



LES SVC Luncheon, Oct-16, 2019

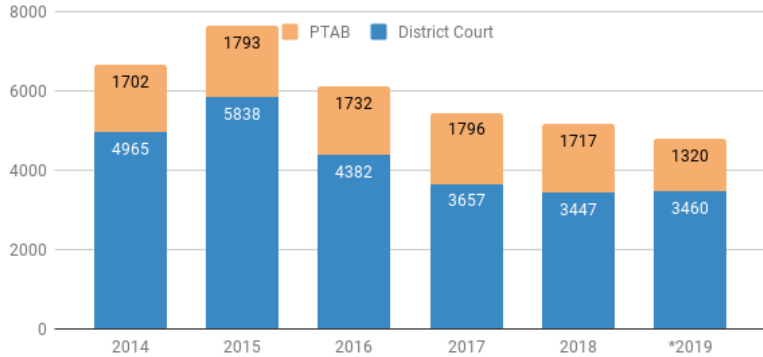
Protecting Your Secret Sauce!

Techniques & Technologies for Securing Your Systems, Data, & Intellectual Assets Against Hacking, Theft, & Industrial Espionage

Rambus
Data • Faster • Safer

Patents Disputes Down - Trade Secret Litigation Up

Patent Dispute Report: 2014 - 2019



*Total litigation for 2019 is an estimate based on 1H 2019 filings.

Figure 2: DTSA Cases Filed from May 11, 2016 to 2018 Q2

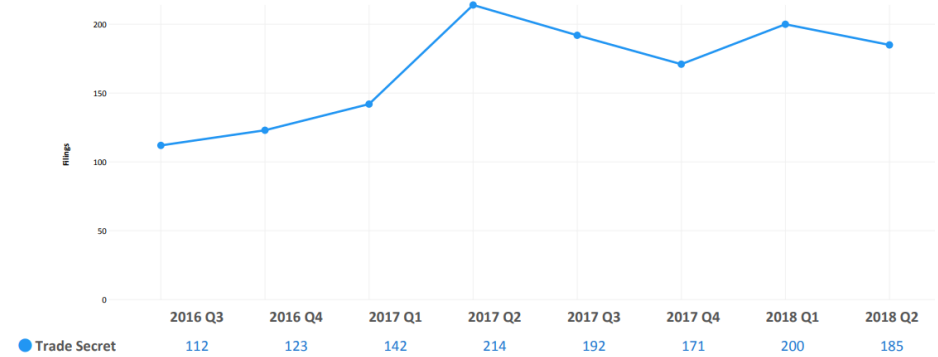
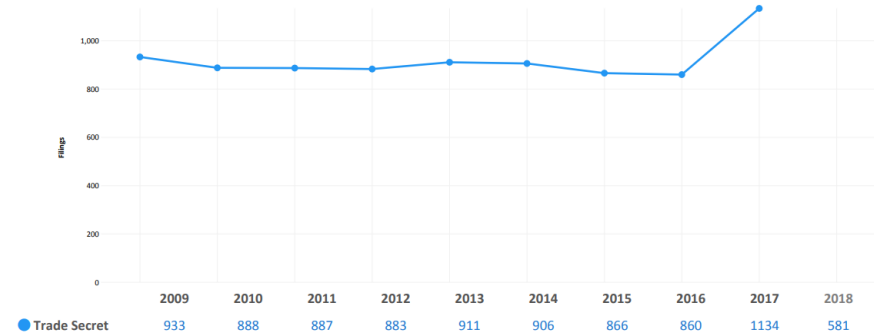


