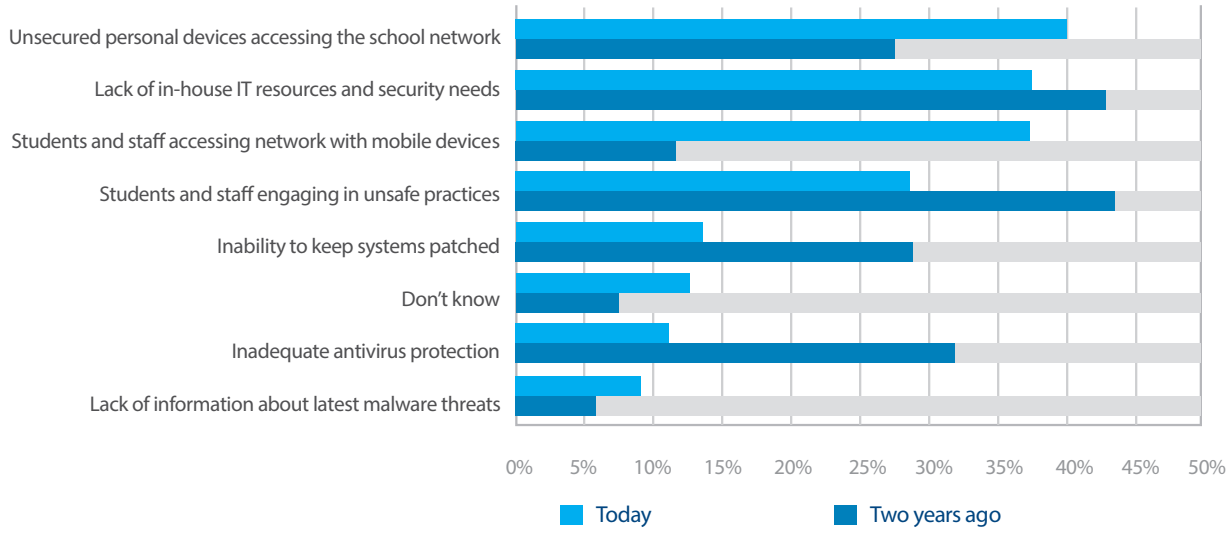
- Securing mobile devices accessing the school network saw a 34 percent increase in respondents citing it as a key concern.
- Students, faculty and employees accessing the network with mobile devices saw a 26 percent increase in respondents citing it as a key weakness.

Two years ago, half the respondents (51 percent) cited malware prevention as one of their top concerns. Other major concerns two years ago were securing personal computers accessing the school network (34 percent), email security (29 percent) and end user network security education (30 percent). The factors that caused the lowest rates of concern two years ago were regulatory compliance (15 percent), securing mobile devices accessing the school network (18 percent) and data privacy (17 percent). Today, the biggest concern is securing mobile devices accessing the school network, cited by half the respondents (51 percent), up significantly from only 18 percent two years ago. Concerns about securing personal computers accessing the school network (34 percent) and end user network security education (31 percent) remained about the same. Only 9 percent of respondents now cite email security as a concern, representing the biggest decline in the past two years. While malware prevention is no longer in the number one spot, it is still the top concern for one-third (33 percent) of the respondents.



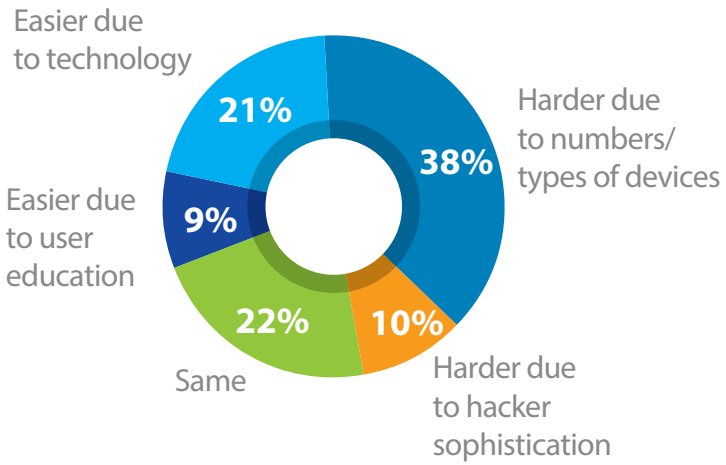
Top IT network security concerns

IT and network security weaknesses have also changed in the past two years. Two years ago, almost half of the respondents cited poorly trained students, faculty and employees engaging in unsafe Internet and email practices (43 percent) and lack of in-house resources and personnel to adequately manage security priorities (43 percent) as the top weaknesses. Other major weaknesses two years ago were inadequate antivirus protection such as failed detections, false positives, management issues, etc. (32 percent), inability to keep systems up-to-date with the latest patches, signatures and definitions (29 percent) and students, faculty and employees accessing the network with personal laptops and portable storage devices that lack adequate antivirus protection (28 percent). Lack of information about the latest malware and exploits is not seen as a critical weakness and was cited by only 6 percent of respondents as a top weakness two years ago, although that number grew slightly to 10 percent today. Today, students, faculty and employees accessing the network with personal laptops and portable storage devices that lack adequate antivirus protection has grown to be the top weakness (40 percent) and is joined by students, faculty and employees accessing the network with mobile devices (38 percent). Lack of in-house resources and personnel to adequately manage security priorities continues to be a weakness, though it is down slightly to 38 percent from 43 percent two years ago. Only 11 percent of respondents now cite inadequate antivirus protection (failed detections, false positives, management issues, etc.) as a top weakness today.

