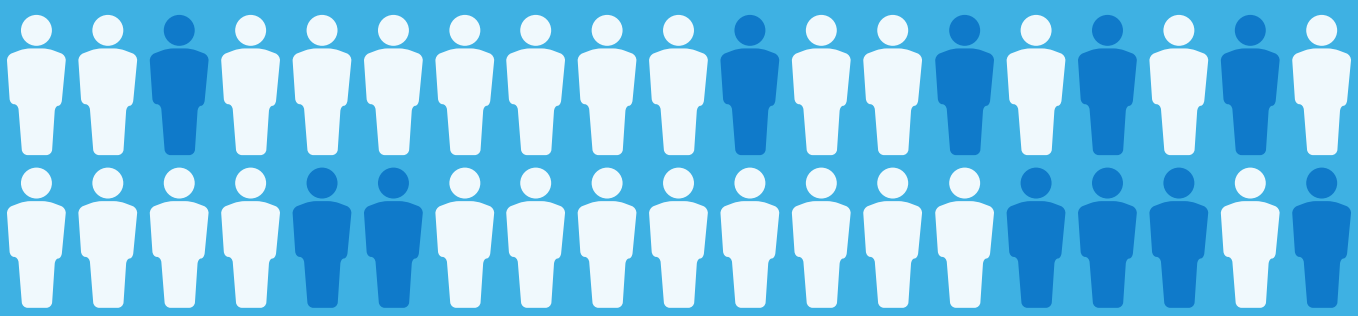
THE EX-EMPLOYEE MENACE

Intermedia's 2014 SMB Rogue Access Study

TABLE OF CONTENTS



What can happen when an employee leaves?	4
The Ex-Employee Menace	6
Is there such thing as too many cloud apps?	8
Interview with Felix Yanko, President of ServNET Technologies	12
Three methods for preventing rogue access	16
Interview with Michael Osterman, President of Osterman Research	20
6 Reasons Why Dropbox Isn't Secure Enough for Business	26
Interview with Eric Aguado, COO and Partner at ThrottleNet Inc	30
4 Reasons You Need a Single Sign-On Portal	36
Interview with Chris Sousa, Vice President of Enterprise Design at Dataprise, Inc.	40
Intermedia can help	44

WHAT CAN HAPPEN WHEN AN EMPLOYEE LEAVES?

Recently, we came across an interesting story on Richmond.com. A disgruntled ex-employee of a Richmond, VA wine shop hacked into the company email system and sent out an email to the store's entire mailing list to complain about being fired. And this was AFTER the store changed everyone's passwords.

Somehow, this ex-employee was still able to get into the company email system and wreak havoc. And while it may seem like minor damage, it still required the company to spend the rest of the day doing damage control with their customer base.

Imagine what could have happened if this ex-employee had wanted to be more malicious. What if she had access to the store's bank accounts? Or if they had erased client records or sales data? How much could this small business have lost because of one angry ex-employee?

This is a prime example of the kind of threat posed by ex-employees who retain "rogue" access to company systems after they leave. And it's not just the potential for malicious behavior. It can be as simple as not knowing where your company data is being stored in case you need to access it.

If you've got employees using personal file sync and share services to store company data, you've got rogue access. If they leave, your data leaves with them—even if they didn't take it intentionally. How will losing that data impact your business?

Intermedia's 2014 SMB Rogue Access Study takes a deep look at the rogue access issue and the potential harm that can come when current and former employees walk away with your data. In this eBook, we give you our detailed report, including key things you can do to solve the issue. We also include several interviews with Intermedia partners offering their experiences and advice.

The rogue access threat is real for many businesses, but it is solvable. Read on to find out how.

THE EX-EMPLOYEE MENACE

Ex-employees walk away with their passwords...

89%

retained access

to Salesforce, PayPal, email, SharePoint, Facebook and other sensitive corporate apps.

On August 12, 2014, the Bureau of Labor Statistics released its latest Job Openings and Labor Turnover Survey. It found that 973,000 people in the Professional and Business Services industry left their jobs in June, 2014.

The critical question is: what kind of IT access did those 973,000 people take with them? Can they still copy leads from Salesforce? Can they log in to corporate Twitter accounts? Do they retain passwords for Quickbooks or Paypal? Are confidential files stored in their personal Dropbox accounts?

Intermedia and Osterman Research teamed to up to quantify the scope of the "Rogue Access" problem. What we learned should be a wake-up call for every business in the country.

EX-EMPLOYEES ARE WALKING AWAY WITH THEIR PASSWORDS

89% of the survey respondents retained access (that is, a valid login and password) to at least one application from a former employer. They named nearly every major app you can think of: Basecamp, Shopify, Desk.com, Office 365, Google Apps, MailChimp, Wordpress, and many more.

45%

retained access to "confidential" or "highly confidential" data

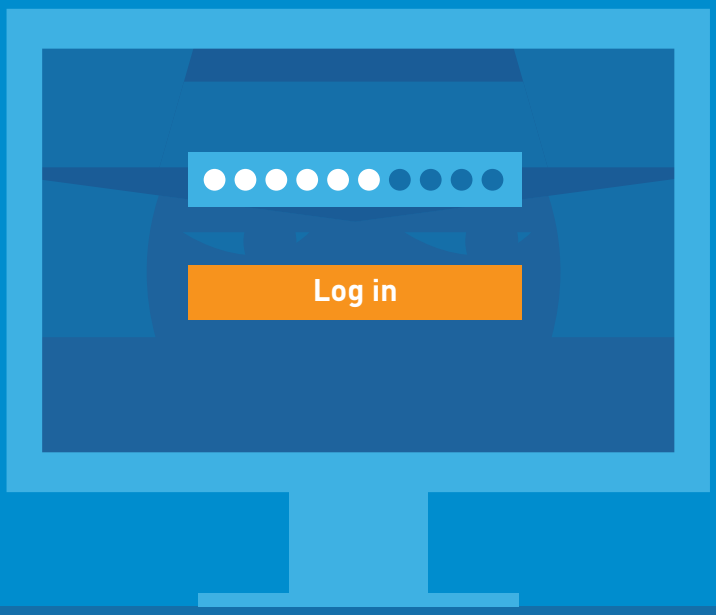
49%

logged into an account **AFTER** leaving the company

MAYBE YOUR EXIT INTERVIEW IS MISSING SOMETHING?

