



TESTING THE DEFENSES

CYBERSECURITY
DUE DILIGENCE
IN M&A

Contributors



Sean Curran
Director, Security & Infrastructure

Sean Curran is a director in West Monroe Partners' Security and Infrastructure practice, based in Chicago. He has more than 20 years of business consulting large-scale infrastructure experience across a

range of industries and IT domains, including extensive work in the areas of data and information security. He has experience designing secure environments, helping clients adhere to industry and government compliance frameworks including PCI DSS, HIPAA and ISO 27000.

312.386.6195

scurran@westmonroepartners.com



Paul Cotter
Senior Architect, Security & Infrastructure

Paul is an experienced and practiced security professional, with over 15 years of experience in software, infrastructure and organizational security for

Fortune 100 companies. Paul has performed several functional diligences in the security product space, including Endpoint Protection, Network Intrusion Detection, Threat Intelligence, and Deep Packet Inspection products.

312.846.9974

pcotter@westmonroepartners.com



Matt Sondag
Managing Director, Mergers & Acquisitions

Matt Sondag is a managing director in West Monroe Partners' New York office. A skilled business consultant with a strong technology background,

Matt is responsible for expanding and deepening the firm's unique offerings to the private equity market, including its merger and acquisition services. Matt works with private equity and strategic buyers involved in or preparing for investments and acquisitions. He assists buyers with pre-deal IT and operational due diligence, as well as post-close projects (integration and carve-out activities).

312.980.9446

msondag@westmonroepartners.com



John Stiffler
Senior Director, Mergers & Acquisitions

John Stiffler is a senior director and the leader of West Monroe Partners' Mergers and Acquisitions practice in Chicago. He specializes in corporate divestitures and

operates as a client partner, combining strategy, financial, people, process, and technology disciplines to deliver technology-enabled business change. He has over 30 years of global business and technology consulting experience across multiple industries with heavy emphasis in manufacturing and distribution, healthcare, high tech and professional services.

312.980.9427

jstiffler@westmonroepartners.com



westmonroepartners.com | 800.828.6708

BUSINESS
CONSULTANTS

DEEP
TECHNOLOGISTS

Contents

Foreword	4
Sounding the alarm	6
Assessing the risks	8
PE paying up	12
Hitting the escape button	13
Good governance	14
Unpleasant discoveries	18
Conclusion	20
Appendix: Respondent profiles	21

Foreword

Big data and IT are becoming ever more critical to the modern corporate world. As their importance rises, data security has become vital for ensuring business continuity and protecting a company's most prized assets – its customer information and intellectual property.

The costs of failing to keep data secure are increasing rapidly. In 2015, the average cost of a data breach reached US\$3.79m, a 7.6% increase over 2014, according to a survey commissioned by IBM. Overall, the total cost of cybercrime to the global economy as estimated by software-maker McAfee can reach up to US\$575bn per year.

In the realm of M&A, concerns about cybersecurity are becoming a critical issue when companies target acquisitions. A company's cybersecurity infrastructure – or lack thereof – can affect the deal price, and at times determine whether a potential acquirer goes through with a deal at all.

Data security has long been an issue for M&A activity in certain sectors, such as retail and technology. In recent years, however, it has become relevant across industries. Take healthcare: in 2015, major insurer Anthem suffered a breach of an estimated 80 million customer records after hackers broke into its network, part of a string of breaches at medical firms. In the telecom industry, British firm TalkTalk saw the data of 157,000 customers exposed, and the company predicted the incident would cost it over US\$50m.

In order to protect themselves from security lapses, acquirers are turning to vigorous due diligence to examine the IT infrastructure of deal targets. Diligence procedures are quickly expanding and improving – but many companies continue to identify shortcomings in the process.

Our report surveyed top-level corporate executives and private equity partners about their companies' practices in order to better understand the state of cybersecurity diligence for M&A. The results provide a window into the trends that shape the diligence process, as well as insights into the ways it can be improved. We hope the report proves useful to you as you navigate the increasingly complex dealmaking landscape.

“When a data breach lands on the front page of CNN.com or The Wall Street Journal, companies start to pay closer attention to the issue. In the last 18 to 24 months, we have really started to see the importance of cybersecurity resonate with our clients.”

Matt Sondag, Managing Director,
West Monroe

Key findings include:



Cybersecurity diligence is no longer optional. Seventy-seven percent of our respondents said the importance of data security issues at M&A targets has increased significantly over the last two years. The costs associated with data breaches have led acquirers to take the issue much more seriously.



Good governance trumps bells and whistles. The abundance of new data security tools has made it easier to have cutting-edge technology in place. But the way in which tools are used and relationships are managed remains paramount when it comes to maintaining sound cybersecurity.



Knowledgeable personnel is key. Given the velocity at which cybersecurity trends evolve, it is essential for the team vetting a deal target to be experienced and well-versed in the field. Almost one-third (32%) of our survey respondents said not enough qualified people were involved in the diligence process in recent deals.



Be practical when assessing risks. In the diligence process, 47% of our respondents focus on planning for fixes to problems they uncover, since most targets can be expected to have a few issues. The price tag for making the necessary changes is key as well, as fixes can require considerable expense.



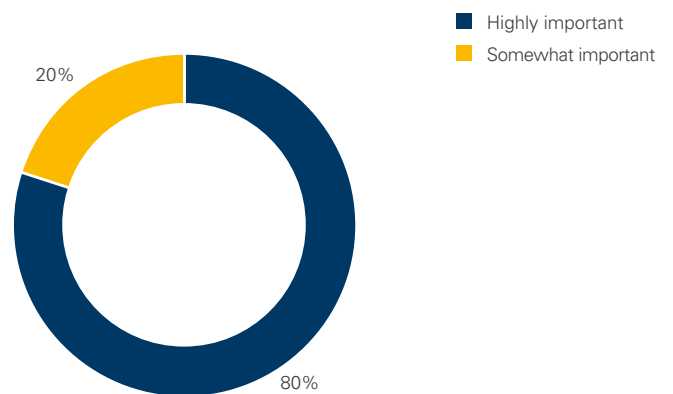
Remember to implement deal protections. Acquirers can be held legally liable for undisclosed data breaches or other cybersecurity problems at an M&A target. As a result, protections such as representations and warranty insurance and closing conditions are trusted safeguards against undue harm.

