Tech
JOURNAL™

SECURITY

How To Secure Your Remote Workforce

All-In:
FACING DOWN CYBERCRIME
♠ ♥ **With a Fold-Proof Strategy** ♣ ♦

3 Key Challenges Facing Business Optimisation

How a Cyberattack Can Threaten Your Business in a Post-Covid Era

Insight®

Contents

Letter From the Editor

Are You All-In?

To be honest, I'm not much of a gambler. It's not that I'm entirely risk averse, it's just that I recognise the difference between a risk and a gamble. With proper insight, support and planning, a risk can really pay off. But a gamble — that's purely a game of chance, and it's hard to feel lucky when you know the odds are never in your favour.

That's how it is right now with cybersecurity. Security leaders are doing the best they can to play their cards right, but it's a raw deal when everyone else at the table isn't playing by the rules. So how do you win at something when you're playing with cheaters?

You outsmart them.

In this issue of the Tech Journal, we're going all-in on cybersecurity. We invite you to take a seat while our cybersecurity experts divulge how a programmatic and strategic approach can strengthen your odds at gaining — and keeping — the upper hand. You'll learn how advanced tools are helping to detect the "tells" of cyberthreats and how to play your ace against ransomware (page 4).

We outline how you can protect your hybrid workforce against technology fatigue (page 37), consider how to reboot your business on a shoe-string budget (page 57) and keep a close eye on the hot computer vision trends (page 46).

We hope you enjoy this issue and walk away with greater confidence that, even when the stakes are high, there's a path to ensure you're holding all the aces.

Jill Murray
Vice President
Marketing, EMEA

All-In:

Facing Down Cybercrime

With a Fold-Proof Strategy

How do you take a high-stakes game of chance and make it work to your advantage? You perfect what isn't left to chance — and start playing a better version of the game.

Right now, the battle between hackers and security teams feels like an unrelenting poker game with high stakes: your data.

You don't know what tool sets cybercriminals have — or what hand they're playing — and they don't know what you have, either (unless you've got a clear tell). Your data is powering the pot, and it's growing relentlessly whether you like it or not.
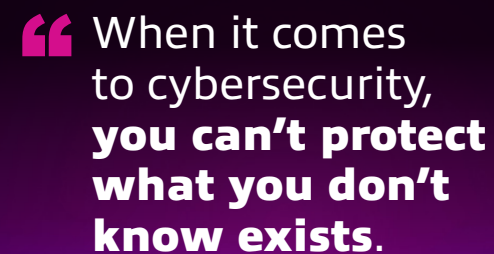
After working in the cybersecurity space for 25 years, I think there will always be some elements of murkiness or chance when it comes to cybersecurity. But I also see an opportunity to lean into what you can control, learn to play the hand you have now and graduate to a more measured game.

As the national director of network and cloud security for Cloud + Data Center Transformation at Insight, here's how I help organisations do it.

It all starts with the north star of cybersecurity maturity: The National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The framework offers best-practices guidance across five areas: Identify, Protect, Detect, Respond and Recover. It was created precisely because too many organisations were betting most of their resources in one area and getting compromised in others.

Here's my take on the NIST Cybersecurity Framework — along with some poker mantras that will put you on a path to mastering it.

> " When it comes to cybersecurity, **you can't protect what you don't know exists**.

Know thy hand, know thyself.

Let's say you're brand new to the game of poker. You have no concept of hand rankings. If you're playing a three of a kind, how would you know that it's better than a pair? If you have a strong hand, such as a flush, how would you know that a full house can beat it? Getting good at anything — a sport, an art or cybersecurity — requires arming yourself with foundational knowledge around what you have and how it works.

Admittedly, it concerns me when security teams say, "I don't know what I don't know." When it comes to cybersecurity, you can't protect what you don't know exists. It's why assessments are wildly important to Insight's approach. It's also why governance falls under this bucket, which means defining what your objectives are, the overall risk associated with those objectives, and the assets or endpoints you're trying to secure.

The good news is that this mantra spans across the entire NIST Cybersecurity Framework. There are assessments built to improve your awareness in every one of the five areas across a variety of use cases, so it's always possible to know what you're bringing to the table.

But even once you have that foundational knowledge, you should always be evolving your cybersecurity program — the way the best poker players continue studying the game and learning new strategies. Remember: The game of poker is ongoing. You're regularly getting dealt new hands (new technologies, tool sets and methodologies). So are cybercriminals. Because of that, you always need to know what you're working with, because it will change.

$345 million*

The estimated global cost of ransomware attacks in 2015.

This figure is predicted to reach $265 billion* by 2031

*Cybersecurity Ventures

2. Protect

Ace your poker face.

In the NIST Cybersecurity Framework, the Protect category is all about prevention — making sure you aren't letting your guard down or exposing a weak spot that can be exploited.

I find that organisations' security controls are largely protective and include:

- Identity and access
- Perimeter controls
- Data encryption
- Regular backups and updates
- End-user training

But even with the wealth of protective solutions available, many security teams remain unsure. According to Cybersecurity Insiders' 2020 State of Enterprise Security Posture Report, 64% of organisations said they lack confidence in their security posture.

Perfecting your cybersecurity poker face isn't so much about concealing a good or bad hand. Rather, it's about doing what needs to be done to keep people from even thinking about taking advantage of your team. Someone with a great poker face sends the same message that good protective controls do: I'm a fortress, and I can't be rattled.

3. Detect

Watch the table. Play your opponent.

I'm a big fan of the poker scene in the 2006 James Bond film, "Casino Royale." In the scene, Bond spends the first few rounds keenly observing his main opponent, Le Chiffre, to find out what his tell is. Bond even mucks his cards on purpose early on, eventually learning Le Chiffre's tell: placing a single finger on the left temple. This know-your-enemy strategy pays off for our hero to the tune of $115 million in winnings.

In many ways, it was a masterful display of tuning in to the table (the way great security teams invest in thoughtful detection processes). In the NIST Cybersecurity Framework, the detect layer is about scanning for anomalies and events, and continuously monitoring your software, hardware and network. It's also worth noting that detection is largely procedural. It's critical to have a clearly defined process in order to detect, as well as know what to do once something is detected.

Phishing emails: Top subject lines helping hackers cash in

According to Q4 2020 analysis from KnowBe4

| Password Check Required Immediately |
| Touch Base on Meeting Next Week |
| Vacation Policy Update |
| COVID-19 Remote Work Policy Update |
| Important: Dress Code Changes |

With the variety of tool sets hackers use to exploit your environment, threat intelligence can play a huge part in shifting your cybersecurity strategy. Take advantage of the array of premium and free threat intelligence feeds to validate the traffic you see on your network. Operationalising this technology — and making it your security team's modus operandi — is very much worth the effort when playing the long game of cybersecurity.

Remember: If you don't have the best hand during the game, it's possible to tip the scales in your favor simply by paying attention.

Don't let setbacks throw your game off.

Tilt is a fascinating phenomenon in poker. It hits when a player is mentally unnerved by a bump in the road, whether it's a string of bad hands or a trash-talking opponent. Tilt causes players to play emotionally, make bad calls or even lose entire games. Even though it's widely dreaded, many players don't have a thoughtful plan to deal with tilt. They'd much rather work on other aspects of their game.

It's common for organisations to silo a lot of money, time and resources into one cybersecurity category, leaving response for last. If and when a breach occurs, this proves to be a flawed approach. Mitigate the chances of getting caught off guard by building a response playbook guided by questions like:

- How will we notify users of incidents and whose data may be at risk?
- How will we investigate and contain the breach?
- How will we report the incident to law enforcement and other authorities?

- How will we document lessons learned and update our methods as needed?

Every minute you put into planning your response is going to save you days, hours and dollars on the backend.

Live to play another day.

Cybersecurity response is planning what you'll do in the heat of a setback to prevent a downward spiral — and avoid tilt. Recovery is your process for picking yourself back up and playing on.

Classic security has long been about putting up walls, keeping the bad guys out or locking down your protective controls. There's a wealth of options for protection. But how many options are there for recovery-corrective-based controls? Not a lot. Because of this, it's critical to take the corrective options that do exist, such as restoring from backup or malware deletion, and get very clear about the how these types of tools

World's fastest hacker?

Kevin Mitnick made the FBI's Most Wanted list by hacking into 40 major corporations. After serving time, Mitnick now uses his skills for good — offering highly sought after security consulting and awareness training.

integrate with your environment. Beyond that, it's all about rebuilding and getting back to business with as little disruption or further damage as possible.

This can be done through:

- Having a detailed cyber incident recovery strategy and plan
- Training all parties on that strategy
- Testing the strategy in a variety of ways (tabletop, simulation, etc.)
- Updating that plan when changes occur or whenever necessary

Security analytics is evolving.

Artificial Intelligence (AI) and Machine Learning (ML) aggregate user and entity behaviors, combining with threat intelligence to give you the best odds at winning at detection and shutting down formidable opponents.

When it comes to cybercrime, it's no longer if, but when. The goal shouldn't be to never have a security event. It's that when an incident occurs, it doesn't decimate your business.

Are you going to take some hits in poker? Yes. But you can employ strategies that could help you win your money back — or even the whole game in the end.

The **worst** time to figure out what to do — is when it's critical that **you do it now**.

Types of poker tilt

Loose tilt: This is the most common type of tilt caused by frustration, too much confidence, impatience or a longing to make up for losses.

Passive tilt: Difficult to detect, this tilt leads to unassertive, weak playing. It's frequently caused by a loss of confidence or fear of taking risks.

Stereotypical tilt: This means playing by the book in a fixed pattern without adapting to the game at hand, causing slipups.

Fancy play syndrome: This occurs when a player overthinks and uses an over-the-top strategy to dupe an opponent.

Transcending chance

There's hot debate whether poker is mostly skill or chance. I think it's both.

A single hand of poker is an irrefutable instance of chance. Playing a full game, or a tournament, is a different story. That's when you can use the controllable aspects of the game to your advantage: your understanding of the deck, the players and the rules; the risk you have related to what you've got; how much you're betting and how much is at stake.

Organisations already have people, processes and technologies in place. That's why poker is a good analogy for the current state of most organisations. Maybe you already have a king and an ace. Maybe your protective controls are over a 10. Maybe you have all hearts, or products, that integrate well together. But remember that in poker, you don't just play one hand, and you certainly don't bet it all on the first hand. That's the iterative process of security — it's many hands.

With a programmatic approach, I believe that organisations can transcend the chance aspect of poker and even graduate to a new, more measured game.

