



# The Top 8 Security Blind Spots in Your SaaS Environment

DAVID POLITIS

CEO, BetterCloud

JOIN THE CONVERSATION on **BetterIT** in the #webinars channel! To join, visit [betterit.cloud](https://betterit.cloud)

What is a blind spot?

# Remember when employees started accessing corporate data on mobile devices?

The New York Times

*New Palm Pilot Links to Internet Wirelessly*

The New York Times, 1999

ComputerWeekly

**The changing face of the mobile workplace**

Computer Weekly, 1999



**Effects of  
Wireless Mobile Technology  
on Employee Productivity**

Wireless mobility changes the way employees work

Intel, 2003

The  
Economist

**A different way of working**

All sorts of companies are finding mobile Internet technology surprisingly useful

The Economist, 2001

# Then **this** happened...

The Washington Post

**Lost a BlackBerry? Data Could Open A Security Breach**

Washington Post, 2005



**The hidden threat: Residual data security risks of PDAs and smartphones**

TechTarget, 2005



**Mobile phones: the next frontier for hackers?**

IEEE, 2005

**COMPUTERWORLD**

OPINION

**Balancing the benefits and risks of mobility**

Computer World, 2003

The same thing is happening with **SaaS** now.

FASTCOMPANY

**Five Ways the New Google Docs Speeds Up Teamwork**

Fast Company, 2010

lifehacker

**How to Use Dropbox as a Killer Collaborative Work Tool**

Lifehacker, 2011

**strategy+business**

**The Promise of the Cloud Workplace**

strategy+business, 2010

**WIRED**

**CLOUD CHANGES THE WAY EMPLOYEES EXPECT TO WORK**

Wired, 2012

TIME

**How E-Mail Killer Slack Will Change the Future of Work**

TIME, 2015

# SaaS is creating unforeseen **security challenges**.

FASTCOMPANY

## Why Slack, Chatbots, And Freelance Workers Have Your IT Department Freaking Out

The rise of collaboration tools and the mixed workforce of full-time and freelance staff that use them means more security risks.

Fast Company, 2017

THE HILL

## Government tech team in hot water for 'data breach' tied to Slack

The Hill, 2016

ZDNet

## Hundreds of companies expose PII, private emails through Google Groups error

Oversight, not flaws, has led to some serious data exposure for firms including IBM's Weather Company and SpotX.

ZDNet, 2017

InformationWeek  
DARKReading

## How SaaS Adoption Is Changing Cloud Security

Dark Reading, 2014

CSO

## Data leakage risk rises with cloud storage services

CSO, 2013



**of IT professionals are just  
getting started managing SaaS  
apps, or teaching themselves**

You don't know what you don't know.

**And it's not your fault.**

# 5 Stages of Learning

NAIVELY CONFIDENT

MASTERY ACHIEVED

TEACHING OTHERS



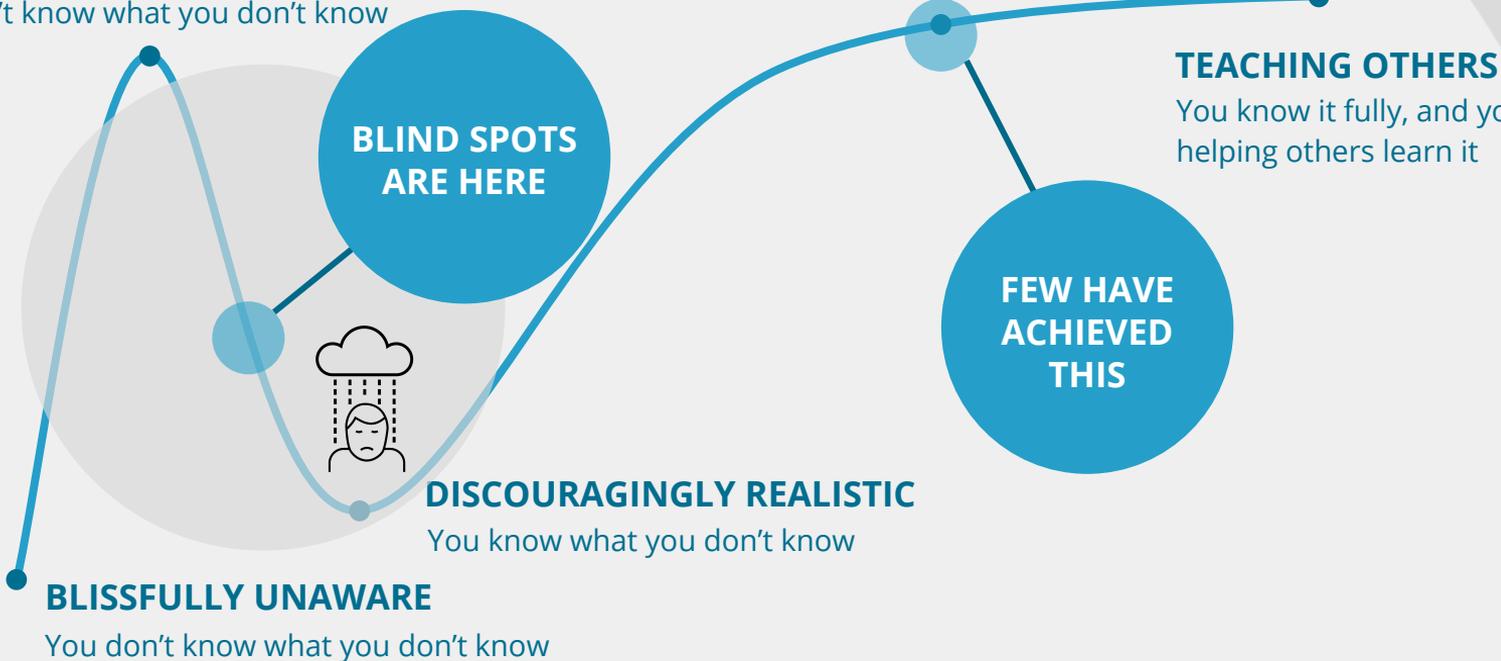
Kruger, Justin, and Dunning, David (1999). Unskilled and Unaware Of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments. *Journal of Personality and Social Psychology*. American Psychological Association. 77(6): 1121–1134.

