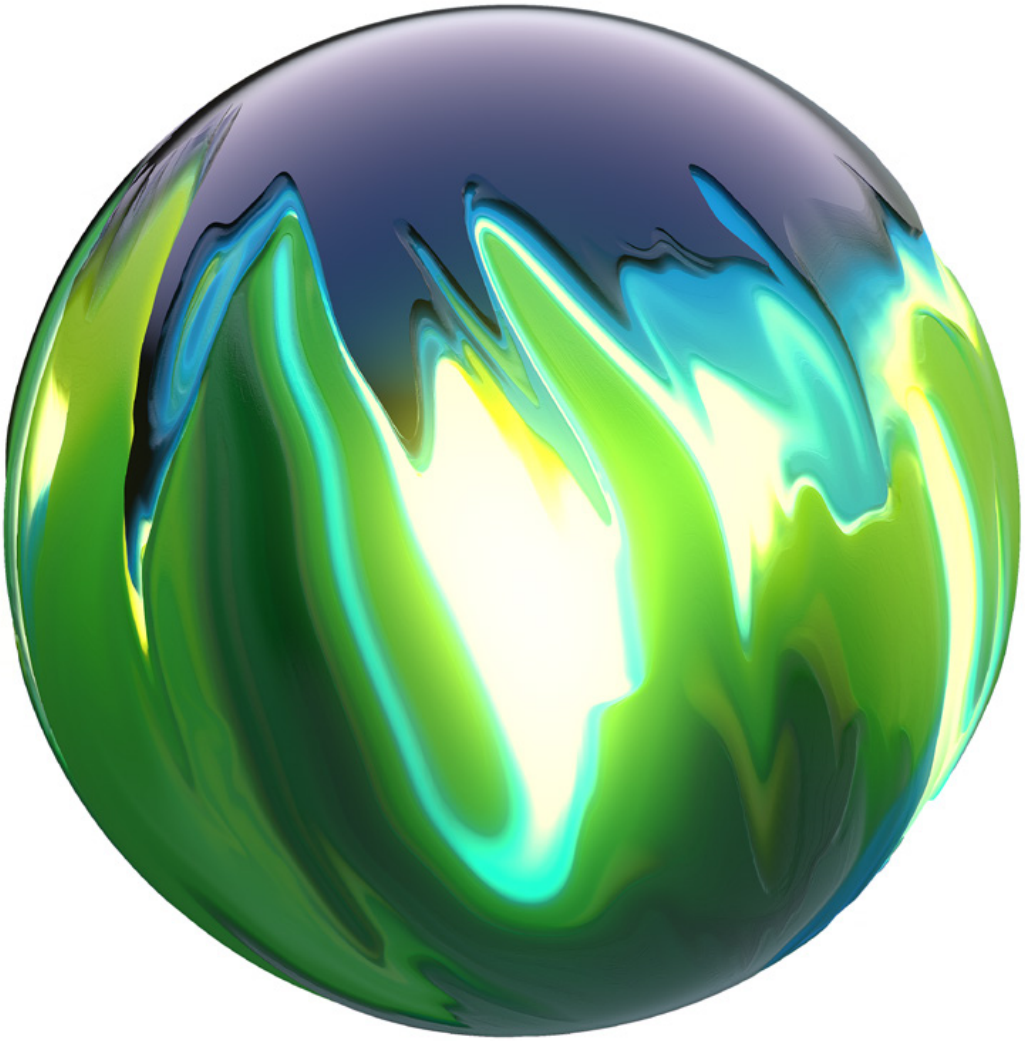
Deloitte.



2021 Future of Cyber Survey

Complexity is the new normal. How companies are achieving visibility.

Deloitte Cyber | Empowering your people for the future

MAKING AN IMPACT THAT MATTERS since 1845

Future of Cyber Survey

Methodology

The **Deloitte 2021 Future of Cyber Survey**, conducted by both Deloitte and Wakefield Research, polled nearly 600 C-level executives about cyber security at companies with at least $500 million in annual revenue including nearly 200 CISOs, 100 CIOs, 100 CEOs, 100 CFOs, and 100 CMOs between June 6 – August 24, 2021 using an online survey.

Gaining visibility into complexity

Today, we find ourselves living the reality of a cyber everywhere world where digital transformation initiatives continue to accelerate amid the emergence of a pervasive remote workforce. It often appears as if technological innovation and the culture it produces are surging ahead of our ability to understand, measure and respond to exponentially increasing risk.

Despite the elevated risk environment, digital transformation and migration to the cloud continue to be priorities for our clients. More than simply improving efficiency, as data flows across organisations it drives new ways of value creation, connecting lines of business and using customer data to enrich experiences. Our survey data underscores this migration – 94% of CFO respondents indicated they are considering moving their financial systems or enterprise resource planning (ERP) to the cloud.

600
C-level executives

$500M
Minimum revenue

Headquartered

40% Americas
28% EMEA
32% Asia Pacific

The state of play

In order to remain competitive, today's enterprises run an array of technologies that combine on-premises infrastructure with hybrid information technology (IT) and an assortment of third-party cloud providers. These sophisticated integrated environments require new forms of management distinct from traditional in-house IT architectures. A clear plurality of the CIOs and CISOs we surveyed (41%) acknowledge that transformation and gaining visibility across increasingly complex hybrid ecosystems is the greatest challenge they face.

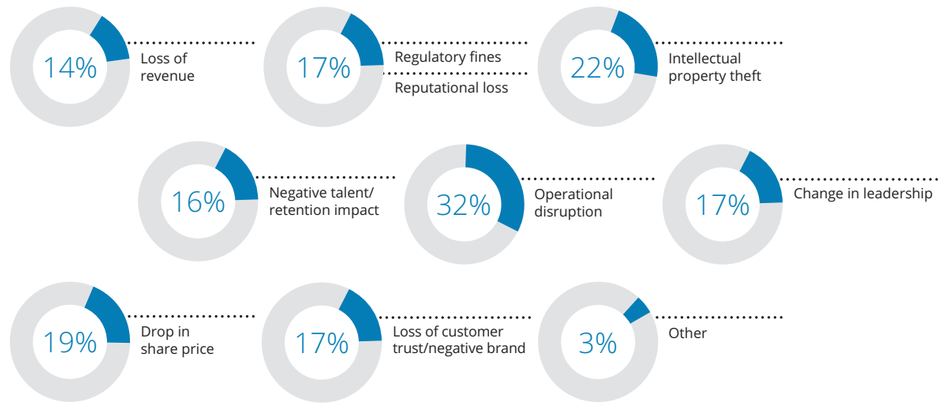
In addition to the pressures of the marketplace, the pandemic heralds the arrival of remote work as a permanent feature of employment. Organisations, large and small, have rapidly transformed work environments and in doing so dramatically increased their attack surfaces, often with little to no time to consider security implications. Not surprisingly, there's been an uptick in attacks, with 69% of respondents reporting an increase or significant increase in threats to their business between early 2020 and May 2021–this was consistent across industries and geographies. 32% of our global C-suite respondents indicated operational disruption was the greatest impact, followed by intellectual property (IP) theft (22%) and drops in share price (19%).

Never trust. Always verify.

