whistic

State of Transparency and Trust

Why publishing security information publicly increases trust with customers and influences purchase decisions

Introduction

It's no secret that everyone's data is at an increasing level of risk due to the potential for a breach, and those breaches can have a lasting impact beyond the financial cost of cleanup. They can also cause a loss of trust with consumers that may never be repaired.

As a result, customers aren't just concerned about data breaches after they happen. They are being more and more vigilant about working with companies that have a good reputation and are showing what they're doing to protect confidential information. The best way companies accomplish this is by being transparent about security policies and procedures, which results in increased trust with customers and ultimately accelerates the sales process for vendors.

In an effort to identify trends in this space, we reviewed security and compliance content contained on the websites of the *Forbes* Cloud 100 companies, which is a list of the top private cloud companies in the world compiled annually. We also surveyed more than 500 cyber and information security practitioners to gauge their opinions on transparency and what vendors can do to build trust with customers. What follows are the findings from that research along with recommendations for building a vendor security program that helps establish trust at critical points in the sales cycle.

Key Findings

Cloud 100 companies

Early in 2021, we set out to discover how the top SaaS businesses in the world were projecting their security and privacy posture publicly. We scoured the websites of *Forbes* Cloud 100 companies to see what type of security information and documentation they were providing customers and prospects access to. Below are some of our key findings.

The importance of security certifications and audits

Many Cloud 100 businesses are emphasizing certifications and audits on their privacy pages, including SOC 2 (43%), ISO 27001 (33%), PCI Compliance (21%), and HIPAA (15%), among others.

TIP **With a Whistic Profile, you can easily highlight badges of all of the questionnaires, certifications, and audits your company has completed.**

Cloud 100 companies project compliance

With news of data breaches becoming more and more prevalent, cloud businesses are being more proactive about publishing privacy policies and showing what they're doing to protect their customers' private information. In fact, our research found that 87% of businesses in the Cloud 100 have privacy pages on their website.

Additionally, as more legislation is passed to protect consumer data—like CCPA and GDPR—businesses that handle personal information need to show what they're doing to comply with various privacy laws. As a result, 63% of Cloud 100 businesses display their compliance with GDPR, while 57% display CCPA compliance.

Contact information is hard to come by

Only 18% of Cloud 100 companies include contact information for privacy teams, while just three percent include an email address for the security team.

Few offer vulnerability disclosure information

Just two percent of Cloud 100 companies' security or privacy pages included a vulnerability disclosure email or phone number, while only nine percent included details about a bug bounty program.

Survey results

Contents of security and trust pages

In September 2021, we surveyed 520 information security and cybersecurity practitioners about what items they think are most important when evaluating a company's security posture, which of those items they include on their security pages, and finally, what respondents expect from their vendors during a security review.

Higher frequency of security pages than Cloud 100

Eighty-one percent of respondents indicated they had a security page on their company's website, which is significantly higher than we found among Cloud 100 companies, but more in line with the number of privacy pages found among the Cloud 100. One reason for this may be that some companies view privacy and security pages as synonymous and don't feel the need to include web pages for both.

Publishing contact information publicly should be a priority

Priorities for survey respondents are consistent with Cloud 100 as privacy policies and security questionnaires are the most important type of information companies need to display on their website. Where our survey respondents differ from the Cloud 100 is the importance of contact information for the security or privacy team.

Our survey found that 40% of respondents thought it was important to include that contact information on their security page, while just 18% of Cloud 100 websites included that information on their security pages.

SOC 2 and ISO 27001 more important to survey respondents

Additionally, there was more of an emphasis on including information related to GDPR and CCSA for Cloud 100 companies, while our survey found ISO 27001, SOC 1, SOC 2, HIPAA, and PCI Compliance more important.
There are a number of reasons this might be the case, but the most obvious is that Cloud 100 companies may have more dealings in California and Europe than our survey respondents and have built their security program around the most rigorous regulations they are required to follow.

