FORESCOUT

THE ROLE OF CYBERSECURITY IN MERGERS AND ACQUISITIONS DILIGENCE

A research study to better understand the cybersecurity risks companies face while acquiring another company.

PURPOSE OF THE STUDY

This study was designed to examine the growing concern of cyber risks and the importance of cyber assessment during mergers and acquisitions (M&A) and determine how well companies are prepared to deal with cyber risk during M&A from the perspective of IT Decision Makers (ITDMs) and Business Decision Makers (BDMs).

Are key decision makers concerned about cyber during an acquisition? What factors are considered as part of the due diligence and evaluation process before, during and after acquisition? Do cyber incidents lead to delays in acquisition? What does cyber risk mean for companies looking to acquire? How can they best protect themselves during this important process to minimize risk and protect their companies? This report explores these questions and others, and provides recommendations for effectively managing cybersecurity risks during an acquisition.

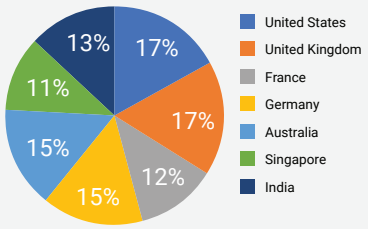
This research and report was commissioned by Forescout Technologies with respondents sourced from Quest Mindshare.

ABOUT THE STUDY

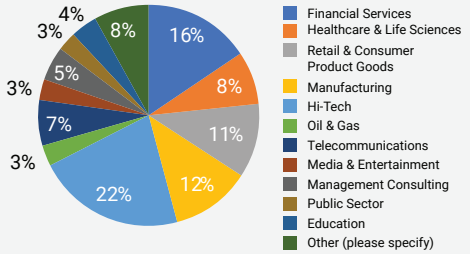
This report is based upon a survey conducted from February 20 through March 10, 2019, and was commissioned by Forescout Technologies with respondents sourced from Quest Mindshare to better understand cyber risk within the M&A lifecycle. There were a total of 2,779 respondents from around the globe. Two audiences were chosen for this study: IT Decision Makers (ITDMs; n=1283) and Business Decision Makers (BDMs; n=1496). The data was weighted to evenly represent audiences and regions. To qualify, respondents had to be employed full-time, senior manager level or higher, and the primary decision maker for IT purchasing decisions or involved in M&A strategy. The survey was conducted in the United States, France, United Kingdom, Germany, Australia, Singapore, and India. The margin of error is +/- 1.73 percentage points.

Percentage of Respondents

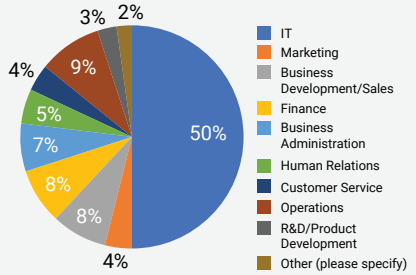
Country



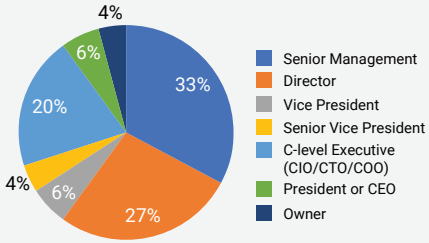
Primary Type of Business



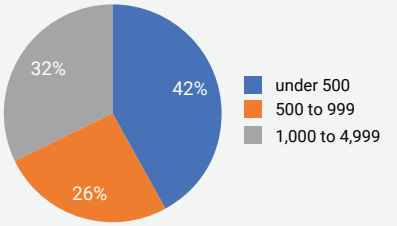
Job Function



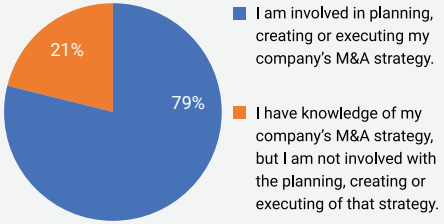
Job Level



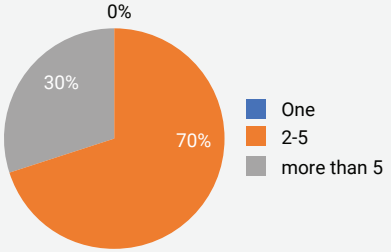
Number of Employees

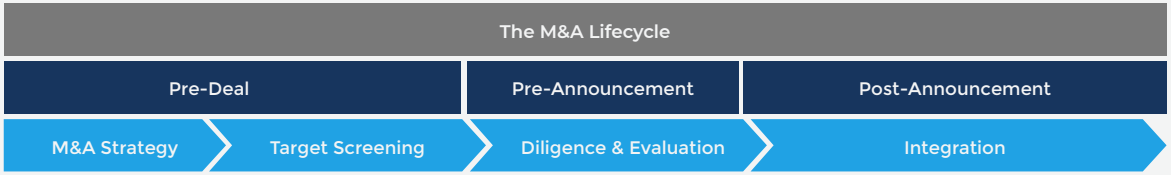


Level of Involvement



Number of M&As involved with





EXECUTIVE SUMMARY

By 2022, Gartner reports that 60% of organizations engaging in M&A activity will consider cybersecurity posture as a critical factor[1] in their due diligence process, up from less than 5% today. In our survey of 2,779 IT and business decision makers from around the globe, 73% of respondents agreed that technology acquisition is their top priority for their M&A strategy over the next 12 months—and, 62% agreed that not only does their company face significant cybersecurity risk by acquiring new companies, they also expressed that cyber risk is their biggest concern post-acquisition.

