# CLOUD CYBERSECURITY CHEAT SHEET

## 1 Cloud Computing

Cloud computing is just a new term for "Using someone else's computer." It sure sounds good & easy. But ready on... Technically, it refers to the use of networked infrastructure software and capacity to provide resources to users in an on-demand environment. With cloud computing, information is stored in centralized servers and cached temporarily on clients that can include desktop computers, notebooks, handhelds and other devices.

## 2 Business Challenges

Public cloud-based software as a service (SaaS) has become a common delivery model for business applications, i including office applications and sales-and-marketing software etc. in use at enterprises. Popularity of cloud- based applications, platform and infrastructure stem from the following business requirements:

- Quick Adoption: Business units looking for quick adoption of new applications as well as quickly change from one application provider to another.
- Cost Benefit: Short term cost-effective licensing
- Effective Collaboration: Business groups looking to collaborate with partners and customers, suppliers, subsidiaries and acquisitions
- Bring your own cloud (BYOC) - Employees are not waiting for IT; they're bringing cloud services to work.

As a result, business groups and employees, external partners and customers require IT organizations to support a diverse set of cloud-based SaaS applications.

## Balance Risk vs Productivity 3

Determine whether controls are sufficient and appropriate and if they provide adequate protection against anticipated threats along with a plan for risk mitigation... You must focus on making security measures easy to use, implement and maintain can balance security and productivity. Security controls shouldn't be viewed just as a static configuration, but rather with a scalable design – one where any instance of the service that is invoked provides the same risk posture and such that when a vulnerability is discovered, appropriate action can be taken to fix the design..

Continue reading on next page >

# CLOUD CYBERSECURITY CHEAT SHEET

## ④ Public Cloud Services

1. Application and Information clouds – Sometimes referred to as **Software-as-a-Service**, this type of cloud is referring to a business-level service...
2. Development clouds – Sometimes referred to as **Platform-as-a-Service**, cloud development platforms enable application authoring and provide runtime environments without hardware investment.
3. Infrastructure clouds – Also referred to as **Infrastructure-as-a-Service**, this type of cloud enables IT infrastructure to be deployed and used via remote access and made available on an elastic basis.

## ⑤ Cloud Benefits

Expand scalability – By utilizing cloud computing, IT staff can quickly meet changing user loads without having to engineer for peak loads.

**Lower infrastructure costs** – With external clouds, customers do not own the infrastructure. This enables enterprises to eliminate capital expenditures and consume resources as a service, paying only for what they use. Clouds enable IT departments to save on application implementation, maintenance and security costs, while benefiting from the economies of scale a cloud can offer compared to even a large company network.

(CONTINUED)

## Cloud Benefits ⑤

**Increased utilization** – By sharing computing power between multiple clients, cloud computing can increase utilization rates, further reducing IT infrastructure costs.

**Improved end-user productivity** – With cloud computing, users can access systems, regardless of their location or what device they are using (e.g., PCs, laptops, etc.).

Improve reliability – Cloud computing can cost-effectively provide multiple redundant sites, facilitating business continuity and disaster recovery scenarios.

**Increased security** – Due to centralization of data and increased security-focused resources from cloud computing providers, cloud computing can enhance data security. Cloud computing can also relieve an IT organization from routine tasks, including backup and recovery. External cloud service providers typically have more infrastructure to handle data security than the average small to midsize business.Gain access to more sophisticated applications – External clouds can offer CRM and other advanced tools that were previously out of reach for many businesses with smaller IT budgets.

**Downsized IT department** – By moving applications out to a cloud, IT departments can reduce the number of application administrators needed for deployment, maintenance and updates. It departments can then reassign key IT personnel to more strategic tasks.

**Save energy** – Going "green" is a key focus for many enterprises. Clouds help IT organizations reduce power, cooling and space usage to help the enterprise create environmentally responsible datacenters.

Continue reading on next page >

# CLOUD CYBERSECURITY CHEAT SHEET

CRAIG PETERSØN.COM

(CONTINUED)

## ⑥ Cloud Challenges

A lack of interoperability – The absence of standardization across cloud computing platforms creates unnecessary complexity and results in high switching costs. Each cloud vendor has a different application model, many of which are proprietary, vertically integrated stacks that limit platform choice. Customers don't want to be locked into a single provider and are often reluctant to relinquish control of their mission-critical applications to hosting service providers.