Sounding the alarm

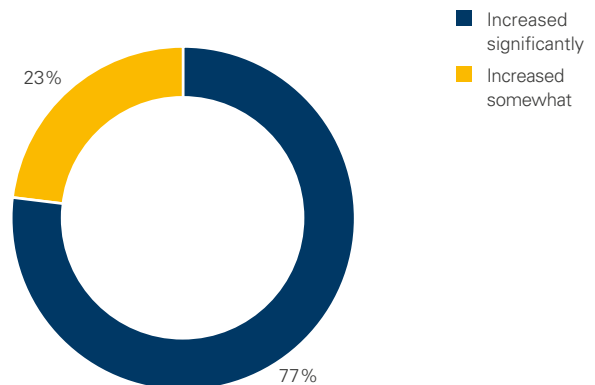
Acquirers are finally taking note: Cybersecurity has become a crucial part of the due diligence process for M&A. Ignore a target's data breaches at your peril.

As the value of data rises across industries, companies are becoming increasingly concerned about IT security at deal targets. Eighty percent of our respondents said cybersecurity issues are highly important in due diligence, compared to just 20% who said they are somewhat important. At the same time, 77% said the importance of cybersecurity at M&A targets had increased significantly over the last 24 months, reflecting the rapid growth of risks related to cybercrime and the growing number of costly data breaches.

When conducting due diligence for a deal, how important are cybersecurity issues at the target company?



Over the last two years, how has the importance of cybersecurity issues at target firms changed for you in dealmaking?



West Monroe managing director Matt Sondag said acquirers have become much better-informed of late about the risks of inadequate cybersecurity. "When a data breach lands on the front page of CNN.com or The Wall Street Journal, companies start to pay closer attention to the issue," he said. "In the last 18 to 24 months, we have really started to see the importance of cybersecurity resonate with our clients."

Indeed, instances of major financial loss due to breaches are becoming increasingly common. In one of the most notorious cases, retailer Target suffered a breach in late 2013 at its point-of-sale systems. As of Q1 2015, the company had accrued a loss of US\$252m in connection with the breach and has faced legal action by credit card companies, government agencies, and consumers.

Vulnerable IT systems can indicate poor risk management at a company as well as lead to concrete business losses, said a partner at a mid-market private equity firm with over 80 active investments. "Data security issues that arise while conducting due diligence are highly important, as they are indicators of risk exposure and may lead to damages related to non-compliance or reputational harm," the PE partner said.

The proactive approach

Cybersecurity due diligence is about more than deciding whether a company

is an appropriate target, according to our respondents. Almost half (47%) said their top priority for using the information they gain in the process is to plan for fixes – meaning they presume that they will go through with the deal once the process has begun. One-third (33%) said they use the information to decide whether to do the deal and one-fifth (20%) said they focus on negotiating better deal terms.

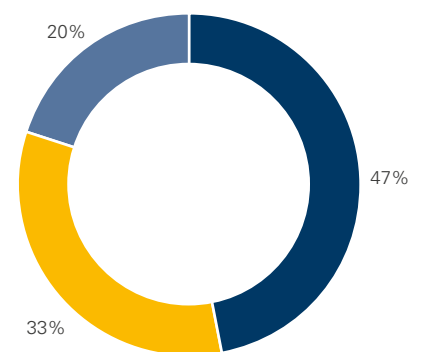
Respondents who said they prioritize planning for security fixes argued that it was realistic to expect companies to have some issues. "We don't think there are any companies without inadequacies in their data security," said a managing director at a mid-market private equity firm focused on industrials and business services. "It is obvious there will be some issues. But we have to know the quantity and complexity of the issues so that we can resolve them."

One respondent, the director of M&A at a technology firm that completes more than 10 acquisitions a year, said his company needed to determine whether or not to go through with a deal, since data security is crucial to their industry. "Information collected through data security diligence plays the most important part in deciding the future course of the deal," the M&A director said. "We operate in an industry where data security is of utmost importance and therefore any breach or intrusion could permanently harm the company's image and operations."

The bottom line

It's realistic to expect most M&A targets to have a few cybersecurity issues. The key is identifying them and determining how easily they can be addressed.

What is your main priority when using the information gleaned in the cybersecurity diligence process?



- Planning for fixes to uncovered problems
- Deciding whether to go through with the deal
- Negotiating down the purchase price (or other deal terms)

Assessing the risks

Whether a target needs a network overhaul or could face legal action over a breach, the potential costs of security problems can be immense.

The practical concerns related to security problems at a target – such as the cost of fixing them and the implications for integration – are often the most pressing, according to our respondents. Exactly half of them said the cost of correcting existing problems topped their list of worries and 43% said future integration issues concerned them most.

The amount companies need to spend to close loopholes or overhaul networks can vary widely, depending on the size of the firm and the scale of the problem. But the cost can easily run into the hundreds of thousands of dollars, even for a mid-market company – and that's not counting

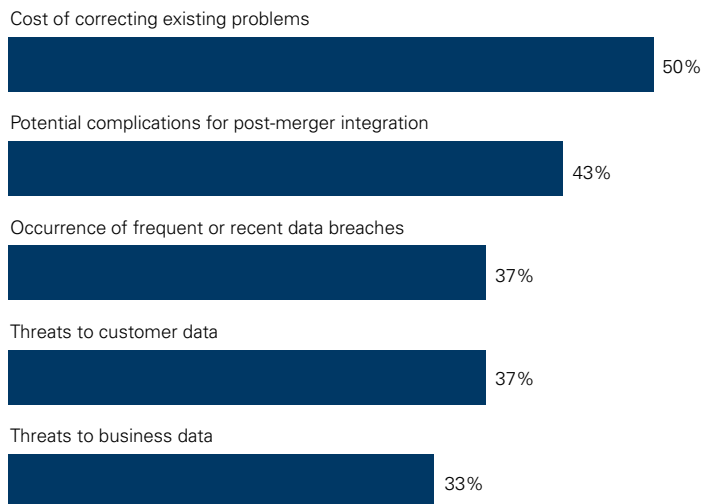
potential legal costs down the line. "Data security is no small thing to deal with," said a managing director at a PE firm with investments in over 20 countries. "There is the cost of correcting the existing problems, and then the firm could have unresolved litigation or lawsuits that could surface after the deal has closed."

More than a third of respondents (37%) said they are highly concerned about the occurrence of frequent or recent data breaches. According to West Monroe senior director John Stiffler, looking at a target's incident history provides valuable insight into its overall security posture. "One of the first things we do in the diligence process is to ask the potential acquisition about past breaches," Stiffler said.