And on we'll play.

Five data breach downswings in 2021
As reported by Identity Force

1. **Guess**: A ransomware attack on the retail fashion giant resulted in a data breach compromising sensitive customer information. The breach exposed Social Security numbers, passport numbers and financial account numbers.

2. **Volkswagen & Audi**: A third-party marketing services supplier disclosed the personal information of 3.3 million customers, including names, addresses and phone numbers.

3. **Facebook**: The personal data of 533 million Facebook users from 106 countries was leaked and released to a low-level hacking forum.

4. **Hobby Lobby**: A cloud-bucket misconfiguration led to a database leak of 300,000 customer records, including names, the last four digits of payment cards and the Hobby Lobby app source code.

5. **California DMV**: Personal information from the last 20 months of California vehicle registration records were stolen, including names, addresses and license plate numbers.

Strengthen your hand.
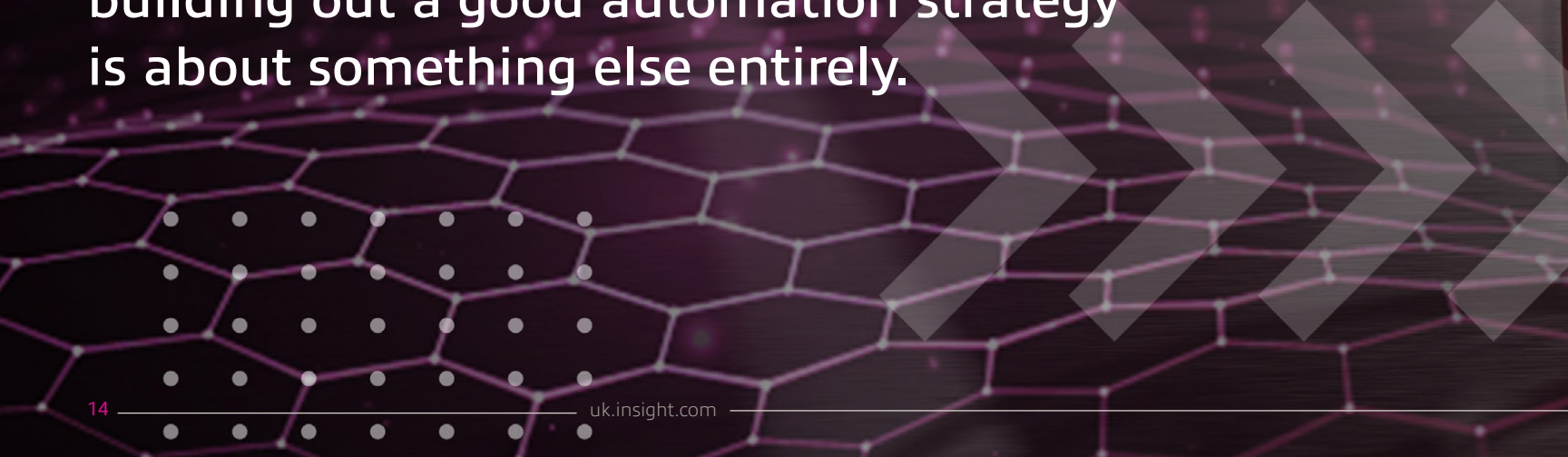See how Insight is helping organisations strategically align to the NIST Cybersecurity Framework.

About the author
Jason Rader
National Director of Network and Cloud Security for Cloud + Data Center Transformation, Insight

How to Build a

Winning Automation Strategy

IT automation is about going faster —
building out a good automation strategy
is about something else entirely.

Have you ever been riding a bike when suddenly, you get speed wobbles? You feel like you're going at warp speed. The bike seems to take on a life of its own. You can't pedal any faster to get back on track.

On the surface, IT automation and cycling have nothing to do with each other. But automation without a thoughtful strategy is a lot like riding a bike with speed wobbles: In the race to go faster with automation, you have to slow down to regain control.

So, how do you automate with purpose? Here's an approach for creating a thoughtful automation strategy for a more enjoyable ride.

Define why you're making the trek.

Start by asking a few questions: "What does automation mean to our organisation? Why do we want to automate? What business outcomes are we hoping to achieve? Is our desire to automate making up for a step we're skipping in business decisions?"

The process of asking and answering questions like these uncovers intent. It unearths valuable information that will help you set realistic and measurable goals. During automation projects, it's common to not consider the implications for the entire ecosystem — and often, there isn't enough discussion about how to turn the ideas you have into reality. Those early discussions matter. They force you to take a bird's eye view before zooming in on the details.

Once you've figured out your organisational goals, it's imperative to understand what your organisation's policy and guidelines

---

92% of business leaders agree:

Automation is key to succeeding in a post-COVID-19 world.
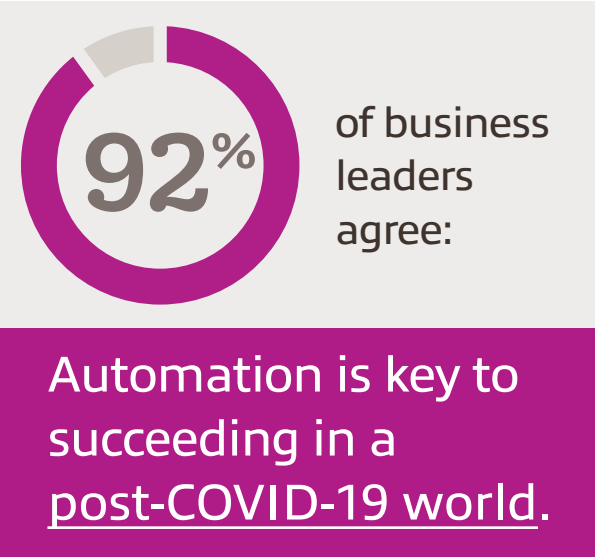
are for automated releases. Without understanding these aspects of your environment, automation can cause problems like backpedaling, failed adoption and more inefficiencies.

After you've determined your purpose for automation and figured out where you can get the greatest gains, assess your cultural readiness. For many organisations, this is often the biggest roadblock.

What makes IT automation worth the journey?

Enhanced agility and scalability for the workforce

Greater focus on customer experience

Improved end-to-end process flow

Increased efficiency through process standardisation

Commit to a mindset shift.

Automating with purpose requires addressing silos that happen all too frequently within an organisation.

As a senior consultant for Cloud + Data Center Transformation at Insight, when I talk to clients, I often find that they want to implement an overarching governance policy — and yet, there are too many silos preventing effective coordination. In order to implement automation that makes sense across teams, you must work on deconstructing siloes, as well as shifting a change-resistant culture.

In my experience, changing culture always starts with relationships. It requires talking to different people within the organisation and building trust through cross-team visibility. Although it's tempting to only operate within the clearly defined boundaries of your own role, once you determine what you need from other people in the organisation — and what they need from you in return — you can begin figuring out what types of automation initiatives can realistically be embraced across teams.

Generating buy-in for automation doesn't happen organically and requires the weight of leadership behind it. So, finding a high-level champion who will use their influence to help change the culture is also critical.

For instance, your organisation may have a center of excellence with staff working on plenty of exciting automation projects. But if there's a certain culture within the company sending the message that these projects aren't necessary, then it's doomed to fail. Alternatively, if you have a high-level person championing the technicians working on these projects, the projects are much more likely to succeed in the long term.

Only

1 in 5

organisations are embracing process automation in its most advanced forms — and nearly

1 in 10

have only taken the initial steps toward automation.

Now, map your route.

Once you've slowed down, asked thoughtful questions and ensured cultural buy-in, the nuts and bolts can take center stage via a process map and Value Stream Mapping.

This involves:

• Test validations (unit, system, integration and user acceptance)
• Service-Level Agreements (SLAs)
• Service-Level Objectives (SLOs)
• Service-Level Indicators (SLIs), which can be defined once SLAs and SLOs are intact
• Objective and Key Results (OKRs)
• Key-Performance Indicators (KPIs), which can be defined once OKRs are intact; will be how you measure the speed which results from your automation

4 main test validations
for easy coasting

Unit testing	Integration testing	System testing	User acceptance testing
Vetting individual components of a system and fixing bugs as needed	Ensuring various interfaces function together well	Testing your programming framework against predefined needs	Using the product through the eyes of the end user

The process of Value Stream Mapping can be intensive. But for every client I've worked with, it's a worthy endeavor and a key piece to successful automation adoption.

"Observability should always come before a release — never after."

There's nothing worse than getting something out to market, then finding out something else broke along the chain

because testing protocols weren't defined or acted upon beforehand. Observability should always come before a release — never after.

Ride on.
It can be easy to confuse automation with orchestration. Automation is about a set of repetitive tasks, while orchestration is about a lot of tasks working together for an outcome. But orchestration doesn't happen hastily. It's deliberate. It's intentional. It forces you to take a step back, the way speed wobbles force you to slow down. If we can start thinking about automation as a strategic journey with purpose, we'll be far more likely to hit our strides and thrive.

Automate with purpose.
Building out a multilayered strategy can seem daunting. Enrolling guidance at every phase can help ensure long-term success.
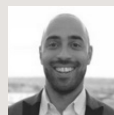
About the author
Jonathan Parnell
Senior Consultant for Cloud + Data Center Transformation, Insight

Fixing The Disconnect Between IT and Business

Failure to Listen to IT Teams Leaves **55% of Businesses Failing** to Take Advantage of New Technology

A longstanding disconnect between IT teams and the wider business is preventing organisations from adopting new technologies and jeopardising their long-term response to the pandemic, research from Insight has revealed.[1]

Pandemic exposes significant disconnect between IT and the wider business

Despite the importance of IT to delivering on organisations' strategic objectives, almost three quarters (**72%**) treat IT as a utility rather than a business enabler, with just **22%** giving IT a seat on the board. This has direct consequences for enterprises: **55%** of organisations are failing to take advantage of new technologies because they aren't listening to IT.

The pandemic has shone a light on this disconnect. **83%** of senior IT decision makers believe ways of working have been permanently transformed. Yet across the wider business, at least **61%** of organisations are reluctant to invest in projects that could improve the employee experience or optimise the business because they believe things will eventually return to a pre-COVID-19 "normal".

Without addressing this, there is a real risk that enterprises will invest in projects without believing in their goals; fail to understand the impact of new ways of working on employees; or base strategies on incorrect assumptions. As a result, they will almost certainly see investments wasted, projects failing and competitors taking advantage.