Application Compatibility – Most of the existing public compute clouds are not interoperable with existing applications and they limit the addressable market to those willing to write new applications from scratch.Difficulty in meeting compliance regulations – Regulatory compliance requirements may limit the use of the shared infrastructure and utility model of external cloud computing for some environments.

Achieving compliance often requires complete transparency of the underlying IT infrastructure that supports business-critical applications, while cloud computing by design places IT infrastructure into a 'black box."

## Cloud Challenges (con't) ⑥

accessible only through well-defined interfaces. As a result, internal compute clouds may be a better solution for some applications that must meet stringent compliance requirements.Inadequate security – By design, cloud vendors typically support multi-tenancy compute environments. IT managers must look for a balance between the security of an internal, dedicated infrastructure versus the improved economics of a shared cloud environment.

Security can be a key inhibitor to adoption of cloud computing.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We are not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, we make no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of the information and is not responsible for misprints, out-of-date information, or errors. We make no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.
If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

# CLOUD CYBERSECURITY CHEAT SHEET

**CRAIG PETERSØN.COM**

(CONTINUED)

## ⑦ Cloud Computing Security

When moving to the cloud take the time to review your security posture and what changes and controls need to be implemented to operate securely. You want a cloud platform that offers a wide variety of security services to address various requirements and by doing so you benefit from all the new features as they become available. Cloud security involves maintaining adequate preventative protections so you:

- Know that the data and systems are safe.
- Can see the current state of security.
- Know immediately if anything unusual happens.
- Can trace and respond to unexpected events.

Security has a lot to do with access. Traditional environments usually control access using a perimeter security model.

Cloud environments are highly connected, making it easier for traffic to bypass traditional perimeter defenses. Insecure application programming interfaces (APIs), weak identity and credentials management, account hijacks, and malicious insiders may pose threats to the system and data.

- Preventing unauthorized access in the cloud requires shifting to a data-centric approach. Encrypt the data.
- Strengthen the authorization process.
- Require strong passwords and 2 factor authentication.
- Build security into every level.

## Security Risks ⑧

1. Loss or theft of intellectual property - When cloud services is breached the cybercriminals get access your sensitive data. Additionally with certain services you face risks from their terms and conditions claiming ownership of the data that you uploaded to them.

2. Compliance violations and regulatory actions - Most companies today operate under some sort of regulatory control of their information,

Under these mandates, companies must know where their data is, who is able to access it, and how it is being protected. If not configured properly cloud computing services are often in violation of these requirements, putting the organization in a state of non-compliance, which can have serious repercussions.

3. Loss of control over end user actions - Companies may be in the dark about employees who are using cloud services, without their knowledge—until it's too late.

4. Malware infections that unleash a targeted attack -Cloud services can be used as a vector of data exfiltration of sensitive data.

5. Contractual breaches with customers or business partners - Contracts among business parties often restrict how data is used and who is authorized to access it. W If employees move restricted data into the cloud without authorization, the business contracts may be violated and legal action could ensue. Some cloud services.

# CLOUD CYBERSECURITY CHEAT SHEET

## 8 Security Risks (con't.)

maintain.the right to share all data uploaded to the service with third parties in its terms and conditions, resulting in a breach of a confidentiality agreement the company made with a business partner.

6. Diminished customer trust - Data breaches inevitably result in diminished trust by customers leading to a loss of business for the company, which ultimately impacted the company's revenue.
7. Data breach requiring disclosure and notification to victims - If sensitive or regulated data is put in the cloud and a breach occurs, the company may be required to disclose the breach and send notifications to potential victims. By Following legally-mandated breach disclosures, regulators can levy fines against a company and it's not uncommon for consumers whose data was compromised to file lawsuits.
8. Increased customer churn - If customers even suspect that their data is not fully protected by enterprise-grade security controls, they may take their business elsewhere to a company they can trust. There are a number of critics warning consumers to avoid cloud companies who do not protect customer privacy.
9. Revenue losses - This is a reason that many are now calling for increased oversight by the board of directors over cyber security programs.

## Concluding Thoughts 9

In order to reduce the risks of unmanaged cloud usage, companies first need visibility into the cloud services they choose and those in use by their employees. They need to understand what data is being uploaded to which cloud services and by whom. Their IT teams must assure that they are enforcing corporate data security, compliance, and governance policies to protect corporate data in the cloud. The cloud is here to stay, and companies must balance the risks of cloud services with the clear benefits they bring.