

the adventures of alice & bob



From the War Room to the Board Room

从IT控制室到董事会会议室

Cloud Computing Risk Management

云计算风险管理

Challenges & Solutions

挑战与解决方案

Speaker 演讲人 : Lee Zeichner

Job Title 职位 : President 总裁

Company Name 公司名 : Zeichner Risk Analytics, LLC

OVERVIEW 总览



1. Our Challenge 我们的挑战
2. My Background & Lessons Learned 我的背景和经验所学
3. Cloud Environment 云环境
 - A. Public/Private sectors need cloud– but risks too high
公共或私人领域都需要云计算—但是风险太大
 - B. Sophisticated risk frameworks are essential, but missing
高级的风险框架是必须的，但是现在还不存在
 - C. Security requires special attention
安全需要特别关注
4. Case Studies 案例研究
5. Future Roadmap 未来工作蓝图
6. Conclusions 结论

OUR CHALLENGE 我们的挑战



Challenge

Lessons Learned

Cloud
Environment

Case Studies

Roadmap

Conclusions

Global businesses and governments will not deploy Cloud Computing solutions unless our community can develop sophisticated frameworks for managing cloud computing risk.

全球的商业和政府将不会部署云计算解决方案，除非我们的社会能开发出高级的云计算风险管理框架。

OUR CHALLENGE 我们的挑战



全球的商业和政府将不会部署云计算解决方案，除非我们的社会能开发出高级的云计算风险管理框架。这包括：

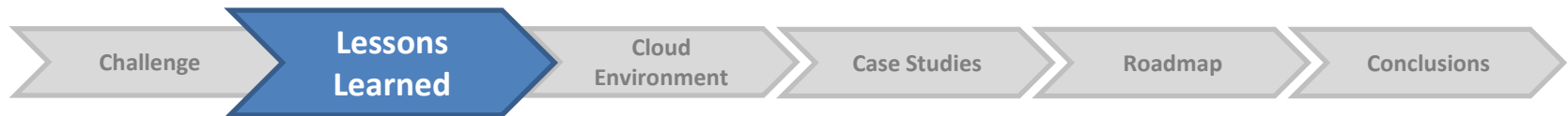
- Risk Identification 风险识别
- Risk Assessment 风险评估
- Risk Management 风险管理
- Risk Mitigation 风险消减
- Risk Transfer 风险转移

MY LESSONS LEARNED

RSACONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

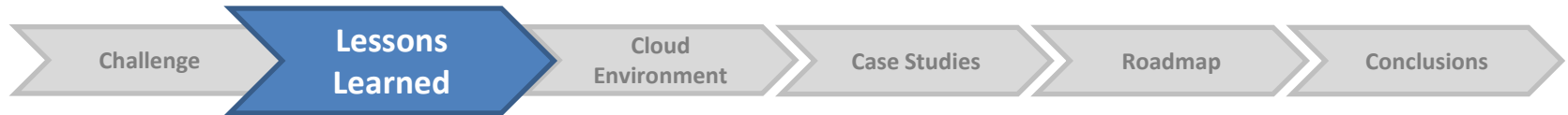
我的经验所学

BACKGROUND 背景



- Education 教育背景
- Risk management, IT audit & security expertise
风险管理和网络安全专长, 审计师
- Author –Cybersecurity & Corporate Liability
我是《网络安全和企业责任》的作者
- Security Counsel, Business Roundtable
商业圆桌会议的安全律师顾问
- Visiting Scientist, Software Engineering Institute
卡内基梅隆大学软件工程学院的访问科学家

我的经验所学

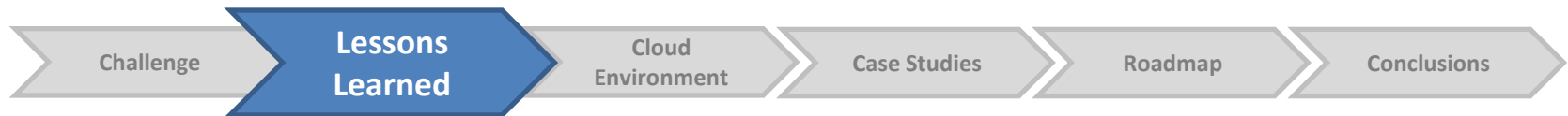


Lessons Learned #1 经验所学1

- Cloud computing lowers costs, offers new ways to beat business competition, and helps to implement innovative business strategies – BUT, even with these benefits, business and government might not ultimately adopt cloud computing.