61%
of organisations are reluctant to invest in projects that could improve the employee experience.

"The pandemic has brought about permanent changes to the way many of us live and work. We are not going to see a return to the status quo, and it's absolutely imperative that organisations adapt,"

"There's already a huge risk associated with making investments in the wrong place. But an incorrect investment at this moment in time could prove more damaging than ever before, leaving the enterprise unequipped for new ways of working and doing business. The gap between IT teams and the wider business must be closed as an urgent priority: businesses have to engage with IT on a more strategic basis, and measure it against businesses objectives."

Emma de Sousa, President, EMEA at Insight.

66%

of organisations have duplicate hardware and software because of lockdown.

Other findings from the research include:

IT teams must measure business impact	Skills gaps must be overcome for new ways of working to succeed	Disconnect between IT and the business puts projects at risk	The costs of not engaging IT
81% of IT departments have freedom to invest in the skills they need, and	**57%** of organisations say they need to invest more in the skills and technology needed to support a remote workforce, and	**67%** of organisations are working on projects designed to improve the employee experience, and	The failure to engage with and listen to IT, coupled with the clear disconnect between IT and the wider business, has almost certainly contributed to enterprises'
82% are engaged to support business projects. Yet	**60%** need to invest more in the skills and technology needed to optimise the business.	**55%** on projects to optimise the business. However, the belief of the wider business that things will return to "normal" means that many of these projects do not have the full support of the business, and so are more likely to fail.	**£3.81m (€4.19m)** spend from 2018-2020 on projects that either did not provide the full benefits, or failed.
59% aren't measured against business KPIs.			

"The way IT is perceived and used within businesses has to fundamentally change.

Having IT at arm's length from the board is simply not good enough: it must be given a seat at the top table. Without this, businesses risk falling behind at a time when digital technology is driving change across all sectors. IT must be put front and centre, driving organisational change and being made directly accountable for doing so. If organisations give IT a voice on the board to drive strategy; let IT use that voice to support innovation; consult IT on what approaches will best meet the business's objectives; and trust IT to perform against business KPIs, they will be positioned to face the challenges of 2021 and beyond."

Emma de Sousa, President, EMEA at Insight.

Fixing The Disconnect Between IT and Business
Read the complete report

About Insight

Today, every business is a technology business. Insight Enterprises Inc. empowers organisations of all sizes with Insight Intelligent Technology Solutions™ and services to maximise the business value of IT. As a Fortune 500-ranked global provider of Digital Innovation, Cloud + Data Centre Transformation, Connected Workforce, and Supply Chain Optimisation solutions and services, we help clients successfully manage their IT today while transforming for tomorrow. From IT strategy and design to implementation and management, our 11,000 teammates help clients innovate and optimise their operations to run business smarter.

Discover more at uk.insight.com

ir End

IT Support
in the Era of
Hybrid Work

The pandemic introduced another level of complexity to IT services. Now, organisations are left trying to figure out how to provide the modern workforce with end-user support to match.

The definition of the word "workplace" has become a little fuzzy lately. Where we once pictured a vast landscape of cubicles, we may now think of home offices, collaboration spaces and even outdoor landscapes.

It's unlikely that these changes will cease to exist in the post-pandemic world, especially as the emerging workforce demands more flexibility. With the Great Resignation in full swing and office re-openings fluctuating, businesses are left trying to figure out how to seamlessly maintain a hybrid workplace, today and for the future.

> The overnight switch to remote work not only taught us that an office doesn't have to be confined to four walls, fluorescent lighting and water cooler small talk, but also introduced an unseen level of complexity to IT services.

Figuring out IT support for the anywhere workplace

The dramatic shift to online channels has increased the demand for IT hardware, software and services. And there's no sign of this change reverting anytime soon.

But to thrive in the post-pandemic workplace, organisations must figure out what their hybrid environment will look like, especially when it comes to IT support. Gone are the days of dropping by to pay your IT team a deskside visit. Nor can IT technicians venture into an end user's home to solve a problem that requires in-person service. Organisations are now grappling with how to provide the same quality of face-to-face support that was once available in the office.

Say goodbye to the old IT service model.

Pre-pandemic, the IT industry was already dealing with some pain points, including slow resolution times, an inadequate response to hardware issues and low Customer Satisfaction (CSAT) scores with IT support. While IT teams are

In fact, according to PwC, 83% of employers say the shift to remote work has been successful for their company, with less than one in five executives saying they want to return to a pre-pandemic office structure.

fully capable of resolving issues for end users, focusing on these needs causes them to lose sight of other strategic problems they could be solving for their organisation.

Despite budgets increasing, the cost of supporting remote users can add to a team's budget needs. In addition, IT support isn't always just about technical problems. Sometimes it's nice to just "drop in" and get face-to-face assurance to relieve the stress of some technical issues. IT support is indispensable for any organisation. Tasks ranging from access requests to device replacement can be challenging in an in-office setting — now imagine how complex they can be in a remote work setting.

Say hello to your trusted partner.

A trusted partner can provide an IT support model anywhere the end user requires. No matter where your team is located, end users need a single place to go for help where they can receive intuitive support that feels like a natural extension of the team.

Organisations are now grappling with how to provide the same quality of support that was available before the pandemic.

Modern IT support can be enhanced by procuring IT vending machines, smart lockers and kiosks.

How does one IT team meet the needs of a dispersed workforce? They don't do it alone.

These solutions can result in lower labor costs and reduced downtime — and can be fully integrated into your ITSM and ITAM systems. Whether you decide to establish these services as standalone vending appliances throughout the office or walk-up virtual support kiosks, your hybrid and on-site workforce can be fully supported with 24/7/365 access to equipment and virtual services.

A hybrid IT support experience doesn't have to put a dent in the budget either. Solutions like these can sound costly but are easily affordable through financing models that allow both leasing and purchasing options.

The dispersed workforce is here to stay.

As a result, the demand for modern workplace services will only continue to grow. Services that maintain the device lifecycle when devices live outside the office can improve the experience for hybrid users by delivering personalised services that empower them to choose when, where and how they'd like to receive support.

A trusted partner for your IT services can eliminate 20% or more (on average) of your business's IT support costs and provide the modern solutions your end users need.

About the authors

Ian Murray
Director of Technical Architects & Presales for Connected Workforce, Insight

David Downs
Services Product Manager for Connected Workforce, Insight

End-user support for the hybrid workplace doesn't have to be a burden. Discover Insight's Managed Workplace Services.

How a **Cyberattack** Can **Threaten** Your Business in a Post-Covid Era

The pandemic has changed how we work forever. In the first wave of lockdowns and social distancing measures, businesses had no guarantee of survival, but they managed to pull through thanks to an ability to adapt to rapidly changing circumstances.

Organisations of all sizes have been affected by the disruption, including the SMBs that make up 99.99% of the UK's estimated 6 million businesses.[1] In nearly all cases, technology has proved critical in allowing companies to continue to operate and maintain existing levels of customer experiences.

Cloud and mobile technologies in particular have become universally adopted business tools. Staff can collaborate, access company applications and data, and communicate with customers from any location.

The efficiency and flexibility that technology has made possible mean many of the changes introduced over the past year will become permanent. Two thirds of employees at organisations of all sizes can now work remotely and two fifths will continue to do so post-pandemic.[2] Among SMBs that figure is even greater, with 75% now relying on a distributed workforce.[3]

Unless this shift in working patterns is accompanied by an evolution in cybersecurity strategy, a single cyberattack could jeopardise this recovery. This threat is universal, but the potential consequences are even greater for SMBs that lack the financial resources to cope with a breach.

Growing risks

The growing importance of technology to operations increases the potential damage of an attack, while available evidence suggests the cybersecurity landscape is growing ever more treacherous.

As staff become more dependent on digital tools, an attack that affects their ability to access key systems will do more damage to their productivity. And as staff create and store more data, the reward – and temptation – for cybercrime increases.

Compounding this risk is the fact that users are accessing company applications and data on devices and on networks that are beyond the traditional control of IT. A greater number of attack surfaces gives hackers more opportunities to launch assaults that can affect the entire company.

The volume of cyberattacks in increasing, with perpetrators looking to exploit loopholes in organisation's digital infrastructure and create as much disruption as possible. Some are even

using Covid-19 itself to stage phishing attacks.

The desire for information on the virus, vaccines, and financial assistance has provided scammers with plenty of source material. Indeed, the UK National Cyber Security Centre estimates that one in a quarter of all cyber incidents in the past year related to Covid-19.[4]

Financial impact

The operational, reputational and financial damage of a successful cyberattack can be significant. Prior to Covid-19, it is estimated that cyberattacks cost the UK economy up to £34 billion a year.[5] But given the increase in cyberattacks since then, the current figure could be even greater.

According to one study, 41% of SMBs have experienced some form of cyber-attack in the past 12 months and a fifth had suffered from six or more attacks. The bill for a breach can run into the millions for a large enterprise but even the average £3,230 cost can be hugely damaging for a smaller organisation.[6]

Nearly a quarter of all SMBs (23%) say they would not be able to survive a cyberattack – that's 1.3 million businesses. A further 16% said a cyber-attack would result in a reduced headcount and 23% said they would have to use financial reserves. Only 22% of all SMBs said that an average cost of a cyber-attack would not have a material impact on their business.[7]

A new approach

SMBs have been through a lot over the past year and have had to overcome many challenges just to survive. In this context, it's easy to see why cybersecurity has been overlooked and why 41% of businesses admit their remote working solutions are not as secure as the office.[8]

Attacks that exploit recently discovered (and now patched) vulnerabilities in Microsoft Exchange Server, enabling allow hackers to access servers and steal data or deploy malware are an example of this threat. Email systems provide a treasure trove of data and any disruption to what an essential communication tool can be very serious.

41% of SMBs
have experienced a
cyberattack
in the past year

The past year has showcased the ingenuity, resilience, and entrepreneurial spirit of small businesses at their best. But just one incident can jeopardise what remains a fragile recovery in so many cases.

Security strategies should reflect the changing nature of work and an increasingly complex and ever-evolving threat landscape. Perimeter-based security approaches (such as firewalls) must be replaced by dynamic-based security measures that protect data and applications at all times – regardless of physical network.

Advanced anti-malware and monitoring capabilities, coupled with cloud-based infrastructure and applications that automatically receive security updates can also help. It is notable that the cloud-based version of Exchange Online was not affected by the recent vulnerabilities, for example.

