wickr
an AWS Company

# A Guide to Taking on a More Proactive Approach with Data Security

A recent report from Forrester Consulting, commissioned by IBM, makes the case that data privacy is the new strategic priority for many businesses. Data privacy is undoubtedly a priority for consumers who are tired of having their personal data used by big companies. These consumers are worried about their privacy and want to take more control over their data. In fact, 70% of Americans feel that their personal information is less secure than it was five years ago, which worries them.

Should data privacy be a strategic priority for your business? The short answer: absolutely.

## Data Privacy Should Be a Strategic Priority

Data privacy is important to consumers, and it should be equally important to businesses. Making data privacy a priority is not only essential from a legal and regulatory standpoint; it's also good business. Your customers want their data to remain private and secure, and you win their trust – and their future business – by treating their data with the respect it deserves.

It's a perfect storm of regulations meeting customer demand. You have to meet the data protection guidelines, of course, but that alone isn't enough to assuage your customers. You need to go above and beyond the regulations in a way that earns your customers' trust and respect. If your data privacy policies are merely reactive to what's legally required, your customers will abandon you for competitors that take their privacy more seriously. To remain competitive and best serve your customers, data privacy has to become a strategic priority.

If you do it right – if you commit to keeping your customers' information private and secure – you will realize a wealth of benefits. You can't afford to play catch up with data privacy. You have to get ahead of the game and give customers what they want. That means total transparency about how you collect and use customer data, ensuring a high level of privacy for that data, and providing customers with control over their data.

## Complying with Data Privacy Regulations

Your business needs to comply with all relevant data privacy laws and regulations. These laws differ from country to country and from industry to industry, but complying with these regulations is literally the bare minimum you can do regarding data privacy.

Only ensuring compliance isn't enough, however. Data privacy regulations typically lag behind real-world developments; malicious actors are constantly developing new ways to breach company data and use that data for their own purposes. Not only is complying with regulations a priority, so is staying abreast of new developments in the world of cybersecurity. You need to ensure – and assure your customers – that the data you collect is used legally and is secure from cyber attacks.

## Meeting Customer Expectations

Customers today are more aware of data privacy than they have been in the past — 84% of consumers say they care about the privacy of their own data and the data of others in society. They also want more control over how companies use their personal data.

Knowing this, meeting customer expectations about data privacy needs to be a strategic priority. If your company isn't transparent about collecting and using customer data, you will lose customers. If your data privacy policy is not as pro-consumer as your customers expect, you will lose customers. If you don't give customers some control over how you use their data, you will lose them.

## Prioritizing Data Privacy Has Multiple Benefits

Making data privacy a strategic priority takes time and money. What will you gain from those efforts?

First, by complying with all appropriate data privacy regulations, you gain the peace of mind that you won't be fined or otherwise penalized for being noncompliant. Data privacy laws are important, and you have to prioritize them.

Second, you gain the trust of your customer base – and customer trust is invaluable. If customers know you treat their data seriously, they will trust you in other aspects of business, as well.

Third, over time, you should gain more customers and increase your sales. Showing that you care about your customers will pay off in the long term.

## Why You Need to Be More Proactive to Secure Your Data

When it comes to cybersecurity, you can take a reactive or a proactive approach. With a reactive approach, you wait until your organization experiences a data breach or cyber attack, then you take steps to deal with it. With a proactive approach, you enact security measures in advance to try to prevent breaches and attacks.

Not surprisingly, the proactive approach is more effective and less costly than simply reacting when bad things happen. When all you do is react, you have a significantly greater risk of being attacked – and suffering the financial and structural damages of an attack. The global cost of cyber attacks is expected to hit $6 trillion this year.

When you proactively prepare for potential cyber attacks, you reduce your risk. A proactive approach sets up defenses to protect against attackers and allows you to be ready with a plan for what to do if you are attacked. You won't be caught by surprise.

Bottom line, it's much more difficult – and more costly – to recover from a data breach or cyber attack than it is to plan to prevent one. In the world of cybersecurity, an ounce of prevention is demonstrably more effective than a pound of cure.

## 5 Ways to Be Proactive with Data Security

There are many things you can do to be more proactive with your organization's data security. Here are five of them.

### 1. Inventory All of Your Assets

Before you can enact stronger data security, you need to know what you need to secure. That means conducting a thorough inventory of all of your data assets. Detail what data is stored where and who has access to it. You should also inventory your physical IT assets – servers, routers, computers, and mobile devices, both on-premise and remote. Only when you know what you have can you determine how to best protect it.

### 2. Assess Your Security Measures

You also need to know what cybersecurity measures you currently have in place. Assess all of your current security tools and processes and how they're protecting your digital assets.

You should then conduct a cybersecurity risk assessment. This inspects your system and data to determine how secure it is against various types of threats. You can do this either internally or hire a third-party to conduct the audit. It's important to understand both your strengths and weaknesses, so you know where you need to improve your cybersecurity efforts.