Almost equally important is to look at the remedial action taken by the firm in response. In some cases, the "battle scars" of going through a breach can actually make a company strengthen its security policies, Stiffler said.

Thirty-seven percent of respondents said they especially worried about threats to customer data, while 33% said threats to business data concerned them. Many executives are well aware of the costs that accompany breaches, which become more likely if specific threats to corporate data are present. In the 2007 breach of Heartland Payment Systems, for instance, the cost in fines and legal expenses alone reached US\$150m, CEO Robert Carr said in 2014.

When it comes to cybersecurity issues at a target firm, what are your top concerns? (Select up to two)



The bottom line

A proper due diligence must look at the full gamut of risks: breach history, specific data threats, problems for integration, and the cost of potential fixes.

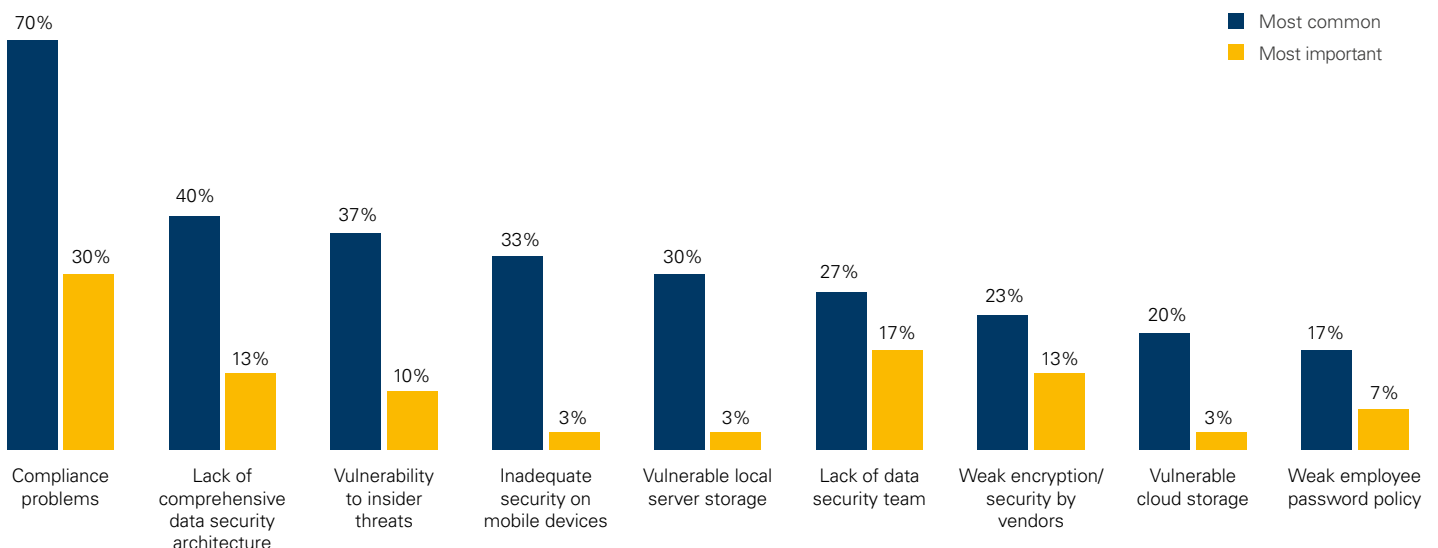
Compliance in focus

As privacy laws evolve quickly around the world, compliance issues are the most common and important problem uncovered at deal targets, our respondents said. Seventy percent named them as one of the most frequent data security issues and 30% called them the most important.

In the US, three federal agencies take responsibility for policing data privacy: the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), and now the Consumer Financial Protection Bureau (CFPB) as well. In a 2015 case, the US Court of Appeals for the Third Circuit ruled that the FTC could hold companies responsible for weak data security practices that lead to breaches. In an even more surprising case, the CFPB announced a settlement in March 2016 with payments startup Dwolla over privacy concerns – despite the fact that Dwolla had not even experienced a breach.

The scope of oversight appears to be growing in proportion to the scale of data being collected by most companies – and that scale is on the rise. “We have seen an increase in compliance issues due to the vast amounts of data within enterprise systems,” said a finance director at a software firm that makes fewer than five acquisitions a year. “Managing compliance effectively is a top concern, and most companies are seen as being in a weak position due to the magnitude of the data and the complexities of newer technologies.”

What are the most common and important types of cybersecurity problems uncovered at a deal target? (Select up to three most common and one most important)



Infrastructure red flags

Beyond broad agreement about the prominence of compliance issues, opinion was split among respondents regarding the most common and troublesome data security problems at targets. The concerns most commonly seen included the lack of a comprehensive data security architecture (40%), inadequate security on mobile devices (33%), and vulnerable local server storage (30%).

West Monroe's Matt Sondag explained the process of analyzing a company's security architecture with the analogy of looking at a person's home security. "When we look at a target's network setup, their firewalls, and their overall infrastructure topology, it's like looking at a house," he said. "We ask: Do you always lock your doors? Do you always put the alarm on? Do you always shut the windows? Do you always close the garage door?"

"By checking these issues, we can start to understand whether they have processes and procedures in place that will be there in the future and that will ultimately tell us whether a network is secure," Sondag added.

At the same time, an analysis must look beyond the overall infrastructure. "Application security, which includes internal access control, is also key," Sondag said.

In the realm of mobile security, new safeguards are becoming necessary, such as the ability to remotely wipe a phone or laptop. In the event a device is lost or stolen, fines can be reduced if you can prove that sensitive data was deleted.

Insider threats

Vulnerability to insider threats, cited by 37% of respondents as a common problem found at targets, is a mounting concern. A 2015 study by IT industry association CompTIA showed that a slight majority of security breaches (52%) result from employee action, whether malicious or unintentional, as opposed to outside attackers. "Internal systems that are not fully secured usually create the most challenges, since insider risks or threats can arise in the process," said the CFO at a mid-cap broadcasting company.

Interestingly, in terms of importance, the problem cited second-most by respondents was the lack of a data security team (17%). The CFO at a telecommunications company said locking down technical systems can prove challenging without properly trained IT personnel. "The lack of a dedicated team makes it difficult to ensure adequate specialization and effectiveness in managing security concerns," he said.

