www.pwccn.com

2016 阿里安全峰会

网络安全与区块链

2016年7月

pwc

普华永道

“A blockchain is a distributed database that maintains a continuously-growing list of data records **hardened against tampering and revision**…”

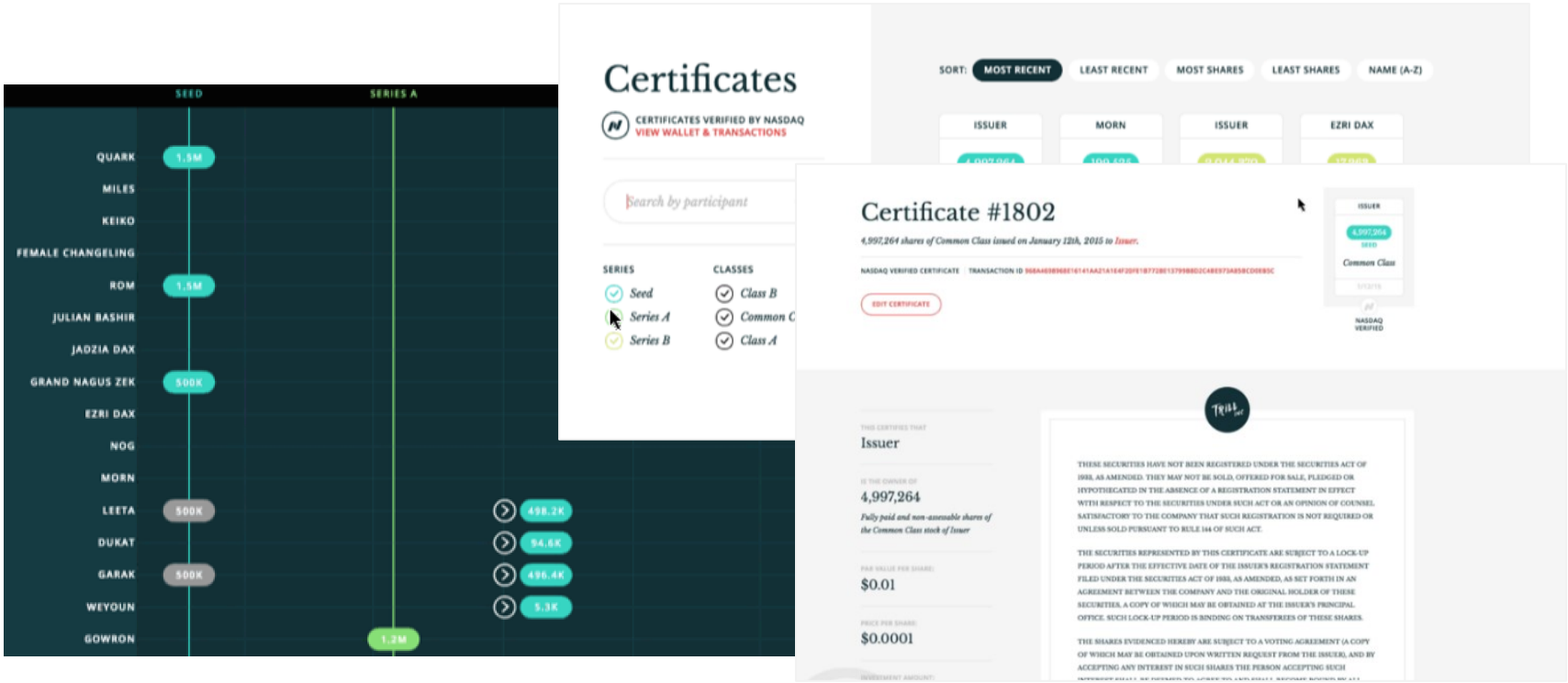
Source: https://en.wikipedia.org/wiki/Blockchain_(database)

