ThreatTrack Security

Enterprise Executives and Consumers Lack Confidence About Cybersecurity

Are Enterprises Doing Enough To Protect Their Businesses and Their Customers?

At a time when Advanced Persistent Threats (APT), targeted attacks, Zero-day threats and other sophisticated malware have become profitable businesses for cybercriminals and fodder for alarming headlines about cyber war and foreign espionage, many enterprises are struggling with how to protect their data. Meanwhile, personal experiences by many consumers has led to serious mistrust and doubts among the public about whether or not their data is secure.

A ThreatTrack Security study of C-level enterprise executives and consumers in June 2013 revealed a pervasive uncertainty among enterprises about the vulnerability of their networks to cyber attacks and an overwhelming lack of confidence among consumers about enterprises' ability to safeguard their personal data.

The findings illustrate that many organizations are concerned about security from a broad perspective, but these fears have had little impact in encouraging executives to protect their networks by universally adopting best practices in cyber-defense technologies and specialized personnel.

When asked about their concerns and strategies to thwart cyber attacks, 68.5% of enterprise executives said they are concerned their organization might not be as protected as they should be against sophisticated attacks, and only 41.5% said they have an Incident Response Team (IRT) in place that can identify, react to and remediate cyber attacks launched against their networks. In addition, less than half (49%) of enterprises said their current cyber defense includes an advanced malware analysis too, such as a malware analysis sandbox.

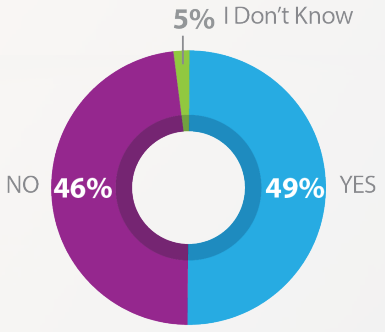
Money Misspent?

The survey findings suggest that enterprises with smaller security budgets are surprisingly less concerned about their company being vulnerable than larger companies. Almost 97% of companies with security budgets of more than $1 million are concerned that their organizations could be vulnerable to malware attacks.

Summary

Enterprises are concerned that their organizations may be vulnerable to targeted malware attacks and Advanced Persistent Threats, but many are not taking the proper precautions to prevent cybercrime from occurring. In addition, many consumers don't believe that enterprises are doing enough to protect their personal data, underscoring the need for enterprises to rethink their cyber-defense strategies and pay more attention to their customers' security concerns.

ENTERPRISES USING ADVANCED MALWARE ANALYSIS TOOLS



Less than half of enterprises include advanced malware analysis sandboxes in their cyber defense strategy.

Even though many larger companies have big bucks to spend on security solutions, they still remain concerned about their vulnerability, according to the study, indicating that the solutions they have in place still aren't buying peace of mind.

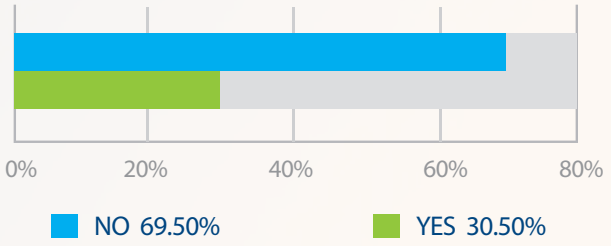
Not surprisingly, larger enterprises were more likely to have sandboxes and other advanced malware analysis tools than smaller companies. The tipping point to utilize those tools seems to be a security budget of $300,000. About 40 percent of companies with security budgets below that number utilize advanced malware analysis tools, while 92 percent of enterprises with security budgets of more than $300,000 use those tools.

Do You Know An Attack Is Underway?

66% of enterprises said they were not aware of any attack launched against their organization, and 83% said they have never had to notify customers of a breach of their personal data.

But the concern is there. In fact, one in five enterprises said their biggest concern about a data breach is not knowing if a significant cyber attack is under way against them or if data has been compromised.

