Cyber Defense & Breach Response

Privacy Issues

LATHAM & WATKINS

Kevin Boyle

Partner

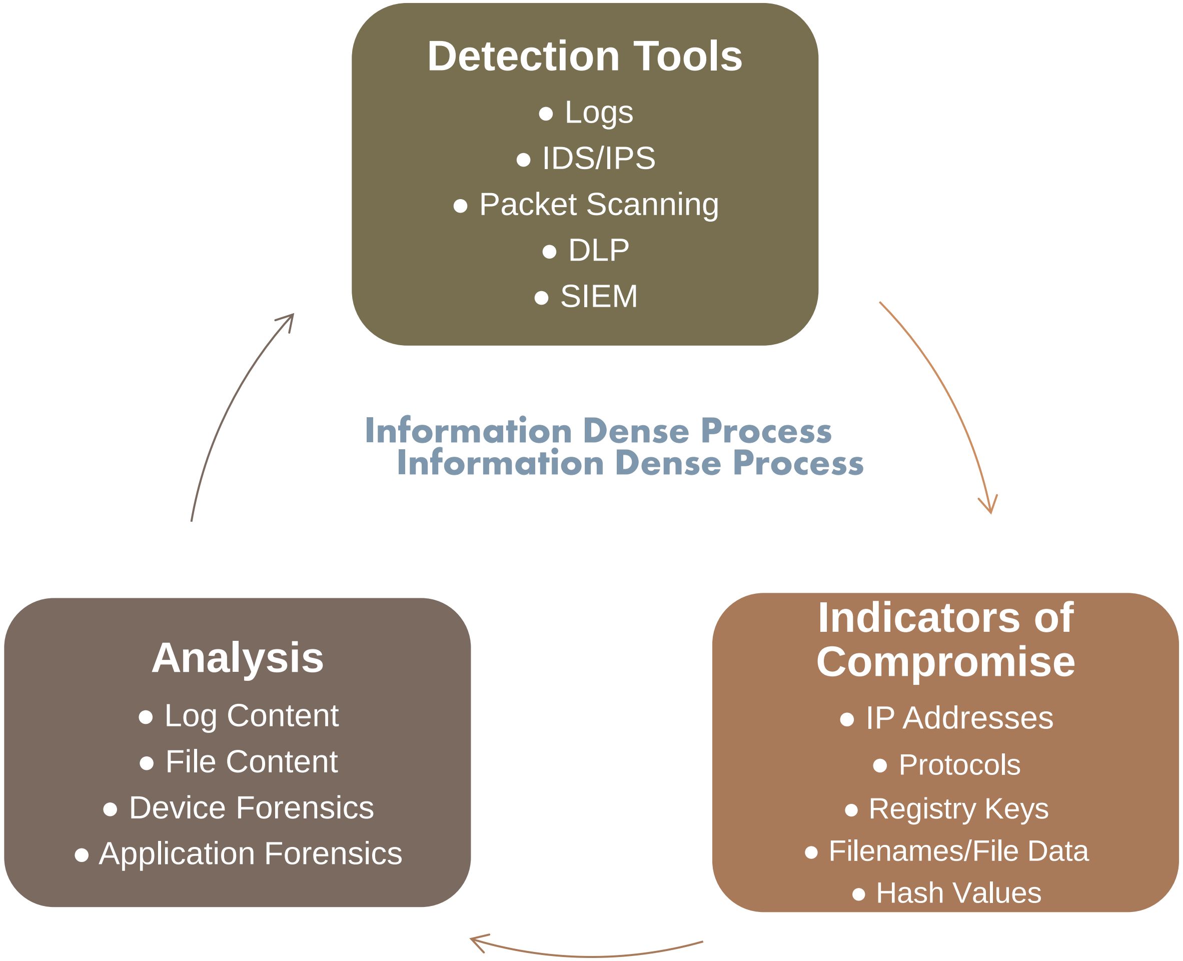
17 November 2014

Latham & Watkins is the business name of Latham & Watkins (London) LLP, a registered limited liability partnership organised under the laws of New York and authorised and regulated by the Solicitors Regulation Authority (SRA No. 203820). We are affiliated with the firm Latham & Watkins LLP, a limited liability partnership organised under the laws of Delaware. © Copyright 2014 Latham & Watkins. All Rights Reserved.