While the companies in a deal may honor clawback clauses, malware has no bounds. Once you're connected, bad actors will have free reign unless you take appropriate, preemptive action.

Cybersecurity risk is a growing challenge and concern for a number of reasons. Human error is an age-old network compromise culprit, with human negligence and innate curiosity often cited as main reasons[2] for a security incident or data breach. However, the IT and cyber landscape have changed dramatically in recent decades, bringing both technical advances and new risks. The birth of the Internet of Things (IoT) has altered the way people live and communicate, and with the number of IoT devices anticipated to surpass 20.4 billion by 2020[3], it's also requiring innovative approaches to managing IoT cyber risks. In our survey, 72% of respondents considered IoT devices (printers, smart lighting, VoIP phones, security cameras, etc.) as most vulnerable to external adversarial actors. IoT devices have also played a role in the ongoing convergence of traditional IT with operational technology (OT), potentially exposing operational networks that were previously much harder to attack.

There's been a myriad of changes and advancements in recent years, but the increased connectivity has also presented more opportunities for adversaries to launch malicious attacks, steal data or intellectual property, or attempt to disrupt a business or economy. All of these factors have greatly complicated the evaluation and decision making process for ITDMs and BDMs when it comes to M&A. Not only do they present unique cyber risks that must be evaluated, but those risks are also hard to evaluate because many assets aren't tracked via asset inventory. A hurried, uninformed, or

M&A Strategy over the next 12 months

73%

agreed that technology acquisition is their top priority for their M&A strategy over the next 12 months

62%

agreed their company faces significant cybersecurity risk acquiring new companies, and cyber risk is their biggest concern post-acquisition.

[1] *Cybersecurity is Critical to the M&A Due Diligence Process, Gartner,* April 2018, https://www.gartner.com/en/documents/3873604

[2] *The biggest cybersecurity risk to US businesses is employee negligence, CNBC,* June 2018, https://www.cnbc.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html

[3] *8.4 Billion Connected "Things" Will be in Use in 2017,* Gartner, February 2017, https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

scope-limited evaluation can have very real financial implications for both the company being acquiredd as well as the acquiring company, as evidenced by the $350 million acquisition price cut[4] following Yahoo's security breach disclosures, as well as the $1.5 million data breach settlement[5] retailer Neiman Marcus had to pay, even though acquisition had already closed.

M&A diligence has traditionally focused on Finance, Legal, Business, Operations, Human Resources and IT, among others. Our survey findings suggest that although there is recognition of potential cyber risks during an acquisition, organizations considering an acquisition could benefit from greater, dedicated cyber evaluation. Our findings also suggest that evaluation and due diligence shouldn't just be a point-in-time exercise; cybersecurity due diligence and risk assessment should be an ongoing activity. While it should be continuous, acquiring companies can only go so far in their investigations and due diligence processes—so inherently, there's a certain amount of risk in any acquisition. You never truly know what you have until you're connected—and that makes it that much more important to evaluate as much as you can as thoroughly as you can prior to integration. While the companies in a deal may honor clawback clauses, malware has no bounds. Once you're connected, bad actors will have free reign unless you take appropriate, preemptive action.

[4] *Verizon cuts Yahoo deal price by $350 million*, CNN, February 2017, https://money.cnn.com/2017/02/21/technology/yahoo-verizon-deal/index.html

[5] *Neiman Marcus to pay $1.5M settlement over 2013 data breach, RetailDive*, January 2019, https://www.retaildive.com/news/neiman-marcus-to-pay-15m-settlement-over-2013-data-breach/545641/

KEY FINDINGS

- **Cybersecurity issues are prevalent and can put a deal into jeopardy:** Over half of respondents (53%) report their organization has encountered a critical cybersecurity issue or incident during an M&A deal that put the deal into jeopardy.
- **Organizations are placing more focus on a target's cybersecurity posture than they did previously:** Eighty-one percent of ITDMs and BDMs agree that they are putting more of a focus on a target's cybersecurity posture than in the past, highlighting that cyber is a top priority for both IT and business decision makers.
- **An undisclosed data breach is a deal breaker for most companies:** Seventy-three percent of respondents agreed that a company with an undisclosed data breach is an immediate deal breaker in their company's M&A strategy.
- **Decision makers sometimes feel they don't get enough time to perform a cyber evaluation:** Only 36% of respondents strongly agree that their IT team is given time to review the company's cybersecurity standards, processes and protocols before their company acquires another company.
- **Internal IT teams may lack the skills to conduct cybersecurity assessments:** Among ITDMs, only 37% strongly agree that their IT team has the skills necessary to conduct a cybersecurity assessment for an acquisition.
- **Organizations allocate third party resources to their cybersecurity assessments:** Nearly all respondents (97%) reported that their organizations spend money on outside contractors for IT audits or cybersecurity risk assessments.
- **Connected devices and human error put organizations at risk:** When asked what makes organizations most at risk during the information and technology process, two answers stood out: human error and configuration weakness (51%) and connected devices (50%).
- **Devices often get overlooked and missed during integration:** Over half (53%) of ITDMs say they find unaccounted for devices after completing the integration of a new acquisition.
- **Failure to address cyber risk can lead to major acquisition regrets:** Nearly two-thirds of respondents (65%) said their companies experienced regrets in making an M&A deal due to cybersecurity concerns.

CURRENT CYBER RISK LANDSCAPE IN M&A

Cyber issues are prevalent and can put a deal into jeopardy:

53%

Fifty three percent of respondents report that their organization has encountered a critical cybersecurity issue or incident during an M&A deal that put the deal in jeopardy.

