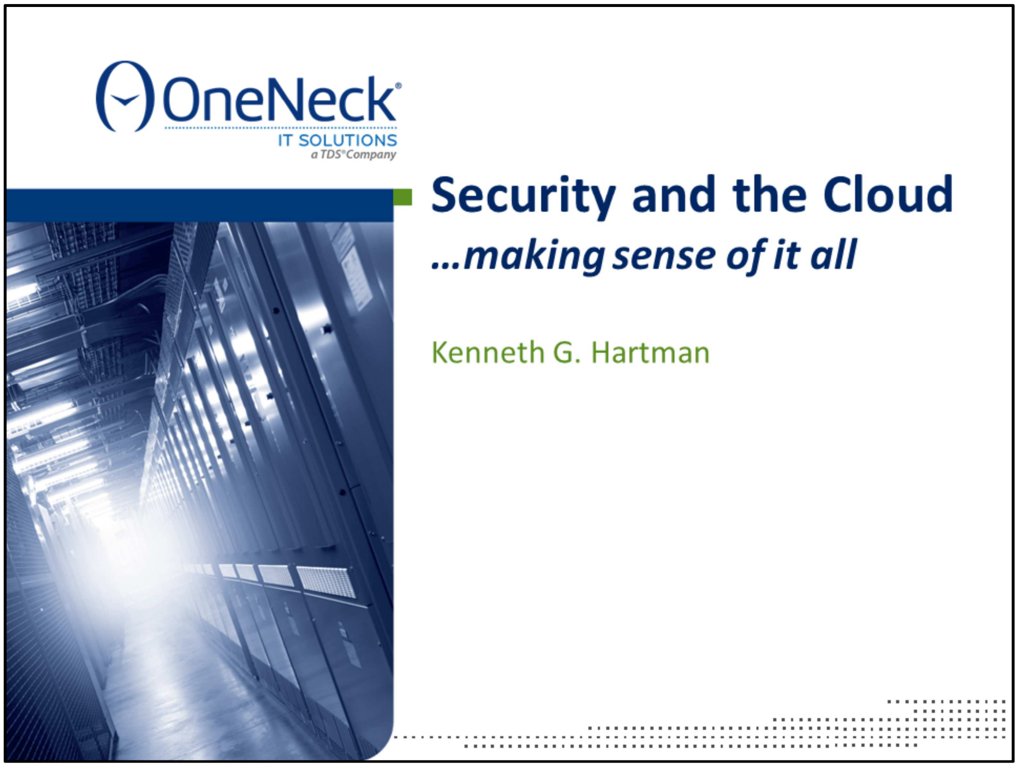
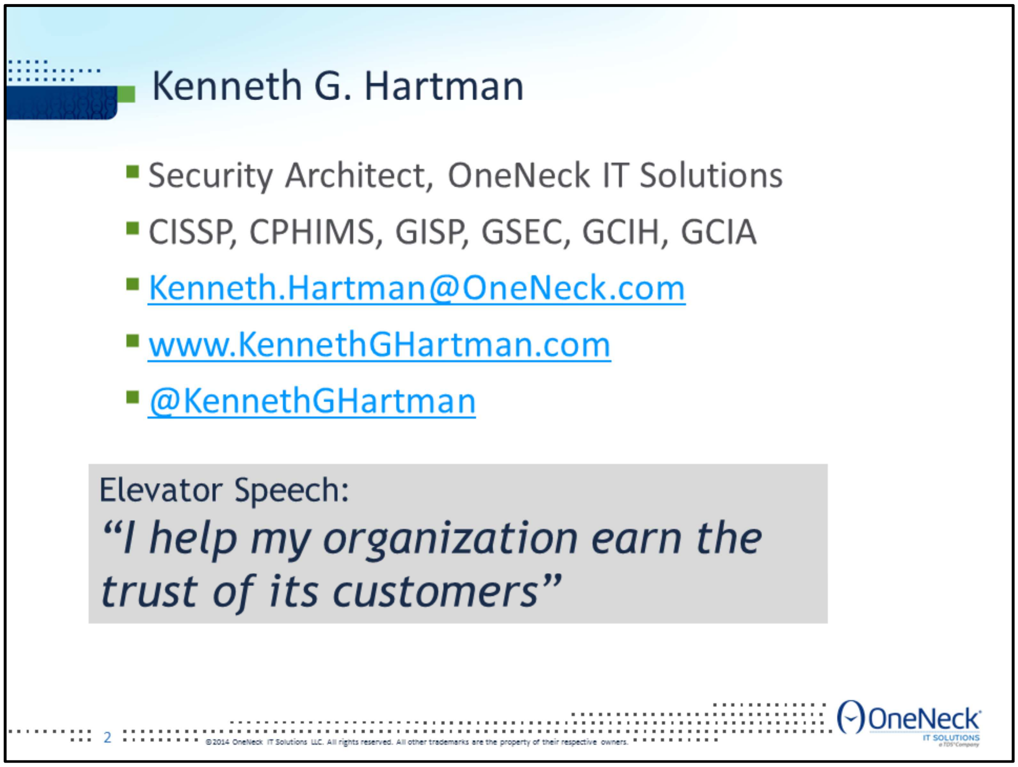


OneNeck®
IT SOLUTIONS
a TDS® Company

Security and the Cloud

…making sense of it all

Kenneth G. Hartman



Kenneth G. Hartman

- Security Architect, OneNeck IT Solutions
- CISSP, CPHIMS, GISP, GSEC, GCIH, GCIA
- Kenneth.Hartman@OneNeck.com
- www.KennethGHartman.com
- @KennethGHartman

Elevator Speech:
"I help my organization earn the trust of its customers"

2 ©2014 OneNeck IT Solutions LLC. All rights reserved. All other trademarks are the property of their respective owners.

OneNeck IT SOLUTIONS a TDS Company

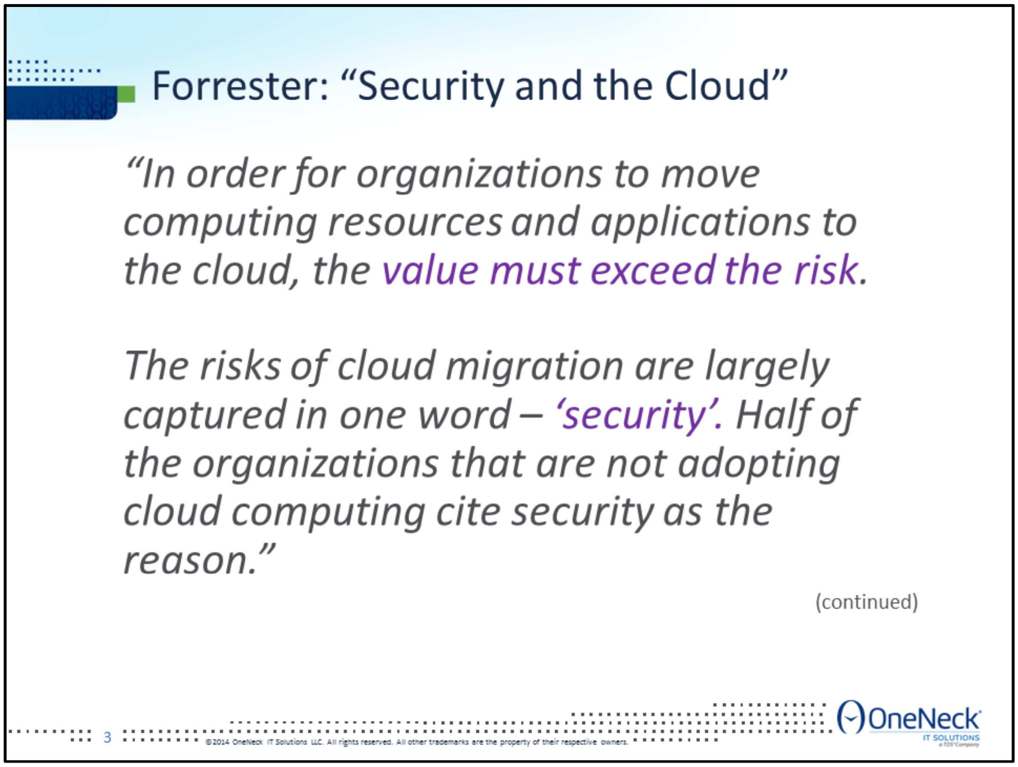
I'm Ken Hartman, the Security Architect for OneNeck IT Solutions. OneNeck is the growth services arm of TDS, providing Colocation, Cloud, Managed Services. We are also a Value Added Reseller.