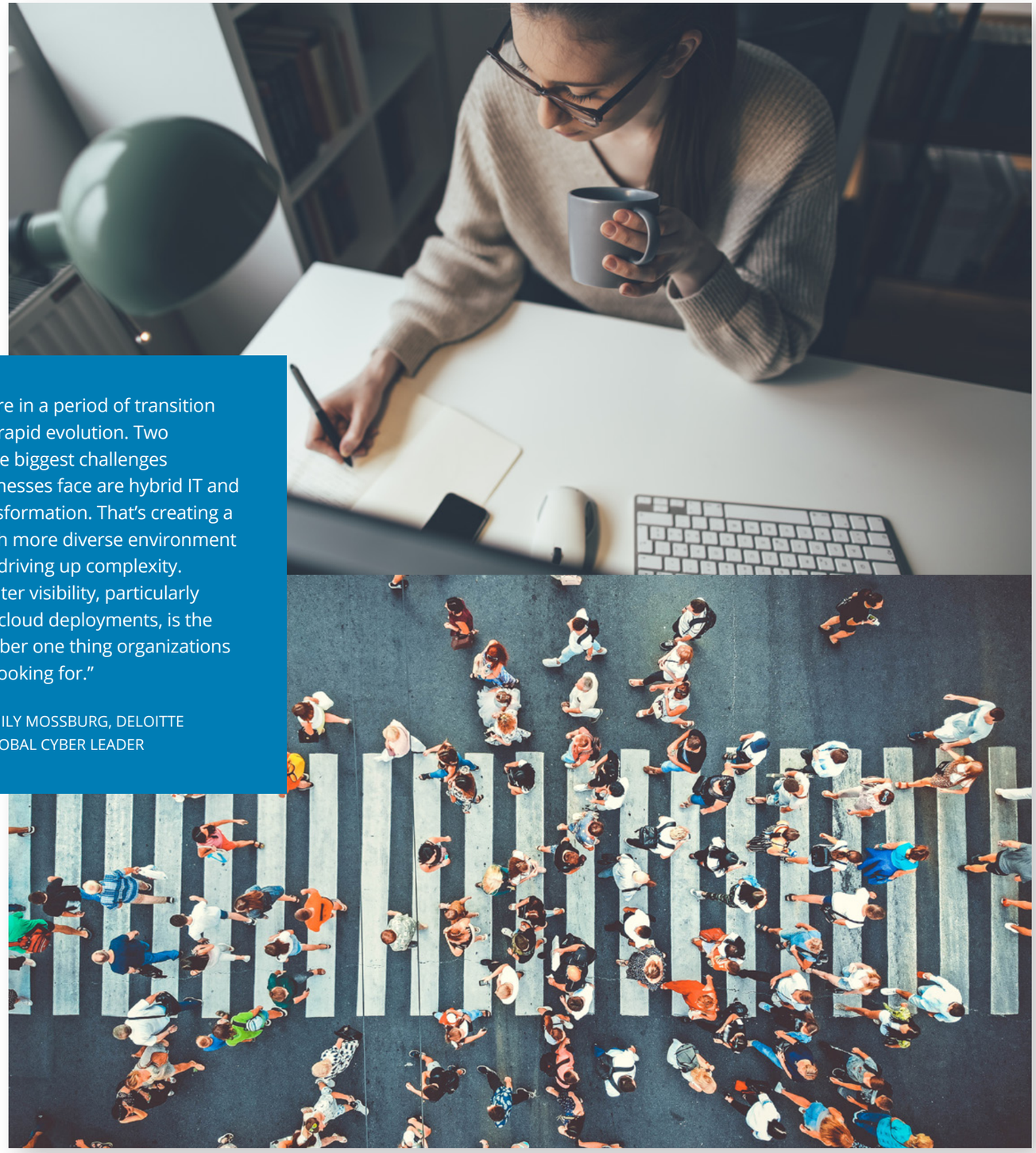
When asked, What are the greatest barriers to managing cyber security across their organisations? Respondents ranked data management traversing complex perimeters the highest (44%), followed by a need for better prioritisation of cyber risk across the enterprise (31%). Fortunately, it's now feasible to deploy Zero Trust architecture, which replaces simple verification of entities with real-time access decisions based on continuous risk assessment. When implemented it is an effective response to the dissolution of perimeters in today's ecosystems, recognising that every component in an architecture is vulnerable and every layer needs protection.

Made possible by recent advances in computational power, Zero Trust's emergence and adoption point to wider cultural shifts in organisations that reveal how the role of cyber is changing and its importance elevating. More than a technological fix, Zero Trust's set of interwoven solutions provide visibility into adversarial activity, associated business risk, and insight into changes needed to reduce the risk. This insight demands coordination between IT and business lines as well as enterprise-wide education and training.

Biggest cyber incident impacts*



*Respondents were asked to select up to two responses, so percentages will not add up to 100%.



"We're in a period of transition and rapid evolution. Two of the biggest challenges businesses face are hybrid IT and transformation. That's creating a much more diverse environment and driving up complexity. Greater visibility, particularly into cloud deployments, is the number one thing organizations are looking for."

— EMILY MOSSBURG, DELOITTE GLOBAL CYBER LEADER

Realigning your defenses

As hackers grow more sophisticated and understand the market value of assets – whether it's pharmaceutical IP, engineering and product patents, customer or other critical data – organisations continue to step up their cyber defense budgets. Almost 75% of respondents who had more than $30B in revenue said they will spend more than $100M on cyber security this year.

The challenge is to ensure this expenditure results in greater visibility into the amplified risk of today's increasingly complex ecosystems. Beyond acquiring technology and expertise, it requires organisational change to facilitate programmatic governance that extends beyond the enterprise to include partners and third-party providers.

As technology changes, so does the role of the CISO. Once cyber permeates an enterprise, it's imperative to reposition where the CISO sits in the organisation chart. Beyond simplifying reporting, closer relationships to the CEO enhance the CISO's ability to understand business priorities and to have visibility into innovations as they occur. This new operational role of the CISO with greater engagement across the organisation enables the cyber team to ensure necessary requirements, technical solutions and controls can be built into innovation initiatives from the ground up. This not only minimises risk at the outset but risk of overall product and service development.

This deeper cultural impact of cyber is why in this year's edition we've expanded the current survey beyond leaders with direct oversight for cyber to include those who should be cyber's greatest champions: CEOs, CFOs, CMOs, CIOs and CISOs. Their sentiments are similar to one another, with variations seen across geographies and industries.

The view to the future

There is no simple solution, organisational or technological, to gaining visibility into the growing complexity of integrated ecosystems that underpin modern business. However, there are a number of measures, organisational, cultural and operational, when taken together, that can enable organizations to embed cyber in the core of their business initiatives, in their culture and into their continuously evolving technology ecosystems.

In this report, we explore some of those measures and underscore the importance of organisations' ability to gain visibility into the risk which complexity creates now, and into the future as the next wave of technological evolution continues to increase our interconnectivity.

Cyber and the challenge of transformation

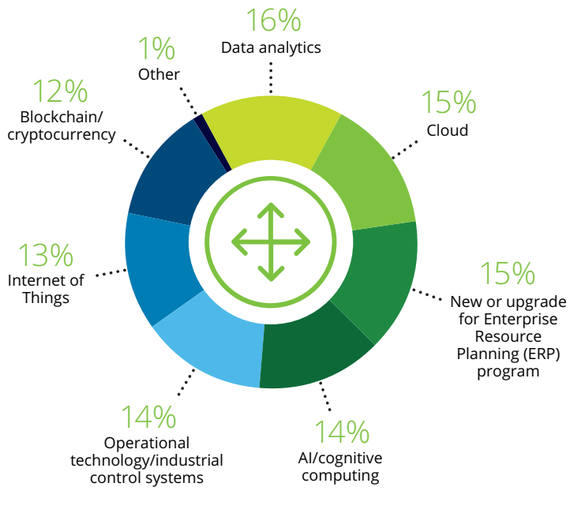
Across every industry, remaining competitive requires new services and products be rapidly developed and brought to market.

Much more than simply digitising existing processes, innovative business models are enveloping supply chains and creating novel realms of customer experience. This transformation also exposes enterprises to new forms of cyber risk, requiring new cyber strategies to protect evolving business models. To manage these risks, C-suite and Board members need to embrace the change, create effective governance across lines of business, and evolve risk management processes to achieve end-to-end visibility of all newly connected areas of business, including those run by third parties. Success depends upon the commitment of senior management, their ability to understand cyber risk followed by effective investment in security.

When asked to rank their digital transformation initiatives in the next 12 months, survey respondents rated data analytics number one (16%), followed by cloud (15%) and new or upgraded ERP programs (15%) as their top priorities. The addition of the operational technology/industrial control systems (OT/ICS) response option and resulting response selection (14% designated this as a top priority) to this year's survey is indicative of the efforts we are seeing across industry to digitise and modernise factories and operating technology environments.

The speed and scale of change is truly revolutionary. When the world rushed online at the advent of COVID-19 this became immediately apparent. Entire business sectors were transformed almost instantly as huge sections of the workforce suddenly began operating remotely. Fortunately, much of the required digital ecosystem – from cloud and shadow IT to ICS – was already in place and ready to scale up rapidly. But less obvious are the myriad cyber risks underlying this transformation, and few businesses currently possess the means to understand and mitigate them to an acceptable level.

How organisations are prioritising digital transformation initiatives



"The main objective for C-suite and Board members must be gaining a full understanding of the actual risk that digital transformation is exposing their companies to, as well as having the levers to manage that risk on a level playing field with all other types of risk."

— MATTHEW HOLT, GLOBAL CYBER STRATEGY & TRANSFORMATION LEADER, DELOITTE CYBER

Understanding cyber risk

Because today's cyber threats impact entire businesses, potentially crippling operations and rapidly destroying hard-won reputations, it is vital that boards assess cyber risk in terms they can understand. They need to be able to compare cyber threats to risks they are experienced at handling. Analysing cyber risk profiles should be as familiar as grasping the health of their balance sheet.

Once they can comprehend the nature and scale of the cyber risks they are exposed to, they will know where to invest to best mitigate dangers.

