FUJITSU

Five key actions to empower secure digital transformation

Make the leap – with a built-in secure environment

shaping tomorrow with you

Cyber security as the enabler of DX

Digital transformation (DX) is paving the way for the future of business, requiring the rapid adoption of novel digital technologies. This is the key to tomorrow's success.

However every change involves risks. And cyber attacks and breaches in cyber security are among the largest risk factors. The very systems introduced to drive growth increase the risk surface. Along with the data they collect to create a more appealing customer experience. As well as a stronger interaction with partners in ecosystems. Organizations like yours need to be aware of this and make sure that the relevant cyber security measures are in place. Right from the start. It's vital that your enterprise securely enables innovation by allowing executive teams to identify and prioritize risks. And weigh these risks against business value and opportunity.

Based on our extensive experience as a leading global security and digital transformation partner, Fujitsu has highlighted five key actions that CISOs, CIOs, CROs, and other business leaders need to consider to enable and de-risk digital business strategies. By integrating these measures you'll be ready to embrace DX.

82%

of responders to a recent Ponemon study believe they've experienced at least one data breach as a result of DX, and 55% claimed this was caused by a 3rd party.

2020

has seen the world's fastest rate of digital transformation ever. Microsoft CEO Satya Nadella says there's been the equivalent of 2 years of DX in 2 months.

Align security strategies to business goals

KEY ACTION 1

First and foremost, a sustainable cyber security strategy supports the business. It aligns its actions with the enterprise goals and ensures the right balance between mitigating risk and enabling business innovation.

As such, cyber security is a prerequisite for successfully running a business. And those in charge of security must map everything onto business imperatives. While avoiding those issues that are only relevant to IT decision making.

This shift in thinking delivers benefits beyond security alone. It allows your people to work more productively, innovate faster, and implement projects more quickly at lower costs. And at the same time satisfying those customers who trust you with their personalized information. In short: it’s a must for digital business.

‹ ›

KEY ACTION 2

Find the balance between risk and reward

Today, perhaps more than ever, your organization needs to work with risk-based decision making. That means understanding the risks DX initiatives pose and whether the business benefit outweighs the cost of managing them. For example, enabling your employees to work from home or any other location involves a greater risk that their devices will be infiltrated and used to access the corporate network. Yet it's hard to ignore the finding that those organizations that established remote working and implemented measures to manage the security risks have seen less disruption compared to those who were unable to do so. Plus they've strengthened their business resilience.

In other words, a risk-based approach enables clear, fact-driven decision making based on the best outcome for your company. As such, decisions must take into account the technology, people, and processes involved in your organization.

Now that dispersed workforces and remote customers have become central to our future, the most successful organizations will adapt to protect their revenue and reputation in the long term. Just as importantly, they'll strive to create outstanding digital experiences that set them apart from the competition.

‹ ›

Run your future business with cyber security

KEY ACTION 3 1

Secure-by-design

Business risks go beyond cyber security and extend to the long-term survival of organizations. This is why we'll all have to think differently to survive in the next normal. Your enterprise will have to address the challenges and opportunities to bring about competitive advantages while neutralizing new cyber risks. Digital leaders will need to securely adapt their customer experience, everyday operations, and employee experience. If they're to deliver resilience and lead the change.

Customer experience

Customer experience is key. Consumers now expect a seamless and personalized experience. As highlighted in an article by Forbes, one third of those who ended their relationship with a company did so because the experience was not personalized enough. However, a user experience that brings advantages for your customers requires their data to be collected and analyzed.

For both the benefit of the business and the consumer it's necessary to find a balance between protecting and serving your customers. By putting the right measures in place, cyber security becomes the foundation for retaining trust with consumers. This is because it can provide an enhanced and highly personalized user experience without risking their personal data. As your users enjoy trusted access to resources and information from anywhere in the world, this secure customer journey can easily become a competitive advantage.

Everyday operations

Security for digital transformation in everyday operations is centered around automation and the Cloud. Automation helps build an unprecedented level of business resilience, allowing operations to continue with less human intervention. While Cloud resources provide a new degree of scalability that gives your organization the ability to flex up and down according to business needs. And use the best applications available in each case.