By education, I am an Electrical Engineer who specialized in automatic control systems. This systems engineering perspective informs my thinking about processes, closed-loop feedback, and security controls.

**

Elevator Speech: *"I help my organization earn the trust of its customers"*

I thought that I would start off with a quotation from Forester that succinctly illustrates the "Security and the Cloud" concern. Next we will talk about some foundational security principles that are still applicable in the cloud. After that we will discuss what we mean by cloud services briefly, because it establishes a framework from which to discuss cloud security. Lastly, we will end with things to consider when securing your cloud or discussing security with a cloud provider.

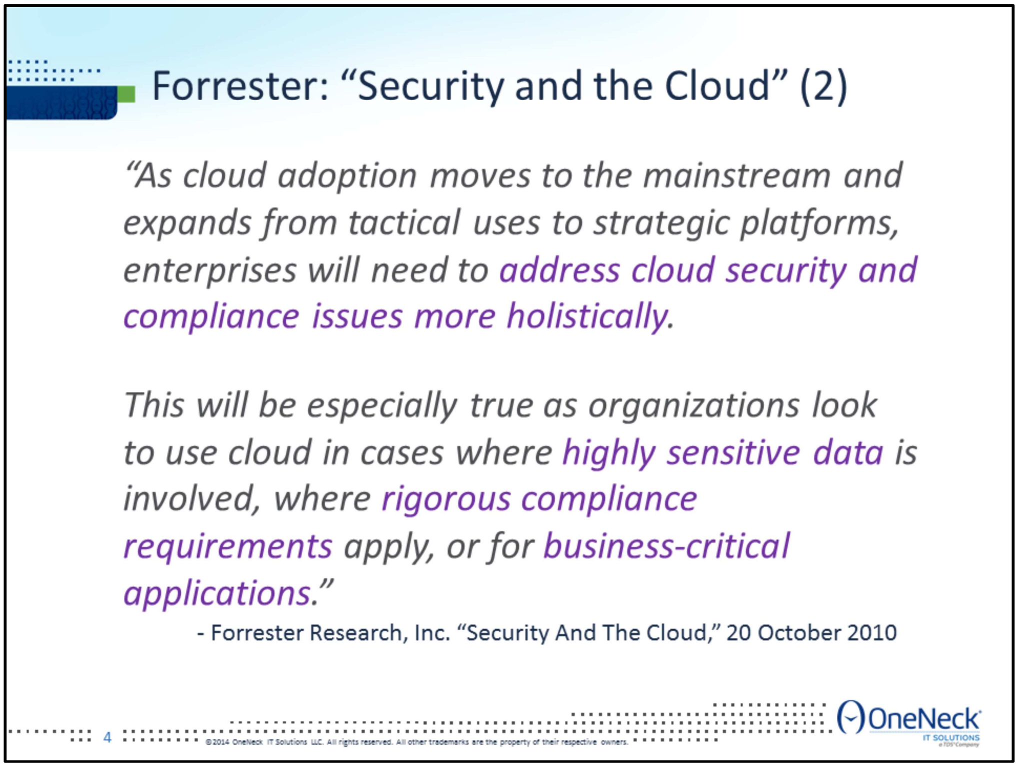


Forrester: “Security and the Cloud”

“In order for organizations to move computing resources and applications to the cloud, the value must exceed the risk.

The risks of cloud migration are largely captured in one word – ‘security’. Half of the organizations that are not adopting cloud computing cite security as the reason.”

(continued)

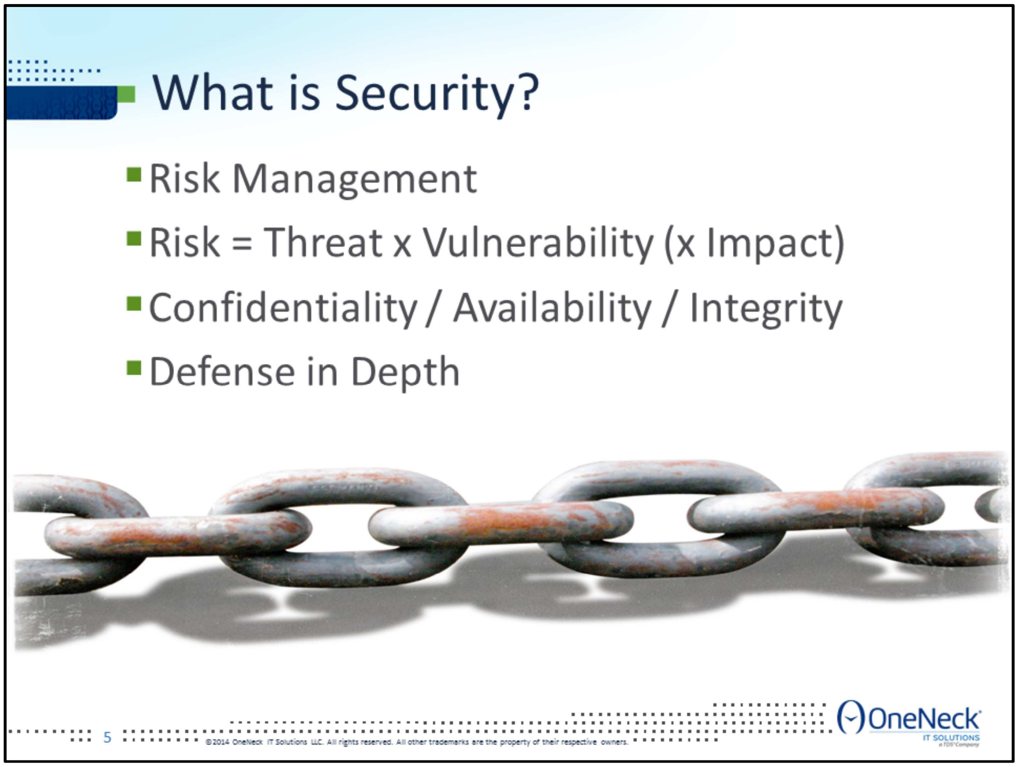


Forrester: “Security and the Cloud” (2)

“As cloud adoption moves to the mainstream and expands from tactical uses to strategic platforms, enterprises will need to address cloud security and compliance issues more holistically.