当前区块链应用实例

1

LINQ：纳斯达克区块链私募股权市场项目

LINQ：以区块链为基础的平台，支持私人证券发行，是纳斯达克私募股权市场的一部分



产业联盟：R3CEV和中国分布式总账基础协议联盟（Chinaledger）

R3CEV

R3成立于2014年，引领着约50家金融服务企业，致力于金融服务领域区块链技术的发展研究。

2016年4月，R3宣布正在开发Corda —— 一个为金融机构量身定做的分布式总账。

2016年5月，平安集团成为首个加入R3区域块联盟的中国金融机构。

Chinaledger 联盟

Chinaledger 成立于2015年5月，由11 家机构联合发起，致力于共同研究发展符合中国政策法规的区块链技术。

LedgerX

LedgerX 可能是首个由联邦政府监管，为美国的机构参与者设立的比特币衍生品交易所及清算所。目前，它正在等待美国商品期货委员会（CFTC）的监管批准。

中国人民银行

“... 区块链技术是一项可选的技术，其特点是分布式簿记、不基于账户，**而且无法篡改** ... 我们会与金融界、科技界合作，进一步加大对各种新型创新技术的研究和合理利用，优化完善数字货币发行流通的技术框架，并充分预见、及时反应、有效解决在应用推广中可能出现的风险。为此，人民银行殷切希望有关各界大力支持、参与，取得成果，作出贡献。”

