本人经历“6550”=本人服务过的6家国际化知名企业+5个研究生学位+写了50万页报告(积累15TB资料)



从产业维度看信息安全

—全球信息安全概况及汽车行业信息安全现状与展望

- 工作有价值
- 产业前景光明
- 对待风险，要时刻绷紧弦，莫说绝对不可能，宁可信其有，不可信其无

对于“他山之石”、国外经验，本着“学标杆、找差距、谋发展”的战略思维，对国外经验重点解读

北汽福田汽车 生产力研究专家、特级总师

任起龙

2016年5月12日

FOTON

非常感谢工业控制信息系统安全产业联盟秘书处的盛情邀请，来和大家交流！

祝大家身体健康，工作顺利，生活快乐，万事如意!

内容简介

《全球信息安全报告》研究方法

- **谁做的：***2015年全球信息安全调查报告，是由PwC公司和CEO、CIO、CSO杂志一起进行的。*
  The Global State of Information Security® Survey 2015 is a worldwide study by PwC, CIO, and CSO.

- **执行时间：***本调查是2014.3.27-2014.5.25之间，通过网络在线进行的；CIO和CSO杂志读者和PwC全球客户则是通过邮件进行的。*
  The 2015 survey was conducted online from March 27, 2014 to May 25, 2014; readers of *CIO, CSO, and clients of PwC* from around the globe were invited via e-mail to take the survey.

- **样本数量：***调查结果通过超过154个国家、超过**9700个**企业CEO、CFO、CIO、CISO、CSO、VP和IT及信息安全总监。*
  The results discussed in this report are based on the responses of more than 9,700 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security practices across more than 154 countries.

- **样本分区域分配**

Asia Pacific	North America	South America	Europe	Africa, Middle East
14%	35%	13%	34%	4%

《全球信息安全报告》内容概要

口报告共包括6部分：

1. Main report—信息安全主报告

2. Industrial products—工业领域信息安全

3. Financial Services—金融服务领域信息安全

4. Power & utilities —电力和公共服务领域信息安全

5. Healthcare payers and providers —医疗服务提供者和使用者信息安全

6. Retail and consumer —零售和消费领域信息安全

由于时间和篇幅限制，在这里，仅从**《全球信息安全报告》**中给大家从主报告、电力与公共服务领域信息安全的内容中，选择信息安全技术本身以外的一些内容分享大家。

如果这能对您有所脾益，我将感到万分欣慰！

信息安全风险—是现实的且严重的

Cyber risks: A severe and present danger

□信息安全是永久的商业风险 Cybersecurity is now a persistent business risk
□信息安全风险远超过设备本身And the risks go beyond devices

◆ 信息安全公司IOActive 出版了研究报告，**详细展示黑客如何控制某汽车ECU（电子控制单元），**并且提出了如何诊断这些攻击的策略。
Security firm IOActive has published research that demonstrates in detail how hackers can control the Electronic Control Units of specific automobiles and proposes mechanisms to detect attacks.

◆ 惠普公司评审了10类最常用的设备，结果发现70%设备包含致命病毒。
HP reviewed 10 of the most commonly used connected devices and found that **70%　contain serious vulnerabilities.**

◆ SEC宣布将检查信息安全系统，不遵守规则的证券交易部门将被处以高达78.9万美元的罚款。
the US　Securities and Exchange Commission recently announced that it plans to examine the cybersecurity preparedness of more than 50 registered broker-dealers and investment advisers. Organizations that do not comply with the act are subject to financial penalties of **up $788,995 (USD).**

信息安全服务业务迅速扩张—前景光明

信息安全服务的市场在快速扩张Cybersecurity services market is expanding

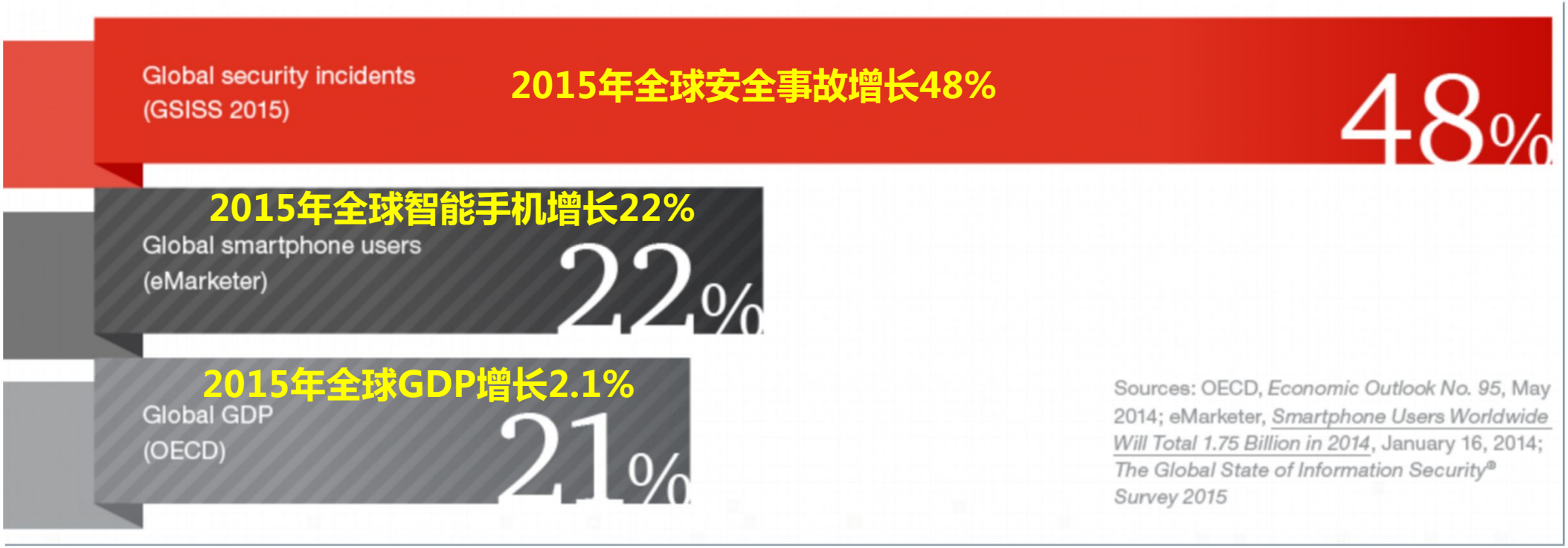
◆ 示例1： 网络安全提供商放火眼公司(FireEye)，在2013年IPO时的市值3.04亿美元，到三年后的今天，市值扩张到46亿美元。
Network security provider FireEye, after a $304 million initial public offering (IPO) in 2013, now has a market cap of approximately 4.6 billion US dollars.

◆ 示例2： 企业安全防火墙领导者PAN(Palo Alto Networks)网络安全提供商放火眼公司(FireEye)，在2012年IPO时的市值2.60亿美元，到四年后的今天，市值扩张到62亿美元。
Enterprise firewall specialist Palo Alto Networks raised $260 million in a 2012 IPO and now has a market cap of approximately 6.2 billion US dollars.

信息安全问题快速增长

□2014年信息安全事故数量同比增长率超过了智能手机和GDP增长率

Security incidents outpace GDP and mobile phone growth *Year-over-year growth, 2013–2014*

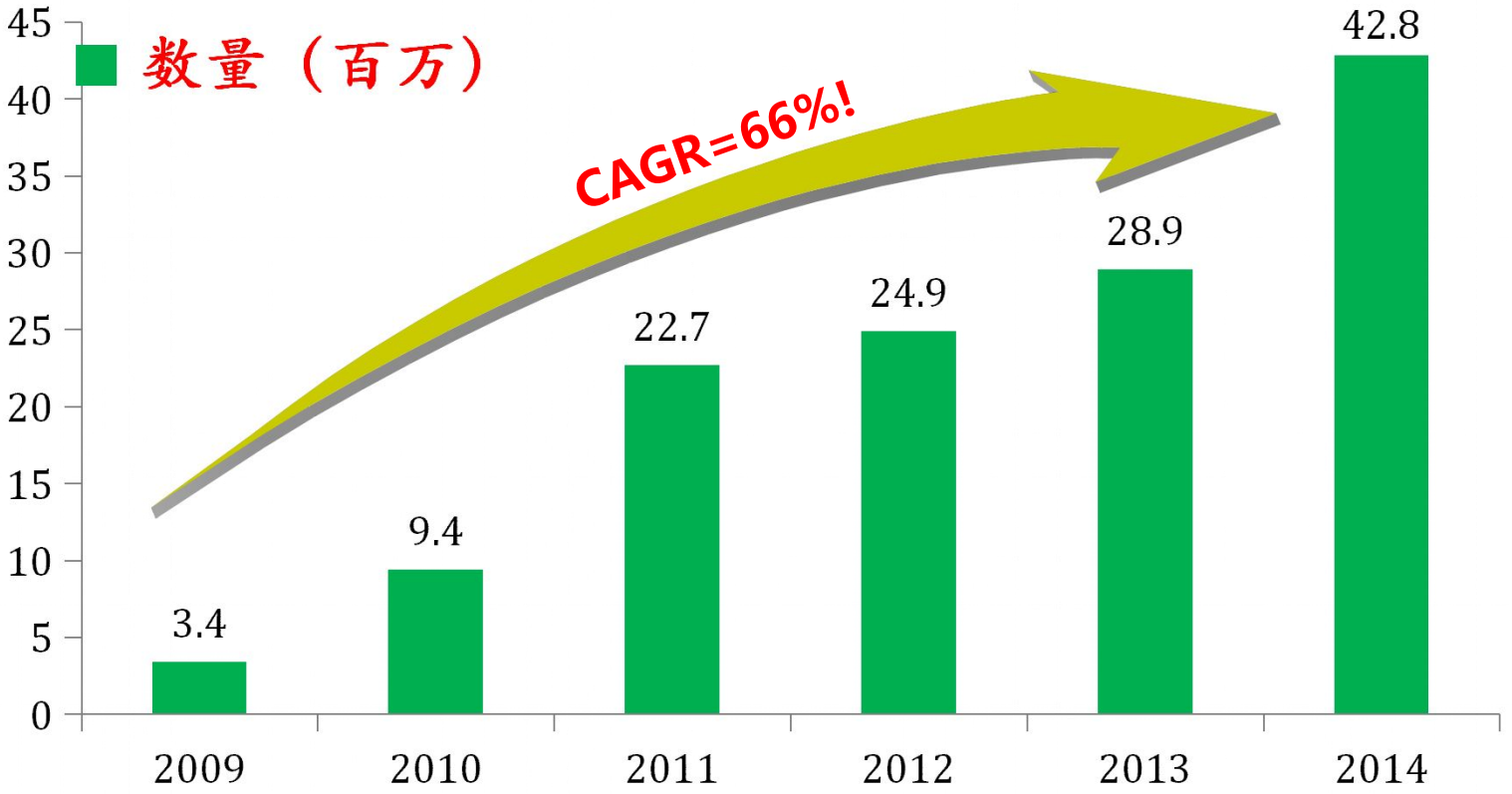


信息安全事故和经济代价飞速增长

Incidents and financial impacts continue to soar

- 自2009年以来，**信息安全事故数量年复合增长率（CAGR）高达66%**。

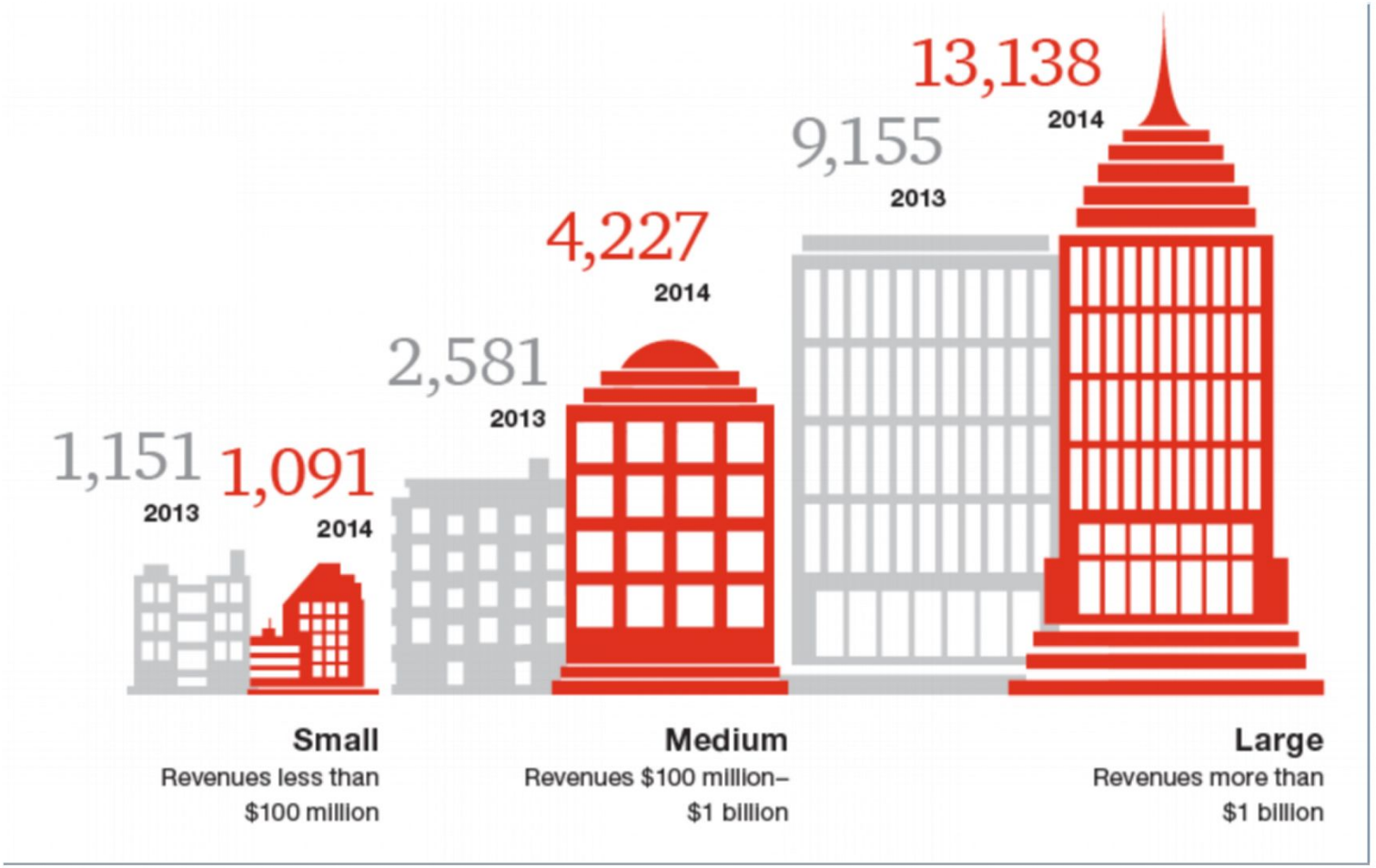
Security incidents (*Total number of detected incidents)* grow 66% CAGR since 2009.