According to our survey, 41% of respondents indicated cyber maturity assessments are used to guide cyber investment decisions, 35% said they employ risk quantification tools, and 23% say they rely on the experience of the company's cyber leadership. When asked how often they conduct risk analyses/threat modeling for new and/or existing applications, 37% of CIOs and CISOs indicated they do so quarterly, and 29% do so monthly. While the responsibility for these assessments typically falls to CIOs and CISOs, it is critical the broader set of stakeholders understand the relevance and importance of such efforts.

Full speed ahead?

The pressure to compete at scale very often means business leaders' digital transformation efforts focus on outcomes without fully contemplating cyber risks. Beating the competition to market creates tunnel vision with significant blind spots.

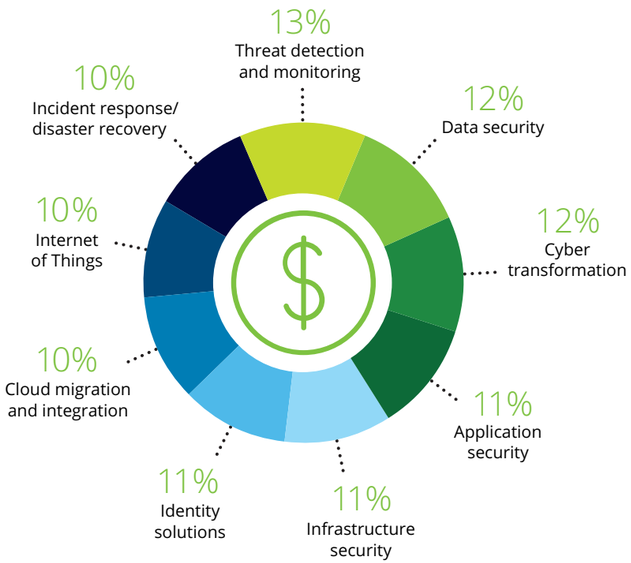
With cyber permeating everywhere from customer touchpoints to intelligent factories and the remote devices of employees, the days of a siloed IT department managing antivirus software and passwords are over. It's no longer enough to just keep the network running, broader and deeper thinking is required.

Today's CISO now needs the authority to influence all the lines of business, gather information from across the enterprise and be able to communicate directly with the board and senior management. Not to mention the investment of resources and talent to adequately safeguard the organisation's most strategic priorities and assets.

This is often a hard sell to the CFO, as what you hope to show from a large cyber investment is usually...nothing. Meaning, zero cyber incidents is money well spent. So how are CISOs planning their cyber budgets? In 2019, CISOs and CIOs told us that their cyber budget was evenly spread across various cyber programs. In 2021, this hasn't changed – CISO and CIO respondents again reported budgets are similarly divided. C-suite leaders should understand that to manage cyber risk there is not a one and done solution.

Therefore, cyber budgets are increasing with greater attention given to threat intelligence, detection and monitoring, cyber transformation plus data security. Across the globe, CISOs and CIOs are consistently investing in scaled cyber solutions in/for the cloud; cyber/technical resilience; and artificial intelligence (AI)-driven threat assessment and identification, to build their organisations' cyber defense.

Organisations' cyber budget is relatively evenly spread to broadly mitigate risk



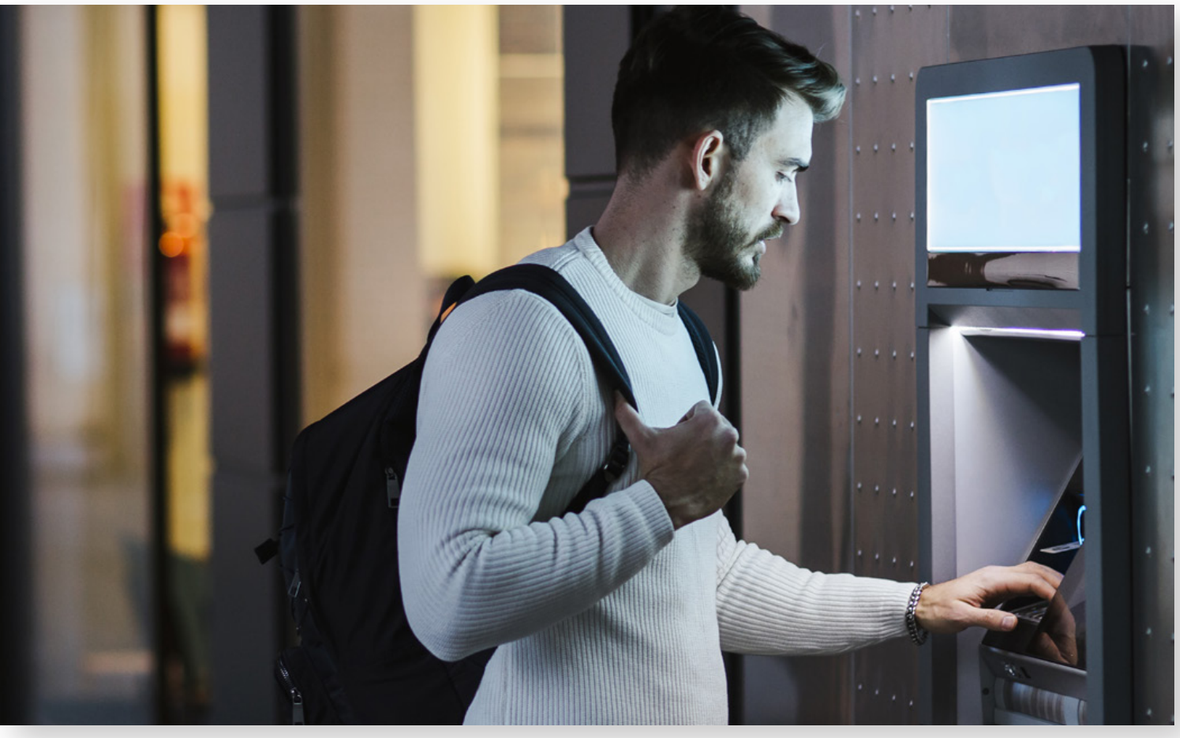
Building the right cyber team

It's not realistic to expect board members or the C-suite to become cyber security experts. But it's up to the board to build a cyber team that gives them the visibility they need and to provide pertinent information in terms they can understand. The key hiring decision needs to occur at the board or senior management level.

Individualised or intrusive? Using personal data ethically

People expect personalised, targeted experiences. We want everything from food delivery to travel and healthcare to be frictionless, based on our past interactions. What we don't want is the sense we're being followed everywhere by marketers feeding us an endless diet of coupons for things we're not interested in.

How companies manage customer data, connect online and in-person experiences while protecting privacy can be the difference between profit or loss and even long-term survival.



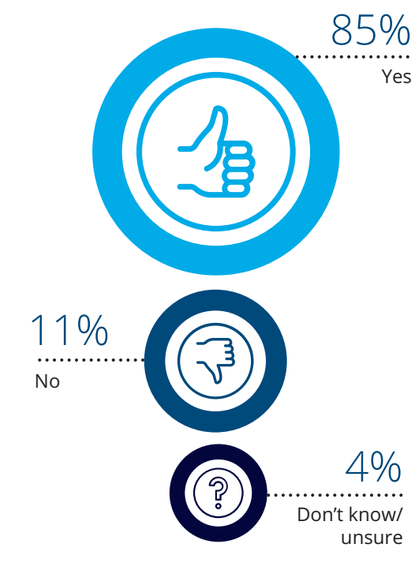
Privacy by design

For every customer-facing project, it's important to take privacy and security into account at the beginning. Ask yourself, how important for our business model is having this degree of intimacy with our customers? Carefully think through the type of information you need to provide the right level of service. Then understand who needs to access it and how it will be stored and protected. When we asked Chief Marketing Officers if they were able to measure and demonstrate compliance with global data privacy regulations, the majority (85%) responded that they could.

Avoid data bloat

Simply harvesting reams of data in the hope that it's useful in the future is a drag on resources and likely a recipe for failure. Customers resent giving up personal information when they don't clearly see a benefit. Collecting and effectively using data to create authentic, personalised and human experiences is a catalyst for growth. The flip side is the more data you have, the more risk you encounter. It's all about balance. When asked, the CMOs we polled were evenly split between answering it was more important to collect data to personalise customer experience versus more important not to collect personal data in order to protect against a breach.

Are you able to measure and demonstrate compliance with global data privacy regulations?



Value and trust

Today, people realise their personal data has intrinsic value. They see handing it over as an investment and want to know what is the return: providing personal information should make life easier. Like anything of worth, it must also be safe and secure. Also, people are demanding agency, seeking to choose how and when their data
is used. When companies reliably deliver on their promises, customer relationships deepen.