CIOS, CTOs SAY NO ATTACKS HAPPENING



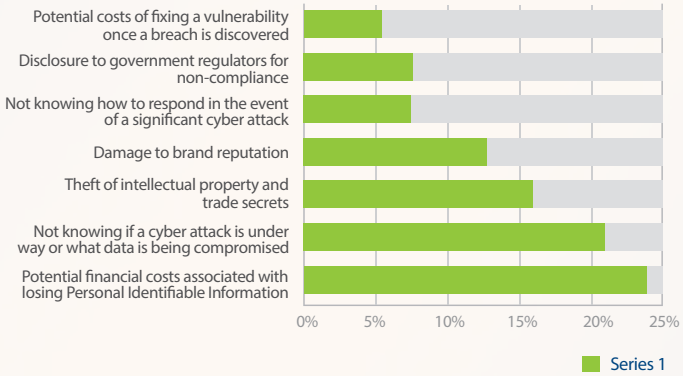
Most CIOs and CTOs were not aware of a malware attack, Advanced Persistent Threat (APT) or other sophisticated cyber attack launched against their organization.

Not knowing about an ongoing threat finished second behind another concern to the C-level executives surveyed: the potential financial costs (such as lawsuits and fines) associated with losing personal identifiable information such as customers' or employees' credit card or Social Security numbers.

Other top concerns of data breaches cited by survey respondents included the theft of intellectual property and trade secrets and damage to brand reputation.

Customers Come First

The possibility of losing personal identifiable information apparently weighs heavy on the minds of the C-level executives. In another part of the survey, enterprises indicated they are more worried about compromising customer information as opposed to their own intellectual property should they have a security breach. 64% of respondents said they're most concerned about someone gaining access to patient records, credit card numbers, social security numbers, etc. The remaining 36% are most concerned about losing their own intellectual property and trade secrets.

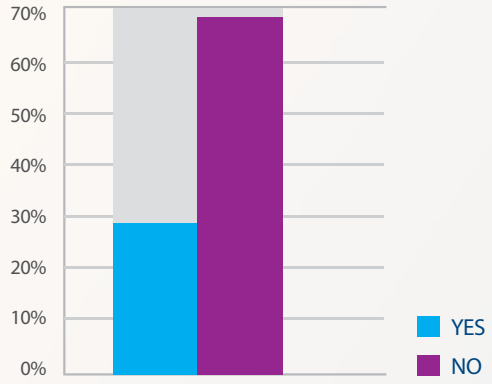


The potential costs of losing customers' personal information in a data breach weighs heaviest on the minds of enterprise executives.

An Industry View

Within specific sectors, 82% of respondents in the finance industry expressed concern about being vulnerable to an attack, but only half include advanced malware analysis tools in their cyber toolbox, and 40% don't have an incident response team in place.

MOST CONCERNED INDUSTRIES UNLIKELY TO USE ADVANCED MALAWARE ANALYSIS TOOLS



While finance and manufacturing customers are most worried about malware attacks, they're still not likely to utilize advanced malware analysis tools or have an Incident Response Team.

Maybe it's a good idea that finance firms be so concerned. The study found that half of the financial services companies surveyed have been the target of a malware attack, APT or other sophisticated

cybercrime tactic. Only retailers reported being targeted by cyber attacks at such a high rate.

34% of all enterprises surveyed said they'd been cyber attacked, with larger companies apparently having bigger targets on their backs. Just over 72% of companies with more than $1 million security budgets said they were aware they were attacked.

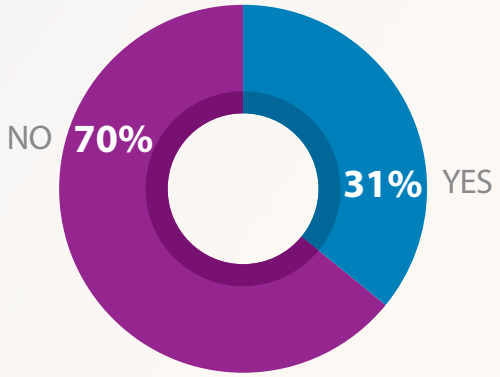
Meanwhile, only 33% of professional services companies and 27% of educational organizations have advanced malware analysis tools in place, and more than half of the respondents in those two industries also don't have incident response teams in place.

Consumers Not Confident

The concerns that C-level executives have regarding losing customers' personal information in a data breach may well be warranted.

About 30% of consumers believe that companies are doing everything they can to safeguard their personal identifiable information such as credit cards and Social Security numbers. Almost 43% said companies aren't doing enough to protect that information and 27.6% said they weren't sure.

