Vietnam Security Briefing

IBM Security Team

Crispin Bui
Country Manager – Software
IBM Vietnam
New technologies are changing security challenges

- 1 trillion connected objects
- 1 billion mobile workers
- Social business
- Bring your own IT
- Cloud and virtualization

New technologies are changing security challenges.
New technologies are changing security challenges

1 trillion connected objects

Multiple Mobile Applications

Social business

Consolidation and virtualization

Bring your own IT
We are in an era of continuous breaches

*Attackers are relentless, victims are targeted, and the damage toll is rising*

---

**Operational Sophistication**

IBM X-Force® declared the **Year of the Security Breach**

---

**Near Daily Leaks of Sensitive Data**

- 40% increase in reported data breaches and incidents

---

**Relentless Use of Multiple Methods**

- 500,000,000+ records were leaked, while the future shows no sign of change

---

<table>
<thead>
<tr>
<th>Attack types</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL injection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spear phishing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DDoS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third-party software</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XSS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Watering hole</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undisclosed</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2014

Note: Size of circle estimates relative impact of incident in terms of cost to business.
Cyber attacks are much closer to home than we think...below are some incidents that happened in 2014 in ASEAN countries.
Is there a disconnect?

Where are your “security risks” vs your “spend”?

Source:
The State of Risk-Based Security Management,
A Research Study by Ponemon Institute, 2013
Early detection and rapid response are the best defense against rising cyber threats and sophisticated attacks. Compromises take days or more to discover in 96% of cases; and over 91% weeks or more to contain.

<table>
<thead>
<tr>
<th>Time span of events by percent of breaches</th>
<th>Seconds</th>
<th>Minutes</th>
<th>Hours</th>
<th>Days</th>
<th>Weeks</th>
<th>Months</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Attack to Initial Compromise</td>
<td>10%</td>
<td>75%</td>
<td>12%</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Initial Compromise to Data Exfiltration</td>
<td>8%</td>
<td>38%</td>
<td>14%</td>
<td>25%</td>
<td>8%</td>
<td>8%</td>
<td>0%</td>
</tr>
<tr>
<td>Initial Compromise to Discovery</td>
<td>0%</td>
<td>0%</td>
<td>2%</td>
<td>13%</td>
<td>29%</td>
<td>54%+</td>
<td>2%</td>
</tr>
<tr>
<td>Discovery to Containment/Restoration</td>
<td>0%</td>
<td>1%</td>
<td>9%</td>
<td>32%</td>
<td>38%</td>
<td>17%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Criminals attack the weak link

Employee / Customer Protection

Anti Virus

Employees / Customers / Partners

Easy

Cyber Criminals

Difficult

Firewall

Intrusion Prevention System

Anti-Virus Gateway

Encryption

Customer Data and Intellectual Property

Enterprise Protection
Malware and Phishing: Common threat to Customers and Employees

Three Losing Battles
- Humans will always make mistakes
- System and application vulnerabilities continue to emerge
- Malware detection will always lag

Two Major Impacts

Widespread Fraud
- $3.4B est lost to online fraud in 2012\(^1\)

Advanced Threats and Breaches
- 85% of breaches go undetected\(^2\)
- $8.9M average cost of cyber-attacks\(^3\)

\(^1\)JPMorgan: 2012 Online Fraud Report , \(^2\)Gartner: 2290415 , \(^3\)Ponemon Institute: 2012 Cost of Cybercrime Report: US
IT Security is a board room discussion

Increasingly, companies are appointing CROs and CISOs with a direct line to the Audit Committee.

- **CEO**
  - Loss of market share and reputation
  - Legal exposure

- **CFO/COO**
  - Audit failure
  - Fines and criminal charges
  - Financial loss

- **CIO**
  - Loss of data confidentiality, integrity and/or availability

- **CHRO**
  - Violation of employee privacy

- **CMO**
  - Loss of customer trust
  - Loss of brand reputation

Source: Discussions with more than 13,000 C-suite executives as part of the IBM C-suite Study Series
Security Silos FAIL!

