ISE North America Leadership Summit and Awards

Nominee Showcase Presentation

October 27- 28, 2010

Company Name:	PayPal
Project Name:	Why every company needs an ISG team
Presenter:	Michael Barrett
Presenter Title:	Chief Information Security Officer

TEN
TECH EXEC NETWORKS

PayPal Overview

- PayPal is the leading global online payments company
- Roughly 6,000 employees
- Annual revenue of $2.8bn in 2009
- A global company with 90mm active online customers in 190 countries
- Total payment volume continuing to grow rapidly - 26% YoY

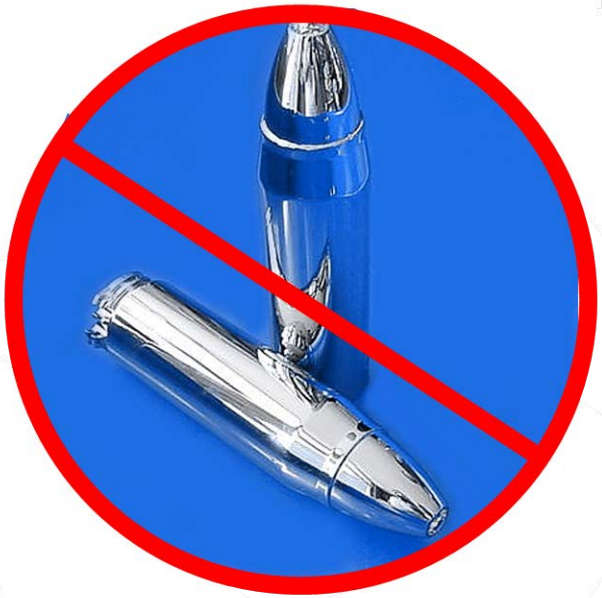
All CISOs wear two hats, whether we know it or not

Herding the cats inside our organization

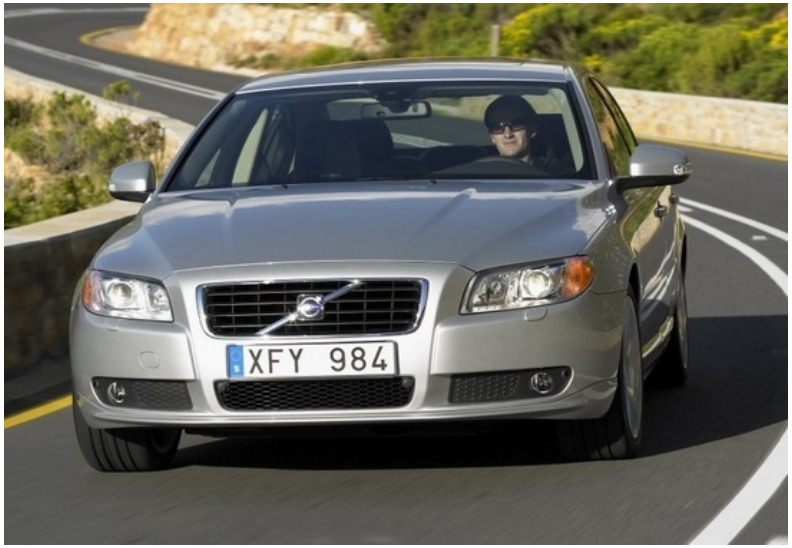
Ensuring that the hordes of Huns and Visigoths don't overrun Rome

It's apparent that our profession knows what to do with the first role, but we haven't yet collectively worked out how to deal with the second…

This is not an easy problem...



Build your walls higher, but you can't *directly* stop criminals from abusing your customers



Q: Who's responsible for road safety?
A: Shared responsibility of Government, Industry and vehicle owners & drivers.
Then substitute "Internet" for "road" and re-ask the question…

If it's an ecosystem problem, what are the parameters of the solution?

- We think there are three main aspects:
  - Broken Internet technology standards
  - Ineffective Internet governance
  - Necessary regulation is not in place / government doesn't (yet) understand its responsibilities

Broken Internet technology standards

- Routing can be compromised
- Trust boot model is weak (DHCP, bootp, etc.)
- Same Origin policy
- Browsers assume HTTP; server redirects to HTTPS (we addressed this via STS, in IETF)
- The entire SSL edifice rests on the integrity of the CA ecosystem
- etc.

Ineffective Internet governance

- After the Kaminsky DNS break, it became apparent that DNSSEC implementation was urgently needed – where were you?
- Many issues within the Internet ecosystem can be directly attributed to weak policing by appropriate stakeholders:
  - Slow shutdown of evidently criminal domains by (thin) registries
  - Poor quality whois information
  - etc.

Necessary regulation is not in place / government doesn't (yet) understand its responsibilities

- Little understanding yet of what the right regulatory model should look like
- We assert that:
  - It should try to minimize negative externalities
  - Do the things that free markets cannot
  - Do no more than is needed

A call to action

- We all need to get involved
- Educate yourself on the issues
- Don't try to tackle this at scale – pick one topic that you have passion around, where you think that you may be able to make a difference, personally

"Whether you think you can, or whether you think you can't, you're right." Henry Ford

Thank you and Questions

- Questions?