HOLD SECURITY, LLC

REAL THREAT AND REAL DEFENSES

CASE STUDY OF THE UNKNOWN

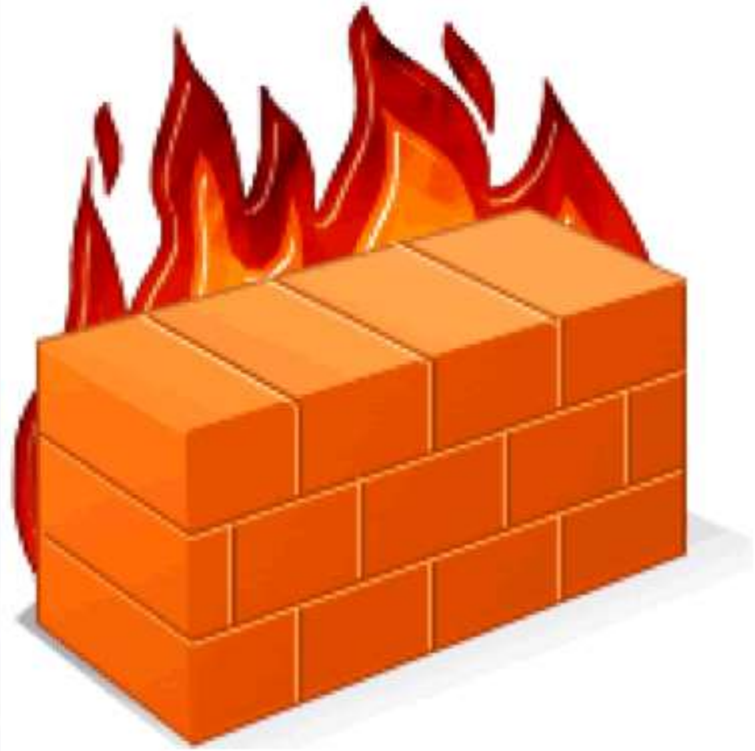
Alex Holden, CISSP
Chief Information Security Officer

INFORMATION SECURITY – EVOLVING TARGET

- Rapid evolution of technology creates ample opportunity for cybercrime to thrive.
- Technology infiltrated our culture faster than education about safety.

LINE OF DEFENSE - TECHNOLOGY

- Firewalls
- Anti-virus
- Encryption
- Monitoring
- Authentication



LINE OF DEFENSE - PEOPLE

- C-suite
- Legal
- Information Technology
- Business Units
- Privacy & Audit

LINE OF DEFENSE - COMPLIANCE

- Laws
- Regulations
- Rules
- Policies

HACKERS – THE OTHER SIDE

- State or Corporate Sponsored
- Hacktivists – Driven by Political or Social Agendas
- Profit Seekers
- Revenge
- Employees

WHO IS THE MODERN HACKER?

MODERN HACKER

- Не говорит по-английски
- Semi-educated
- Lazy
- Money-hungry
- Addicted to drugs, alcohol, gambling

MODERN HACKER

- 99% of hackers fail in their carriers
- On a run from the law
- On a run from competition
- On a run from street gangs

HACKERS VIEW OF US

- War of stereotypes

“I’m fighting a holy war against the West… They drive their Rolls Royces and go home to their million-dollar houses, while people here are struggling. I will never harm my fellow Slavs; but America, Europe, and Australia deserve it.”

- aqua (jabberzeus)

LEARNING FROM EXPERIENCE

- Target Breach 2013
- CyberVor Breach 2013-2014
- Sony Pictures Breach 2014
- Anthem Breach 2014-2015

TARGET BREACH

- Hackers learned from their bad experience with BlackPOS with Verifone POS attempted breach in Russia (Feb-Mar 2013)
- Breach planned for several months
- Botnet breach of a vendor
- A week before the Black Friday – extensive testing
- Two weeks of data collection before putting the data up for sale

TARGET BREACH

- Kartoxa POS Malware author - Rinat Shabaev was looking for a regular job programming, asking for about $12 / hour

- After failing to find any significant project he turns to hacker community who use his skills write malware