The extent customers trust your company is reflected in their behaviour. High trust scores correlate closely with repeat business – their chance of buying again rises 540% when they believe companies are reliable. Perhaps just as significantly, they will support you strongly on social media. As a result, trusted businesses greatly outperform the rest – for example, trusted companies were 2x more resilient during the past year.*

According to our survey, 91% of CMOs stated they feel their organisations balance data collection with engendering trust either "very well" or "somewhat well." Such a high confidence level begs the question, is this view shared by other C-suite members? It certainly points to the need for a collaborative approach to ensure blind spots aren't overlooked.

Ethics over regulation

Increasingly, consumers are deploying their purchasing power to support companies with sustainable environmental policies and are proactive on social issues. Their concern also applies to how companies use personal data.

Traditionally, companies have sought guidance from regulators about what they should and shouldn't do. While compliance with the various laws around the globe is vital, it's no longer sufficient to just assume people are willing to share personal data at all if you cannot explain the purpose. Plus, the explanation needs to be in plain language and easily understood.

Regardless of location, companies who bring trust into their DNA and clearly communicate their willingness to adhere to the privacy rights of customers are benefitting from greater faithfulness. Making it easy for customers to access, delete or move their data should be part of your simple and straightforward user agreement. When customers see that a company thinks through its data policies and can chart its own course, they are more willing to put their data onboard.

In your opinion, how well do you feel your marketing organization balances data collection with engendering consumer trust?

*Deloitte HX TrustID research October 2020 – June 2021

Make trust your guiding light

Outline the experience you're trying to create and understand the data that you need (and don't need) to do it. Hold everyone in the organisation accountable for building trust.

01 Begin with privacy by design.

02 Use the data that you collect. Don't collect data you don't need.

03 Dissolve silos so information is accessible and flows freely throughout your organisation.

04 Create seamless experiences that engender trust.

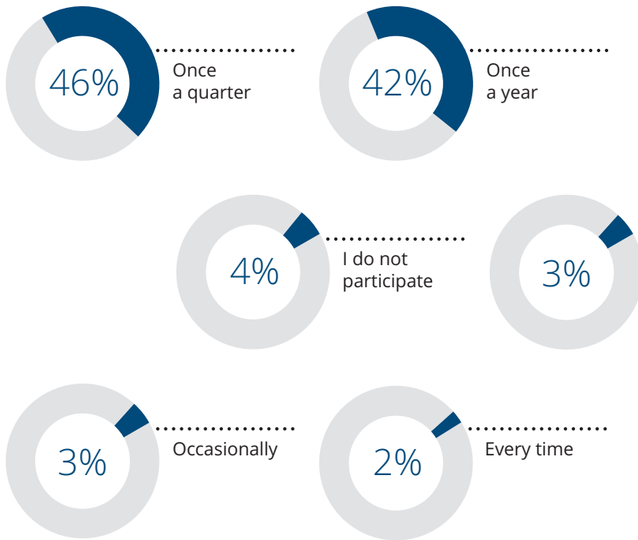
05 If/when there is a breach, use the moment to learn and build more trust from your mistakes.

06 Make your communication department integral to everything you do.

Dissolve the silos

CMOs and experience officers tend to make decisions based on brand and marketing requirements and only at the very end check with the CISO if data has been gathered correctly (and usually, the answer is, "No!"). Everyone is on a different team. One team sees their job as gathering as much data as they can, the other wants to only gather what's necessary and protect it. A better approach is to examine together what is the right balance between capturing the information required to deliver a seamless experience and the need to mitigate risk for both the company and its customers. Before using data to connect the dots of customer experience, organisations need people who can make connections outside of their silos. It's a two-way street. When designing privacy policies and communications, bring in marketing. This is increasingly central to brand intentions and messaging, so they can help.

How often do you participate in your organisation's Cyber Incident Response planning and testing?



Into the breach

Despite taking the greatest precautions, data breaches happen. It's wise to consider them an eventuality and be prepared. Getting caught flatfooted will make a bad situation worse. How you respond sends clear signals about your brand. Not only should you rehearse an incident response plan alongside your cyber team testing scenarios around a data breach but also collaborate on the recovery plan and related communications strategy.

According to our survey, CMOs indicated that work is being done to fully align with the cyber organisation with 46% saying they participate in such planning and testing once a quarter. Global responses vary with CMOs in Argentina, Germany and Australia revealing a higher level of integration with cyber teams over other countries.

> "Customers don't think about their data like businesses in terms of privacy, security, and identity. They think, 'Does the company have my best interests in mind? Are they using my data in a way that benefits me or them? Are they doing everything they can to keep my personal information tight?' "
>
> — ANNIKA SPONSELEE, GLOBAL DATA & PRIVACY LEADER, DELOITTE CYBER

When a breach does occur, regard it as your obligation to fully inform customers about what has occurred. Clearly outline the services you are providing in response and think about which channels of communication best convey your message: Does it warrant a personal letter from the CEO? A gift? Or other compensation?

Despite the gravity of the circumstances, deftly communicating with your customers can also be an opportunity to deepen your relationship with them. Handling a difficult situation well by putting the interests of your customers first can help your reputation to quickly rebound and inspire even greater trust.

Securing a world without boundaries

In legacy environments, IT resources were contained within clearly defined boundaries. Whatever resided externally was untrusted and all internal traffic was inherently trusted. And now? We live in a hyper-connected world, where everything is increasingly interconnected. The perimeter has essentially dissolved for most modern enterprises.

72% of survey respondents indicated their organisations experienced between one and 10 cyber incidents and breaches in the last year alone. When securing the enterprise, we can no longer inherently trust anything. The challenge today becomes, "how can you remove inherent trust altogether?" It's a revolutionary change to the way we build modern security architectures. Fortunately, Zero Trust has the capabilities to meet the task.

What is driving the move to Zero Trust

01 The rapid pace of digitisation is increasing IT complexity and driving up cost.

02 An increasingly mobile workforce now expects to be able to work from anywhere, on any device.

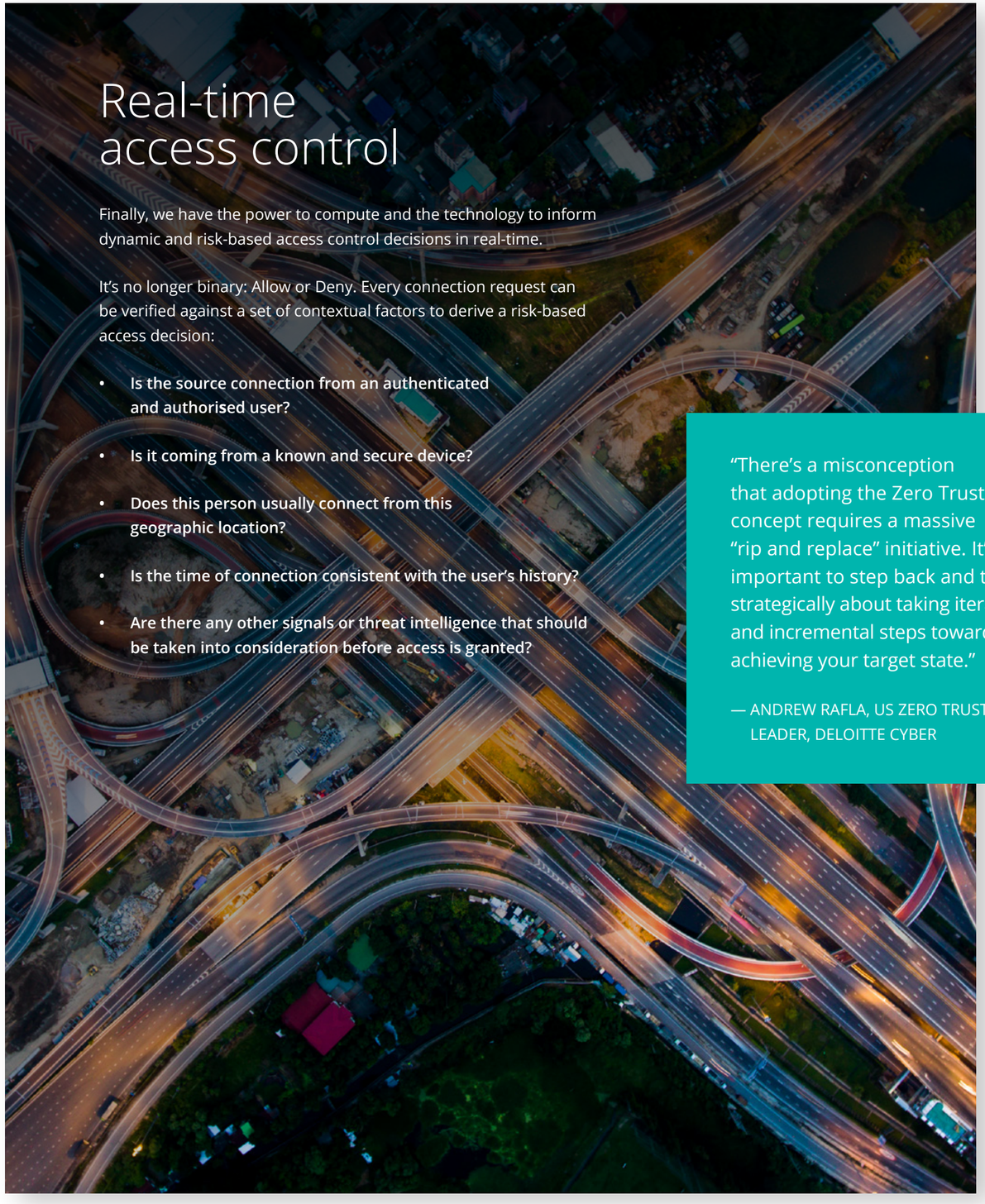
03 The development of digital products and services shifting towards cloud adoption.