公司越大信息安全事故越多

口越大型公司（按收入），被诊断出存在的信息安全事故越多

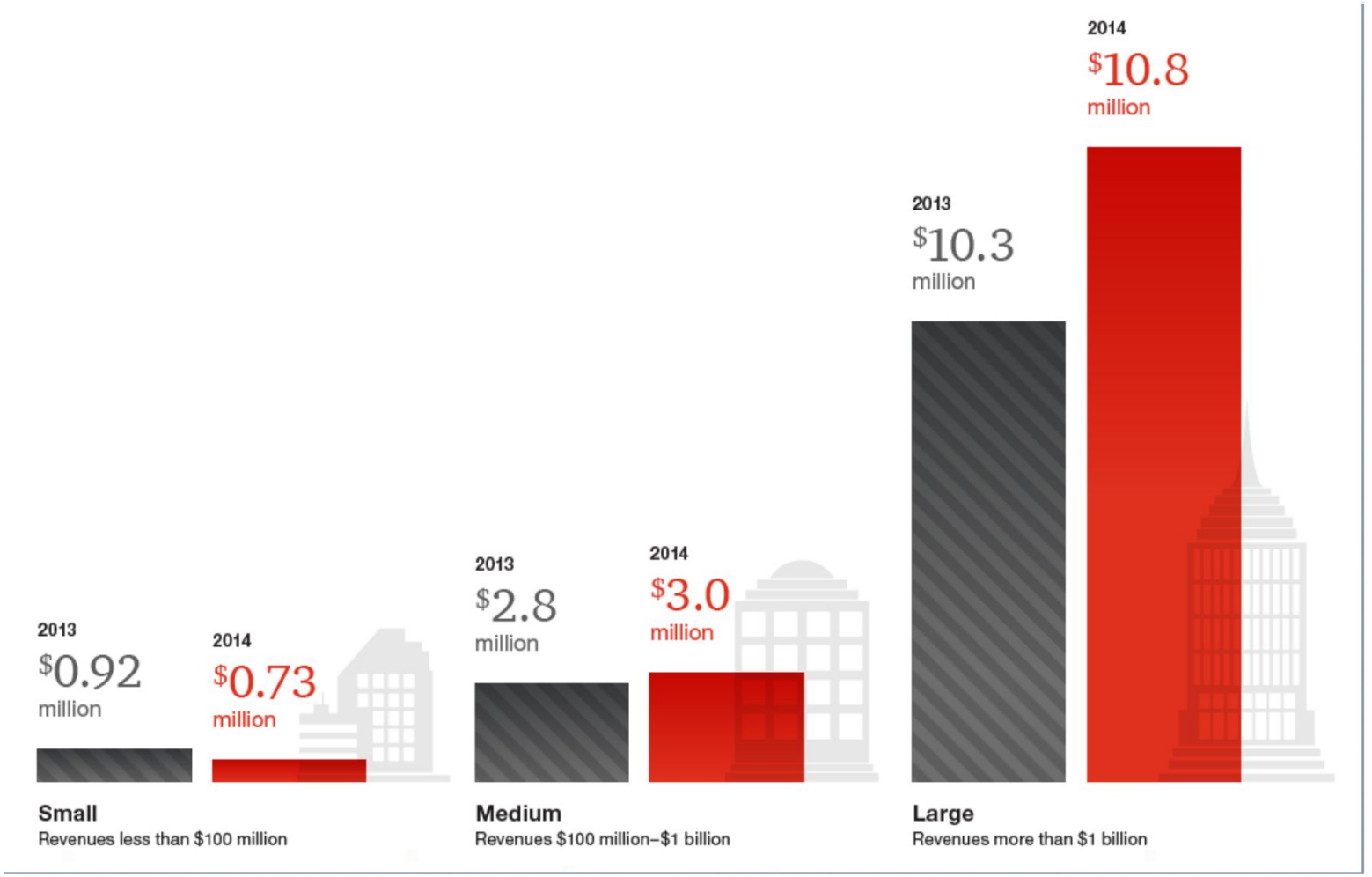
Larger companies detect more incidents *Detected security incidents by company size (revenue)*



按公司收入信息安全花费

□按公司大小（根据收入），信息安全花费

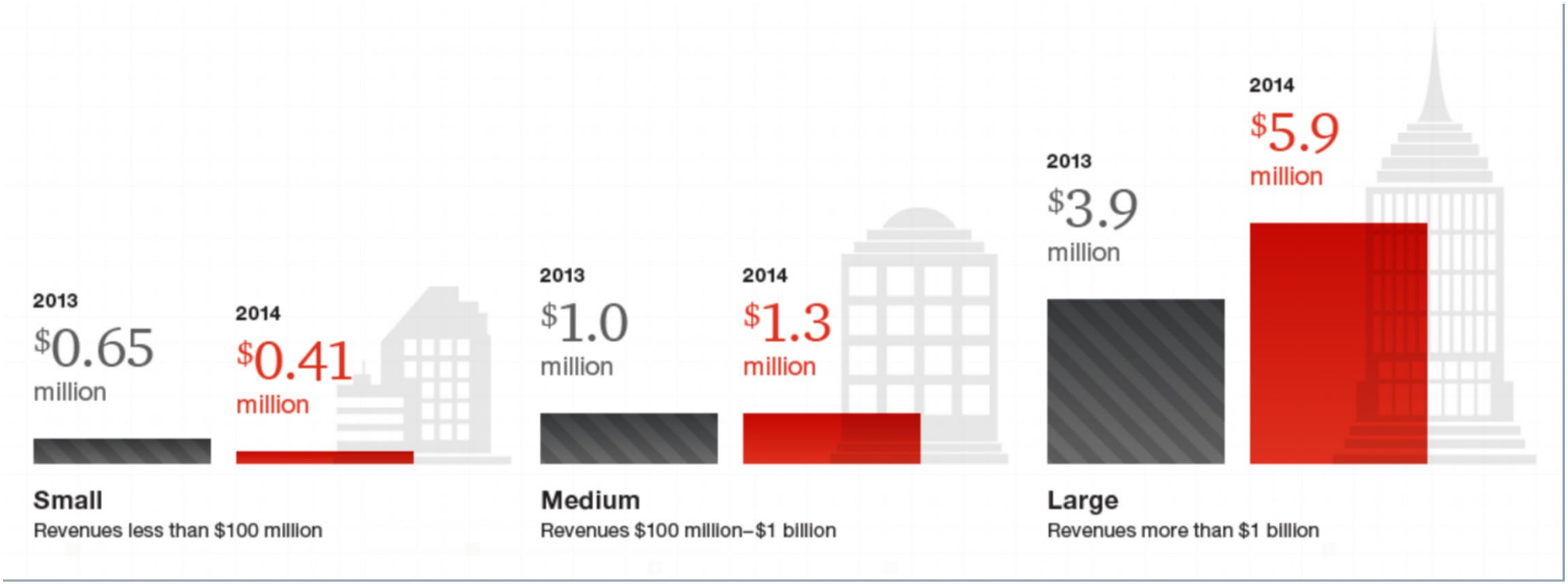
Information security budget by company size (revenue) *2013–2014*



按公司收入信息安全事故财务损失

口按公司大小（根据收入），大公司信息安全事故财务损失越大

Incidents are more costly to large organizations *Average financial losses due to security incidents, 2013–2014*

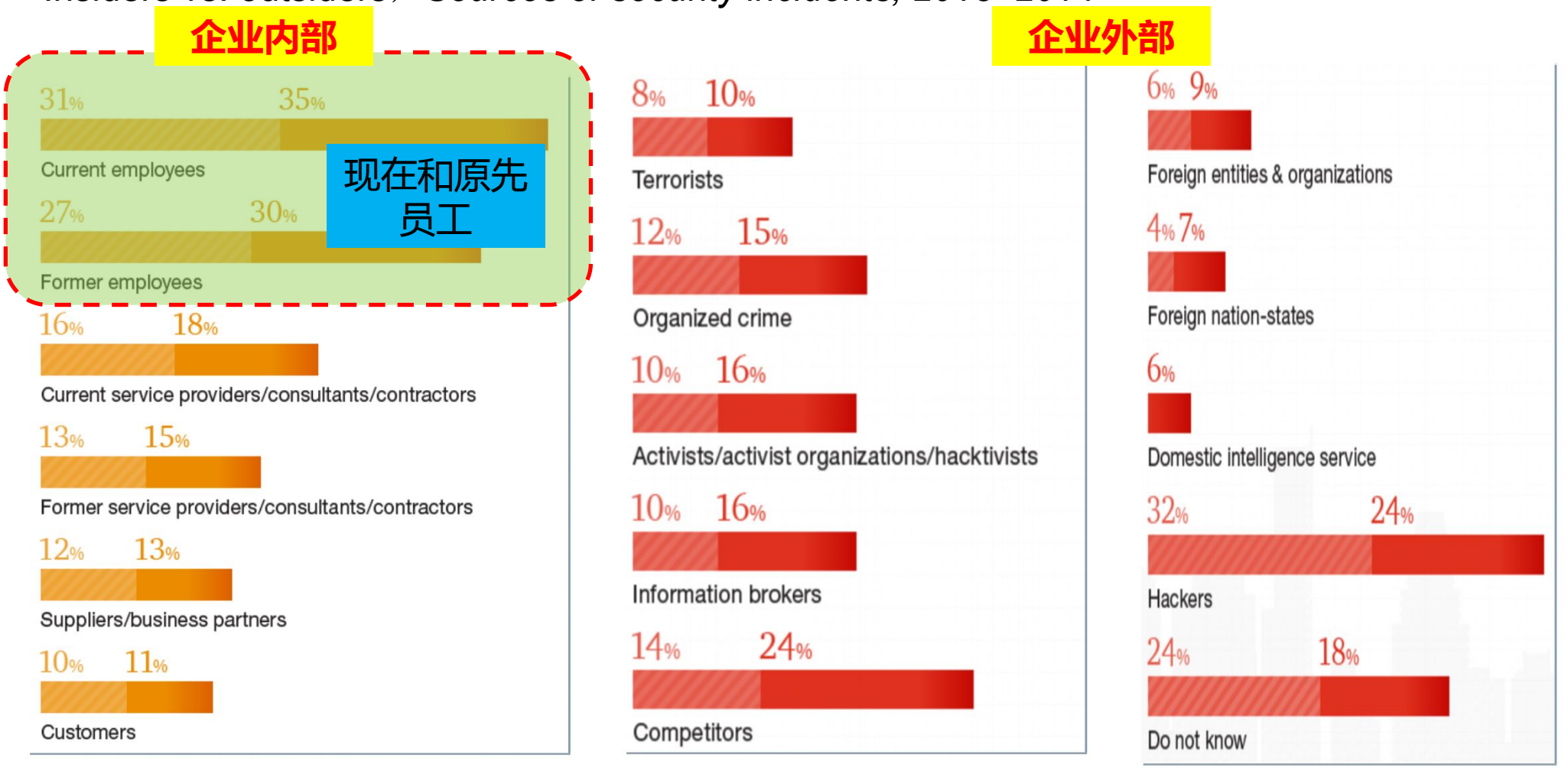


公司内部员工是导致信息安全的最大风险

Employees are the most-cited culprits of incidents

口公司内部、外部人员导致信息安全对比

Insiders vs. outsiders， *Sources of security incidents, 2013–2014*

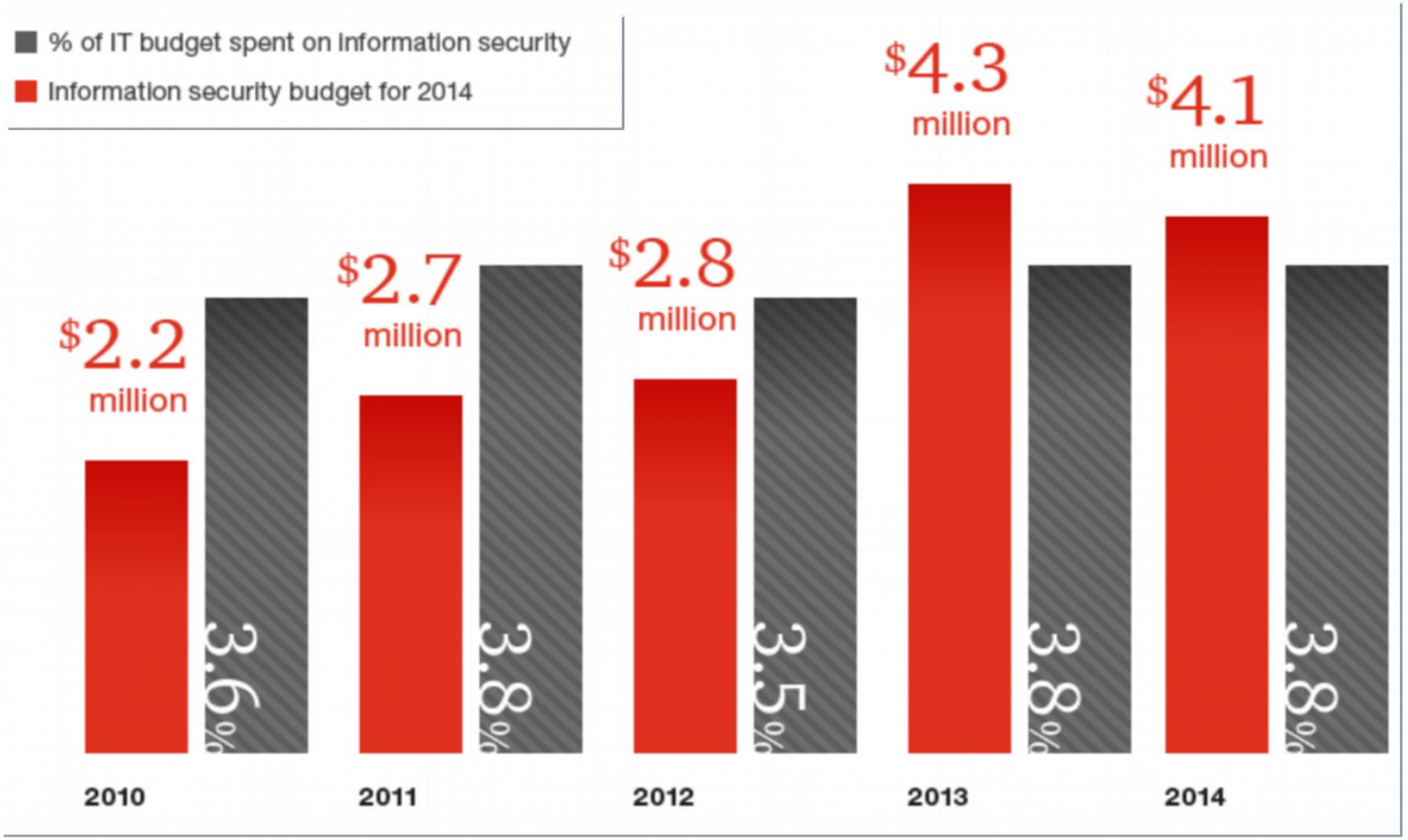


信息安全事故在增加，但防范风险的资金却在下降

As incidents rise, security spending falls

- 总体来说，2014年平均信息安全投资在减少，反转了在此之前的连增三年趋势

Overall, average security budgets decrease slightly, reversing a three-year trend



信息安全没有被公司最高层引起足够的重视

□在多数企业，董事会成员不参加关键信息安全活动。
At most organizations, the Board of Directors does not participate in key information security activities.

内容简介

一、全球信息安全调查结果摘录

二、全球电力和公共事业信息安全调查结果摘录

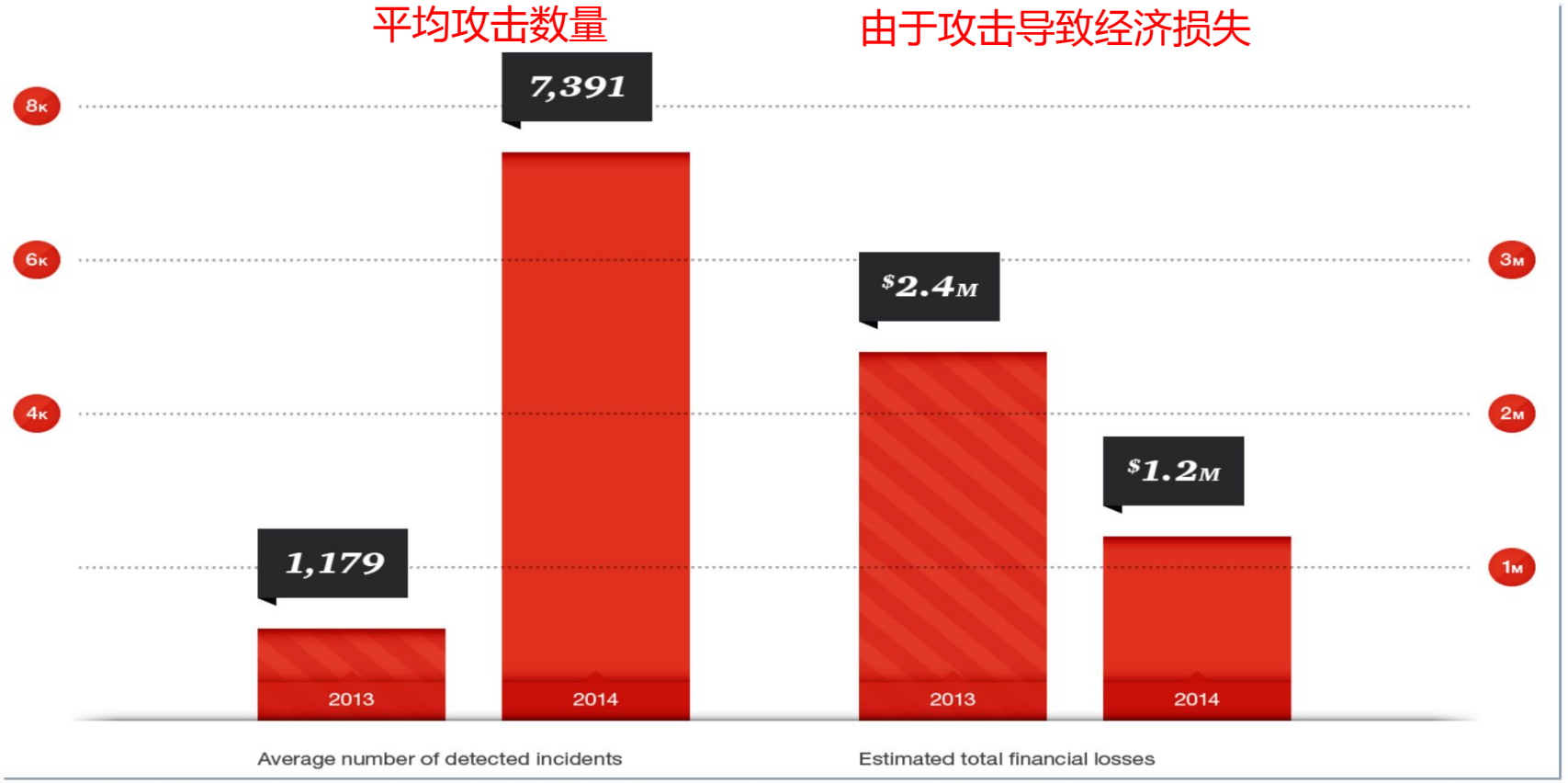
三、汽车行业信息安全概要

对电力和公共事业信息安全攻击已经从理论变为现实

Cyber attacks against power and utilities organizations have transitioned from theoretical to indisputable.

