VERITAS

The Vulnerability Lag

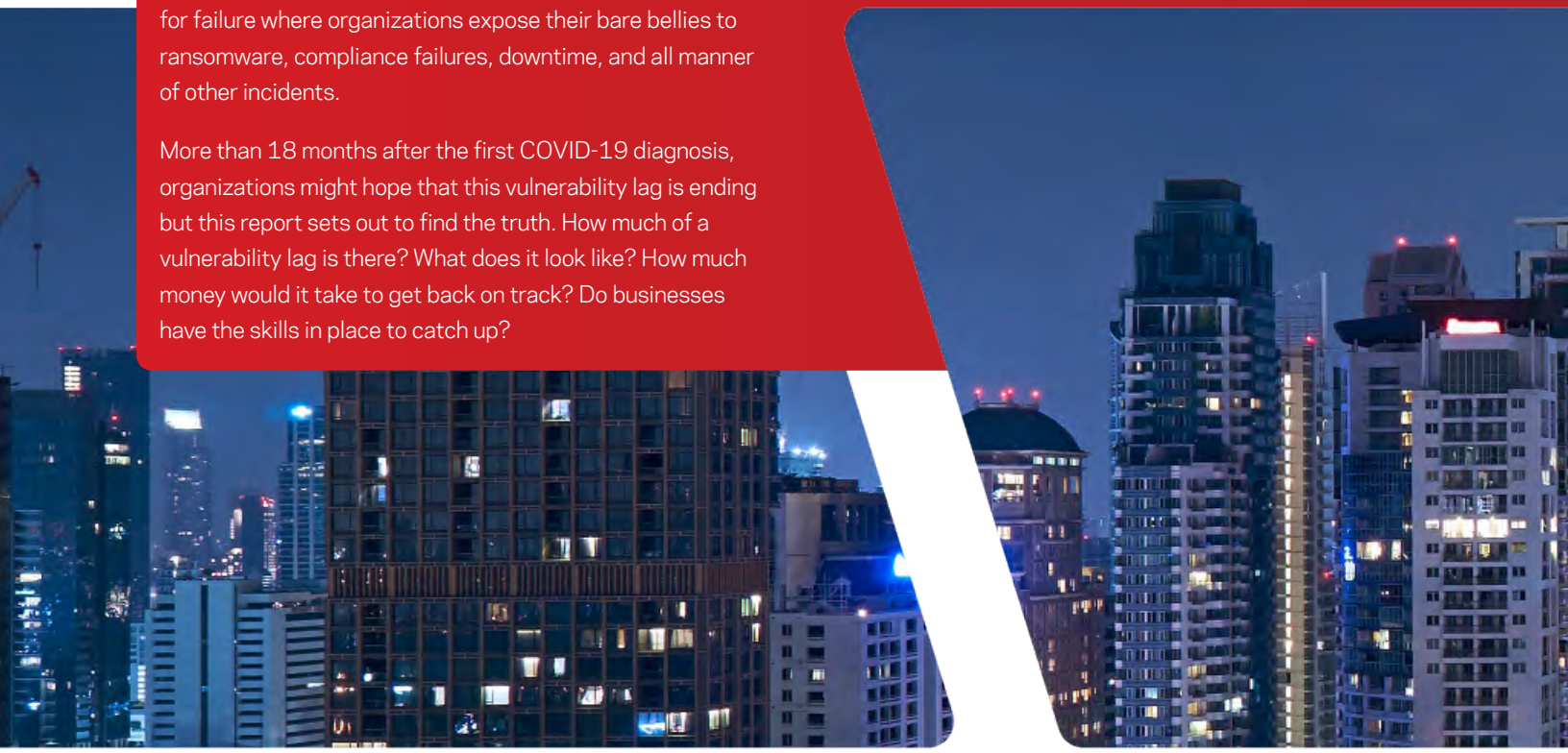
Exploring the ransomware risks resulting from accelerated digital transformation in the wake of the COVID-19 pandemic

Introduction

For organizations to protect themselves against vulnerability to data threats, such as ransomware, their production and protection environments have to evolve in parallel: as each new application, system, or workload is introduced into the organization's technology stack, new tools need to be put in place to protect them. However, all too often, the need (or desire) to innovate at speed throws this balance out of kilter, creating a vulnerability lag, where systems and data are left wide open to attack.

COVID-19 was a catalyst for creating vulnerability lags in organizations around the world. The need to rapidly introduce new systems to support evolving business practices such as remote working, contactless interaction and providing consumers with 'online everything', meant that IT departments were often forced to prioritize the delivery of functionality over security. This introduced a thunder-and-lightning effect, where we first saw the lightning flash of new innovation and then had to wait for the thunderclap of protection to follow. The intervening period is the biggest window of opportunity for failure where organizations expose their bare bellies to ransomware, compliance failures, downtime, and all manner of other incidents.

More than 18 months after the first COVID-19 diagnosis, organizations might hope that this vulnerability lag is ending but this report sets out to find the truth. How much of a vulnerability lag is there? What does it look like? How much money would it take to get back on track? Do businesses have the skills in place to catch up?



Key findings

HOW BIG IS THE VULNERABILITY LAG?

