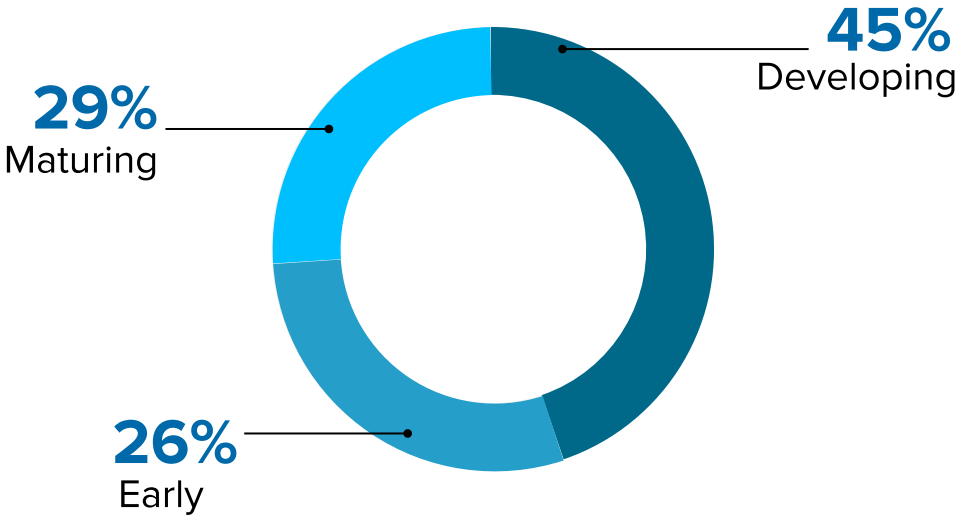
# The 10 Commandments of the SaaS-Powered Workplace

**TIM BURKE**
Director of IT, *BetterCloud*

# Why are you here?

# Every organization is undergoing digital transformation.




MIT Sloan Management Review, 2015

# 31

is the median number of sanctioned SaaS applications in organizations with 500 or more employees.

**POLL QUESTION**

# Which stage best characterizes your level of IT expertise in operating a digitally mature organization?

# 1.

# Thou shall know thy environment.

# HALF

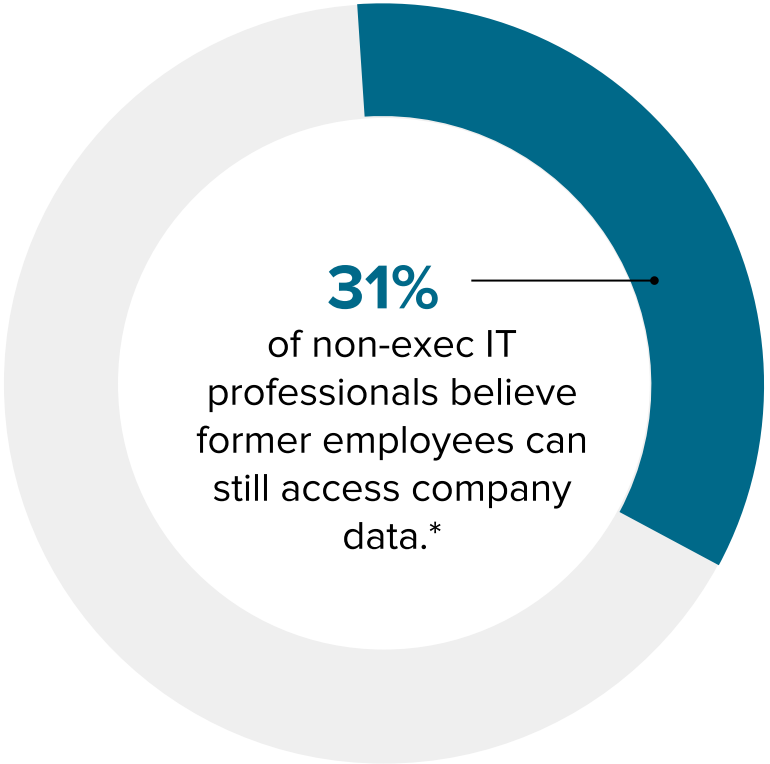
of IT professionals believe they lack visibility into their SaaS applications.

# 61%

of IT professionals do not believe they have complete control over their SaaS applications.