It's not surprising that cloud apps are falling through the cracks during the employee offboarding process. In many companies, the responsibility for provisioning apps falls to different departments: email is provisioned by IT, payroll apps are provisioned by HR, and line-of-business apps are provisioned by department managers.

With this approach, there is no clear responsibility for decommissioning and deprovisioning. The result: rampant rogue access.



60%

of respondents were NOT askedfor their cloud logins whenthey left their companies

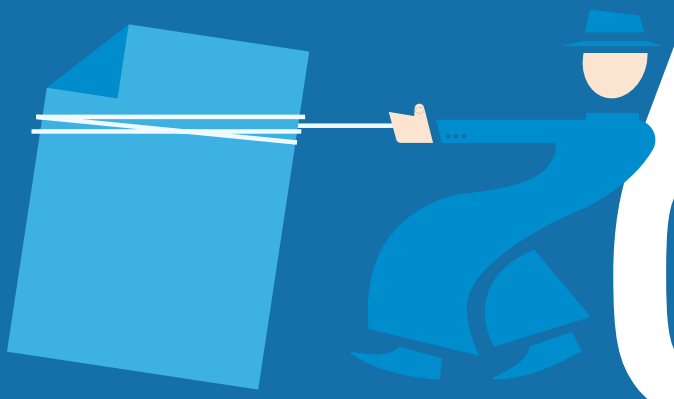
EX-EMPLOYEES ARE ALSO WALKING AWAY WITH YOUR FILES

If you've heard of the Bring Your Own Device trend, then you may have heard of its sequel: Bring Your Own Service/App. As part of this trend, employees are creating project plans in Google Docs, or using SurveyMonkey instead of the corporate Qualtrics account, or spinning up AWS servers because there's too much red tape inside the corporate datacenter.

This makes users more productive. And it also introduces huge security holes. Because if IT doesn't know the where the company's data is, how can it control what ex-employees can access?

Personal file sync and share services are probably the worst offenders. What's the likelihood that IT will be able to access, secure or wipe corporate files stored in a personal Dropbox or Google Docs account?

Ex-employees are also walking away with your files



68%

stored work files in personal cloud storage

88%

retain access to the file sharing services they used at their old job

WHAT KIND OF RISKS DOES THIS "ROGUE ACCESS" CREATE?

- **Stolen secrets.** An ex-employee could bring account and billing data to your competitors. Or they could use your product plans to beat you to market.
- **Lost data.** One day, an ex-employee casually purges her personal cloud storage accounts—and suddenly you've lost the only copy of all their work.
- **Regulatory compliance failures.** How can you comply with regulatory obligations to protect sensitive data if ex-employees can still enter your systems and delete or modify data? Fines and legal costs can be substantial.
- **Data breaches.** Forty-six US states require you to notify parties whose data has been breached. Does "rogue access" constitute a breach?
- **eDiscovery risks.** Can you satisfy an eDiscovery order if you don't have full and ready access to all of your discoverable data—such as data stored on ex-employees' personal accounts?
- **Self-offboarding gone wrong.** A well-intentioned employee could spend their last day deleting files or cancelling cloud accounts—and unwittingly destroy the value of all the work he or she did for you.
- **Out-and-out sabotage.** Imagine what just one disgruntled ex-employee could do with access to your social media accounts, or the price settings on your ecommerce site, or the leads in your CRM...
- **Hacker field days.** What if the bad guys nab an ex-employee's device—with all the passwords to your systems stored in plain text?

INTERVIEW WITH FELIX YANKO, PRESIDENT OF SERVNET TECHNOLOGIES

Pittsburgh-based ServNet Technologies was founded in 2008 by Jim Gatto and Felix Yanko. ServNet helps SMBs leverage the cloud to access enterprise-quality technologies at affordable prices and secure their systems. We spoke to Mr. Yanko recently to get a first-hand view of the security risks that come with employees using personal cloud apps for work and taking access and data with them when they leave.

89 PERCENT OF EX-EMPLOYEES RETAINED ACCESS TO CORPORATE APPS. ARE YOU SURPRISED BY THESE NUMBERS?

I would think that would be even higher for small business owners. We're as security centric as you can get, and I think even for a few days after an employee leaves, they'll have access to certain things that will take us time to turn-off.

HOW BIG OF AN ISSUE IS THIS FOR ORGANIZATIONS? SHOULD BUSINESSES BE CONCERNED? PARTICULARLY SMBS?

It's never a big issue—until something happens. Most people will say, "Oh you know, most people are leaving on good terms." Well, that's USUALLY the case.

"I think the potential for damage and liability is way more than any business can risk. I think if you were to ask an attorney, they'd say that companies need to have a process, policy and software in place to prevent access by ex-employees from happening."

HAVE YOU FOUND THIS TO BE A CONCERN AMONG YOUR CUSTOMERS?

Yes. There are quite a few stories I've heard. Whether its access to certain files, or exporting certain things after they leave to take home, or accessing systems to get customer lists, etc. Not many actually do bad stuff that damages the employer directly. But even just taking information that can be used by competitors is probably not something you want to leave open.

WHAT HORROR STORIES HAVE YOU ENCOUNTERED WITH CUSTOMERS AROUND ROGUE ACCESS?

I've definitely heard a lot of stories around salespeople who export their customer lists. Or tech people that have FTP access and download company files and make copies.