04 The demand for better and easier business collaboration and supply chain integration.

05 Adversaries are very sophisticated and are outmatching current cyber defenses.

Enter Zero Trust

Zero Trust is not a technology or a single solution. It is a set of architectural policies that are based on the fundamental principle of "never trust, always verify". The concept commits to shifting from the traditional perimeter-based or "castle and moat approach" of managing security, to one where trust is established between individual resources and consumers, as and when required. With Zero Trust, trusted connections are established based on internal and external factors, which are constantly revalidated.



Real-time access control

Finally, we have the power to compute and the technology to inform dynamic and risk-based access control decisions in real-time.

It's no longer binary: Allow or Deny. Every connection request can be verified against a set of contextual factors to derive a risk-based access decision:

- **Is the source connection from an authenticated and authorised user?**
- **Is it coming from a known and secure device?**
- **Does this person usually connect from this geographic location?**
- **Is the time of connection consistent with the user's history?**
- **Are there any other signals or threat intelligence that should be taken into consideration before access is granted?**

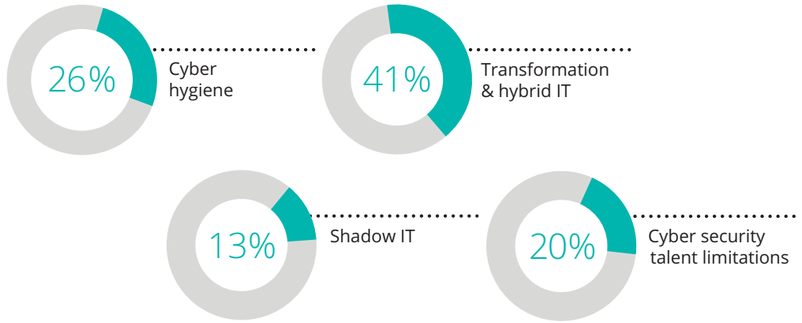
"There's a misconception that adopting the Zero Trust concept requires a massive "rip and replace" initiative. It's important to step back and think strategically about taking iterative and incremental steps towards achieving your target state."

— ANDREW RAFLA, US ZERO TRUST LEADER, DELOITTE CYBER

The current situation

Our 2021 survey outlines the challenges of managing cyber risk across the enterprise faced by CIOs and CISOs. Their greatest challenges are transformation and Hybrid IT, with cyber hygiene, talent limitations and shadow IT not far behind. Those challenges will only get more complex through accelerated digital transformations. We must start over and build security architectures that can sustain the increasing speed of digital transformation. The time to act is now!

Which of the following is the most challenging aspect of cyber security management across your organisation's infrastructure?



Step by step

Most companies – knowingly or unknowingly – have embarked on a Zero Trust trajectory. Their approaches differ by the degree they are tactical, architectural or strategically led. While Zero Trust is relevant across all industries and sectors, there is no one-size-fits-all solution. Zero Trust is a multiyear initiative – a transformational change, that breaks down the silos between business, IT and the various cyber domains. Any Zero Trust journey will face pitfalls and obstacles requiring strong leadership support, investment and buy-in from across your organisation to ensure success.

Consideration needs to be given to the business drivers, existing capabilities, and use cases relevant to your organization. It's important to keep cyber fundamentals in mind: What are you trying to protect? Where do those assets reside? Who (identities) and what (devices) should be able to access those assets, and under what conditions? To answer these questions, organisations need to prioritise IT asset management and data governance capabilities to understand the classification and criticality of their assets and data…and leverage this context when creating access control policies. Then defining your goals and embedding them in your end-to-end strategy is the surest way to achieve your desired business outcomes. This, however, isn't easy. When asked about their biggest challenge in managing cyber security across their organisation, "increase of data management/perimeter and complexities" was the number one hurdle cited by respondents.

Much more than a technology solution, Zero Trust is a cultural change. The change to the overall organization cannot be underestimated. Softer factors such as communications, role-specific training, awareness, and operational process adjustments are key elements for success. Overall, such programs require a strategy aligned to the business, supported by strong leadership, dedicated architecture, technical workstreams and compelling pilots, that coalesce the commitment across all stakeholders.

The road ahead

Tech giants are leading the Zero Trust maturity journey and apply these principles to develop, run and deliver secure services. Other leading organisations are adopting Zero-Trust strategies to support business priorities, digital transformation, and corporate risk strategies. When modernising your own architectures, understanding how the leaders innovated and achieved tremendous scale can help drive your digital transformation, too. There is no doubt the change is happening. The sooner you take charge of your transition to Zero Trust, the safer the journey will be. It's far better to be in the driver's seat, determining your destination…the time for Zero Trust is now.

An enormous upside

Embedded in a corporate strategy, Zero Trust can bring a series of strategic advantages. By reducing operational complexity and simplifying ecosystem integration it can:

- **Improve customer experience**
- **Enhance business agility**
- **Improve business resilience**
- **Reduce the threat surface**
- **Realise cost savings**
- **Improve collaboration with business partners**
- **Accelerate cloud adoption**

"The time has come to fully leverage Zero Trust principles and build modern security architectures, that can keep up and enable digital transformation."

— MARIUS VON SPRETI, GLOBAL ZERO TRUST LEADER, DELOITTE CYBER

"Many organisations overlook the risks associated with connecting existing technologies already in their environments. The attack surface increases across the entire ecosystem."

— DANA SPATARU, GLOBAL CYBER EMERGING TECHNOLOGY LEADER, DELOITTE CYBER

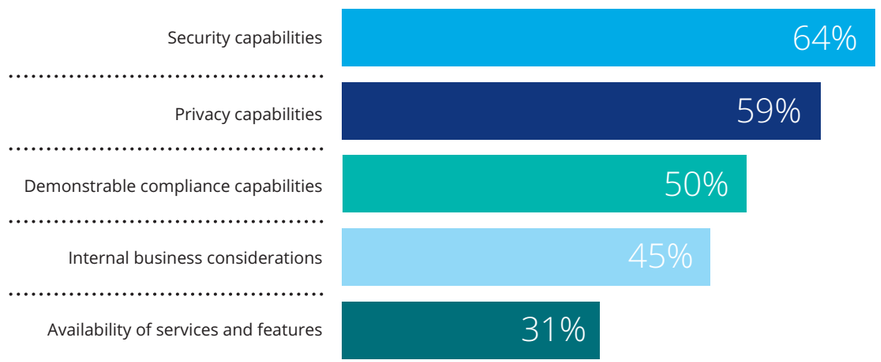
Connecting the emerging technologies spectrum

Headlines often focus on cutting-edge technologies like quantum computing, 5G, and digital twins but the full spectrum also includes brownfield technologies, like operational technology, that have existed for decades in the manufacturing environment.

What's "emerging," whether the technology is brand new or has long been deployed, is its connection to the Internet, and how the physical and digital worlds are becoming connected in nearly every way imaginable. We're witnessing a digital metamorphosis across everything from medical devices to transportation to agriculture and beyond. Not only is it transforming the way we make and use almost everything, but it brings security risks that were never conceivable before.

When CIOs and CISOs ranked what will drive their adoption of emerging technologies in the next three years, security capabilities came out on top (64%), followed by enhancing data privacy capabilities (59%), and compliance capabilities (50%).

Which of the following will drive adoption of emerging technologies?*



*Respondents were asked to select as many responses as apply, so percentages will not total 100%.