Cloud technology (**56%**) and security (**51%**) are the two most commonly reported gaps that now exist in respondents' organizations' IT strategies, that are leaving them open to attack

Organizations would need to spend an average of **$2.47 million** (USD) to close the gaps in their technology strategy within the next 12 months

On average, it will take another **two years** to eliminate the current vulnerabilities that organizations face today

On average, respondents think that their organization would need to hire **27 full-time IT employees** to close the gaps in their technology strategy within the next 12 months

WHAT IS CAUSING THE VULNERABILITY LAG?

Organizations are unable to keep pace.
Only 61% believe that their organization's security measures have fully kept up since the implementation of COVID-led digital transformation initiatives over the past 18 months

Technologies had to be introduced unexpectedly.
Since COVID-led digital transformation initiatives began, 80% of respondents' organizations newly implemented or expanded their deployment of cloud infrastructure beyond their original plans

There is a lack of clarity around what technology has been introduced.
Only 58% of surveyed senior IT decision makers believe that they can confidently and accurately state the exact number of cloud services that their organization is currently using

There is a lack of clarity on what needs to be protected.
On average, respondents' organizations' data is made up of 35% dark data, 50% redundant, obsolete, or trivial (ROT) data, and only 16% business critical data

HOW VULNERABLE ARE BUSINESSES AS A RESULT?

88% **of organizations have experienced downtime in the last 12 months**

2.57

The average organization has experienced 2.57 ransomware attacks that led to downtime in the last 12 months, with 14% having been hit five times, or more

5x

Organizations with at least one gap in their technology strategy have, on average, experienced around five times more ransomware attacks leading to downtime in the last year, than those with no gaps

64%

report that their organization's focus on software updates and upgrades has changed/increased for security purposes as a result of COVID

How big is the vulnerability lag?

Over the last 18 months businesses around the world have found themselves dealing with the consequences of an event they couldn't have seen coming. However, to their credit, they did everything they could to make the best of a bad situation. And the survival of many businesses is in no small part due to the way in which IT teams reacted and managed to rapidly implement new tools that supported the necessary transitions to keep business operations going, including the massive shift to remote working.

Unfortunately, as a result of their rapid transformation, many organizations are now lagging behind where they need to be when it comes to protecting their IT environment, leaving them badly exposed to digital risk. For example, new workloads, often in the cloud, have become open to data-loss incidents, like ransomware, due to their lack of protection. This is something that we have coined the vulnerability lag, and any reference to this or "gaps" throughout this report indicates where digital risks exist and will continue to exist until organizations can bring their production and protection environments back into alignment with one another.

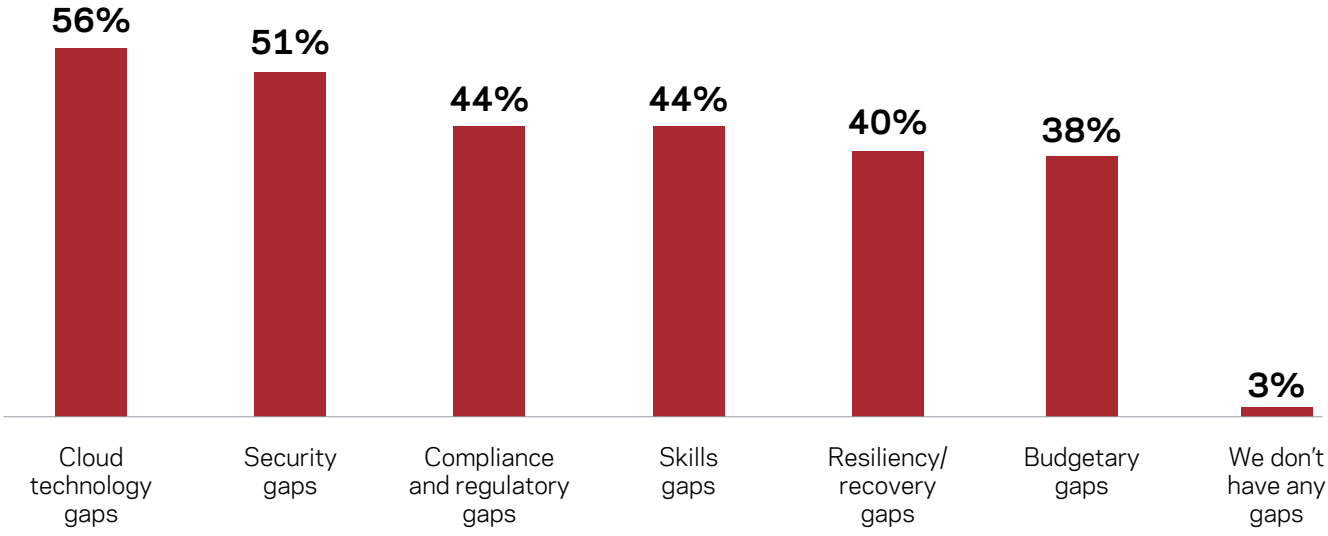
How this came about is completely understandable but finding concrete solutions to plug these vulnerabilities is of paramount importance if businesses hope to regain operational security. So, how big is the problem today?