### 3. Train Your Employees

The strongest data security plan can fall apart when just one employee clicks a malicious link. Phishing is a growing security risk, accounting for 1 in every 4,200 emails. It's essential that you train your employees – all of them, at every level – on the latest data security procedures. You want to instill in your entire workforce an understanding and respect for data security. Place a special emphasis on securing personal devices, working securely from remote locations, and guarding against phishing and other social engineering schemes.

### 4. Think Like the Enemy

When it comes to protecting your valuable data, it's important to know who might want to steal it and why. When you can get inside the heads of potential malicious actors, you gain a better understanding of how that data may be targeted and what techniques might be used.

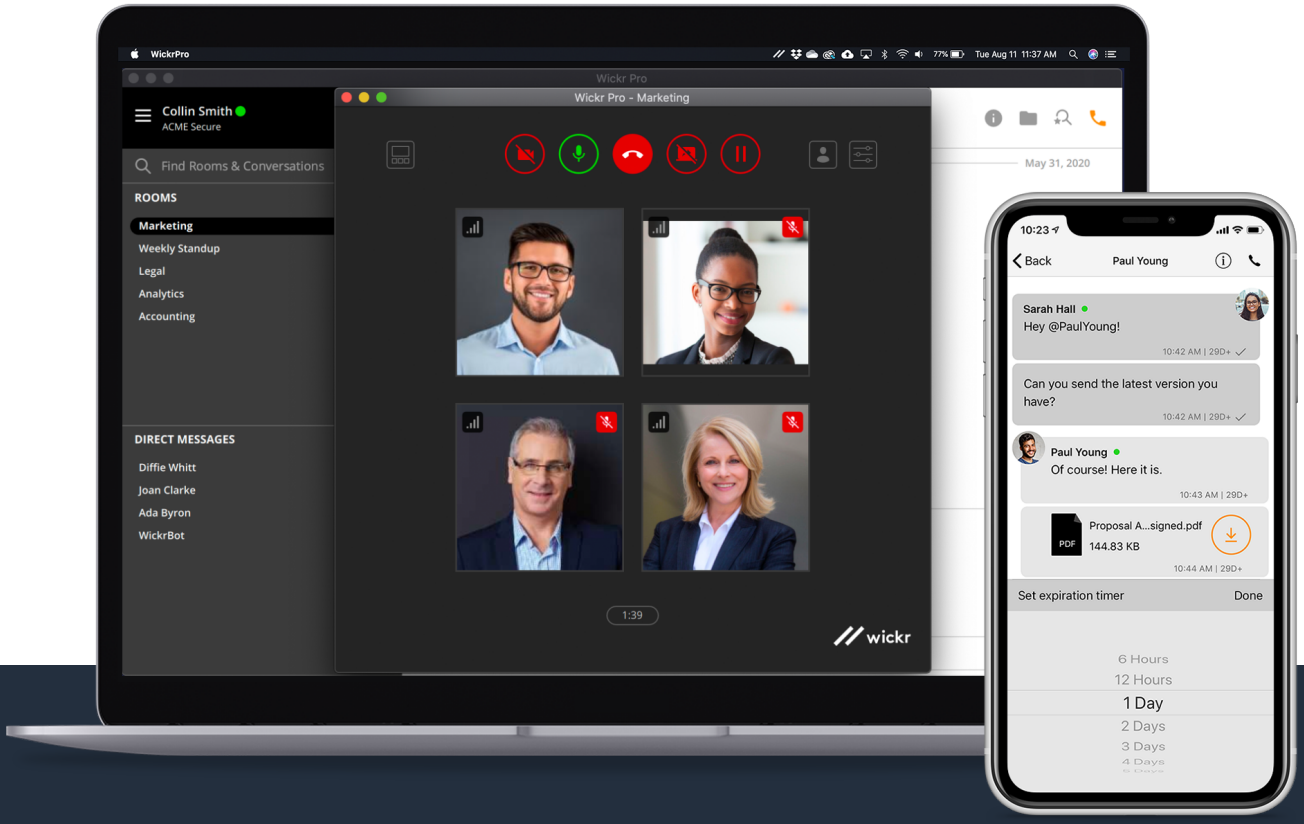
### 5. Use Encryption

Raw data can easily be viewed by any malicious actor who breaches your defenses. If you encrypt that data, however, even the most determined hackers can't view any data they access. To thwart cybercriminals, you must encrypt both your stored data and your ongoing communications. Even better, employ end-to-end encryption so that messages can't be viewed while in transit.

wickr
an AWS Company

## Let Wickr Secure Your Organization's Communications

When you're looking for a secure communications platform, Wickr is the smart choice. Wickr provides secure messaging, audio and video conferencing, file sharing, and collaboration tools, all protected by end-to-end encryption. Wickr is ideal for all types and sizes of organizations, including large enterprises. Contact us to discover how Wickr can help you embrace a more proactive approach to secure data with the industry's leading secure communications platform.




## Wickr – For End-to-End Data Encryption

Wickr is the most robust and secure encrypted messaging solution available today and should be part of your organization's data encryption best practices. Wickr is fully encrypted, enterprise-ready, and easy to set up and manage. Wickr's end-to-end encrypted platform enables you to secure text messaging, voice and video calls, and file transfers.

**Learn More About Wickr ▸**