MAXIMUM SECURITY ENTRANCE
IBM Security Systems
IBM helps protect against new, complex security challenges

**IBM helps clients…**

1. **Stop advanced threats**
   *Use analytics and insights for smarter defense*

2. **Secure cloud and mobile**
   *Employ cloud and mobile to improve security*

3. **Optimize security program**
   *Integrate security silos, reduce complexity, and lower costs*

---

**IBM Security**

- **Top 3** enterprise security software vendor in total revenue
- **13** industry analyst reports rank IBM Security as a LEADER
- **133** countries where IBM delivers managed security services
- **24** of the top 33 banks in Japan, North America, and Australia
IBM Security

*Integrated capabilities delivered across a comprehensive security framework*

The IBM Security Framework

- **Strategy, Risk and Compliance**
  - Security Intelligence and Analytics
    - Advanced Fraud Protection
    - Advanced Security and Threat Research
  - Managed, Cloud, and Professional Services

- **Detect, analyze, and prioritize threats**
  - QRadar

- **Reduce fraud and malware**
  - Trusteer

- **Manage users and their access**
  - Identity and Access Management

- **Discover and harden valuable assets**
  - InfoSphere Guardium

- **Secure critical business applications**
  - AppScan

- **Protect infrastructure against attacks**
  - Network and Endpoint Protection

- **Monitor and evaluate today’s threats**
  - IBM X-Force
At IBM, the world is our security lab

6,000+ IBM researchers, developers, and subject matter experts focused on security

3,000+ IBM security patents
IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape

The IBM X-Force Mission

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow’s security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter
Security Intelligence: Embedded intelligence to find true offenses

Extensive Data Sources

- Security devices
- Servers and mainframes
- Network and virtual activity
- Data activity
- Application activity
- Configuration information
- Vulnerabilities and threats
- Users and identities
- Global threat intelligence

Embedded Intelligence

- Automated data collection, asset discovery and profiling
- Automated, real-time, and integrated analytics
- Massive data reduction
- Activity baselining and anomaly detection
- Out-of-the-box rules and templates

...Suspected Incidents

True Offenses

Automated Offense Identification
### The IBM fundamental approach to threat protection

#### VULNERABILITY vs. EXPLOIT

- **VULNERABILITY:** A weakness in a system
  - Can be used to do something unintended
  - Can be exploited in multiple ways

- **EXPLOIT:** A method used to gain system entry
  - Many different exploits can target a single vulnerability
  - Not all exploits are publicly available, and mutation is common

#### IBM PROTECTION vs. OTHER PRODUCTS

- **IBM PROTECTION:** IBM protects the vulnerability
  - Stays ahead of the threat with pre-emptive protection that stops things from breaking the window

- **OTHER PRODUCTS:** Other products only block the exploits
  - Looks for methods that can break the window
  - Keeping up can be challenging
Avoiding the Shock

IBM’s preemptive security helps protect customers against the Bash “Shellshock” vulnerability.

IBM Security Network Protection XGS

6.12.2007
IBM X-Force releases heuristic protection for Shell Command Injection

CVE-2014-6271 (better known as Shellshock) is disclosed and exploitation begins. IBM Security customers already have protection

Shellshock disclosed and exploits begin

9.25.2014
Network Security vendors publish Signatures

Ongoing
Exploits expected to mutate, requiring new Signatures

IBM Security Network Protection XGS is the only network security solution to offer protection 2661 days before impact.
Four truths about advanced threat protection

Despite increasing challenges, organizations can protect themselves by adopting the right strategy

1. Prevention is mandatory
   Traditional methods of prevention have often failed, leaving many to believe detection is the only way forward. This is a dangerous proposition.

2. Security Intelligence is the underpinning
   Specialized knowledge in one domain is not enough. It takes enterprise-wide visibility and maximum use of data to stop today’s threats.

3. Integration enables protection
   The best defense is relentless improvement. Technologies must seamlessly integrate with processes and people across the entire lifecycle of attacks.

4. Openness must be embraced
   Security teams need the ability to share context and invoke actions between communities of interest and numerous new and existing security investments.
IBM is uniquely positioned to offer integrated protection

1. Smarter Prevention
   - Trusteer Apex Endpoint Malware Protection
     - Java Lockdown Protection - granular control of untrusted code, cloud-based file inspection, and QRadar integration
   - IBM Security Network Protection XGS
     - Advanced Threat Quarantine integration from QRadar and third-party products, inclusion of Trusteer intelligence into XGS

2. Security Intelligence
   - IBM Security QRadar Security Intelligence
     - Data Node appliance, new flow and event APIs, and vulnerability management improvements
   - Threat Monitoring and Intelligence Services
     - Managed SIEM enhancements, new cyber threat intelligence

3. Continuous Response
   - IBM Security QRadar Incident Forensics
     - Integrated forensics module with full packet search and visual reconstruction of threat actor relationships
   - IBM Emergency Response Services
     - Increased global coverage and expertise related to malware analysis and forensics

4. Global Threat Intelligence
   - IBM X-Force Threat Intelligence
     - New virtual real-time sharing of Trusteer threat intelligence from 100M+ endpoints with X-Force

5. Open Integrations
   - Ready for IBM Security Intelligence Ecosystem
     - New functionality from partners including FireEye, TrendMicro, Damballa and other protection vendors
Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Thank You

www.ibm.com/security