Figure 1: All Trade Secret Cases Filed from 2009 to 2018 Q2



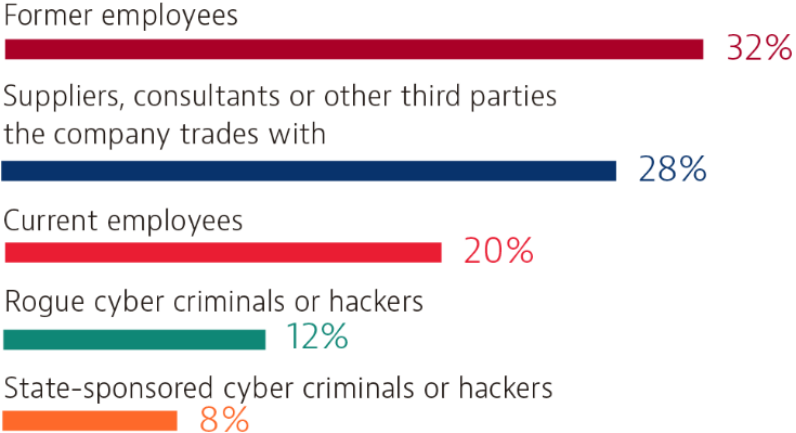
Lex Machina distinguishes cases brought under the Defend Trade Secrets Act through case tagging using natural language processing. Below is a focused look at filings under the act since its enactment. Cases including a claim under the DTSA steadily increase over the first four quarters since enactment.

https://www.gordonrees.com/Templates/media/files/pdf/Trade_Secret_Litigation_Report_2018.pdf

DTSA & EU Trade Secrets Directive Target Trillion Dollar Problem



In terms of where trade secrets theft originates from, which of the following are you most fearful of?



<https://insight.bakermckenzie.com/trade-secret-theft-a-trillion-dollar-problem>

Some Recent High-Profile Examples



ADAM ROGERS BUSINESS 11. 01. 2019 08:25 PM

US Accuses Chinese Company of Stealing Micron Trade Secrets

The indictment alleges a state-owned company and rogue employees stole plans so China could make memory chips—further straining China-US relations.

Intel gets court order telling former engineer to return confidential docs in Micron row

Defense insists there's nothing to return. And those Perl files? Purely sentimental.

By Thomas Claburn in San Francisco 25 Mar 2019 at 06:57 27 SHARE



Philips Medical Systems accuses ex-engineer of pilfering trade secrets

APRIL 22, 2019 BY BRAD PERRIELLO — [LEAVE A COMMENT](#)



PHILIPS

A former engineer at Philips Medical Systems in Illinois allegedly transferred confidential trade secrets and then tried to destroy the evidence, the company said in a lawsuit filed last week.

Speakers:

- **Lee Gardner** - IP Counsel, Google
 - **Adelaida Hernandez** - Special Agent, FBI
 - **Elizabeth McBride** – Managing Director, Global Litigation, Investigations & IP, Applied Materials
 - **Neeraj Paliwal** – VP & GM Rambus Security
-
- **Moderator:** Stefan Tamme, VP IP Strategy & Licensing, Rambus

Trade Secret Management

In-house Counsel Perspective



Lee Gardner / 10-16-2019

Trade Secret Risks

Infiltration

Unauthorized storage or use of third-party proprietary information

Exfiltration

Unauthorized copying, transfer, or retrieval of proprietary Google data

Partnership

Exceeding the authorized scope of use in a partnership

Information Governance Stakeholders



Legal



IT



Product &
Engineering



HR

Training Policies Training

Thank You

LES SVC Luncheon: Protecting Your Secret Sauce!

Techniques & Technologies for Securing Your Systems, Data,
& Intellectual Assets Against Hacking, Theft, & Industrial
Espionage

Elizabeth C. McBride

Managing Director, Global Litigation & Investigations

October 16 ,2019

Applied Materials: World's #1 semiconductor and display equipment company



\$17.3 billion
revenue



\$2.0 billion
R&D spending



>12,500
patents



AMAT stock
listing on
NASDAQ



Headquartered
in California's
Silicon Valley



~21,000 employees
93 locations
In **17** countries

Understanding the Risk Landscape



Employee mobility
Contingent workforce
Partners
Cyber attacks
Foreign state actors
Speed & connectivity

Insider Risk

Who is an Insider?

- ▶ Any employee, contingent worker, or trusted business partner who has authorized access to internal corporate resources.

Types of Insider Risk Actors

- ▶ **Malicious actor** (employee, contingent worker, supplier) with access to corporate systems, networks and data who has exceeded authorized access or breached systems to compromise the company.
- ▶ **Unintentional actor** whose careless or inadvertent conduct causes damage or creates vulnerabilities to the company's systems.