This will be especially true as organizations look to use cloud in cases where highly sensitive data is involved, where rigorous compliance requirements apply, or for business-critical applications.”

- Forrester Research, Inc. “Security And The Cloud,” 20 October 2010



What is Security?

- Risk Management
- Risk = Threat x Vulnerability (x Impact)
- Confidentiality / Availability / Integrity
- Defense in Depth

5

OneNeck
IT SOLUTIONS
a TDS Company

Security is all about Risk Management. Capturing lessons learned in the past and applying that learning to new and evolving situations.

The Forrester quote captures it nicely “address cloud security and compliance issues more holistically”
When we address cloud security, we must use the same disciplined approach that we would take to secure any other environment. This may sound self-evident, but the security issues that I encounter are often the result of missing the basic blocking and tackling of security. I want to take a moment to hit on these, because it will lay a solid foundation as we work through the rest of today’s agenda. For some, this may be new and for others you will have heard it all before. But consider this: The martial arts masters spend years perfecting their basic movements so that they can reflexively handle any new situation.

The classical definition of Risk is Threat x Vulnerability. A threat agent must exercise an existing vulnerability for a specific risk to be present. {Heartbleed}
The worst kind of vulnerability are the ones that present the highest adverse impact to the business, so risks are mitigated in risk priority order.

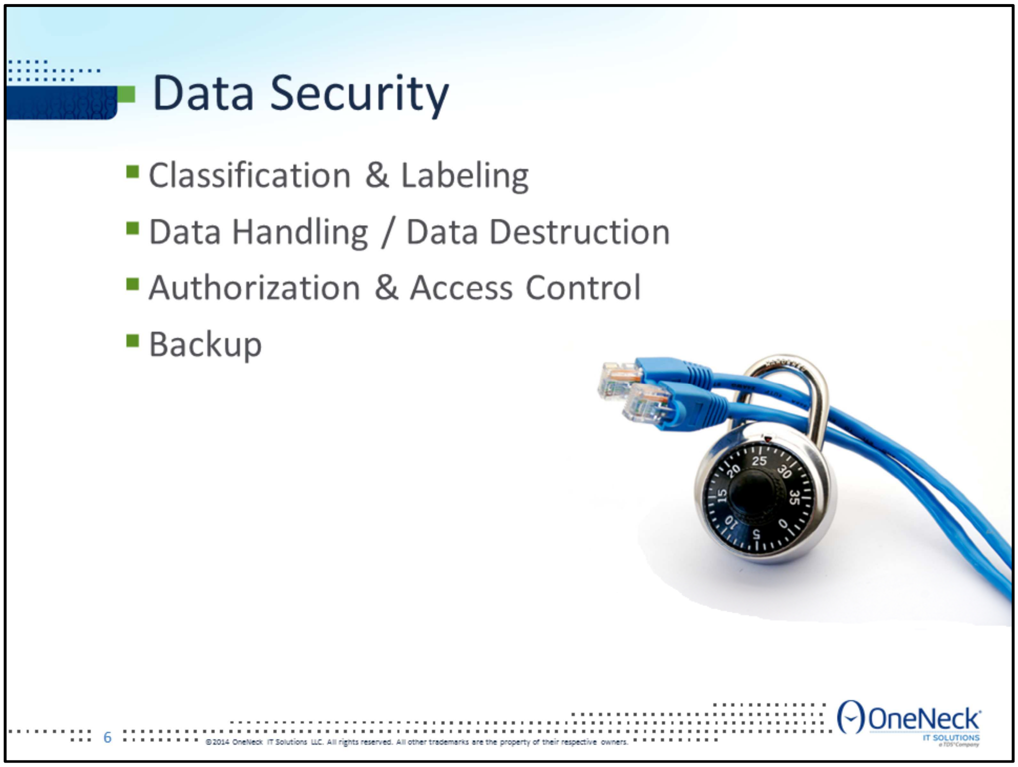
What about the vulnerabilities that you don’t know about? On-going vulnerability assessment. Staying abreast of Industry consensus and the latest research.

The single biggest mistake that I see when implementing security controls is failing to consider what specific risk that the security control is designed to mitigate. For Example:

Having your web application encrypt data does not protect it from attacks that come through the application, such as SQL Injection. When we forget that a given control will mitigate specific risks then compliance becomes a "to-do" checklist rather than a requirements framework for your information security management system.

REMEMBER: Attackers target your information assets to either abscond the value for themselves or to make those assets less valuable to you. These are attacks against confidentiality, availability, or integrity. Hence, our security controls must mitigate against specific risks to C-I-A. We must also use a layered approach and have overlapping controls for Defense-in-Depth. I wrote a two part blog posting on this where I used the counter example of failing to use host-based firewalls because the server is behind a network firewall.

Remember, when it comes to security, there is no magic bullet! You cannot buy a security product, whether it is a Web-Application Firewall or Intrusion Detection System or what have you and expect to plug it in like a toaster and think you are secure. It will need constant care and feeding…like a bonsai tree.



Data Security

- Classification & Labeling
- Data Handling / Data Destruction
- Authorization & Access Control
- Backup

OneNeck
IT SOLUTIONS
a TDS Company

Another often overlooked part of an information security management system is classifying your information assets. Examples of this include electronic protected health information (HIPAA) and Cardholder data (PCI-DSS) as well as proprietary and trade secret information as opposed to public information. Select a few classifications based on the rank order of the adverse impact if the information was improperly disclosed.

Limit the number of systems that transmit and store your most sensitive information. Mark Twain (The Legend of Puddin Head Wilson) “Put all of your eggs in one basket and watch that basket closely.”

Chances are that your organization already has this in place. But this “blocking and tackling” of security also applies in the cloud. The systems that contain your sensitive data should not be directly exposed to the Internet, but should be on dedicated servers and separate network segments—accessed only through defined interfaces. More on that later.

Next comes one of the biggest concerns of cloud security: Data Handling and Data Destruction.

Depending on the nature of your sensitive data, there are either regulatory or industry best practices that dictate how the information should be handled. Generally these are codified in policy that dictates what types of systems can process the data and how it must be encrypted and destroyed when no longer needed. Make sure that your cloud vendor understands your data handling requirements and can meet them. Invest the time and

discuss this with your cloud vendor.

Think for a moment: What makes your information valuable? That the right people can access it when needed and that the wrong people cannot. This creates and preserves competitive advantage. Authorization is the process used to define the set of “right people” and access control is the means of limiting access. The scary thing about the cloud, is now you have a vendor that can access your sensitive information. Nonetheless, a good vendor’s authorization process can dovetail with yours and still leave you in control. Make sure that you discuss authorization and access control with your cloud providers. Can they provide a record of exactly who has accessed your systems and when?

No discussion about access control would be complete without mentioning Multi-Factor Authentication: What you know (password), what you have (token), who you are (biometric), and where you are (location). There are multiple Vendor solutions out there but don’t buy a “product,” implement a solution.

Control Types

Categories

- Administrative
- Technical

Formal Risk Acceptance

Control Types

- Deterrent
- Preventive
- Detective
- Forensic

7

Administrative Controls – These are your policies and procedures. How do policies and procedures make you more secure? They document management's expectation about how security is to be implemented and create the standard to be audited against.

Preventive Controls—This is technology that is intended to prevent a risk from being realized. Examples include firewalls on the network as well as locked doors and cages for physical security.