Definitely, I've seen employees that delete data, and that's the concern: they go in and delete and wipe all the data that is on their drive. There was a time when somebody went into our system afterward and changed some things, but we couldn't prove it and couldn't see who it was.

We had a situation with a client where an employee was let go, and the company leadership claimed that the employee hacked back into the company's system, but I think the real story was that the company information wasn't properly secured. No company wants to admit that it's happened to them.

WHAT'S THE RISK THAT THIS CREATES FOR SMBS?

For a small business, if something happens and they get sued and their clients are affected, they usually go out of business. If something bad happens they usually don't survive it. They don't really think about risk, it's more along the lines of "if that happens I probably won't make it." Which is why they should have some protection in place.

WHAT ADVICE WOULD YOU PROVIDE YOUR CUSTOMERS FOR PREVENTING ROGUE ACCESS?

I think the right technology and strict policies are the way to go. Making sure that non-disclosure agreements specify what employees are supposed to have access to, what's theirs, what isn't theirs. A lot of people when they leave will look up those options just to see if they can do stuff that they shouldn't be able to do. On top of that, having technology and policies in place to prevent these risks. Change passwords when people leave. Make sure you know all the accounts that they created and all the things that they've worked on.

IS THERE ANYTHING ELSE THAT YOU HELP DO WITH CUSTOMERS SO THAT THEY CAN MITIGATE THIS RISK?

Well, if we're selling a client SecuriSync, then we'll blacklist Dropbox, so that if users try to install Dropbox on the computer it will automatically not work. Same goes for Box as well. We'll actually just block applications that shouldn't be there.

AS YOU LOOK AT BYOD, WHAT ADVICE DO YOU HAVE FOR CUSTOMERS MANAGING THE PROLIFERATION OF BYOD?

If a user wants to access corporate wi-fi with their mobile device, we need to put a security app or Webroot on it. That way, the device is owned by the employee, but the security is managed by the company. Webroot allows us to monitor which apps are installed, so we can shut apps off, and push Wi-Fi and VPN settings. An end-to-end solution is what we would advise for anybody that's trying to access the company network.

WITH 60% OF EMPLOYEES NOT ASKED FOR CORPORATE LOGINS WHEN THEY LEFT THEIR COMPANY, WHY DO YOU THINK THAT SO FEW SMBS ADDRESS THIS PROBLEM? IS IT JUST A LACK OF AWARENESS, A LACK OF RESOURCES?

I think for many business owners, they've never been burned. It's like people that leave their car unlocked in their driveway. It doesn't take much to press the button to lock it, but some people think they're safe. Of course, that's until they get robbed, and then they're going to have a security system and protect their car. For most it's just too late by the time that all happens.

That's why having a backup is one of the things we're most focused on. For 60% or 70% of businesses, if their system fails and they don't have a backup, they lose their emails or CRM or whatever data they have on the customer. They won't recover from that. They go out of business within 12 months. If a HIPAA violation happens at a medical office, then they're going to go out of business.

IS THERE ANYTHING ELSE THAT YOU'VE SEEN AS YOU THINK ABOUT ROGUE ACCESS AND WHAT THIS REALLY MEANS FROM A SECURITY PERSPECTIVE FOR SMB'S?

There are a lot of compliance aspects for accounting, HIPAA, etc. A regulated businesses need to protect sensitive customer information that is sensitive. And if there is a potential for exposure or for allowing an unauthorized person to have access to that information, those companies are breaking the law. And they might not even realize that.

THREE METHODS FOR PREVENTING ROGUE ACCESS

IMPLEMENT RIGOROUS ACCESS MANAGEMENT AND IT OFFBOARDING PROCESSES.

To successfully manage user access during employment—and revoke it when they leave—your business needs to build processes around the best practices for user lifecycle management. This includes managing employee access to IT services, maintaining awareness of access privileges, and instituting a rigorous IT offboarding checklist for departing employees.

Good news: we've done the research for you. At the bottom of our web report (intermedia.net/RogueAccess), you'll find guidelines for setting up internal processes as well as specific actions to take when onboarding and offboarding employees. In addition, you'll find recommendations specific to regulated industries such as financial services, legal services and healthcare.

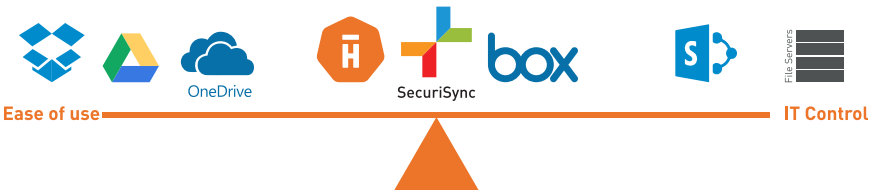
DEPLOY A CLOUD STORAGE SERVICE THAT'S MORE ATTRACTIVE THAN PERSONAL SERVICES.

Users want to access and share their files across multiple devices and collaborators. Personal services like Dropbox or Google Docs make that absolutely simple. If your corporate tools require even marginally more effort—even if it's just logging in to the VPN—then people will naturally gravitate to the simpler solution.

That's why you must provide a file sync and share service that's as user-friendly as consumer tools but also gives IT full control over access privileges. (We, of course, recommend Intermedia's SecuriSync.)

There are many obvious reasons you need IT control over shared files. But there are also some not-so-obvious ones. "If an employee stores sensitive or confidential data in personal Dropbox or Google Drive accounts, then this data is potentially accessible by outsiders the day he or she becomes an 'ex-employee'," says Michael Osterman, president of Osterman Research. "In many cases, this runs afoul of data breach notification laws. This also complicates eDiscovery audits that require you to place legal holds on corporate data."

And there's one more risk: many well-intentioned employees spend their final day at a company clearing out their computers. What happens if, weeks later, you realize you're missing some critical files? If they were stored on corporate cloud storage, then they're simple to recover. If they were on a personal Dropbox, it's much more challenging.



UTILIZE A SINGLE SIGN-ON PORTAL TO MANAGE AND CONTROL ACCESS.