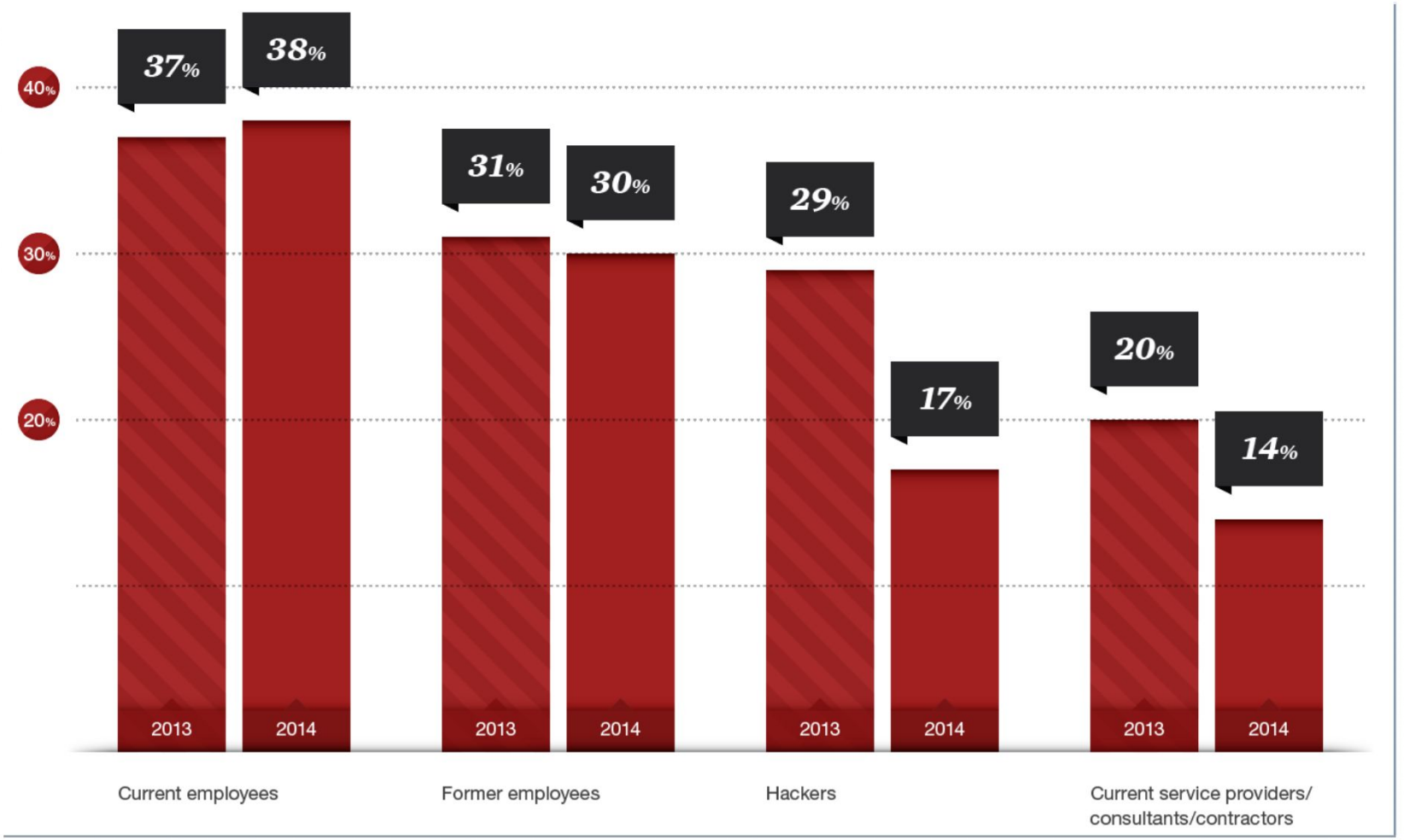
- **许多电力和公共事业公司，还没有准备好迎接伴随全球网络化带来的**信息安全攻击带来的巨大挑战

  All things considered, many power and utilities companies seem to be unready for the increasing risks of today’ s interconnected world.



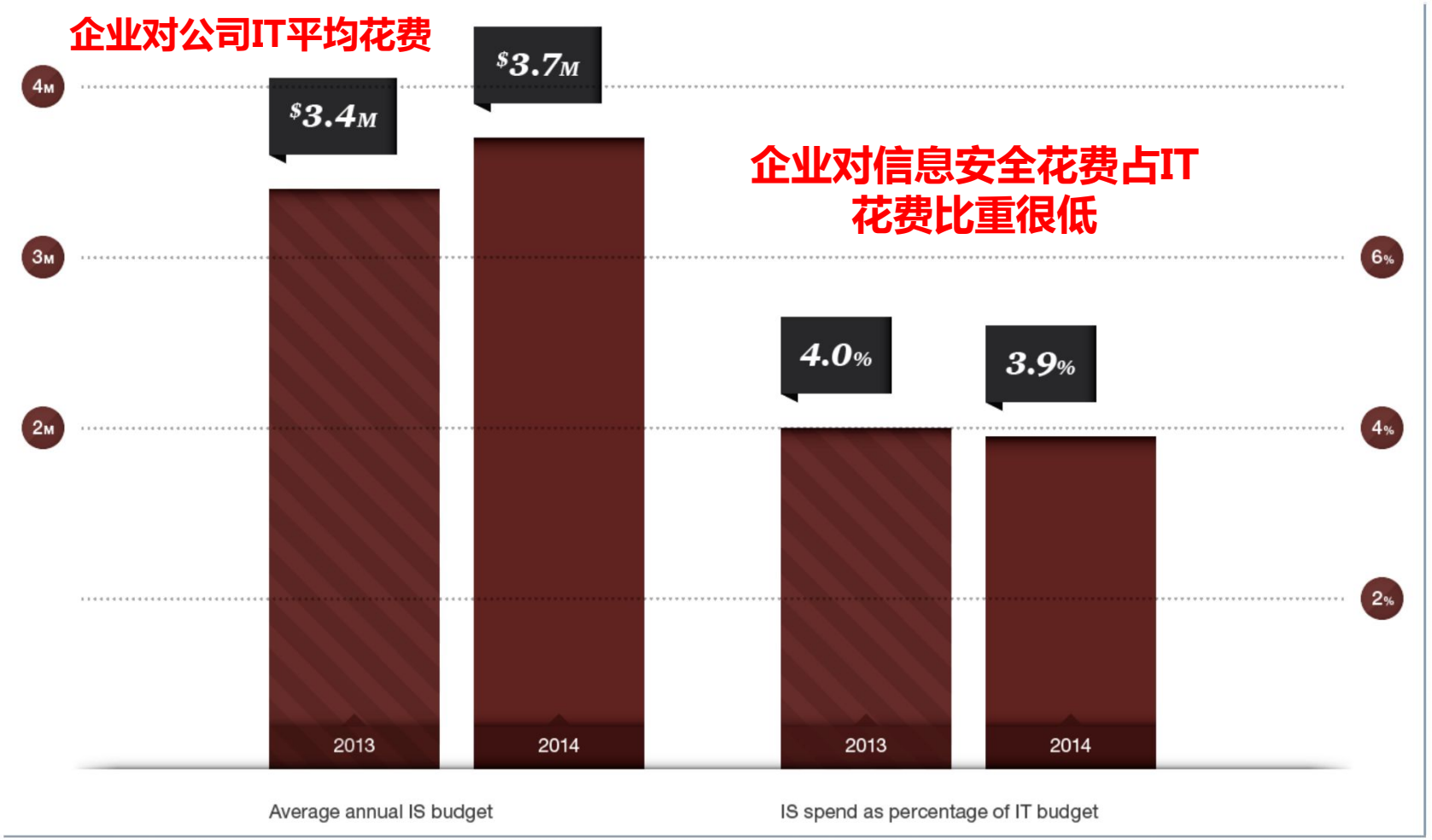
信息安全攻击来源

口令人吃惊的是，对公司信息安全风险的主要来源是现在员工，其次是离职员工



信息安全的花费

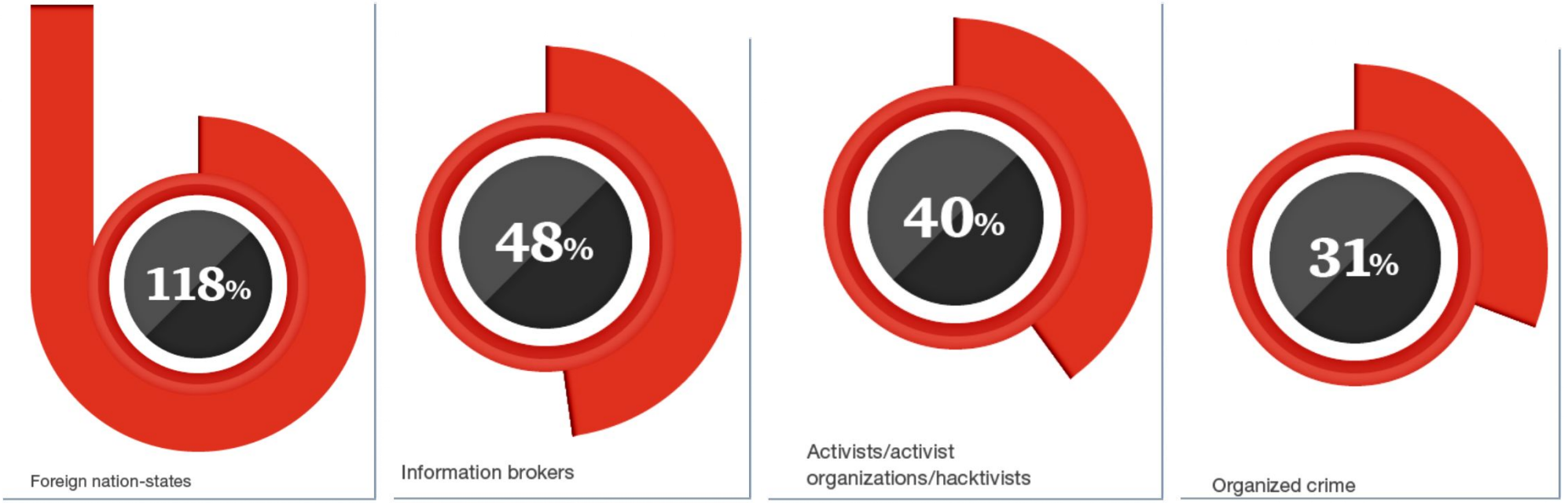
□企业对公司IT及信息安全平均花费



信息安全风险来源快速增长

□信息安全攻击来源快速增长

The fastest-growing sources of security incidents

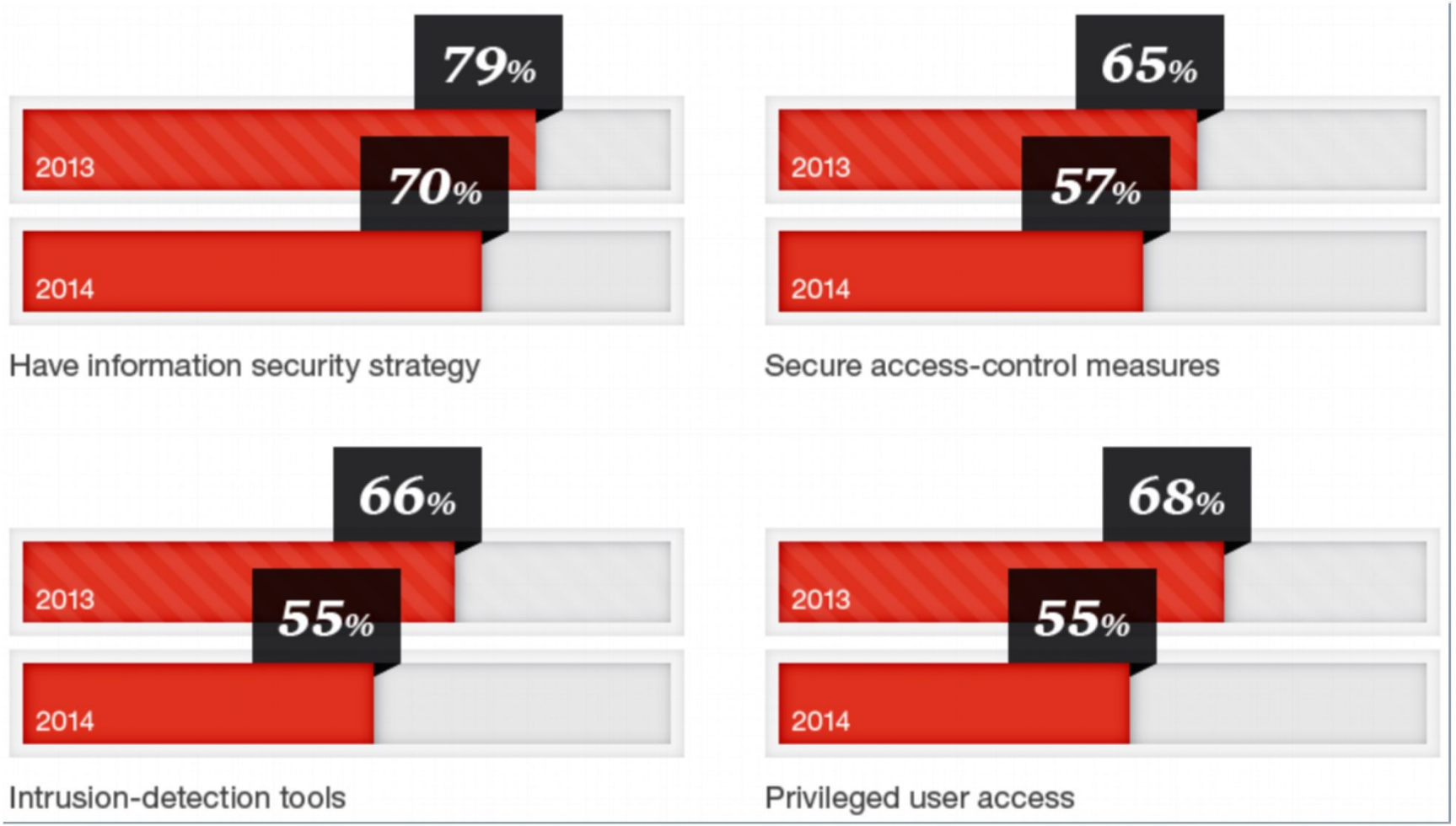


That, in part, may account for the 43% rise in respondents who report that data was exploited as a result of security incidents, the most cited impact.