What security requirements respondents require of vendors

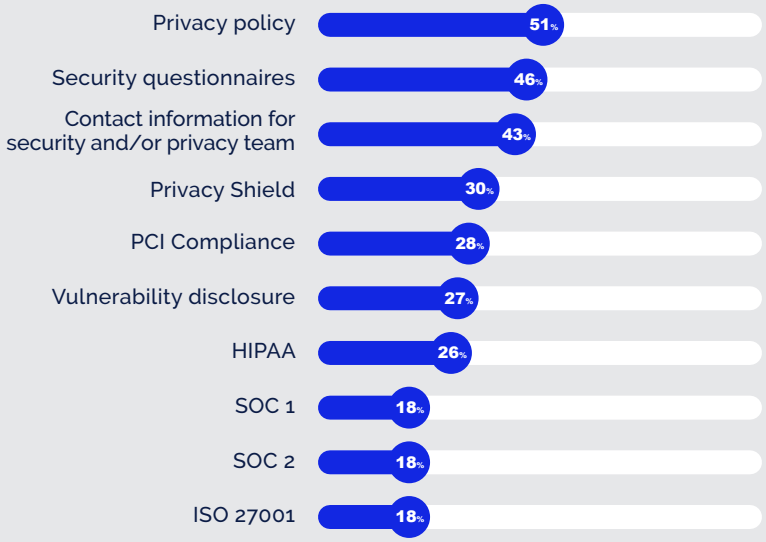
For the most part, what security information respondents require of their customers and what security information they think is most important is consistent. They only differ in the order of importance.

Majority of respondents are flexible with what security information they would accept from vendors

Seventy-seven percent of respondents say they are flexible and accept various audits, certifications, standards, and questionnaires from vendors, while 13% say it depends on the vendor, and only 10% say vendors must complete the questionnaire that is sent to them.

TIP **Compiling all of your security documentation in a Whistic Profile makes it easy for customers to assess you and for your InfoSec team to keep tabs on your security info.**

Which of the following would you require vendors to provide as part of your vendor assessment program?



Percent of respondents say they are flexible and accept various audits, certifications, and questionnaires

Percent of respondents say it's important to include contact information on their security page

Percent of respondents indicated they had a security page on their company's website

Percent of respondents say vendors must complete the questionnaire that is sent to them

Key Findings

How transparency impacts the vendor assessment process

In addition, we surveyed this same group about the importance of transparent security practices not only for their vendors, but for their business as well. The following are some of our key findings.

Transparent security practices influence purchase decisions

The most compelling piece of information gleaned from our research is related to purchase intent. We found that 96% of respondents said they would be more likely to purchase from a vendor that is transparent about its security posture.

Vast majority of businesses believe it's important to share security information

Eighty-four percent of respondents feel that it is at least somewhat important for businesses to share security information publicly, with 52% indicating that it is very important. Almost no company in the survey (just two percent) feel that sharing security information is unimportant for businesses.

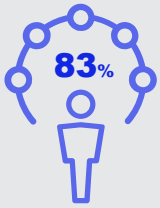
Sharing security information proactively simplifies security reviews

The two biggest benefits of sharing security documentation proactively with customers cited by respondents are that it simplifies the security review process (33%) and that it shows a commitment to transparency (33%). That is followed by speeding up the sales or buying process (25%) and enabling sales to focus on selling (9%).

But that's not all, Ninety percent of respondents indicated that when a company publishes their security and compliance information publicly it increases their trust in that business.

TIP **Proactively sharing your Whistic Profile or publishing it on your website and/or the Whistic Vendor Security Network™ builds trust with customers and accelerates the sales process.**

Percent of respondents indicate that if a company's security documentation were available on-demand it would speed up the vendor assessment process



Percent of respondents indicate that proactively defining and publishing their security requirements helps vendors respond more quickly

On-demand access to security documentation improves productivity by 20%

Ninety percent of respondents indicated that if a company's security documentation, including questionnaires, certifications, and audits, were available on-demand on a security page it would speed up the vendor assessment process. In fact, respondents said having on-demand access to security documentation would save them 12.3 hours per week, on average, assessing vendors.