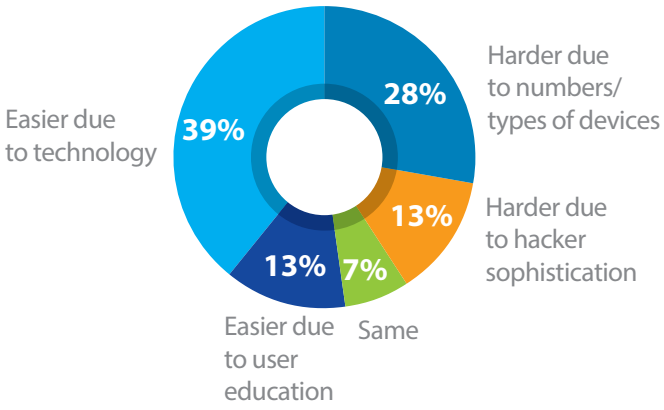


Top IT and network security weaknesses

When asked whether securing the network is easier, more difficult or neither easier nor more difficult than in the past, results were mixed. Almost half (48 percent) of the respondents stated that securing the network is more difficult today. The majority (80 percent) of those who find it more difficult cite the number and types of devices accessing the network as the primary reason. One-third (30 percent) of respondents, however, state that it is now easier to secure the network. The majority of this group (71 percent) says that securing the network has become easier as technology has evolved and delivers increasingly comprehensive protection.



Change in ability to secure the network

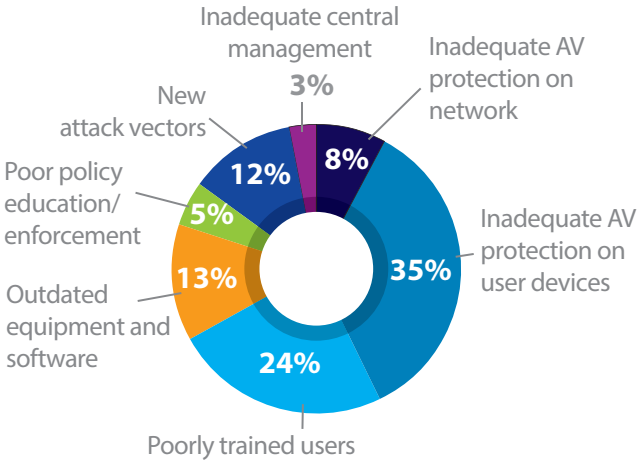


Change in ability to secure the network for respondents who rate their security readiness as strong

Interestingly, when looking at just the respondents who rated their general security readiness as strong ("we have a comprehensive strategy and policies in place to defend against common threats like malware and unauthorized network access, as well as more complex and advanced threats"), which was 33 percent of the total respondents, the picture looks very different. More than half (52 percent) say it is easier to secure the network than in the past, with the majority (75 percent) citing technology as the reason. Less than half of this group (41 percent) say it is more difficult to secure the network than in the past, with the majority (68 percent) citing the numbers and types of devices as the reason.

Malware risk factors

Malware continues to pose significant security risks to networks and respondents were asked to indicate what leaves their network most exposed to infection. The top risk, selected by more than one-third of respondents (35 percent), was students, faculty and employees accessing the network with PCs and portable storage devices that lack adequate antivirus protection. The second most prevalent risk, selected by one-quarter of respondents (24 percent), was poorly trained faculty and employees demonstrating unsafe Internet- and email-use practices. Again, this echoes the sentiments that the biggest network security concerns and weaknesses are in areas over which IT staff has less control: users and their personal devices.



Biggest exposure to malware infection

Despite the high level of concern with inadequate antivirus protection on user devices accessing the network, more than two-thirds of respondents (68 percent) do not offer free or discounted antivirus software to their user populations.

Security challenges unique to schools

The survey included an open-ended question that asked respondents to indicate, as an educational institution, what unique security challenges they face when protecting the network. When categorizing the responses, the most prevalent by far – one-third (33 percent) of responses – described the challenges of securing a wide range of mobile and other devices brought in by students, faculty and other users.

Conclusion

Survey results indicate that while network and security administrators at K-12 schools are confident in their overall network security readiness, they still face significant challenges. Today's challenges require schools to look for ways to control sources of vulnerability that are inherently difficult to control – end users and their devices. A clear

understanding of these challenges will enable school IT administrators, vendors, consultants and other industry stakeholders to focus on the critical issues and develop technologies and best practices to address them. In two years, it's unlikely that a repeat study would report that K-12 schools have solved all their security challenges – what is more likely is that we'll see new challenges emerge that reflect the ever-evolving landscape of technology and malware.

About VIPRE® Business Premium™

VIPRE Business Premium is the small-footprint antivirus software that enables IT administrators in K-12 schools to secure all devices that access their network with Mobile Device Management for iPhones, iPads and Android smartphones and tablets, built-in Mac support, removable media scanning and unprotected computer identification. In addition, VIPRE includes integrated patch management, a groundbreaking feature that eliminates the number one cause of PC infections and attacks: unpatched machines.

Visit **www.ThreatTrackSecurity.com/VIPRE** to evaluate VIPRE Business Premium free for 30 days.

Jan 2013