THE CYBERVOR BREACH

- **Spam**
  - Credentials
  - Distribution

- **1.2 billion credential breach from 420,000 websites (CyberVor)**
  - Credential attack for hire
    - Spam via email and social media
    - Travel Scams
    - Financial Services
  - Moderate profits

DEFENSE 101

- Understand your enemy
  - Emerging patterns
  - Hackers types
  - Hackers business models

DEFENSE 101 (CONT'D)

Common vectors

- Viruses
- 0-day vulnerabilities
  - Heartbleed
  - Shellshock
  - SQL injection
- Stolen/re-used credentials

ADVISE - QUANTITATIVE ANALYSIS

- Sony breach lessons
- How much of your data is transferred?
- What is normal? What is not?
- Learn to look at statistics

ADVICE - HONEYPOTS

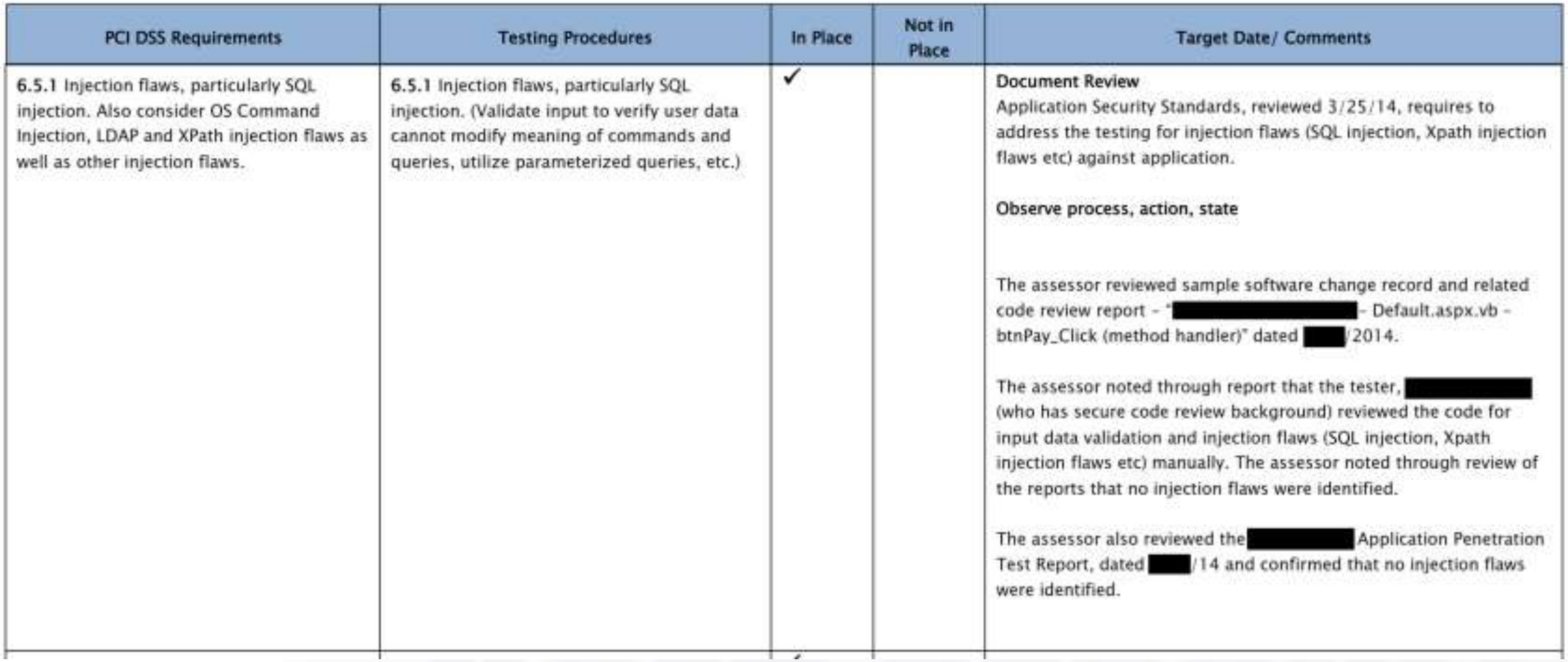
Honeypots are not only systems

- Components
- Credentials
- Features

DEFENSE 101 (CONT'D)

