Alex Pearce

Data security law:

Managing the legal risks of cloud and collaboration tools

As anyone with a Dropbox or Google Drive account knows, consumer-grade cloud storage and collaboration services are a convenient way to store and share personal photos, music, video and documents. Employees who use these cloud services outside the workplace naturally want their convenience and ease of use inside the workplace. So they often turn to familiar consumer-grade offerings. In a recent study by cybersecurity company Stroz Friedberg, more than half of information workers surveyed uploaded corporate documents and data to their personal cloud storage accounts.

This phenomenon is frequently referred to as BYOC — Bring Your Own Cloud. As with the more familiar Bring Your Own Device — BYOD — phenomenon, employee adoption of BYOC can offer certain benefits to a company, including greater productivity and increased employee satisfaction. They also eliminate purchasing or supporting equivalent corporate solutions.

But those benefits can come with serious drawbacks. This article will discuss the dangers presented by BYOC and suggest steps that companies can take to manage and mitigate their exposure.

BYOC: RISK IN THE FORECAST

Theft or loss of intellectual property

One of the most common — and dangerous — risks of a laissez-faire approach to BYOC is theft of trade secrets and other proprietary data. It often arises when employees leave and use corporate documents they've stored in BYOC accounts for the benefit of a new employer.

Indeed, numerous recent trade secret theft cases indicate that BYOC accounts are becoming the preferred means for departing employees to steal sensitive corporate documents. These cases typically involve sensitive materials such as customer lists, pricing and financial data, and proprietary technical specifications. In some, the employee's resort to BYOC was unknown and unauthorized. But in others, the company condoned the use of BYOC accounts without considering the consequences of when the employee departed.

Data breach and regulatory violations

Another significant BYOC risk is the violation of federal, state or international privacy and data security laws. These laws vary significantly in their scope and requirements, but all obligate companies to take certain steps to protect personal information from unauthorized use or disclosure.

Many require that companies take steps to ensure that third parties who receive this information are bound to protect it. Almost all impose some duty to notify individuals or regulators in the event the information is lost in a security breach or sent to parties who are not authorized to receive it.

Employees who transmit corporate data to personal cloud accounts can unwittingly violate these laws. And they may expose the data to security breaches that can result in substantial response costs, monetary fines and reputational damage for the company.

Litigation risk and electronic discovery exposure

Unsupervised use of BYOC accounts also can create substantial risks if the company becomes involved in litigation. One risk is failing to preserve and collect discoverable evidence. Electronic discovery can be challenging and expensive even when the evidence resides wholly within a corporate information-technology environment. When that evidence migrates to employee-controlled BYOC accounts, the cost and degree of difficulty can increase substantially.

Even so, courts may still hold companies responsible if relevant data in an employee's BYOC account isn't properly preserved and collected. In one recent case, a Florida court faulted a company for its employee's destruction of files stored in his personal Box.com account when the company had reason to know about those files but didn't instruct him to preserve or produce them.

The storage and sharing of sensitive information in BYOC accounts also can compromise a company's ability to assert the attorney-client privilege. A Virginia court recently found that an employee's use of an unsecured Box.com link to share a file with the company's outside attorney waived any claim of attorney-client privilege to that file. The court reasoned that the employee's actions were the cyber equivalent of leaving the file "on a bench in the public square and telling its counsel where they could find it."

WEATHERING THE BYOC STORM

Companies have several options to reduce these risks. Used alone or in

combination, they can help a company take back control of its information.

Prohibit

One option is to require employees to use only company-managed equipment and systems to store and share corporate documents and data, thus prohibiting BYOC entirely.

Companies can adopt and implement policies that clearly prohibit the transmission or storage of company data using personal cloud services. Such policies also should be supported by technical controls designed to prevent the transmission of corporate data to BYOC accounts. These can include blocking employee access to known file sharing or collaboration sites and implementing "data loss prevention" tools that track or block uploads from corporate computer systems to non-approved sites.

The main problem with this approach is that it can alienate employees and cause them to look for ways to subvert the prohibition. And in a world of rapid technological change, it's likely they'll find one. In one recent case, a company blocked access to well-known cloud storage services such as Dropbox. The company later discovered that a departed employee had used a new and relatively unknown cloud service — Jottacloud — that her employer had not blocked. She used it as a workaround to steal sensitive data for her new employer.

Companies who use this approach must therefore devote enough resources to keep those policies and technical controls current and monitor and enforce employee compliance.

Permit and regulate

A second approach is for the organization to accept BYOC as a fact of life and implement a program to manage the risks without sacrificing all the benefits.

Companies inclined to take this approach should consider the following steps, at a minimum:

- Create a list of approved consumer cloud offerings that are acceptable for business use based on a review of the providers' terms of use, privacy policies and security practices.
- Restrict the use of BYOC accounts to non-sensitive or less-sensitive documents while still prohibiting their use to store and transmit sensitive data whose compromise would pose a risk to the company.
- Require registration and approval for use of a BYOC account, based on the conditions that the employee acknowledges the company's IT security and data protection policies and agrees to allow the company to access the account upon request.
- Update the company's termination procedures to incorporate a review of employees' BYOC accounts and the removal of corporate data from those accounts before their departure.

The downside of this approach is that it requires significant IT and compliance resources but still leaves the company vulnerable to the risks presented by employees' failure — innocent or otherwise — to comply with the program.

Provide a corporate-managed alternative

The safest option for dealing with BYOC is to provide employees with an alternative enterprise-grade cloud storage and collaboration solution, thereby avoiding the need to resort to BYOC in the first place. Key benefits of enterprise-grade solutions typically include:

- The opportunity to ensure the offering meets the organization's information security and privacy standards.
- Centralized management of account creation and deactivation to ensure that only authorized individuals can access corporate data.
- Data governance and auditing capabilities that allow the organization to understand and manage the locations in which its data is stored.
- Streamlined electronic discovery capabilities to facilitate legal holds and the collection of relevant data in the event of litigation.

This option provides employees the flexibility and ease of use they expect without a corresponding loss of control over corporate data. But it does have drawbacks. One is the significant cost associated with procuring a corporate solution and managing it. There also is the risk that the solution a company selects today will not be the one preferred by employees — or the company — in the future.

For companies that operate in regulated industries or that handle especially sensitive data this may be the only realistic option.

CONCLUSION

Whatever BYOC direction a company decides, it's critical to document the choice in a well-drafted policy that clearly communicates the company's expectations. The company should then train employees on that policy and remind them regularly of the risks of unapproved personal cloud use.

But simply telling employees what not to do isn't enough. To be successful, any BYOC strategy must present workable alternatives that employees actually can use to get their jobs done. Otherwise, personal clouds will continue to darken the prospects for securing corporate data.

ALEX PEARCE is of counsel at Ellis & Winters LLP's Raleigh office. His work centers on privacy and data-security law. He provides strategic and practical guidance on matters that implicate domestic and international privacy and data-security considerations. His experience includes counseling on state and federal privacy, consumer protection and breach notification laws; designing and implementing global data protection compliance; negotiating cloud computing, data license and data sharing agreements; and representing clients in privacy and data security issues.