Business Risks of Using Personal Email Accounts in the Workplace

"When is it OK to use a personal email for business purposes?"

*The short answer is **never**, but individuals will often revert to "personal" email accounts for business-specific communication. For employees, the inherent risks along with the general availability of mobile email should be enough to preclude using a personal email account for business purposes. If for example that user is out-of-the-office, they should be able to access their office mail from a smartphone or computer, and this is a far better route than simply resorting to their personal email account.*

Personal email accounts exist outside of the IT department's control. They are not subject to backup, archiving, security or governance so using them for business purposes, is a clear violation of compliance regulations.

And since personal emails are not stored on company servers, discovery and FOIA requests are seriously compromised presenting legal risks to your organization – let alone the cost involved if lawyers are able to gain access to these accounts for eDiscovery.

What are the legal risks of using a personal account for business?

Allowing employees to use personal email accounts to conduct business means that your company's business information is being stored on mail servers outside of your control, anywhere in the world. You have no way of knowing all the places where your company data is stored, or where it's been transmitted.

And a personal email account is not covered by your company's security policies. Your employee may have agreed to Gmail's Terms and Conditions (which allow for email content searches), but your company didn't. You may have a good data privacy policy in place—but personal email accounts can bypass it with one click of the "Send" button.

Understanding the risks and implications of using personal accounts for business is not always apparent until there are Freedom of Information requests, internal investigations, or eDiscovery. In all of these cases, those personal accounts may contain relevant information and as such have to be offered-up for search and retrieval.

Even the act of discovery is difficult - Personal emails are not discoverable in standard legal discovery procedures. Google for example prohibits external scanning of users' emails (several cases are currently under way), meaning the company will have to instruct the user to scan his or her email themselves and runs a big risk of spoliation sanctions. If the issue is regulatory, the company is likely to be found out-of-compliance.

June 2024

If an employee is using personal email accounts to send business related email using a company device, it doesn't necessarily mean the organization has the right to search those emails. It could be very difficult to convince a requester or a court that all relevant information was discovered and produced - even if heroic (and expensive) measures were undertaken such as copying the individual's entire mailbox to a company server for search and retrieval. And few users would agree to a complete copy of their personal email being held on their company's servers.

There is also a corporate risk to be considered

There are a number of other ways in which using personal accounts for business purposes generates corporate risk. Allowing employees to use personal email for work poses serious risks of IP theft, losing company privacy or violating customer privacy, and disrupting network operations due to exploits which can be implemented on computers not secured by your internal policies.

Using personal email compromises company secrets and potentially exposes company correspondence to uncontrolled mining and searching. Virtually all personal accounts can be subject to legal (and in some cases questionable) collection and searching by various security agencies.

According to current FISA law, the NSA has the right to record data from BOTH endpoints in an email conversation, if ONE of those endpoints cooperates with NSA procedures. Since the big personal email providers like Google, Microsoft, AOL, and Yahoo! have all cooperated with the NSA, allowing them to scan and store any emails they like on NSA's servers, this means anyone who receives an email from their accounts is put at risk for surveillance – even though they didn't agree to the provider's Terms and Conditions at all. So if your employee uses personal email to send project blueprints to a customer's work email, that customer has unwittingly lost their privacy to the NSA!

The lack of security behind these collections (think WikiLeaks) has compromised entire governments, and businesses should expect no real protection for themselves or their customers!

Continuity can be a big issue - what if this employee leaves the company? Those emails leave with that individual - along with any relevant information, making future searches more challenging.

It's not just email that is the problem. Employees might use a personal email address to set up any number of functions critical to your company's day to day operations, for example web hosting accounts or purchasing domains. The employee's personal email address then becomes the owner of the account so if that employee leaves, you may have a difficult time taking ownership of the assets they set up on the company's behalf. What effect could this have on your ability to do business?

What about credibility? Does allowing employees to send email from *theirname@gmail.com* present a professional image problem for your organization?

The solution might be obvious but companies still need to reinforce it

First and foremost, setting strict policies against the use of personal email for business is the only course of action but despite all the reasons why company business should only be done through company email, users will still take the path of least resistance and use whatever email is most straightforward for them. The burden falls to the organization, then, to make sure that the "path of least resistance" is the right path.

Organizations can be proactive and ensure that remote or field employees can easily access company email systems using their own devices. Webmail interfaces are easy to set-up, and any compliance capture will see and preserve those mails even when sent from a home pc, laptop, smartphone or tablet. When composing a new email, particularly on mobiles, employees need to be reminded to always choose the company email address, not their personal one. For non-employees such as contractors and consultants, the issue is the same. If the contractor or consultant is doing business on behalf of the company, then it's a smart step to provide a company email address for them and enforce strict guidelines on using this is part of the arrangement.

IT departments should always be able to retain central control and visibility of all emails being sent or received on the company's behalf to avoid the problems that result from business being conducted from personal email accounts, but it does require some simple policies and an IT organization that is both proactive and persistent. The problem might not go away entirely, but it will be a nominal problem, not a big one.

June 2024