The bottom line

The stickiest problems at deal targets tend to be compliance concerns and an inadequate cybersecurity infrastructure.

"Internal systems that are not fully secured usually create the most challenges, since insider risks or threats can arise in the process."

CFO at a mid-cap broadcasting company

781

the number of data breaches at
companies in the US in 2015,
according to the Identity Theft
Resource Center

US\$3.79m

the average cost of a data breach
in 2015, according to a survey
commissioned by IBM



PE paying up

Private equity is taking heed of the potential for data security issues at portfolio companies.

The rise in cybersecurity concerns at companies is making them a hot topic in corporate and private equity boardrooms. As West Monroe's Matt Sondag explained, this is leading to some rare occurrences.

"I recently got a call from a private equity client who said that they wanted to do a cybersecurity analysis on four of their portfolio companies – and that they were going to pay for it themselves," Sondag said. "It's rather unique for a PE firm to pay for this, and it means that they are really concerned about it. Obviously, if there is any remediation to be done, the portfolio companies will pay for it themselves. But I think private equity firms are becoming more and more cognizant of the issue."

Hitting the escape button

If cybersecurity problems are especially severe at an M&A target, they can be deal-breakers.

In 2015, an Italy-based surveillance company called Hacking Team was breached. All it took for the person to break in was a single password of an unsuspecting engineer. His password? "PasswOrd." The infiltrator then planted a backdoor into the network, granting him permanent access to the company's systems. In the resulting breach, nearly 400GB of sensitive data was released to the public.

The Hacking Team intrusion demonstrates the dangers inherent in something as simple as a weak corporate password policy. Indeed, it can signal the presence of other vulnerabilities within the company that extend beyond cybersecurity. "A weak corporate password policy may be a sign of bigger issues within the company," said Sean Curran, director of West Monroe's Security & Infrastructure practice. "If basic policies don't exist and aren't enforced, what other exposures are there? More serious issues may exist, like unencrypted credit card data in their databases, and those will be deal killers."

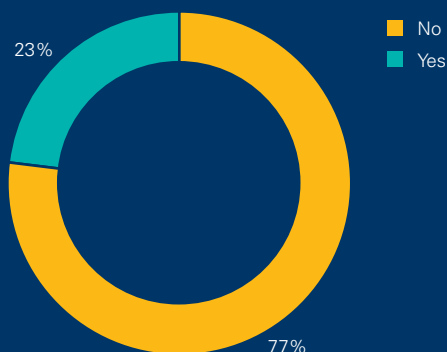
In the majority of cases, cybersecurity issues alone are not enough to cause a buyer to abandon an acquisition: 77% of our respondents said they have never walked away from a deal for that reason. Some respondents said they were able to avoid it by investigating a company's data security infrastructure in the targeting phase, before a preliminary purchase agreement had been signed. A vice president for strategy at a global medical products firm said they had adjusted the terms of a deal over cybersecurity concerns, but never cancelled a deal: "We have never walked away from a deal due to data security issues, although one deal process suffered turbulence because of security concerns. The deal timelines were affected and the deal value was also reduced."

When a company is deciding whether to make an acquisition, security problems can also indicate poor risk management at the target. "We noticed data security issues at one target firm that were not negligible and we preferred to walk away from the deal," said a managing director at a PE firm that primarily uses a buy-and-build strategy. "The volume of issues was an alarming signal of the risks the organization would face."

The bottom line

Cybersecurity risks aren't ending many deals during the current M&A boom, but they need to be better managed. And if buyers become more selective in their deal criteria, the importance of cybersecurity could rise further.

Have you ever walked away from a deal due to data security issues at the target?



Good governance

High-tech software and qualified personnel are only part of the equation when it comes to effective data security.

You're starting the due diligence process at a potential acquisition and the initial signs are good. The target uses cutting-edge security tools, such as privilege identity management and endpoint detection and response software. The in-house security team is small (three people) but elite – each member has immaculate credentials. The team insists it can handle the security duties even as the company experiences rapid growth. In fact, they are so confident that they don't have all of the firm's security policies written down. Instead, they say, the policies are simply etched in their brains.

So – just how well protected is this company from cyber attacks? Its data and computer systems appear to be secure, but it's difficult to verify. The reason is that its security governance is weak. The individual elements of the security apparatus appear to be strong, and yet the infrastructure is fragile and vulnerable to sudden change.

“In reality, it doesn't matter how many tools you have and how good or bad they are if you're not actively managing the use of them and constantly adjusting your security program.”

Paul Cotter, Senior Data Security Architect, West Monroe

“In reality, it doesn't matter how many tools you have and how good or bad they are if you're not actively managing the use of them and constantly adjusting your security program,” said Paul Cotter, a senior data security architect at West Monroe. “No matter which security tools you have in place, the situation is going to degrade over time.”

Review and renew

Effective security governance is integral to a high-functioning cybersecurity strategy. Perhaps the most important aspect of effective governance is ongoing review and renewal, since best practices evolve quickly as technology changes and hackers seek to exploit open loopholes.

When scrutinizing a potential M&A target's security governance, several questions are important to answer. First of all, does the company have adequate policies and procedures in place? Then, how well are those policies documented? And finally, does the company actively review and manage its policies?

“Solid documentation of the infrastructure is key, since you can't assess the risk of a system if you don't know the details,” Cotter said. “The company needs a common understanding of what the environment looks like and how everything is linked together. They also need to know where the security controls are actually implemented, who manages them, and whether they are actively enforced.”

Relationship guidance

Another critical aspect of security governance is the management of vendor relationships – especially as companies increasingly turn to managed security service providers (MSSPs) to handle their data protection. Small, tight-knit security teams can be effective when a company has limited needs, but MSSPs are helpful for duties such as around-the-clock monitoring.

For security to be properly managed with an MSSP, communication between the MSSP and the company needs to be regular and substantive. The performance of the security provider must also be frequently re-evaluated.

“When we see a company leveraging an external vendor, we want to see a lot of documentation on how they’re managing that relationship, where the hand-off points are, and how specifically an incident gets escalated,” Cotter said. “If one of these service providers finds a problem, how does it get escalated to the target’s internal resources?”

After a deal is completed, it’s important to remain vigilant about the acquisition’s security policies – especially if the firm is not being fully integrated with the acquirer, as with a private equity purchase. Over time, the security systems vetted during due diligence will require periodic checking and updating.