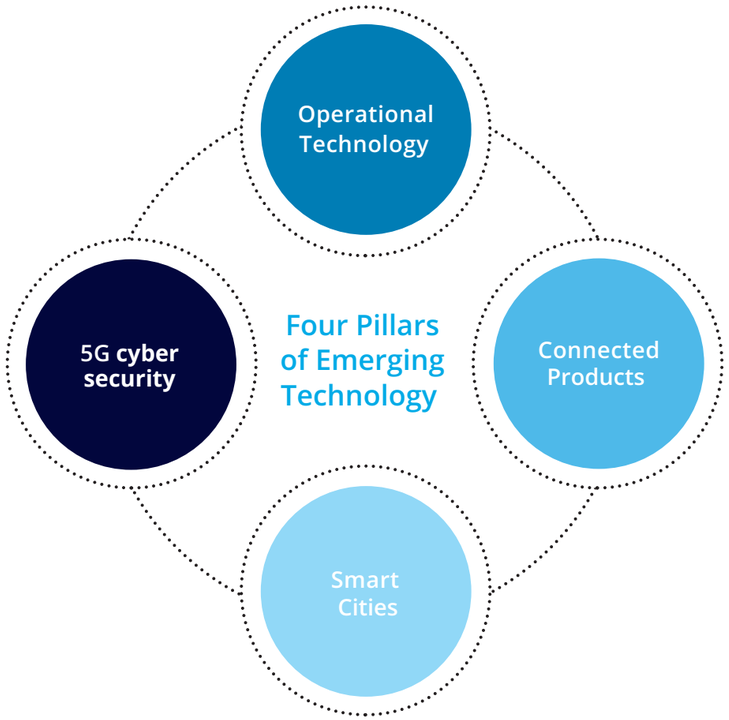
Growing connectivity

Traditionally isolated from the Internet, the Operational Technology (OT) space has recently experienced waves of ransomware attacks. The immediate impact on production has drawn attention to the vulnerabilities of connectedness, a situation exacerbated by COVID-19 as more companies have opted to remotely manage plants and equipment.

It's important to understand that all connected ecosystems, whether for medical devices, vehicles, or even entire cities, share similar risk characteristics. Medical devices may have been built for old on-premises platforms in hospitals but are now used at home via the Internet. Electric cars – expected to rapidly replace fossil fuel-powered fleets across the globe – often require connectivity for enablement. These connected vehicles need parts from a slew of geographically dispersed suppliers who may not have built security into their components. As cities connect more of their services and critical infrastructure, they are partnering with numerous third parties from cloud providers to platform owners. In every situation the attack surface grows, risks multiply and responsibility blurs.

To simplify a field that can encompass an endless array of technology, Deloitte Cyber focuses on these specific areas:

Together they cover the vast majority of scenarios we encounter in our practice.



Out of sight. But in touch.

For small all-digital organisations, a single view of cyber risk is still possible. In the short term, for larger entities with complex interconnected ecosystems that's no longer a reality. The solution is letting each party assume security responsibility and accountability for the processes under its purview. When everybody is effectively covering their part of the ecosystem making that more secure, overall risk reduces, even if there is no holistic view of it.

The speed with which entities can do that differs based on the type and complexity of technologies, but the idea is to effectively cover the basics of security and safely share information. Right now, the fix is simple. Over the long run, organisations should keep in mind there is a lot to gain in efficiency and effectiveness if processes are aligned between areas. The sooner that alignment happens, the faster higher security maturity can be reached. Both centralised and decentralised models can be effective but they should ultimately combine into an integrated single cyber risk view.

The heart of business

From a governance standpoint, emerging technology stacks can be very complex, but someone needs to own the security agenda. Having board recognition and support helps facilitate not only acquiring and managing technology but creating the right strategic partnerships. What's making this easier is that unlike traditional IT, emerging technology is closely connected to the core business.

For example, if a manufacturing business experienced a cyberattack on its OT, it's easy to see how this would quickly become a problem beyond the CISO. With production grinding to a halt, the head of operations would be immediately concerned, revenue loss would pull in the CFO, and CEO, negative publicity would afflict the CMO, and so on.

Security as an asset

The mirror image of the above scenario is that emerging technology makes the positive impact of cyber security more apparent to business leaders. If a CEO wants to sell more products building security into them makes them more appealing in our increasingly connected world. The focus shifts from security as a cost to seeing it in terms of value creation. This enables conversations about how reducing downtime leads to improved processes. Security, of course, is necessary, and although it underpins the discourse, it becomes the secondary argument.

"Despite the general belief that recent major cyber attacks are the result of increased sophistication, most of them are actually happening due to a lack of basic security controls and hygiene. It's not necessarily complicated."

— DANA SPATARU, GLOBAL CYBER EMERGING TECHNOLOGY LEADER, DELOITTE CYBER

Not one size fits all

Cyber consistently ranks in the top three enterprise risks across industries – a view shared by those on the Board and Executive Committee as well as those tasked with managing cyber risk. There is an increased understanding in all industries of how IP is vulnerable and customer trust is fragile.

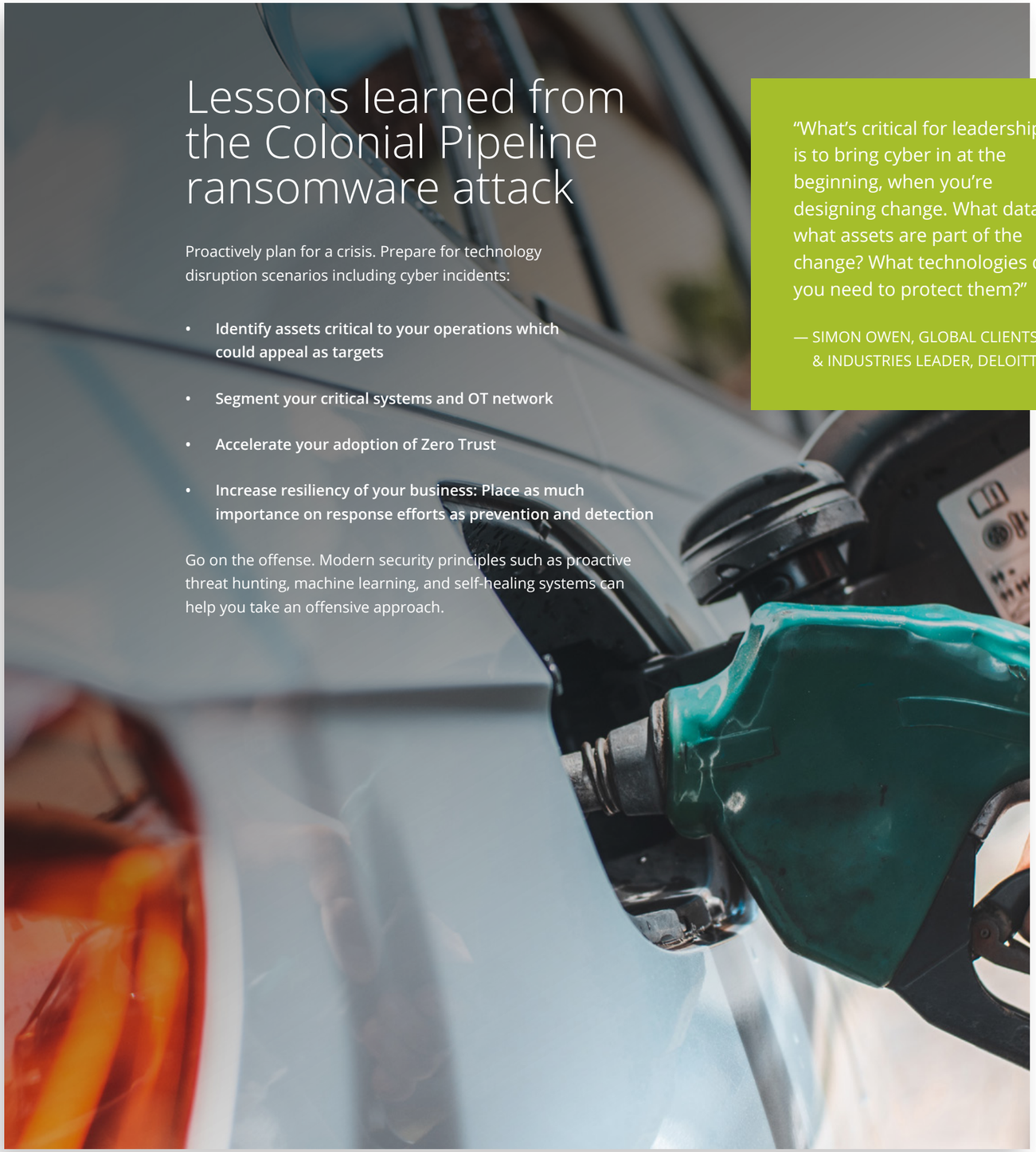
However, industries lie across a spectrum of digital transformation with varying degrees of regulatory maturity around cyber as well as a host of geographical and other considerations. While many common themes have emerged during the pandemic, such as supply chain security and remote work accelerating the need for Zero Trust, there isn't a single approach to solving the cyber challenge applicable to all industries.