Detective Controls –This is technology that indicates that an attack is in progress because the attacker has made it past the preventive controls designed to keep him out. Examples of this are Intrusion Detection Systems and physical security alarms. Detective controls require a human to intervene and generally speaking the earlier the intervention the less damage.

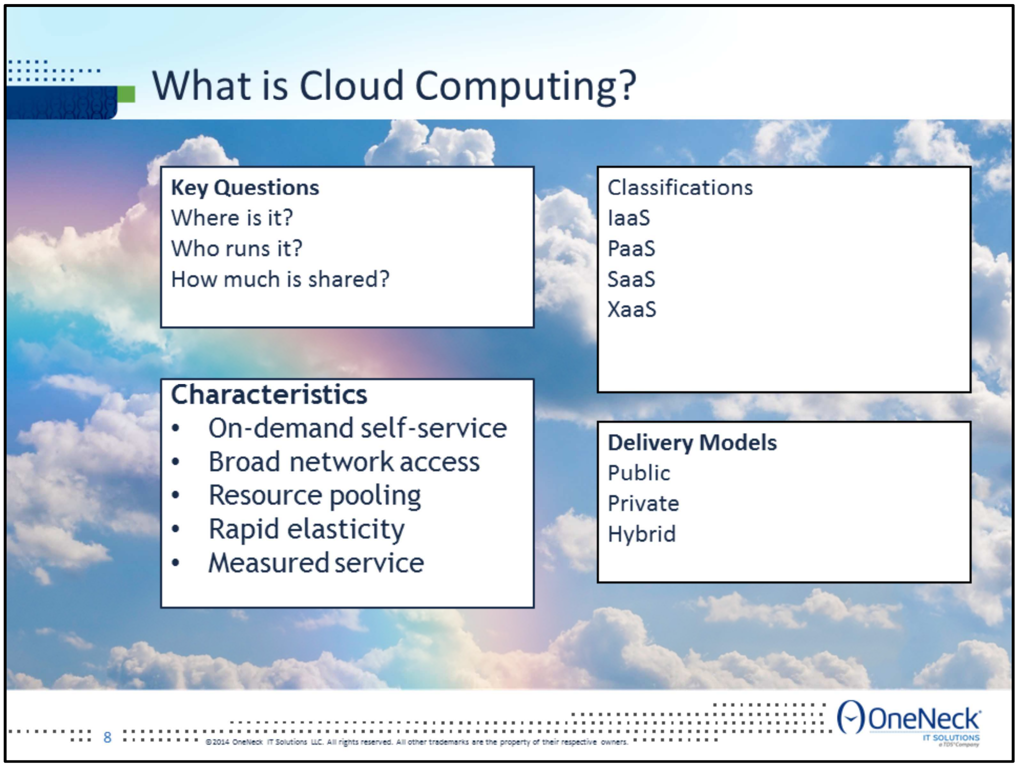
In security, we have a saying "Prevention is good, but detection is a must!" Unfortunately the FBI is still finding too many instances of unknown breaches when investigating seemingly unrelated cases in other environments.

Design your detective controls to augment and overlap your preventive controls. Just like you would use a motion detector behind a locked door, use rules in your Intrusion Detection System to verify that your Firewall Rules are still working effectively. This is DiD (Believe me, this is not always done)

I am spending time here on security essentials, but these apply equally well in the cloud.

How do you know which controls to implement? That is driven by your Risk Assessment. You implement them in risk priority order.

There is one last point to this slide. You will never be able to mitigate every single risk. Security is about reducing risk to an acceptable level. A risk acceptance process helps management balance the impact of loss with the financial costs of mitigating it. Certain risks that have a lower impact may be tolerated. Risk Acceptance formalizes that process and makes sure that the right level of authority accepts the risk.



What is Cloud Computing?

Key Questions
Where is it?
Who runs it?
How much is shared?

Classifications
IaaS
PaaS
SaaS
XaaS

Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Delivery Models
Public
Private
Hybrid

8

Cloud – The very term conjures up images of things that are big, fluffy and lacking substance

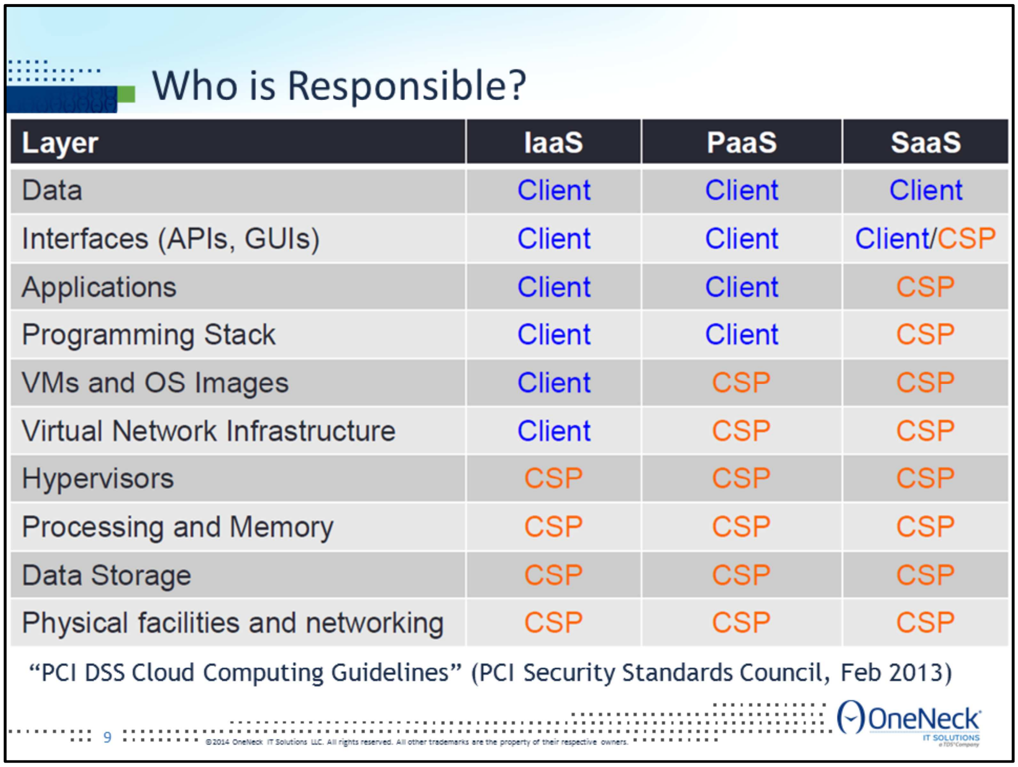
In his 2005 book, "The World is Flat," Thomas Friedman provides example after example to show that "everything which can be outsourced, will be outsourced"
That is how I see Cloud computing.

I can get as much compute, memory, or storage as I need when I need it – and pay for only what I consume

Compute/Memory/Storage →IaaS
PaaS: On top of that you can add Platforms, such as Operating Systems, Databases, and Applications such as Microsoft Dynamics
SaaS: Software as a Service – SalesForce.com or Office365
"X" as a Service– Storage / DR / Security / etc… (Anything that can be outsourced / Made into a utility)

Public Cloud – Resources for a customer are pulled from a public pool of resources and allocated to the customer for the duration of their subscription
Private Cloud— Dedicated resources are operated for a single customer organization. Some may even use the term "Private Cloud" to refer to a company's in-house virtualization infrastructure
Hybrid Cloud – Various combinations of public and private cloud combinations

Why are the questions important?
--Make sure that you and your vendor assign the same meaning to the Industry Buzz Words



Who is Responsible?

