Overlooked SaaS Security Risks

What you need to know for safeguarding your business & earning customer trust

INSIDE YOU'LL FIND:

+ Top 5 Cloud Security Threats
+ How to Tackle Cloud Threats
+ Tips to Gain Trust and a Competitive Advantage
+ An Insider Look into Your Customers' Evaluation Checklist

Software-as-a-Service (SaaS) is Here to Stay

Take the Time to Think About It

It's expected by the close of this year that 94% of organisations will be using a cloud services[i]. Why? Simply because businesses understand the operational benefits of incorporating cloud computing. **However, the security risks associated with cloud adoption cannot be overlooked.** Businesses see the security risks associated. Buying decisions, whether for B2B or B2C organisations, revolve around assessing the risks associated with software applications before purchasing and integrating them into their environments.

In this guide, we will identify the top security threats to cloud platforms and cover how to these minimise risks — to gain a strong security posture and earn client trust. Let's look at the bigger picture first to address the current cloud-based business landscape.

The Landscape

Cloud Adoption Rates Rise

During the global pandemic, cloud adoption was a vital solution to allow staff to work from home. It has now shifted to become a viable solution to support environmental sustainability — reducing the on-premises carbon footprint.

Simply put, SaaS is convenient and enables businesses to maintain operations, scale up and follow mandated corporate governance guidelines.

Demand and Competition Increase

Now that demand has increased there is more competition among cloud service providers as over 90% of organisations utilise not just one cloud service but use a multi-cloud operational strategy[ii].

This should not only be acknowledged but understand that to gain a competitive advantage, SaaS providers must facilitate sustainable and secure solutions to protect customers' data.

Information and Data Security Are in Demand

It is estimated that by 2025, there will be 175 zettabytes of stored data on the cloud which makes the threat landscape larger and more enticing for threat actors to facilitate a breach[iii]. Clients trust that SaaS platforms have strong controls to help mitigate the chances of a security breach. Even more so after the Solar Winds attack that heightened the awareness of how many businesses can suffer just from one supplier breach. Due diligence and trust are now being demanded by customers.

Educated clients often base cloud platform buying decisions on whether the provider can demonstrate information security integrity and provide proof that data controls are governed through compliance frameworks. 93% of businesses identify cloud security as one of their main security concerns[iiii]. To gain and maintain a competitive advantage, cloud-based providers must be positioned as trustworthy with a good brand reputation.

SaaS platforms transmit and store client data. Clients trust that SaaS platforms have controls that ensure strong confidentiality, integrity and availability of their information, to mitigate the chance of a security breach. Whether the data is considered Personally Identifiable Information (PII) or not, customers hold you, as the supplier, accountable for the privacy, risk and security of their data.

Read on for our top five security threats and tips from security and risk professionals with over 30 years of experience — covering important measures in your security programme to mitigate breaches and build customer trust.

Top 5 Cloud Security Threats

Embrace Risks Before They Embrace You

1. Inadequate Due Diligence – Lack of Security Testing

As the profit margins of SaaS providers continue to grow, challenges arise with implementing short System Development Life Cycles (SDLC) to go to market quickly. More often than not, security in software development is fast-tracked or left out of the development process entirely.

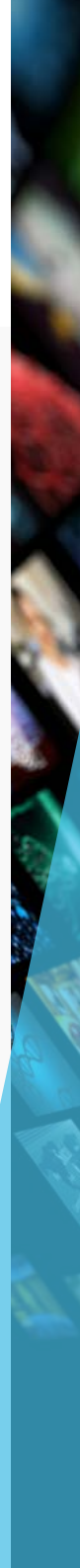
Failure to secure the app puts your company and customers' data at risk. Common app security vulnerabilities include failure to identify threats in injection flaws, broken access control, cryptographic security, insecure design, security misconfiguration, software and data integrity and potentially vulnerable and outdated components. Learn more about the top 10 most common application vulnerabilities identified by OWASP.

2. Non-Compliance with Regulations

Non-compliance is fraught with the risks of data breaches, hefty fines and reputational damage. To avoid breaching laws associated with compliance, there should be complete transparency between you and your customers in terms of where their data is being stored and what jurisdictions apply. Additionally, customers need to be able to trust that you are following best practice to secure their data.

Depending on the type of your app and location of your customers — the regulations and frameworks you may need to adhere to could include:

- **General Data Protection Regulations (GDPR)** - if your company provides services in the European Union and the European Economic Area you will be required to comply.
- **DPA 2018** - if your company provides services in the United Kingdom, you will be required to comply with the following data protection regulations.
- **Payment Card Industry Data Security Standard (PCI DSS)** - applies to all entities that collect, transmit or store credit card information.
- **ISO/IEC 27001** - an internationally recognised standard that provides a best-practice Information Security framework.
- **SOC 2** – a compliance standard specifically for cloud-based SaaS organisations operating in the US or providing services to customers in the US. The framework is based on Trust Service Criteria that specify how organisations should manage customer data.



3. Supply Chain Attacks

A 2022 global survey revealed that ransomware attacks on SaaS data were more successful than attacks on any other environment[iiiiii]. Threat actors are taking full advantage of vulnerable cloud-based platforms and capitalising on the large chain of user data to capture. Just look at the 2022 history of attacks that included GitHub and MailChimp.

The GitHub attack shows the connected risk in insecure software supply chains. Okta Inc. which provides products for Authentication, API Access Management, User Management, Multi-factor Authentication and Access Gateway MFA was one of the many that suffered the consequences of the breach[iiiiii]. The company used GitHub to store code in private repositories.