A single sign-on (SSO) portal gives employees access to all their apps with just one password. For users, it makes cloud IT as simple to use as the good-old "Start" menu: once you're logged in, you click on any app—such as Salesforce, Quickbooks, webmail or thousands of others—and it launches immediately. There's no need to type in any further passwords.

For users, SSO portals are popular because they eliminate the need to hunt for logins and passwords. This makes them more productive in the face of a sprawling cloud footprint. (In Intermedia's previous report, Death by 1,000 Cloud Apps, we talked a lot more about the challenges posed when there are too many apps.)

For admins, SSO portals have a deeper benefit: they reduce the potential for Rogue Access. Here's how single sign-on makes leaks less likely:

- Users can be de-provisioned in a single click. This makes it harder for a departing employee to retain access or cause mischief.
- Users are less likely to remember their passwords. A Single Sign-On portal requires users type passwords only when configuring an app or when the app requires a password reset. Compared to non-SSO users—who type in their passwords multiple times a day—an SSO user is less likely to depart the company with all of his or her logins and passwords memorized.
- IT admins can see what apps an employee has been using. Many security holes are introduced when employees use apps without IT's knowledge. With an SSO portal, IT can review the logins saved by a departing employee to spot any unknown services and flag them for deprovisioning.
- The safest password? No password at all. Some SSO services let admins provision apps without users ever knowing their password. This is an especially powerful tool for preventing Rogue Access, because it means that users are effectively stripped of their access as soon as their SSO portal is suspended. (This functionality is currently available with Intermedia AppID Enterprise.)

INTERVIEW WITH MICHAEL OSTERMAN, PRESIDENT OF OSTERMAN RESEARCH

Michael Osterman, a leading analyst of communication and collaboration technology within SMBs, conducted the research that is central to "The Ex-Employee Menace" report. In this interview from August 2014, we asked him about the security risks faced by SMBs when employees leave a company, as well as his recommendations for mitigating rogue access and protecting company data.

HOW BIG OF AN ISSUE IS ROGUE ACCESS FOR ORGANIZATIONS?

It's a fairly serious one, and one that fairly under the radar. You don't see a lot about this in the trade press. It's the kind of thing that people may understand intellectually, but really haven't done much about, because this hasn't been enough of a priority for them. I think this research is going to help to shake some things up and hopefully make people more aware of the kinds of issues they face by not managing these applications well enough.

WHAT ARE THE RAMIFICATIONS FOR ROGUE ACCESS, PARTICULARLY AS WE LOOK AT IT FOR SMALL AND MEDIUM-SIZED BUSINESSES?

Also, if you ever have to go through e-discovery or some sort of a regulatory audit, it's much more difficult to do. Because now you've got all of this data in a variety of repositories that other people in other companies also have access to. And it means that you potentially could have spoliation of data—that an employee could delete your information.

"If you have sensitive data that you're not managing appropriately, that is now accessible by someone in another company, that means, in many cases, you have violated the data breach notification requirements that require you to protect consumer financial data, protected health information, etc., from unauthorized parties. And certainly, an ex-employee would be an "unauthorized party".

SO, WITH 89% OF EX-EMPLOYEES STILL RETAINING ACCESS TO CORPORATE DATA, WHY AREN'T SMBS DOING MORE TO ADDRESS THIS ISSUE?

Most SMBs don't really have an IT department or a full-time IT person. And so, an employee will take it upon themselves to sort of implement file sharing technology for the good of the company and for their own productivity. But these organizations really won't have official policies or best practices in place.

The problem is that over time, things get out of control. Nothing is being managed in a coordinated way and certainly not managed according to any sort of corporate policy.

WHEN YOU LOOK AT THE 60% OF EMPLOYERS THAT DIDN'T ASK FOR CORPORATE LOGINS WHEN AN EMPLOYEE LEAVES, IS THIS ALSO JUST THE LACK OF AWARENESS? OR LACK OF RESOURCES? WHAT DO YOU THINK IS ACCOUNTING FOR THAT?

Certainly, it's a lack of corporate policy that says, "The IT Department is going to be in charge of managing all of the access to the corporate accounts." In many cases, you really don't have one central authority that manages all of the access. IT gives users a few things, the user's department gives them access to others, HR might give out access, etc.

The larger the company, the more potentially distributed that deployment might be. So, when an employee leaves, there's not one person who will go and ask for all of the access to all of the different systems an employee has. It might be that the IT Department cuts off access to email or FTP, but they know nothing about the CRM access from Sales, or the Dropbox access that the individual has implemented for themselves.

"Regardless, companies need to implement policies about where corporate data is stored and how corporate data is accessed. Before you implement any technology or choose any providers, those policies need to be in place. If an employee wants access to cloud storage or they need a CRM system, then it should all funnel through one function, so you have more centralized management of that access."

HOW CAN SMBS ENSURE SECURITY WHEN THEY MAYBE DON'T HAVE THE BUDGET OR THE RESOURCE ALLOCATION OF A LARGER ENTERPRISE ORGANIZATION?

It's easier if you have a central authority. But, you might have a cloud provider for email, a different cloud provider for CRM, a different cloud provider for cloud storage and so forth. To the extent that you can bring all of that under one provider, it's going to be easier to manage that process.

HOW MUCH IS TOO MUCH WHEN IT COMES TO SETTING IT POLICIES ACROSS YOUR ORGANIZATION?

We actively recommend against establishing draconian policies that say, "You cannot use this or that." It's important to allow employees to have some freedom so that they have the capabilities that they need to do their job.

It's not that people are enamored with Dropbox or Google Drive, per se. They're enamored with the ability to have access to all of their files on any platform. So, you need to provide a really good substitute that is just as easy to use, but giving the organization more security controls.

So, really, the key is to offer good alternatives with the same ease-of-use that employees can find on their own, but that puts IT back in charge.

