rightworks

eBook

Navigate digital transformation without risking data security

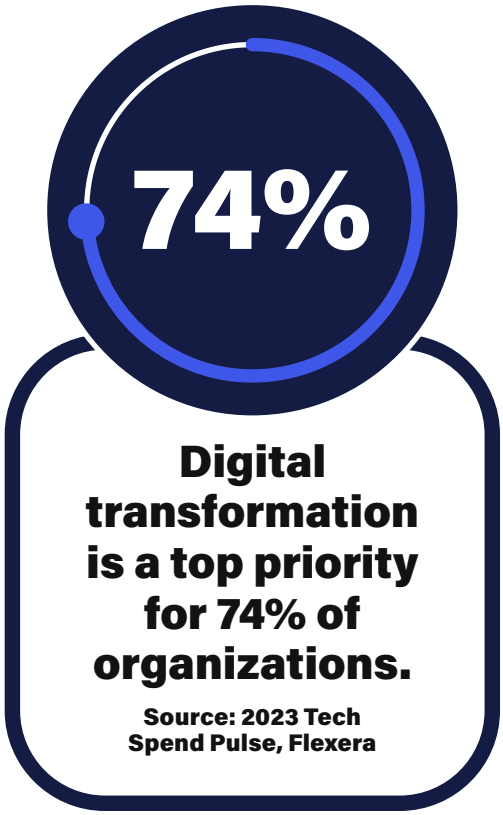
Can digital transformation and cybersecurity coexist?

The phrase “digital transformation” isn’t as hot as it was a few years ago, when just about every business and technology expert was throwing those two words around without necessarily explaining what they meant. But that doesn’t mean it’s not relevant. In fact, it’s likely to be relevant for years to come.

Accenture’s **definition of digital transformation** is as tight as any: “The process by which companies embed technologies across their businesses to drive fundamental change.” What does that mean, exactly? Basically, digital transformation involves getting rid of old processes and replacing them with new, more efficient ones by investing in and using technology. And then endlessly doing that over and over again.

An early form of digital transformation was the move from paper to email. Moving from spreadsheets to one of the QuickBooks® applications was another. Automating repetitive processes such as payroll and expense reports is yet another.

That’s the thing about digital transformation: **It never ends**. There are always new technologies and new opportunities to drive efficiency. And there’s always a new way to do things better with less work and, in many cases, ultimately for less money.



The nagging downside of digital transformation: cybersecurity

We can't talk about digital transformation without talking about the security threats. Moving everything that can be moved to a digital format doesn't happen without risk. As businesses link systems and applications together to maximize efficiency, and as they move away from manual and paper-based processes, they increase the vector for cyberattacks.

In other words, connecting systems, data and users, all of which drive efficiency, **can be dangerous**.

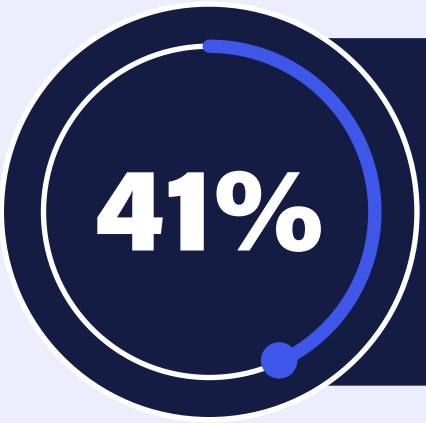
In fact, in one survey, 40% of chief security officers said their organizations were **underprepared for rapidly changing cyberthreats**. In the survey, 41% of executives who felt their organizations weren't adequately prepared for threats cited "the fast pace of digital innovation" as a reason for not being ready. A quarter cited the "convergence of digital and physical assets." Both of those choices are rooted in digital transformation. And this was a survey of executives in large organizations with huge technology budgets and lots of expertise.

Small businesses and accounting firms have far fewer resources to deal with cybersecurity as they continue their digital transformation journeys. So, is automating worth doing at all? Maybe if moving everything to an electronic format is so risky, it's better to keep the old file cabinet around or just keep doing everything via email.

The reality, however, is that moving work and files to electronic formats is necessary. Here's why:

- Creating a more efficient workplace is essential for recruiting and retaining employees at a time of low unemployment when fewer potential workers are willing to put in extended hours.
- Automation enables firms and companies to get more done by doing less work.
- It lets employees focus on doing their jobs rather than wasting time on manual grunt work. Companies that go digital will race ahead of their counterparts.

Not to mention, it's also critical for businesses that want to keep up with competitors big and small.



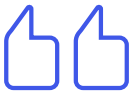
41% of executives who felt their organizations weren't adequately prepared for threats cited "the fast pace of digital innovation" as a reason for not being ready.

