Harvard Business Review

A REPORT BY HARVARD BUSINESS REVIEW ANALYTIC SERVICES

Aggressive and Persistent: Using Frameworks to Defend Against Cyber Attacks

Sponsored by

TREND MICRO™

Aggressive and Persistent: Using Frameworks to Defend Against Cyber Attacks

IT AND BUSINESS MANAGERS are scared of targeted attacks on their data and systems, but the fact that senior decision makers are unsure or skeptical of the exact business risks and impacts of such attacks makes it harder to secure funding to be prepared and fight them.

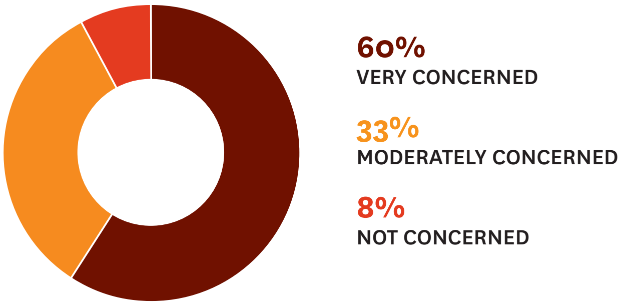
A Harvard Business Review Analytic Services survey found that 60% of the 142 business executives from respondent organizations with more than 500 employees are concerned about such attacks, in which cyberthieves seek to steal intellectual property or to otherwise harm an organization. figure 1

A lack of deeper understanding at top levels of the business, however, means that all too often that concern doesn't translate into action. A full third of respondents don't know what data might have been compromised in such attacks and more than two-thirds said that "decision makers need to better understand the real threat and consequences" to approve appropriate levels of security funding.

Figure 1

Almost All Concerned with Cyber Attacks

Overall, how concerned is your organization with becoming the victim of a targeted attack, i.e., an attack that is custom-built to permeate your organization and network and to steal your data, intellectual property and other confidential information?



NOTE AMOUNTS ADD UP TO MORE THAN 100 DUE TO ROUNDING

SUMMARY

60%
of survey respondents are very concerned about attacks on their organizations' IT systems and data.

70%
said that senior decision makers need to better understand each threat and its consequences.

17%
of survey respondents are certain their organization is fully protected against an attack.

Despite ever-growing threats and almost weekly disclosures of major data breaches, chief information officers (CIOs) and chief information security officers (CISOs) are still not doing a good enough job of explaining the nature and scope of targeted attacks to their business counterparts and superiors, according to survey respondents and leading experts.

Often, the reason that such explanations are not sufficiently effective is that the line of business (LOB) managers think differently than security professionals. The problem can be that IT is not explaining security issues in business terms. The constant vigilant thinking required by security execs is not typically in the LOB manager mindset. They let others worry about security, which is very dangerous. Put another way, they view security as either an afterthought or somebody else's problem.

"There's a great lack of awareness of what specifically is being targeted," says Dave Burg, a principal in PricewaterhouseCoopers' Forensic Services unit. PwC research shows that only 26% of those surveyed had identified which of their information assets are the most sensitive and thus deserve the most effort and budget to protect. Giving all data within the organization the same level of protection, he says, is ineffective and wasteful when attackers are specifically targeting an organization's most sensitive information, processes or people. If you're not sure what the biggest threats are, the danger is you just protect everything, leading to inefficiency and waste.

Widespread Concern

The lack of focus or effort on cybersecurity is especially surprising considering recent history and expectations about the future. Nearly one-third of respondents to the Harvard Business Review Analytic Services survey said they are currently targeted, and an equal number said that they expect their organization will be more aggressively targeted in the future. And these responses may underestimate the problem.

"If you talk to anyone in the business, they'll say you 'should probably assume every network has already been subverted by a nation-state somewhere,'" said a security professional with a Midwestern utility. His organization "geoblocks" all network access from countries such as China and Russia with whom the utility does not do business, because traffic from those areas is clearly potential source of attacks.