中国人民银行行长周小川，《财新周刊》采访，2016年2月

区块链应用潜在领域

贸易执行和结算

资产注册和交易

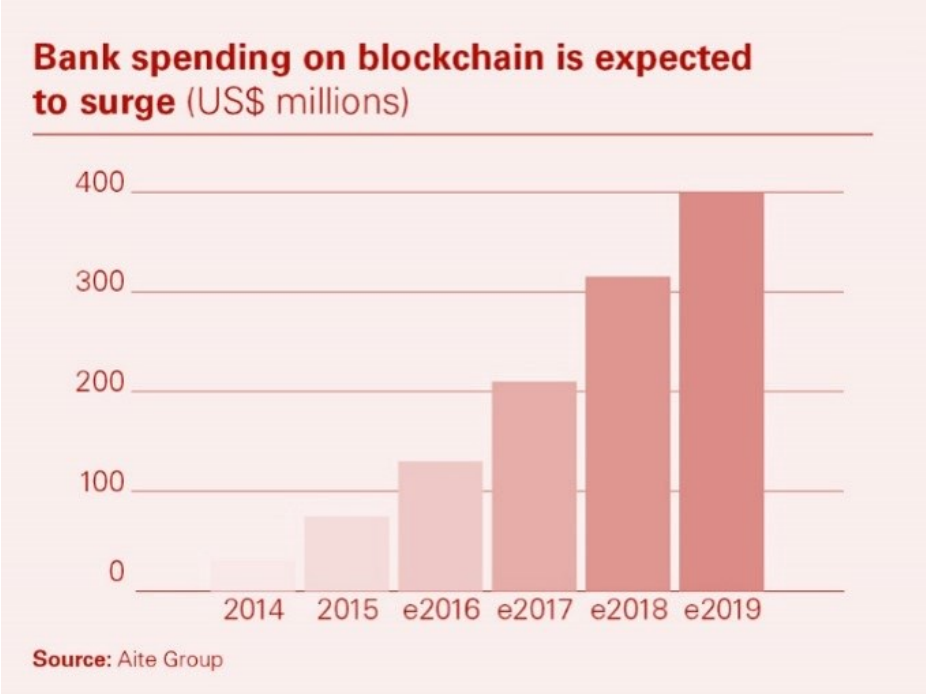
供应链管理

现金储蓄管理

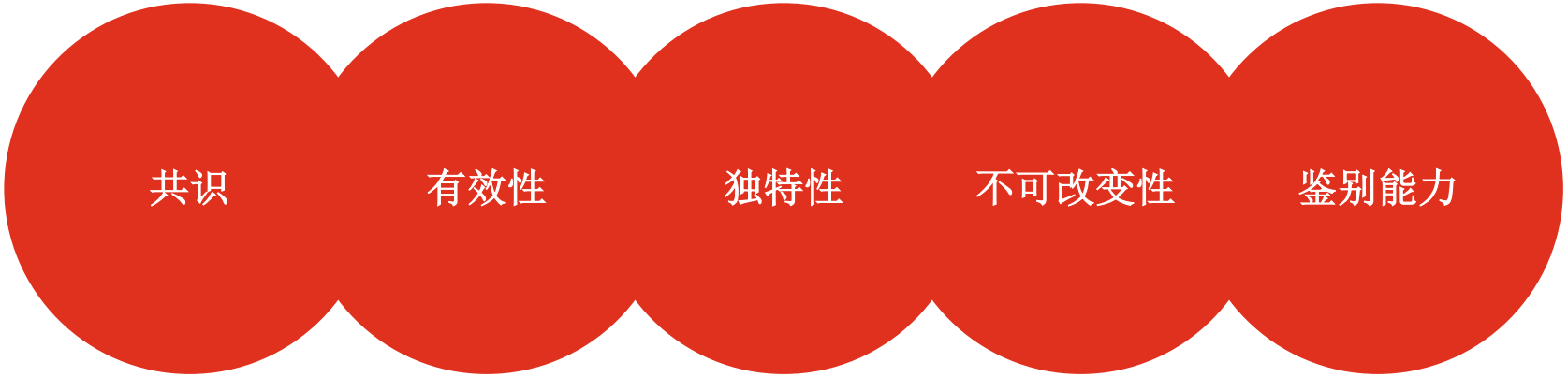
智能合约

智能监管

...



区块链解决方案的主要特点



过往的安全事件

2

Mt.Gox

Then a major Bitcoin-trading website

2014 • 2

Unknown attackers exploited a Mt. Gox's wallet software design flaw to record fake transactions. The flaw allows these attackers to make a withdrawal from their own account and tamper with the record of that transaction. So they could cash out, but claim they never received the Bitcoins.

Impact:

Suspended trading, closed its website and exchange service, and filed for a form of bankruptcy protection

850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $450 million at the time.

Source: http://www.extremetech.com/extreme/176341-mt-gox-tries-to-pin-its-own-incompetence-on-bitcoin-bug

BitStamp
World's largest Bitcoin exchange

2014 • 2

The attack resulted in Bitstamp having to prevent customers from withdrawing their money and blaming a technical glitch. The attack uses transaction malleability to temporarily disrupt balance checking.

Although there was no monetary loss, Bitstamp was unable to process withdrawals consistently.

Source: http://money.cnn.com/2014/02/11/technology/bitcoin-bitstamp/?iid=EL

Impact:

Bitstamp was unable to process withdrawals consistently

Flexcoin
A Bitcoin bank

2014 • 3

Impact:

Hackers stole 896 bitcoin, worth £365,000, and Flexcoin was forced to close after the attack

On 2 March 2014 Flexcoin was attacked and robbed of all coins in the hot wallet. The attacker first created a new Flexcoin account and deposited some bitcoins into it, then successfully exploited a flaw in the code which allows transfers between Flexcoin users by sending thousands of simultaneous requests, the attacker was able to 'move' coins from one user account to another until the sending account was overdrawn, before balances were updated. This was then repeated through multiple accounts, snowballing the amount, until the attacker withdrew the coins.

Source: https://www.theguardian.com/technology/2014/mar/04/bitcoin-bank-flexcoin-closes-after-hack-attack

BitStamp
World's largest Bitcoin exchange

2015 • 1

Attackers used Skype and email to communicate with employees and attempt to distribute files containing malware by appealing to their personal histories and interests. Bitstamp's system became compromised after one systems administrator downloaded a file that he believed had been sent by a representative for an organization that was seeking his membership. Bitstamp suspended operations to investigate the attack, rebuilt its website, deployed new hardware, and implemented other measures to make stealing bitcoins more difficult.

Impact:

Loss of 19,000 bitcoins, approx $5m worth; forced to shut down for almost one week to fix problem

Source: http://www.computerworld.com/article/2865800/hackers-steal-5m-in-bitcoin-currency-during-bitstamp-exchange-attack.html

BTER

Digital currency exchange

2015 • 2

BTER announced loss of 7,170 bitcoins, roughly $1.75 million, in an apparent hack on its cold wallet system.

In a statement posted to the China-based exchange's website, the company said that it had shut down its platform in the wake of the attack and that withdrawals for user balances "will be arranged later".

Impact:

Loss amounted approx $1.75m; forced service shutdown

The stolen funds were broadcast through this transaction, according to the announcement, and the bitcoins appear to have been split into a number of separate wallets since the alleged intrusion.

Source: http://www.coindesk.com/bter-bitcoin-stolen-cold-wallet-hack/

Cloudminr

Bitcoin mining service

2015 • 7

A bitcoin mining service called Cloudminr.io has collapsed, resulting in the loss of bitcoins, the publishing of personal user information and accusations of fraud.

