One step ahead
Security lessons learnt

Petr Hněvkovský, CISA, CISSP
HP Enterprise Security

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Experts Marvel At How Cyberthieves Stole $45 Million

Global Network of Hackers Steal $45 Million From ATMs

In Hours, Thieves Took $45 Million in A.T.M. Scheme

The Circuit: Hackers took $45 million in ATM heist
$45M stolen
...in a matter of hours
but planned over a number of years...
“If you know the enemy and know yourself, you need not fear the result of a hundred battles.”

—Sun Tzu, The Art of War
Challenges you are facing

1. Nature and motivation of attacks
   (Fame to fortune, market adversary)

2. Transformation of enterprise IT
   (Delivery and consumption changes)

3. Regulatory pressures
   (Increasing cost and complexity)

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Organize our capability to disrupt the market

Research -> Infiltration -> Discovery -> Capture -> Exfiltration

Our enterprise

Their ecosystem

$ $ $ $
Rethink our capability investments

Our enterprise

Their ecosystem

Exfiltration

Infiltration

Discovery

Capture

Research

5X

1X

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Organize our capability to disrupt the market

**Educating users**
**Counter intel**

**Their ecosystem**

**Our enterprise**

**Infiltration**

**Discovery**

**Capture**

**Exfiltration**
HP Security Research (results known as TippingPoint)

Microsoft Vulnerability Discoveries

Adobe Vulnerability Discoveries

The stats are compiled from public data http://www.microsoft.com/technet/security/current.aspx
Organize our capability to disrupt the market

- Educating users
- Counter intel
- Blocking access
- Discovery
- Capture
- Exfiltration

Their ecosystem

Our enterprise

$ $ $ $ $ $ $ $ 

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
84% of breaches occur at the application layer.
9/10

Of 1000 Fortune applications are vulnerable
Organize our capability to disrupt the market

- Educating users
- Counter intel

Blocking access

Their ecosystem

Finding them

Capture

Our enterprise

Exfiltration

Educating users

Counter intel

Blocking access

Their ecosystem

Finding them

Capture

Our enterprise

Exfiltration
243 days average time to detect breach

2014 January February March April May June July August September October November December 2015
94% of breaches are reported by a 3rd party
Organize our capability to disrupt the market

- Educating users
- Counter intel
- Blocking access
- Finding them
- Protecting the target asset
- Planning damage mitigation
- Their ecosystem
- Our enterprise

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
The resolve an attack has grown since last year.
Use our intelligence
HP Security

Disrupt the adversary, manage risk, and extend your capabilities

Disrupt the adversary
Security technology

Manage risk
Risk & compliance

Reduce cost & complexity
Advisory & management

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
HP’s industry-leading scale

- **Monthly security events**: 2.3 billion
- **HP Secured User Accounts**: 47 million
- **HP Security Professionals**: 5,000+
- **Top telecoms**: 10 out of 10
- **Top software companies**: 9 out of 10
- **Major banks**: 9 out of 10
- **Top telecoms**: 10 out of 10
- **US Department of Defense**: All major branches
- **Global Security Operations Centers**: 8
- **Planned regional SOC**: 8
- **HP managed security customers**: 900+
I follow ISO, PCI and other security standards.

Our predictability is well known.

I work within budget cycles.

I stitch technology together across functions.
Defining the adversary

Cybercrime
- Market with distinct process
- Organize and specialize
- Intelligence is bought and sold

Hacktivist

Nation state

The adversary
Industry Leading Scale

8 Global Cyber Centers

- Global cyber centers
- Planned regional centers

Monthly Security Events: 2.3bn
HP Managed Security Customers: 900+
HP Security Professionals: 3000+
HP Secured User Accounts: 47m

>35 innovative new security products & services released in the last 12 months