(ISC)²

Cybersecurity Assessments in Mergers and Acquisitions

The ROI of Sound Cybersecurity Programs

An (ISC)² Research Report

TABLE OF CONTENTS

INTRODUCTION

In mergers and acquisitions (M&A) negotiations, buyers look closely at factors such as a company's balance sheet, intellectual property and market share. How well a company performs in each of these areas can make or break a deal, but what some potential sellers may not realize is that another factor has become just as important in M&A activities – a company's cybersecurity program.

Cybersecurity audits are now essential to the M&A process: 100% of respondents in an (ISC)[2] survey of executives and advisors involved in M&A activity say the audits have become standard practice. And what's more, an organization's cybersecurity tools and practices, and overall security posture, can determine the fate of a deal, the survey found.

Buyers also take into consideration how a company has handled security breaches in the past, and in most cases that will affect a company's selling price. The survey shows that buyers are forgiving to companies that demonstrate they took the right steps to address past breaches, but less so when it comes to previously undisclosed security breaches.

Breaches that come to light during the due diligence process can derail a transaction, something that about half of respondents (49%) say they have seen happen.

Furthermore, about three quarters of respondents (77%) have made recommendations on whether to proceed with an M&A deal based on the strength of the target company's cybersecurity program. So even if a company runs an efficient supply chain and offers great products and customer service, the absence of a robust cybersecurity program is a problem. There is inherent value in cybersecurity tools and practices, and any decision-maker considering M&A activity must not ignore this fact.

KEY FINDINGS

Based on the (ISC)² survey's results, it's safe to say no M&A deal can go forward without a review of a company's cybersecurity posture. Here are the report's key findings:

100%

All 250 respondents (100%) say cyber audits are a standard M&A practice.

49%

About half (49%) say the discovery of previously undisclosed breaches would derail a deal.

77%

Three quarters (77%) make M&A recommendations based on the strength of the cybersecurity program.

95%

The vast majority (95%) consider cybersecurity programs a tangible asset.

DEMOGRAPHICS: WHO ARE THEY?

The survey focused on a very targeted group of 250 U.S.-based professionals with M&A expertise. All participants are involved in M&A activities in some capacity, including investment and research analysts, venture partners, general partners, principals, and risk and compliance officers. The role with the greatest representation – 34% of respondents – was that of managing director.

For a comprehensive look at the business spectrum, the survey polled individuals in companies of various sizes. There was an almost even split of organizations with 250 employees or fewer (47%) and those with more than 250 (53%). One third of respondents are from companies with more than 1,000 employees.

CYBER AUDITS ARE STANDARD

The (ISC)^2 report offers conclusive evidence that completing a cybersecurity audit is now standard practice in M&A due diligence. This is a reflection of how much of a concern cyber threats have become in the boardroom. Recent research clearly shows CEOs view cyber threats as a top challenge – one that if left unaddressed is bound to hinder corporate growth.

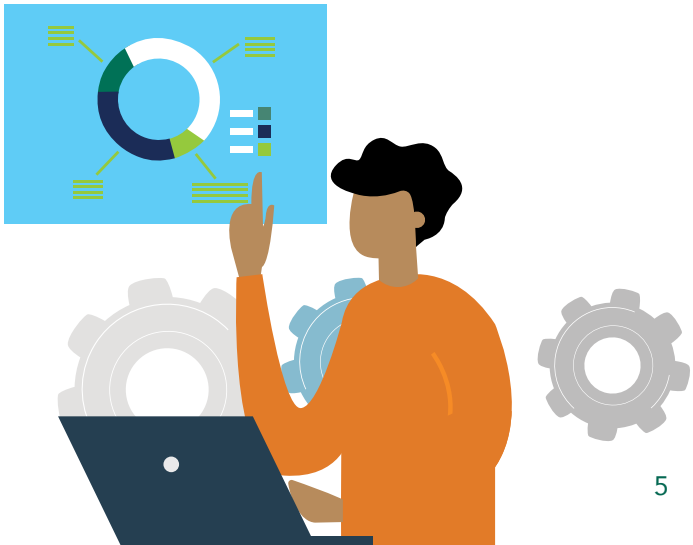
Companies approach cybersecurity audits in the M&A process in different ways, according to the (ISC)^2 study. More than half of participants (60%) say their organizations use an in-house team of security auditors, while 35% say they retain outside consultants for the job. The remainder say their company allows the acquisition or merger target to self-audit but requires a signed affidavit. This latter approach poses the most risk. The risk associated with this practice explains why only 5% of respondents use it.

Larger companies – those with more than 250 employees – are more likely to have an in-house team of cybersecurity auditors (71% vs. 46%). This is almost certainly a function of resource availability – the bigger the company, the more likely it is to have the financial resources to employ an in-house team.

When performing due diligence, buyers treat cybersecurity programs as an asset, and the vast majority (96%) of them take into account cybersecurity readiness to determine the overall monetary value of the selling company.