Over one weekend, the main Cloudminr page was altered with an offer to sell a list of passwords, email addresses and usernames for 79,267 individuals. One thousand entries from that list were published on the site at the time. The website is currently offline.

Source: http://www.coindesk.com/bitcoin-cloud-mining-collapse-data/

Impact:

Data leakage resulted in reputational loss and collapse

Purse
Bitcoin mining service

2015 • 10

Purse customer funds were stolen as one of its email service providers had been compromised.

Customers reporting that they had received emails about password resets and withdrawals.

Source: http://www.coindesk.com/customer-bitcoin-stolen-purse-email-breach/

Impact:

Reputational damage and service disruptions

LocalBitcoins
P2P Bitcoin trading

2015 • 11

A fake LocalBitcoins app distributed on the Google Play store in a bid to steal user bitcoins.

Five reviewers on the Google Play store posted claims that their bitcoins had been stolen as a result of downloading the app.

Source: http://www.coindesk.com/fake-localbitcoins-android-app-is-phishing-for-your-bitcoins/

Impact:

Reputational damage; financial loss (if any) not disclosed

ShapeShift
Digital currency exchange

2015 • 11

Impact:

Offline and moved to rebuild the service in a week

ShapeShift lost as much as $230,000 in three separate thefts over the course of a month, and the theft was reported to be an inside job where an employee stole $130,000 from ShapeShift in mid-March.

The employee, who was not identified, later sold sensitive security information to an outside hacker after being fired from the exchange.

Another $100,000 in funds denominated in bitcoin, ether and litecoin were reported stolen on 7th and 9th April.

Source: http://www.coindesk.com/digital-currency-exchange-shapeshift-says-lost-230k-3-separate-hacks/

Gatecoin

Bitcoin and ETH exchange

2016 • 5

Experienced a cyberattack on its hot wallets that resulted in the loss of funds.

"We have previously communicated the fact that most clients' crypto-asset funds are stored in multi-signature cold wallets. However, the malicious external party involved in this breach, managed to alter our system so that ETH deposit transfers by-passed the multi-sig cold storage and went directly to the hot wallet during the breach period. This means that losses of ETH funds exceed the 5% limit that we imposed on our hot wallets."

Source: http://www.coindesk.com/gatecoin-2-million-bitcoin-ether-security-breach/

Impact:

Lost as much as 185,000 ethers and 250 bitcoins, worth approx. $2.14m; the website was offline due to the attack

The DAO
Decentralized Autonomous Organization

2016 • 6

A leaderless organization comprised of a series of smart contracts written on the ethereum codebase.

The DAO lost 3.6m ether, which is currently sitting in a separate wallet after being split off into a separate grouping dubbed a "child DAO".

