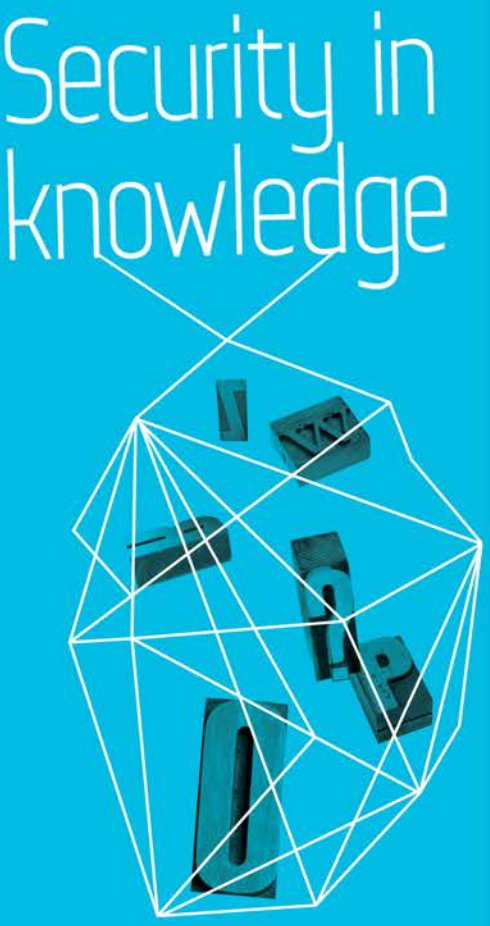
RSA CONFERENCE ASIA PACIFIC 2013



Common IT Security Mistakes Made by Asian Organisations

Paul Craig
Dimension Data

Session ID: SPO-W02B

Session Classification: Intermediate

Who Am I?

- My name is Paul Craig
  - I find problems for a living.
  - Otherwise known as a “ethical hacker” aka Penetration Tester
  - I lead a technical team here in Singapore, at Dimension Data.

  - My career gives me a unique perspective of IT Security.
    - I see the best and the worst of IT Security in Asia.
    - Fortune 50’s / Startups / Multi-national Banks / Wealth Funds / Insurance / Telecommunications / Government

    - I know how most people are doing security, and the mistakes they are making.

A question.

A burning question..

- “As 2013, FSIs still invest heavily into Security and IT Risk; and yet, my team can break into a multinational Asian bank in less than two hours. Why?

- “A show and tell of the mistakes FSI's are making in Asia”
  - The problems that I see…
  - Mistakes implementing Audit, Compliance, Policy and Banking Regulations.
    - A bank that is compli nd practices, considered secure.
    - My team usually ends to steal money.
  - The solutions.

Why does this still happen in one of the most technologically advanced parts of the world?

When we appear to be trying so hard?

Cultural Differences

- Culture and Security – Working in Asia
  - How a business functions and the decisions made are often a result of cultural influence.
  - This can have both positive and a negative impact.
  - This is particularly visible in Asia, where culture can have a large influence on business.
  - Business impacts security.

  - IT security always boils down to people.
    - The decisions one person makes can drastically impact your organizations security stance.
    - Security is never about the process, the policy or compliance.

The bearer of bad news.

- In my career I am usually the bearer of bad news…
  - Boardrooms full: Security Manager, Project Managers, Head of Risk, Head of Audit, CSO/CIO..
    - *I have to tell them that me and my team were able to compromise their bank on the first day. Most of the IT staff and many of the vendors are at fault.*
    - *We had access to pretty much everything..*

Sadly, this is where the security journey begins for some of my clients…

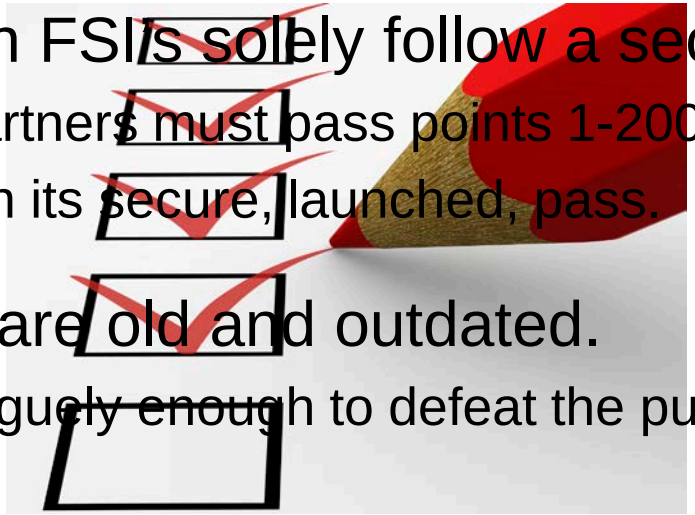
Hostility

- Hostile Situations..
  - No one wants to accept any blame
  - Slow, painful, stressful experience.
  - Asian term “Saving Face”
  - Very little return or value gained by the client.
- Discovering your weaknesses is a good thing
  - Don’t ask the question .. Why did it happen? Who's to blame.
  - Be happy, and ask.. Why did you not know about it previously?

FSI’s who are approach security positively as an organization are typically more secure.

Mistake – checklists

- Security is often seen as a function of Audit
  - Want to see my checklist?”
  - Security is not about a checklist or a tick in the box.
  - Checklists give the appearance of security.
- Frequently Asian FSIs solely follow a security checklist.
  - Vendors and partners must pass points 1-200 of security.
  - If 200 ticks, then its secure, launched, pass.
- Most checklists are old and outdated.
  - OR: Worded vaguely enough to defeat the purpose.