Trends in Cloud IT, 2016

# Do you *really* know everything about your environment?




*Trends in Cloud IT, 2016

# You can’t fix what you don’t understand.

## Build an IT Service Catalog

1. Name
2. Vendor
3. Precedence
4. Type
5. Login
6. 1st Owner
7. 2nd Owner
8. $/User/Month
9. Usage
10. Billing Model
11. Billing Terms
12. Contract Details
13. URL
14. Admin URL
15. Notes

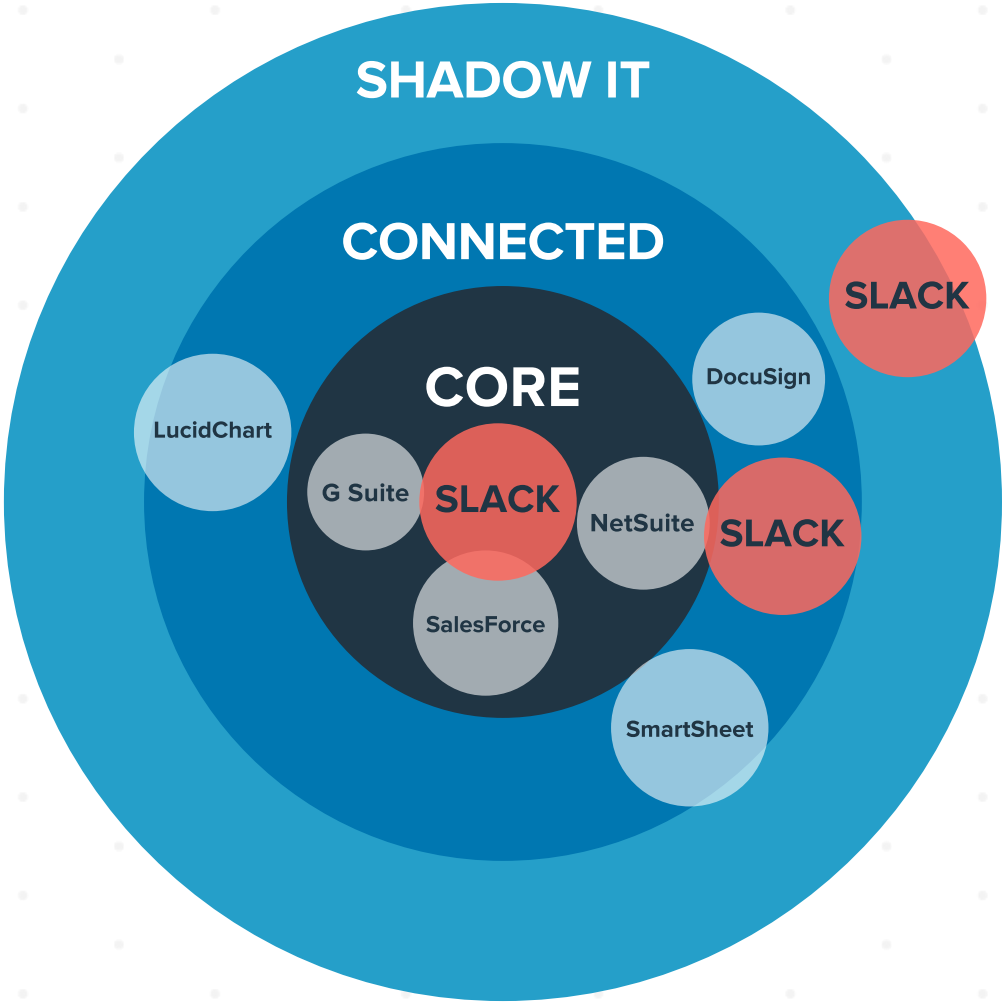
## The IT Budget

- Your IT budget is your baseline.
- Your IT budget will likely never tell the whole story.

## Shadow & Survey Users

- IT should take on a consultative role.
- Shadow IT isn’t always a bad thing.
- Don’t let ego get in the way. Listen to your end users because they know their needs better than anyone and you’re the only person that capable of tying everything together.

Which apps are core to your organization, and which apps are connected to them?



# 2.

## Thou shall always seek simplicity.

# Sometimes, less is more.

**Backend Systems**

- Virtualization Platform
- Servers
- Databases
- Data Networks
- Storage Networks
- PBX / Voice Services
- Automation
- Fault-tolerance
- Contingency Ops
- Customized hardware
- *Best practices*

**Applications**

- Connectivity
- Custom installations
- Managing privileges
- Security configuration
- Data backup
- Failover
- Interoperability
- Data import/export
- Local system configs
- Mobile dev management
- *Best practices*