Types of Risk

IT Sabotage

IP / Trade Secret Theft

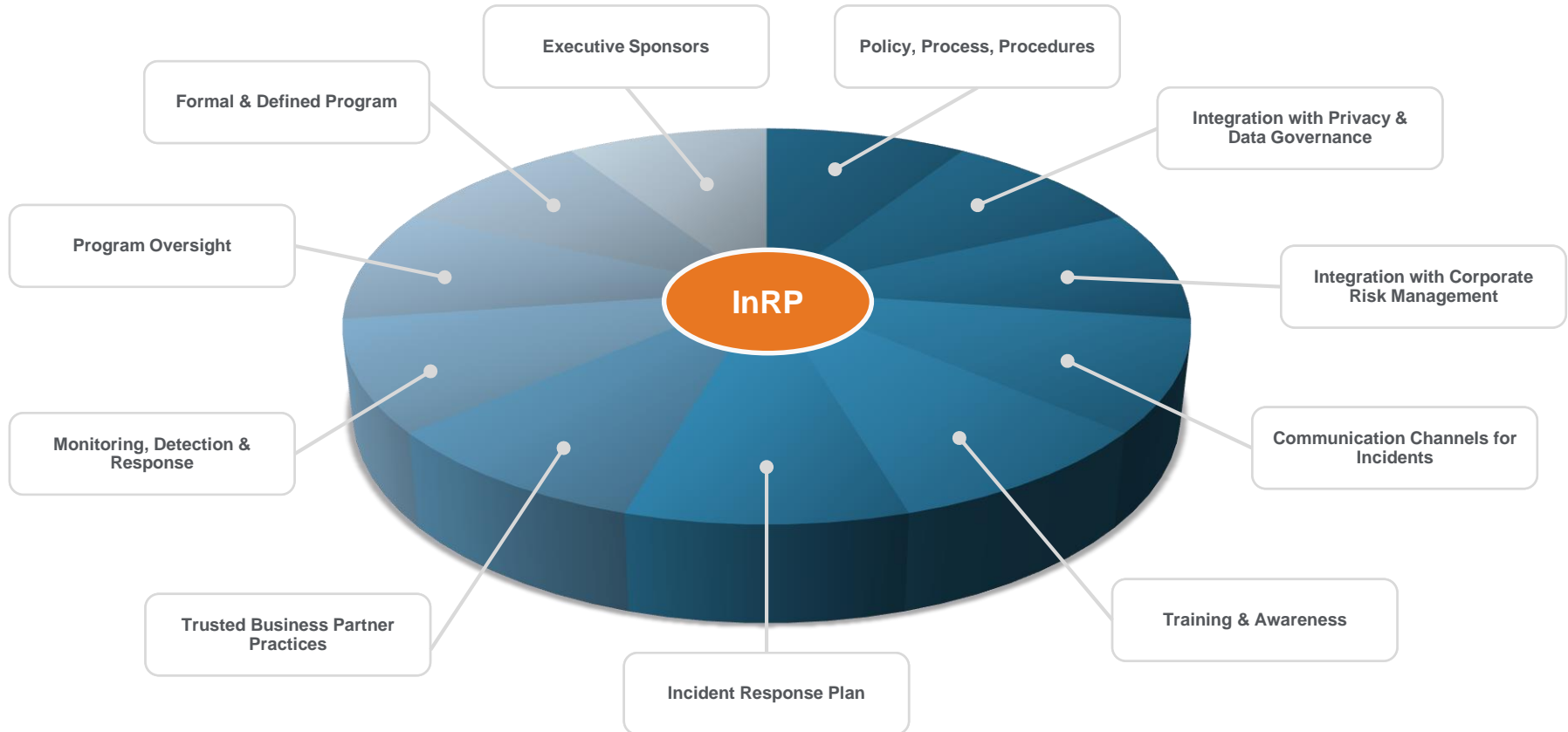
Fraud

Espionage

Unintentional Insider

Other

Overview an Insider Risk Program





Strategies for Protection

Onboarding and Exiting
Contingent Workforce Risk Management
Monitoring & Strategic Response
Data Security and Data Segregation
Information Sharing with Trusted Partners
Programs, Policies, and Org



APPLIED
MATERIALS[®]

make possible