23% of SMBs
would not be able to survive a
cyberattack

91% of UK CEOs are concerned about cyber threats compared to **80%** last year[9]

SMBs have shown their adaptability in coping with challenges caused by the pandemic. Technology has been a major factor in allowing businesses to operate as close to normal as possible, but any recovery will remain perilous without a cybersecurity strategy that reflects the current climate.

Mobile Device Management (MDM) capabilities, such as those included in Microsoft 365, give organisations control over which users, applications, and devices can access corporate assets and also ensure that cybersecurity policies are applied at all times. Windows Virtual Desktop goes one step further by providing a virtual desktop that doesn't require any data to be stored locally at all.

Finally, staff should be engaged and trained to ensure they follow policies and understand the threats they face. All it takes is for one user or system to be compromised for a cyber threat to become a cyber reality.

Find out how Insight can help your organisation develop a robust security strategy that will allow you to adapt and thrive in the current, everchanging climate.

[1] Federation of Small Businesses (2021)
[2] Gartner CIO Survey (2021)
[3, 5, 6, 7] Vodafone (2021)
[4] National Cyber Security Centre (2020)
[8] Cloud Industry Forum (2020)
[9] PwC (2021)

The Innovation Equation

Maximise the value of your data by making the most of your infrastructure.

By now, most organisations are leveraging the cloud in some way, and usage is only increasing. Gartner forecasts worldwide public cloud spending will grow by 23% in 2021 as organisations face ongoing pressure to support complex workloads and the demands of hybrid work.

While some continue to focus on core business functions such as IT cost optimisation, risk reduction and the digitisation of processes, the majority of organisations are now looking further ahead — seeking opportunities to leverage their infrastructure to drive growth, accelerate product development and scale innovation.

Cloud foundations

The reason many organisations fail to transform — and therefore survive long term — comes down to a lack of skills needed to rapidly adopt new technologies. By providing access to democratised services and capabilities, the public cloud brings solutions such as Artificial Intelligence (AI) or the Internet of Things (IoT) within reach, without requiring deep, in-house expertise. This enables businesses to do more with less, faster.

No matter the intended outcome, the effectiveness of these solutions begins with the availability and accessibility of good, clean, unbiased data. Today's cloud providers make it easy to ingest, store, query and visualise massive amounts of data in support of a wide range of use cases. Backed by security, resiliency and geoproximity capabilities, the cloud enables users to access the tools and information they need to make better business decisions from anywhere in the world — without the need to connect to an on-premises data center.

Ultimately, accelerated innovation in the cloud supports accelerated innovation across your company. Having the tools to execute on individual projects more effectively empowers your organisation to ideate and transform faster, driving disruption and competitive advantage. This is why, according to McKinsey, 75% of the cloud's predicted value comes from its ability to enable innovation.

But while public cloud has been established as foundational to enterprise innovation, focus is increasingly shifting to the edge. IDC reports companies worldwide are on pace to spend $240.6 billion on edge computing through 2024, investing in hardware, software and services at a compound annual growth rate of more than 15%.

75%

75% of the cloud's predicted value comes from its ability to enable innovation.
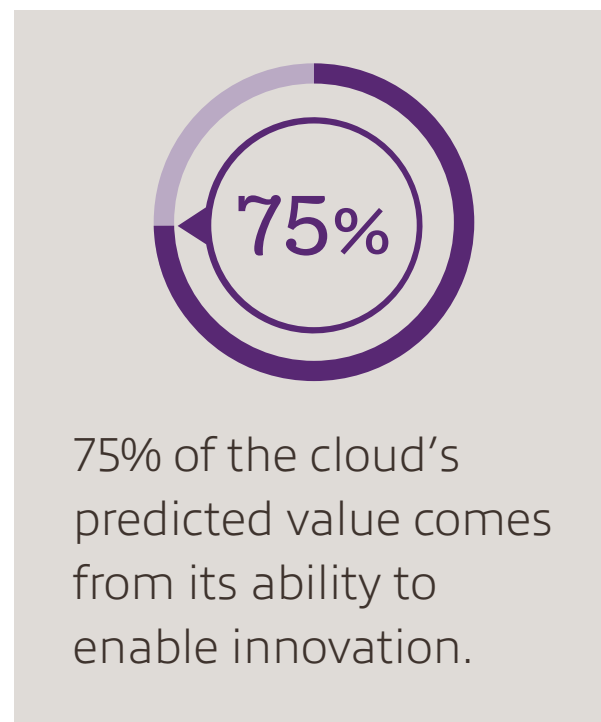
So, what value does edge computing add to the innovation equation?

The edge advantage

Put simply, edge computing is an extension of your organisation's distributed or hybrid architecture which allows data to be processed closer to its source. As a result, one of the primary benefits of the edge is low latency.

Sending data back to a centralised public cloud for analysis causes lag, which may render the information unusable or, more importantly, result in missed opportunities to provide services within the critical user experience window. This is a key consideration for many AI- or IoT-based solutions, including predictive maintenance, defect detection, security and surveillance, and more. On a product assembly or food processing line, for example, data often has an extremely limited lifespan. Anomaly

response must occur immediately to prevent low-quality products from reaching distribution. Other solutions such as Augmented Reality (AR) or Virtual Reality (VR) also depend on low latency to deliver real-time experiences.

The edge also supports innovation initiatives on the whole by reducing the technical, financial and security burdens associated with storing massive amounts of data in the cloud. Running workloads at the edge enables organisations to build solutions that leverage short-term or single-use data that can be discarded to reserve storage space or protect Personally Identifiable Information (PII). Sending only the inferences or insights derived from this data to the cloud informs broader decision-making while reducing risk, preserving privacy and improving overall bandwidth.

But in order to effectively leverage your architecture from core to edge, there are a few things to consider.

1. Tools and services

When designing an architectural strategy that supports innovation, public cloud managed services are key. While the specific offerings will vary by cloud provider, they typically support security and compliance, monitoring and management, solution design, modernisation and more. By offloading the technical burdens associated with managing cloud and edge environments, these services accelerate time to value while lowering your overall cost profile.

There are also many solution-specific cloud platforms which can be leveraged by internal teams to build and deploy custom AI (Azure AI, Google Cloud AI, Amazon SageMaker, IBM Watson), IoT solutions (Azure IoT Central, Google Cloud IoT, AWS IoT Core, IBM Watson IoT) as well as chatbots, computer vision models and more. These tools provide the foundations to make complex solutions more approachable without the need for custom code.

By 2025, Gartner predicts 75% of enterprise-generated data will be created and processed at the edge.

Cloud providers are also increasingly expanding their offerings to simplify the process of operationalising data at the edge. Frameworks such as Google Anthos, Azure Arc, AWS Outposts and others can be used to manage clusters and the workloads deployed on them.

New tools and services are released regularly, so as part of your architectural strategy, it's important to reevaluate which solutions may be best suited to your environment. Relying on a static approach will result in missed opportunities to reduce operating costs and improve efficiency or scale.

Cloud + edge benefits

While both cloud and edge solutions offer distinct benefits, when it comes to driving innovation, the most effective strategies capitalise on the complementary features of both approaches.

The cloud provides:

- The tools and managed services to easily develop applications, IoT and AI solutions
- The scale to manage the data needed to develop and refine solutions, as well as to gather insights from these solutions over time
- The ability to manage edge devices from both an Operational Technology (OT) and Information Technology (IT) perspective
- The flexibility to swap out edge workloads quickly as new use cases arise
- Automated and remote management capabilities — rather than relying on manual, on-prem processes to achieve these goals

The edge:

- Demystifies the implementation of solutions from AI to IoT
- Enables rapid deployment, testing and modification of these solutions
- Reduces latency and improves the value of real-time data
- Increases flexibility, allowing workloads to be shifted quickly with minimal disruption
- Provides a more effective way to process massive amounts of data, enabling key insights to be sent to the cloud

Together, cloud + edge establishes a robust framework for rapidly developing, delivering, managing and modifying your approach to innovation. Rather than requiring a full week to build an on-prem solution, cloud services may be used to prototype a concept overnight. It can then be deployed to the edge for rapid testing, modification and proof of value. The faster your organisation can test and learn, the faster you can transform over time.

2. Data alignment

Intel's The Edge Outlook report shows that while most businesses understand the edge is integral to unlocking future innovations — 76% say identifying "the ideal" location for data is a challenge.

There's no one right way to determine where data should be managed and stored; the decision ultimately comes down to where a particular workload will be most useful, practical or desirable. But in general, applications or workloads that benefit from being processed at the edge are those that require low latency, high bandwidth, strict data privacy and/or a short data lifespan. Edge applications also tend to be more "lightweight" and specialised, while solutions that are more broadly focused and more compute intensive tend to be better suited to the cloud.

Industry- or company-specific privacy policies, such as HIPAA or GDPR, will also play a role in determining where your data will live.

3. Managing complexity

As your cloud + edge architecture becomes increasingly distributed, challenges of scale and complexity are bound to arise, particularly if edge deployments are treated as point solutions rather than integrated aspects of your network.

To enable operational efficiency, organisations must manage edge and core cloud workloads in a secure, maintainable and scalable way. This requires a consistent operational approach to automate processing and execution as data is sent from the edge to the cloud and back again.

Leveraging a microservice or container-based approach can simplify the process of extending cloud-native services and applications to the edge. A container-based application is scalable and can run in the cloud or on the edge, making it easier to manage. This reduces the cost of managing different frameworks and deployment strategies.

4. Security factors

As with any technology implementation, security must be considered when implementing solutions at the edge. This is a broad topic with many areas to evaluate, but in general you'll want to prioritise:

- **The physical security of each edge device**
- **The framework used for onboarding these devices**
- **The security of your data pipeline and configuration**
- **Imaging and securing at the OS level, as well as the solution level**
- **Out-of-band management and patch management**
- **Securing data at rest**

The good news is that some of these requirements can be managed by your cloud provider. The rest should be kept top of mind as your team moves applications and workloads from proof of concept to production at the edge.

Take a deeper dive into innovation at the edge with expert panels, breakouts and a keynote from Forrester Research. Insight *Accelerate* is now on demand.

A calculated approach

The ability to "fall quickly" — not *fail* quickly but *fall* quickly — then get up and move on to the next solution is a cornerstone of innovation. A robust cloud + edge strategy enables this approach by circumventing many of the lengthy, manual processes associated with a traditional on-prem or core cloud architecture.

By building on the benefits of each aspect of your infrastructure, your business will ultimately be able to develop a robust approach to data-driven innovation that's greater than the sum of its parts.