Hackers do not follow checklists.

Mistakes in Policy

- Large Indonesian bank
  - *SO MANY* policy documents.
    - Host Hardening, Network Architecture & Design, Application, ISO 20071.
  - IT Ops team response:
    - *"Have you read the policy documents ?"* – Yes, they are big.
    - *"Did you use them in your production environment?"* - No…
    - *"Why not?"* – "If we follow most of the rules, our environment breaks"

"Why didn't you just tell the Operational Security Team that this policy breaks your environment?"

"It does not work this way, I cannot give feedback to the security team."

Mistake - Security Naivety

- Many FSI's are naive about IT Risk and Security.
- Need to justify security to an organization.
  - "We are not a target for hackers"
  - "This isn't a security risk, you need a high level of skill to impact this"
  - "We have a back-office process that manually validate this"
- I have worked in Forensic Incident Response
- Be assured - Online the Risk is very Real.

Mistake - Underestimated Risk

- The Risk:
  - Meet John Dilinger.
  - His gang robbed two dozen banks and four police stations in the 1920's.
  - **A reporter asked him after he was caught**
    - "Why did you rob banks John?"
  - **He replied**
    - "That's where the money is kept"

  - The Risk is Real - yet still underestimated in Asian businesses.

Mistake – Guideline Interpretation

- Banking Regulations – MAS/HKMA
  - Guidelines supplied by the Monetary Authority of Singapore

    Compliance Checklist for Internet Banking and Technology Risk Management Guidelines aka IBTRM.

  - These checklists have become the de-facto standard for Technical Risk.
  - HKMAS/ MAS / CIB / Central Bank regulation – all very similar.

  - Due to wording of the items the IBTRM can be short-cut and overlooked.

59.	5.2.1 (e)	Perform application security review using a combination of source code review, stress loading and exception testing to identify insecure coding techniques and systems vulnerabilities.

“Just review the source code for 1 day.

We only need partial source code reviewed”

Engage independent security specialists to assess the strengths and weaknesses of internet-based applications, systems and networks before each initial implementation, and at least annually thereafter, preferably without forewarning to internal staff

Quality of the vendor, or vendor selection is not mentioned.

“Independent security specialist”

We need to do this, lets just use the cheapest vendor possible.

That vendor may not even know what MAS or IBTRM is.

Mistake – Rudimentary, Outdated Methodology

- MAS encourages an Audit based approach

> 6.2.2 A methodology approved by senior management should set out how and what system testing[6] should be conducted. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

  - We use an internal methodology for security testing.
    - Application testing methodology is updated every 6 months
    - 92 pages in length.
  - Clients frequently provide us with a 2-3 page Checklist
    - Rudimentary, out-dated, missing items.

  - We are told to strictly adhere to points 1-200 of the checklist
  - Same checklist used last year, and the year before…

Hard Requirements

- Sometimes MAS just makes it hard…
  - Financial institutions within Singapore are fined if they have an outage in production, this fine is also public knowledge.
  - FSI's are also required to perform annual external penetration testing in production.

> 6.2.4 Penetration testing should be conducted prior to the commissioning of a new system which offers internet accessibility and open network interfaces. Vulnerability scanning of external and internal network components that support the new system should also be performed. Vulnerability scanning should be conducted at least quarterly with penetration testing at least yearly.

  - With High Risk, comes a decreased scope, limited testing, very controlled… and in the end, a useless engagement..

Hackers don't care about your scope.

Tender/RFP Issues

- Sometimes security is broken from the Tender / RFP
  - Procurement can influence vendor selection and security.
  - Governments in Asia perform vendor selection through a bulk tender process.
  - Vendor bids and prices are shared, and it becomes a price driven exercise.
    - Cheapest vendor will win!
  - Quality of the security provider is not a factor.
  - Procurement often see IT Risk as Audit.

RFP Issues

- Every year back to RFP…

  "Organizations which go to RFP every year for security vendors have a weaker security posture than those who don't""

  - As an outsider coming into your bank, vendors have zero knowledge of your systems, processes and products.
  - Banks are complex organizations.
  - Clients who engage security partners are often more secure.
    - They work within the Systems Development LifeCycle (SDLC)
    - Deeper Understanding / Better Results / More Security

    VS an outsider who has to 'learn' how your entire bank works.

Mistake – When Company Incentives Go Wrong

- A client once asked us to remove several high severity findings in a report.
  - The findings were legitimate..
- First, a bribe was offered… ”much more work will come”
  - Which was refused….
- At this point we were threatened professionally.
  - Walk away politely.

Behaviour all too common

- Several weeks later I met the same client at a function.
  - “I’m sorry”
  - “My KPI’s and job progression are based on the number of findings in your report. If you give me findings, its bad for me”.
- This attitude is more common than you think…
  - Security managers incentivised on the outcome of security testing.
  - No findings must mean they did their job well.
- It is not uncommon to hear a client say:

  “We want to pass a security review”

Conclusion

- Failing a security review should be your goal and shows value.
- Failing should make you happy.
- Security is not static like an Audit process.
- Security is dynamic – Security is all about People.

- *“The road to hell is paved with good intentions”*
  - Guidelines, Policy, Regulations and Incentives are implemented to help and encourage security.
  - Human element very often reverses this effect.

Thanks for your time.

Questions?