Privacy-Security Paradox

Security	vs.	Privacy
Obligation to provide security for personal information and other confidential material		Rules for processing Personal Information (and analogs outside the EU)
Quick response to attacks and changing strategies		Requirements to obtain user consent and register applications/processing
Need to retain log and traffic data for analysis		Restrictions on data retention
Need to consolidate data for analysis		Export limitations on “personal data,” banking information and “state secrets”

Security Process



Detection Tools

- Logs
- IDS/IPS
- Packet Scanning
- DLP
- SIEM

Indicators of Compromise

- IP Addresses
- Protocols
- Registry Keys
- Filenames/File Data
- Hash Values

Analysis

- Log Content
- File Content
- Device Forensics
- Application Forensics

Information Dense Process

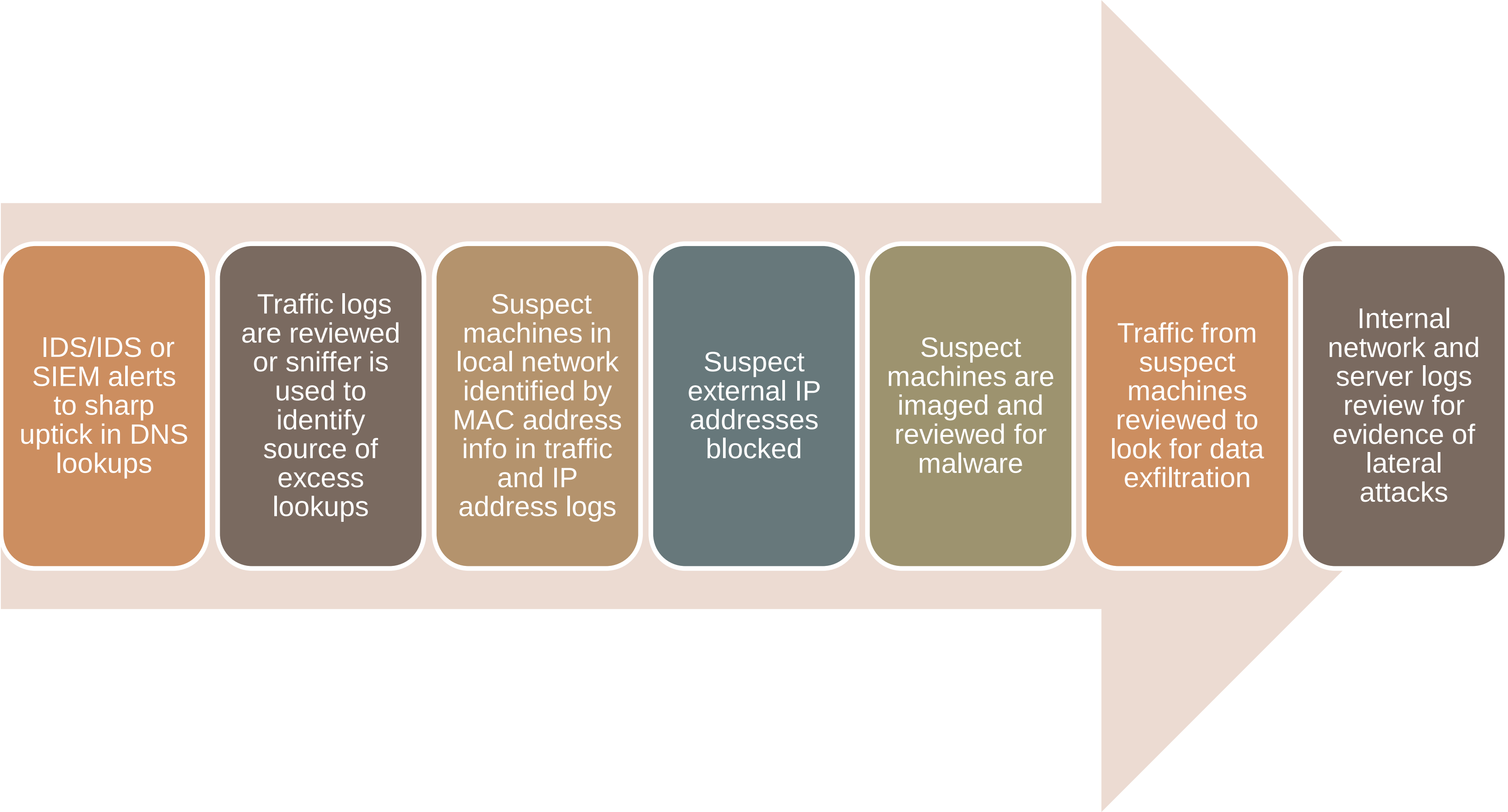
Information Dense Process

Defense & Response Toolkit

Increasing Privacy Impact

Category	Description	Examples
Systems Data Monitoring Tools (IDS, IPS)	These tools send alerts based on rules of non-routine events, patterns of suspicious behavior, or unusual activity. The alerts will contain systems data to provide evidence of the type of issues spotted, e.g. file type, IP address, communications protocols, and what it was communicating with internally. Often programmed to recognize specific malicious signatures.	Proventia, Fidelis XPS, Netflows (SiLK analysis)
Server Monitoring Tools	These tools are similar to the above but work at a server or endpoint rather network level, e.g. monitor a server to look for unusual events.	RSA ECAT, Microsoft Threat Detection System, Symantec CSP