需要更多策略来应对信息安全风险

□需要有更多策略的措施来应对信息安全风险

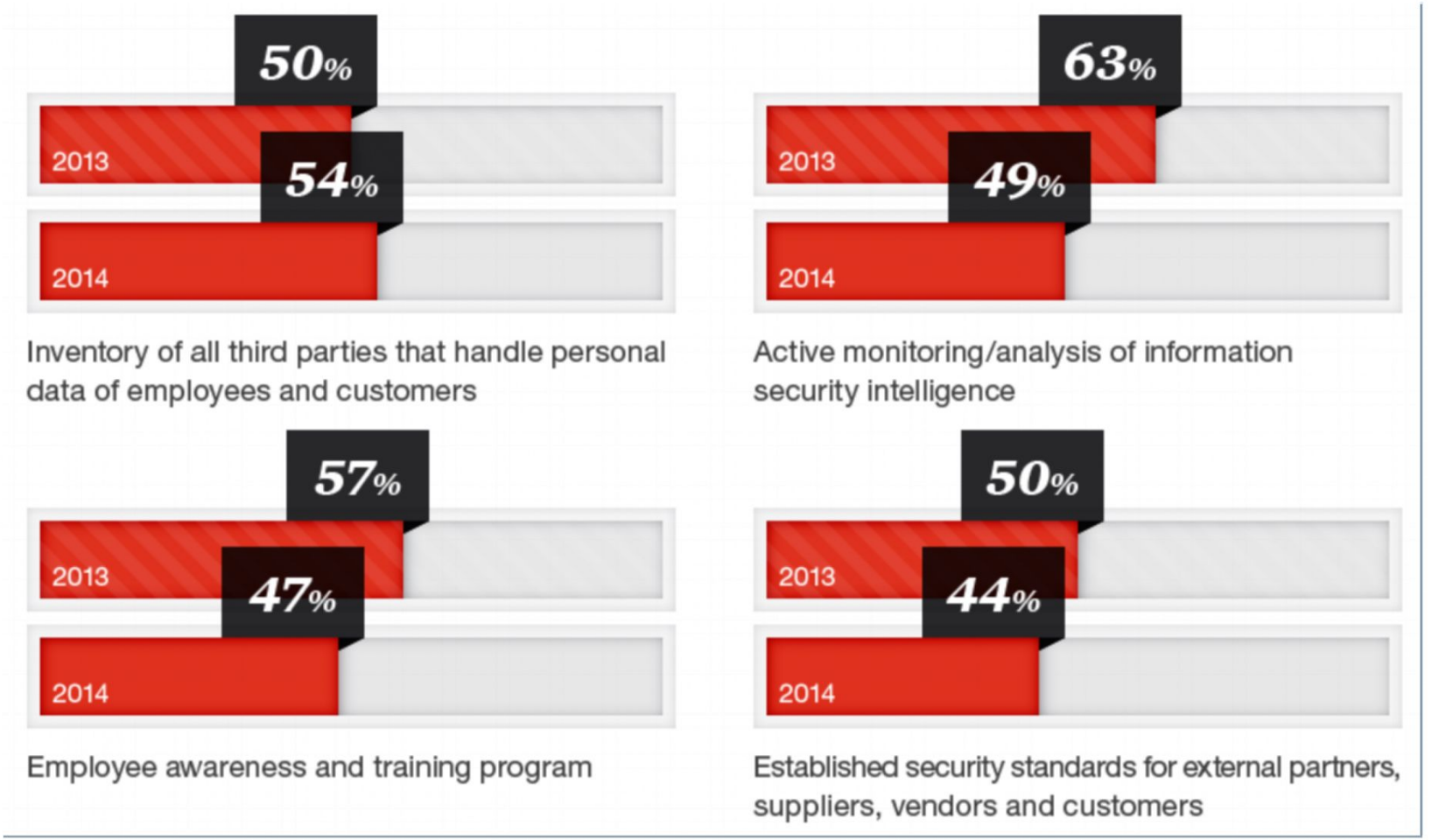
A more strategic approach is needed



需要更多策略来应对信息安全风险

□需要有更多策略的措施来应对信息安全风险

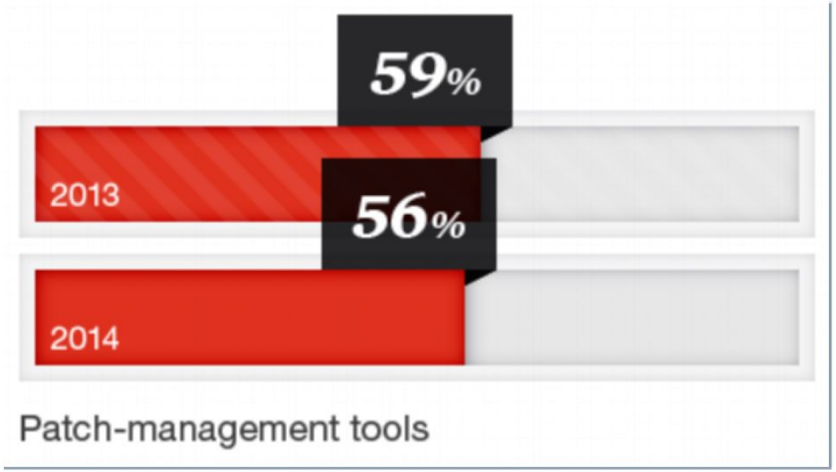
A more strategic approach is needed

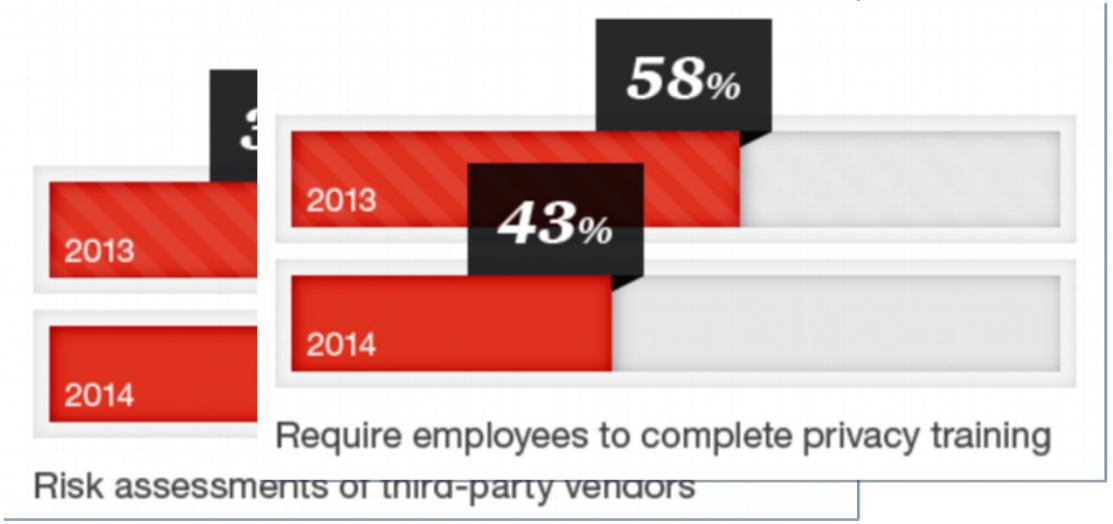


需要更多策略来应对信息安全风险

□需要有更多策略的措施来应对信息安全风险

A more strategic approach is needed





应对信息安全风险的策略流程恰恰缺失

口应对策略流程恰恰缺失*Strategic processes are often lacking*

- An effective security program will require top-down commitment and communication.

内容简介

一、全球信息安全调查结果摘录

二、工业领域信息安全调查概要

三、汽车行业信息安全概要

三个时代

1、某车企信息安全体系案例

2、某车联网信息安全平台—某军区车辆管理控制系统

3、未来智能时代汽车行业信息安全

1、某车企信息安全体系案例—行业特点

□当前汽车制造企业内部数据信息安全环境主要有以下五大特点：

1、企业规模庞大，多以集团形式存在，分支机构繁多，信息管理难度较大。

2、企业信息环境复杂，应用系统数量庞大，信息环境复杂。

3、产业链较长，设计外部数据信息接入以及对外交互数据信息需求频繁。

4、在数据安全管理和数据应用效率两方面的难以均衡。

5、信息环境高度安全性与信息安全整体解决方案高成本之间矛盾突出 。

- 可见，汽车制造行业作为大型企业，在日常运营当中涉及到的数据信息安全组织结构数量种类庞大，意味着与之相应的数据信息泄露的渠道必定数量巨大。
- 随着汽车制造行业企业业务的不断发展，大量核心技术、专利、图纸以及财务等核心数据信息在不同的组织结构不同的信息环境当中大量产生。