Layer	IaaS	PaaS	SaaS
Data	Client	Client	Client
Interfaces (APIs, GUIs)	Client	Client	Client/CSP
Applications	Client	Client	CSP
Programming Stack	Client	Client	CSP
VMs and OS Images	Client	CSP	CSP
Virtual Network Infrastructure	Client	CSP	CSP
Hypervisors	CSP	CSP	CSP
Processing and Memory	CSP	CSP	CSP
Data Storage	CSP	CSP	CSP
Physical facilities and networking	CSP	CSP	CSP

“PCI DSS Cloud Computing Guidelines” (PCI Security Standards Council, Feb 2013)

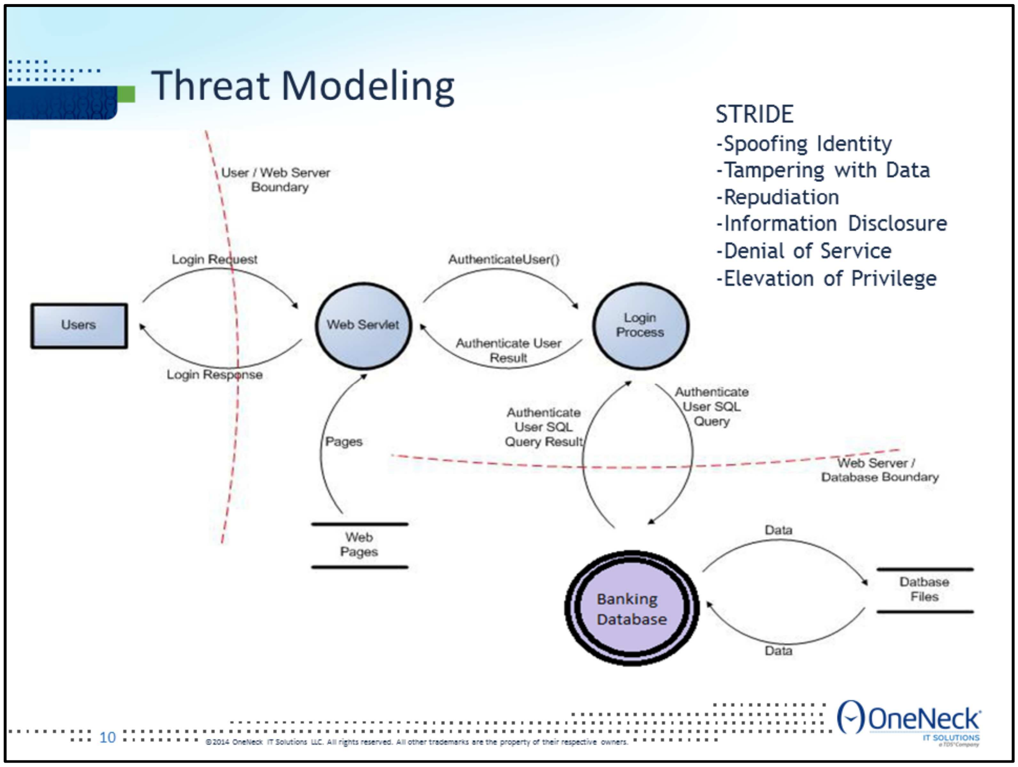
9

OneNeck IT SOLUTIONS a TDS Company

Do the security practices change as you move from IaaS → PaaS → SaaS? Possibly because the ownership of the responsibility changes.
The classification scheme is helpful because the responsibility ownership changes with the scope of the services provided.

At OneNeck, we are starting to map this out for the different compliance frameworks, like PCI and HIPAA. Who owns which specific control—based on the set of services that we are delivering to the customer. It is in everyone’s best interests to have clear support boundaries.

Credit for this slide to Michael Pomraning, @ Trustware



Threat Modeling

STRIDE
-Spoofing Identity
-Tampering with Data
-Repudiation
-Information Disclosure
-Denial of Service
-Elevation of Privilege

10

©2014 OneNeck IT Solutions LLC. All rights reserved. All other trademarks are the property of their respective owners.

OneNeck IT SOLUTIONS

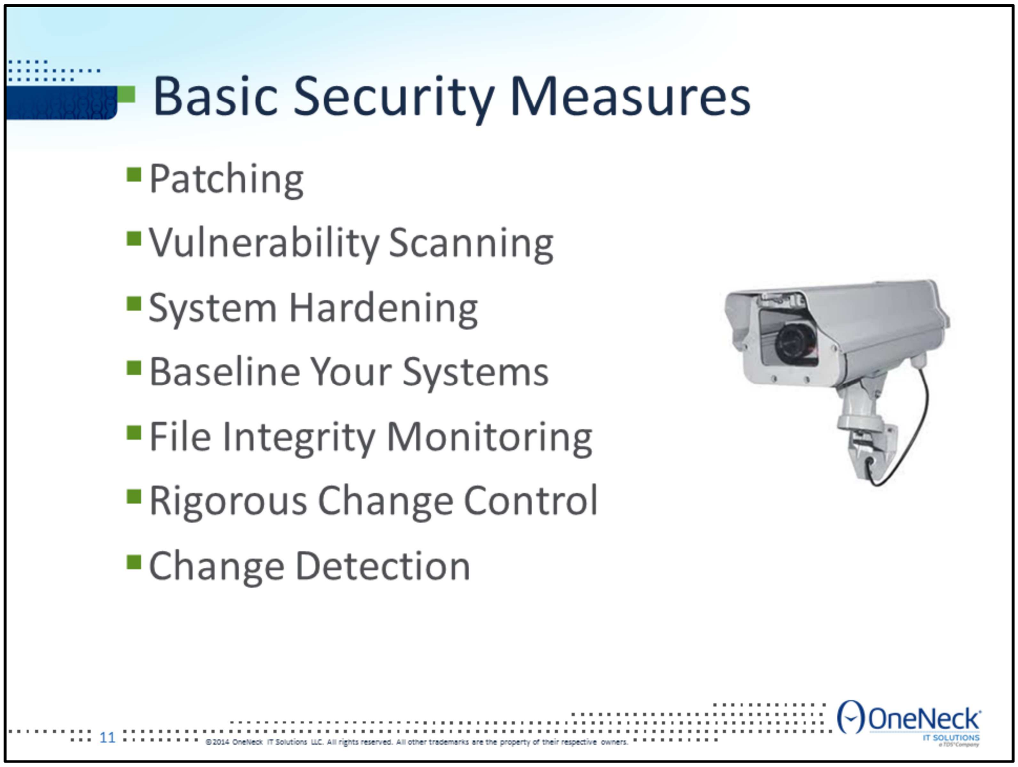
What I like about the way that the cloud has evolved is that everything can be viewed as an interaction between a supplier and a customer and it is at the interface that the magic happens. Take a banking website for example. The sensitive information in the web application is for certain customers only. Those customers who have entered into a specific agreement with the bank defining the relationship. The customer must authenticate his or herself to the web application before the application will honor any requests for information.

But let’s delve deeper into this example. The customer is actually interacting with a web-front end, that is in all likelihood load-balancing and proxying requests to a cluster of web application servers that then are making calls to various databases, or better yet, other web services.