US	UK	FR	DE	AUS	SG	IN
47%	52%	61%	56%	40%	50%	63%

Companies merge or acquire other companies for a myriad of reasons—more efficiencies, access to a larger market, unique intellectual property or competitive advantages, or influence over supply chains, to name a few. Whether the acquisition is a conglomerate, a market or product acquisition, or a horizontal or vertical merger, there's typically a diligence and evaluation process that spans Financial, Legal, Business, Operations, Human Resources and IT.

This process allows for proper disclosure and assessment of risk. Yet, even during small mergers, the number of contributing factors in risk and the decision making process is extraordinary. And, the growing number of cyber risks only further complicates the matter—the assessment of a company's digital assets requires the inventorying of the nearly invisible materiality of a bad cyber history. Given that complexity, then, it's not surprising that over half of respondents (53%) reported their organization encountered a critical cybersecurity issue or incident during an M&A deal that put the deal into jeopardy. Additionally, the survey revealed that:

- IT decision makers were more likely to report that their organizations had encountered a critical, jeopardizing incident (57%) compared to business decision makers (48%).
- Respondents in France (61%) and India (63%) report the highest levels of encountering a cybersecurity issue or incident.
- Larger companies (5,000 or more employees) (59%) and mid-sized companies (1,000 to 4,999 employees) (56%) also encountered cybersecurity issues more often than smaller companies of less than 1,000 employees (49%).

Our findings suggest that the higher the number of mergers and acquisitions an individual is involved with, the more likely they are to report their organization had encountered a critical cybersecurity issue or incident that put an M&A deal in jeopardy.

- Respondents in High-Tech (57%) and Financial Services (56%) are also more likely to have encountered a cybersecurity issue or incident than other sectors.
- Individuals that had been involved with more than five mergers were more likely to say their organization had encountered a critical cybersecurity issue or incident that put an M&A deal in jeopardy (60%) compared to respondents who had been involved in two to five mergers (43%).
- Respondents from more mature organizations that utilize more controls to mitigate cybersecurity risk were less likely to have encountered an issue or incident (46%) indicating that controls may play an important part in reducing cybersecurity risk.

Individuals that had been involved with more than five mergers were more likely to say their organization had encountered a critical cybersecurity issue or incident that put an M&A deal in jeopardy

60%

Individuals involved in two to four mergers

43%

Individuals involved with more than five mergers

DILIGENCE & EVALUATION

Organizations are placing more focus on a target's cybersecurity posture than they did previously:

81%

Eighty one percent agree that they are putting more of a focus on a target's cybersecurity posture than in the past.

US	UK	FR	DE	AUS	SG	IN
84%	77%	79%	72%	73%	85%	94%

Assessing Cyber Risk in M&A Diligence

Nearly all respondents (93%) indicated they view cybersecurity evaluations as important to their company's M&A decision making.

Unsurprisingly, when asked to rank the importance of a cyber evaluation as very important, important, somewhat important, or not important, more ITDMs viewed cybersecurity evaluations as very important (71% vs 64% of BDMs), but it is worth noting that both audiences see these evaluations as an important part of their company's M&A process.

acquisition have become increasingly important priorities for acquiring companies. Seventy-nine percent of respondents indicate digital strategy is a top priority over the next 12 months and 77% indicate technology acquisition is a top priority over the next 12 months.

Cybersecurity is playing a greater role in M&A strategy than it did previously, and it can even be a deal-breaker in certain circumstances.

Seventy-three percent of respondents agreed that a company with an undisclosed data breach is an immediate deal breaker in their company's M&A strategy.

Seventy-three percent of respondents agreed that a company with an undisclosed data breach is an immediate deal breaker in their company's M&A strategy.

Companies are very concerned with exposure to potential cybersecurity risks and 83% agree that they take a target's cybersecurity posture very seriously when conducting due diligence on possible M&A targets. What is more is that 81% also agree that they are putting more of a focus on a target's cybersecurity posture than in the past.

As the importance of digital transformation in business continues to grow, digital strategy and technology

Critical Due Diligence Factors

When asked what the most important factors were when their company performs its due diligence on M&A targets, respondents listed financial statements as most important. The second most important factor was history of cyber security incidents, as shown in the graphic to the right from most (1) to least (6) important. Cybersecurity incidents are very important in the minds of the people making the deals and conducting the due diligence process.

Results when asked: What are the most important factors when your company performs its due diligence on M&A targets? (listed in order of importance).

1. Financial statements
2. History of cybersecurity incidents
3. Competitive positioning
4. Outstanding litigation
5. Customer satisfaction scores
6. Cyber risk scores

However, while the history of cyber incidents ranks as number two in the list, it's important to consider how that history and potential threats are evaluated during the due diligence process.