- Regulatory Security
  - Why is it important
- Real-World Security
  - Why it is essential

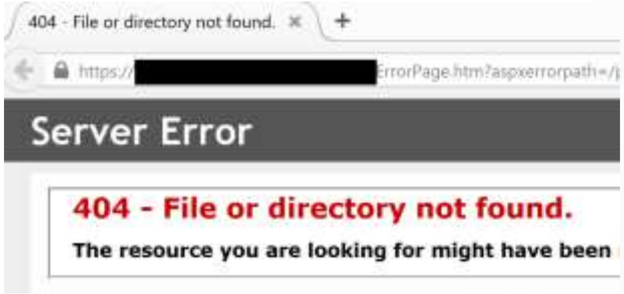
REGULATORY SECURITY



PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**6.5.1** Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)	✓		**Document Review** Application Security Standards, reviewed 3/25/14, requires to address the testing for injection flaws (SQL injection, Xpath injection flaws etc) against application. **Observe process, action, state** The assessor reviewed sample software change record and related code review report - "[redacted]- Default.aspx.vb - btnPay_Click (method handler)" dated [redacted]/2014. The assessor noted through report that the tester, [redacted] (who has secure code review background) reviewed the code for input data validation and injection flaws (SQL injection, Xpath injection flaws etc) manually. The assessor noted through review of the reports that no injection flaws were identified. The assessor also reviewed the [redacted] Application Penetration Test Report, dated [redacted]/14 and confirmed that no injection flaws were identified.

REAL WORLD SECURITY

?b=0 or 1=a--



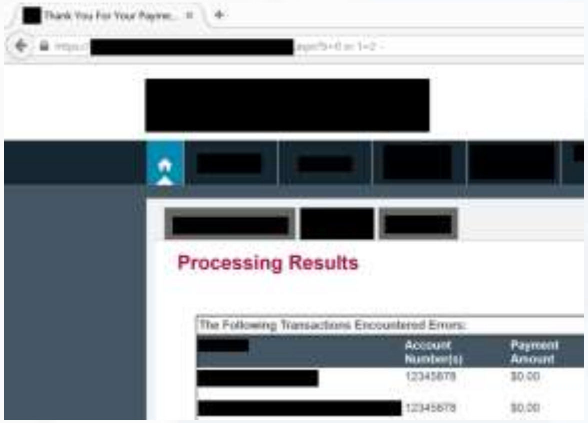
https://[redacted]ErrorPage.htm?aspxerrorpath=/

Server Error

404 - File or directory not found.

The resource you are looking for might have been

?b=0 or 1=2--



https://[redacted]aspx?b=0 or 1=2 --

[redacted]

[redacted] [redacted] [redacted] [redacted] [redacted]

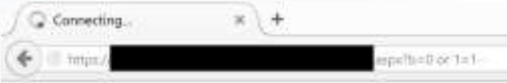
[redacted] [redacted] [redacted]

Processing Results

The Following Transactions Encountered Errors:

[redacted]	Account Number(s)	Payment Amount
[redacted]	12345678	$0.00
[redacted]	12345678	$0.00