Fortunately, the same defensive mechanisms that would repel attacks from government agents of North Korea or Russia would also block attacks from citizens of those geographies. This defense is not perfect, of course, as cyberthieves often try and hide their paths, just as they clean up security logs. That said, it certainly will block some of the attacks.

Respondents to the Harvard Business Review Analytic Services survey said their top concerns about targeted attacks include:

- Potential brand damage (56%)
- Damage to professional reputation (54%)
- Potential loss of intellectual property (52%)
- Potential loss of revenue (49%)
- Unfavorable publicity (45%)

Adding to the urgency are regulatory pressures. More than half said that complying with legislation and industry rules was a high priority. Indeed, more than a quarter gave such compliance concerns the highest rating.

What's more, the actual scale of attacks may be greater than reported because many are designed to evade detection, by (for example) copying data rather than deleting or altering it. Even in some of the highest-profile recent incidents (Target and Neiman Marcus), the major retailers only learned of the attacks through law enforcement, payment processors or others in the payment chain.

Lack of Awareness and Confidence

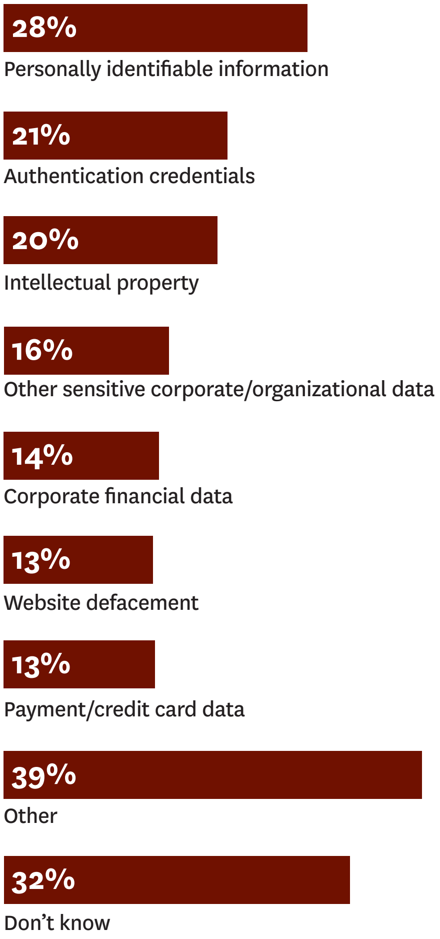
This high level of concern, however, is not matched by detailed knowledge of the nature of the threats that might help unlock or realign security budgets. For example, "don't know" was the highest single response when respondents were asked which of their data might have been compromised. figure 2

The lack of information about past incidents seems to be more widespread than expected, considering the high level of concern about cyber attacks. PwC's June 2013 State of Cybercrime Survey showed similar results: Only 40% of the organizations surveyed had a methodology in place to determine the effectiveness of their security measures.

Figure 2

What's at Greatest Risk

Which of the following types of data, if any, have been potentially compromised or breached in the past 12 months? [SELECT ALL THAT APPLY]



NOTE PERCENTAGE OF RESPONDENTS IDENTIFYING A SPECIFIC DATA TYPE POTENTIALLY COMPROMISED OR BREACHED IN THE LAST YEAR. TOTALS EXCEED 100% DUE TO OPTION TO CHOOSE MULTIPLE ANSWERS.

A surprisingly large number of survey respondents have had personal experience with the results of cyber attacks. More than one in four of the survey respondents have lost “personally identifiable information” and one in five has lost authentication credentials in the prior 12 months.

The reported loss of authentication credentials is also very troublesome, given the fact many customers use the same passwords on multiple sites to avoid having to remember multiple complex passwords. This means the theft of one password could give cyberthieves access to multiple customer accounts.