A secure-by-design approach requires that security policies are consistently integrated and managed across various platforms and systems. This approach allows you to take advantage of the latest technologies and take leaps in your DX while managing the risk of new vulnerabilities.

Employee experience

As part of a work-life balance, many organizations had already implemented adaptive working (AW) prior to the covid-19 pandemic and were thus better prepared for the situation. AW is now expected to stay as it offers safety for workers and resilience for the business. As well as access to a much wider and geographically distributed pool of talent. Yet, as more business processes are becoming digital and more staff are working from widely distributed locations, securing applications, data, and devices is becoming more of a challenge.

‹ ›

This means IT teams must respond with tools and methods to attain the same level of security that was formerly in place within the perimeter of the enterprise. Each endpoint is a priority nowadays, as each one represents a potential target and needs to be kept up to date with company security policies. Other key areas here are reliably confirming user identity when staff log in from remote locations, and shadow IT, instead of: users accessing unapproved resources for speed or convenience.

Your IT experts can deploy strong endpoint security, but many threats target unwitting users. So it's vital that your users are aware that cyber security is their responsibility, too. Your employees must understand that they form the human firewall. Then your people can work how, when, and where they want – all in a secure and productive way.

Drive productivity and convenience

KEY ACTION 4

Since they go hand-in-hand, cyber security needs to support and underpin digital transformation. Because secure data and systems are cornerstones of business success.

In turn, digital transformation needs to support new business models that appeal to customers. While making daily work easier for employees. Examples here are secure use of online resources via Cloud Access Security Brokers (CASB) services and secure single sign-on. Of equal, if not greater, concern is harmonizing security and usability for your customers. Since frustrated customers will just turn to another supplier. The competition is only a click away.

A risk-based approach that balances acceptable risks against convenience means that security teams can focus their attention on helping your organization thrive. Security needs to proceed at the same pace as all the other innovations within DX so as not to hamper progress. Furthermore, security measures that are built to enable usability are much more likely to be accepted and adopted by your users

Security teams must be equipped to predict, detect, and respond to these risks. This involves having the right security monitoring tools, collecting the right information, and providing this data to the right systems and the right people. So they can assess and react in time.

KEY ACTION 5

Build a secure culture

For DX to be a success, cyber security has to be seen as an important driver of your larger business goals. Adding competitive advantage to product value propositions, the customer experience, employee productivity, and supply chain frameworks. Digital businesses need to embed security into the very core of their systems and processes. They have to build a secure and convenient user experience. And create digital value chains that protect your customers’ data.