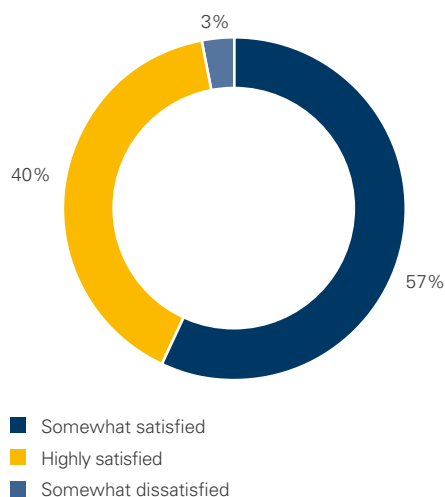
The bottom line

How a company manages the procedures and policies for its cybersecurity system – its security governance – is just as important as the system’s level of technical sophistication.

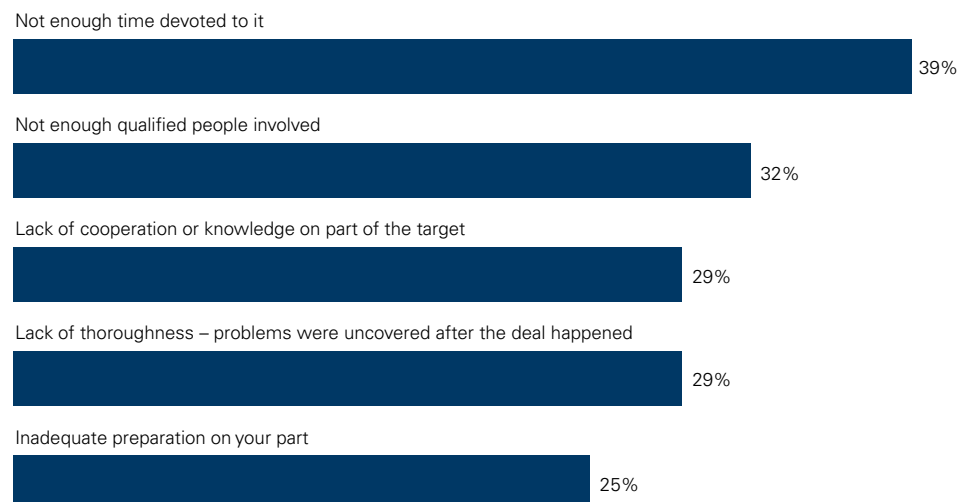
Evaluating the process

The history of cybersecurity risk essentially goes back as far as the Internet – meaning only about 25 years – and due diligence on data security is an even younger phenomenon. The process has advanced significantly as companies have become more cognizant of the risks that come with vulnerabilities, but problems remain.

Overall, how satisfied have you been with the cybersecurity due diligence conducted for recent deals?



What, if anything, did you find inadequate about the cybersecurity diligence process for recent deals? (Select up to two)



The vast majority of respondents in our survey have been highly satisfied (40%) or somewhat satisfied (57%) by the data security diligence in recent deals. Those who have been somewhat satisfied, however, cite a significant number of caveats in their evaluations of the process.

A managing director at a private equity firm that has completed more than 200 investments said the “information received was incomplete and the process took a longer period of time” than they had expected, adding that the missing information was “not negligible.” In a deal done by a managing director of a mid-market PE firm, the diligence process overlooked “issues like identity theft and intrusions in the internal systems.”

Out of time

In terms of specific inadequacies in the due diligence process, 39% of respondents explained that not enough time had been devoted to it and 32% said it lacked a sufficient number of qualified personnel. “Even the advisers we hired were not experts in the field – their market knowledge was way less than we had expected,” said the finance director at a healthcare technology firm.

One way to gauge the expertise of cybersecurity advisers is to look at what related services they offer. For instance, firms that regularly put in place data security fixes in addition to conducting M&A due diligence often have better awareness of the relevant red flags and best practices. “We conduct over 120 security diligences a year, but a large part of why we bring value to the diligence process is that we’re not just doing diligences all day long,” said Paul Cotter,

a senior data security architect at West Monroe. “The people we bring are practitioners who are implementing solutions in the field.”

A potentially more significant problem is a lack of cooperation or knowledge on the part of a target, cited by 29% of respondents as an inadequacy. “One recent target did not possess sufficient knowledge or experience with the things that were required for a deal,” said the CFO at a mid-cap telecommunications firm. “There were delays in the procedure due to the lack of thoroughness. In spite of the planning done, the deal faced a lot of problems due to the target company’s inefficiency.”

The bottom line

It is vital to have an experienced and well informed team carry out diligence on data security issues. Otherwise, major problems can be overlooked.

“A large part of why we bring value to the diligence process is that we’re not just doing diligences all day long. The people we bring are practitioners who are implementing solutions in the field.”

Paul Cotter, Senior Data Security Architect, West Monroe



Limiting liabilities

Typically, when you buy something like an old house or a used car, you can't take out insurance that will reimburse you if you uncover a problem after the purchase goes through. But with M&A targets, you can – the prevalence of transaction insurance is on the rise, including for cybersecurity risks. US insurer Marsh calculated that policy limits it placed in 2015 rose by 45% year-over-year, reaching a record level of US\$11.2bn.

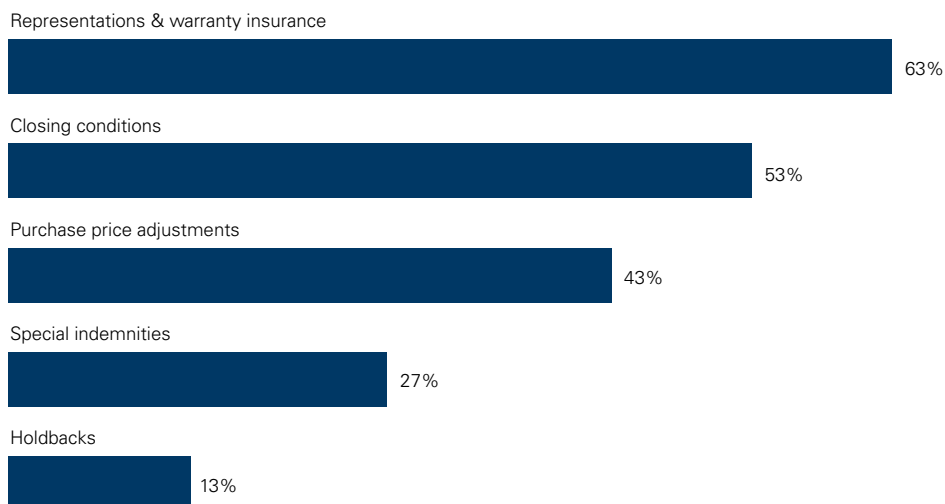
Nearly two-thirds of respondents (63%) said representations & warranty insurance is among the most important protections in mitigating data security risk, while over half (53%) said closing conditions are vital. The head of one private equity firm's healthcare division said representation & warranty policies are especially useful because they are flexible in scope. "The most favorable special protections for mitigating data security risks are representations & warranty insurance, as this is highly customized coverage for a specific transaction, with a specific set of values," he said.