1、某车企信息安全体系案例—追求目标

- 7“不”+1“可”目标

进不来

拿不走

改不了

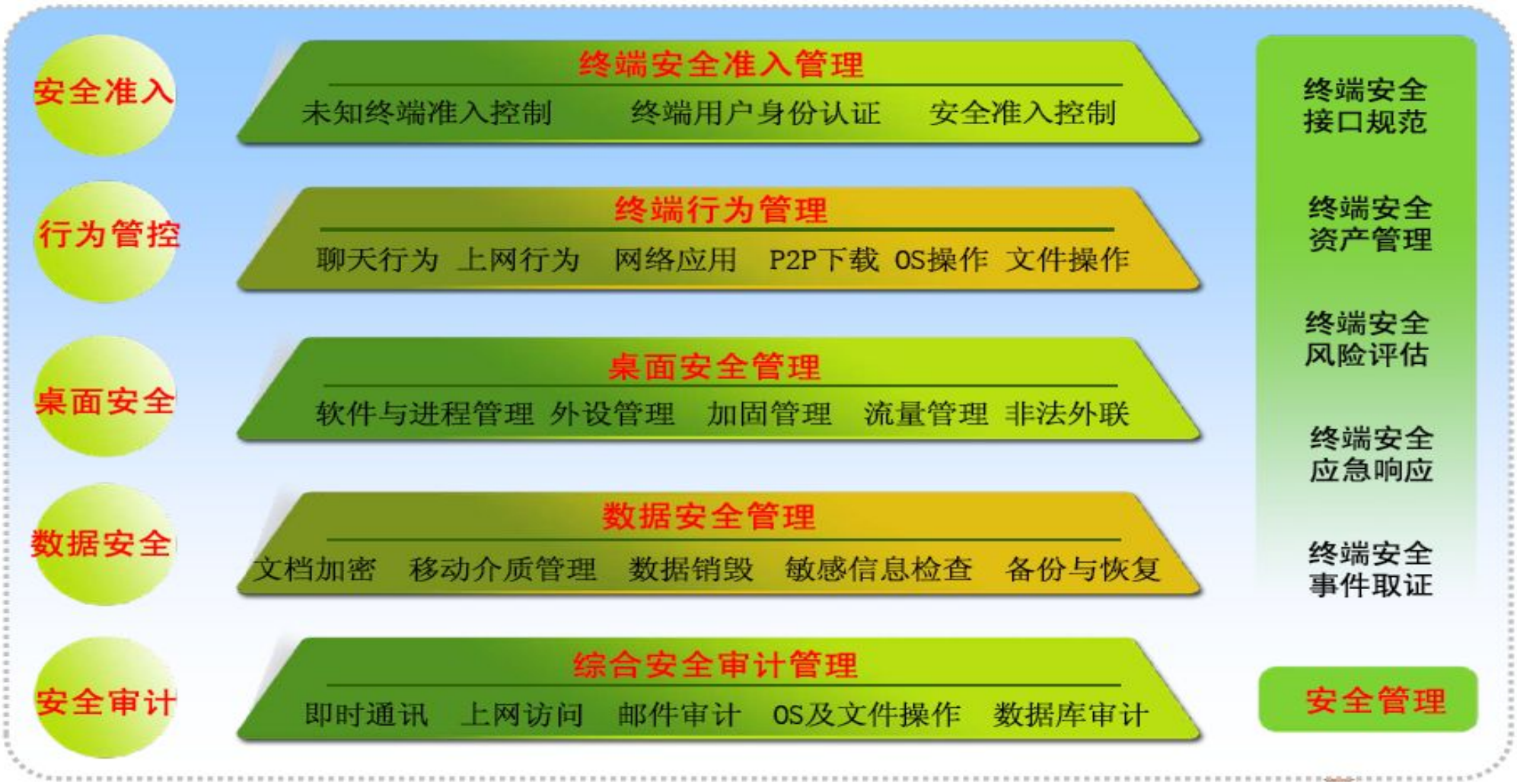
看不懂

跑不了

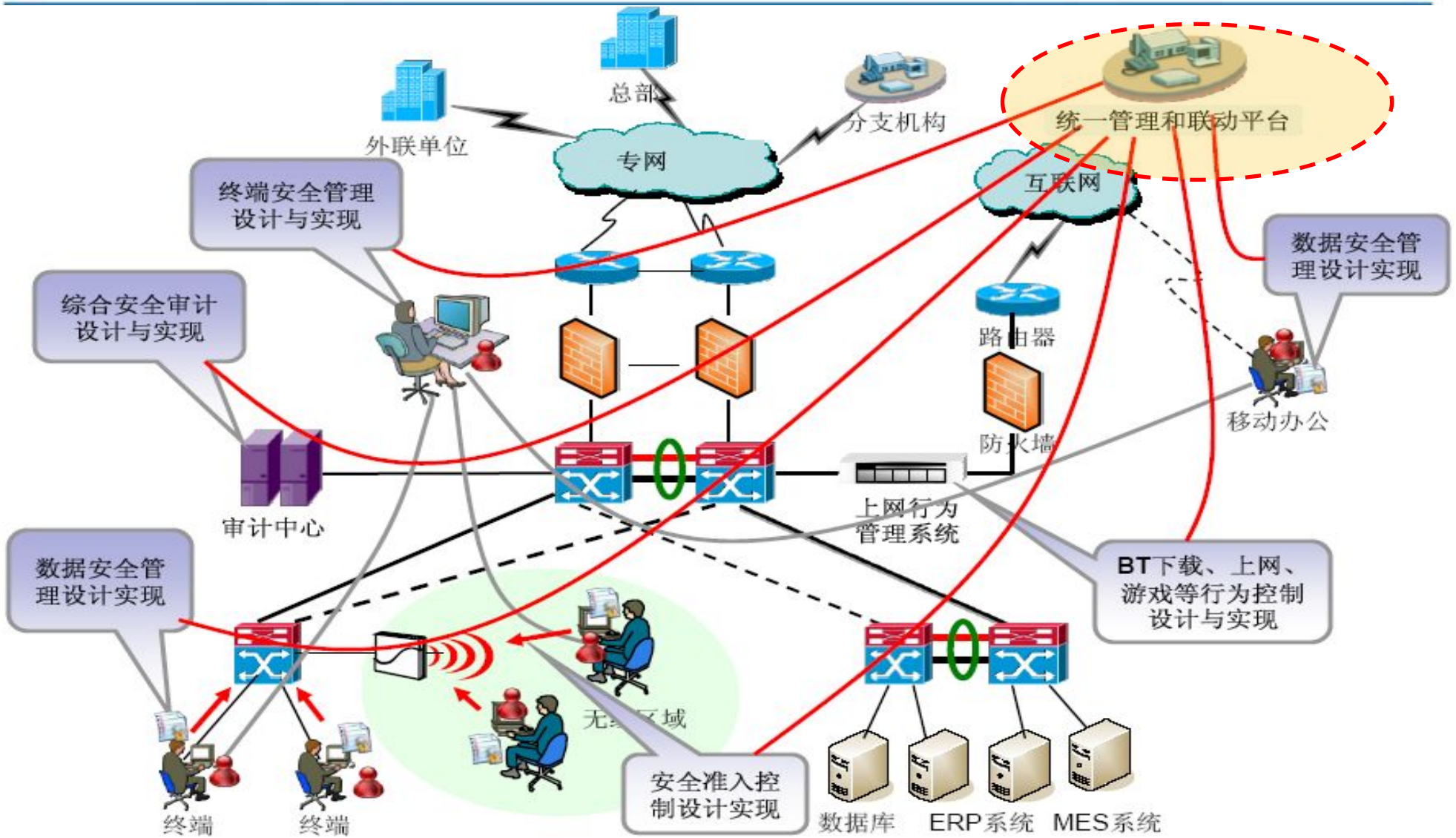
可审查

打不垮

1、某车企信息安全体系案例—模型



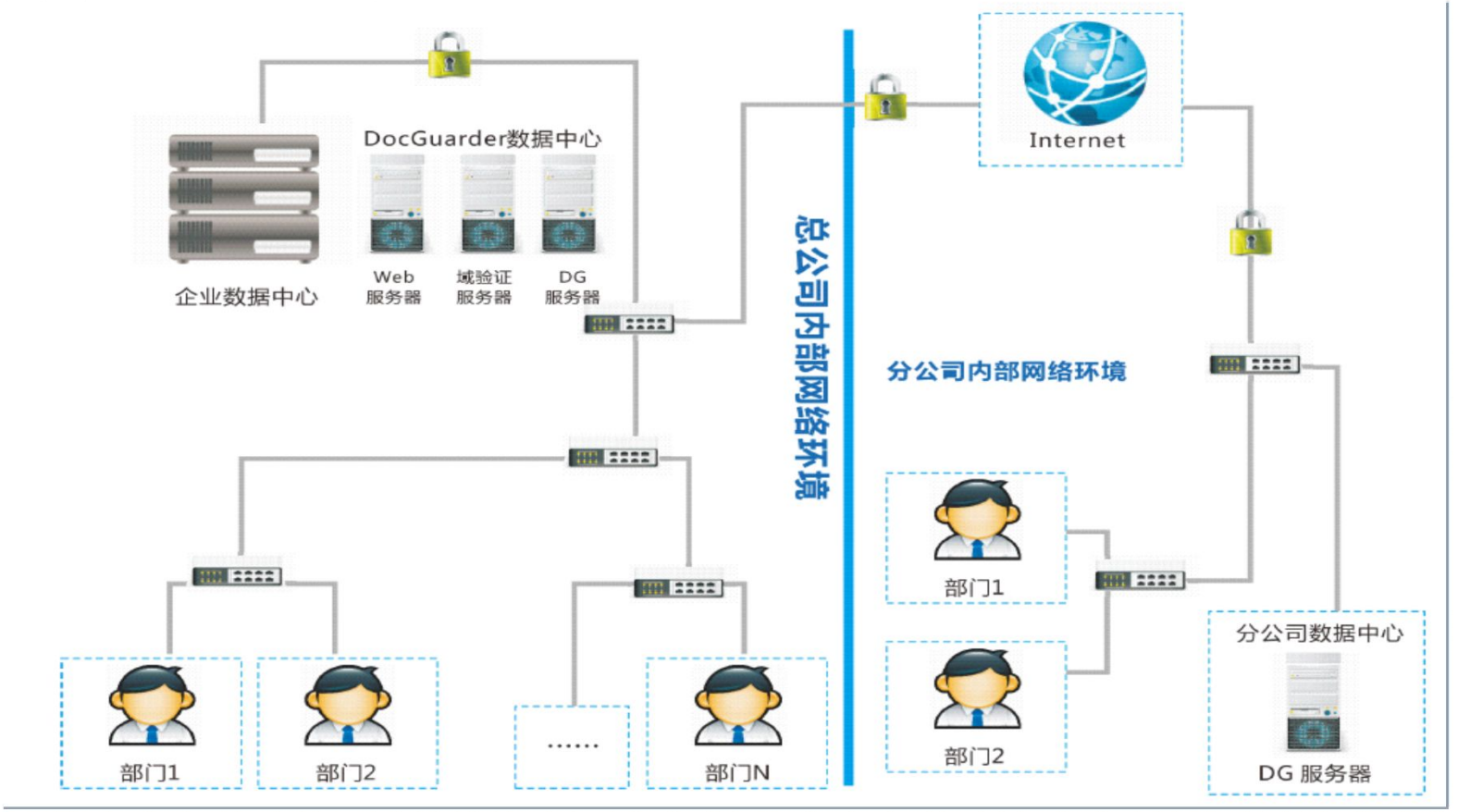
1、某车企信息安全体系案例—设计方案示意



1、某车企信息安全体系案例—系统部署

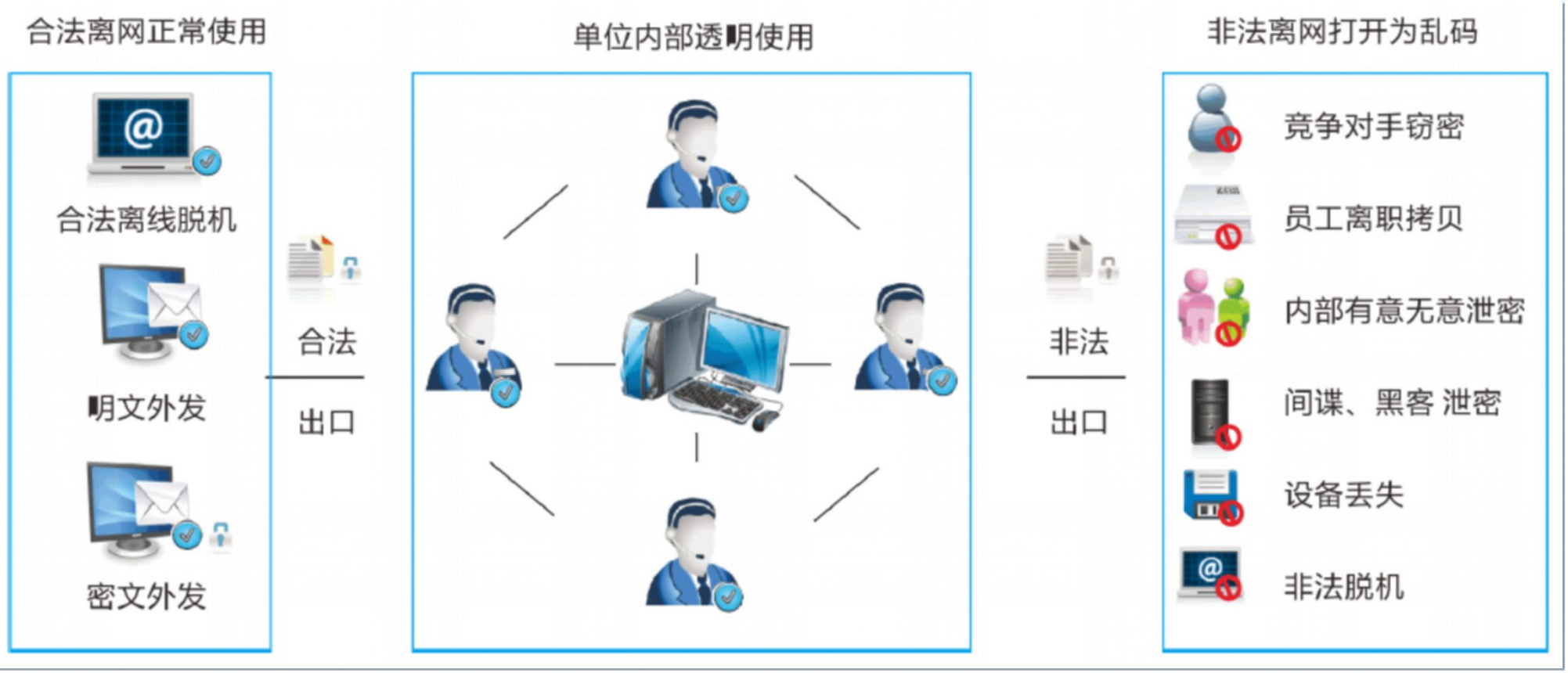
- 汽车企业内部数据安全体系建设，需要突出重点；
- 切实关注文件外带保密需求，充分考虑敏感性数据面临的各种主动泄密和被动泄密风险；
- 同时，应充分考虑系统对员工的业务影响范围，尽可能降低安全行为带来的系统性能损耗和应用约束，在安全性和可用性之间保持合理的平衡。

系统部署图



1、某车企信息安全体系案例—防护效果

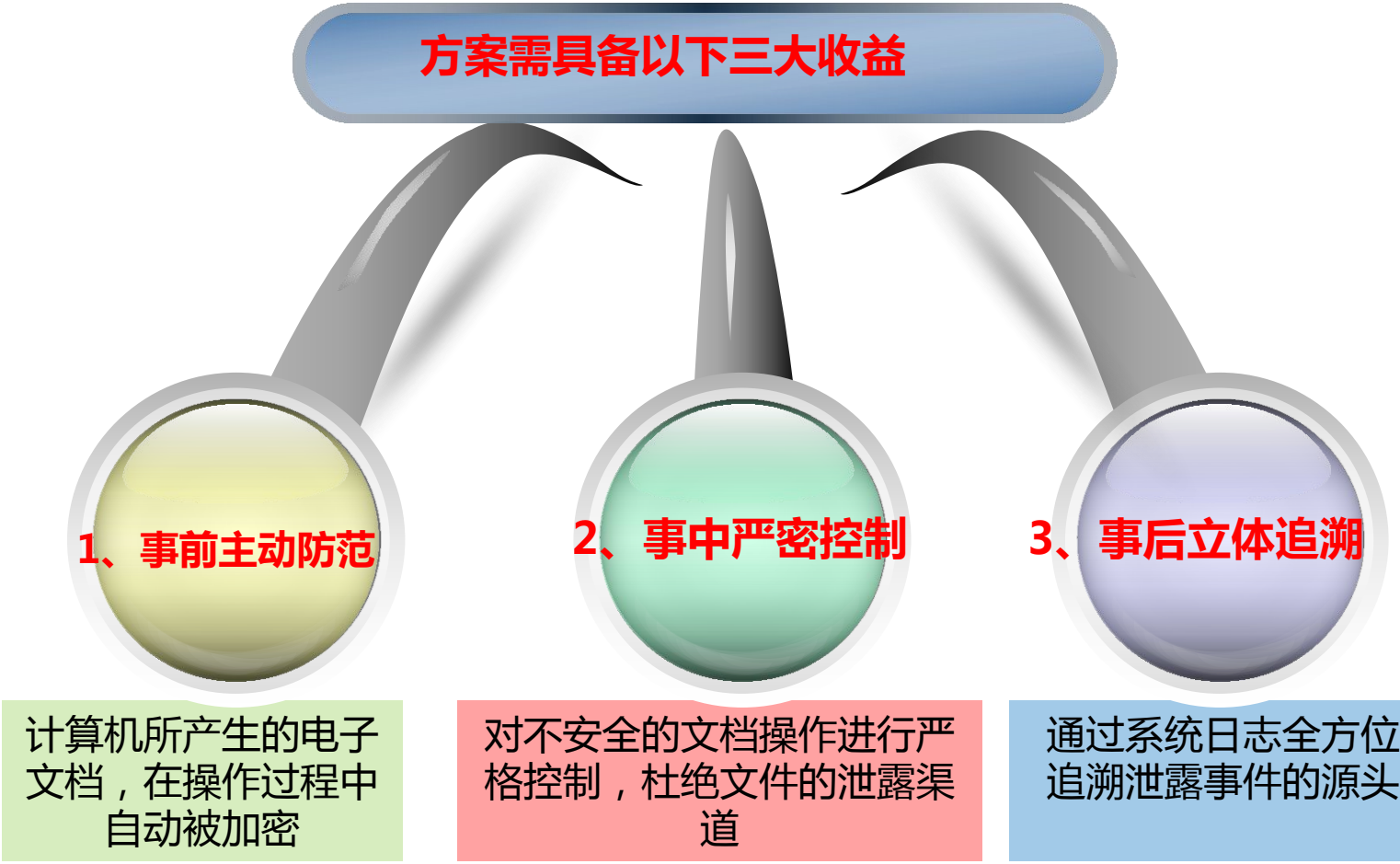
口防护效果图



1、某车企信息安全体系案例—具有效益

□方案需要具备以下效益

通过整体方案的有效实施，要有效增强电子文档防泄密力度，企业可充分保护商业机密和技术机密。



1、某车企信息安全体系案例—功能价值详述

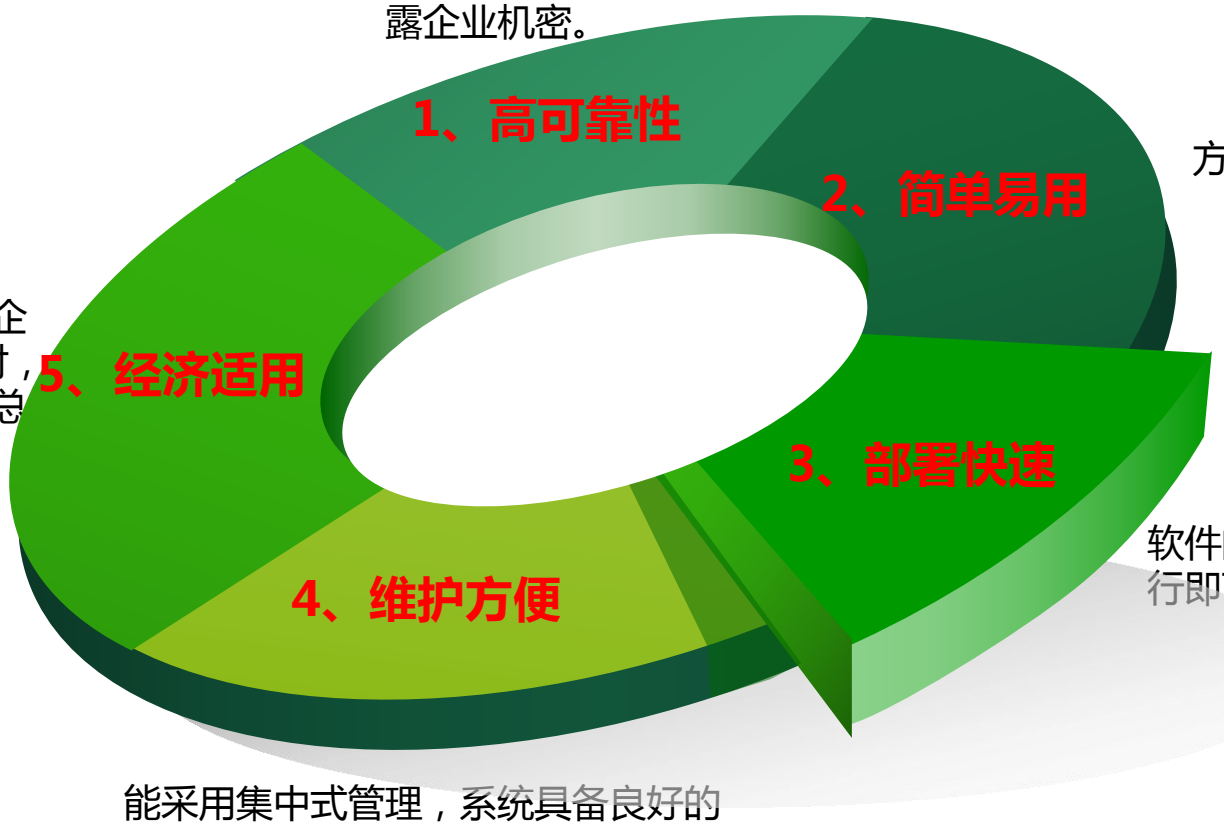
口方案需要具备的功能价值

- 要可集成PDM系统、ERP系统、OA系统、CPC系统、设计分析系统等使用广泛的管理系统，对控制列表中不存在的管理系统，提供现场集成功能，能充分满足企业的复杂需求；
- 要支持所有应用程序控制，如设计类的Pro/E、UG、CATIA、AutoCAD等，办公类Office系列等，汇编类VC、VB系列等可以产生文件的程序；
- 要具备大用户数管理模式，能满足大规模端点控制需求，可以实现负载均衡、热备和多级管理模式等；
- 要具有高度的模块化和扩展性，可以根据制造业信息系统发展的需要，扩展其他功能，比如：电子邮件加密，输出内容监控等模块；
- 要防止内部员工通过邮件、MSN、QQ、FTP下载等网络端口发送重要文档。
- 要完全兼容现有网络、硬件系统，如路由器、网关及防火墙；完全兼容已知的安全软件，如杀毒软件、防火墙软件，加密进程不会被安全软件误判为病毒或木马并被清除或终止；也兼容最新的Windows系统平台，如Windows Vista、Win7等。

1、某车企信息安全体系案例—方案特点

□方案需要具备以下5大特点

可以全面防止内部人员和外来人员直接从客户端泄露企业机密。



方案总体操作简单、界面直观、需培训量小。

方案在满足汽车企业安全需求的同时，可有效控制系统总成本要求。

软件的升级要在系统服务端进行即可，应能快速部署应用程序，高效工作。

能采用集中式管理，系统具备良好的可维护性，可大大减轻维护人员的工作量。

1、某车企信息安全体系案例—策略概要

口应对策略

规范

- 工作人员签订企业数据保密协议
- 遵守《企业内部控制基本规范》
- 制定企业文档管理制度

网络安全技术

- 合理的系统安全设计，避免应用程序被恶意攻击、篡改
- 通过防火墙、IDS、防病毒等软硬件措施提高网络安全
- 规定使用机密数据的电脑不允许上外网，只能上内网

设备安全技术

- 规定只能用工作电脑
- Windows系统底层对存储设备读写进行控制
- 必要时，屏蔽工作电脑的USB插口

文档安全管理技术

- 文档强制加密（透明、密钥）
- 细分权限设置（用户、操作、范围、时间）
- 内容拷贝控制 (限制应用程序)
- 截屏控制和打印控制管理
- 终端离线办公（时限、补时码）
- 工作模式切换 (工作模式与个人模式的切换)
- 操作日志记录 (监控、跟踪)
- 应用文件的定期、异地备份，系统双机热备
- 智能识别技术(数字签名认证体系)