DO ENTERPRISES DO ENOUGH?



Consumers aren't confident that enterprises are adequately protecting their personal information.

Consumers aged 25-34 were especially critical of enterprises, as 64.3% of survey respondents within that age range don't believe companies are adequately protecting their information.

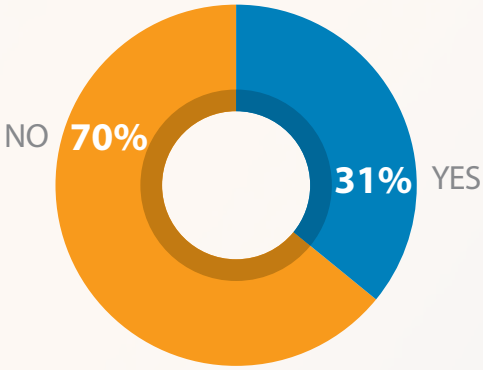
Not only do consumers have concerns about the security of their personally identifiable information, they also believe their information will be lost in a data breach. An alarming 75.4% believe companies will be attacked and their information will be compromised.

Consumers may feel that way because nearly half of them have already had their personal information compromised, according to the study. Nearly 47% said they have been notified by their bank or another company that personal information was compromised and that they needed to take measure such as changing their password or being issued a new card.

No To Government Intervention

Despite their experiences and a lack of confidence after an attack, 69.5% of survey respondents do not believe government should dictate to private companies how they should handle and store their private data, nor dictate which technologies businesses should use to secure their networks.

SHOULD THE GOVERNMENT TELL COMPANIES HOW TO HANDLE DATA?



Consumers don't want the government dictating how private enterprises store and control their data.

And yet, 31.5% of consumers said government isn't doing enough to control how private companies protect their data, while only 20.7% believe the government is adequately controlling how private companies manage data. Nearly half (47.8%) of respondents said they didn't know if the government was doing a strong job in that area.

What Scares Consumers Most

The majority of consumers (59%) said they are most concerned about sharing their Social Security number with third parties online.

A distant second choice was credit card numbers (13.8%) while debit card numbers (7.9%), mailing addresses and telephone numbers (4.4%), personal data shared on social media sites (3.9%) and medical records (2.5%) were also cited.

The fact that few consumers were concerned about medical records, which are frequently targeted by hackers because they may contain both financial and

personal information such as Social Security numbers, illustrates the need for more consumer awareness about their digital footprint and the risk it creates. Additionally, consumers were more concerned about credit card numbers than debit cards, even though consumers are typically better protected by credit cards than their debit card brethren. Only 6.4% of consumers said they were not concerned about sharing any data with third parties.

Conclusion

Enterprise executives are rightfully concerned about being the target of advanced cyber threats. On one hand, it speaks to their understanding of malware threats that they're more concerned about losing customer data (or at least the financial implications that come with it) than their own intellectual property. But on the other hand, what are they doing about it? If less than half of enterprises have Incident Response Teams and advanced malware analysis tools, they're not taking enough precautions to prevent the cybercrimes they're so worried about. It's not surprising that consumers think companies aren't doing enough to thwart sophisticated attacks.

And those same consumers may have a right to be leery of enterprises' cyber security strategies. After all, many of them have already had their personal information compromised. Enterprises need to re-examine their cyber-defense strategies in order to be more vigilant against a growing and more complex world of threats. That accomplished, they may finally give customers –and themselves – the peace of mind they desperately seek.

Study Methodology

This independent, blind survey of 200 C-level executives at U.S.-based enterprises and 203 U.S. consumers was conducted by Opinion Matters on behalf of ThreatTrack Security in June 2013.

About ThreatTrack Security

ThreatTrack Security Inc. specializes in helping organizations identify and stop Advanced Persistent Threats (APTs), targeted attacks, Zero-day threats and other sophisticated malware designed to evade the traditional cyber-defenses deployed by enterprises around the world.

ThreatAnalyzer, ThreatTrack Security's malware analysis sandbox, is used by government security, defense and intelligence agencies, making it an integral component of the U.S. cybersecurity infrastructure.

More information on ThreatTrack Security can be found at **www.ThreatTrackSecurity.com**.