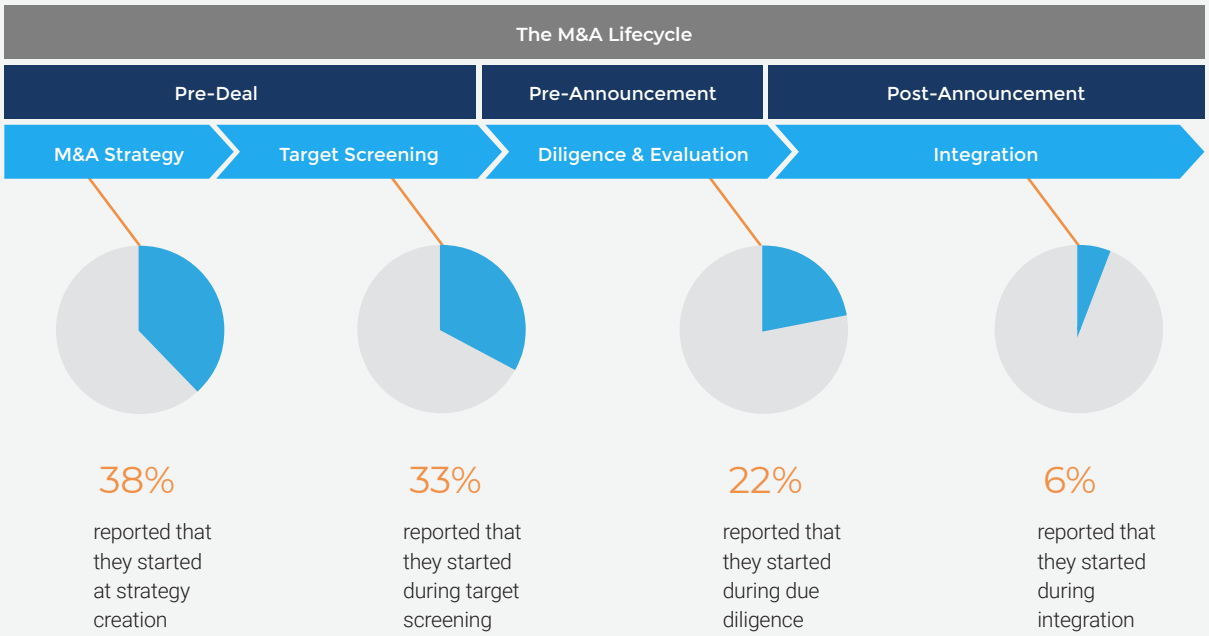
Conducting Due Diligence

M&A cyber due diligence usually includes both internal and external evaluations. Nearly all respondents (97%) indicated that their companies spend money on outside contractors and over half of respondents (57%) indicated that their company hires a Big 4 Auditor to conduct a cybersecurity assessment. And, 80% of respondents indicated that their company performed an internal in-depth inspection of IT-related systems and devices prior to completing an acquisition.

Those findings suggest that even though a Big 4 Auditor isn't always leveraged, most companies are at least performing an internal assessment or leveraging outside contractors for evaluations. But it's important to also consider the approach that's taken in performing due diligence and assessments.

Cyber assessments should be a major part of the acquisition evaluation process—not only at the point of integration, but throughout the entire acquisition. Yet, 6% of respondents reported that integration—the last phase of an acquisition—was the point at which cyber assessments began. Another 22% reported that they started during due diligence, 33% reported they started during target screening, and only 38% reported that they started at strategy creation—the very beginning of the acquisition process. Not only do these findings highlight very disparate views as to when cyber assessment should begin, but they

When asked at which phase cyber assessment occurs, respondents reported:



It is absolutely critical that the assessment of a target company's cyber posture and the evaluation of potential vulnerabilities start from the very beginning of the M&A process and continue through integration and post-integration.

Decision makers sometimes feel they don't get enough time to perform cyber evaluation:

36%

Only 36% strongly agree that their IT team is given time to review the company's cybersecurity standards, processes and protocols before their company acquires another company.

process. And, at any point, the target company's assets and devices could become vulnerable. Apart from continuous evaluation, it can be very difficult to develop and maintain a comprehensive view of cyber risks.

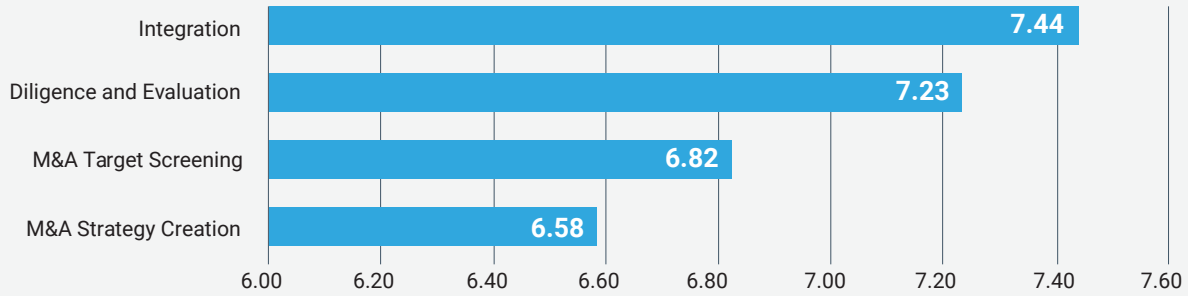
Interestingly, when ITDMs and BDMs were asked to rank their level of concern for cybersecurity risk during each phase of the M&A lifecycle process (strategy creation, target screening, diligence and evaluation and integration) on a scale of 1-10, there was more concern around integration (7.44), with less concern for the other three areas – diligence and evaluation (7.23), M&A target screening (6.82), M&A strategy creation (6.58).

systems (37%), patching practices (36%), and SIEM (27%). Organizations utilizing more of these processes and systems have more mature and developed cybersecurity risk M&A strategies than ones who use only one or two. These controls can play a very important role in managing and reducing cybersecurity risk.

Proper Evaluation Takes Time

In a world of increasing pressure to move quickly to complete an acquisition, time is of the essence. Well-executed deals are ones where diligence and prudence result in a successful acquisition with minimal-to-no

Results when asked to rank their level of concern for cybersecurity risk during each phase of the M&A lifecycle proceess.



also suggest that cyber assessment may be viewed by many as a point-in-time exercise. It is absolutely critical that the assessment of a target company's cyber posture and the evaluation of potential vulnerabilities start from the very beginning of the M&A process and continue through integration and post-integration. It's important to remember that even if the initial evaluation does not find any significant cyber risks, the target company will continue to operate—with current employees, customers, vendors and the connected world at large—throughout the M&A

For this exercise, 10 represents the highest level of concern and 1 the lowest level of concern. Again, cyber evaluation should span across the entire lifespan of the acquisition with importance placed on each phase.

