Security in a Dangerous Time:

WHERE EXECUTIVES FOCUS THEIR ATTENTION

CSO
Strategic Marketing Services

SPONSORED BY:
FORTINET

IT security executives around the world are acutely aware of the many threats they face. In fact, a recent IDG Research Services survey shows that IT security professionals across the U.S., UK, and Hong Kong/Singapore are even more concerned today about the same issues that worried them a year ago. This white paper shares insights from the survey, including what security professionals consider to be their top priorities, what they are most concerned about protecting, and how they prefer to address threats.

Insight 1: The top security concerns of 2014 are even more urgent now.

In 2015, the top three IT security priorities worldwide remain unchanged, with protection from/detection of advanced persistent threats (APTs) at No. 1, followed closely by next-generation firewalls, and mobile device management. Clearly, last year's response was not a knee-jerk reaction but a serious commitment to addressing these needs.

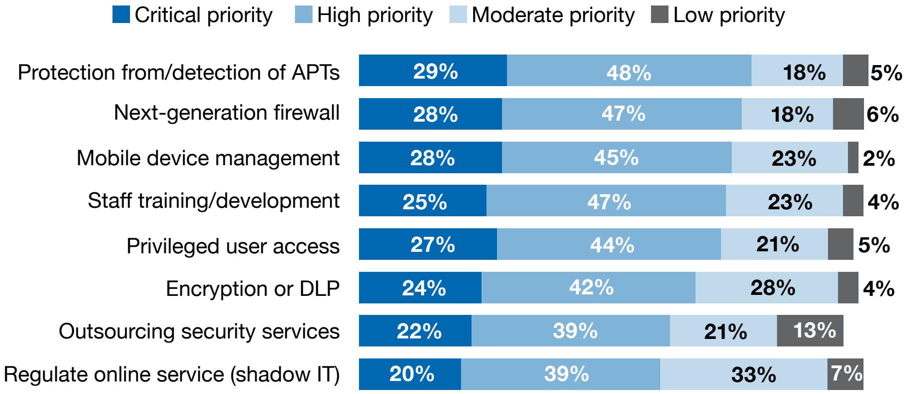
Further, these top priorities rose in importance from last year and were cited by 3 in 4 executives as either high or critical priorities for 2015. It isn't just that the threats themselves have grown; it's also that companies are constantly aware of threats in a way they may not have been even a year ago.

Outsourcing security services shows the greatest increase from last year—leaping 14% to a total of 61% of respondents who cite this as a high or critical priority in 2015. While the survey did not ask respondents for the reasons behind their rankings, it's highly likely that a steady stream of negative security events is forcing respondents to acknowledge that they lack the internal expertise to address newer and more sophisticated threats.

Insight 2: Companies are most concerned about safeguarding customer information and business operations.

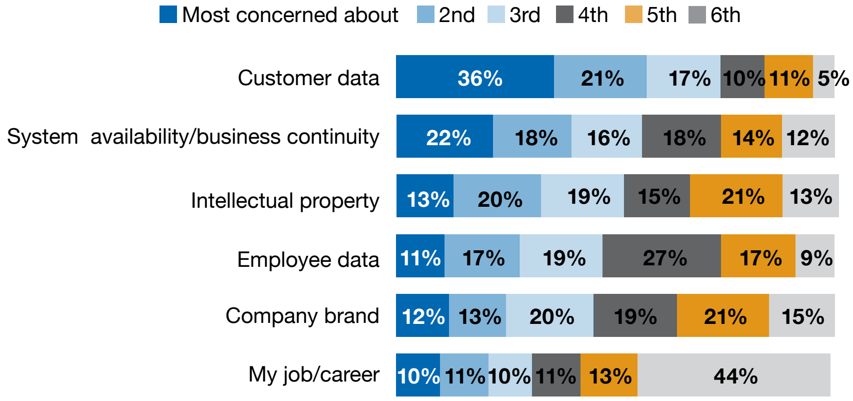
Publicity is also the most probable reason why the survey finds that the main security goal by far is to protect customer data. The majority of security breaches and headlines over the last few years have focused on cybercriminals' intensive efforts to capture personally identifiable information (PII) like credit card and Social Security numbers—and unsurprisingly, these breaches are clearly top-of-mind for high-level