1、某车企信息安全体系案例—隐患源头举例

□企业信息安全隐患—源头

制造业

研发类企业

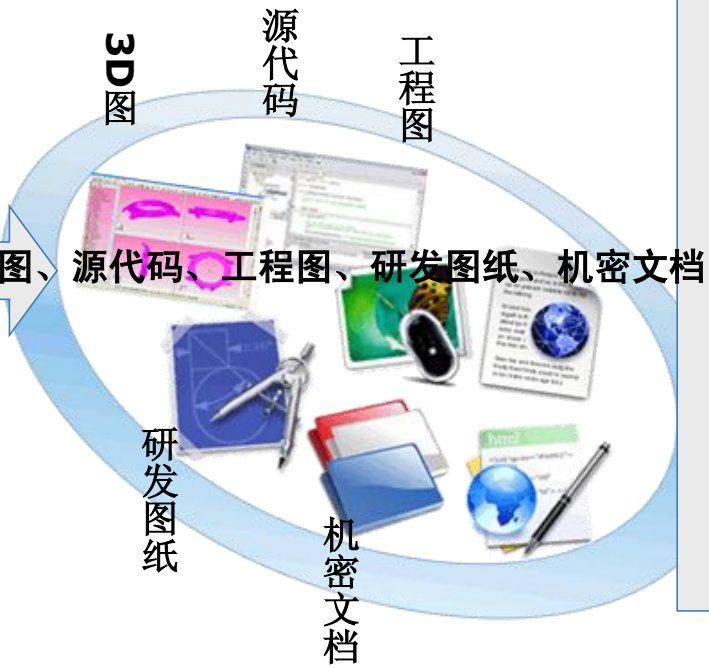
设计公司

金融业

通信业

……

3D图、源代码、工程图、研发图纸、机密文档。。。。



QQ\Email

即时通讯工具

U盘\移动硬盘

内存窃取

拷贝

截屏

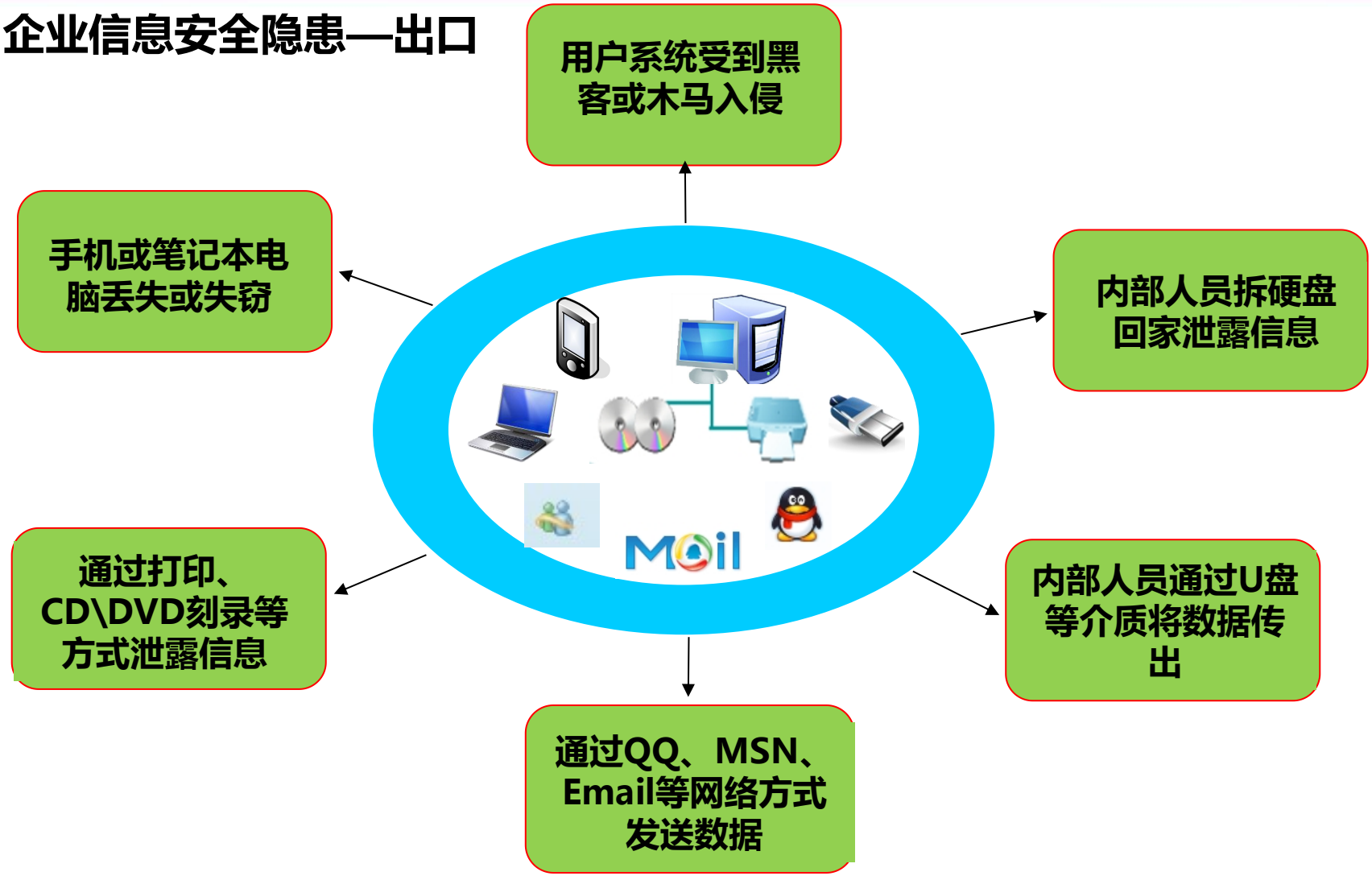
拖拽录制

打印

……

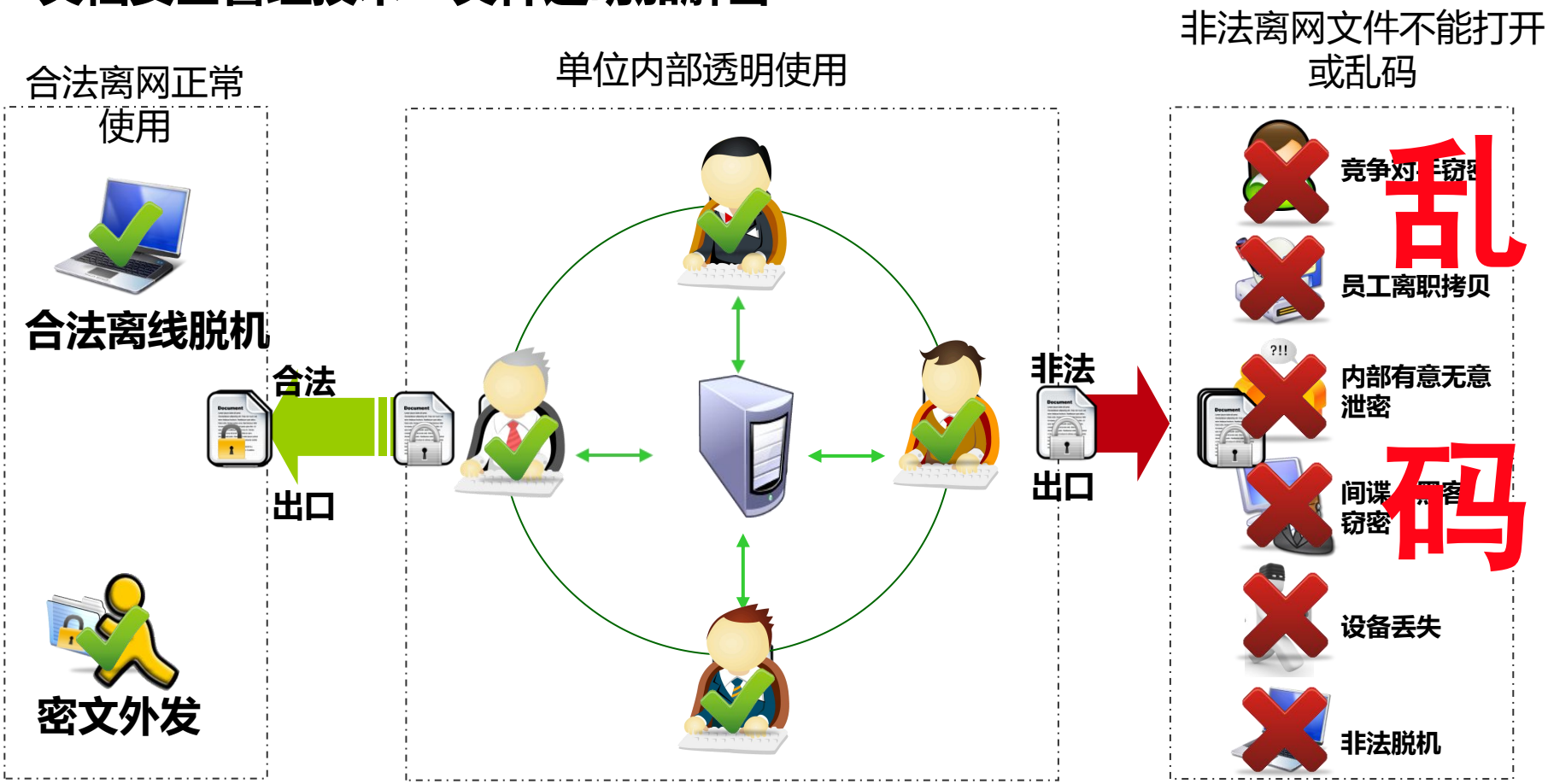
1、某车企信息安全体系案例—隐患出口举例

口企业信息安全隐患—出口



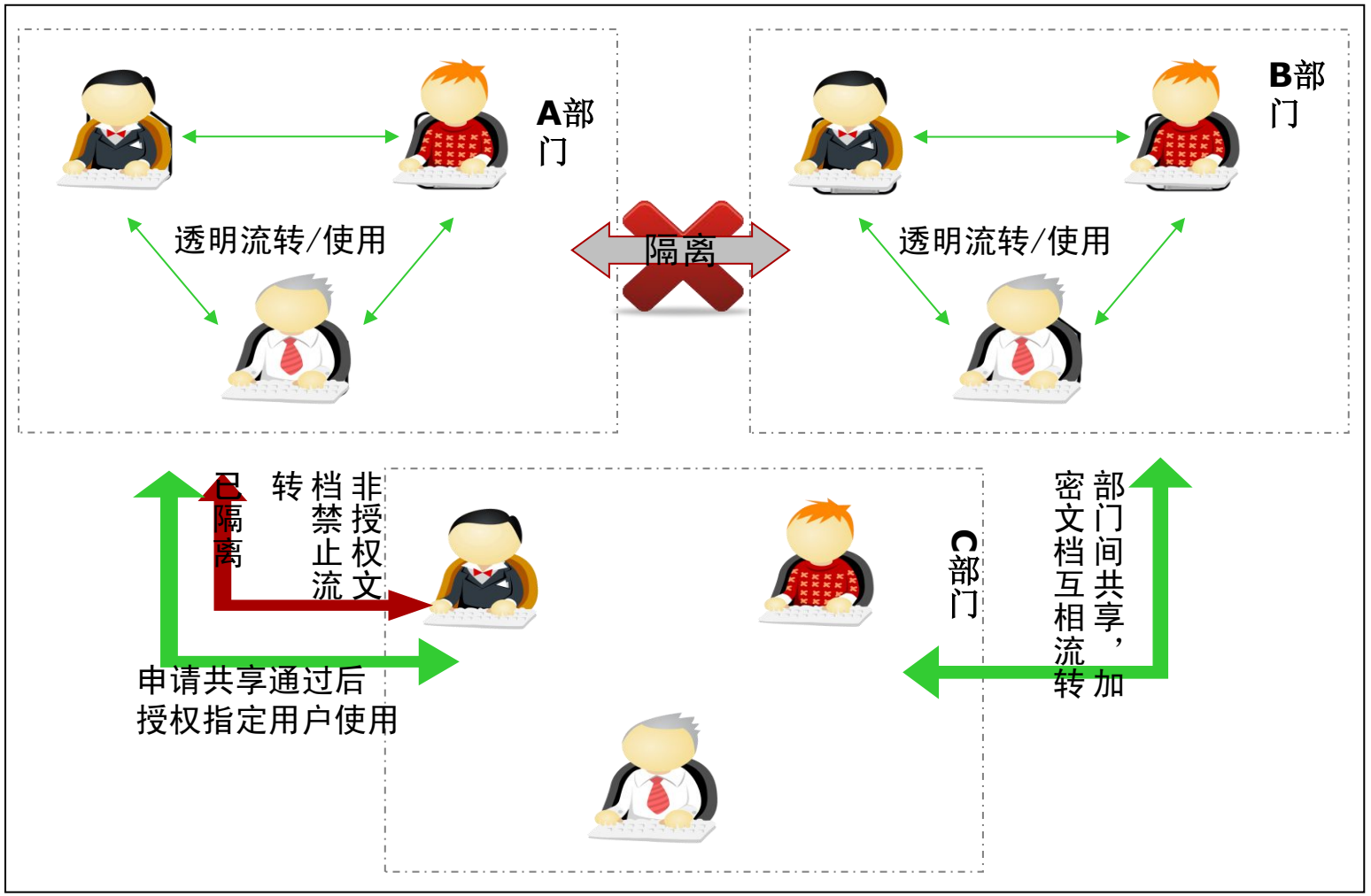
1、某车企信息安全体系案例—具体防护策略示例

口文档安全管理技术—文件透明加解密



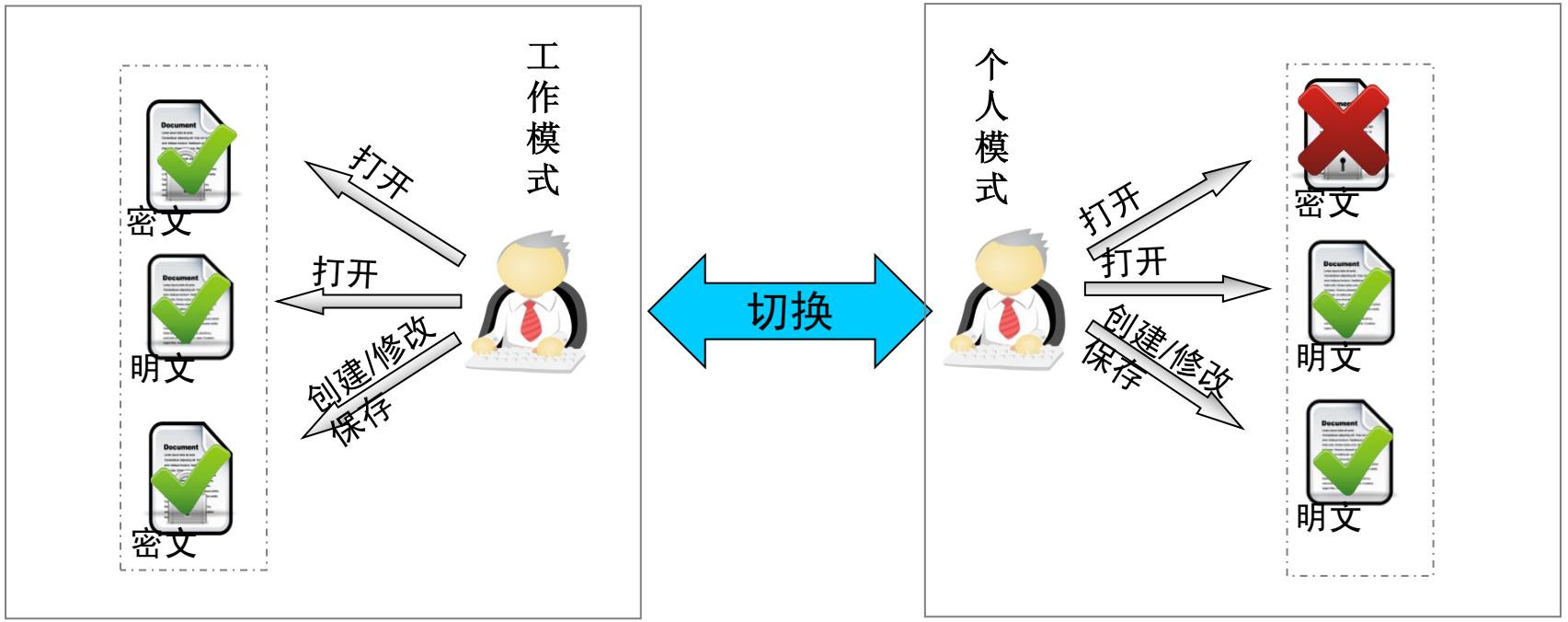
1、某车企信息安全体系案例—具体防护策略示例

口文档安全管理技术—部门隔离与共享



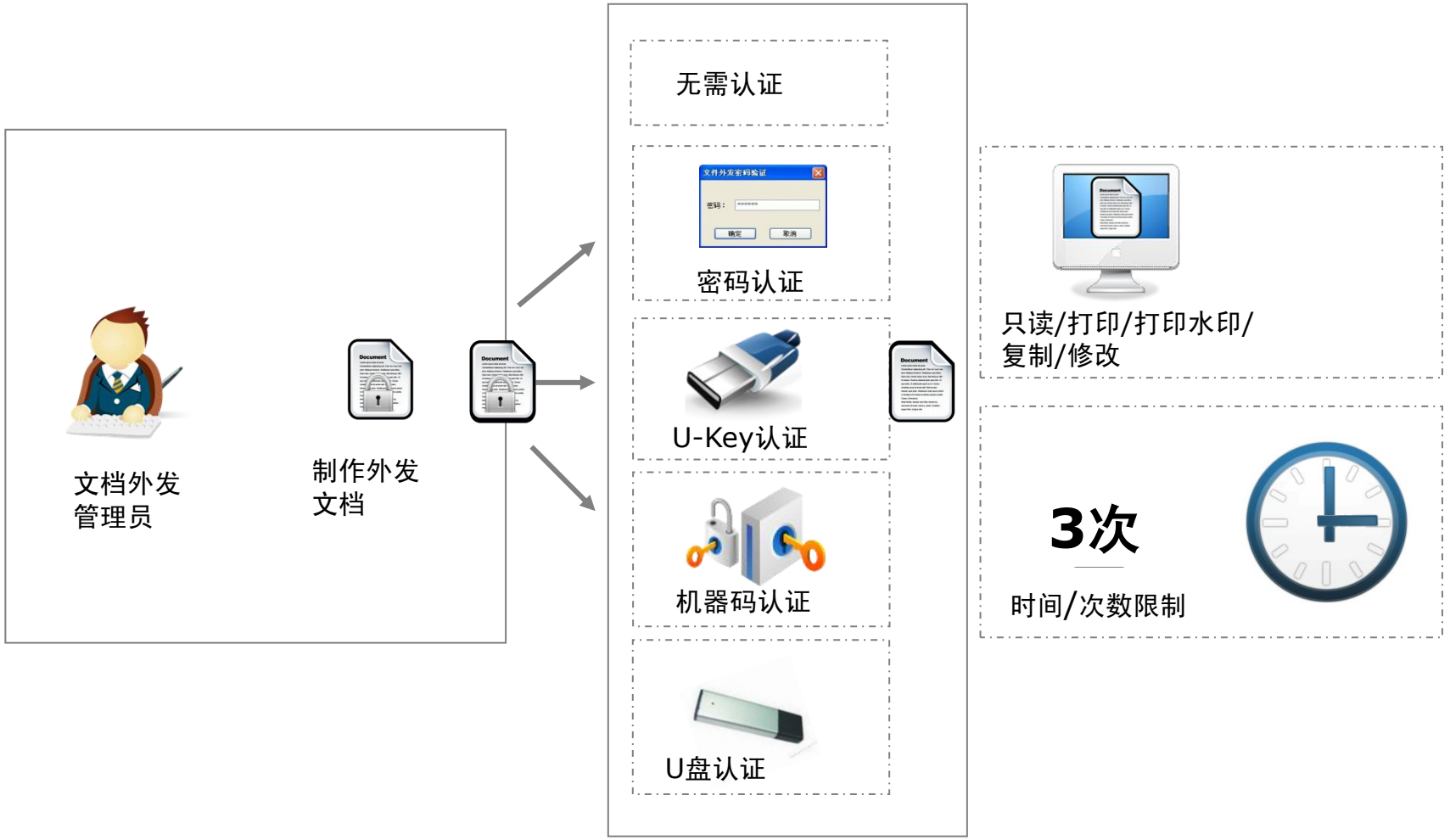
1、某车企信息安全体系案例—具体防护策略示例

口文档安全管理技术—工作模式与个人模式切换

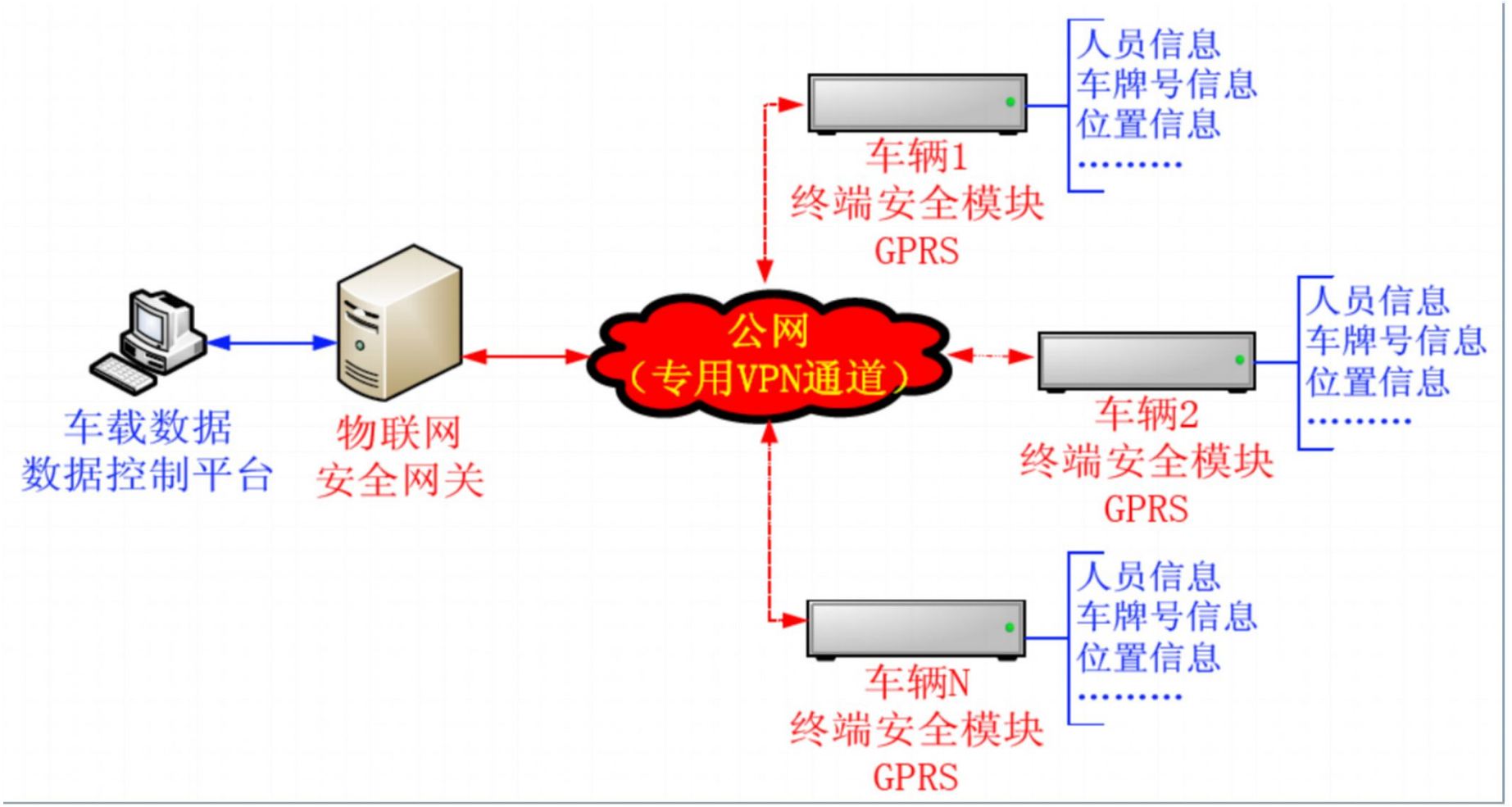


