



**BlackBerry®**

---

**CYLANCE®**

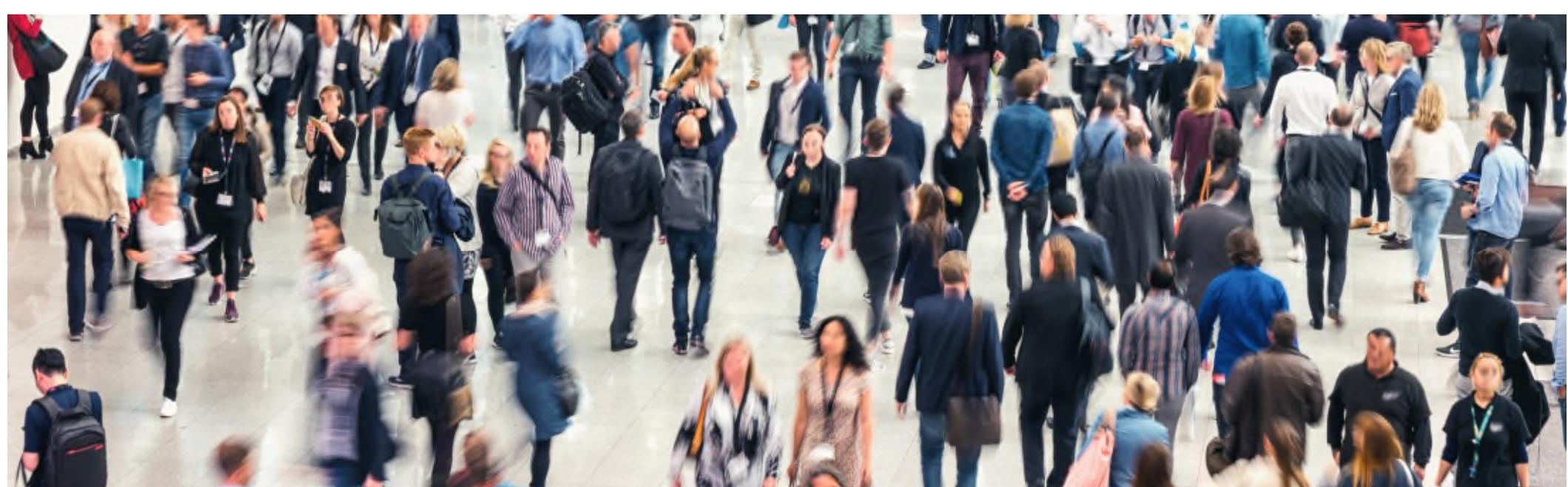
## **The Reality and Impact of IP Theft**

**Debevoise  
& Plimpton**

# What is IP?

---

- There is a lack of understanding of what IP is
  - How it is created?
  - How it is handled?
  - Who owns it?
  - Where does it go?
- This is very much a human problem
  - People can be adapted to a workflow



# Why Steal Data?



## Financial targets

(experimental formulary, clinical trials database, acquisition timing plans, pre-public news EDGAR)



## Disrupt what you are doing

(copy patent filing, R&D operations, company integration, distraction)



## Reputation damage

(psychological, blackmail)

# Threat Assessment

- Understand why a company is targeted and realize by whom they are targeted
- How is data exfiltrated
  - Where does it go?
  - Can it be tracked?
  - DRM?
- What role does malware play in the overall IP theft arena
  - How can it be stopped?
- Is it easier to walk in the front door?

# Case Law

---

- 1. AMSC Sinovel – wind turbines**  
<https://www.justice.gov/opa/pr/chinese-company-sinovel-wind-group-convicted-theft-trade-secrets>
- 2. Monsanto / Dupont seeds theft**  
<https://www.justice.gov/opa/pr/chinese-national-sentenced-prison-conspiracy-steal-trade-secrets>
- 3. GSK pharma theft**  
<https://www.justice.gov/usao-edpa/pr/second-former-glaxosmithkline-scientist-pleads-guilty-stealing-trade-secrets-benefit>
- 4. Dupont Kevlar theft**  
<https://www.fbi.gov/contact-us/field-offices/richmond/news/press-releases/kolon-industries-inc.-pleads-guilty-for-conspiring-to-steal-dupont-trade-secrets-involving-kevlar-technology>

# Where to Focus

---

IP cannot be insured so there is a need to have human/policy and technical safeguards in place

Management ownership of IP protection

Data Classification strategy and application

Contracts, onboarding process and agreements, security policies/procedures

Physical plant security/access

# Best Practices & Closing Thoughts

---

- Understand the data you create, disseminate, and utilize in your environment
- Understand the value that data can have both privately and publicly
  - Does someone having public data early give them an advantage?
- Prepare yourself to be a target of interest even if you're not
  - Someone you're associated with may be
- Design your defenses to prevent infection, deter persistence, and isolate critical data access
- Not all IP is generated or stored in computers, many research organizations still use notebooks and store scans
  - The source of the IP is as valuable as its digital version

# Luke Dembosky

---



## **Partner**

*Debevoise & Plimpton*

Luke Dembosky co-chairs Debevoise & Plimpton’s global cyber and data privacy practice and is recognized as a leading practitioner by *Chambers*, *The Legal 500*, and the *National Law Journal*. He joined the firm in March 2016 after 14 years specializing in cyber matters for the Justice Department, including as Deputy Assistant Attorney General for National Security over DOJ’s first national security cyber portfolio; Deputy Chief for Litigation at the Computer Crime and IP Section; DOJ representative at the U.S. Embassy in Moscow, Russia; and as a federal cybercrimes prosecutor. He led DOJ’s work on the Target, Sony Pictures, Home Depot, Anthem and OPM breaches, among many others, and received the Attorney General’s Distinguished Service Award for leading the GameOver Zeus botnet takedown. He participated in the negotiation of a 2013 cyber accord with Russia and the historic 5-point agreement signed by President Obama and President Xi Jinping of China in 2015.

# Rob Bathurst

---



**Managing Director  
Healthcare/Embedded**  
*BlackBerry Cylance*

Rob Bathurst is a recognized leader in the reverse engineering and strategic information security spaces. Rob started and helped build the technical vulnerability assessment team at the Mayo Clinic specializing in healthcare-focused security assessments and in-house medical device testing, a first of its kind. During his career, he has lead over 150 security engagements ranging from penetration testing to strategic planning aiding government, military and private entities. Through these engagements, Rob has developed and experienced a wide variety of worldclass techniques to create effective solutions for securing high-assurance and safety-critical systems against real world threats.