Additionally, there is a high likelihood that businesses would be willing to conduct a Zero-touch Assessment™ using an on-demand questionnaire, provided the information were thorough. Our research shows that 37% of respondents said they would be very likely to conduct zero-touch assessments, while another 37% indicated they would be somewhat likely.

On the flip side, 83% of respondents indicated that proactively defining and publishing their security requirements helps vendors respond more quickly.

Best practices for building effective security and privacy pages

Based on these findings, combined with decades of experience, the team at Whistic has innovated the way trust and transparency is built through solutions like our Vendor Security Network. We've compiled some simple suggestions every company can implement to improve transparency and build trust with customers.

Be open and honest about security and compliance

Transparency in your security and compliance practices demonstrates the commitment and confidence your business has in the program you've built. In addition, being transparent helps you build trust with customers at a critical point in the buying cycle and could be a key differentiator that sets you apart from the competition and influences purchasing decisions.

Post clear links to security and compliance

As our research shows, the most important piece of information is access to security and compliance information, as well as a description of the business's commitment to confidentiality and any service level agreements related to uptime. As a result, SaaS vendors should make this information easy to access on their websites.

Provide on-demand access to standard security questionnaires

One of the key pieces of information potential customers ask when evaluating your security posture is response to security questionnaires, like the CAIQ, SIG, VSA, etc. Our research shows that a vast majority of businesses are willing to conduct zero-touch assessments of a business using on-demand questionnaires.

To help facilitate this, we recommend conducting self-assessments of your security posture using the most common standardized frameworks relevant to your industry. Then securely link to those completed questionnaires on the security page of your website, so customers can access them when they need to.

List relevant certifications and audits

In addition to security questionnaires, it's important to list or display the badges of all the certifications and audits you've completed (e.g., SOC 2, ISO 27001, etc.). As our research shows, the certifications and audits that are important differ from business to business. Most survey respondents place a high value on SOC 2 and ISO 27001 compliance, so providing access to these certifications will give customers peace of mind that you are doing everything you can to protect sensitive information. This can be managed with software like Whistic that can package those documents along with questionnaires and deliver it to your customers in one Profile to make it easier to review.

TIP **With Whistic, you can create multiple Profiles that contain varying degrees of information related to your security posture. For example, if there is certain information you would like to keep confidential, you can create a profile that requires an NDA before accessing.**

Information on vulnerability disclosure and bug bounty programs

Another way to show customers that you take security seriously is by including information about your vulnerability disclosure and bug bounty programs. Knowing you're actively tracking potential vulnerabilities and bugs in your software and taking the necessary steps to mitigate and eliminate them helps assure customers that their customer data is safe in your hands.

Contact information for privacy and security teams

One area that many companies can improve is making it easy for customers to connect with members of their security and privacy teams. It doesn't have to be anything complicated. It can be as simple as including an email address on the page, or it can be a little more nuanced, like a form that ties into your IT ticketing system.

Include an overview of your security program

Finally, you should include an overview of your security program, including information on what encryption you use, your incident response plan, and information related to your disaster recovery/business continuity plan. To keep your page streamlined and concise, you can also include whitepapers that cover that information.

How Whistic can help

Whistic is the best way for companies to assess, publish, and share security information, which enables them to be more transparent with their customers to build trust and help close deals faster. Below we highlight some of the ways we help companies do this.

Build once, share forever

With a Whistic Profile, you can consolidate all of your security questionnaires, frameworks, certifications, and audits into one place where it's easy for you to share and easy for your customers to access everything they need to conduct a security review.

Provide on-demand access to all of your security information

Grant access to your Whistic Profile directly from your website making it easy for customers and prospects to perform Zero-touch Assessments™ on your company.

Take advantage of the Whistic Vendor Security Network

Earn the trust of your customers before they even engage your sales team by publishing your security documentation to the Whistic Vendor Security Network, which simplifies the process to assess your security posture and results in faster sales cycles.

www.whistic.com