Priority of IT Security Initiatives in 2015



SOURCE: IDG Research Services, March 2015

Most Concerned About Protecting from Cyber Criminals



SOURCE: IDG Research Services, March 2015

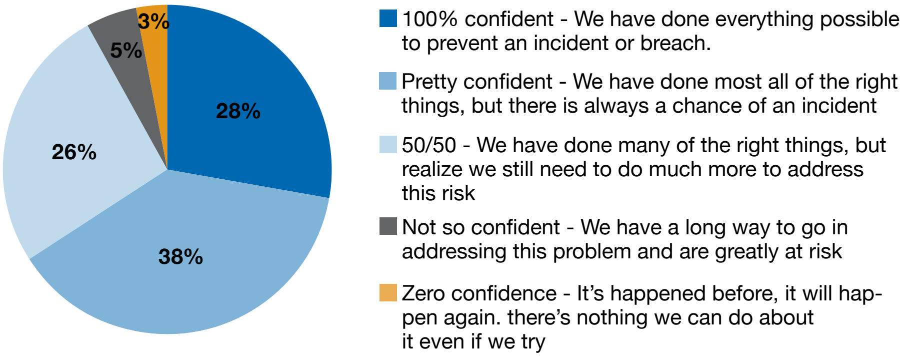
IT decision makers. As shown above, protecting customer data from cybercriminals is the most common primary concern stated by executives as well as most cited among the top three concerns.

By comparison, respondents overall view protecting employee data, corporate intellectual property, and the company brand as significantly less important. This could be interpreted as confidence that other problems are manageable as long as the organization focuses on maintaining customer satisfaction and uninterrupted business operations. Or, less charitably, it could be a result of headline rubber-necking. Regardless, the low concern placed on protecting intellectual property—a strategic asset of any company—is worrisome, says David Finger, director of product marketing for Fortinet, a leading provider of network security solutions.

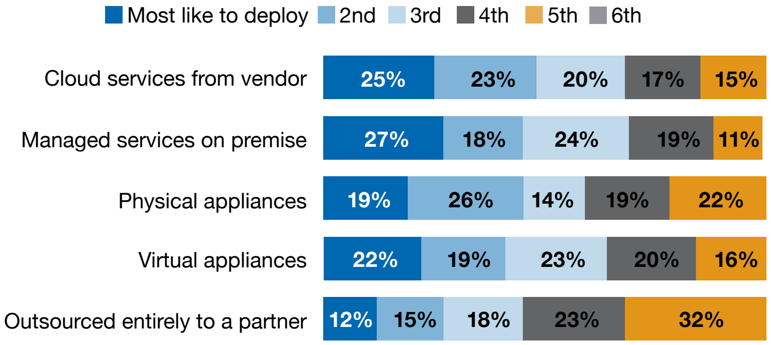
Insight 3: Companies overstate their confidence in current security measures.

People may be unlikely to admit to being unhappy with their own security stance, so it may make sense that more than a quarter of survey respondents feel they've done everything possible to protect themselves against threats, and another 38% are "pretty confident" in what they've done. To be fair, though, 1 in 4 feels they

Confidence That Current Security Measures Will Provide Protection from Cyber Criminals



SOURCE: IDG Research Services, March 2015



Preferred Method for Deploying Network Security Solutions

SOURCE: IDG Research Services, March 2015

could do a lot more.

That said, there does seem to be a bit of a disconnect between so many executives (3 in 4) citing protection from APTs and next-generation firewalls as high/critical priority (as mentioned at the outset) and so many of the same folks (2 in 3) feel they have done almost all or all they can do to prevent an incident or breach. Perhaps the IT staffers "in the trenches" might have different confidence levels.