Systems Data Storage Tools	These tools save all log / network data so it can be reviewed at a later date. These differ from the monitoring tools as the monitoring tools do not save all data but only provide information of suspicious events.	SPLUNK
Consolidation Tools (SIEM)	These tools take feeds from all of the other tools to enable suspicious events to be cross referenced. This technology can correlate event information and bring together a larger picture of activity above and beyond individual technology collection and analysis.	ArcSight, Alien Vault SIEM
Content Monitoring Tools (DLP)	These tools undertake deep packet inspection (looking at Business Content) based on a set of rules to try and identify content being exfiltrated or moved around the network by the attackers.	Symantec DLP
Content and Log Storage Tools	These tools effectively store all log and content data that passes over a certain point in the network, e.g. firewall, mail server, VPN tunnels. Capable of storing a complete record of all communications entering and leaving the network which can subsequently be reviewed if necessary to investigate suspicious behavior and modes of attack. Length of data retention key driver.	RSA Security Analytics

Active Defense Example



IDS/IDS or SIEM alerts to sharp uptick in DNS lookups

Traffic logs are reviewed or sniffer is used to identify source of excess lookups

Suspect machines in local network identified by MAC address info in traffic and IP address logs

Suspect external IP addresses blocked

Suspect machines are imaged and reviewed for malware

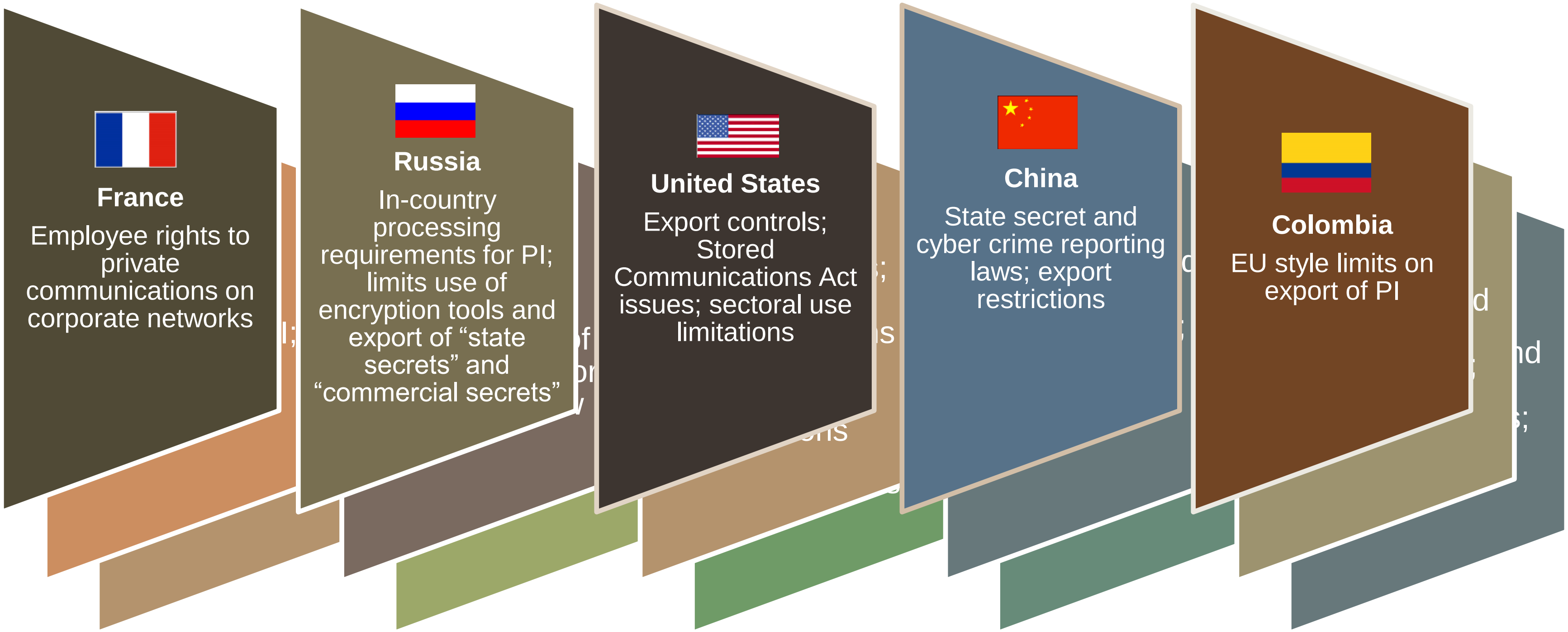
Traffic from suspect machines reviewed to look for data exfiltration

