talla

Enterprise Data Security and Chatbots:

What IT Teams Need to Know

INTRODUCTION

As more companies adopt chat platforms like Slack, Hipchat, Microsoft Teams, and Google Hangouts, they are increasingly looking at chatbots to help streamline operations and help employees be more productive.

However, chatbots are an entirely new category of software. Their unique, text-based user experience presents some unique challenges to the I.T. department that is tasked with vetting them and protecting corporate data. At Talla, we've thought a lot about the issues that enterprises face as we've built a chatbot to replace the traditional I.T. or HR service desk. Our team is comprised of people that have built software for the enterprise, and we understand the issues that affect enterprise deployments.

This guide outlines considerations and tips that will help you evaluate and mitigate risks from enterprise chatbot deployments. It will help you understand whether a bot is suitable for enterprise, how to protect your corporate data, and how to deploy successfully across your organization. In creating this guide, we've made the assumption that bots are both invaluable tools and inevitable at organizations. Similar to the way the mobile revolution drove a BYOD policy to many work I.T. environments, we think user demand for bots will drive a BYOB (bring your own bot) policy that may be difficult to prevent. We hope the information contained in this book help you better educate your users about bots and make better decisions about how to deploy them safely.

1. EVALUATE WHETHER A CHATBOT IS ENTERPRISE-READY

Evaluating chatbot vendors is similar to evaluating cloud software. Your concerns should primarily be around safety and security procedures, and data access. Given that chatbots are a new category of software, most chatbot vendors are startups. As a result, many are still working through the necessary qualifications that would make them suitable for an enterprise deployment. Questions to ask:

- Do you have the right certifications? (SSAE16, SOC2, HIIPA, etc.)
- Under what conditions can your employees read my employees' interactions with the bot? Who at your organization has access to those interactions?
- Is data encrypted at rest?
- How are encryption keys managed?

Another key considering is data availability. Given their newness, many chatbot vendors are not yet offering SLAs. However, you should reconsider running any core business functions through a chatbot that doesn't have one. When asking about availability, make sure the vendor lists any 3rd-party apps or services used by their bot and ask about the SLAs of those services as well. Questions to ask:

- Do you offer an SLA?
- What happens if/when the bot goes down? How are customers notified?
- How is chatbot availability managed?
- What 3rd party services are used to deliver the chatbot, and what are their SLAs?

You should also ask about backups of the insights generated by the interaction of your users and the bot. Whose responsibility are those backups? If the bot is learning over time, does it "forget" if you have to roll back to an earlier version?

2. DEFINE WHO CAN INSTALL BOTS AND APPS

The technical process for installing chatbots varies by platform. Slack, Microsoft, and other vendors are still figuring out how it should work, and what level of control companies should have to limit who can install a bot. For example, Slack by default grants all users within a team to install apps. As an admin, you can turn off this ability, but it's on you to proactively do so.

The incentives of the chat platform vendors are conflicting because they both want to encourage bot adoption and cater to enterprise needs. On one hand, easier bot installation will lead to more bots being installed and used by more people, which makes the chat app itself stickier and drives a 3rd-party app developer ecosystem. On the other hand, enterprises want control over their I.T. environments and tools. Before you deploy your chat platform of choice, you should take the time to decide on an internal process for installing chatbots. Determine how they are evaluated. For example, does I.T. evaluate all of them, even if the install request came from a different department, or can departments evaluate and install their own bots?

You should also understand how risks are identified and managed in chatbot installations. Much of this will flow from your core I.T. philosophy. If you allow shadow I.T. to exist, then chatbots will be part of it. In this case, we suggest you still educate end users on chatbot issues so they can make smart decisions about what they install.

3. PROTECT YOUR CORPORATE INFORMATION

Like other software, chatbots will have access to your company's data, so you should be sure that data is being appropriately protected. Many bot companies, and machine learning companies, will use services like Amazon's Mechanical Turk or Crowdflower as a way to have a scalable "human in the loop" component to their service. The humans, in this case, often perform classification and identification tasks that help train the computer models. This is an important thing to understand because it is possible that your corporate data ends up being viewed by someone on one of these sites. Be sure to clarify whether or not a chatbot uses an external service for training, or whether there are any "humans in the loop" who don't work at the company directly.

Some companies have business models that rely on gathering data and training it across customers in order to resell a larger or smarter data project. This may be acceptable to you if the data is cleaned and anonymized, but you should ask questions to be sure.