Insight 4: Companies prefer to outsource network security, though not to the extent of handing over all responsibility.

In addressing these and other security priorities, respondents prefer cloud security services or on-premise managed security services to physical or virtual appliances they manage themselves. This should not be a complete surprise given the priority (mentioned at the outset) placed on the importance of supplementing in-house teams with outsourced security services.

Nonetheless, while their support for outsourcing network security services increased significantly over 2014, "outsourcing entirely to a partner" is their least preferred way to deploy a network security solution.

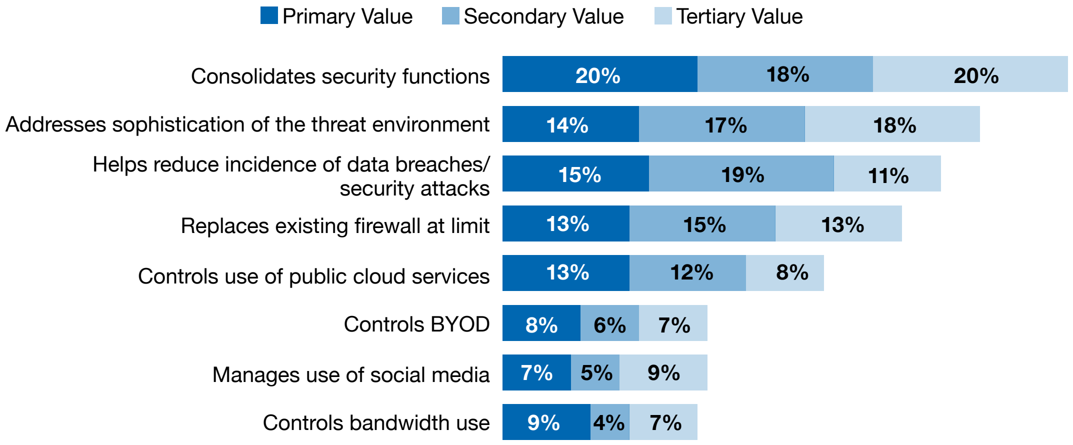
Although this seems contradictory, the word "entirely" may be the key. While companies may need more security expertise than they have in-house, they don't want to wash their hands of ultimate responsibility for their own network—which is a good thing.

Insight 5: Companies see consolidation of security technology as a way to address the fast-changing threat landscape.

Among the most surprising results of this year's survey are responses about the primary value of their No. 2 security priority—next-generation firewalls. Cited by 20% of respondents as the primary value and by 58% as a top-three value, the ability to consolidate security functions such as IPS and filtering is cited the most. This is a near-10% increase over 2014. It is followed by last year's top response—addressing APTs and security breaches.

It is possible that this latest challenge of advanced threats is the straw that broke the proverbial camel's back in regard to "best of breed" point solutions. For years, organizations have added new products to address new threats, and the survey results may indicate that executives have had enough—they are looking to next-generation firewalls to both roll up a number of established network security functions and address the newest threat of APTs. It will be most interesting to explore this topic in subsequent surveys.

Primary Value of Next-Gen Firewalls - 2015



SOURCE: IDG Research Services, March 2015

Conclusion

Organizations remain on high alert against APTs, perceiving them to be the top security priority for 2015 and a greater threat than ever. However, while they're particularly concerned about finding ways to protect customer data and maintain availability and continuity of systems that support the business, they are surprisingly less concerned about safeguarding employee data and intellectual property, which are arguably just as critical to both daily operations and long-range business survival. Given this discrepancy, some respondents have unexpected—and possibly unrealistic—high levels of confidence in their ability to fend off threats and prevent potential losses. That said, executives still have next-generation firewalls as a top security priority, with a primary value of consolidating security functions and combating advanced threats. ■

For more information, visit http://www.fortinet.com/solutions/advanced-threat-protection.html.