About the authors

Amol Ajgaonkar
CTO of Intelligent Edge, Insight

Carmen Taglienti
Principal Cloud & AI Architect, Insight

How to Protect Your Hybrid Workforce Against *Technology Fatigue*

Technology has proven essential in helping organisations with the abrupt shift to remote working. Through the power of technology, businesses have been able to ensure staff can communicate and collaborate from any location, whilst maintaining the same level of customer experience.

Since that abrupt shift at the start of the Covid-19 pandemic, organisations, employees and customers have become more comfortable with the situation and remote working has become normalised.

A ¹/₄ of Brits will work from home on a full-time basis by 2025, compared to just 5% in 2019.[2]

Covid-19 has accelerated internal digitisation by up to 4 years

The reopening of offices might be viewed as a 'return to normal', but many of the changes enacted are likely to become permanent. While it is possible that many people will be eager to return to the office, others will be keen to retain the freedom that flexible working has provided.

Businesses have also seen the benefits of having a remote workforce. Fewer staff on-site means office space can be reduced and repurposed, saving money, while a happier, more engaged workforce has led to increased productivity. A study by one major bank revealed its staff believe they made better decisions from home.

Going forward, many businesses will adopt a hybrid model that combines office-based and home-based workers.

Indeed, a quarter of Brits will work from home on a full-time basis by 2025, compared to just 5% in 2019.

Evolving strategies

Most organisations now have a technological foundation in place to support this latest evolution in working. Cloud-based infrastructure provides secure access to applications and data from any location and enables office- and home-based staff to collaborate with each other or communicate with clients.

Videoconferencing tools like Microsoft Teams will remain ubiquitous in the hybrid era and, by 2024, it is estimated that in-person meetings will account for just 25% of all enterprise meetings – a drop from 60% prior to the pandemic.

But just because something has worked well for the past 12 months doesn't mean it will continue to do

so indefinitely. It is imperative that businesses refine their approach and the types of technologies they use so that their strategy meets the needs of the businesses and the workforce.

Digital Transformation is as much about culture as it is about technology, and without the latter, the potential of the former will be diluted.

Guarding against technology fatigue

It is thought that Covid-19 has accelerated internal digitisation by up to four years. While this has brought benefits, it is perhaps inevitable that potential issues have reared their head earlier than expected too. An example of this is 'video fatigue'.

As meetings have shifted from in-person to online, they have had a noticeable impact on the human mind and body. Affected staff are more stressed, less productive, and more likely to be disengaged, according to researchers at Stanford University who have explored the causes of the psychological phenomenon.

By 2024 in-person meetings will account for just 25% of all enterprise meetings

One cause is the dramatic increase in eye contact compared to a physical meeting. Because everyone's face is on screen all the time, it feels as though everyone is looking at you even when you're not talking, amplifying common anxieties about social speaking.

Participants can also become concerned about their appearance when they can see themselves on the screen constantly. Studies show that people become more self-critical when they view their reflection, and this can undermine confidence.

Another issue with video conferencing is that fixed camera positions tie users to their desk more than audio calls or in person sessions. This inability to move around affects cognitive performance.

Refine your strategy

Video fatigue illustrates that technology alone is not the answer and that all hybrid strategies but constantly be adapted or assessed to ensure that technology fatigue doesn't undermine the benefits of innovation.

Organisations need to be able to communicate the benefits of technology, offer training, and ensure that all tools are intuitive and easy to use. There should be efforts to understand the preferences and requirements of staff, and to examine technologies that can deliver the most desirable outcomes.

For example, Virtual and Augmented Reality (VR and AR) technologies might be a more engaging tool for collaboration and communication than a video conference. Alder Hey Children's Hospital in Liverpool is using Microsoft HoloLens 2 and Dynamics 365 Remote Assist to improve quality of service while reducing physical interaction. For example, the technology enables clinicians in the operating theatre to consult medical experts located elsewhere. It also allows just one staff member to conduct a 'virtual ward round', while other participants join remotely. The solution also has great potential for remote training.

Remote working has provided most businesses with a technological foundation to support a hybrid workplace that combines office-based and home-based workers. But to maximise the benefits, organisations must adapt their strategy to guard against technology fatigue

That's not to say video won't remain an essential tool in the hybrid future – far from it. Practical steps such as setting expectations at the start of any meeting, making video optional, or encouraging participants to take breaks so they can move around can help. Teams also lets users set backgrounds, switch off 'grid mode' and hide their own video feed.

But the hybrid workplace will require an adapted approach to get the best out of a hybrid workforce. Organisations that fail to act will be less successful than those who do.

Find out how your business can adapt to the hybrid future with an Insight Business Change Readiness Assessment.

[1] BBC   [2] Deloitte (2021)   [3] Gartner (2020)   [4] McKinsey (2020)

The Evolution of Cybersecurity and the Role of the CISO

Q&A With Arun DeSouza, CISO and CPO, Nexteer Automotive

The large-scale migration to remote work redefined the threatscape for cybersecurity leaders everywhere. Now, more than a year later, many are still trying to identify and close potential security gaps, while staying one step ahead of cybercriminals. We wanted to know, what role does the Chief Information Security Officer (CISO) play in this constantly evolving, cat-and-mouse game of threat detection and prevention? We sat down with Arun DeSouza, CISO and CPO for Nexteer Automotive, to find out.
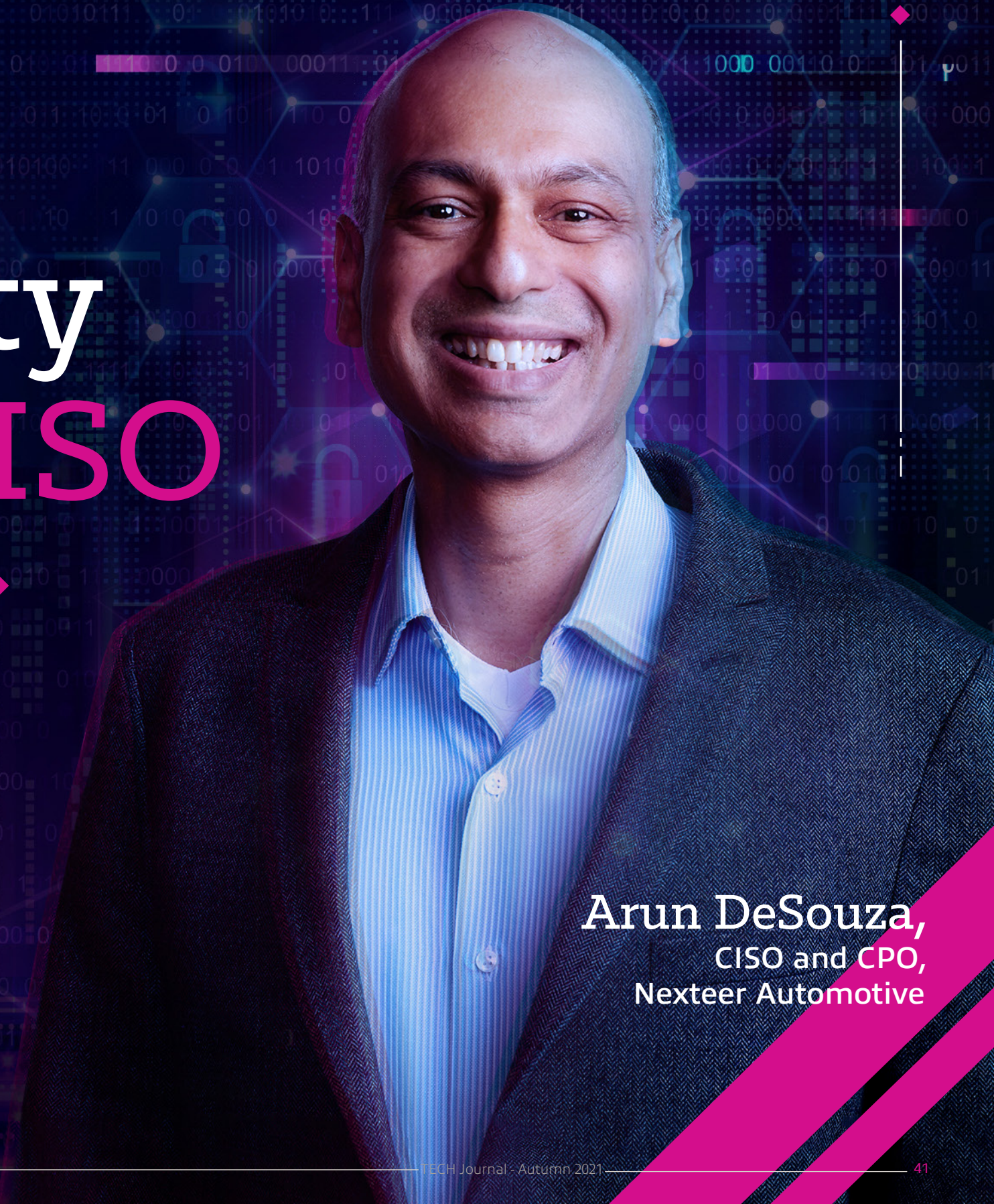
Arun DeSouza,
CISO and CPO,
Nexteer Automotive

What's your role today? How has it evolved and where do you see it going?

I'm the Chief Information Security and Privacy Officer (CISO & CPO). I pioneered an integrated global InfoSec and Privacy program, developed a long-range strategic roadmap linked to business objectives and built a strong team from the ground up. I'm responsible for the delivery of multiple services, including but not limited to:

- Strategic planning
- Identity and access management
- Incident management
- Privacy management
- Risk management
- Governance and standards
- Security operations
- Training and awareness

The CISO role has evolved significantly in this decade. Depending on the risk appetite and scale of digital transformation in organisations, the CISO role now spans across some or all of the following personas:

- Technical
- Business aligned
- Risk focused
- Transformational

When I started my career as a CISO in 2003, I was spending most of my time in persona one. Currently, my role spans personas two through four. The convergence of security, privacy and enterprise risk also offers potential for CISOs to become Chief Risk Officers (CROs) of organisations going forward.

Cybersecurity is top of mind for IT and security professionals today. Why is cybersecurity so challenging right now?

The winds of change are blowing through today's workplaces. Macro trends such as Industry 4.0 and distributed work require

companies to enact and accelerate digital transformation powered by the cloud. Technologies such as Artificial Intelligence (AI), blockchain, edge computing, the Internet of Things (IoT), autonomous vehicles, robotic process automation, etc., are helping to foster innovation and competitive advantage.