1、某车企信息安全体系案例—具体防护策略示例

口文档安全管理技术—文件外发控制



2、某车联网信息安全平台-某军区车辆管理控制系统



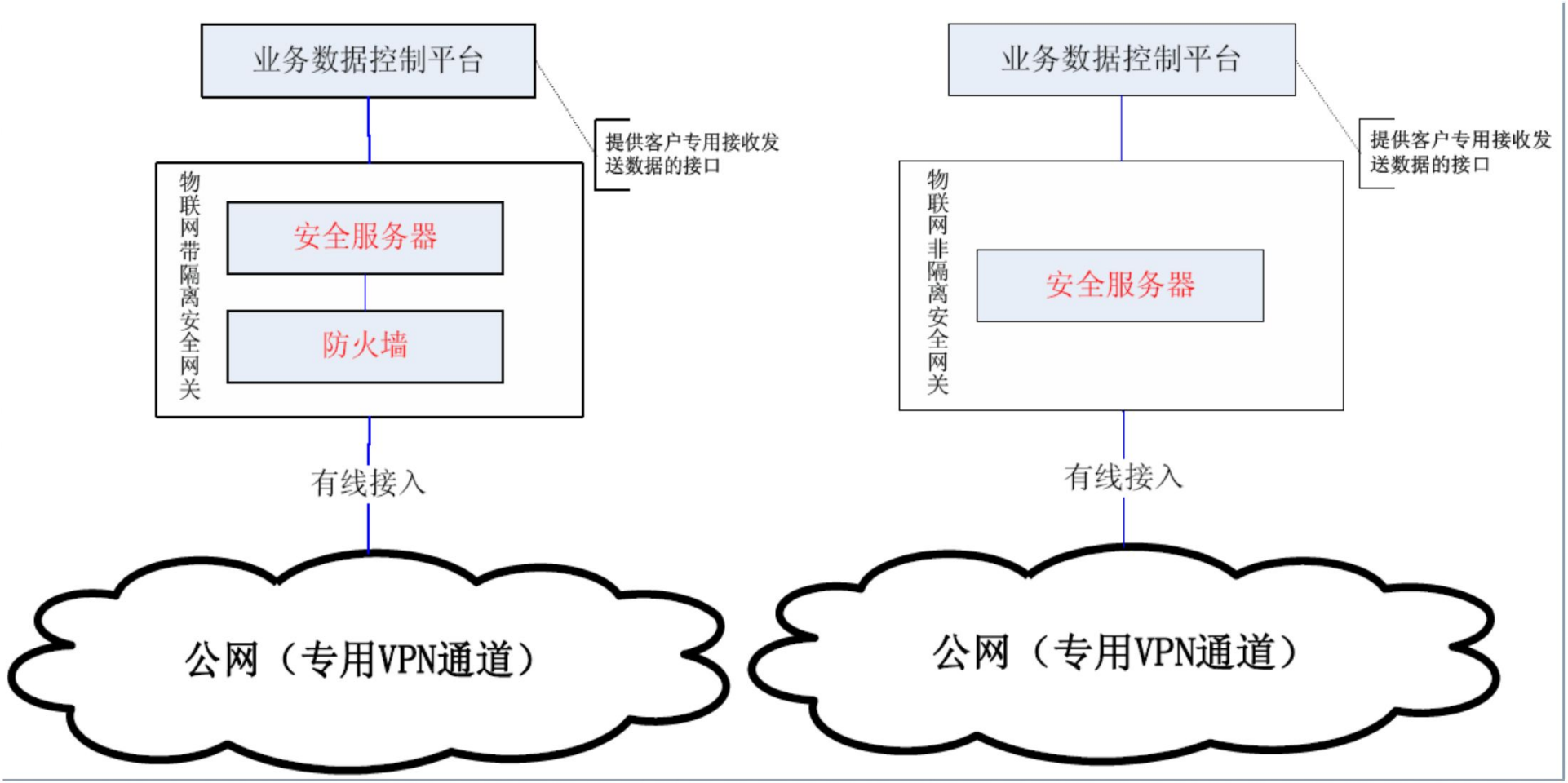
2、某车联网信息安全平台—系统构架

口系统构架

2、某车联网信息安全平台—安全网关

□安全网关

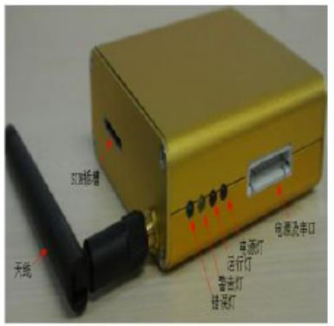
◆功能概述：解密待进入内网的数据；加密待发向外网的数据。



2、某车联网信息安全平台—终端模块

口终端安全模块

◆功能概述：解密来自于公网的数据；加密待发向公网的数据



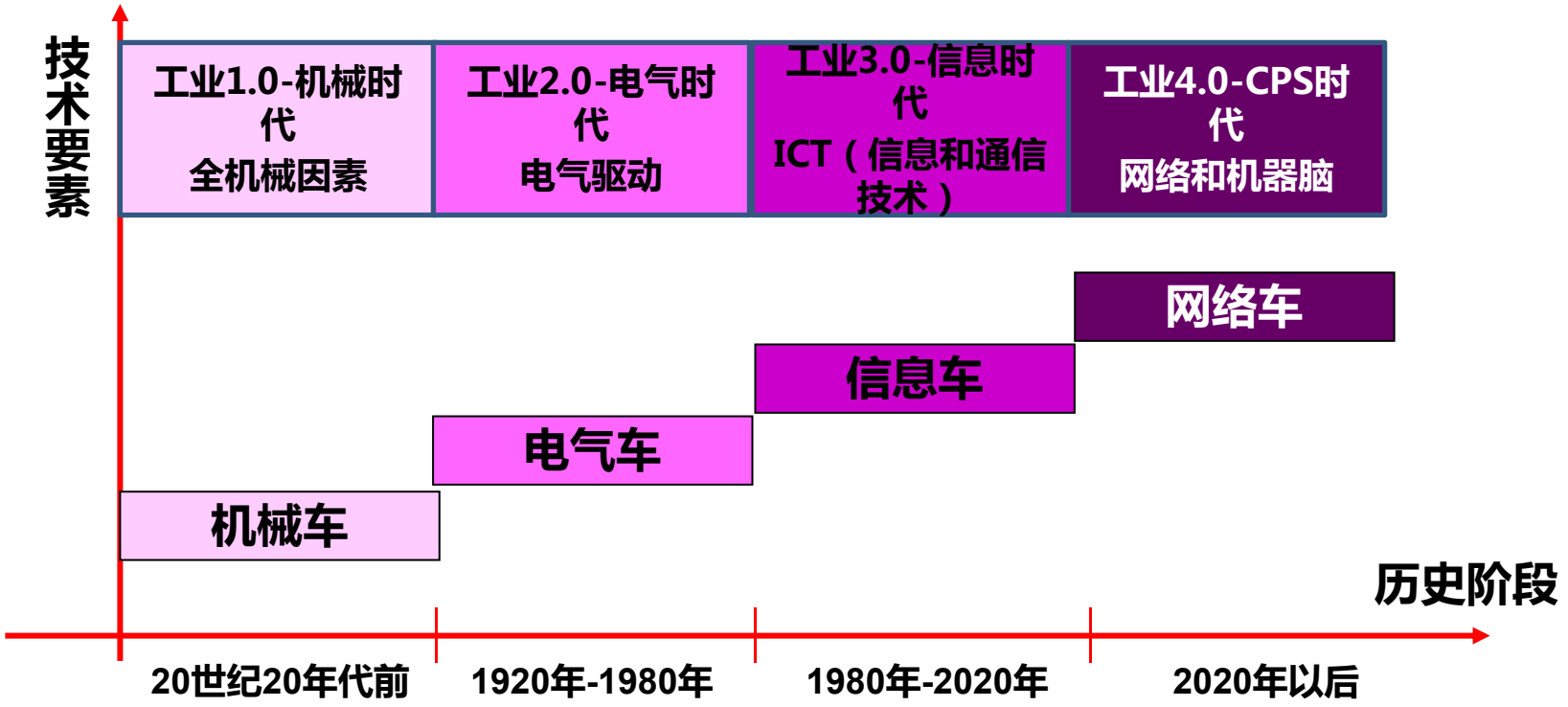
2、某车联网信息安全平台—平台优势

□安全平台优势

低成本架设	• 采用公网传输，与专用硬件传输通道相比，成本低廉，信道后期维护、变更灵活。
安全性保障	• 采用国密认证的IPSEC VPN专用标准，在公网上打造虚拟的安全传输通道。
升级改动小	• 客户端设备仅需支持串口或是以太网通信即可通过软件调整实现安全平台升级。
研发周期短	• 对于客户来讲仅需将数据送入此平台即可，无需关心加密过程。
硬件级加密	• 数据加解密过程硬件实现，并且保证关键数据密钥不出芯片。