The enduring pervasiveness of the struggles being faced are highlighted by the fact that almost all (97%) surveyed senior IT decision makers (ITDMs) admit that they still have unresolved issues, left behind by their COVID-led initiatives, in at least one key area of their IT strategies – something that clearly increases digital risk exposure.

Cloud technology (56%) and security (51%) appear to be the most common areas where vulnerability lags have arisen. This is a prime example of where production environments have undergone significant changes, and as a result of rapid implementations, protection environments must now be brought up to speed in order to safeguard the organization against pervasive threats such as ransomware.

QUESTION

Which of the following gaps do you believe exist in your organization's technology strategy as a result of COVID-led digital transformation initiatives? [2,050 respondents, omitting some answers]



While cloud and security concerns are clearly not the only issues that organizations must deal with if they hope to get their technology strategies back on track, they do seem to be the most pressing. Almost half (47%) of those surveyed report that the challenges caused by their adoption of cloud technologies is among the top three issues to resolve that have arisen in the wake of their COVID initiatives. 20% even cite it as the single most important challenge ahead of them. It's a similar picture for security – just over four in ten respondents (41%) place it in their top three and approaching a fifth (16%) say that it's the number one gap to resolve.

However, organizations will need to distribute their efforts wisely if they are to effectively address all of the areas that are lagging and, perhaps, this is why decision makers anticipate this process taking so long. On average, respondents believe that it will take their organization two years to close the gaps in their technology strategy that have been caused by COVID-led digital initiatives.

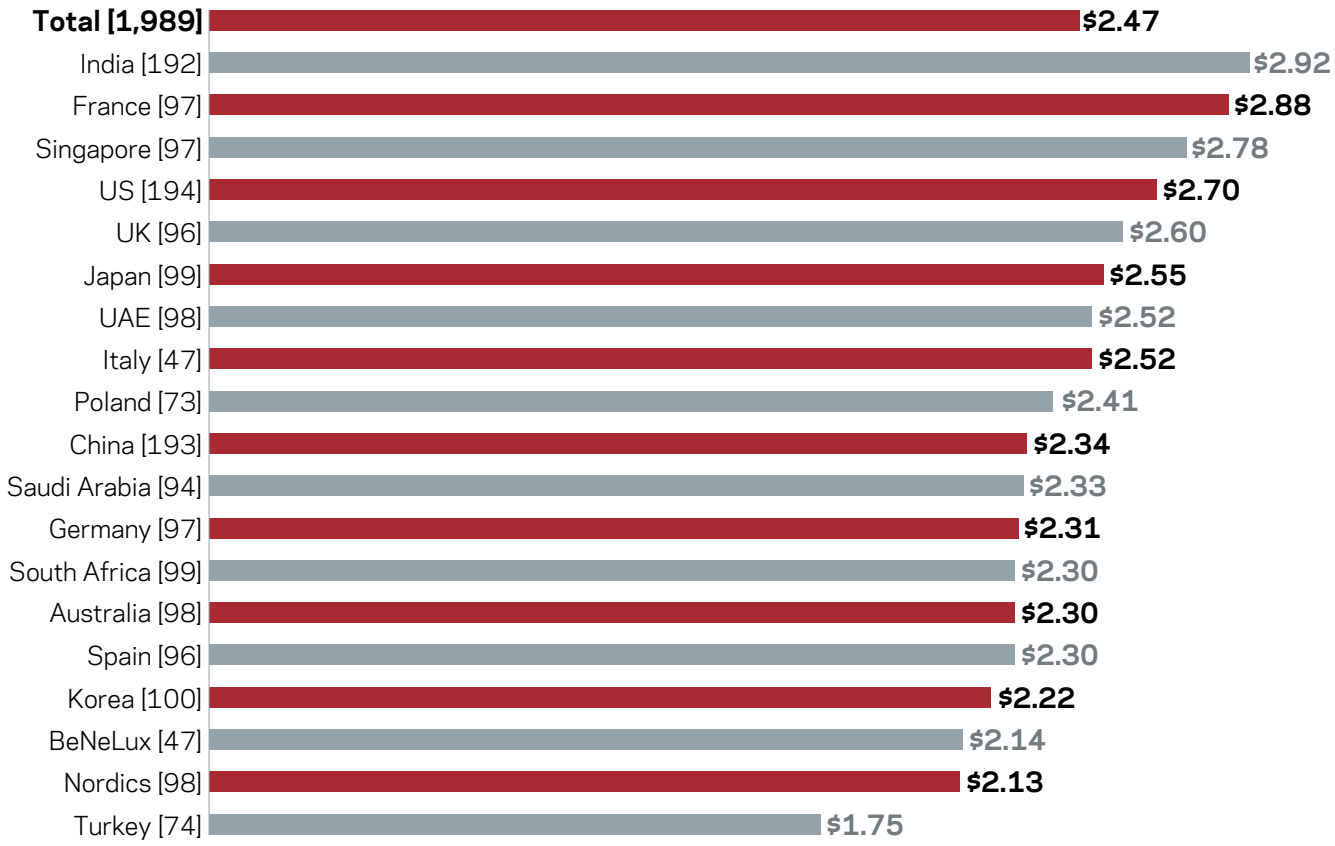
More worrying still, 42% think that it will take more than two years before they will be able to put this behind them.