Just more than a third (35%) of the respondents said they are not aware of the occurrence of targeted attacks on their networks in the last year, while only 34% are confident they have full network visibility and can monitor and manage it in an effective and timely way. Just under one in five said they “are certain we are fully protected against an attack.” About a fifth replied “don’t know” to important questions such as whether their financial losses to targeted attacks had changed over the last 12 months, which proactive steps they are taking to prevent such attacks and even the size of their security budgets.

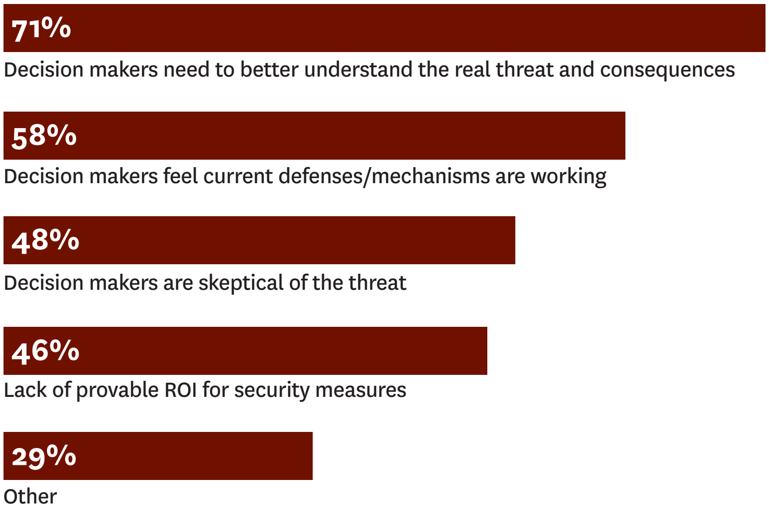
Budget Shortfalls

A lack of senior management understanding and awareness of the danger, and impact, of targeted attacks makes it harder to properly fund security efforts, Harvard Business Review Analytic Services survey respondents said. Indeed, more than two-thirds noted that “decision makers need to better understand the real threat and consequences” as a prerequisite to increasing and/or realigning security funding. Other barriers to additional funding to improve information security include complacency (decision makers consider current defenses adequate) or budget issues. figure 3

Figure 3

Lack of Understanding Hinders Additional Funding

Please rate the extent to which you agree that each of the following is a barrier in funding efforts to fight targeted attacks.



> Research shows a growing trend to systematic, ongoing evaluation of risks rather than reflexive spending hikes tied to the cost of the most recent breach.

However, about a third of Harvard Business Review Analytic Services survey respondents said that they expect their security budgets to rise by more than 10% this year. That is a good sign of progress because it is a much higher increase than is customary in other areas of IT. Even these organizations may still be underfunding their security efforts, though.

Security is still "often thought of as just another expense," explains Burg. He added that while PwC research also sees security spending rising, it makes up only about 3.8% of total IT spending, "a relatively small investment."

The situation is not entirely dire for information security, though. The research did show a growing trend to systematic, ongoing evaluation of risks as the driver of security budgets, rather than reflexive spending hikes tied to the cost of the most recent breach. Four out of ten respondents indicated they expect to be taking such an approach in the next 12 months.

What's Needed

Education and awareness are still required for executives to understand the need for and provide proper funding to defend against targeted attacks.

"We must assume though that no defense is 100% effective," said the security manager for the Midwestern utility, who said an organization's true "secret sauce," or intellectual property may deserve higher levels of protection or even be stored offline. He also recommends periodic professional penetration testing that mimics a targeted attack. A regulatory "stick" is useful to drive needed spending on security, he says, but "in the end, it is necessary to demonstrate what the risk is, what that return on investment is with respect to reducing losses and reputational issues."

Taking the crucial up-front step of identifying which data is most at risk helps show the ROI of defenses and helps focus budget dollars on the most critical risks, Burg said. This allows security managers to speak in terms business managers are more likely to understand. Such an assessment might actually reduce the need for some security spending, he says, which is always welcome news.