Whatever direction you take, it's vital to be aware of some increasingly important areas of interest. Many governments are ramping up regulatory efforts to counter widespread cyber threats, making cutting-edge security initiatives imperative. Where regulations aren't driving change, the growing connectivity and personalisation of technology is also forcing ecosystems to be rearchitected on secure footings. Finally, the realization that all industries are vulnerable has led to broader efforts to share knowledge – being adaptable and learning what works in other industries will become increasingly relevant.

A regulatory explosion

In some industries, cyber attacks have resulted in an outsized regulatory response. In May 2021, the ransomware attack on Colonial Pipeline, the largest supplier of gasoline, diesel, and jet fuel on the US east coast, precipitated a new executive order and directives for energy companies to improve their cyber security.

Across Energy Resources and Industrials (ER&I) the urgent pressure to upgrade cyber defenses exist alongside other longer-term directives such as the move to decarbonisation. With compressed timelines – 2035 the recently revised goal in the US – the transformation of the energy landscape will require tremendous digitization to achieve its goals. This includes shifting to 5G and deploying an array of connected technologies, which bring their own increased demands for cyber security.



Lessons learned from the Colonial Pipeline ransomware attack

Proactively plan for a crisis. Prepare for technology disruption scenarios including cyber incidents:

- **Identify assets critical to your operations which could appeal as targets**
- **Segment your critical systems and OT network**
- **Accelerate your adoption of Zero Trust**
- **Increase resiliency of your business: Place as much importance on response efforts as prevention and detection**

Go on the offense. Modern security principles such as proactive threat hunting, machine learning, and self-healing systems can help you take an offensive approach.

"What's critical for leadership is to bring cyber in at the beginning, when you're designing change. What data, what assets are part of the change? What technologies do you need to protect them?"

— SIMON OWEN, GLOBAL CLIENTS & INDUSTRIES LEADER, DELOITTE

Balancing opportunity and risk

In life sciences and health care a new model of direct interaction with patients is driving the need for increased cyber security. As health care providers seek to monitor recipients' progress, and life sciences companies focus on patient-centered services to improve health outcomes, using remote devices and apps raises concerns about data protection and privacy.

This monitoring and use of apps allow for the rapid accumulation of aggregate data enabling companies to create cloud-based data lakes to gather insights that can lead to improvements in research and development (R&D), treatments and support, patient adherence, and product launches. All these technological advances have cyber security consequences. Ecosystems need to be designed and built so they protect, encrypt and anonymize data plus prevent leakage.

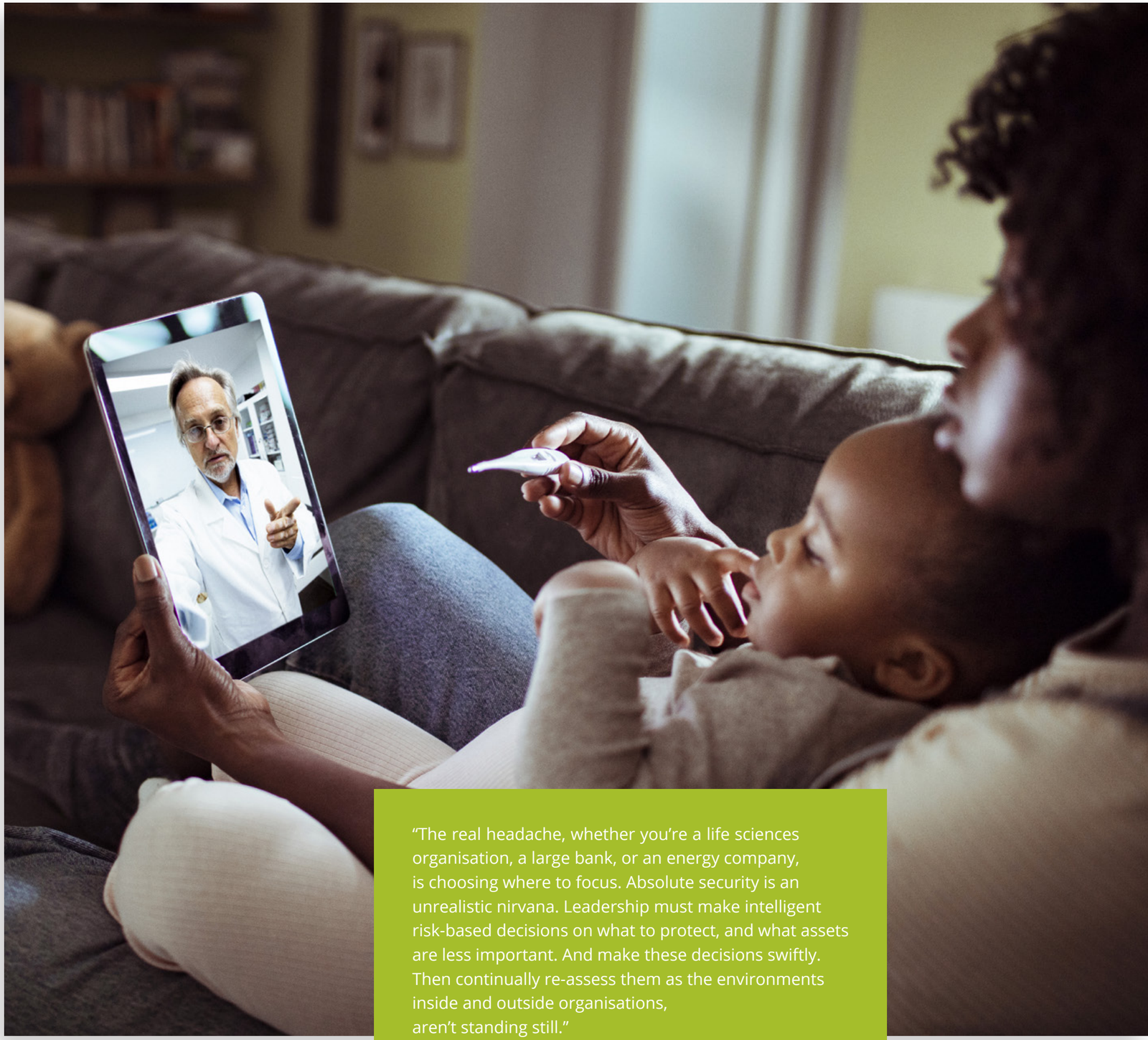
In general, global Life Sciences companies are more fearful about being hacked than they are preoccupied grappling with regulations, which are often inconsistent across territories. Establishing then maintaining trust is vital when connecting with their customers, and protecting IP is paramount for business.

Knowledge sharing

The ubiquity of cyber threats and the vulnerabilities that have been exposed during the pandemic has had an effect on the way knowledge is shared inside industries. While reputational damage remains a side-effect of attack, sharing information about incidents is regarded as valuable and helpful, often perceived as a redemptive step helping to repair brand reputations. Enterprises have realised that being secretive about cyber security doesn't confer competitive advantage but can, in fact, compromise their entire sector.

Governments have acknowledged the importance of collective defense, helping to establish public/private partnerships for information sharing such as the Information Sharing and Analytics Centers (ISACs) in the US. Less formally, CISOs are eager to learn from each other. Although it's more common for them to connect with peers inside their industry, cross-pollination from more mature industries like financial services and oil & gas to less mature ones such as life sciences and manufacturing is starting to occur. Also, CISOs themselves often migrate from one industry to another bringing their experience with them. We hope to see more connections and sharing across industry and internationally in the near future.