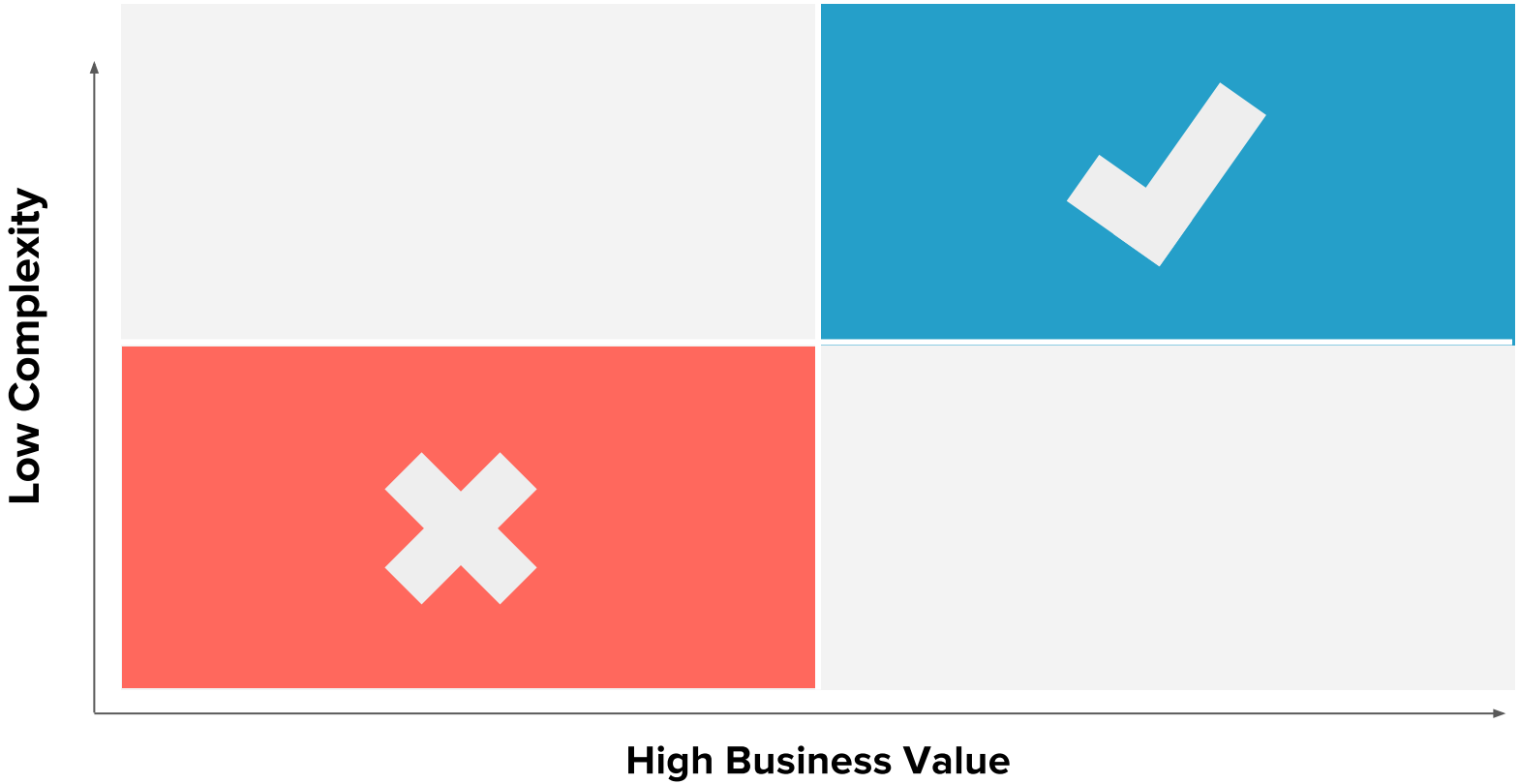
**People**

- Application familiarization
- Internal collaboration
- External communication
- Information management
- Workflow development
- Security awareness
- Privileged user training
- Change management
- Consumerization
- Shadow IT
- *Best practices*

**It is impossible to do *everything* well**

*Slide Credit: Andy Schwab, Author of Ultralight IT

# Identify and reduce unnecessary complexity.



# 3.

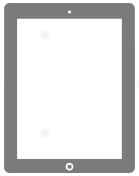
**Thou shall know that change be thy only constant.**

# The pace of tech adoption is speeding up.

## 10% market penetration

30 years

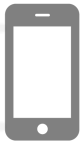
25 years



5 years

## 40% market penetration

64 years



10 years

Harvard Business Review, 2013

# Use shorter planning cycles, prioritize, and constantly update

## Shorter Planning Cycles

- Break plan into 3 segments
  - Short term
  - Long term
  - Over-the-horizon

## Prioritize Projects

- Break your projects into 3 segments
  - Critical
  - Important
  - Nice-to-have

## Get Ahead of Change

- Get your IT team on early access programs.
- Be agile because plans change.