The security and privacy risk nexus of the IoT brings a unique set of challenges. Nation-state hacking and supply chain threats are also major factors in the evolution of cyber risk.

Cybersecurity Ventures projected there would be 3.5 million open positions by the end of 2021. Thus, companies are not able to staff up appropriately with the highly skilled resources needed to protect the enterprise. Ultimately, the exponential rise in security threats and the acute shortage of InfoSec resources makes these very challenging times in cybersecurity.

Some IT leaders have argued that IT spending is being wasted on cybersecurity that supports remote work. Yet, the workforce is demanding "anywhere work" flexibility. What are your thoughts on this?

Remote or distributed work is here to stay. There's a paradigm shift underway due to:

- **Flexibility and work-life balance:** Many employees enjoy this feature, especially if their daily commute is significant.
- **Talent acquisition:** Companies can leverage distributed talent and hire the best people. In many instances, this allows both parties to make a win-win arrangement.
- **Executive buy-in:** Companies like Twitter have embraced this trend and are enabling their employees to work remotely indefinitely.

As a CISO, I believe I should help enable the business. Given the above trends, it's now par for the course. Further, the trifecta of identity,

Zero Trust and software-defined perimeter power seamless access to "anytime, anywhere, authorised" access to digital applications and services.

How do you think security will evolve in response to trends such as anywhere operations and edge computing?

I believe that adoption of Zero Trust will accelerate. Dynamic threat protection will be further propagated by security providers banding together in alliances and tightly integrating their platforms to strengthen Zero Trust. One such example is the Spectra alliance between Okta, Proofpoint, Crowdstrike and Netskope. Another example is the Zero Trust alliance between ZScaler, Cloudflare and SentinelOne. This trend benefits enterprises and providers. I expect that this trend will grow. InfoSec professionals will also band together to share best practices via organisations like the Cloud Security Alliance.

Nexteer Automotive received the 2021 CSO50 Award from IDG. The award recognises security initiatives that demonstrate "outstanding business value and thought leadership." Your project was NEXTINTRUST. Can you tell us about it?

This is the second CSO50 award for Nexteer during my tenure — our first was for identity lifecycle management. Our 2020 award was for the thought leadership and deployment of an IoT security platform in our manufacturing plants. This platform enables:

- Device visibility
- Policy definition
- Behavior and risk analysis
- Enforcement of policies and standards

As Nexteer embraces digital manufacturing to increase efficiency and optimise operating costs, there's been an explosion of IoT devices

on the plant floor. Further, more and more of our home devices are becoming internet connected. The exponential proliferation of IoT devices and immature security practices make them targets for attack.

Key CISO guiding principles for Nexteer's IoT security deployment are as follows:

1 Characterise – Identify and classify assets and stratify them by business value and risk.

2 Demarcate – Implement network zones with a clear demarcation between IT and OT networks.

3 Understand – Visualise and identify threats and vulnerabilities across networks inclusive of devices, traffic, etc.

4 Unify – Control access by users and devices across both secure wireless and wired access.

5 Adapt – Leverage Zero Trust to enact adaptive control schemes in real time.

6 Converge – Develop explicit, third-party access and risk management protocols, including Privileged Remote Access. These are particularly relevant to OT networks to strengthen the security architecture.

7 Beware – The following root causes have led to IoT device security issues in the past:

- Static credentials embedded in the device
- Lack of encryption
- No software updates
- API security gaps

The IoT security platform enables visibility to all devices on the manufacturing network. It allows us to identify device posture in real time, detect embedded threats and drive proactive control strategies. This enables enterprise risk management and strengthens cybersecurity.

IT talent, particularly for cybersecurity, is in high demand and short supply. How is your team designed for success?

My first step was to build a detailed services and competency framework with the skills needed for each role as well as a strategic hiring plan. We periodically review and update this framework. It can also be used for career pathing and succession planning.

Further, I employ the following steps and strategies to manage and develop talent:

- Define an appropriate mix of in-house and outsourced services.
- Conduct cross training across service tiers.
- Utilise managed services.
- Leverage training and development and succession plans.
- Negotiate cost savings to "self-fund" key roles.
- Develop a "grassroots" talent pipeline (students and co-ops).
- Identify talent early and strengthen the pipeline.
- Build affiliations with industry groups and universities to identify interested talent.

I'm also pleased to say that my team is diverse, with 50% men and 50% women. This has also helped drive synergies and creativity.

What's been the most profound executive decision you've made as a CISO?

Early in my CISO career, I was on the cusp of enacting a global network and security transformation. I worked hard to build a strong business case and payback to illustrate the value. However, times were tough, so my budget was reduced, and I was still asked to lead and complete the transformation.

I embraced what I now call "the power of federation." I reached out to all the key partners for help and found win-win strategies. I obtained significant discounts for professional services. For software, I consolidated contracts in the U.S., since our budget was euro-based, allowing us to benefit from the exchange rate. Ultimately, we finished the project under budget.

We saved significantly on operating costs, strengthened enterprise security, enhanced network quality of service and consolidated servers. The project inspired multiple case studies and resulted in a Network World All Star award.

Essentially, the most profound executive decision I made was to ask for help and not quit. I learned early on that building strategic, trusted partnerships and strong business relationships can be a great asset to all parties.

◆◆◆ ——————— - —

Key takeaways

Follow these guiding principles:

- Embrace change fearlessly.
- Build and maintain trusted partnerships.
- Manage priorities effectively.
- Foster a culture of respect and trust.
- Leverage communication and relationship management.
- Differentiate requirements from "desirements" in projects.
- Manage stakeholder expectations.

These ingredients are key to success:

- Collaboration and communication
- Envisioning and storytelling
- Program management
- Negotiation and vendor management
- Strategic cost optimisation

Want to learn more from IT leaders like Arun DeSouza? Browse our full CXO Corner collection, featuring thought leaders from Westerra Credit Union, Google, Ignite Brewing, VMware and more.

6 Computer Vision Trends
Transforming the Business Landscape

New data from Insight and IDG reveals how the success of early adopters is driving new perspectives, investments and applications of computer vision across industries.

Computer vision:
The use of machine learning to recognise and respond to input from cameras or video

This emerging technology ranks among the fastest growing applications of Artificial Intelligence (AI) today — and early adopters already report significant benefits.

To help businesses navigate this rapidly evolving landscape, Insight commissioned a MarketPulse Research survey from IDG, uncovering key computer vision trends across energy, manufacturing, transportation, retail and healthcare industries.

---

1 Adoption is accelerating.

86% of businesses expect investments in AI to increase over the next 12 months.

While just **10%** of organisations are using computer vision today, **81%** report they're currently **investigating or actively implementing the technology**.

Plans to implement computer vision by industry:

Industry	%
Retail	58%
Manufacturing	38%
Transportation	35%
Healthcare	35%
Energy	20%

---
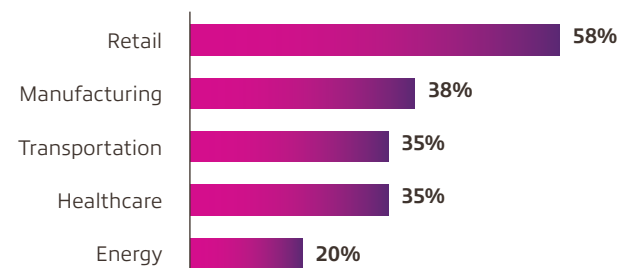
4 Seeing is believing.

As organisations investigate the value and feasibility of implementing computer vision, time-to-ROI is a key consideration.

72% of businesses expect to see a Return on Investment (ROI) within two to three years. But those that have put computer vision into production are more likely to expect **ROI within just one year**.

Early adopters are also the most likely to strongly agree that computer vision has the potential to grow revenue.

---

2 The value of visibility is clear.

96% of respondents agree computer vision can help their organisation **grow revenue**.

97% agree computer vision can help their organisation **save time and money**.

Among those investigating, planning to implement or actively using computer vision:

45% see opportunities for **cost cutting** and **efficiency gains**.

45% cite the technology as a **driver for innovation**.

---

5 Expertise is essential.

As with any new technology, there are bound to be challenges or concerns inhibiting early investment. Across industries, **organisations reported common obstacles**:

Obstacle	%
Security, privacy and/or compliance	68%
Concerns about data overload	53%
Lack of knowledge or capacity to manage	52%

To overcome these challenges, the majority of organisations report a high likelihood to **seek support from external consultants** or system integrators.

	%
Strategy and planning	90%
Implementation	87%
Production	84%

---

3 Common drivers include safety and security.

Specific applications for computer vision vary by industry, but across the board, **the most common use cases include:**

Use case	%
Improving security	78%
Improving employee safety	71%
Improving customer experience	58%
Anomaly or defect detection	58%
Process optimisation	57%

---

6 Early adopters gain an early advantage.

While just 10% of organisations have positioned themselves at the forefront of this trend, there's ample opportunity for other early adopters to capitalise on the benefits of computer vision.

As more organisations shift from investigating to investing in this technology, those that get ahead of the curve and put the technology into motion will capture ROI and gain a competitive edge.

For deeper industry analysis and a breakdown of the survey results, access the full report: **Early Adopters See Value in Computer Vision**.

IDG

How To Secure Your Remote Workforce

41%
of businesses concede that their remote working solutions aren't as secure as the office

Almost overnight, millions of people were forced to grapple with the challenge of flexible working. Meanwhile businesses had to find new ways to support a disparate workforce and maintain the same quality of experience for clients.

The idea of remote working is not a new one and is a pillar of most digitalisation programmes. But different companies are at different stages of their transformation and many did not have the processes and technologies in place to cope with such abrupt change. In early March 2020, 54% of HR leaders said that poor infrastructure was the biggest barrier to effective remote working in their organisation.[1]

The consequence was that many businesses were forced to adopt ad-hoc solutions and improvise where necessary.

But in this rush, there is a risk that cybersecurity may have been neglected. Many businesses may have viewed the risks as acceptable given the need to ensure business continuity and the other financial and operational challenges that the pandemic had created.

When countries across the world first entered lockdown early last year, businesses were faced with unprecedented disruption, as all but essential workers were told to stay at home.

This reality is something that many businesses acknowledge, with 41% conceding their remote working solutions are not as secure as their office-based infrastructure.[2]

Such a situation is untenable. Half of workers (48%) will likely work remotely at least part of time in a post-Covid-19 world as many businesses shift towards a hybrid office model.[3] Without appropriate action, businesses face catastrophic data breaches and jeopardise the benefits of long-term digital transformation.