Unfortunately for organizations, time isn't on their side, as the longer they allow their issues to linger, the longer they will be vulnerable to a host of potentially damaging cyber-attacks. But, as is so often the case when trying to find solutions to a problem, budget will likely be a key sticking point.

If organizations want to shorten the time that their protection infrastructure lags behind their production system and shore themselves up against vulnerabilities within the next 12 months, they will need to spend $2.47 million (USD), on average. And given that total IT spend in 2020 equated to an average of $54.80 million (USD), finding an additional 5%, or so, in their IT budget to fill their voids within a year could prove difficult for many businesses.

QUESTION

The average amount (millions, USD) that respondents believe their organization needs to spend to close the gaps in their technology strategy in the next 12 months [bases in chart], respondents from organizations with gaps in their technology strategy as a result of COVID-led digital transformation initiatives, split by country



To add to these practical concerns around the length of time it will take, and the amount it will cost to remove vulnerabilities in technology strategies, there is another difficult obstacle to overcome – personnel. Prior to the pandemic, the skills gap that had been developing within IT departments around the globe was well publicized. So, when the worst happened, you would be forgiven for thinking that these teams might have crumbled under the pressure being placed upon them.

But, for the most part, it seems that IT departments rose to the challenge and, at the very least, kept their organizations operational. As it turns out though, this was only half the battle, and now, rather than taking a well-earned rest, their attention needs to turn to tackling the vulnerabilities in their technology ecosystem resulting from the transition that occurred.

This means that the skills gap has once again reared its ugly head, and decision makers are now realizing the urgency with which they must address this problem if they hope to have any chance of eliminating the lags and fixing their broader technology strategy. Not only are organizations saying that they need to spend an extra $2.47 million (USD), to shorten the time that they remain vulnerable, but they also say they will need to hire 27 full-time IT employees.

"Not only are organizations saying that they need to spend an extra $2.47 million (USD), to shorten the time that they remain vulnerable, but they also say they will need to hire 27 full-time IT employees."

Given the personnel difficulties that were being grappled with pre-pandemic, this seems unrealistic. So, it helps to explain why it's anticipated that closing all of the gaps in their strategy will still take companies an average of two years.

One thing is for certain – the headaches that addressing the lags and the investment required will both be worth it if they help to prevent, or limit the effects of, a ransomware attack, or similar, further down the road.

What is causing the vulnerability lag?

Under the circumstances created by the pandemic, the importance of security, took on a new dimension. Cyber criminals redoubled their efforts during the height of the pandemic to target organizations while they were putting out fires elsewhere in the business. And, in light of recent ransomware attacks on critical infrastructure and software supply chains, it doesn't appear as though they plan on letting them off the hook in the near future.

However, only just over six in ten (61%) respondents believe that their organization's security measures have fully kept up since the implementation of COVID-led digital transformation initiatives over the last 18 months, with 39% experiencing some form of security deficit.

Bringing security measures up to the level where they need to be will, no doubt, be a challenge for organizations, but it is one that they must meet head on if they hope to prevent cyber criminals from reaching their objectives.

It stands to reason that one of the main contributing factors to this security lag is the rapid and unexpected need to adopt new technologies as businesses reacted to the pandemic. And cloud technology was one of the main focal points for new implementations – 80% of respondents report that since their organization's COVID-led digital initiatives began, they newly implemented, or expanded their deployment of cloud infrastructure beyond their original roll out plans.