# 5 Stages of Learning

## How to Manage SaaS Applications

### NAIVELY CONFIDENT

You think you know, but still don't know what you don't know



**BLIND SPOTS  
ARE HERE**



### DISCOURAGINGLY REALISTIC

You know what you don't know

### BLISSFULLY UNAWARE

You don't know what you don't know

### MASTERY ACHIEVED

You know it

**FEW HAVE  
ACHIEVED  
THIS**

### TEACHING OTHERS

You know it fully, and you're helping others learn it

# The 3 Most Dangerous Blind Spots

# POLL QUESTION #1

## BLIND SPOT #1

# Admin Permissions

The # of super admins in your org is higher than you think, which is a security risk.



1-3

BLIND SPOT #1 | Admin Permissions

## Why should I care?

Super admins can make changes that are disastrous.

Regulations like GDPR require you to limit admin permissions as much as possible.

CSO

**Time to drop unnecessary admin privileges**

*information age*

**GDPR compliance begins with privileged access management**

CSO

**Too many admins spoil your security**

BLIND SPOT #1 | Admin Permissions

## Why does this happen?

SaaS apps lack granular admin roles, so you end up giving everybody super admin access.

You don't think about admin permissions when you first deploy SaaS.





# CUSTOMER STORY

# POLL QUESTION #2

## BLIND SPOT #2

# Offboarding

The percentage of ex-employees who still have access to your data is higher than you think.



BLIND SPOT #2 | Offboarding

## Why should I care?

Ex-employees who retain access can steal, tamper with, or destroy confidential data.



Fired IT guy puts porn in ex-boss' PowerPoint, gets sweet revenge

*The Washington Times*

**Health care facility hacked by ex-employee using 2-year-old credentials: Justice Department**

BLIND SPOT #2 | Offboarding

## Why does this happen?

Offboarding is a very manual, time-consuming process that nobody wants to do.



A photograph of a person's hands typing on a computer keyboard, overlaid with a semi-transparent blue filter. In the upper left corner, there is a faint, glowing pattern of binary code (0s and 1s). The overall aesthetic is digital and professional.

# CUSTOMER STORY

# POLL QUESTION #3

## BLIND SPOT #3

# Data Exposure

Whether it's done accidentally or maliciously, your data is more exposed than you think.



BLIND SPOT #3 | Data Exposure

## Why should I care?

Sensitive or confidential information can be exposed to the entire org, or worse — the public. Hackers are mining information for phishing attacks.

BUSINESS INSIDER

Your salary info might be exposed due to this common mistake in the Google Groups settings

PCWorld

NEWS

Corporate Data Slips Out Via Google Calendar

ars technica

Doxed by Microsoft's Docs.com: Users unwittingly shared sensitive docs publicly

Thousands of docs with sensitive data still reachable from search engines, including health data.

BLIND SPOT #3 | Data Exposure

# Why does this happen?

SaaS apps are prone to very simple misconfiguration errors, making it easy to accidentally expose data.

G Suite

Sharing Options

Outside this domain - access to group members

Select the highest level of access to your group

- Public on the Internet** - Anyone on the Internet can access this content.
- Private** - No one outside this domain can access this content.

