Security Matters

Fighting the insider threat

Kevin Eley, LogRhythm

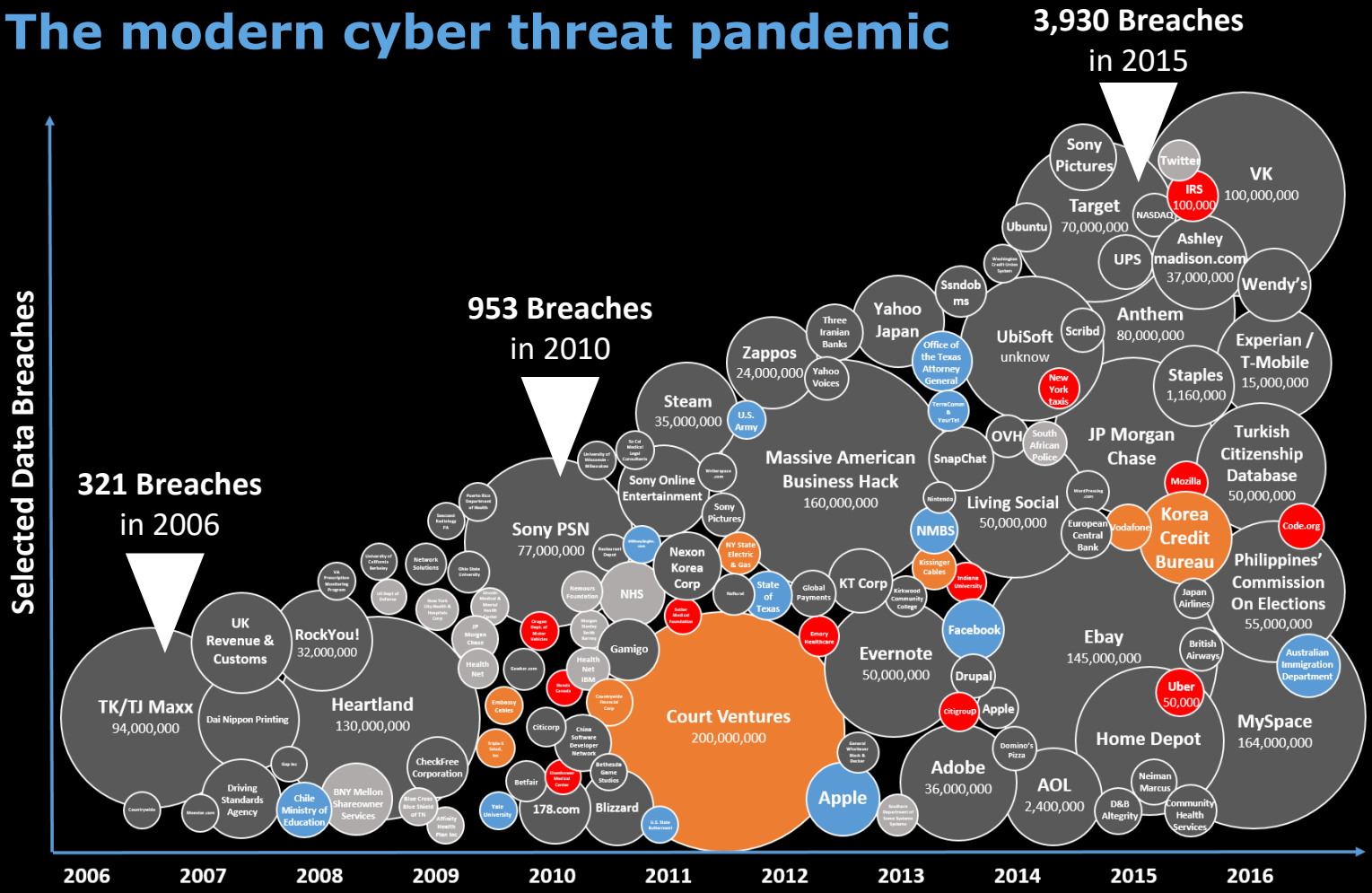
22nd March 2018

LogRhythm®
The Security Intelligence Company

LogRhythm Mission

To improve your ability to rapidly detect and respond to Cyber Threats in whatever form they take thereby reducing the likelihood of data breach

The modern cyber threat pandemic



Source: World's Biggest Data Breaches, Information is Beautiful

The names have been changed …

One trillion dollars and rising

A ‘gifted’ employee

A result but no silver lining

The Compromised Insider

- Malware victims
- Impersonated users

The Malicious Insider

- Rogues employees
- Criminal actor employees

The Accidental Insider

- Inadvertent actors
- Convenience seekers

Collect and act on the clues

- The unusual out of hours system log on activity, particularly when compared to other users performing the same duties / in the same AD OU
- Correlated that two user credentials were simultaneously being used by a device on the same IP
- Spotted the transfer of data to the users alternate identities
- Use of File Integrity Monitoring to spot the rogue employee deleting files.

Technology to combat insider threats

- Artificial intelligence
- UEBA
- Advanced analytics

Recommendations

- Ensure employment contracts contain acceptable use, confidentiality, intellectual property and monitoring clauses
- Understand your MVEs and HVTs, threats and risks
- Closely monitor environments these environments / users
- Monitor for known TTPs \ kill chain \ anomalies
- Unusual authorised / unauthorised access alarms critical
- Unusual working patterns / unusual data flows
- Record and keep evidence in digital evidence locker
- Educate line management and HR about rogue employee
- Be vigilant!

Thank you

kevin.eley@logrhythm.com