The web application can be modeled as a collection of processes (circles on the diagram) that are either suppliers (producers) or customers (consumers) of information or both producers and consumers. Note that the processes can reside on the same or different servers and the servers may exist on other networks or may even be in other environments and accessed across the network.

The security magic happens at the interface between the different processes. Each interface can have a service level agreement (SLA) that defines exactly how the producer and consumer will share information. Furthermore, where there exists different levels of trust between the processes, that is called a trust gradient. This is shown by a dotted line in the diagram. The processes that interact across a trust gradient should mutually authenticate and may also require encryption.

This diagram is called a threat model. This allows the architects to determine the most likely areas to be attacked and to ensure that the threat is mitigated



Basic Security Measures

- Patching
- Vulnerability Scanning
- System Hardening
- Baseline Your Systems
- File Integrity Monitoring
- Rigorous Change Control
- Change Detection

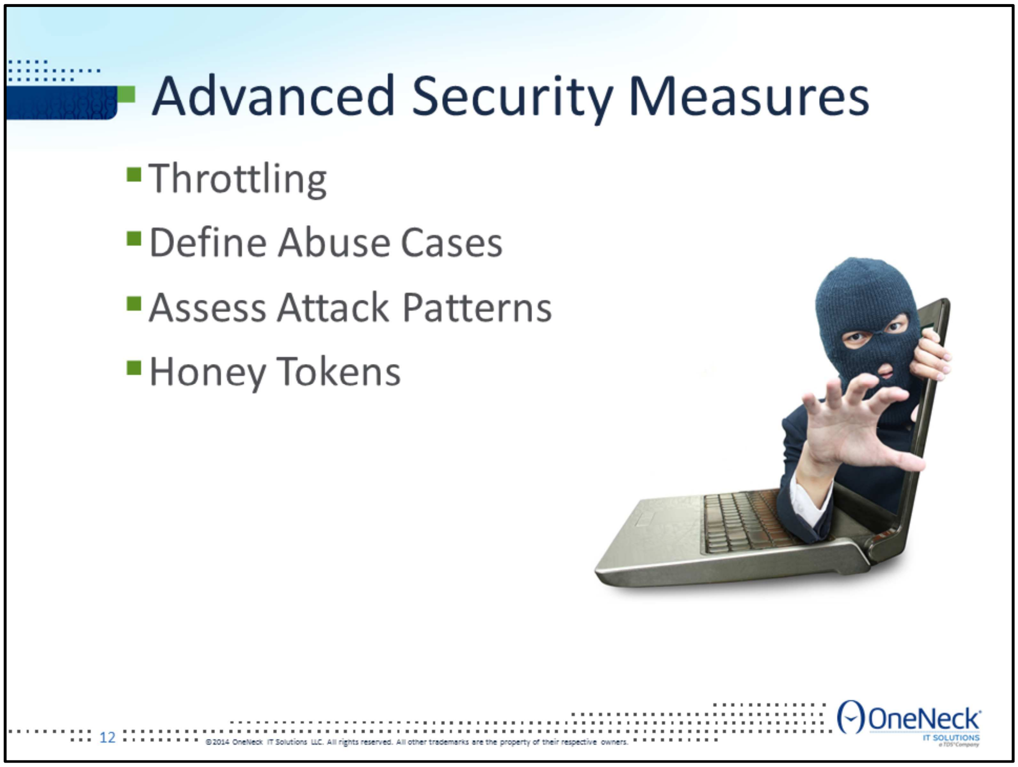
OneNeck
IT SOLUTIONS
a TDS® Company

There is an old saying "an ounce of prevention is worth a pound of cure" Many of the following recommendations fall into that category

Harden your systems in the cloud. If the vendor is responsible for that, make sure that you understand how and why they harden the systems the way that they do. Make sure it makes sense. The security magic happens at the interface. As the customer take the time to ensure that this is all spelled out.

Baseline Your Systems. Remember the ancient Greek maxim "Know thyself." How about "Know thy Systems"
If you don't know the state of your systems, how can you tell if there has been an unauthorized change?

Enforce change control. Every change tied to a ticket. All significant changes approved by a change control board. Use your detective security controls to detect unauthorized change and treat that unauthorized change as a security incident. This is what the Visible Ops handbook calls "electrifying the fence"



Advanced Security Measures

- Throttling
- Define Abuse Cases
- Assess Attack Patterns
- Honey Tokens

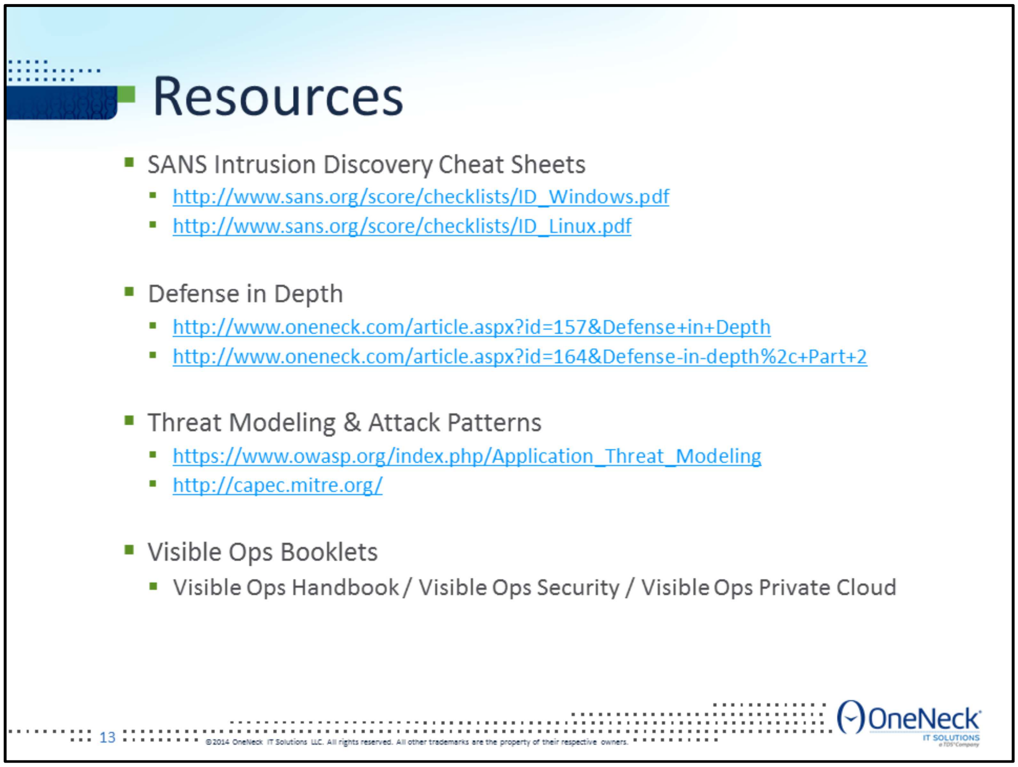
OneNeck
IT SOLUTIONS
a TDS Company

Periodically review and update your abuse cases. This is when you document the ways that someone will try to misuse your system. Excellent training tool.