Given ongoing funding challenges, respondents said they need single tools that can fight many different threats and that do not cause major increases in management and support costs. The ability to detect and stop a broad spectrum of threats was the most common requirement, mentioned by 63% of respondents, followed by "easy to implement, deploy and manage across all my networks" at 54%, "ability to analyze a wide variety of suspicious files and payloads" at 44%, and "single, easy to manage all-in-one solution" at 39%.

In an era when a greater number of cyberthieves are targeting a wider range of data with increasingly sophisticated threats, organizations cannot afford unrealistic assumptions.

Action Items

When faced with a wide variety of hard-to-find, serious threats but no clear avenue to escape them, humans tend to deny the threat or ignore it. So it is with organizations facing targeted attacks.

To move their organizations past complacency or ignorance to action, chief information officers and chief information security officers owe their business counterparts:

- Realistic, believable assessments of true threat levels
- Security budgets justified in business terms such as risk mitigation rather than wreathed in technical jargon
- Security strategies that focus scarce funds on the most critical threats

Although his security budget is "not a bottomless, endless pit," the security manager for the Midwestern utility said that "if the justification is there, I'm able to get the budget."

In an era when a greater number of cyberthieves are targeting a wider range of data with increasingly sophisticated threats, organizations cannot afford unrealistic assumptions such as "We're 100% protected" or ignorance about the risk. Although business and marketing executives can't be expected to choose security tools, their awareness of the business implications of targeted attacks makes it far more likely they will properly fund them. ◆

METHODOLOGY

An online survey with the readers of *Harvard Business Review* from mid-December 2013 through early January 2014 asked respondents at organizations with more than 500 employees to answer 18 questions.

- IT was the most common functional unit represented among the 142 respondents, at 29%, followed by general management at 12%.
- Manager/supervisor was the most common title, at 27%, followed by senior manager/department head at 21% and director at 15%.
- A third of the respondents were from the Asia Pacific region; 32% from Europe, Middle East and Africa; 28% from North America; and 8% from the rest of the world.

Sponsor's Perspective

KEVIN SIMZER

SENIOR VICE PRESIDENT, MARKETING & BUSINESS DEVELOPMENT

TREND MICRO

AS THE NEW RESEARCH from Harvard Business Review Analytic Services shows, executives around the world know that cyber attacks threaten the strategic security of every company. Yet grasping the severity of the problem and establishing corrective mechanisms in the face of targeted attacks and advanced threats is still a huge challenge for far too many.

And unless top executives understand the vulnerability of their organizations to the rapidly evolving threats of cybercrime, cybertheft, and cyber espionage, the survey found that prioritizing and expanding the budgets for security will be limited—leaving companies dangerously exposed.

At Trend Micro, in our work with customers, we have built a deep understanding of cyber attacks and the best practices in combating these threats.

In our experience, we have found that attackers conduct advance reconnaissance on your employees, networks and infrastructure, and then custom-design an attack to permeate your network. These attackers are tenacious and will use any means and methods at their disposal to breach your network. Attackers select from a wide range of applications, communication channels, network ports and attack patterns in order to ensure the lowest probability of detection and the highest probability of successfully extracting the data, intellectual property and communications they are seeking.

In the face of these threats, our Forward Threat Research team and innovative Smart Protection Network enable Trend Micro to provide our customers with a unique level of visibility and awareness of targeted attacks and advanced threats.

As Threat Defense Experts with more than 25 years of experience, Trend Micro is recognized as the only pure-play security provider, delivering top-ranked solutions to over 500,000 commercial customers.

We welcome the opportunity to work with you and your teams to address what can be a devastating loss of information and intellectual capital to targeted attacks and advanced threats.

ACCESS THE REPORT AT:
www.TrendMicro.com/CustomDefense

Sponsored by

TREND MICRO™

Trend Micro™ Deep Discovery
TOP SCORE
in breach detection
NSS LABS
RECOMMENDED
2014 Breach Detection Tests