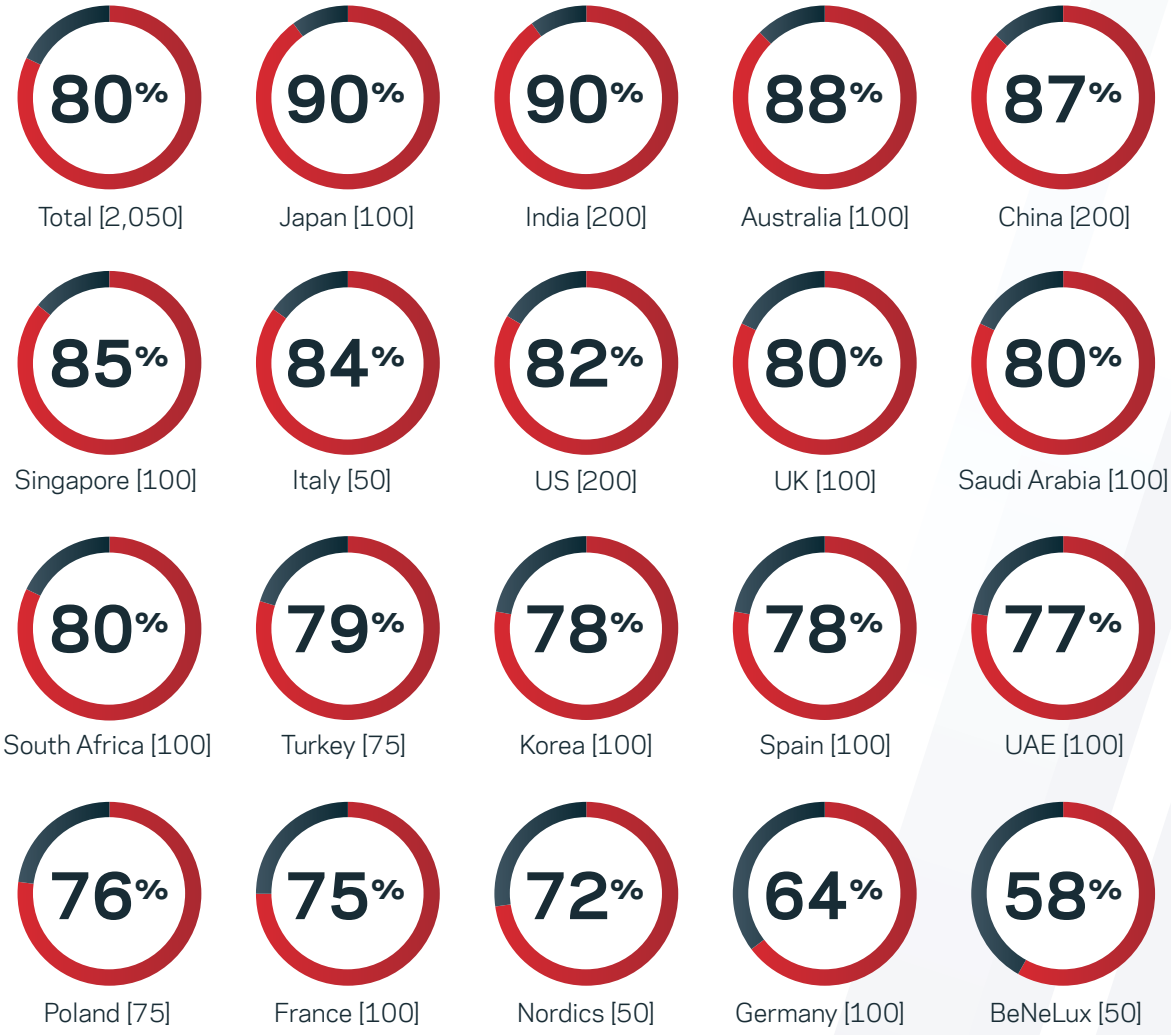
By now, the benefits of cloud technology are well understood, and these benefits, particularly those centering around agility and collaboration, will have been amplified during the height of the pandemic.

However, when implementing a vast amount of new technology at such high speed, it's almost inevitable that difficulties begin to surface – in this instance, visibility has become a key challenge that organizations must address.

Only 58% of surveyed senior ITDMs believe that they could confidently and accurately state the exact number of cloud services that their organization is currently using. If this doesn't set alarm bells ringing as to the scale of the problem facing IT departments when it comes to effectively managing and securing their cloud infrastructure, then nothing will. Ultimately, the buck stops with senior IT leaders, so they must find a way of getting a grip on this situation before a serious security event occurs – they cannot protect what they don't have visibility over.

QUESTION

The percentage of respondents who report that since their organization's COVID-led digital transformation initiatives began, they newly implemented, or expanded their deployment of cloud infrastructure, over and above their original rollout plans [bases in chart], split by country



Regrettably for surveyed companies, their visibility issue doesn't stop with the number of cloud services they're using – keeping tabs on the vast amounts of data that they hold is also proving problematic. This is despite the average IT spend for data risk management initiatives such as security, data protection, and resiliency increasing by +6.72% in 2020, compared to the previous year.

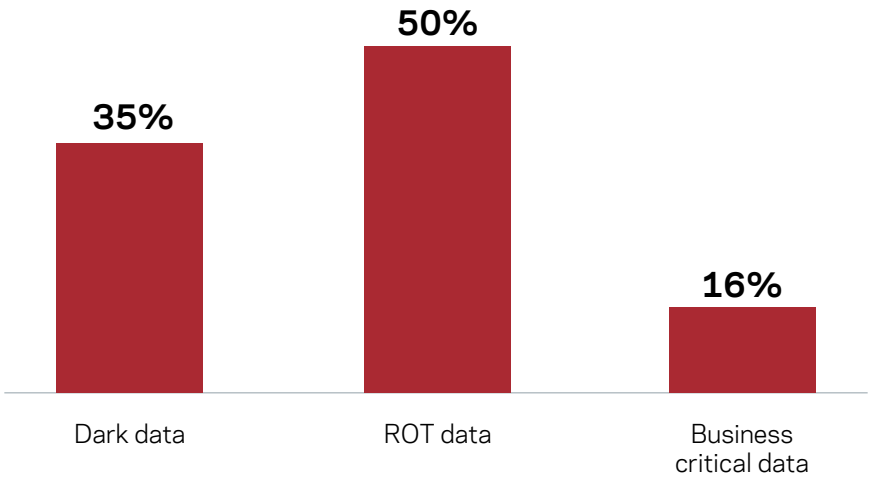
In fact, ITDMs are blind to the value of more than a third of their data. On average, respondents believe that only 65% of their organization's stored data is classified or tagged, leaving 35% that is "dark" – which is the data on their network that they do not know anything about, particularly in terms of its value, if it has any at all.