HOW CAN SMBS REALLY BEST TACKLE AND MANAGE THIS PROLIFERATION OF BYOS?

First and foremost, find out what users are using. We would recommend a survey to find out what employees are using, where they're storing corporate data, and so forth.

Then, offer a better alternative. And provide the appropriate training so that you're bringing all of your users under one umbrella. That really is critical, because I think that if you can satisfy users and satisfy IT at the same time, you've now killed two birds with one stone.

WHAT SHOULD SMBS BE LOOKING FOR IN A FILE SYNC AND SHARE SOLUTION THAT CAN COMBAT THE USE OF PERSONAL SHARING ACCOUNTS?

Allow employees the freedom to store files in the cloud, but give IT the freedom to access that content and manage it according to corporate policies.

HOW CAN SMBS USE A SINGLE SIGN-ON SOLUTION TO BETTER MANAGE ROGUE ACCESS?

Single sign-on is critical for any sized organizations, SMBs included. With single sign-on, the cloud is easier for employees, because now they have a single, very strong password that they can remember to access all of the different functions that they're going to need: CRM, email, file sync and share, whatever it might be. And you've also got the benefit of employees not even needing to know what the individual passwords are for each of those different apps.

And when an employee leaves the company, IT can simply change that one password or turn off that access. With a single action, you've eliminated access to all the different capabilities that a user has.

WHAT SHOULD SMBS DO DURING THE OFF-BOARDING PROCESS TO HELP ENSURE DATA AND ACCOUNTS DON'T FALL THROUGH THE CRACKS?

Ask employees for all of the account login information that they have for all of the different accounts they're using. And maybe, if it's legal in a particular jurisdiction, to ask the employee to sign a statement that they have turned over all company data, that they've turned over all of their login credentials, and that they promise not to access content after they leave.

LOOKING AT PREVENTATIVE MEASURES SMBS CAN TAKE, IS THERE ANYTHING THAT THEY CAN DO DURING THE ON-BOARDING PROCESS THAT WOULD HELP PREVENT ROGUE ACCESS?

The organization should establish policies and then implement the appropriate technologies to enable users to have all of the functionality they need. SMBs should probably choose a really solid file sync and share solution that IT manages. And do the same for CRM, cloud storage, all of the functions that they think employees might require.

It doesn't mean that employees won't do it. It doesn't mean that if you give them a really good file sync and share solution that they also won't implement Google Drive on their own. But now if you have a corporate policy against it and you've provided a good alternative, you have a much lower likelihood of that occurring.

"Regardless, companies need to implement policies about where corporate data is stored and how corporate data is accessed. Before you implement any technology or choose any providers, those policies need to be in place. If an employee wants access to cloud storage or they need a CRM system, then it should all funnel through one function, so you have more centralized management of that access."

6 REASONS WHY DROPBOX ISN'T SECURE ENOUGH FOR BUSINESS

When it comes to sharing photos and storing family recipes, Dropbox is wonderful. That's why it's so popular with consumers. But Dropbox wasn't made for the business world, and that lack of business-grade features can put your company data at risk.

Because people are so used to using it at home, millions of users have brought Dropbox into their work environment. According to Osterman Research, Dropbox has found its way into 70% of companies.

And this is a problem. Because, when it comes to business, Dropbox's consumer roots show through. It's not right for business. In fact, Dropbox ended up on Bloomberg BusinessWeek's list of top banned apps because there are many file management use-cases for which Dropbox will actually leave you vulnerable.

HERE ARE 6 REASONS WHY DROPBOX MAY NOT BE SUITABLE FOR YOUR OFFICE:

1.
IT has no control or visibility.
With Dropbox, IT administrators can't control which users are syncing files. Nor can they control who has access to shared files. Dropbox does not allow companies to view an audit log, so if sensitive data is leaked, admins have no way of knowing who may have accessed it. What's more, Dropbox doesn't provide remote wipe—so if an employee's laptop is stolen, IT can't remotely remove Dropbox data like they can remove Exchange data.

2.
Users can't set granular permissions.
Business users collaborate on files differently than individuals. Business collaboration requires granular control over permissions to ensure appropriate access levels for dozens of collaborators and stakeholders. This protects against accidental overwrites or deletions, but it also preserves security and secrecy. In this regard, Dropbox falls short: it doesn't let you customize read and write privileges for individual users.

3.
Data encryption is limited.
If you're storing financial reports, strategy documents or competitive analyses, you want them protected. But Dropbox has limited encryption and security features that can leave customers' data exposed. Your data is sitting on the same public cloud next to content from millions of other users, without adequate isolation.

4.
You can't set different sharing permissions for sub-folders.
Sometimes a subfolder will contain data that shouldn't be shared with everyone who can access the enclosing folder. But Dropbox doesn't let you specify permissions for sub-folders. To protect your data, you're forced to redo your entire folder structure. A business tool should adapt to your business processes, not force you to change them.

5.
You can't share password-protected web links.
Dropbox is great for sharing photos and videos between friends, but what if you want to share files over the web with a secure password? Or what if you want to add a password to a file you've already shared? When you send a business file with Dropbox, you lose control over who can access the file.

6. You can't lock files for collaborative editing.
There's nothing worse than losing productivity while you try to sort out version conflicts. If you're working on a file that's shared with multiple people, you want to be able to lock it so nobody else can overwrite it. Dropbox doesn't support locking files for editing—and this lack of protection risks the resiliency of your data.

Employees love Dropbox so much because it's so simple to use. Which means an out-and-out ban on Dropbox probably won't be effective in your organization. In fact, IT is often unaware when employees start using Dropbox, so a ban may just drive users underground and increase the risks that much more.

THERE'S A BETTER SOLUTION OUT THERE—SECURISYNC FROM INTERMEDIA

To get the behavior you want out of your users, you need to provide file sync and share tools that enable the exact same functionality—but without the business risk. When it comes to getting employees to drop their Dropbox, the user experience is key.