INDUSTRY-CENTRIC CYBER

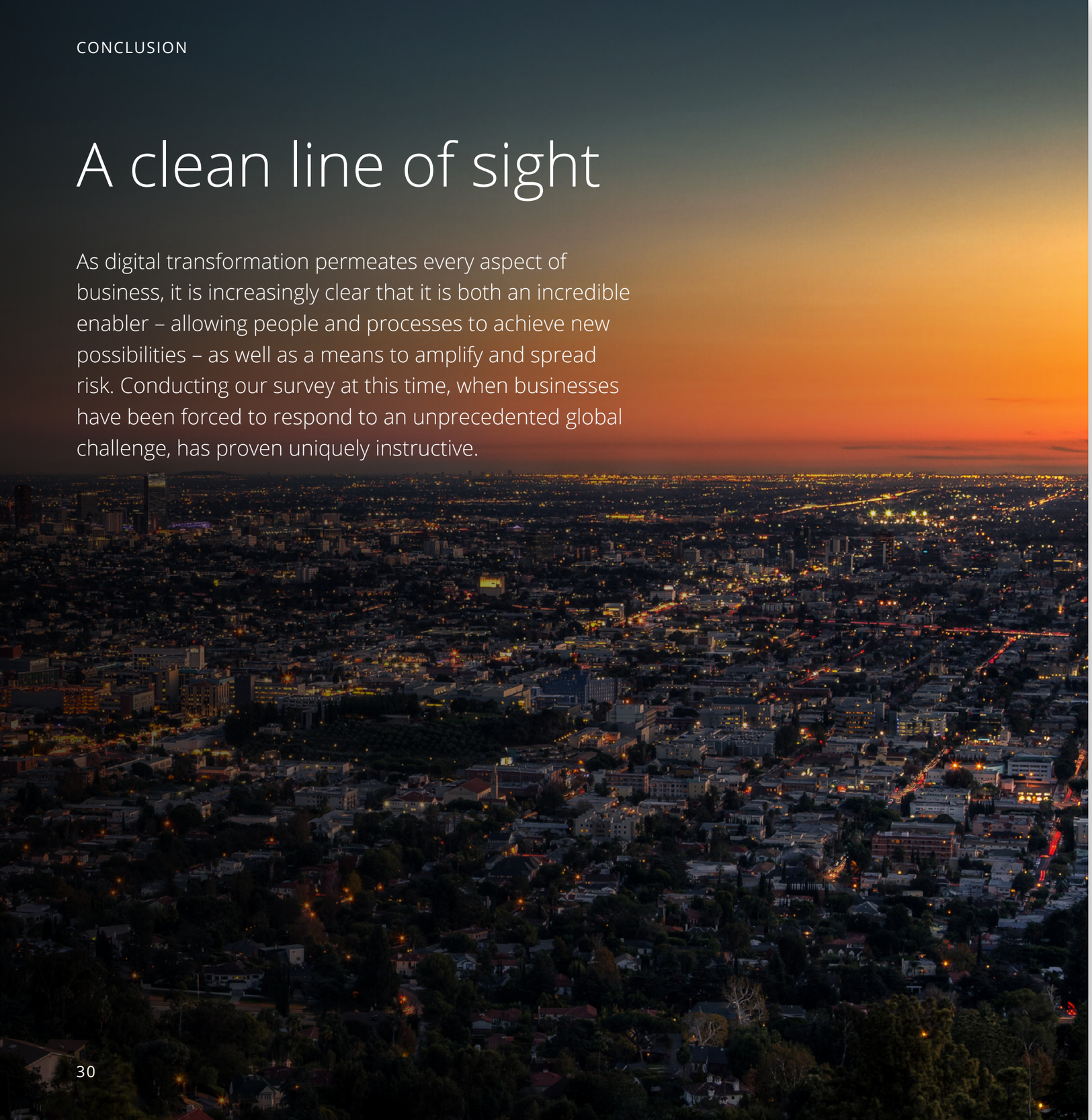


"The real headache, whether you're a life sciences organisation, a large bank, or an energy company, is choosing where to focus. Absolute security is an unrealistic nirvana. Leadership must make intelligent risk-based decisions on what to protect, and what assets are less important. And make these decisions swiftly. Then continually re-assess them as the environments inside and outside organisations, aren't standing still."

— SIMON OWEN, GLOBAL CLIENTS & INDUSTRIES LEADER, DELOITTE

A clean line of sight

As digital transformation permeates every aspect of business, it is increasingly clear that it is both an incredible enabler – allowing people and processes to achieve new possibilities – as well as a means to amplify and spread risk. Conducting our survey at this time, when businesses have been forced to respond to an unprecedented global challenge, has proven uniquely instructive.



Complexity is here to stay. Hybrid work environments are becoming a fixture, the cloud is growing in importance to almost every type of enterprise and as devices and applications evolve they are evermore connected.

There is no choice but to gain greater visibility across ecosystems lacking clearly defined perimeters. The stakes – be they operational disruption, reputational loss or deflated equity valuations – are too high. Just as complexity is the problem, the solutions are also far from simple.

Shift responsibility upwards

The clear takeaway is, organisations that do not incorporate cyber security into every aspect of their business risk leaving much of digital transformation's value on the table as well as increase their vulnerability to attack.

Our most important recommendation in this regard is to fully empower the CISO. This means directly reporting to the CEO. Just as significantly, this move must give the CISO visibility across all lines of business. It's a two-way street. The CISO must provide risk assessments in a manner that is comprehensible to the board. But not only does the CISO report up, he or she needs to be involved in new business developments from the start to ensure proper cyber governance down the line.

Reach across silos

As technology allows information to flow freely throughout organizations, humans must follow suit. It's critical to break down institutional silos and get lines of business to collaborate on cyber. Facilitate strategy, product development, compliance, IT and marketing sitting down together to understand the data assets needed and the security and privacy requirements around them at the very beginning of new initiatives. Designing with security and privacy in mind is the best way to avoid headaches later.

Implement Zero Trust

Complexity is a reality. Relying on the methods of the past to authenticate users and other entities is courting disaster, a situation easily exploited by hackers, often with dire impacts. Fortunately, the ability to continuously evaluate risk and apply real-time review to access controls is now something that can be incorporated in complex architectures.

Zero Trust is as much a cultural innovation as a technological one. Getting people to change their behaviour requires communication and training. Zero Trust enables secure execution of innovation and business strategy; it's crucial that everyone realises the ongoing benefits of its deployment in supporting evolving digital transformation.

Security is an asset

Data is the lifeblood of digital transformation. While it's vital to recognise the functionality of data–how it drives business outcomes and customer experience – it's just as important to appreciate how it creates value over the long run. Companies that are associated with exemplary data governance, thoughtful privacy policy and robust security earn the trust of customers and business partners alike. Although it's tempting to think about cyber security only as an expense, considering its impact on brand and sustaining shareholder value is central in the new world of hyperconnectivity. Implementing security is not a project, but a promise to carefully handle data, communication and business interaction end-to-end.

Sharing knowledge

While there isn't a single simple solution to managing cyber security, many of the threats facing organisations on the road of digital transformation are shared. With cyber attacks becoming more prevalent, no industry or geography is immune from them, but we can learn from each other how to effectively handle an incident when one does occur. To this end, sharing experiences and knowledge with peers is an essential element of improving the security environment all round.

Risk and reward

Whatever your cyber budget, adopting these approaches will help ensure that your resources are used more effectively.

It's tempting to focus on the complexity and plethora of risks that transformation heralds, but it's equally important to recognize the upside. When you gain the visibility you need, and you experience the agility that hybrid IT brings to your organisation, when you've earned the trust of your customers and you feel confident with complexity, you experience rewards at an entirely new scale.

CONTRIBUTORS

Authors

Emily Mossburg
Global Cyber Leader

+1 571 766 7048
emossburg@deloitte.com

Simon Owen
Global Clients & Industries Leader

+44 20 7303 5133
sxowen@deloitte.co.uk

Annika Sponselee
Global Data & Privacy Leader

+31882882463
asponselee@deloitte.nl

Dana Spataru
Global Emerging Technologies Leader

+31882888882
dspataru@deloitte.nl

Matthew Holt
Global Strategy & Transformation Leader

+393351421906
maholt@deloitte.it

Marius von Spreti
Global Zero Trust Leader

+49 89 290365999
mvonspreti@deloitte.de

Ashley Reichheld
US Customer & Marketing Leader

+1 617 449 5067
areichheld@deloitte.com

Andrew Rafla
US Zero Trust Leader

+1 201 912 6535
arafla@deloitte.com

Contacts

Shahil Kanjee
Africa Cyber Leader

+27 11 806 5353
skanjee@deloitte.co.za

Leishen Pillay
Director
Risk Advisory Africa

+27 11 209 6418
+27 76 827 0782
lpillay@deloitte.co.za

Tiaan van Schalkwyk
Senior Associate Director
Risk Advisory Africa

+27 83 475 3551
tvanschalkwyk@deloitte.co.za

Tope Aladenusi
Partner
Risk Advisory
West Africa

+ 23419041730
taladenusi@deloitte.com.ng

Melanie Harrison
Director
Risk Advisory
Namibia

+264 61 285 5003
+264 81 224 0899
melharrison@deloitte.co.za

Urvi Patel
Director
Risk Advisory
East Africa

+254719039012
ubpatel@deloitte.co.ke

Interested to learn more?
Drop us a note and we'll connect you to the right people:
Futureofcybersurvey@deloitte.com

Deloitte.