Questions to ask:

- Is any of our data sold directly?
- Is any anonymized version of our data sold?
- Are any models trained on some derivative of our data sold?

You should also think about how bots protect the integrity of information in an organization. If part of data collection is done by asking your employees questions, what happens when the bot gets five different answers from five different people? You should understand how the bot reconciles information to avoid it being manipulated.

4. UNDERSTAND TRAINING AND MACHINE LEARNING ISSUES

Chatbots are freeform and as a result, may lack data integrity or input validation controls. Whereas data in a traditional system would be more strongly typed. Data validation becomes an issue that bot vendors need to account for when building for the enterprise. As an example, when setting up a customer in a web app, each form field can be validated as the right data type, right length, etc. Most chatbots do not currently have the ability to do that. If you use a chatbot to set up a bank payment, does the bot ask you to enter the account number a second time to validate that it's correct? If not, how does it let you know that it has validated your input? What does it do if your input is the wrong format?

Because most companies train models based on data from end users, you definitely want to understand how that training works, and which models are global across all customers and which models are unique just to your company and your data.

5. EDUCATE EMPLOYEES ON HOW TO INTERACT WITH BOTS

End user education is important when deploying chatbots. While bots are a piece of software, many are anthropomorphic, meaning that they are given human-like qualities. An example of this would be Apple's Siri or Amazon's Alexa. Both have distinct personalities and give users the ability to converse with them as they would a human. Because of this, there is sometimes confusion over how to interact with bots. Employees may treat the chatbot as another "system" and assume it properly handles the information it is given. People are used to relying on system controls like roles/permissions; but regarding bots, they should be treated as people and not reveal information that is classified as sensitive.

Much like humans, chatbots will learn the rules of an organization over time. When a chatbot does break the rules, like revealing sensitive information, can it be trained not to do that again? Are mistakes correctable in the chatbot framework? Be sure to look for bots that have more control over this type of training.

6. DETERMINE HACKABILITY OF INFORMATION

Chatbots can't always easily distinguish between what is sensitive information and what's not, so evaluate whether there's a potential risk of revealing information to the wrong parties. Very few bots at this point have any sort of information classification scheme. As bots do more, and access more of your information, it's important to know how that information can be accessed by your employees.

Most I.T. system hacks don't come from brute force technical tactics. They rely on social engineering. This raises an issue - can a bot be socially engineered? For example, could a clever user ask a bot a series of questions and piece together the answers in ways that expose information they shouldn't have access to? It is important to find a way to monitor bots and understand if this is happening. Be sure to ask questions about bot information classification architecture when evaluating chatbots

SUMMARY

Conversational interfaces are starting to take over the workplace. Their powerful impact on productivity, and simple user experience of chat, mean they aren't going away. But because they are new, there may be "unknown unknowns" related to security and privacy. The best advice we can give you is to deploy bots early so you can learn about these issues as the industry grows, and develop your own set of best practices that are appropriate for your company. Here's a roundup of the tips we covered:

Tip #1: Evaluate whether a chatbot is enterprise-ready: Understand what policies and procedures are in place to protect your data, including vendor certifications, who has access to your data, how it's encrypted, and whether SLAs exist.

Tip #2: Define who can install bots and apps: Put a policy in place and make sure that it is supported by your chat platform to determine who within your organization has the ability to evaluate, add, and delete apps and chatbots from your organization's instance.

Tip #3: Protect your corporate information: Understand how the chatbot vendor uses your data and whether or not they sell/provide it to 3rd parties for processing.

Tip #4: Understand training and machine learning issues: Find out from your chatbot vendor how they maintain data integrity and control input validation. Since most bot companies train their models based on data from end users, you want to understand how the training works.

Tip #5: Educate employees on how to interact with bots: Train your employees proactively on how best to use bots and what information is appropriate to share with them. Since often times bots are given human-like qualities, employees may treat them as humans rather than software, which can lead to issues.

Tip #6: Determine hackability of information: Ensure that bots you use are monitored to prevent employees from accessing information they shouldn't have access to.

ABOUT TALLA

Talla is your Service Assistant, bringing an A.I.-powered service desk to HR, IT, and other internal service teams. Manage and prioritize inquiries, automate answering FAQs, and proactively educate your employees, all within chat apps like Slack and Microsoft Teams. Deliver a better employee experience to your team and keep everyone knowledgeable, engaged, and productive. To get started with Talla, visit http://www.talla.com or contact us at sales@talla.com.