4. Failure to Educate Customers

Both provider and customer have a shared responsibility regarding security, but often this is not communicated from the beginning of the relationship. Far too often, customers expect the supplier to be accountable for the security of their data. Over 95% of cloud security breaches are caused by customers' misconfigurations and other missed steps[iiiiiii]. These breaches can impact not only the customer but your brand image even when it is not your fault as the provider.

5. Incident Response Inefficiency

In general, incident and breach response inefficiency is widespread among businesses not just the SaaS industry. Those that have policies and procedures in place often overlook the importance of practising response exercises with the team. This can lead to not only reputational damage and fines but the cost of legal counsel as well.

Regulations call for shorter reporting deadlines. If you are doing business in the EU, the GDPR requires data breaches to be reported within 72 hours. If you have customers in California, you will have to adhere to the California Consumer Privacy Act (CCPA) and notify each individual affected "without unreasonable delay." Both regulations bear hefty fines if not responded to in the allotted time.

How to Tackle Cloud Threats

Don't Play the Odds — Reduce Them

1. Implement Cloud Security Mechanisms

Security assurance activities include architecture analysis during design, code review during coding and build, and penetration testing before release. Perform Penetration Testing regularly to include testing People, Process and Technology. Testing will identify vulnerabilities and allow for remediation to secure your systems.

While remediation activities are crucial, protective measures including heightened visibility, management, proactive risk assessment and mitigation efforts should be incorporated into organisational security protocols.

2. Assess Compliance Regularly

With cyber threats on the rise, implementing risk management and being security compliant with SOC 2, ISO 27001, HIPAA, etc. has become necessary for SaaS companies. It helps to earn customer trust to patronise their services. If you are already compliant — ensure you are maintaining that compliance.

3. Conduct a Supply Chain Audit

You should consider third and fourth party supply chain risks. Even if you have policies and procedures for supplier management, it's still well worth the time to conduct an audit.

Audits help with identifying, assessing, and mitigating the cyber risks associated with the complex and connected nature of the extended chain of your product and service suppliers.

You can get an even closer look at your supplier's risks by integrating tools, such as those which Lab1 provides. This innovative tool can help identify if your suppliers (or you) have been compromised in a breach. It shows what and when the incident occurred and gives insight on what you can do about it.

4. Educate Your Staff and Customers

Your first line of defence is your staff. Information security and data protection training should start with them. Remember not to just provide training but integrate processes into everyday practices to instil a security culture within the organisation.

The second line of defence is customers. Security should be a shared responsibility but it's your duty to make this clear in the Service Level Agreement and on-boarding process. Educate customers that each party logically has certain security and compliance obligations.

5. Establish an Incident Response Plan & Practice

We've all heard it before, 'don't wait for a breach, prepare for one.' Every organisation should have a cyber security incident response plan but that's not enough. The plan must be put into practice so that when a breach occurs everyone is prepared on how to respond in a timely manner.

The plan should address key items like when to report the breach, mitigation protocols and how to respond to the press. Attending a data breach incident response course (such as the Cordery Breach Academy) can help you prepare and practice.

Now You Know the Threats & Solutions...It's Time to Take Action.

Tips to Gain a Competitive Advantage

Place Your Company Ahead with SOC 2, ISO 27001 and GDPR Compliance

Implementing a best practice standard will assure your customers the company has taken steps to secure systems and data. Many high-profile contracts will require you to have these certifications before conducting business.

Empower Sales to Use Compliance as a Unique Selling Proposition

You have worked hard to implement compliance and it is a value-added proposition. Encourage sales to highlight compliance in initial talks with customers.

Get Marketing to Promote Certifications and Compliance

Display your badge proudly on the website, wall and in all marketing collateral. It will put you ahead of your competition who may not have best-practice security measures in place.

Communicate with Customers

Letting your customers know straight away that security is a shared responsibility will show them that you understand its importance and are dedicated to information and data security.

An Insider Look into Your Customers' Evaluation Checklist

Know the supplier criteria your customer is considering when choosing a provider. In most cases, the IT team will carefully vet providers against certain criteria to present and convince leadership to support taking on a new SaaS platform. They will use an evaluation checklist that addresses the following topics:

Provider Name: [Insert Here]

- ☐ Is the cloud provider proven and is their reputation trusted?
- ☐ Has the provider been involved with any security breaches? If yes, how did they respond?
- ☐ Does the provider adhere with best practice security, privacy and compliance?
- ☐ What information security compliance certifications do they have?
- ☐ Is the SaaS reliable and can it meet the performance required?
- ☐ Does the provider offer customer support and what is their average response time?
- ☐ Is there a vendor lock-in clause in the SLA that will tie the company to a certain amount of years without incurring a cost to break the agreement?
- ☐ Does the platform integrate with our current SaaS platform(s)?
- ☐ Where is data stored? Who can access it? What measure do they use to protected it?
- ☐ Does the SaaS solution's backup and recovery capability?
- ☐ What is the vendor's roadmap for updates and improvements to the platform?

Aim Higher

Now that you have good insight into security risks and how to mitigate them — you are on the right track to success. The first step is knowing and the second is putting measures into place and practice.

If you have questions about getting started with compliance, how to conduct risk assessments, implementing staff awareness training or security penetration testing... the Risk Crew Team is always happy to help — It's what we do.

Sometimes to Get it Right — You Need the Right Crew

ABOUT RISK CREW

We are an elite group of information security governance, risk & compliance experts and the forerunners in the design & delivery of innovative & effective solutions with a 100% satisfaction guarantee.

Contact us for more information

+44 (0) 20 3653 1234
riskcrew.com
info@riskcrew.com

5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB
United Kingdom

Sources:
i: zippia
ii: hashicorp
iii: zippia
iiii: zippia
iiiii: odaseva
iiiiii: ExtraHop
iiiiiii: BleepingComputer
iiiiiiii: TechBeacon