In terms of the systems and processes M&A companies use to determine the level of risk during the diligence and evaluation phase, the most commonly used among ITDMs and BDMs are IT infrastructure and IT supply chain (54%), results from an internal IT cybersecurity audit (48%), and breach and security incident history (46%). The three least commonly used systems and processes were GRC

issues. Yet often we see an issue where ITDMs don't feel they get enough time. Only 36% strongly agree that their IT team is given adequate time to review the company's cybersecurity standards, processes and protocols before their company acquires another company. Although cybersecurity diligence may require more investment and time during the process by the acquiring company, a M&A that analyzes all the cybersecurity issues in advance is likely to have a better overall outcome and encounter fewer surprises along the way.

ASSET ASSESSMENT & INVENTORY

Internal IT teams may lack the skills to conduct cybersecurity assessments:

37%

Among ITDMs, only 37% strongly agree that their IT team has the skills necessary to conduct a cybersecurity assessment for acquisition.

US	UK	FR	DE	AUS	SG	IN
49%	30%	36%	28%	31%	31%	54%

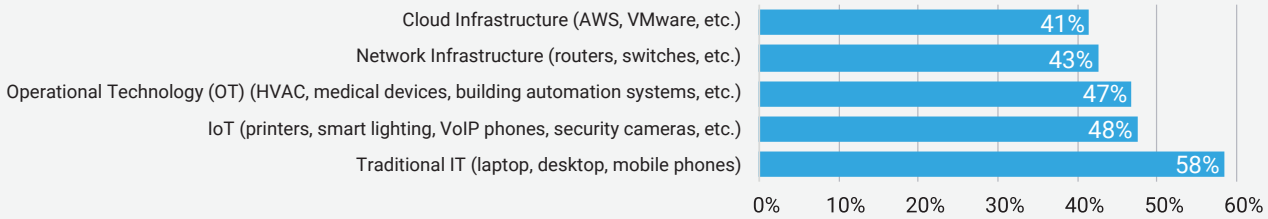
Devices Assessed

Complete asset inventory is an essential part of a sound defense strategy and the ability to gain visibility into what's on the network can enable timely action and response that can mitigate cybersecurity and operational risks. When companies look at assets, they should attempt to holistically examine everything that could be a potential vulnerability. Yet, despite the need for asset inventory and device assessment, the survey results indicate that respondents had varying perspectives on the importance of asset inventory across the five device categories: network infrastructure, IoT, OT, traditional IT, and cloud infrastructure.

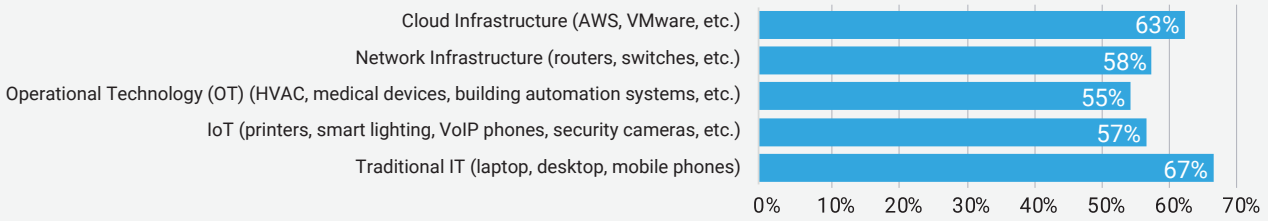
The survey findings suggest a misalignment between the devices and assets that are considered most vulnerable to external adversarial actors, and the devices and assets that are actually assessed as part of the new acquisition evaluation. For example, 78% of respondents considered network infrastructure (routers, switches, etc.) as most vulnerable to external adversarial actors; however, only 58% of ITDMs reported that network infrastructure was assessed as part of the new acquisition evaluation. Additionally, 43% of ITDMs reported that network infrastructure was most likely to be missed during asset inventory.

Similarly, 72% of respondents considered IoT devices (printers, smart lighting, VoIP phones, security cameras, etc.) as most vulnerable to external adversarial actors; however, only 57% of ITDMs reported that IoT devices were assessed as part of the new acquisition evaluation. Additionally, 48% of ITDMs reported that IoT devices were most likely to be missed during asset inventory.

When asked: Which assets are most likely to be missed during asset inventory?



When asked: What are the types of devices that your organization looks at when assessing the cybersecurity posture of a new acquisition integration?



With respect to operational technology, 73% of respondents considered OT as most vulnerable; 55% of ITDMs reported that OT was assessed, and 47% reported that OT assets were most likely to be missed during asset inventory. These findings reveal that even though there's considerable concern about asset and device vulnerability across traditional IT, OT, IoT, cloud infrastructure and network infrastructure, the measure of concern is not always equal with the level of action taken; and, consequently, there's also considerable concern about missing those devices and assets during inventory.

Based on these findings, it's clear that while asset inventory is viewed by decision makers as an important step in the evaluation process, asset inventory is often a struggle for acquiring companies during M&A.

Possible misalignment between devices and assets considered most vulnerable and those actually assessed as part of the evaluation:

78%
network infrastructure vulnerable

58%
network infrastructure assessed

43%
network infrastructure most likely missed

Devices often get overlooked and missed during integration:

53%

Fifty three percent of ITDMs say they find unaccounted for devices after completing the integration of a new acquisition.