Classify attack patterns. This allows you to prepare standard responses to the most frequent attacks. Can you tell when someone is attempting SQL injection? What about Cross-Site Scripting? A slow Loris attack? SSH Brute force? An ounce of prevention, worth a pound of cure. Mitre: Common Attack Pattern Enumeration & Classification

Remember, “prevention is good but detection is a must.” Does your service need to return the entire list of user names (for example) or can it be designed to return only one at a time with no impact on normal operations? This is an example of throttling. Throttling means that it will take longer for a successful attacker to enumerate the entire record set AND that it will create many more log entries (making it easier to detect). Throttling Use Case: Credit Card Processor stores your cardholder data for you (so you don’t have to) and provides a web service API that returns only data on a single card at a time. Security is about risk management. Its much better to have a few credit cards breached than tens of thousands.

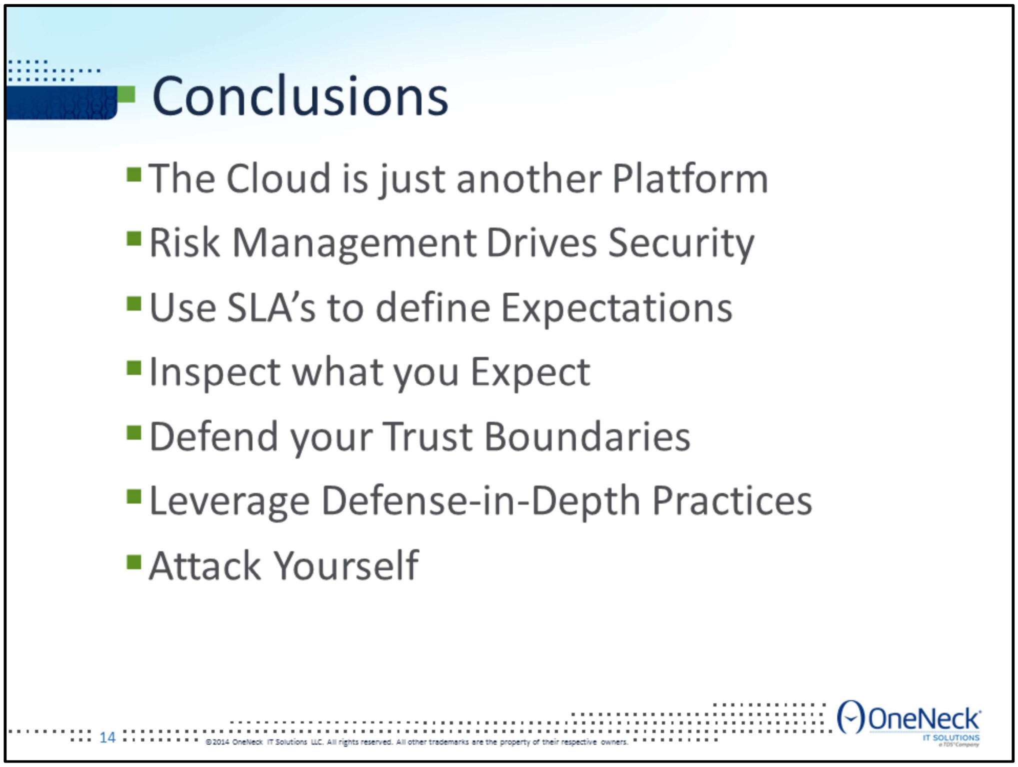
In healthcare, it is common to create fake patient records when a celebrity is admitted. Anyone who accesses these fake records gets fired, because there is not a legitimate business need to access them. You can do this too with records, and even whole database tables, or files in the file system. Just configure alerts. These are detective controls, but think overlapping layers to ensure detection and to detect earlier.



Resources

- SANS Intrusion Discovery Cheat Sheets
  - http://www.sans.org/score/checklists/ID_Windows.pdf
  - http://www.sans.org/score/checklists/ID_Linux.pdf
- Defense in Depth
  - http://www.oneneck.com/article.aspx?id=157&Defense+in+Depth
  - http://www.oneneck.com/article.aspx?id=164&Defense-in-depth%2c+Part+2
- Threat Modeling & Attack Patterns
  - https://www.owasp.org/index.php/Application_Threat_Modeling
  - http://capec.mitre.org/
- Visible Ops Booklets
  - Visible Ops Handbook / Visible Ops Security / Visible Ops Private Cloud

Mitre: Common Attack Pattern Enumeration & Classification



Conclusions

- The Cloud is just another Platform
- Risk Management Drives Security
- Use SLA's to define Expectations
- Inspect what you Expect
- Defend your Trust Boundaries
- Leverage Defense-in-Depth Practices
- Attack Yourself

14

OneNeck IT SOLUTIONS a TDS Company

I wanted to lay a solid foundation by showing how the risk can be managed with solid security practices like any other platform.

Remember: Risk drives the train. Do everything in rank order of risk

Cloud Computing actually encourages SLA's. Use these to define exactly what is expected at every interface at all appropriate levels of abstraction

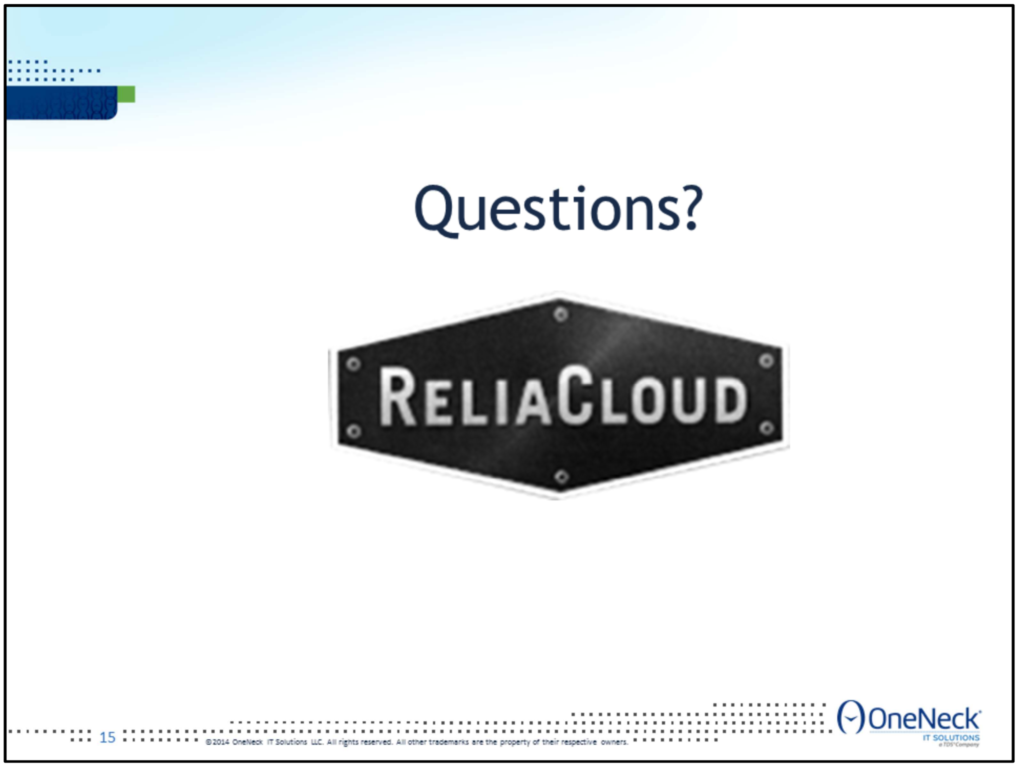
Inspect what you expect. Remember YOUR customers are holding YOU accountable for the safekeeping of your data (not YOUR VENDORS)

Define trust boundaries that you can defend. Put all your eggs in one basket and watch that basket closely. To expand the metaphor, use the smallest basket possible. Shrink the scope of your most sensitive networks and systems.