Source: Cybersecurity Solutions for a Riskier World, ThoughtLab

A double-edged sword?

It's not as though the old ways were more secure. Paper files have always been susceptible to old-fashioned theft, the kind that involves someone with a crowbar and a ski mask. Worse, paper burns. It molds. It's vulnerable to pretty much any element. Chances are, you're not using paper anymore, anyway. But some methods you're using to share and work in files might still be dangerous.

Take email, for instance. The email clients you've used for decades now are absolute security minefields. One study found that **92% of organizations were victims of phishing**. Artificial intelligence has enabled cyberattackers to abandon their clunky writing styles and create email content that's clean and convincing. If you're running a server in your office, you need to maintain it constantly. That means applying every patch available as soon as possible.



Phones, tablets and home laptops could be running any sort of malware at any time, and your organization could be totally unaware.

But there's more to the emerging threat landscape than just the dangers of email. As employees shift freely between working in the office and working elsewhere—or abandon the office altogether—more and more of them are using devices that don't fall under their organizations' IT policies. Phones, tablets and home laptops could be running any sort of malware at any time, and your organization could be totally unaware. In fact, about a quarter of connected devices in most organizations **are not part of the traditional IT setup**.

The digital learning curve as a security threat

Regardless of how people access your company or firm's data, going digital is supposed to make work easier. It does, but there can also be a learning curve for some employees. Workers who have worked with manual processes for years will love automation, but they'll also need to learn how to use it effectively. That period of education, though generally brief, can leave your organization vulnerable to an attack.

Most phishing attacks won't work unless someone clicks on a malicious email. Human error, carelessness or genuine ignorance is still the starting point for most successful cyberattacks. When your employees are learning new processes and using new applications, they might be more likely to commit a disastrous click. A single click can start a rapid chain of events that can end in disaster for your business.

Of course, you do have some backup. Cybersecurity insurance can help protect your business from the worst ravages of a cyberattack. Unfortunately, cybersecurity insurance premiums are costly and **getting more expensive all the time**. Plus, you might **not be able to get an insurance policy** if your business doesn't meet what the insurer considers minimum cybersecurity standards.

The truth is that managing cybersecurity is prohibitively difficult if you're trying to do it in-house. Constant application and server management, device protection, email protection and employee training are just too much for almost any small business or firm to take on. When large organizations are struggling with cybersecurity while going digital, it's a sign that smaller businesses will need lots of help.

Even better news about cloud services and cybersecurity

All of that is great, but the same issue remains: How are you going to protect critical data in a new digital environment? As it happens, the same cloud service can do that, too. And it's all part of the same monthly plan. It's a package that brings digital transformation and cybersecurity together.

1. The right cloud service protects your data in enterprise-level storage facilities, with support experts at your disposal whenever you need them.
2. The service backs up your data and minimizes the impact of cyberattacks before they can do any damage.
3. The cloud service can also help you use Microsoft 365 applications safely and easily.

But there's more to it than that. Managed email protection in the cloud goes far above and beyond what you get from a standard email provider, meaning you can minimize your risk of falling victim to an email-based attack.

In addition, the right service also keeps your devices safe—even those that employees use at home or elsewhere. Device protection frees your staff to work from anywhere at any time and on virtually any device.

A cloud-based provider can also do more for your employees. This partner can train your employees to avoid cyberthreats, boosting your best line of defense against a cyberattack.

With a trusted service provider managing your applications and security in the cloud, you can move forward into digital transformation with confidence—and keep the journey going. Your provider maintains and updates your applications and protection for you while you focus on running your firm or business. And it's all a simple line item in your monthly budget.

Rightworks offers the total package of a secure digital environment

With Rightworks, businesses can enjoy complete managed cloud services, including:

Rightworks OneSpace

Maintain peace of mind in a reliable, flexible and secure cloud environment that's customized for accounting firms and small businesses, along with advanced data analytics.

Rightworks Total Security

Experience enterprise-grade protection for applications and devices as well as security training for employees.

Rightworks WISP

Get expert help to create a Written Information Security Plan (WISP)—The IRS recommends businesses have a plan in place to protect personally identifiable information (PII). Our cybersecurity experts will assess your technology, recommend ways to address vulnerabilities and help you create a plan to protect your business in case of a cyberattack.

Productivity applications

Improve workflows and give your team the tools they need, including secure email and managed Microsoft 365 applications.

Rightworks is the catalyst that can set your operation on the path to greater efficiency while boosting cybersecurity. Far from having to be at odds, digital transformation and security can live peacefully together in one place—without any effort on your part.

Get started today!

Contact us today at **888.210.0237**
rightworks.com/contact-us

rightworks
rightworks.com