US	UK	FR	DE	AUS	SG	IN
53%	49%	55%	60%	44%	57%	55%

Why Asset Inventory Is a Struggle

When asked if they felt their company's IT team was given adequate time to review the target company's cybersecurity standards, processes and protocols before acquisition, only 36% of ITDMs strongly agreed.

And, when asked if they felt their company's IT team had the skills necessary to conduct a cybersecurity assessment for any given acquisition, only 37% of ITDMs strongly agreed.

Not only do key decision makers feel that their companies' IT teams are often not given the appropriate amount of time to complete a pre-acquisition cyber assessment, but they also doubt the ability of their IT teams to perform such an evaluation. Given that, one would think that companies would be inclined to invest in an outside assessment. Yet, only 57% of ITDMs and BDMs reported that their company hired a Big 4 auditor to conduct a cybersecurity assessment.

Given these responses, it's unsurprising that 80% of ITDMs agreed that previously unknown or undisclosed cybersecurity-related issues were always uncovered during integration with the acquired company's technologies.

While this survey does not provide specific insight into the volume of missed devices by category, more than half (53%) of ITDMs say they find unaccounted for devices after completing the integration of a new acquisition. The most commonly found devices are traditional IT (laptop, desktop, mobile phones), followed closely by IoT and OT devices. The responses suggest that a significant portion of connected devices are not accounted for before an acquisition occurs. Traditional IT devices are often the easiest devices to locate and track. IoT and OT devices may also be unaccounted, as these devices are often smaller (e.g., sensors are small and hard to detect physically), and other OT devices sometimes run legacy software or obsolete hardware, making them harder to detect and patch. And, organizations sometimes lack the tools necessary to comprehensively identify and track every single connected device. Regardless of the volume of unaccounted devices, anytime a device is overlooked, it's not a surprise when a company inherits cyber risk—because they don't really know what they're inheriting.

Opportunity for Compromise

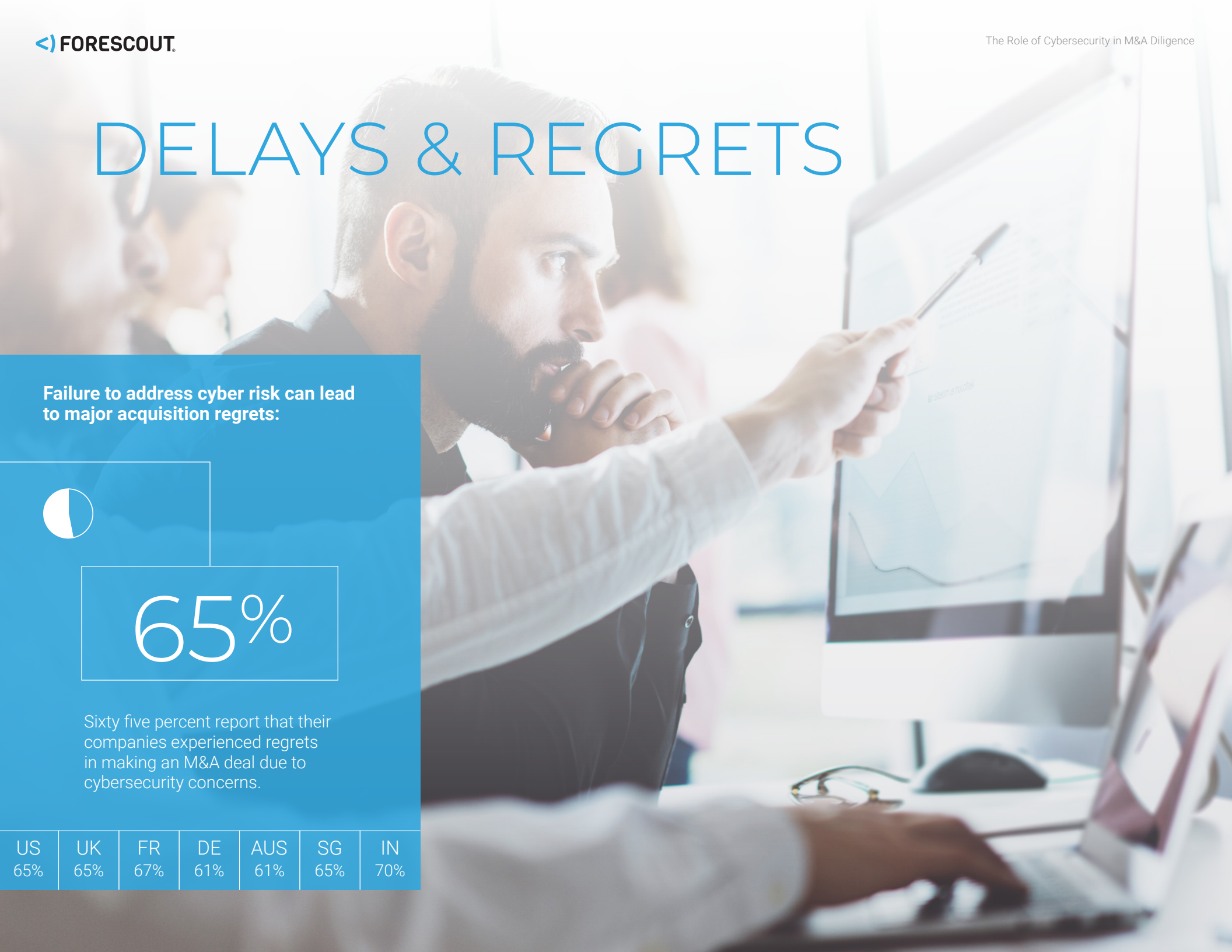
In terms of the volume of devices, on average, 43% of respondents reported that their companies find less than 10,000 connected devices while taking inventory of an acquiring company. Larger companies deal with even more devices with 23% of respondents reporting that their companies find over 500,000 or more devices. What that means is that there are often thousands of devices being acquired as part of an acquisition—devices which may be patched and secure or rogue and rife with malware. And, when you consider that more than half of ITDMs report additional, unaccounted for devices post-integration, the opportunity for compromise or malicious activity becomes evident. All it takes is one bad device to compromise a network.