A managing director at a PE firm with more than US\$2bn in annual revenue said closing conditions are ideal for accomplishing the task of tailoring coverage to a deal. "Every organization and each data breach has unique risk factors based on the industry, the relevant regulatory concerns, the customer base, and technical circumstances," the PE managing director said. "To reduce the likelihood of a data breach, we believe it is important to understand the specific risks and address them before a breach occurs. Due to this, we feel the special protections that are most important in mitigating data security risks are closing conditions, which must specify the required measures."

The bottom line

As with other potential liabilities in an M&A deal, acquirers need to make sure they have protections in place against cybersecurity risk.

What kinds of special protections are most important in mitigating cybersecurity risks in dealmaking? (Select up to two)



Unpleasant discoveries

It's every acquirer's worst nightmare: you've spent countless hours vetting an M&A target, and after the deal goes through, you catch something.

The target had data security vulnerabilities that no one spotted during due diligence. This unfortunate turn of events is relatively common, according to our survey results: 40% of respondents said they had discovered a problem after a deal went through.

Undisclosed data breaches, inadequate security frameworks, and vulnerable cloud storage were among the issues found by respondents after concluding deals. In the case of one acquisition, a managing director at a media and communications-oriented PE firm said they uncovered extensive problems after the purchase. "There was a data security problem at one past target related to the number of users involved in handling data," the PE managing director said. "We conducted an investigation and found that data had been exposed to intrusions by insiders as well as outsiders. There was no proper security framework adopted by the acquired company and they lacked a dedicated security system."

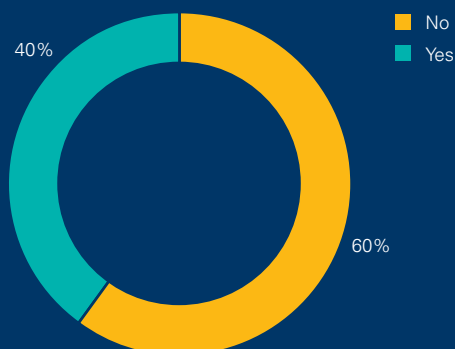
Another respondent, a CFO at a B2B software firm, said that undiscovered cybersecurity problems at an acquired company "cost [them] heavily." He said they had to spend a "fairly high amount of capital" to rectify the situation.

The costs associated with security issues found post-deal can extend beyond the resources needed to fix them; legal liabilities can enter the picture as well. In 2010, Disney bought a company called Playdom, a developer of online social network games, for US\$563m. After the deal went through, the FTC alleged that Playdom had broken privacy protection rules for children and Disney ended up paying a US\$3m settlement over the case.

The bottom line

The prevalence of security problems post-deal indicates that diligence standards remain low. If you're hiring advisers, make sure the firm you choose is equipped to do the job well.

Have you ever discovered a data security problem in an acquisition after the deal went through?



Integrating data

The priorities of cybersecurity diligence depend in part on a company's integration plan for the target. In the case of a technology company making a data-centric acquisition – for example, IBM buying data firms to improve its Watson artificial intelligence product – the new information will need to be closely integrated. On the other hand, healthcare companies buying sensitive medical data may want to limit their potential liability by keeping a firm's data outside their own system.

In many cases, the situation is not so black-and-white. A majority of our survey respondents (56%) said they prefer a combination of securely integrating select data from the acquired firm while keeping some isolated at the target. Thirty-seven percent said they preferred to integrate the new data securely into their own system, while 7% said they tended to leave it separate.

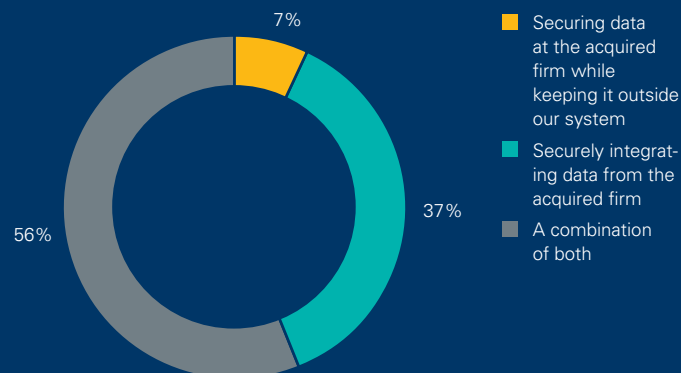
Many respondents said they brought data from acquired firms into their own systems in order to assess it properly, both in terms of value to the company and security vulnerabilities. "Our preferred method for treating the data acquired from a target firm is to securely integrate it into our systems and study the operations, standards and parameters of it," said a large-cap healthcare provider. "This gives us an exact picture of the drawbacks in the data security, which in turn helps us prioritize future requirements."

One respondent, the director of M&A at a major technology company, said they customize their approach to data integration for each individual case. "Our preferred method of data integration highly depends on the nature of the deal," he said. "In most cases, we prefer integrating data from the acquired company within our own data warehouse. This gives us the advantage of securing the acquired data in our own security environment and helps us to reduce redundancies and save on data storage costs."

The bottom line

There's no one right answer when it comes to data integration. Ultimately, it should depend on the nature of the deal.

In the post-merger integration phase, what is your preferred method for treating data from the acquired firm?



Conclusion

In 2015, reports began flowing in of cyber attacks targeting a new industry: hotel chains. Hilton, the Trump Collection, and Starwood Hotels & Resorts all confessed that their payments systems had been accessed by hackers. The revelations led one security expert to argue that potential buyers of Starwood should examine the issue closely. “They need to conduct a compromise assessment of the entity that they are going to acquire — what malware is already living in Starwood?” Tom Kellermann, chief cybersecurity officer at Trend Micro, told the Financial Times. “Is the target already diseased?”