SecuriSync makes file syncing and sharing simple and safe with business-grade protection, as well as Microsoft Office and Outlook integration. SecuriSync provides key security features including:

- At-rest and intransit encryption
- Remote wipe for lost or stolen devices
- Leverages Active Directory user settings, permissions and passwords
- Locking features prevent overwrites, conflicts or deletions
- Permissions can be edited, updated and revoked at any time
- Control content shared externally

SecuriSync is part of Intermedia's Office in the Cloud. And like all Intermedia services, SecuriSync comes with onboarding assistance from our Cloud Concierge as well as 24x7 support.

INTERVIEW WITH ERIC AGUADO, COO AND PARTNER AT THROTTLENET INC.

Since 1999, ThrottleNet Inc. has been providing SMBs in the greater St. Louis and Boston areas with the same superior business technology solutions usually reserved for big corporations, with the goal of helping their customers overcome technology barriers and increase productivity. Mr. Aguado kindly provided us with his take on the rogue access issue and the real threat it poses to securing company data.

WHAT KIND OF HORROR STORIES HAVE YOU ENCOUNTERED WITH CUSTOMERS AROUND ROGUE ACCESS?

We actually had one of our own happened here internally. Shortly after one of our engineers was terminated, that person found employment at another competitor here in town. And that individual actually used remote access software to gain access to our telephony server.

From there, they proceeded to listen in on phone calls, record phone calls and even redirect extensions. They'd retrieve voice mails as well as other sensitive information. We were lucky in that they were unable to gain access beyond this one server, at least that's what we were able to determine. To be honest, we will likely never know the full extent of the breach.

HOW WERE YOU IMPACTED BY THAT?

I think at first there was no immediate apparent impact. However, once we discovered the depth of the intrusion, we had to spend a lot of time and resources towards investigation. We needed to know the extent of the intrusion and damages in terms of data theft or anything else.

We also had to spend quite a bit of additional time working with the ex-employee's new company. I think that because the evidence was so strong, this company cooperated with us in getting to the bottom of everything. Thankfully, as a result we were able to avoid any kind of litigation. In the end, the whole situation could have turned out much worse, but still ended up being a huge waste of company resources.

WE FOUND THAT 60 PERCENT OF EMPLOYEES WERE NOT ASKED FOR THEIR CORPORATE LOGINS WHEN THEY LEFT THEIR COMPANIES. WHY DO YOU THINK SO FEW COMPANIES ADDRESS THIS ISSUE?

I think it generally comes down to ignorance and as a result, no one within that organization takes on the responsibility. In many small and medium sized organizations, there's simply no process or protocol for when you have an IT person leave.

For many of these organizations, we find that there's a single person handling the IT support. When that individual leaves, a number of questions come up. Who's responsible for making sure the system credentials are secured, not just for the Windows domain and server, but for all the systems including both hardware and software? How do they even know what all credentials they need to retrieve and how do they verify the information is correct? Do they take the departing IT guy's word for it? Where is this information stored?

WHAT ADVICE DO YOU PROVIDE YOUR CUSTOMERS FOR MANAGING THE PROLIFERATION OF BYOD?

If the company doesn't already have an acceptable use policy governing overall network usage, they absolutely should have one. In that policy, the company should have a section specifically addressing mobile devices.

WHAT ADVICE DO YOU PROVIDE YOUR CUSTOMERS LOOKING TO PREVENT ROGUE ACCESS?

First and foremost, hire a competent managed service provider (MSP) that can handle your IT needs. Look for a provider with a long track record in the business.

How many employees do they have? How many of those employees are help desk technicians versus seasoned network engineers? Is the company a Microsoft partner? Can they provide you with testimonials of similar sized companies in the same industry? Do they outsource any of their support?

Ask to see resumes and certifications. We find that a lot of organizations, when hiring, are thorough when it comes to reviewing a non-IT candidate's resume and certifications. But, when it comes to hiring the "IT guy" or hiring a MSP, they take shortcuts. This again stems from ignorance when it comes to IT in general and simply not understanding what to look for.

For those organizations looking to outsource their IT needs to an MSP, ask to visit and tour the MSP's office of operations. If it turns out to be an individual working out of his basement, obviously that's a red flag. In a time when IT is more important to your business than ever before, you want a solid, reputable company.

A good MSP will regularly take the time to review your network security, infrastructure as well any other critical aspects of your organization that pertain to IT (i.e. Line of business applications). At ThrottleNet, we also install solid business-grade firewalls, monitoring agent and probe software on all of the key and critical network infrastructure as well as all endpoints (laptops, desktops, etc.). The monitoring solution actually alerts our team using predetermined thresholds. So if there's an attempted breach in the firewall, the system creates a log entry, which is then creates an alert. The entire solution is based on the ideology of being proactive versus reactive.

We also leverage Windows Domain Group Policy using Microsoft Best Practices. This helps us enforce login credentials with complexity, minimum number of characters, variation and failed attempts thresholds. These are really basic fundamentals of security that all companies need, but are often overlooked.

We audit and restrict administrative login access as well as perform routine security maintenance. In some instances such as the medical practice industry (HIPAA), security is paramount. A good MSP should have the resources to help you achieve the level of security required to achieve compliance.

"For actually managing mobile devices, I would definitely recommend a mobile device management solution. This will give you much more control over all mobile devices on your network regardless of whether they are employee-owned (BYOD) or company-issuedA mobile device management solution will regulate what type of company data will be accessible on these devices thereby dramatically reducing risk and increasing security."

IS THERE ANYTHING YOU'D ADVISE CUSTOMERS TO DO, EITHER DURING THE ON-BOARDING OR THE OFF-BOARDING PROCESS TO HELP MITIGATE ANY POTENTIAL RISKS OF ROGUE ACCESS?