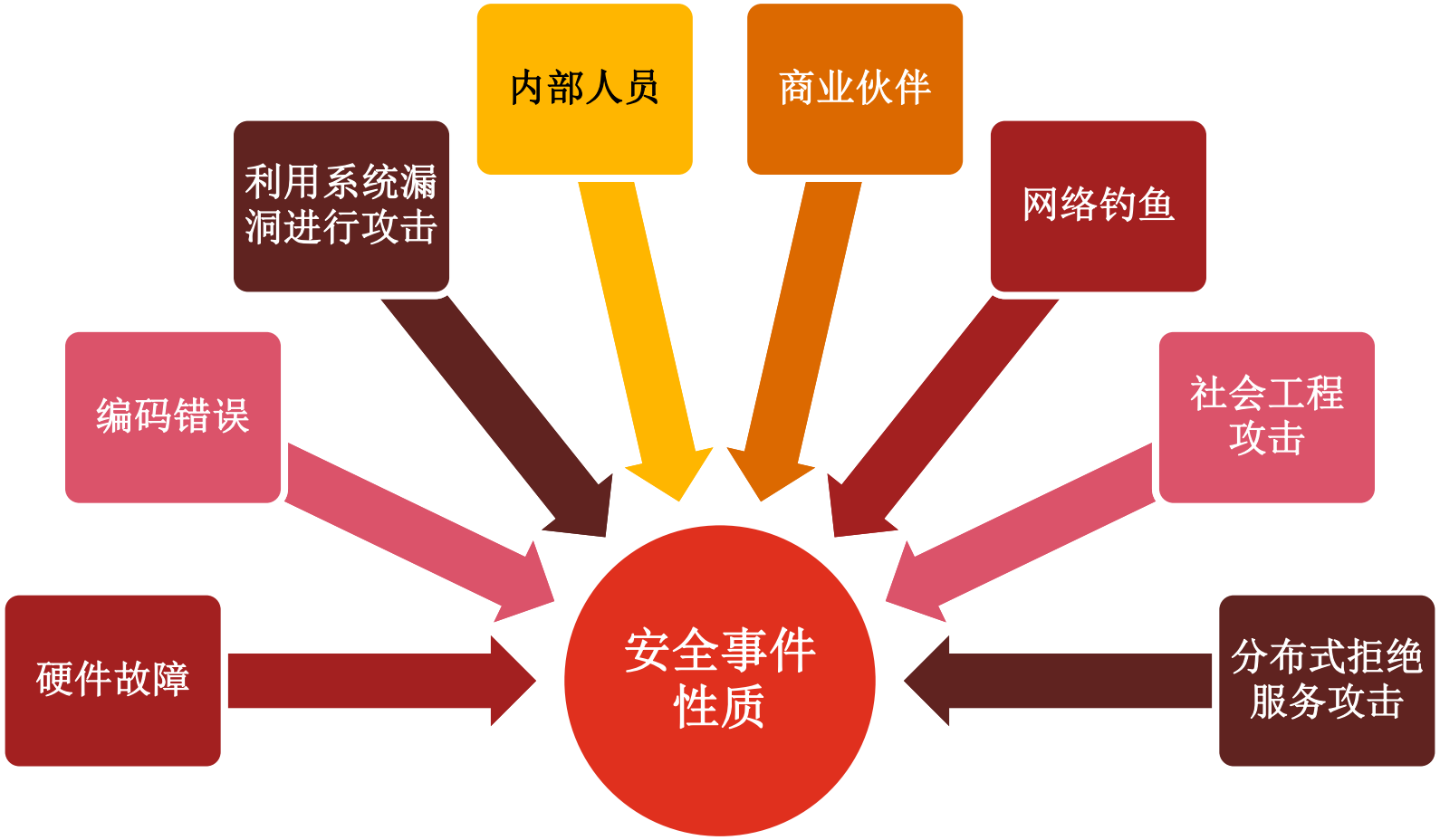
The attack was due to a so-called “recursive call” that could be used to drain some smart contract accounts.

Source: http://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/

Impact:

Lost $60m and triggered a broad market sell-off

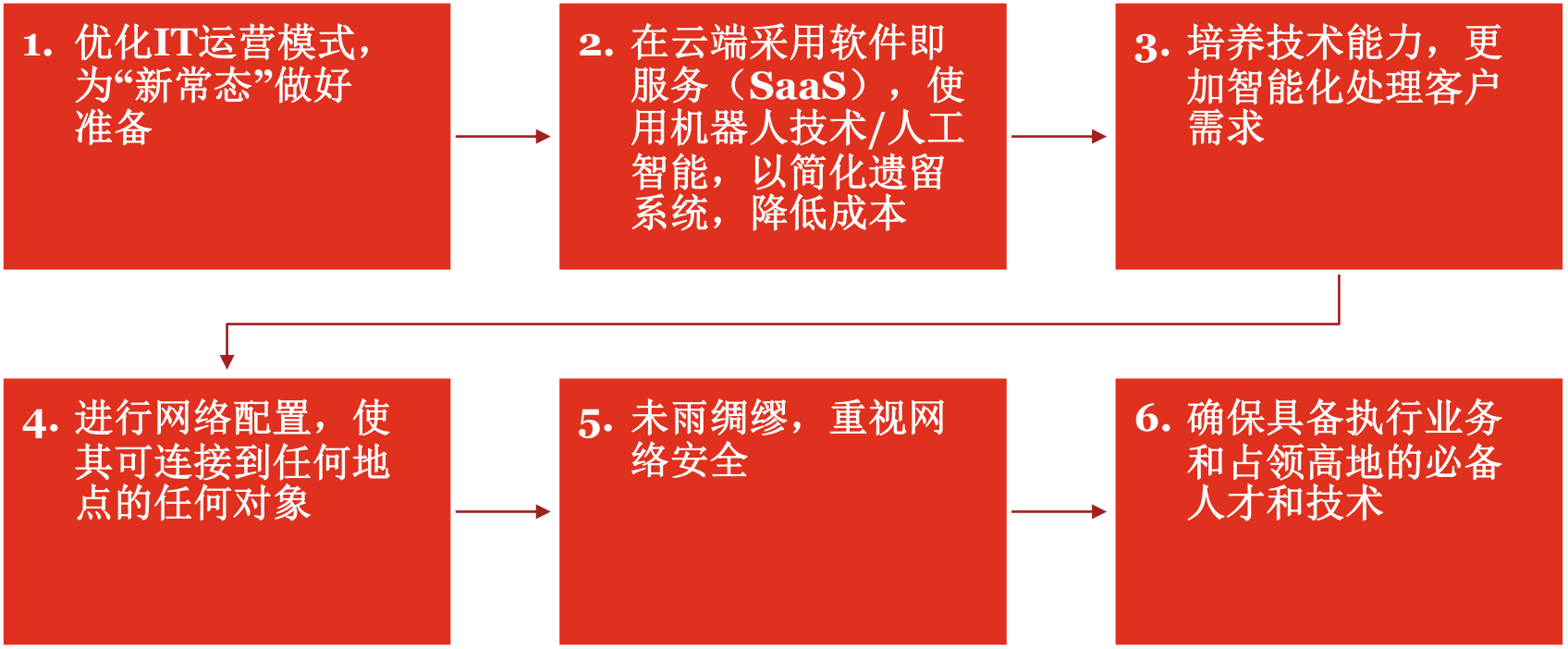
过往的安全事件并不陌生...