The security challenges of remote working

The biggest issue is that the shift to remote working renders traditional approaches to security obsolete. Since data and applications are no longer confined to PCs on a local network in a physical office, static-based security systems characterised by firewalls and perimeter fences no longer work.

A remote workforce is collaborating and sharing corporate data from multiple locations across public Internet connections, possibly on devices that aren't controlled by IT. Combined with poor user habits and the ingredients are there for a potentially disastrous situation.

Consider a scenario where an employee is using unauthorised applications on their own laptop that hasn't been patched with the latest updates on an unsecured public Wi-Fi network. If that isn't concerning enough then what about another employee that accesses corporate data on an

unauthorised smartphone and loses their handset? A hacker can leverage any opening to unleash havoc and steal valuable data.

Steps to take to improve security

As businesses progress to the next stage of their digital transformation, security cannot be an afterthought. It must be included by design.

Firstly, businesses should adopt dynamic-based security measures that focus on data protection and user verification. Mobile Device Management (MDM) tools such as those included in Microsoft 365 allow organisations to determine which users, applications and devices can access corporate data, and require staff to apply encryption-by-default, Two-Factor Authentication (2FA), and PIN codes.

Data Loss Prevention (DLP) and advanced monitoring capabilities prevent the threat of accidental or deliberate dispersal of data by employees. As many as 26% of remote workers have suggested they are tempted to keep copies of valuable company data in case of insolvency or redundancy.[4]

Cloud-based infrastructure not only provides businesses of all sizes with flexibility, cost-efficiency, and advanced capabilities, but can also improve protection. Public cloud platforms such as Microsoft Azure are protected by billion-pound investments in security. Cloud-based applications are updated automatically so users are always using the latest, most secure version.

The cloud can enhance security even further by minimising the amount of data that needs to be stored locally, reducing the surface area vulnerable to cyber-attack and lowering the risk of data being stolen.

More than a quarter of all cybersecurity incidents detected by the UK in 2020 were Covid-related

Windows Virtual Desktop allows staff to access a familiar desktop and key Office 365 applications on any device, and collaborate with each other, entirely in the cloud. This improves both security and productivity as staff don't need to learn any new skills.

The human element

But no matter how secure you make the endpoint, there is one security cliché that happens to ring true for many businesses – humans are the biggest security threat to your organisation. Staff can inadvertently fall victim to social engineering or phishing, unleashing malware onto your network and leaking valuable login credentials. This risk could be heightened if they are distracted at home.

While it's important to have the right processes and protections in place, staff should be educated and trained where appropriate.

This is particularly important given the number of hackers looking to exploit the crisis. The increased number of attack surfaces and lacklustre security strategies have given rise to sophisticated malware and ransomware attacks, while targeted phishing campaigns that use alleged information about furlough schemes, vaccines and tax returns have increased. All it takes is for one staff member to fall victim to a scam.

Indeed, the UK National Cyber Security Centre estimates that one in a quarter of all cyber incidents in the past year related to Covid-19.[5]

Coronavirus has necessitated a rethink about how and where work is done and many of the measures put in place will ease the path towards long term transformation. But an important part of this journey is a modern cybersecurity strategy.

41% of SMBs believe ensuring the security of data in dispersed environments is a major challenge[6]

The abrupt shift to remote working by default has necessitated innovation and improvisation. But in this haste to ensure business continuity, there is a risk that cybersecurity has been neglected. Here's how businesses can sure their remote workforce is safe and secure.

Find out how secure your organisation really is and how you can protect your business from an ever-evolving landscape with a **Microsoft Security Workshop**

[1] Gartner (2020)
[2] Cloud Industry Forum (2020)
[3] Gartner (2020)
[4] Deloitte (2020)
[5] NCSC (2020)
[6] Insight SMB and Mid Market Business Review (2020)

3 Key Challenges Facing Business Optimisation

And How a Technology Partner Can Help

Leveraging trending technology can optimise your business costs and operations — but how do you navigate the constant evolution? With the right tools and technology partner, you'll help your business reach its full potential.

The impact of COVID-19 across industries has driven business optimisation at an unprecedented pace. Virtually overnight, companies were forced to design and execute highly complex projects, including remote work, infrastructure adaptations, digital modernisation and additional security layers to support rapid change. To ensure resilience, organisations have been tasked with overcoming these challenges and more, all while growing and supporting the company.

As pandemic restrictions change, many businesses are permanently transitioning to a hybrid workforce environment: a mix of on-site and remote employees, modern digital experiences, and on-demand access to software and solutions. With this shift, optimisation across the new IT landscape becomes incredibly important. IT departments worked tirelessly to implement urgent transformations in 2020; we'll need to reexamine where those systems stand today, as well as areas for enhancement.

Navigating a post-pandemic world will come with its share of additional challenges, and strategic optimisation can reframe the future of business.

There's a new ask of IT:

Be the innovators. Technology teams are expected to function as a profit center, rather than a cost center. So, how do you optimise costs and increase output? It's all about the right technology.

But let's take a step back: What exactly is business optimisation, and how does it apply to you? At Insight, we look at optimisation as the process of improving the efficiency, productivity and performance of an organisation. This can apply both to internal operations and external products.

Big data and connective technology can be used to influence new approaches that drive business optimisation — allowing organisations to achieve more.

Optimising your business may look like:

- Reducing costs with improved productivity
- Enhancing cybersecurity with modern tools
- Utilising advanced software to streamline operations
- Applying new onboarding systems for hybrid workers

At the heart of each optimisation lies one crucial benefit: speed. By improving the pace at which you accomplish goals, you'll save valuable time — and the old saying holds true: Time is money.

By leveraging trending technology, you'll optimise costs, achieve your goals and thrive in an evolving digital world.

Let's explore three key challenges in today's technology that are apt for optimisation.

At Insight, we offer testing, assessment and auditing services for your current cybersecurity.

Whether you're looking to satisfy compliance requirements or need a long-term remediation roadmap, we can help. Our technicians leverage more than a decade of experience and two dozen testing tools to pinpoint vulnerabilities and security weaknesses.

1. Heightened cybersecurity

When it comes to key risks facing businesses today, it's impossible to overemphasise the importance of security. The rapid transition to remote and hybrid work brought about an urgent need for heightened cyber defense. In today's world, becoming a victim of a cyberattack is a matter of when, not if.

A cyberattack can bring down your entire IT system, resulting in extreme financial loss, damaged reputation and countless additional fallout. Having the most up-to-date cybersecurity in place is vital to detect, stop and respond to attacks in real time.

Particular concern in today's hybrid world surrounds Artificial Intelligence (AI).

The rise of AI in cybersecurity is rapidly evolving, and hackers are utilising its tools and reliance on the cloud for advanced cyberattacks.

You'll want to employ solutions that protect every part of your IT environment, including:

	Endpoint security: Keep your devices safe from cyberthreats and malware — wherever you use them.
	Email security: Unlock tools such as firewalls, encryption and filtering to make it difficult for hackers to gain entry to your internal systems.
	Application security: Minimise the risk of threats, breaches and code hijacking.
	Identity and access management: Enforce appropriate access to critical systems for your workforce and customers.

2. Innovative devices and lifecycle management

Devices are essential to business operations, with billions in use today. Maintaining high workforce productivity (and improved profits) requires the right tools at the right times, and having modern, fast devices will increase employee satisfaction and retention. However, managing the device lifecycle can consume the bulk of your budget. In fact, PCs continue to make up the largest capital component in the annual IT budget for many enterprises.

So, how can you find and utilise the right tools without breaking the bank? A technology partner can eliminate the time and hassle of managing multiple hardware vendors, ensure maximum uptime and lifespan, improve user experience and reduce device total cost ownership. We'll talk more about the benefits of choosing the right partner below, but first, let's look at software optimisation.

3. Software and process automation

In today's constantly evolving digital space, having the right software to support your work is crucial to success. This is especially important if new employees are joining your organisation from a fully remote setting. With devices that are ready to go and equipped with the right software, your team will onboard with ease, and you'll save time (and resources) from the start.

The right tools can also automate repetitive processes, eliminate redundancies and free team members to focus on important tasks. With today's optimisations, you'll see improvements in:

Productivity:	Business applications can streamline your operations and improve efficiency, collaboration and performance.
Creativity:	Your team can produce unparalleled work with feature-rich platforms for designing, editing, drafting and more.
Networking:	Powerful networking applications keep your users and devices connected across your business.
Operating systems:	With an efficient, robust operating system, you can seamlessly manage hardware and software resources.

Applying advanced technology tools in these areas can lead to pivotal optimisation for your business, but staying up to date with trending tech can be a job in and of itself.

New technology is increasingly complex, and we're dealing with an expanded surface area — more devices, a dispersed workforce and accelerated cloud migration. That's where a technology partner comes in.

With advanced technology — and the right partner — optimisation is within reach. Get started with Insight.

About the author

Bob Bogle
Regional Vice President & GM Corporate Technology Sales, Insight

Choosing the right technology partner

We've covered how utilising technology can optimise your business cost processes and more — but what if you could take it one step further and optimise the entire process?

When finding the right technology for your business, you might spend valuable time juggling vendors for the right product, only to be left with no issue support, maintenance, licensing assistance and overall partnership. Procuring software, for example, can come with a host of challenges: unused products, auditing issues, duplicated technologies, wasted resources and more.

A full-service technology partner, like Insight, will subvert these challenges and bring you improved efficiency, effectiveness, compliance and strategic alignment. When you're looking for the right partner, you'll want to ask a few key questions:

- Do they have an extensive breadth of capabilities?
- Do they offer end-to-end solutions?
- Do they provide a seamless marriage of products and solutions?
- Are they adept in modern services and devices that support digital transformation?

The ideal technology partner will not only help you find the right technology, but will also provide unmatched benefits before, after and along the way. Through Insight, you'll find optimised software costs, better forecasting for future needs, consistent compliancy and greater asset visibility. Our powerful tools and deep partnerships become your crucial advantage.

How to Reboot Your Business on a Shoe-String Budget

COVID-19 has acceleratated digitisation by 4 years

Most small business owners expect to face some obstacles on the path to success, but few could have predicted or prepared for the experience of the past 18 months.

Many SMBs have fought for their very survival after lockdown restrictions and social distancing measures.