Internal network and server logs review for evidence of lateral attacks

Activities (Risks)

- AV, IDS/IPS and other pattern based tools (content scanning)
- DLP (content scanning at a more intrusive level than IDS/IPS)
- Capturing network packets (metadata and/or content), logs and assets (even more intrusive content scanning)
- SIEM and log correlation/analysis (behavior tracking, works council issues, potentially ties to content scans)
- Device forensics (content scanning, behavior tracking)
- Global SOC (export controls, privacy controls)

Global Compliance Requirements



France

Employee rights to private communications on corporate networks

Russia

In-country processing requirements for PI; limits use of encryption tools and export of “state secrets” and “commercial secrets”

United States

Export controls; Stored Communications Act issues; sectoral use limitations

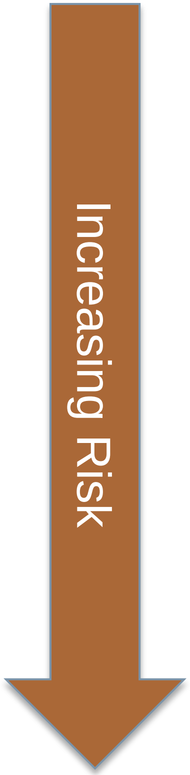
China

State secret and cyber crime reporting laws; export restrictions

Colombia

EU style limits on export of PI

Global Compliance Issues


Increasing Risk

Category	Issues
General	Data subject consent, DP registration
Systems Data Monitoring Tools (IDS, IPS)	IP addresses treated as PI by some jurisdictions; collection/review of physical security data may violate workplace rules, especially when correlated with other data
Server Monitoring Tools	Fact of access to particular servers may reveal protected health information or other PI
Systems Data Storage Tools	Same as above but with data retention issues and increased prospect that substance of communications will be revealed
Consolidation Tools (SIEM)	In addition to above, export issues (as data need to be normalized and compared (depending on configuration); additional retention issues
Content Monitoring Tools (DLP)	Direct review of message content; export issues depending on configuration
Content and Log Storage Tools	Direct review of message content, data retention issues, export issues

A Practical Approach to Compliance

❑ Back to privacy first principles – FIPS
  - Disclosure
  - Transparency
  - Least intrusion necessary (proportionality/necessity)
  - Balance interests

❑ Ensure monitoring is necessary and no less intrusive means available

❑ Obtain employee consent where possible
  - As part of onboarding
  - Sign-on banners
  - As part of ongoing security awareness efforts

❑ BCRs may afford additional flexibility in response

A Practical Approach to Compliance

- Reduce risk of misuse through:
  - appropriate use of safeguards and
  - documented, tool-specific written protocols regarding:
    - export, access, use, need to escalate for express permission to deviate from protocol
- Ensure DP filings and other compliance materials adequately disclose monitoring
- Monitoring notified to and agreed with Works Councils where required
- Necessity
  - Perimeter defenses not enough/zero day
  - Once intruder is in, monitoring may be only approach to eradication
  - Checking communications may be only way to thwart exfiltration of protected data

Data Nationalism – A Trend to Watch

- Revelations by Edward Snowden about mass surveillance by U.S. (and other) intelligence agencies of personal data held/processed by service providers caused companies to review their structures and processes
- Countries mandating storage of citizen data (sometimes solely) within the borders of that country

Russia-Companies collecting personal data over the internet will be required to “*provide recording, systemisation, storage and update of the Russian citizen's personal data using databases located in the territory of the Russian Federation*”

Brazil-Proposed similar local storage provisions to Russia following Snowden revelations, but these plans were dropped

India-Following PRISM, Indian ISPs lobbied Indian Government to force foreign internet companied to set up local servers

EU-Criticised US Safe Harbor and ability to transfer data to US under program. New draft Regulation contains “blocking” provisions – transfer to overseas governments require regulatory approval.

US-Existing limitations on overseas processing by state/local governments

Data Protection Contacts

Jennifer Archie

Partner (Washington)
Phone: +01.202.637.2205
Email: jennifer.archie@lw.com

Luke Grubb

Partner (Singapore)
Phone: +65.6437.5473
Email: luke.grubb@lw.com

Kevin Boyle

Partner (Washington)
Phone: +01.202.637.2245
Email: keivn.boyle@lw.com

Myria Saarinen

Partner (Singapore)
Phone: +33.1.40.62.28.43
Email: myria.saarinen@lw.com

Gail Crawford

Partner (London)
Phone: +44.20.7710.3001
Email: gail.crawford@lw.com

Ulrich Wuermeling

Partner (Singapore)
Phone: +49.69.6062.6502
Email: ulrich.wuermeling@lw.com