计算可以降低成本，提供新的方法赢得商业竞争，帮助实施新的商业战略。但是，尽管云有这些好处，企业和政府最终可能还是不会采用云计算。

我的经验所学

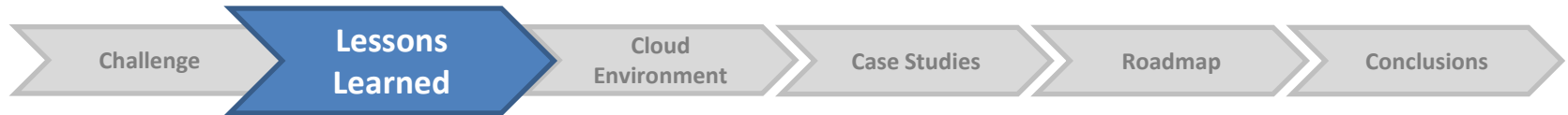


Lessons Learned #2 经验所学2

- Existing cloud computing norms of behavior, best practices, standards, and frameworks are not even remotely sufficient to manage risks of adoption.

现行的云计算规范，最佳操作，标准和风险框架都远远不足以控制管理云计算采用的风险。

我的经验所学



Lessons Learned #3 经验所学3

- Business and government leaders are especially focused on security -- and IT security is potentially a show stopper.

企业和政府领导人特别注重安全问题——而IT安全是其中的潜在杀手。

PUBLIC AND PRIVATE SECTORS NEED CLOUD – BUT RISKS TOO HIGH

公共和私人领域都需要云计算—但是风险太大



Issue #1: Business and government want cloud solutions, need cloud solutions, have funds to buy cloud solutions - but might not ultimately adopt cloud computing.

问题1: 商业和政府都想要云计算解决方案，需要云计算解决方案，并且有资金购买云计算解决方案—但是他们最终可能不会采用云计算。

PUBLIC AND PRIVATE SECTORS NEED CLOUD – BUT RISKS TOO HIGH

公共和私人领域都需要云计算—但是风险太大



- **Business concerns might outweigh cloud benefits** 商业顾虑可能会超出云计算的益处 -可能会给整个公司带来风险
- **Risks not fully understood** -计算比较新，所以我们还没有完全了解它的风险
- **Technical problems overwhelming** 不堪重负的技术问题
- **Operational practices rarely covered** 运行最佳操作很少被执行
- **Legal issues not resolved** 法律问题没有解决
- **Very few metrics** -指标体系和绩效标准还没有完全开发出来
- **No risk transfer – insurance** 没有完善的风险转移方式 (保险)
- **Risks are asymmetric** 风险的不对称性

Corporate governance practices weak 企业治理操作薄弱

PUBLIC AND PRIVATE SECTORS NEED CLOUD – BUT RISKS TOO HIGH

公共和私人领域都需要云计算—但是风险太大



Solution: Recognize serious gap -- Business and Government leaders do not yet have ways to identify and manage risks... for now, risks outweigh profound benefits.

解决办法：认识到严重的差距——商业和政府领导们还没有方法识别和管理风险。

现在，风险大于深远的利益。

CLOUD ENVIRONMENT 云环境

RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

OUR COMMUNITY MUST DELIVER MORE SOPHISTICATED RISK FRAMEWORKS

我们的社会必须提供更复杂的风险框架



Issue #2: Existing cloud frameworks insufficient.