On the other hand, if you're talking about an internal IT guy leaving the organization, it's going to be a bit of a different process. Because of the critical access the typical "IT guy" has at any given organization, a great deal of thought needs to be considered when designating someone responsible for handling a transition. Regardless, someone needs to be delegated this duty.

I'd recommend that person sit down and "interview" your current "IT guy". Get a list of administrative level usernames/passwords for all critical software and hardware. Consider where this is information is stored and updated and always make sure both individuals always have access to this information. On a side note, something we see quite often is the "IT guy" keeps a list of users' passwords such as Windows logins or e-mails. This should never occur and is a huge security risk in itself. There is simply no justifiable reason for this.

Create a step-by-step process with the "IT guy" for everything that would need to happen should he or she ever depart the organization. And finally, even if you are against outsourcing your IT to an MSP, at least consider having an MSP or other professional IT services company come in and evaluate your network from time to time. When it comes to IT, an organization that puts all of their faith and trust in a single individual is begging for a crisis such as rogue access.

"If you're working with an MSP, take the time to sit down with them and establish a process if one hasn't already been established. In other words, what happens when the guy who supports your network leaves the MSP? A good MSP will already have a process for this that will involve changing critical passwords. You can of course and should add to this process based on your additional needs and concerns."

4 REASONS YOU NEED A SINGLE SIGN-ON PORTAL

More and more SMBs are embracing the cloud as a way to increase employee productivity and optimize IT budgets. But the more cloud apps you use, the more complicated things get for users and for IT.

Any individual cloud app delivers tremendous benefits in terms of cost of ownership, user productivity, and IT agility. That's why businesses have embraced the cloud so rapidly—56% of organizations use 6 or more SaaS applications[1] —and why the number of very small companies using paid cloud apps is expected to triple in the next three years.[2]

BUT AS YOU EMBRACE THE CLOUD, THE INCREASING NUMBER OF CLOUD APPS IN THE IT ENVIRONMENT QUICKLY OVERWHELMS IT'S ABILITY TO ASSURE SECURITY, MANAGE COSTS AND MAINTAIN CONTROL. THIS CREATES MULTIPLE PROBLEMS, INCLUDING:

1.
Insecure user password practices.
It's impossible for the average user to remember strong passwords for all the cloud services they use. Even tech savvy users end up taking shortcuts: reusing passwords, creating weak passwords, storing passwords in email, and even writing down passwords and pasting them to their monitors.

2.
Inability to manage access.
In many companies, IT has to scramble to revoke a departing employee's access to cloud apps—and, sometimes, apps can slip through the cracks. Often, users provision themselves for cloud apps—and IT has no idea that company data is being housed in yet another datacenter.

3.
Inefficient employees and lost productivity.
In the days of desktop-based applications, it was easy for employees to find and launch the tools they needed to use. Today, while cloud-based apps offer dramatic benefits to IT and employees alike, the proliferation of these apps has reduced employee productivity by forcing them to constantly hunt for login URLs and remember multiple usernames and passwords.

4.
Lack of cross-service IT efficiencies.
With multiple cloud services to manage for every user, IT is unable to share settings or create efficiencies across them all. They have to manage multiple vendors with multiple control panels, multiple passwords and multiple sources of support—as well as the mobility, integration and security complexities introduced by each one.

[1] Cloud Computing Demands Enterprise-class Password Management and Security, Enterprise Strategy Group, April 2013
[2] Microsoft SMB Business in the Cloud Report, 2012

SINGLE SIGN-ON WILL SOLVE THESE PROBLEMS

A single sign-on (SSO) service can give your employees a single portal with one-click access to all their cloud apps. And because they only have to remember one login and one password, they can more easily comply with strong password policies.

Your IT staff will also love it. They'll be able to quickly build a portal to all the cloud apps your employees use—and just as quickly revoke access to the portal when employees leave.

TRY INTERMEDIA APPID—THE SSO SOLUTION THAT'S MADE FOR SMBS

Intermedia is the world's largest one-stop shop for cloud IT services and business applications. We recently launched Intermedia AppID as an SSO solution made specifically for SMBs. AppID comes pre-configured for over 1,500 cloud apps. And it's simple and quick to add others, including proprietary and custom apps.

If you already use Intermedia services, it's an easy add-on. And if you're new to Intermedia, you can get AppID as a standalone service or as part of our Office in the Cloud suite of IT services.

Dataprise Inc.
IT Services for Growing Businesses

INTERVIEW WITH CHRIS SOUSA, VICE PRESIDENT OF ENTERPRISE DESIGN AT DATAPRISE, INC.

Dataprise is a leading local and national Managed Services Provider (MSP) with over 18 years' experience in providing proactive IT support & infrastructure management, strategic IT consulting services, 24x7 help desk services, and powerful managed cloud services & tools to small and mid-sized organizations. We spoke with Mr. Sousa recently about the issues faced by Dataprise customers when ex-employees walk away with access to company data and the ways his team helps eliminate that threat.

HOW BIG OF AN ISSUE IS ROGUE ACCESS FOR THE ORGANIZATIONS THAT YOU WORK WITH? SHOULD BUSINESSES BE CONCERNED ABOUT ROGUE ACCESS?

The size of the issue is really going to depend on a few different factors: the size of the company and how sensitive their data is. Do they have their customers' data and proprietary information? Also, you have to consider the malice or the intent behind the employee who retains the access.

We were in a sales meeting last week, and one of the big topics that came up was how to protect Social Security numbers and that kind of thing. And the prospective customer was really concerned about liability on their side if there was a data breach, how much they would have to pay out because of that breach, what our liability insurance was, etc.

We're right outside Washington, D.C., and we find that government contractors are very sensitive to this and are really on top of it. But we also deal with some low-tech environments that are relatively small (in the five-to-ten-user range), and they're not nearly as concerned.

Every once in a while they'll ask a question when they see an article on CNN, because Sony got hacked or Amazon or whoever. But we don't see a lot of those really small businesses being very interested or concerned about it.