回归基本
Back to Basics

3

2020年前六大首要任务



来源：普华永道《2020年及以后的金融服务技术：拥抱干扰》

纵深防御

- 安全意识
- 人员安全
- 安全能力
- 操作规范

- 业务安全
- 应用安全
- 数据安全
- 基础安全

- 计划
- 实施
- 检查
- 改进

信息安全实践


与业务保持一致
优先投资，分配资源，并将组织的安全性能与组织的战略目标和计划保持一致
战略、公司治理和管理
与行业相关的解决方案
结合行业具体的经验和观点，应对企业在所在行业和所服务的市场中面临的相关趋势、挑战和机遇。
通过设计实现保护
创造可持续的安全保护方案，提供基础的功能和操作准则。
安全体系与服务
适应未来
评估新采用的技术和不断变化的商业模型带来的机会和风险。
新兴趋势与创新
威胁和漏洞管理
应对威胁和漏洞
通过对影响商业生态系统的内部和外部因素的情景意识来预测风险环境的变化。
Strategy through Execution
管理风险与合规性
有效地识别、评价和管理业务的风险，同时应对不断变化的法规要求。
风险与合规性管理
身份与访问管理
使用安全访问
提供整体和安全的流程、服务和基础设施，保证对关键的系统和资产进行适当的控制。
威胁、事故和危机管理
预测和应对安全危机
制定危机应对计划，检测和调查安全事故、破坏和妥协，并作出及时、彻底的反应。
信息和隐私保护
保护关键性资产
识别、区分优先级和保护敏感或高值的经营资产。
商业导向的方法——多种功能
利用并整合了自身的业务、技术、管理、分析和调查知识和诀窍，制定可操作并可持续的解决方案。

马上行动：迈向战略性安全管控体系的五个步骤

1. 确保信息安全的管控策略与商业目标一致，符合国家和行业监管要求，并使自身成为战略投资
2. 识别最具价值的信息资产，并优先保护高价值数据
3. 为了减少对各类攻击的响应时间，请充分了解您的对手，包括他们的动机，可能会利用的资源，以及他们会使用的攻击方式等等
4. 评估第三方与供应链合作伙伴的信息安全状况，以确保第三方也同样符合企业要求的安全策略及最佳实践
5. 积极参与多方合作，提高企业对网络安全威胁与应对的意识

谢谢！

联系我们：

季瑞华
合伙人
电话: +86 (10) 6533 2269
邮件: william.gee@cn.pwc.com

冼嘉乐
合伙人
电话: +86 (10) 6533 2937
邮件: samuel.sinn@cn.pwc.com