The Biggest Risk Factors

In our research study, respondents were asked what put their companies most at risk during the information and technology integration process of acquisition. Three answers stood out: human error and configuration weakness (51%), connected devices (50%), and data management and storage systems (49%).

The human factor is a challenge that extends beyond M&A—it's commonly cited as the source of compromise: an insider threat, an unintentional data leak, or an inadvertent malware download via a phishing email are only a few ways that users commonly compromise company networks. Training and incentive or disciplinary programs are commonly used methods of reducing human error.

DELAYS & REGRETS



Failure to address cyber risk can lead to major acquisition regrets:

65%

Sixty five percent report that their companies experienced regrets in making an M&A deal due to cybersecurity concerns.

US	UK	FR	DE	AUS	SG	IN
65%	65%	67%	61%	61%	65%	70%

Acquisition Timeline Delays

An organization's timeline, resources and operations can be subject to change, especially in mergers and acquisitions. Just under half (49%) of respondents say they encountered unknown or undisclosed cybersecurity incidents, issues or risks when integrating the acquired company's information and technology that delayed the integration timeline.

These setbacks can cause time delays or monetary losses, both of which can damage the organization and its M&A strategy. Respondents were asked about time delays of less than and more than six months and losses of value of less than and more than $1 million. Over half of respondents (54%) listed a minor delay (less than six months) as a consequence and half (50%) listed a major delay (more than six months) because of a cybersecurity incident. Twenty two percent of respondents listed a loss of value of less than $1 million and only five percent of respondents listed a loss of value of more than $1 million.

Multiple factors can contribute to these delays and costs, but companies can reduce the risks by involving IT decision makers early in the process and by giving them the necessary time and tools to execute their jobs well. And, often, those decision makers will see the need for more invovlvement. In fact, 35% of IT decision makers also feel they need to be more involved with the M&A process at their companies.

Respondents were asked about time delays of less than and more than six months and losses of value of less than and more than $1 million.

54% minor delay (less than six months)

50% major delay (more than six months)

22% loss of value of less than $1 million

5% loss of value of more than $1 million

> Just under half (49%) of respondents say they encountered unknown or undisclosed cybersecurity incidents, issues, or risks when integrating the acquired company's information and technology that delayed the integration timeline.

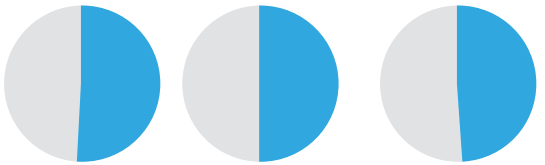
Acquisition Regrets & Issues

Nearly two-thirds of respondents (65%) said their companies experienced regrets in making an M&A deal due to cybersecurity concerns.

Twenty-one percent said their company had experienced major regrets and 44% say their company experienced some regrets, while 35% of respondents said their company has never experienced any regrets.

When asked about the nature of their regrets, many respondents reported cyber-related incidents or issues. The greatest number of references were around lacking due diligence or research, loss of time or money, and breaches or cybersecurity attacks. When asked what they wished their company had done differently, respondents often reported that they wished their company had hired a third-party vendor to check cybersecurity or done greater due diligence. Many added that they wished their companies had spent greater time or less money on the actual purchase or transaction. Examples include:

What put companies most at risk during the information and technology integration process of acquisition.



51% human error and configuration weakness

50% connected devices

49% data management and storage systems

"I think my company wishes it had been more proactive concerning risks surrounding lack of cybersecurity in the foundation of our company and regrets incidents that have occurred due to lax regulations."
–US Business Decision Maker

"We wish we had been more thorough with our due diligence." –UK IT Decision Maker

"If I could have done things differently, I would have given more time for my IT team to do a full inspection." –Singapore IT Decision Maker

"My company wishes that it had more airtight legal agreements with regard to clawback provisions and financial compensation." –Australian Business Decision Maker

Communicating Cyber Risks

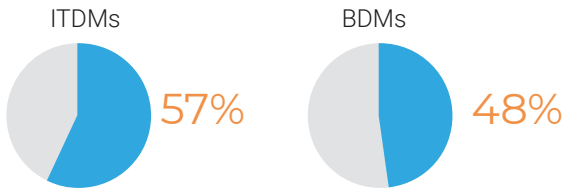
Generally speaking, ITDM and BDM responses were aligned in many regards. For example, there was very close alignment when ITDMs and BDMs were asked to rank their level of concern for cyber risk during each phase of the M&A lifecycle (strategy creation, target screening, diligence and evaluation, and integration). ITDMs ranked integration highest (7.52), as did BDMs (7.36).

However, there were a number of instances that showed a difference—in opinion, involvement or approach to a particular matter.

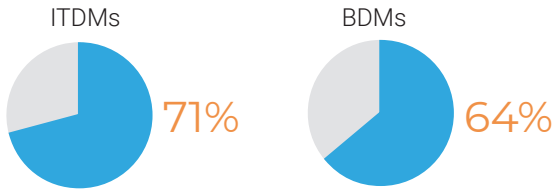
For example, when asked which M&A lifecycle phases they had been involved in, 51% of ITDMs had been involved in integration, while only 35% of BDMs had been involved. One might expect higher ITDM involvement in IT integration specifically, but not necessarily for integration as a whole. And, for the initial phase of strategy creation, 73% of ITDMs reported involvement, while 66% of BDMs reported involvement. In fact, for all four phases, the ITDMs reported being involved more often than BDMs did. These findings suggest that organizations could benefit from greater BDM involvement.