50%

of data is estimated to be Redundant, Obsolete, or Trivial (ROT), meaning that only around 16% is known to be business critical, on average

QUESTION

The average percentages of dark, ROT, and business critical data that respondents' organizations hold [2,050]



The next few months should represent a period of consolidation for organizations – they've had to respond to an unprecedented global event, and for many this has meant rapid technology implementation. But the speed with which these deployments were rolled out has left them vulnerable. There is a lack of clarity around what has been introduced, specifically pertaining to cloud services, and there is a lack of clarity around what needs to be protected – and whose responsibility it is – especially when it comes to data visibility.

As a result, their security measures are lagging, and this is something that they cannot allow to continue. Ransomware attacks, among others, pose a real and present danger to organizations, and given the opportunity, cyber criminals will take advantage of any small vulnerability without hesitation.

Ultimately, one successful breach could make all the hard work that IT teams have put in over the last 18 months seem meaningless. So, addressing their vulnerabilities at speed and with maximum efficacy is crucial if they hope to push on with their broader business objectives, as the dust from the pandemic continues to settle.

How vulnerable are businesses as a result?

Over the course of the pandemic, businesses around the globe have shown a great deal of resiliency and impressive powers of recovery. But there have, of course, been some bumps along the way, and whether they're caused by internal or external factors, if they result in unplanned IT downtime, they can be costly.

Downtime can occur for a range of different reasons – a ransomware attack, natural disaster, or human error, among others. This makes it a near impossibility for IT to plan for and prevent every potential incident that could lead to the organization going down. But it does mean that the pressure is on when it comes to getting the business back up and running again – this must be done as quickly, effectively, and securely as possible.

It appears that most IT teams have had some practice in returning their organization to normal operations over the last year. Almost nine in ten (88%) respondents' organizations have experienced at least some unplanned IT downtime over the last 12 months.

The more concerning aspect around the downtime that organizations have suffered is that ransomware has been a key contributor to these outages. Respondents stated that their employers had experienced an average of 2.57 ransomware attacks that had led to downtime in the last 12 months, and 14% even admit to five, or more, ransomware attacks causing downtime in the last year.

This goes to show how prevalent and aggressive this attack vector currently is and further emphasizes how important it is for organizations to urgently address their vulnerability lags. Not only that, but respondents from organizations with at least one gap in their technology strategy have, on average, experienced around five times more ransomware attacks leading to downtime in the last year than their counterparts with no gaps. This should be motivation enough for those dealing with vulnerability lags to up the pace of their recovery efforts before they suffer an attack that there might be no coming back from.

Reassuringly, businesses seem to be very aware of the precarious situation that they find themselves in. Almost two thirds (64%) of surveyed IT decision makers report that their organization's focus on software updates and upgrades has changed or increased for security purposes since the start of the COVID pandemic.

There is clearly still a long way to go for many companies when it comes to addressing their vulnerability lags, and it's evident that they must work quickly if they hope to bring their protection environments up to speed with their production environments.

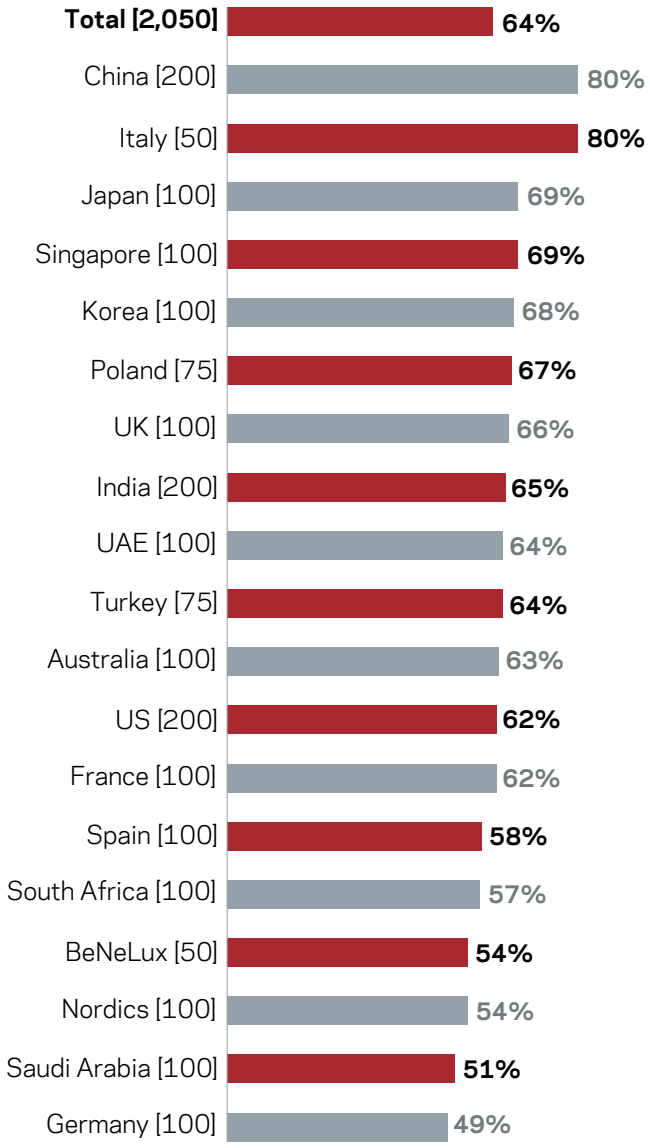
The longer this gap between the two environments remains, the greater their chances of suffering a significant security event, such as a successful ransomware attack, which will undoubtedly lead to unplanned downtime, along with a raft of other negative consequences.