"So we definitely were seeing businesses pay more attention to securing their data, keeping it under tight wraps. Not just because it's a good idea, but because of regulations, the potential for negative publicity and financial impacts."

WHAT KIND OF RISKS DOES ROGUE ACCESS CREATE FOR SMALL- AND MEDIUM-SIZED BUSINESSES?

Well, if Social Security numbers or any sensitive information were released as part of this, my guess would be, they would be on the hook from a legal and liability standpoint if they don't have a written policy in place and procedures to prevent terminated employees from getting into their environment.

ONE OF THE SECONDARY STATISTICS IN OUR SURVEY FOUND THAT 60 PERCENT OF EMPLOYEES WERE NOT ASKED FOR THEIR CORPORATE LOGINS WHEN THEY LEFT THEIR COMPANIES. WHY DO YOU THINK SO FEW COMPANIES ARE ADDRESSING THIS ISSUE?

When a company has in-house IT, the HR department, which typically conducts exit interviews, may not think to ask about that. They're looking at it from an HR standpoint and what they have to do to check off their boxes. As an outsource IT provider, one of the things we do is document the processes for both onboarding and offboarding. We're able to kind of provide them with templates and checklists ahead of time and really streamline the process.

AND HOW DO YOU ADVISE YOUR CUSTOMERS DURING THE ON-BOARDING AND OFF-BOARDING PROCESS? WHAT ADVICE DO YOU PROVIDE THEM TO HELP ENSURE THAT THESE TYPES OF RISKS DON'T HAPPEN?

Well, the biggest thing is to have a process and a checklist, and then review it on a regular basis. Look at all the different applications, all the different access points, all the different logins, etc. Come up with a baseline of items that you need to take care of. And decide who's going to take care of those items.

We then determine if there is a script that we can create or a way to automate it. We are looking for ways to disable access in one place that then disables the user's access elsewhere. We review the process quarterly or annually, depending on how often the environment changes, to see whether we need to implement a new system or add new items to our checklist for that customer.

WHAT KIND OF HORROR STORIES HAVE YOU ENCOUNTERED WITH CUSTOMERS AROUND ROGUE ACCESS?

We haven't heard much from Dataprise customers, to be honest. I think we're pretty good about advising our customers about what they need to do when employees come on board.

We've certainly heard horror stories from prospective customers about outgoing IT personnel and what they've done when they left. Those IT personnel still have access. They log in. They shut down a server. They delete data before they leave. We've also seen salespeople that leave and take customers with them.

WHAT ADVICE DO YOU HAVE FOR CUSTOMERS THAT ARE LOOKING TO PREVENT THIS?

Have a documented process, a policy, a checklist, and then look at it holistically. And not just the internal network. Look at the external applications that employees may be logging into on your behalf or shared-access accounts that have one login to a vendor site or to a portal.

WHAT ADVICE DO YOU PROVIDE YOUR CUSTOMERS FOR MANAGING THE PROLIFERATION OF BYOD AND BYOS?

First you need to decide if you really want to go down that path or not. Right now, it's kind of being forced upon a lot of IT departments by the end users. And sometimes the executives are the ones starting it. And it's IT's responsibility to rein that back in, unfortunately.

So you need to define a policy and a process around that, setting some limits. Also looking into a mobile device management (MDM) solution to help manage, protect and correct loss – remote wipe of those devices that are now going to contain sensitive company information.

AND WHAT ABOUT FOR MANAGING THE PROLIFERATION OF "BRING YOUR OWN APPS"?

One of the things that we're doing with some of our customers that have a lot of cloud apps is single sign-on. It really gives you one central place to secure, manage and lock down the access.

And we try to encourage end users to be open and honest about what apps they're using. Obviously we have tools we can put in place to monitor the network for traffic and everything else. But we'd rather have an open discussion about what functionality users need and how we can recreate that in a secure environment so both users and IT are happy.

In the end, I think the discussion around rogue access is something we're seeing more of. It's becoming an issue that people are paying attention to. I think the more that these bigger companies get hacked, the more that the SMB market's going to pay attention to it and be willing to act and invest to prevent it.

"It's also important to audit along the way. If you're able to determine that a week before an employee left, they downloaded a customer list or they deleted a sentence of data from the company's systems, and you can provide backup documentation, that can really help an organization fight back."

INTERMEDIA

The Business Cloud™

INTERMEDIA CAN HELP

Intermedia's Office in the Cloud offers a suite of cloud IT services that are fully integrated, secure and mobile. They're all managed through our central HostPilot control panel. Services include email, phones, file sync and share, single sign-on, security, mobility, archiving and more. Our services thwart the ex-employee menace by making it simple to revoke access to the entire cloud footprint with just one click.

GET OUR CHECKLIST AND BEST PRACTICES FOR ACCESS MANAGEMENT AND OFFBOARDING

Download our comprehensive checklist and best practices for managing user access to cloud apps during employment and after users leave. We include advice for onboarding new employees and specific recommendations for regulated businesses. Also included in this exclusive toolkit is a white paper by Osterman Research with more insights into avoiding the "ex-employee menace". Download your kit today at intermedia.net/RogueAccess.

DEPLOY INTERMEDIA'S BUSINESS-GRADE FILE SYNC AND SHARE

SecuriSync by Intermedia offers simple, easy-to-use cloud file sharing that's secured by industry-leading access control and protection. Learn more about SecuriSync at intermedia.net/products/securisync.

IMPLEMENT A SINGLE SIGN-ON PORTAL

Intermedia AppID is the only single sign-on solution designed specifically for SMBs—including deployment that doesn't require consultants to execute. Learn more about AppID at intermedia.net/products/appid.

INTERMEDIA The Business Cloud™

Sources: Osterman Research, The Benefits of Vendor Consolidation and Centralized IT Management, June 2014; Bureau of Labor Statistics, Table B 2014; 2013 Data Breach Investigation Report, Verizon, 2013