Use Defense-in-Depth. Remember there is no magic bullet. Expect systems and controls to fail. Bad things happen to good companies. Its all in how you prepare and how you respond.

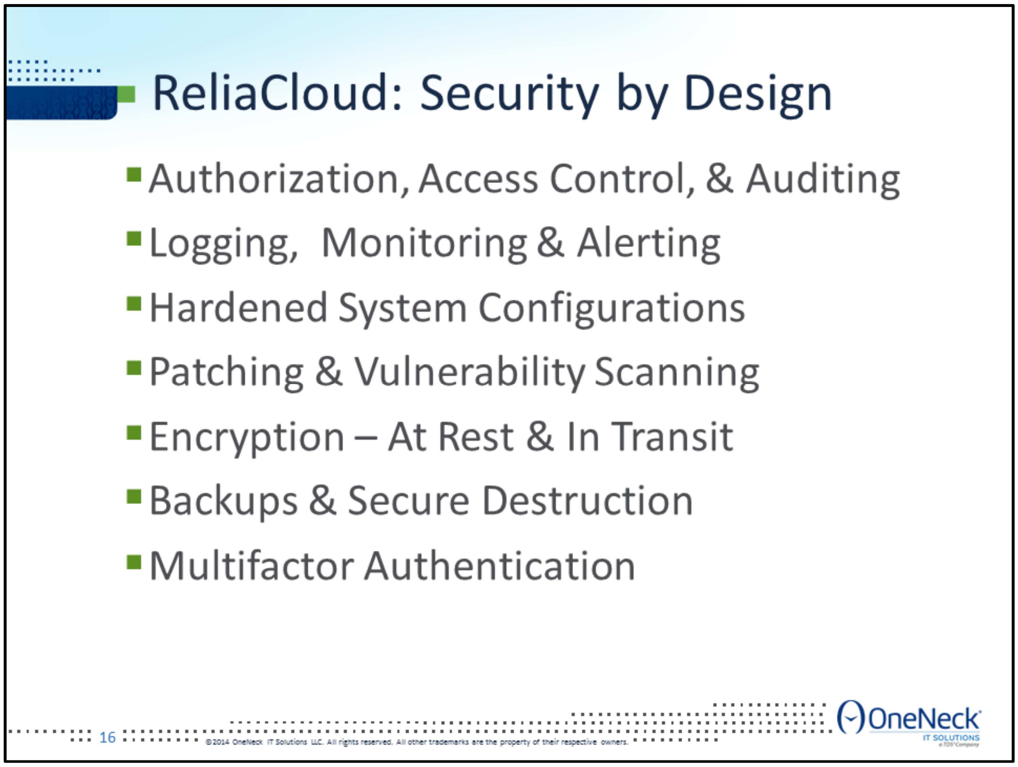
Hack yourself and hire trusted third parties to pentest you. It will force you to stay sharp and open your eyes to weaknesses you cannot see.

Lastly, remember that "perfect is the enemy of good" Security is about balancing priorities and enabling business—not stifling it.



Questions?

RELIACLOUD



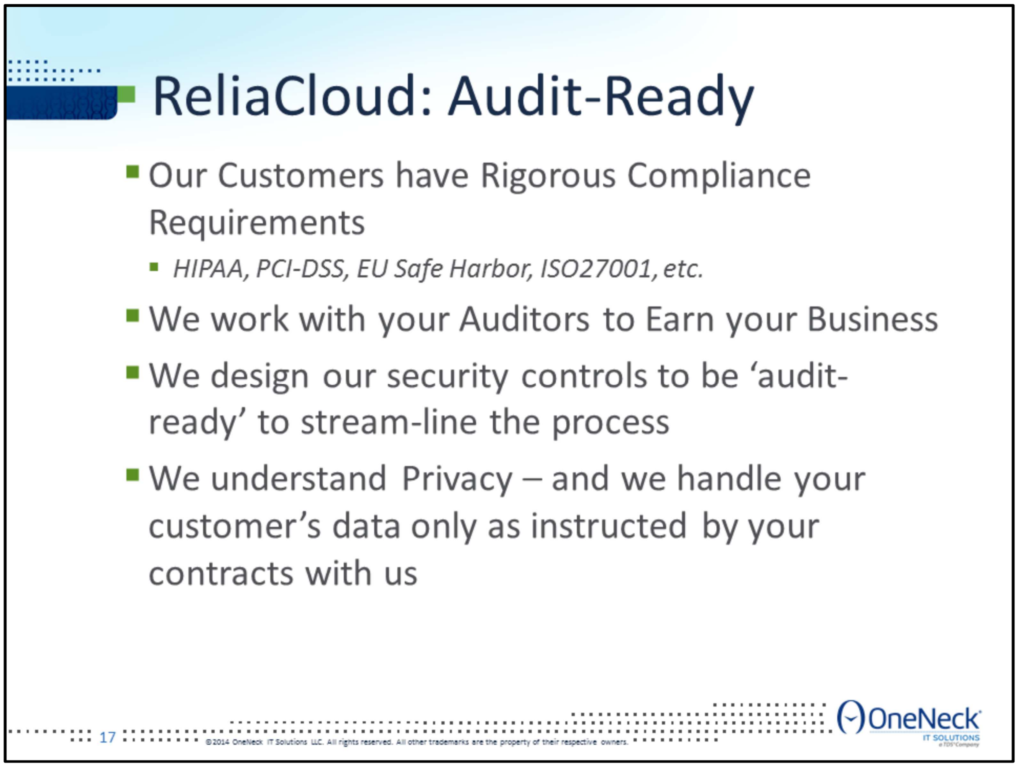
ReliaCloud: Security by Design

- Authorization, Access Control, & Auditing
- Logging, Monitoring & Alerting
- Hardened System Configurations
- Patching & Vulnerability Scanning
- Encryption – At Rest & In Transit
- Backups & Secure Destruction
- Multifactor Authentication

ReliaCloud was designed with your demanding security needs in mind.

Security is all about managing Risk – and attention to the tedious details

Our technical security controls are designed to industry consensus best security practices by engineers with multiple security and vendor certifications



ReliaCloud: Audit-Ready

- Our Customers have Rigorous Compliance Requirements
  - *HIPAA, PCI-DSS, EU Safe Harbor, ISO27001, etc.*
- We work with your Auditors to Earn your Business
- We design our security controls to be 'audit-ready' to stream-line the process
- We understand Privacy – and we handle your customer's data only as instructed by your contracts with us

17

Face it – No one really enjoys being audited, but it gives us a chance to show that we understand your needs.

We know what your auditors expects – and we continuously work to streamline the audit response process, whether this is working with independent consultants, industry certifications such as the SSAE 16, or improving our internal processes based on ITIL, SANS, and the American Institute of CPA's (AICPA)

To simplify compliance with EU Safe Harbor and HIPAA – we process your customer's sensitive data only as needed to provide the ReliaCloud services that you subscribe to as governed by our written agreements with you.

We understand security, privacy and compliance and stand ready to earn your trust as you transition to the secure cloud – ReliaCloud