Currently organizations are vulnerable, but it's time to harness some of the powers of recovery and resiliency already demonstrated during the pandemic in order to finish the job of eliminating the areas that are lagging.

"Almost two thirds (64%) of surveyed IT decision makers report that their organization's focus on software updates and upgrades has changed or increased for security purposes since the start of the COVID pandemic."

QUESTION

The percentage of respondents who report that their organization's focus on software updates and upgrades has changed/increased for security purposes as a result of COVID [Bases in chart], split by country



Conclusion

During the pandemic, cyber criminals have done their best to take advantage of the difficult situation that organizations found themselves in, and they are continuing to try and cause disruption as businesses attempt to recover.

Therefore, it is imperative that IT departments double down on their efforts to reduce the vulnerability lags that now exist at their company – if they don't succeed, then their chances of suffering a successful breach dramatically increase.

However, it seems that there are already positive steps being taken to reduce the risks that these digital lags pose to their security – the **2020 Veritas Ransomware Resiliency report** found that 64% of respondents believed that security measures at their company had not kept pace with IT complexity.

In contrast, 39% of respondents in this 2021 report believe that their organization's security measures have lagged to some extent due to the implementation of COVID-led digital transformation initiatives over the last 18 months. While this only leaves 61% who think that their organization's security measures have fully kept up with these initiatives, it does demonstrate that organizations are heading in the right direction.

But unfortunately, there is still plenty of work to be done, with surveyed IT leaders expecting current vulnerabilities to continue to lag behind for an average of two more years. And, if they wanted to accelerate this process, it would take almost $2.5 million (USD) and 27 new full-time IT employees to implement the appropriate fixes within 12 months, on average.

Clearly this is going to be an uphill battle for businesses, but this should come as little surprise considering the visibility struggles that have resulted from rapid cloud deployments, and the ongoing difficulties with effectively managing their data.

For businesses that don't have access to the additional financial and manpower resources that they are outlining, a good first step to addressing these issues would be to consider prioritizing data management technologies that, through automation, maximize visibility and protection. Not only does this uncover where the issues lie, it also allows them to be addressed too, without needing to magic up a bigger team from nowhere.

Because addressing the issues is critical, especially in the fight against ransomware. This particularly pervasive attack vector has claimed many scalps in recent times, and organizations can be sure that they will be added to that list of victims if they do not act urgently.

Vulnerability lags resulting from COVID-led initiatives must be eliminated – the price to pay is far too great to be ignored in times of such economic instability.