问题2：现有云计算框架的不足

CLOUD ENVIRONMENT 云环境

RSACONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

OUR COMMUNITY MUST DELIVER MORE SOPHISTICATED RISK FRAMEWORKS

我们的社会必须提供更复杂的风险框架



- Sophisticated risk frameworks essential, but missing 高级的风险框架是必须的—但是现在还不存在 - 企业执行官们缺少高级风险框架
 - Is the guidance prepared by our community sufficient? 那我们业内提供的云计算指南足够吗?

CLOUD ENVIRONMENT 云环境

RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

OUR COMMUNITY MUST DELIVER MORE SOPHISTICATED RISK FRAMEWORKS

我们的社会必须提供更复杂的风险框架



- **Good News - Risk management guidance 好消息-风险管理材料:**
 - Provides general support 能很好地为企业和政府提供笼统的，不具体的指导
 - Spots issues, get leaders to think about strategic risks 使人发现关键问题，以及让领导们开始考虑战略风险
 - Helps “raise the bar” on hygiene 很好地解决简单的风险问题

CLOUD ENVIRONMENT 云环境

RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

OUR COMMUNITY MUST DELIVER MORE SOPHISTICATED RISK FRAMEWORKS

我们的社会必须提供更复杂的风险框架



- **Bad News - Risk management guidance 坏消息- 风险管理材料:**
 - **Not sufficient** 完全不足以管理所有的风险，让决策者们投资云计算解决方案
 - **Does not address business impediments** 商业方面的障碍与关注
 - **Does not help lack of corporate governance guidance** 有效公司治理的缺乏
 - **Does not solve legal concerns** 风险管理材料没有完全解决法律关注

CLOUD ENVIRONMENT 云环境

RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

OUR COMMUNITY MUST DELIVER MORE SOPHISTICATED RISK FRAMEWORKS

我们的社会必须提供更复杂的风险框架



- We have frameworks – great achievement 事实上，云计算的很多规范，最佳操作，标准和框架都展现了巨大的成就
 - But, too complicated! 现行的标准和云框架太复杂，以致于多数的组织很难理解和采用
 - Too many! 问题是要考虑的风险和云计算途径实在太多。
- Need new approach and strategy 我非常相信我们应该采用不同的途径和战略

CLOUD ENVIRONMENT 云环境

RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

OUR COMMUNITY MUST DELIVER MORE SOPHISTICATED RISK FRAMEWORKS

我们的社会必须提供更复杂的风险框架



Solution: Overhaul how we design risk management practices for cloud computing. Can't just add more standards... need to come up with an approach for managing complex security relationships.

解决方案：革新我们对云计算风险管理操作的设计。我们不能只增加更多的标准；相反的，我们需要找到一个管理复杂安全关系的途径。

CLOUD ENVIRONMENT 云环境

RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

CLOUD SECURITY VULNERABILITIES REQUIRE SPECIAL ATTENTION

云安全漏洞需要特别关注



Issue #3: Security requires special attention

问题3：安全需要特别关注

CLOUD ENVIRONMENT 云环境

RSACONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

CLOUD SECURITY VULNERABILITIES REQUIRE SPECIAL ATTENTION

云安全漏洞需要特别关注



- Current Formula: Security risks present too many challenges

$$R = \Sigma[T] * [V] * [C]$$

$$\text{风险} = \Sigma[\text{威胁}] * [\text{漏洞}] * [\text{后果}]$$

CLOUD SECURITY REQUIRES SPECIAL ATTENTION

云安全需要特别关注



- New Formula - EXCELLENCE in five areas

新公式 — 卓越的五个方面

A. IT Engineering IT工程

B. Security Assessment 安全评估

C. Audit 审计

D. Corporate Governance 企业治理

E. International Cooperation 国际合作

CLOUD SECURITY REQUIRES SPECIAL ATTENTION

云安全需要特别关注



- Excellence in IT Engineering

卓越的IT工程

- Companies must dramatically improve cloud engineering
公司必须大程度改善云工程
- Build security into the products and services
构建产品和服务的安全
- Improve software development 改善软件发展
- Manage vendors 管理供应商

Need new wave of security engineering!