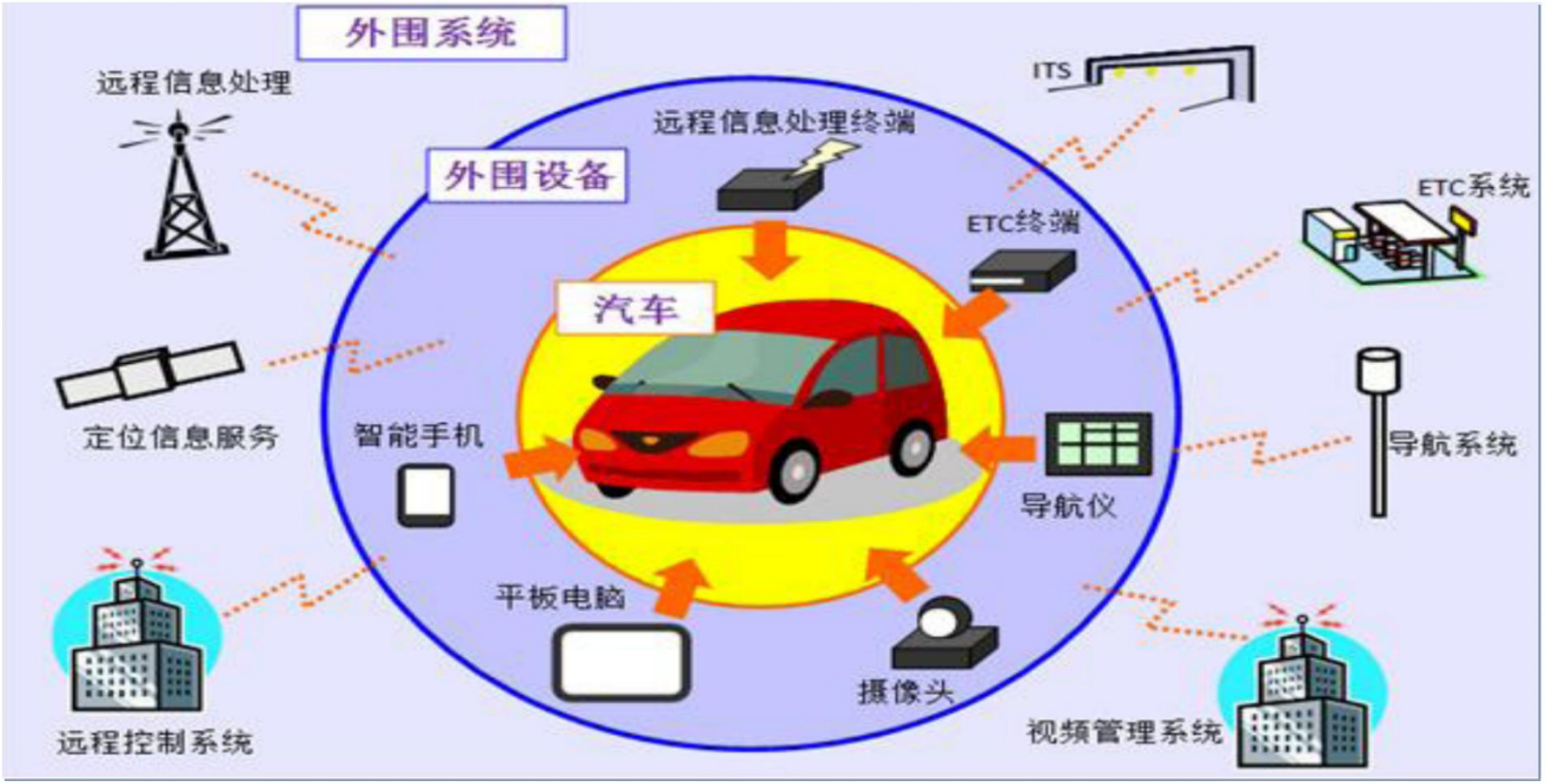
3、未来智能汽车：不同时期特征

□智能汽车不同历史时期的特征要素



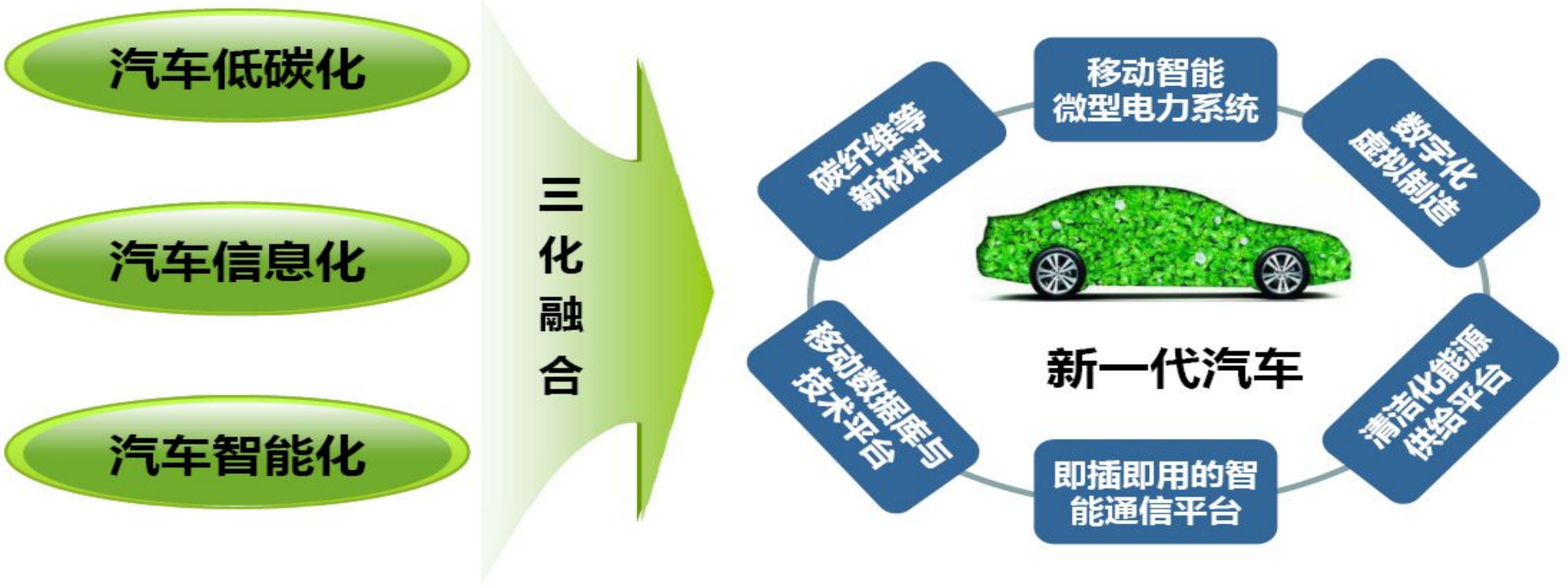
3、未来智能汽车：带轮子的移动信息平台

口带轮子的移动信息平台—更需要信息安全



3、未来智能汽车：更要格外重视信息安全

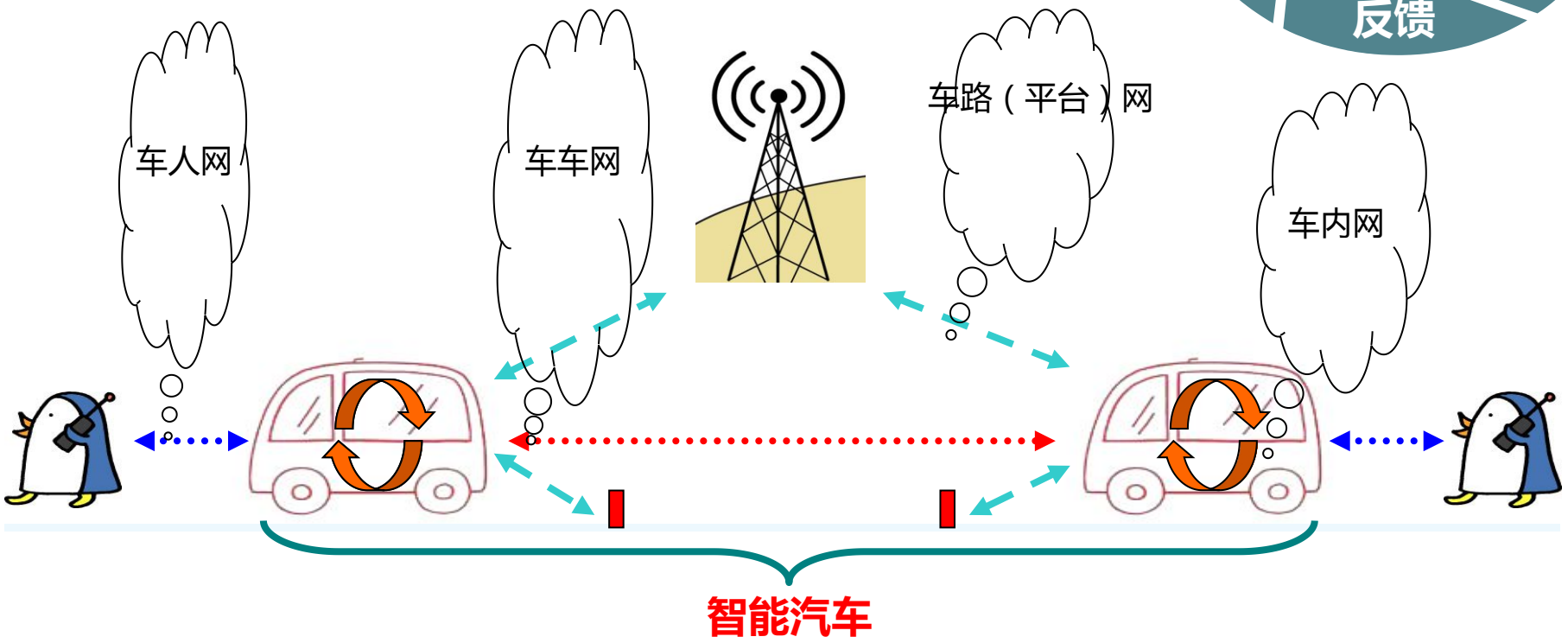
□三化将使下一代汽车发生革命性的变化



- 传统定义汽车电子是汽车的核心竞争力，其中汽车电子内嵌的和软件和软件载体汽车芯片是汽车电子的核心；
- 三化需求下，汽车软件的范畴、定义、功能等发生了变化，参与方也从汽车产业上中下游扩展到与汽车关联的各行各业。

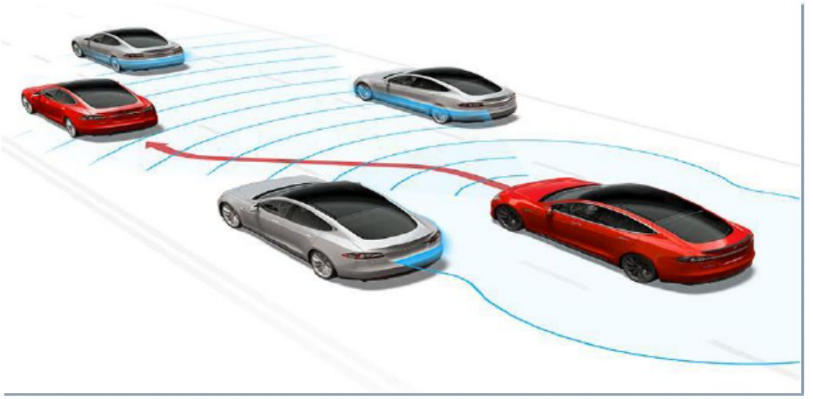
3、未来智能汽车：带轮子的移动信息平台

- **智能汽车定义**：具备感知、决策、执行能力，可以部分或者全部取代人类行为的车辆为智能车辆。
- **智能汽车网络互连**：整个智能汽车系统，用车人网、车车网、车路网、车内网相互链接，行程网略空间。



3、未来智能汽车：更要格外重视信息安全

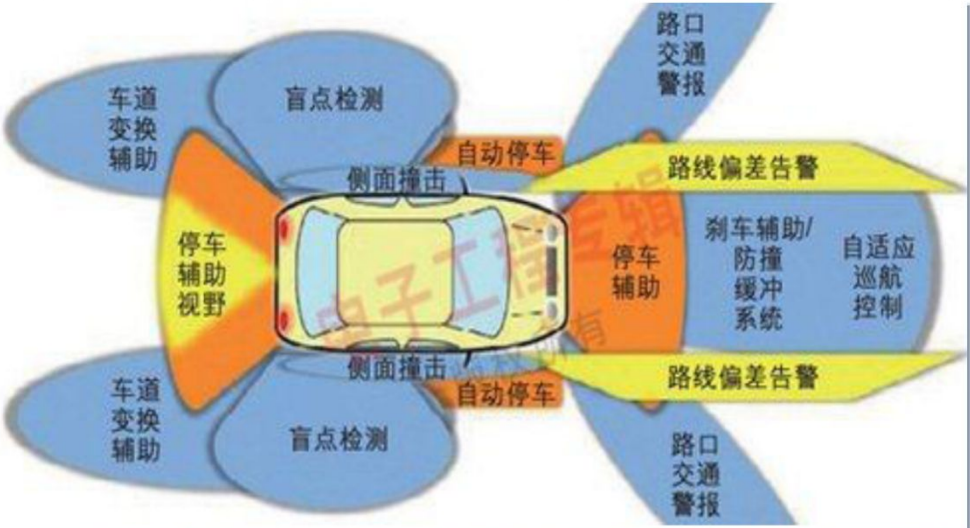
□未来汽车产业价值链的重塑，需求重视信息安全

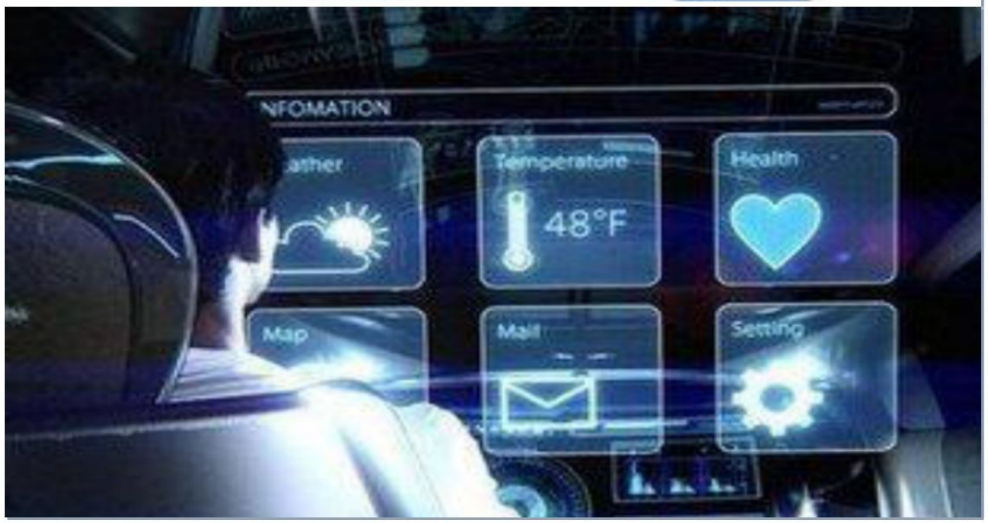


- 可以依靠数据采集、人工智能、视觉计算、雷达、监控装置和全球定位系统协同合作，让电脑在没有任何人类主动的操作下，自动安全地操作机动车辆。
- BCG波士顿咨询预测，**2035年将销售约3000万辆自动驾驶车**，相当于全球新车销量的四分之一。除通用、丰田等传统汽车公司外，谷歌、苹果等也正在加入开发自动驾驶车的行列。

3、未来智能汽车：车辆本身就是智能终端—需要信息安全

口特斯拉未来车型—典型的智能终端





3、未来智能汽车：全新的产品与运营需要安全观念创新

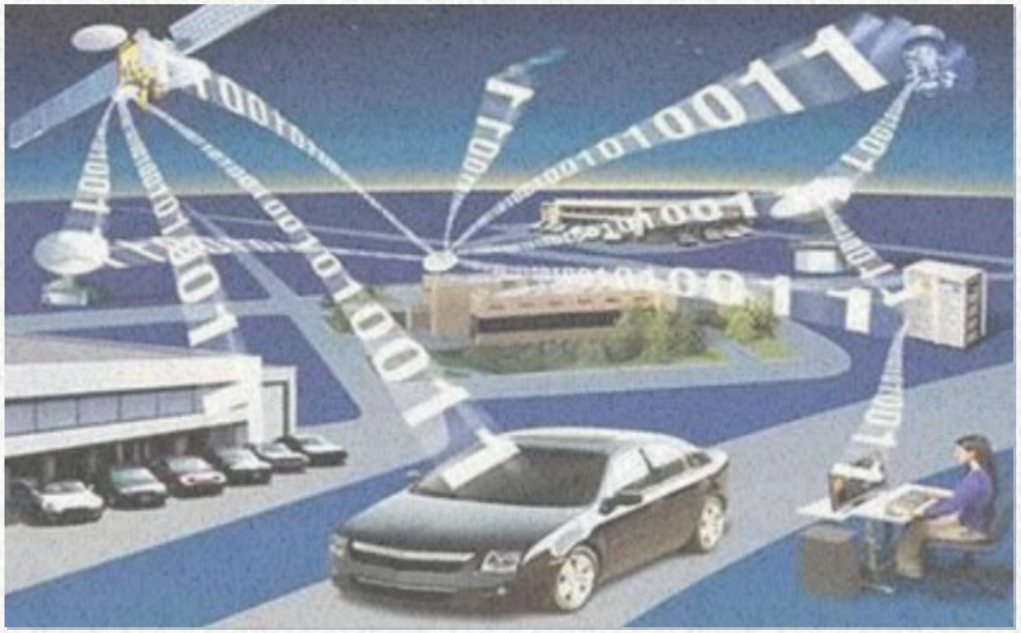
口产品、运营创新—需要信息安全理念创新

信息安全观念需创新

产业政策创新

设计理念创新

管理创新



产业组织创新

产品创新

产业链创新

技术创新

融资模式创新

生产方式创新

应用侧创新

商业模式创新

结束语

回首过去三十载，中国企业取得了举世瞩目的辉煌业绩，让地球人羡慕嫉妒恨！

展望未来，我们更是充满机会与挑战，在“互联网+智能制造”工业4.0新时代，共同迎来了新起点，“大器成于大气，伟业始于微行”，千里之行始于足下，要求我们紧跟时代步伐，打造一大批世界级品牌！铸就新的辉煌！在欣喜取得成就同时，**要时刻紧绷信息安全这根弦。**

丙吉因忧牛喘而不问横道客亡、陈平不谙稻谷之数而成一代贤相，因为分工不同！让我们一起携手努力，分工协作，来改变未来，打造众多知名品牌，进而成为世界品牌，在实现民富国强的康庄大道上，做一颗合格的铺路石子！

美国的创造力 + 欧洲的严谨 + 日本的生产精细化+ 中国企业与时俱进不断创新

=

定将有众多中国企业成就世界一流！

赢

亡—牺牲精神、创业干劲；

口—口碑传播、内实外美；

月—日积月累、不断改进；

贝—利用资源、珍惜平台；

凡—小事做起、脚踏实地！

坚信：中国企业

五项俱全，赢也必然！

共同目标，民富国强中国定赢！！