# 4.

## Thou shall align with thy organization’s goals.

**To align IT with your organization you need to understand two things.**

1. How does your organization make and lose money?

2. How do your organization's employees use technology?

# 5.

## Thou shall reach and maintain security maturity.

# How would you rank your security maturity level?

| Category | Basic Organizations | Progressing Organizations | Advanced Organizations |
|---|---|---|---|
| Philosophy | Cybersecurity is a "necessary evil." | Cybersecurity must be more integrated into the business | Cybersecurity is part of the culture. |
| People | CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover. | CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled. | CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage. |
| Process | Informal and ad-hoc. Subservient to IT. | Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors. | Documented and formal with an eye toward more scale and automation. |
| Technology | Elementary security technologies with simple configurations. De-centralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance. | More advanced use of security technologies and adoption of new tools for incident detection and security analytics. | Building an enterprise security technology architecture. Focus on incident prevention, detection, and response. Adding elements of identity management and data security to deal with cloud and mobile computing security. |

*Source: Enterprise Strategy Group, 2014.*

# Instill a culture of security from day one.

## Onboarding & Ongoing

- Emphasize security during the onboarding process
- Employees should fear falling victim to a security breach, not reporting it
- Practical exercises.
  - Phishing test
  - Lastpass Security Challenge
  - Laptop Bounty Program
  - Lunch and learns

## Bake in Security

- SSO
- Password Management
- Multi-factor Authentication
- Proactive Reporting
- Incident Response Plan

# 6.

## Thou shall always seek to automate thy work.

The best IT professionals are usually the lazy ones.

# Tasks that are ripe for automation.

## ONBOARDING

**Imaging/Building of Devices** (Mac/PC)

**Adding to groups and shared folders**

**Provisioning in 3rd Party SaaS Apps** (Slack, Dropbox Zendesk, etc)

## OFFBOARDING

**Termination of access**

**Transfer of documents**

**Auto-reply/Inbox Delegation**

**Notifications to HR/others**

## SECURITY

**Suspicious login alerts**

**Two-Factor Onboarding**

**Device Updates**

# 7.

## Thou shall work to centralize thy users, apps, and data.

# Centralization gives IT added intelligence and the ability to automate across applications.

## USERS

A unified directory with in-depth user information across apps is now vital.

## APPS

Choose best-in-breed applications, and make sure to avoid overlap as much as possible.

## DATA

Centralize data when possible to keep IT in control and to keep your environment secure.

# 8.

## Thou shall transform, train, and repeat.

# Reacting to technology trends is vital for employee satisfaction.


MIT Sloan Management Review, 2015

# Constantly train your employees.

## LEVERAGE VENDORS

- Free Training Sessions
- Conferences
- Vendor Help Centers

## USE AVAILABLE RESOURCES

- Google
- Youtube
- Newsletters

## INVOLVE POWER USERS

- Find them and reward them
- Let the experts lead training sessions
- Make it part of your company culture (monthly meetings, etc.)

# 9.

## Thou shall document and log.

# Your logs should be extensive, but be wary of alert fatigue.

**Basic Security**

- Web filtering: Phishing, Malware
- Endpoint Protection
- Enterprise Mobility Management/MDM
- Salesforce Data Loss Prevention (DLP)
- DMARC
- Incorrect Login Attempts

**Networking**

- Bandwidth Usage
- Wi-Fi Channel Usage
- Ethernet Errors
- Monitored Clients

**Messaging/Collaboration**

- Slack: Active Users, # of Messages, etc.
- Slack integrations
- Google Drive Usage
- Suspicious mobile activity

**BetterCloud**

- Public Docs
- Two-Factor Report
- Recently Created Users
- Super Admin Users
- BetterCloud Data Loss Prevention
- Apps Audit

It takes time to build out a comprehensive knowledge base.

# 10.

**Thy network be thy rock,**
**and thy backup be thy savior.**

# Neglect your network and backups at your own risk.

## NETWORK

- In the SaaS-Powered Workplace, your network is one of the single most important investment you can make.
- Have a backup network.

## BACKUPS

- If you think you'll ever need it again, back it up.
- 3 backups, 2 locations, 1 bottle of whiskey

# BONUS

**Thou shall thoroughly evaluate thy vendors.**

# Always know what you're getting into.

**ESTABLISH SUCCESS CRITERIA**

Refine depending on the product/department

**RUN PILOTS**

Test with your users (both power users and regular users)

**CHALLENGE SUPPORT**

Even if you don't have an issue, raise one to see how it is handled