需要新一波的安全工程！

CLOUD SECURITY REQUIRES SPECIAL ATTENTION

云安全需要特别关注



- **Excellence in Security Assessment**
卓越的安全评估
 - Companies must dramatically improve how we assess security risk
公司必须大程度改善我们评估安全风险的方式
 - Need new companies to develop sophisticated risk assessments
需要新公司来发展高级的风险评估
 - Focus should be on vulnerabilities and mitigation
应该把重点放在风险漏洞和消减上
 - Must be scalable and easily integrated
 - 必须在规模上可以扩展以及容易整合

Need new generation of technical expertise in IT security!

需要IT安全上新一代的技术专家！

CLOUD SECURITY REQUIRES SPECIAL ATTENTION

云安全需要特别关注



- Excellence in Security Audit

- 卓越的安全审计

- Companies must dramatically improve how we audit for security and compliance
公司必须大程度改善我们在安全和合规上的审计方式
 - Accounting firms have not successfully developed a business model for their clients
会计师事务所还没有为客户成功开发出商业模式
 - Standards are completely insufficient
标准完全不足

Need new generation of audit professionals who are fluent in security!
需要新一代了解安全的审计专业人员！

CLOUD SECURITY REQUIRES SPECIAL ATTENTION

云安全需要特别关注



- Excellence in Corporate Governance

卓越的企业治理

- Companies must improve how they “govern” IT investments and deployments
- 公司必须改善他们治理IT投资和发展的方式
- If CEOs and Boards understand cloud security risks, then shareholders & customers will benefit
- 如果首席执行官们和董事会了解云安全风险，那么股东和客户将会受益
- Corporate leaders must set “the tone at the top.”
- 企业领导们必须从上层设立企业道德文化

Need new generation of corporate leaders who understand IT security!

需要新一代了解IT安全的企业领导人！

CLOUD SECURITY REQUIRES SPECIAL ATTENTION

云安全需要特别关注



- Excellence in International Cooperation

卓越的国际合作

- We must develop a single, global security agenda
我们必须开发一个单一的全球安全日程
- We must NOT develop separate approaches for IT security
我们必须不能有不同IT安全管理途径

Need new generation of diplomats who promote IT security!
需要新一代促进IT安全的外交官！

CASE STUDIES 案例研究



- Case Study #1 – Global Fortune 500 company
案例1—全球500强公司
- Case Study #2 – Small-to-medium company
案例2—中小型企业
- Case Study #3 – Provincial government entity
案例3—省级政府

FUTURE ROADMAP

未来工作蓝图



- **Cloud adoption demands focused action:**
云计算的采用需要有针对的行动:
 - **Achieve excellence for cloud technologies**
云计算技术达到极好的水平
 - **Clarify business needs and benefits – Not only IT**
澄清业务需求和收益—不仅仅是IT
 - **Increase Cloud literacy for corporate decision makers**
增加企业决策者的云计算知识
 - **Overhaul cloud risk management frameworks – science of risk management must be improved**
革新云风险管理框架—风险管理科学必须有所改善
 - **Develop more sophisticated security frameworks**
开发更高级的安全管理框架

FUTURE ROADMAP

未来工作蓝图

RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING



US & China Cooperative Approaches?

中美合作途径？

CONCLUSIONS 结论



Global businesses and governments will not deploy Cloud Computing solutions unless our community can develop sophisticated frameworks for managing cloud computing risk.

全球的商业和政府将不会部署云计算解决方案，除非我们的社会能开发出高级的云计算风险管理框架。

Raise the Bar: Cloud risk and adoption must be more science than art....

提高标准：云计算风险及其采用必须更具科学化，而不是艺术化

CONTACT INFORMATION

联系方式

Lee Zeichner

lee@zra.com

+1 (703) 351-1101