Slightly more than half of organizations (53%) say value varies widely – presumably depending on the maturity and effectiveness of the cybersecurity program – while 45% use a standard plus/minus value assigned in a pass/fail manner. Companies with in-house auditors employ the standard plus/minus valuation more often than companies outsourcing or allowing clients to self-audit. Regardless of which valuation method buyers employ, it's apparent that a robust cybersecurity program helps boost overall value.

> "Breaches that come to light during the due diligence process can derail a transaction, something that about half of respondents (49%) say they have seen happen."



CYBER AUDITS MAKE AND BREAK DEALS

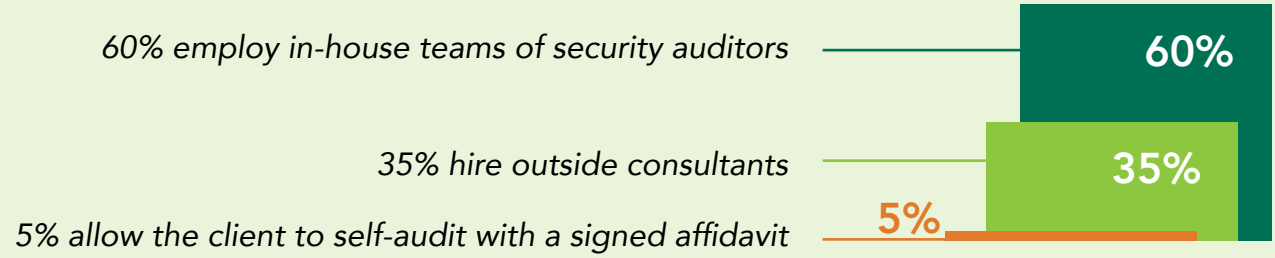
The research shows that the inclusion of a cybersecurity audit in M&A does more than simply fulfill a requirement or serve as window dressing. M&A experts pay close attention to cyber audit results – and take them into account to make decisions. A solid majority of respondents (77%) say the strength of a cybersecurity program affects their recommendation on whether to acquire a company.

One of the factors that can affect the recommendation is how a company has handled past security breaches. For most respondents (86%), a publicly reported breach detracts from the acquisition price. But it's not a deal breaker, if the company can demonstrate it handled the breach appropriately and took steps to prevent further incidents. If the company addressed the breach satisfactorily, fixed its security vulnerabilities and paid its fines (when applicable), 88% say the company's value increases.

This brings serious gravity to lessons learned. If an organization has learned from past incidents and mistakes, it shows a level of maturity and seriousness. It may even provide a kind of immunity, indicating that the organization is resilient in the face of cybersecurity incidents.

WHO PERFORMS AUDITS?

100% of respondents indicated that cybersecurity audits are standard practice during M&A assessments



TANGIBLE ASSET

When acquiring a company, the buyer also acquires its cybersecurity capabilities – and all the implications associated with the quality of the cybersecurity program. For this reason, nearly all study participants (95%) consider cybersecurity a tangible asset. IT tools in general are also factored in as assets, according to 63% of respondents.

Furthermore, 82% of those surveyed say the stronger a company's cybersecurity infrastructure, including soft assets such as risk management policies and security awareness training programs, the higher the value assessed to the organization. If an audit reveals weak security practices, about half of respondents (52%) view that as a liability. The same number of respondents say post-acquisition data breaches in an acquired company have affected the share value of publicly-traded organizations.
This explains why 54% of respondents consider cyber audits already vital to the M&A process, while another 42% believe they will increase in importance in the next two years. For organizations considering a sale or merger, this is a key requirement to keep in mind. They may want to reassess their cybersecurity programs and test their effectiveness before moving forward with any sale or merger plans.

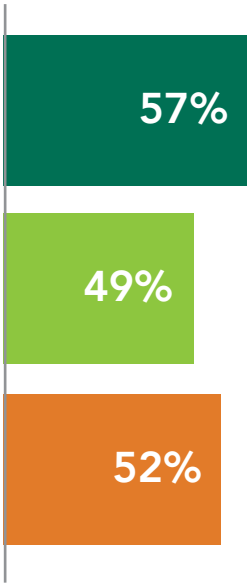
> "If the company addressed the breach satisfactorily, fixed its security vulnerabilities and paid its fines (when applicable), 88% say the company's value increases."

WHEN IT GOES WRONG

57% of respondents have been surprised to learn of an unreported data breach during the audit process

49% said data breaches or weak security practices found in the discovery process have caused an M&A deal to be canceled

52% said the share value of publicly-traded clients has been negatively affected as a result of an acquired company's post-acquisition data breach



NO SURPRISES PLEASE

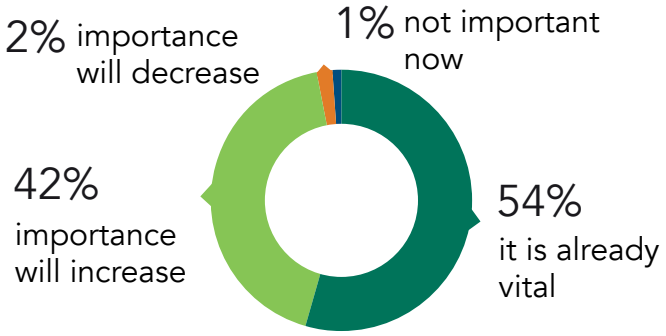
Not surprisingly, executives, analysts and anyone else involved in M&A would rather avoid any curve balls. Yet 57% of respondents in the (ISC)² study say they have been surprised during the auditing process.

