# NEXTGEN THIRD PARTY SECURITY

NATIONAL SUMMIT - THINK TANK

THIEN LA
VP and CISO

# INDUSTRY TRENDS

- In 2017, 56% of companies experienced a third party data breach (+17% from 2016)
- On average, US companies paid $7.3M per breach
- 57% of companies don’t have a complete third party inventory (with whom they share data with)
- 60% of companies feel unprepared to verify their third parties (down from 66% in 2016)
- 15% of companies said that their boards are more involved with third party risk management
- Major breaches: Target, Hancock (recent)

# THIRD PARTY SECURITY UTOPIA

I can manage and monitor my data and business functions at Third Parties as if it was internal

Can I install monitoring software at your facilities sir?

Can I run unannounced penetration tests against you?

… this is not happening anytime soon.

# OBJECTIVES

1. **I**nventory – enumerate and classify.  Do you know all your third parties?
2. **P**artner – engage and assist (they are now in your family, e.g. like a nanny)
3. **R**igor – pre-assessments, surveys, on-site assessments, pen tests, watermark your data, risk framework and governance
4. **O**ngoing – vendors change their infrastructure
5. **B**usiness – relationships, requirements, training, avoid shadow IT
6. **E**nact (Legal Contract) – strong language, penalties ?

**Does it all come down to leverage?  Who has the upper hand?**

# SCENARIOS

1. Tier 1.  No pen test.  Automatic high risk?  Don’t pay for it
2. Tier 1.  Vendor won’t share anything.  They are the “only game in town”..
3. Tier 1.  They host your data at another vendor.
4. Tier 1.  They use cloud.
5. Tier 2.  Shrink wrapped software that sends data out.

# THANK YOU!