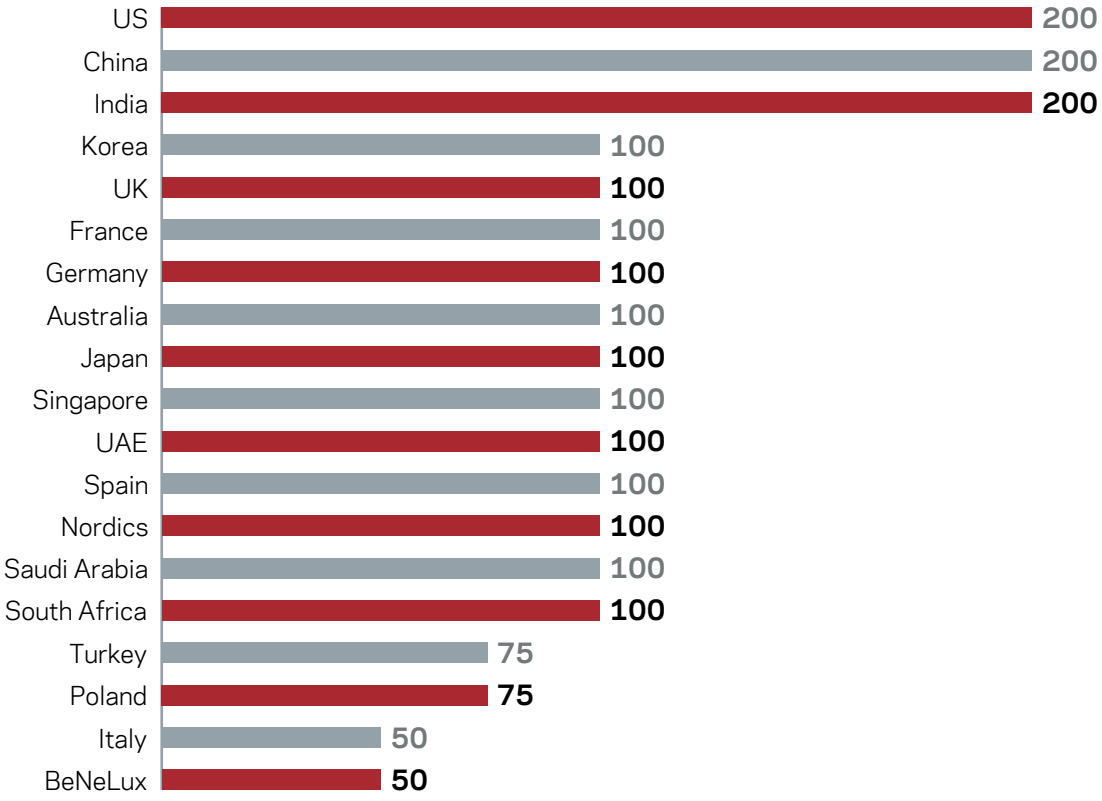
Research scope and methodology

Veritas Technologies commissioned independent market research specialist Vanson Bourne to undertake the quantitative research upon which this whitepaper is based. A total of 2,050 senior IT decision makers were interviewed during June, July, and August 2021, with representation across the US, EMEA, and APAC regions. All respondents had to be from organizations with a global annual revenue of at least $100 million (USD) and are from a range of private and public sectors. These organizations also had to have undertaken some form of COVID-led digital transformation initiative over the last 18 months, defined as the implementation of new tools, changes in infrastructure, increased or new cloud adoption, or an overall digital strategy shift.

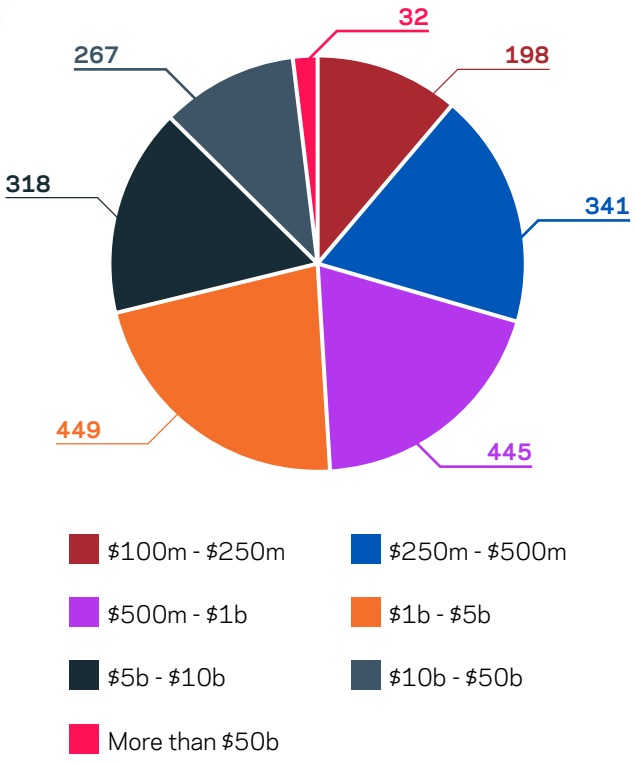
Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

Unless otherwise indicated the results discussed are based on the total sample and include the following number of interviews from each of the below countries, revenue bandings, and sectors:

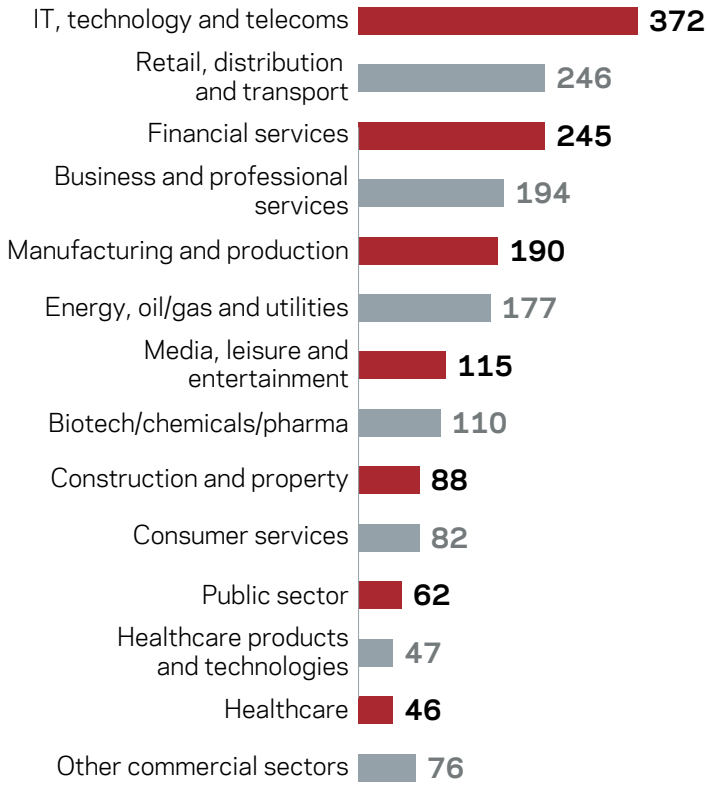
COUNTRY



REVENUE SIZE



SECTOR



About Veritas:

Veritas Technologies is the global leader in enterprise backup and data recovery solutions. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates enterprise data protection, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, the Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms.

Learn more at **www.veritas.com**.
Follow us on Twitter at **@veritastechllc**.

About Vanson Bourne:

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit **www.vansonbourne.com**.