The reality of the modern business environment is that every sector has become vulnerable to cybersecurity problems. Virtually all acquirers must implement a rigorous diligence process when considering M&A targets. The nature of cyber threats is also changing constantly, requiring a nimble approach to due diligence. As security concerns evolve, make sure that your diligence procedures evolve with them.



Companies are starting to appreciate the importance of data security in M&A.

They are committing greater resources to the process. However, they often struggle to find the right talent to do it properly. As cybersecurity becomes a crucial issue, acquirers must sharpen their diligence.



Data security isn't derailing deals.

It's just another risk that needs to be managed – similar to financial risk, IT risk, and operational risk. At the same time, it is very much an emerging discipline, making it vital to partner with the right type of firm in order to attain full value in a deal.



Security is more than fancy tools.

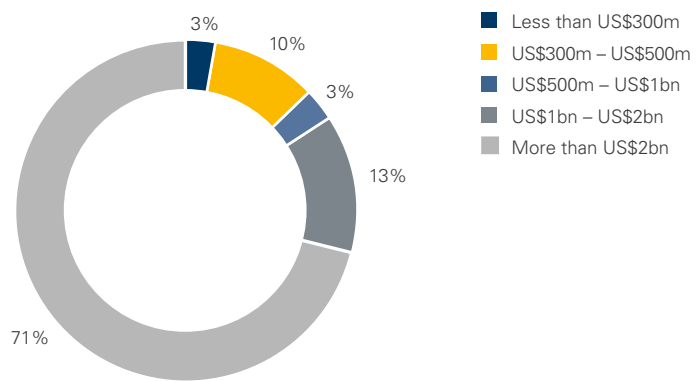
A target firm needs to have codified security policies and a strong IT team in addition to the latest software. The company's entire security ecosystem must be closely examined and evaluated in the deal process.

Appendix: Respondent profiles

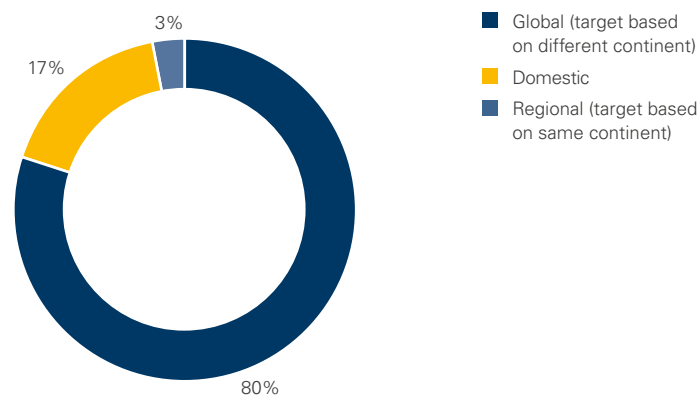
Our report surveyed a diverse group of 30 senior executives at corporates and private equity firms that frequently conduct M&A transactions and where data security is a paramount concern, in order to better understand how they prepare for and perform due diligence on cybersecurity at target companies. More than two-thirds of our respondents (71%) are large-cap companies, with revenues of over US\$2bn per year.

The M&A tendencies of the respondents vary. Fifty-three percent have made fewer than five acquisitions in the last three years, 27% have made 5-10, and 20% are more active, with more than 10 acquisitions. The value of their acquisitions also covers a wide range, although almost half (47%) said their last purchase cost less than US\$300m. Eighty percent said they do not target a specific size of company in terms of revenue.

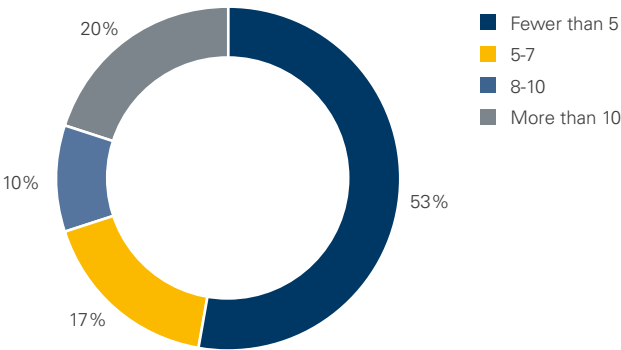
What is your company's annual revenue?



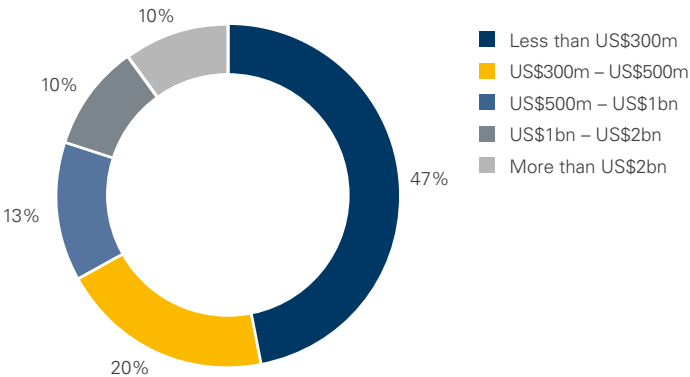
In terms of geography, how would you categorize your most frequent transactions?



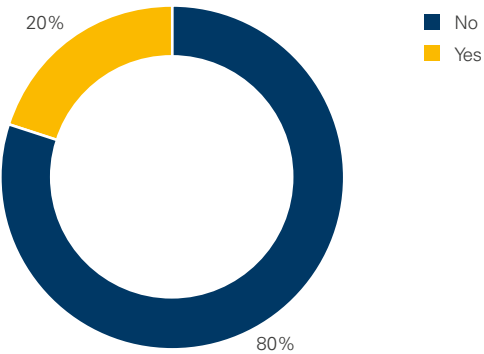
How many acquisitions have you completed in the last 36 months?



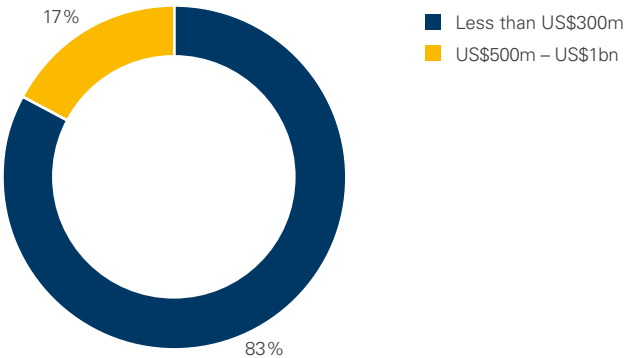
What was the value of your last acquisition?



