Egress Software Technologies

It’s time to turn the tide on email data breaches

Bradley Payne
Senior Lead Finance Account Manager
Agenda

- The insider breach problem
- Prevent and Protect
- New ways to prevent and protect
- Summary
Ponemon Institute: Survey of 1,700 customers

- Majority cited negligent insiders (64%) vs. malicious insiders (23%)
- Employee negligence cost $283,281/incident vs. malicious insider cost of $607,745
- Two month average to contain an insider incident
- Only 16% contained in less than 30 days
Effective email security: Prevent and protect

Prevent
• Ensure the right content is sent to the right person
• “What is the point of sending an encrypted email to the wrong person?”

Protect
• Ensure that the right protection is applied to emails
• “What if you send an email to the right person, but it is breached?”
Prevent: Older signature-based DLP systems

Use static rules to detect breaches

- Manage database of rules on what users can and cannot do
- Require regular maintenance and updates
- Do not account for context, past behaviour and relationships
- Cannot prevent against misdirected emails
Prevent: The new way

**Machine learning** to prevent breaches

- Use parallel processing and cloud to ingest vast quantities of data
- Link relationships and past behaviour to detect anomalies
- Learn as they go: No need to maintain static rules
Prevent: Misdirected email use cases

- Outlook auto-complete mistakes
- Mis-typing of recipients
- Sending the wrong attachment to the wrong person
- Sending sensitive data to the wrong person or domain
- Ethical walls / Internal breach
Prevent: Anti-phishing use cases

- Edge-based solutions block 95% of attacks. Last 5% cause most damage
- Business email compromise (BEC) scams lost over $1.6bn in 2018
  - Scammer pretending to be a manager, co-worker or supplier
  - Google and Facebook transferred over $100m to a fake supplier
  - More targeted / More Frequent
Prevent: Anti-phishing Example

BEC solutions

- Anomaly detection of the individual mailbox based on content and recipients
- Domain type squatting detection
  www.britishairways.com vs. www.brtishairways.com
- Impersonation detection
  Tony Pepper <Tony.Pepper@Egresss.com>
Summary

- **Insider breaches** account for the vast majority of data breaches
- **AI and machine learning** do deliver on specific use cases
- **Prevent and protect** go hand-in-hand for comprehensive email security
Thank you for your time

E: info@egress.com | T: +44 (0) 2076248500 | W: www.egress.com | Twitter: @EgressSoftware