If a previously undisclosed security breach comes to light during discovery, it can derail a deal. 49% of respondents say deals in which they were involved have fallen apart because of undisclosed breaches. This is further evidence that executives and M&A experts take cybersecurity audits seriously, and that they view a company that can demonstrate cybersecurity best practices and hygiene as a more attractive target.

Previous research supports this finding. For instance, in a recent study of 2,700 IT and business-decision makers by Forescout Technologies, 53% of respondents reported that critical cybersecurity issues or incidents have jeopardized M&A deals for their organizations.[1]

The Forescout study found that 65% experienced buyer's remorse because of cybersecurity concerns that surfaced after closing a deal. "Cybersecurity concerns discovered after consummation of the deal often present costly risks that would have been factored into the deal negotiations and/or may have led to the dissolution of the deal," the company said in a statement.[2]

HOW IMPORTANT OF A ROLE WILL CYBERSECURITY AUDITS PLAY IN M&A DURING THE NEXT 2 YEARS?



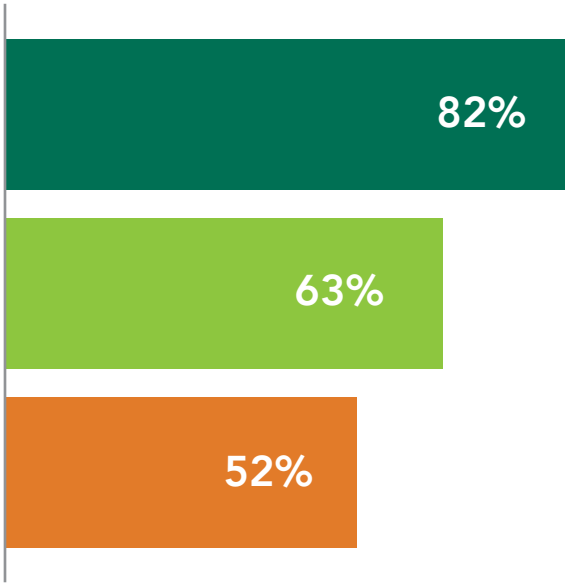
> "82% of those surveyed say the stronger a company's cybersecurity infrastructure, including soft assets such as risk management policies and security awareness training programs, the higher the value assessed to the organization."

HOW CYBERSECURITY INFRASTRUCTURE IS CALCULATED AS ASSET/LIABILITY

The stronger the infrastructure, including soft assets such as risk managment policies and security awareness training programs, the higher the value assessed

Any information technology tools are factored in as assets

If the audit reveals weak security practices, the cybersecurity program as a whole is considered a liability



CONCLUSION

Cybersecurity audits have become an essential step in the M&A due diligence process, which underscores the importance of maintaining a strong security posture. It's clear from the (ISC)^2 study's findings that the health of an organization's cybersecurity program directly affects the value of a potential deal.

A company's cybersecurity history matters. Previously undisclosed breaches can derail deals and weak security practices may be viewed as a liability. Companies that overlook the importance of cybersecurity are not maximizing their value. Cybersecurity strength is a real consideration that affects the bottom line.

For buyers, paying close attention to the cybersecurity history of a target company is a must. While a company ultimately may decide to go ahead with a deal, even if past breaches have occurred, cybersecurity audits are critical. Overlooking troubling signs revealed by the audit can bring repercussions that could devalue the company after a purchase or merger. Therefore, it is incumbent upon buyers to verify a target company has all the necessary security controls in place before proceeding with a deal.

ENDNOTES

[1] Forescout Technologies' "The Role of Cybersecurity in M&A Diligence" report: https://www.forescout.com/solutions/asset-management/merger-and-acquisition-cybersecurity-report/

[2] Forescout Technologies press release: https://www.forescout.com/company/news/press-releases/forescout-study-reveals-cybersecurity-concerns-on-merger-and-acquisition-activity/

ABOUT (ISC)²

Celebrating its 30th anniversary this year, (ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)²offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, more than 140,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry.

For more information on (ISC)², visit www.isc2.org.

METHODOLOGY

Results presented in this report are from an online survey conducted by (ISC)² and Market Cube in December 2018. The total respondent base of 250 professionals is responsible for evaluating and recommending mergers and acquisitions targets for their company or clients. 47% of respondents were from small companies with 250 or fewer employees, and 53% were from companies with at least 251 employees, all based in the United States.