Businesses that were unable to trade remotely had to suspend operations, make redundancies, furlough staff, and exhaust cash reserves just to keep going. Amid such uncertainty, it's no wonder that one in three small firms that closed were unsure if they would ever open again.[1]

But there is now light at the end of the tunnel.

A phased easing of restrictions and gradual restoration of freedom to socialise is set to unleash pent-up demand for goods and services.

Analysts believe the economy will expand by as much as 6.8% in 2021 and this growth represents a huge opportunity for SMBs to get back on track – if they can adapt to the transformation that occurred in their absence.[2]

Changing world

The world has changed significantly since March 2020 and technology has become vital for businesses that were able to work remotely and maintain continuity.

Hurriedly improvised solutions eventually gave way to more sophisticated, holistic strategies that allowed staff to communicate, collaborate and securely access corporate data and applications from any location. Meanwhile, new models of service delivery allowed businesses to continue to serve customers.

Many of these changes will become permanent. Businesses have made significant investments in new technologies, employees have become used to flexible working, and customers now expect digital-first services. Digital is no longer optional or desirable – it is essential. In fact, it is thought that Covid-19 has accelerated internal digitisation by up to four years.[3]

SMBs that resume trading in the coming weeks and months must adapt to a more digitised, expectant customer base, while at the same time to rapidly scaling up to meet demand after a year and a half of hibernation.

If the coffers are bare, then the cost, speed and scale of the required transformation can be daunting – but cloud technologies and the 'as-a-Service' model can be the answer.

Here's how...

Cloud is a cost-effective way to scale up quickly

Cloud providers deliver infrastructure and applications over an Internet connection, providing businesses with systems, services and capabilities that would otherwise be financially or practically beyond their reach. These solutions also give SMBs the agility and flexibility to react to customer demand and support a fluctuating workforce.

All costs for Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), including maintenance and updates, are included a monthly subscription and businesses always have access to the latest version of each application. This model means businesses do not have to make significant investments in on-premise infrastructure and are not burdened with additional maintenance expenses during periods of lower demand.

Greater protection against catastrophic (and expensive) data breaches

The operational, reputational, and financial consequences of a security incident could be fatal for any post-pandemic recovery. Fortunately, the cloud can provide greater protection than on-premise equipment. Public cloud vendors invest billions in security and apply patches automatically, providing greater protection for customer and corporate data and minimising the threat of a breach.

Digital experiences that drive revenue

Cloud provides SMBs with a platform for innovation so they can provide the digital experiences that customers now crave. Cloud infrastructure enables businesses to roll out new services faster and more easily, while cloud-based applications facilitate multiple customer communication channels and the digital delivery of services. More satisfied customers mean greater loyalty and more sales.

Work smarter, drive efficiency, and maximise resources

As separate cloud platforms can aggregate data into a single repository, multiple applications can share information. Businesses can take advantage of cloud-based analytics and AI capabilities to automate processes, offer personalised, targeted services, and make better business decisions.

The result is a more efficient business that maximises resources and ultimately generates more revenue.

SMBs globally are expected to spend $1136bn on IT in 2021[5]

For example, AI chatbots can ingest an entire organisation's database to automatically field customer queries at any time of day. Customers receive instant answers to common queries, boosting satisfaction and reducing the amount of time staff spend fielding enquiries. Meanwhile, Microsoft Office 365 applications learn the behaviour of individual users to automate tasks and make suggestions.

The economy could grow by 6.8% in 2021

Ditch expensive office space with secure remote working

It's not just customers that are more demanding. Employees have become accustomed to working from home during the pandemic and many want this to continue once the world returns to normal. Several major organisations plan to allow continued remote working, and the right to work remotely could eventually be supported by government legislation.[4]

Cloud technologies provide SMBs with a platform to support a remote workforce, help drive productivity and improve employee satisfaction. SMBs can consolidate, abandon, or repurpose physical office space, and businesses that had to close offices during the pandemic will be able to get back up and running more quickly. In the longer-term, businesses will bill benefit from a wider talent pool if jobs are no longer restricted to a single location.

An important caveat is security. Remote workers are not protected by the protections afforded by office networks and systems and there is a need for additional security.

Microsoft 365 includes Mobile Device Management (MDM) capabilities that ensure only approved devices and applications can access corporate information and enforce policies like encryption and mandatory PIN codes. MDM can also remotely wipe a device if it is lost or stolen, but Windows Virtual Desktop goes one step further by offering a virtual machine that ensures no data is stored locally at all.

Cost-effectively equip staff with the right hardware with Device-as-a-Service

The benefits of cloud services can only be realised with the right end user hardware. Although many staff will want to use their own devices for work, outdated or unsuited PCs and smartphones could harm productivity and security and increase maintenance requirements for IT teams. For cash-strapped businesses, the up-front costs of new hardware are prohibitive.

Device-as-a-Service applies the subscription model to hardware procurement, combining the cost, delivery, setup, maintenance, and disposal of devices into a single monthly fee – and this can further ease pressure on budgets.

Optimise resources with outsourced helpdesk and security

The shift away from the office means traditional IT helpdesks are no longer as effective. Outsourced IT helpdesk and security support ensures every part of an organisation's infrastructure is working effectively – regardless of where the member of staff is located. IT departments also gain more time to work on projects that drive genuine transformation, rather than fixing laptops.

It's been a tough year for everyone, but the end is in sight. Businesses that leverage loud technologies and adopt the as-a-Service model businesses are in the best possible place to bounce back without incurring significant financial stress.

Find out how Insight can help your organisation become more resilient and ready to grasp the opportunities that lie ahead.

As the economy reopens, small businesses that have managed to survive the pandemic have an opportunity to bounce back. The cloud and the 'as-a-Service' model can deliver the capability and scalability required to seize opportunities without breaking the bank.

Find out how Insight can help your organisation become more resilient and ready to grasp the opportunities that lie ahead.

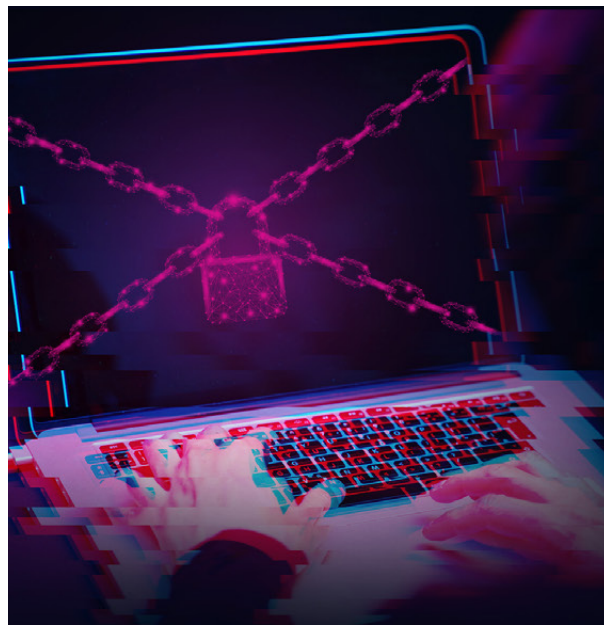[1] Federation of Small Businesses (FSB) (2020)
[2] EY (2021)
[3] McKinsey (2020)
[4] The Guardian (2021)
[5] Analysys Mason (2021)

Mounting a
Ransomware
Defence
for the Big Picture

When it comes to ransomware defense,
protective controls have always been
critical — but more security pros are
saying goodbye to a siloed approach.

The 4 basic ransomware types:

1. **Application-level lockers** prevent users from accessing applications or operating systems until a ransom has been paid.

2. **System-level lockers** overwrite a system's Master Boot Record (MBR) with its own microkernel, preventing any type of use until a ransom has been paid.

3. **File encryptors** encrypt user files and data, demanding a ransom for the release of the decryption key.

4. **Fake ransomware** is malware that claims to have encrypted a user's data but actually hasn't; ransomware language is used to collect a panic-induced payment from the victim.

It's time to go beyond protective controls

A layered approach to preventing ransomware is not all that different than the approach that we take with malware. Yes, it means keeping the bad guys out by deploying effective endpoint security and teaching users not to click on malicious links or unknown documents. It also means improving threat intelligence, particularly around command and control. The protective, or preventive, side of ransomware defense is straight forward — limiting the vectors that the ransomware actor has to inject into an environment.

But when it comes to ransomware, it's not enough to just keep bad actors out. We must also focus on the recovery and continuity aspects of security. To do this, organisations need to ask themselves key questions like:

- What is my storage environment doing to help me recover?
- How can my data protection help me recover?
- How quickly can I restore entire environments in the event of an attack?
- How do I effectively secure these environments?
- How do we get back up and running in a way that avoids putting our last resort data back into a compromised environment?

According to Sophos' State of Ransomware 2021 survey, the number of organisations that paid a ransom increased from 26% in 2020 to 32% in 2021 — but fewer than one in 10 (8%) managed to get back all of their data. As lose-lose situations like these become more commonplace, having the nuclear option has become increasingly helpful to security teams.

Three mantras to live by

As you pursue excellence across your ransomware defense strategy, remember:

1. There's no silver bullet.
We all wish it were true, but there's no one holy grail product that will stop ransomware in its tracks. A tool may be a very important piece of a strategy and response plan, but there's no point solution that covers it all.

2. End-user training will always be vital.
You can have all the sophisticated tools in the world, but the end user will always be the weakest link. Make training a priority. Make it fun. Do whatever you need to do to keep end users invested in your security policies.

3. There's no start and stop.
The most successful teams look at ransomware defense through a business continuity lens. Test your methodology, and test it often — whether it's annually, bi-annually or however often your business deems it appropriate. Every 10–11 seconds, an organisation will fall victim to a ransomware attack according to research compiled by PurpleSec. That's simply too often for a "set it and forget it" strategy.

Options like immutable storage and backup are becoming popular, despite them being last-resort solutions.

As we move from the traditional data center model to centers of data and see more edge computing involving artificial intelligence. These areas, along with remote workstations, need to be protected with the same type of multilayered approach.

> " In the 90s, when there was a security issue, the IT pro might have said 'Let me buy this tool to fix it.' But that's not the case anymore. "

About the author
Chris Kapusta
Senior Manager for Cloud + Data Center Transformation, Insight

Always be evolving. Explore more ways to ensure a strong defense — from assessing readiness to strategising across key focus areas.

Tech
J O U R N A L ™

Events

27th October	**Apple - Buy and Try On-demand** *(live 27th October)*
10th November	**Discover 2022** **Reserve your place**
18th November	**Intel - Skills for innovation Program** **Register now**

Insight.