?b=0 or 1=1--

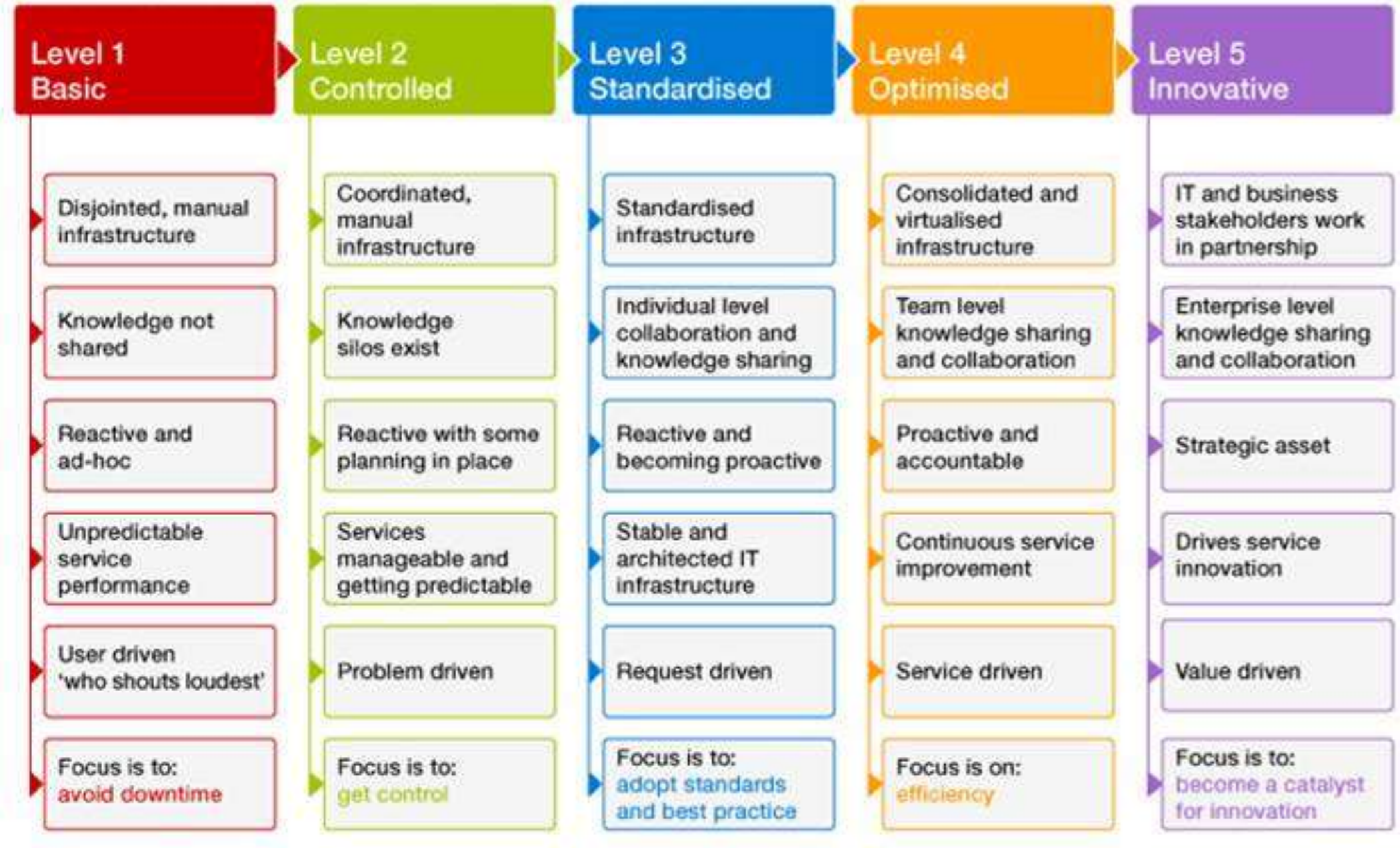


https://[redacted]aspx?b=0 or 1=1--

BREACHES

- You have been breached already
- Look for your data
- Surface Web
- Deep Web
- Dark Web

SECURITY - MATURITY MODEL



Level 1 Basic	Level 2 Controlled	Level 3 Standardised	Level 4 Optimised	Level 5 Innovative
Disjointed, manual infrastructure	Coordinated, manual infrastructure	Standardised infrastructure	Consolidated and virtualised infrastructure	IT and business stakeholders work in partnership
Knowledge not shared	Knowledge silos exist	Individual level collaboration and knowledge sharing	Team level knowledge sharing and collaboration	Enterprise level knowledge sharing and collaboration
Reactive and ad-hoc	Reactive with some planning in place	Reactive and becoming proactive	Proactive and accountable	Strategic asset
Unpredictable service performance	Services manageable and getting predictable	Stable and architected IT infrastructure	Continuous service improvement	Drives service innovation
User driven 'who shouts loudest'	Problem driven	Request driven	Service driven	Value driven
Focus is to: avoid downtime	Focus is to: get control	Focus is to: adopt standards and best practice	Focus is on: efficiency	Focus is to: become a catalyst for innovation

HOLD SECURITY, LLC

ALEX HOLDEN – AHOLDEN@HOLDSECURITY.COM

THANK YOU