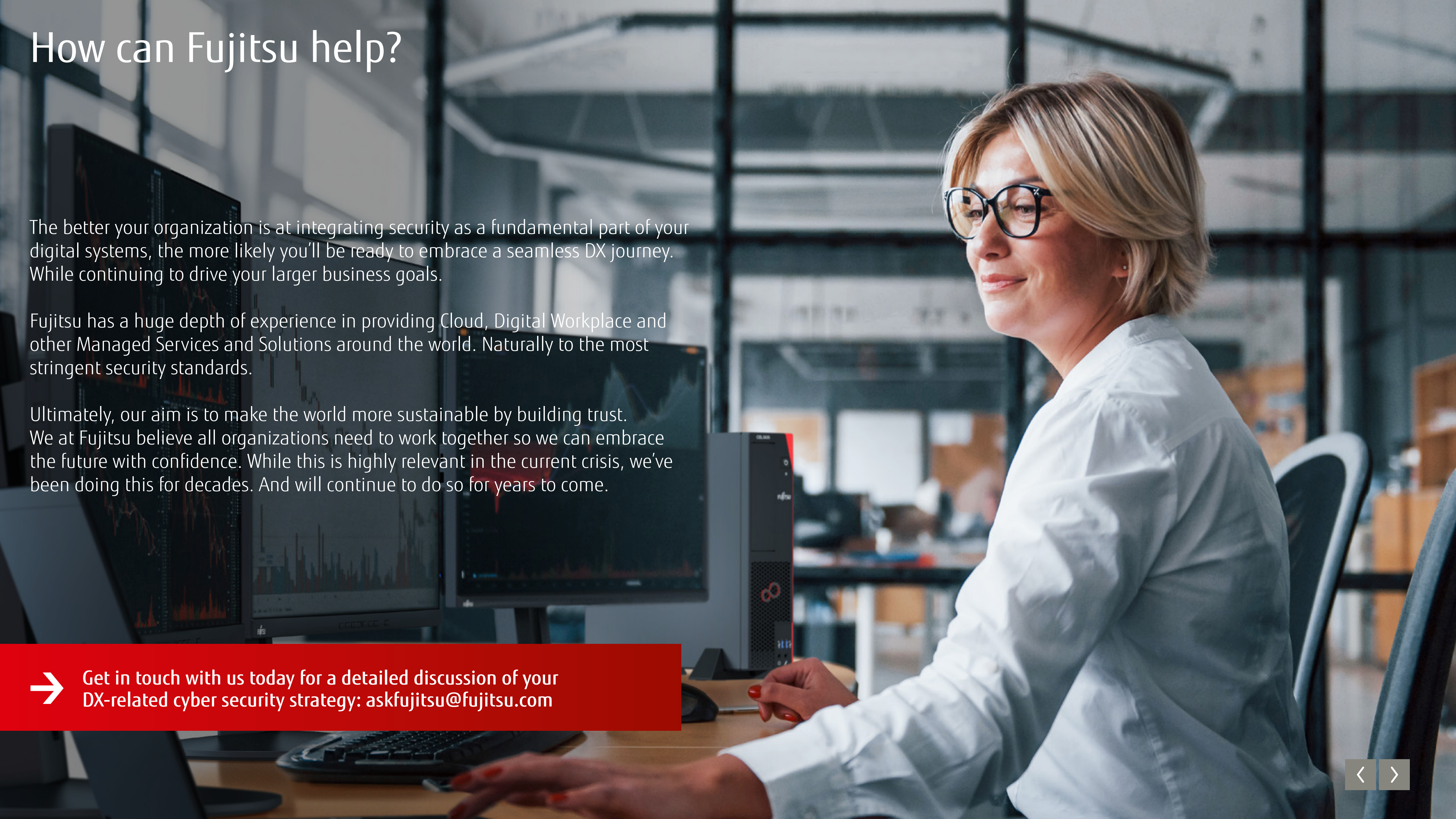
However, digital transformation is not just something that the IT department applies to your organization. It’s far more complex. True DX that delivers game-changing results means bringing together all the right ingredients. And all the right people.

The covid-19 pandemic demonstrated the importance of a secure culture within organizations. Cyber attackers relied on common moves and tactics, which turned out successful when used on many employees working from home. Leaving organizations in need of increasing efforts to train and re-train their employees in cyber security, and embed a sense of responsibility in every member of staff.

As important as reskilling and upskilling employees is collaborating with trusted partners. So your organization is better equipped to adjust to change. And this is of specific importance when it comes to the cyber security measures. You’ll need experienced experts you can trust to secure your business. To keep and unlock more of the advantages that new technology promises. And delivers.

‹ ›

How can Fujitsu help?



The better your organization is at integrating security as a fundamental part of your digital systems, the more likely you'll be ready to embrace a seamless DX journey. While continuing to drive your larger business goals.

Fujitsu has a huge depth of experience in providing Cloud, Digital Workplace and other Managed Services and Solutions around the world. Naturally to the most stringent security standards.

Ultimately, our aim is to make the world more sustainable by building trust. We at Fujitsu believe all organizations need to work together so we can embrace the future with confidence. While this is highly relevant in the current crisis, we've been doing this for decades. And will continue to do so for years to come.

→ Get in touch with us today for a detailed discussion of your DX-related cyber security strategy: askfujitsu@fujitsu.com

Let’s transform your Business in to a secure digital era.

https://www.fujitsu.com/global/themes/security

FUJITSU