Is there a certain size of company in terms of revenue that you target for acquisition?



If so, what is the typical range?



Cybersecurity policies

Nine out of 10 respondents (90%) said their companies have a data security framework in place, but there is a split when it comes to the personnel responsible for fulfilling security tasks. Sixty percent have a dedicated in-house team, while 50% said they outsource the functions to a third party – often, they said, in order to save on cost.

In recent years, most companies' IT budgets have represented about 4 to 6 percent of revenue, according to research by *CIO*, and security can be a significant portion of that budget. The cost-savings of using third-party firms, particularly in foreign countries, can therefore be attractive. "We have outsourced our data security resources to a third party, and the primary reason is to control operating costs and enhance risk management," said a managing director at a diversified, large-cap private equity firm. "We are able to derive the benefits of lower labor costs in certain countries, while maintaining a high level of quality."

Generally, a split can be seen between corporates and PE firms when it comes to data security resources. Among our respondents, 93% of corporates have a dedicated security team, while 80% of PE firms outsource their data security functions. There is, however, near-universal agreement regarding the importance of maintaining a security framework. "We have a data security policy that has been signed by all the employees, including top management, and everyone is made aware of the way data should be handled," said a senior finance director at a global media and entertainment company. "Hence, we have been able to avoid data breaches."

"We have outsourced our data security resources to a third party, and the primary reason is to control operating costs and enhance risk management."

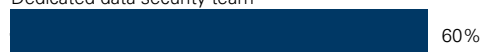
Managing director at a large-cap PE firm

What kinds of cybersecurity resources does your company have? (Select all that apply)

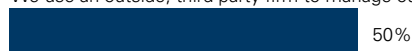
Data security policy/framework



Dedicated data security team



We use an outside, third-party firm to manage our data security



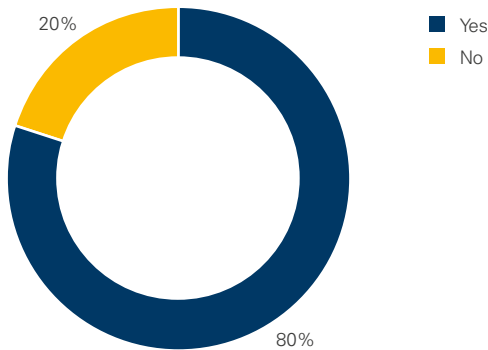
Dealmaking strategy

For 80% of our survey respondents, a transaction must be accretive to complete it. The methods used by respondents to verify the synergy model vary, however. Eighty-three percent employ a third party to validate it using a quality-of-earnings analysis, while 50% verify it with the board's finance committee and 25% check it with the CFO or controller. Just under one third of respondents (29%) also ensure that the deal sponsor is held accountable for the model.

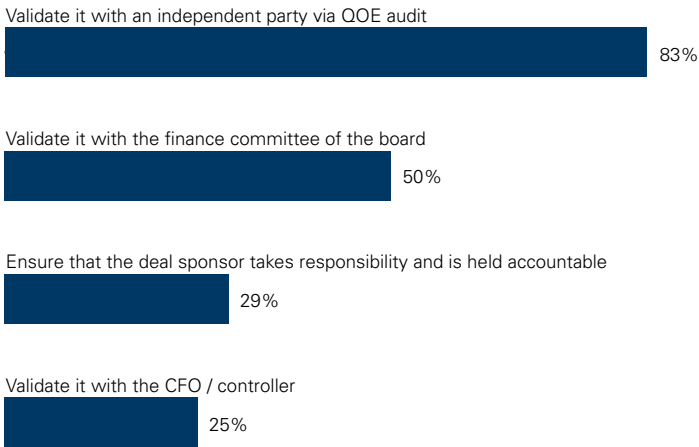
Many of the respondents noted that third-party audits are important because they provide an unbiased view of the target's financials. "A transaction definitely has to be accretive in order for us to complete it," said a senior finance director at a technology company. "For this reason, we prefer validating it with an independent third party and also with the finance committee of the board. With both parties being involved, there is less chance of any wrong moves being made, and the QOE audit committee will not favor any of the parties."

A vice president for strategy at a healthcare firm said they entrust the finance committee with the role of testing the synergy model, since it has all the necessary information to do the job. "We make sure that a transaction is accretive – it is important to improve shareholder value," he said. "The finance committee plays the most important role when authorizing and testing the synergy model, as they have access to the data and tools that are vital in making decisions about the transaction process."

Does a transaction have to be accretive in order for you to complete it?



If so, what steps are taken to test the synergy model? (Select up to two)





125
clients

900
deals

\$130b
value

We tackle the complexities of M&A across the transaction lifecycle – from strategy, analysis and planning through integration and optimization.

About Mergermarket



MERGERMARKET

Mergermarket is an unparalleled, independent mergers & acquisitions (M&A) proprietary intelligence tool. Unlike any other service of its kind, Mergermarket provides a complete overview of the M&A market by offering both a forward-looking intelligence database and a historical deals database, achieving real revenues for Mergermarket clients.



Remark, the events and publications arm of The Mergermarket Group, offers a range of publishing, research and events services that enable clients to enhance their own profile, and to develop new business opportunities with their target audience.

To find out more, please visit:

www.mergermarketgroup.com/events-publications

For more information, please contact:

Katy Cara

Sales Director, Remark

Tel: (646) 412-5368



A TEAM

LIKE NO OTHER

Contacts

Paul Cotter
Senior Architect, Security & Infrastructure
312.846.9974
pcotter@westmonroepartners.com

Sean Curran
Director, Security & Infrastructure
312.386.6195
scurran@westmonroepartners.com

Tom Ewers
Managing Director, Mergers & Acquisitions
612.594.8001
tewers@westmonroepartners.com

Matt Sondag
Managing Director, Mergers & Acquisitions
312.980.9446
msondag@westmonroepartners.com

John Stiffler
Senior Director, Mergers & Acquisitions
312.980.9427
jstiffler@westmonroepartners.com

BUSINESS
CONSULTANTS

DEEP
TECHNOLOGISTS

www.westmonroepartners.com