Link Sharing  
Locally applied

Link Sharing Defaults

Select the default link sharing setting for a newly created file:

- OFF**  
Only the owner has access until he or she shares the file.
- ON - Anyone at Demo BetterCloud with the link**  
Anyone at Demo BetterCloud who have the link can access this content.
- ON - Anyone at Demo BetterCloud**  
Anyone at Demo BetterCloud can find and access the file. ?

box

Default new links to:

- People with the link:** This content is open to people with the link. No login required to log in.
- People in your company:** Only users logged in with a email or users collaborating in the folder can access its content.
- People in this folder:** Only users collaborating in the folder can access its content.

Dropbox

Default shared link privacy

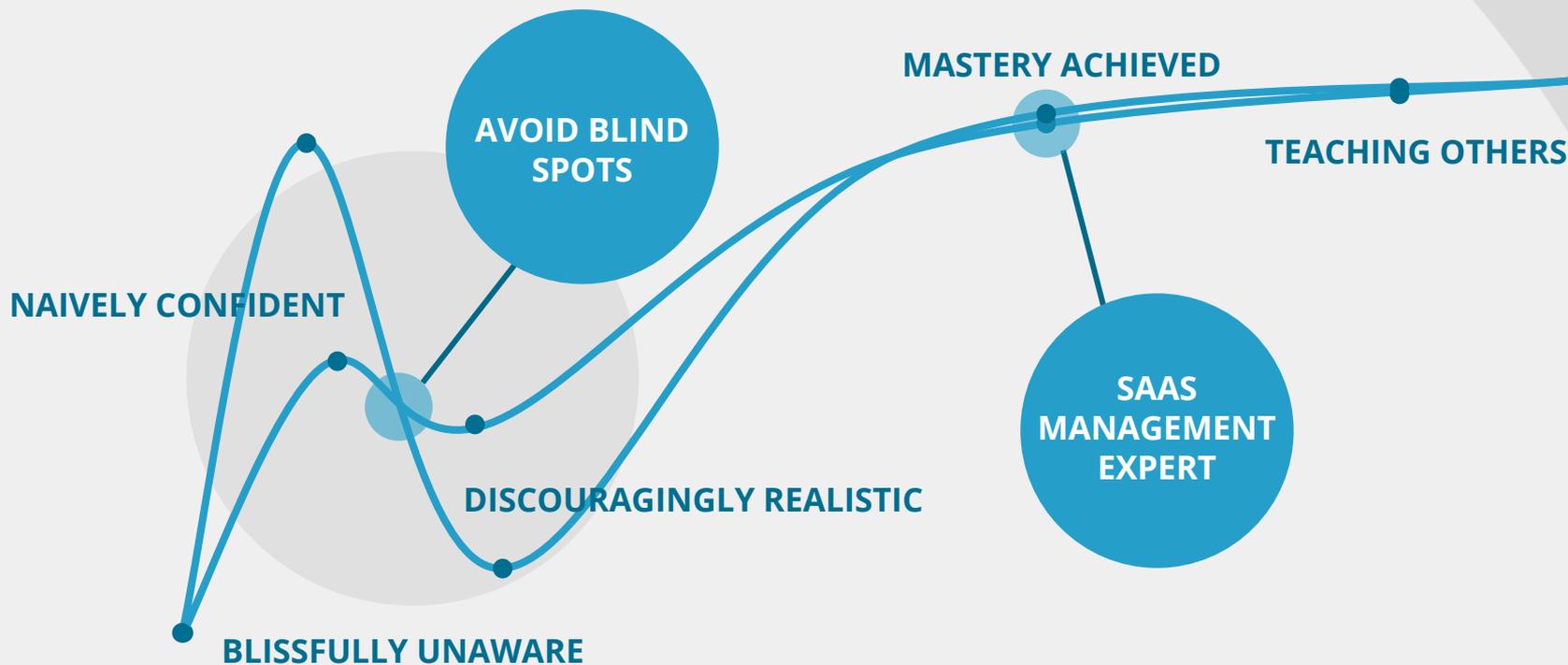
Who can access members' shared links?

Team only **Anyone**

# CUSTOMER STORY

# 5 Stages of Learning

## How to Manage SaaS Applications



# The 8 critical blind spots

1. Admin Permissions
2. Offboarding (User Lifecycle Management)
3. Data Exposure
4. Insider Threats
5. External Access
6. Groups Management
7. Licenses
8. Maintenance



To learn more about all 8 blind spots, download our whitepaper at  
<https://bettercloud.com/blindspots>

**Q & A**

The background is a solid teal color. In the bottom right corner, there are several overlapping, curved, wavy lines in a slightly darker shade of teal, creating a layered, wave-like effect.

BetterCloud

dave@bettercloud.com