Here are a couple additional comparisons:

Respondents reported their organizations had encountered a critical cybersecurity issue or incident that put an M&A deal in jeopardy.



Viewed cybersecurity evaluations as very important.



These responses suggest two things:

First, although ITDMs and BDMs were frequently aligned, that was not always the case. Even when they were aligned, their responses highlight opportunities for improvements in the area of cyber and cyber risk. For example, both ITDMs and BDMs should be more involved throughout every phase of the M&A lifecycle.

Second, the findings suggest that ITDMs and BDMs contemplate and prioritize risks differently. For example, 23% of ITDMs reported that their company had major regrets after an M&A deal due to cyber-related concerns, as opposed to 19% of BDMs. These differences, even though they are slight, indicate that ITDMs and BDMs may quantify risk differently. From an ITDM perspective, a major regret might stem from a critical application crashing during integration, leaving employees and customers without access for hours. From a BDM perspective, however, they might view such a scenario through the lens of financial losses.

From day one of an acquisition, it's critical that ITDMs and BDMs reach consensus as to how they are going to communicate, calculate, assess and mitigate risks. Because they are not always responsible for the same people, processes, resources and organizational missions, they may approach risks differently, with different tolerance thresholds as well as disparate means of communicating the implications of those risks. To make sure all risks are understood, it's important ITDMs and BDMs agree to common terms and measures of risk assessment and communication.

CONCLUSION

Cybersecurity risk is a growing concern to both IT and business decision makers during M&A and integration. As integration occurs, companies are more vulnerable to attack and have more exposure because they cannot see what may be most vulnerable or about to be hacked. The mitigation of that risk lies in the balance of allowing time for the IT teams to do proper assessment, diligence and inventory early on and by having more controls in place to monitor the process.

According to our survey results, there is an opportunity for companies to increase their vigilance in protecting their companies through training IT staff, allowing IT teams to be more involved in the M&A process, ensuring an automated asset inventory program is in place and by giving them the necessary time to complete due diligence.

The findings in this report strongly suggest that the more controls a company utilizes, the better their outcomes are when it comes to reducing risk and protecting their company's assets.

To learn more on how to minimize your cybersecurity risks, you can read the **Mergers and Acquisitions Solution Brief**.

ABOUT FORESCOUT TECHNOLOGIES

Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, real-time discovery and classification of every IP-connected device, as well as continuous posture assessment. As of December 31, 2018, 3,300 customers in over 80 countries rely on Forescout's infrastructure-agnostic solution to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity. Learn how at www.forescout.com.

Forescout researchers constrained the scope and data sample for consistency and the convenience of issuing a one-time brief. We have noted limitations due to study type and time, scope, data de-identification, passive data capture methods, and errors in AI-based classification of device functions, operating systems, and vendors. The reality of using live, production-environment cloud data means sometimes having imperfections in the data supply. Working within these bounds, Forescout researchers have done their best to ensure consistent, reliable, high-integrity reporting.

RECOMMENDATIONS

Acquisitions can be a time- and resource-intensive exercise, and sometimes an acquisition may not even be completed on account of findings from due diligence. Historically, evaluations have focused on Finance, Legal, Business, Operations, Human Resources and IT, among others. And, while cyber hasn't been entirely ignored as its own evaluation area, what's clear is that, given the risks, organizations considering an acquisition could benefit from greater, more dedicated cyber evaluation. Below are a few recommendations organizations should consider as they prepare themselves during their next business deal.

Money well spent early on will prove to be invaluable when it protects you from surprises down the road.

- **Focus on asset management and asset inventory:** If organizations fail to account for devices and assets on their network, then they cannot fully know what risks they might be inheriting as part of an acquisition. It's critical that organizations focus on asset management and asset inventory as a fundamental best practice to reduce cyber risks during M&A. And, to take that a step further, the relative importance of each asset needs to be determined as well as gaining an in-depth understanding of the network to which that asset is connected. In other words, if there's a vulnerable asset on the network, but it's segmented, that asset and associated risk might still be effectively managed.
- **Allow internal teams to conduct a thorough audit and bring in an outside party for additional help (if your internal team is unable to conduct the appropriate levels of the due diligence required)**. Companies need to be willing to acknowledge that they cannot always do this on their own and important training is needed to equip internal teams with the skills to conduct due diligence.
- **Allocate budget for an external cybersecurity audit**: Be prepared to spend the money required to ensure the company does a thorough examination prior to making a deal. Money well spent early on will prove to be invaluable when it protects you from surprises down the road.
- **Provide training to your IT teams so they are properly equipped to handle and prepare for an acquisition**: IT teams need more training on what to look for and how to handle M&A-related issues. Protocols and systems can help them inform the brokers of the deal of any cybersecurity issues they see—but they need to be informed about the latest threats.
- **Utilize more controls to protect your organization**: Companies with more advanced cybersecurity controls better identify, understand, manage and mitigate M&A cybersecurity risk.
- **Include contingencies and clawback clauses**: Although 89% of respondents think their company should include clawback clauses, only 69% currently do. Including a clawback clause is a common way to mitigate risks in the event that unforeseen risks or value leakages are discovered. Contingencies are also used by 73% of respondents and allow the acquiring company to terminate a deal after signing if it determines the representations and warranties were untrue.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591