CyberRisk

Trends and Best Practices

Davis Kessler – May 2020

TRAVELERS

Important Information

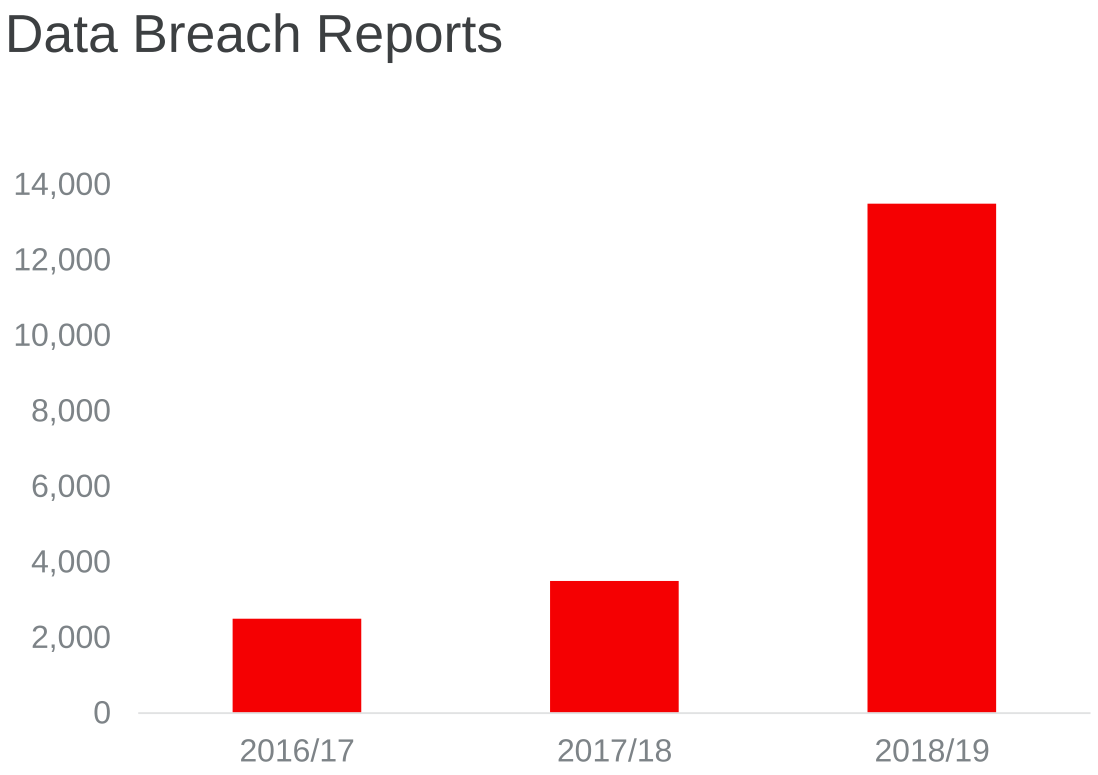
This document contains proprietary and confidential information and is only to be used internally for training by employees of The Travelers Companies, Inc. or any of their subsidiaries or affiliates. Do not distribute this document or any part of it to any person who is not a Travelers employee.

This document does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond issued by Travelers or any of its subsidiaries or affiliates, nor is it a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts circumstances involved in the claim or loss, all applicable policy or bond provisions and any applicable law.

The information provided in this presentation is intended for use as a guideline and is not intended as, nor does it constitute legal or professional advice.

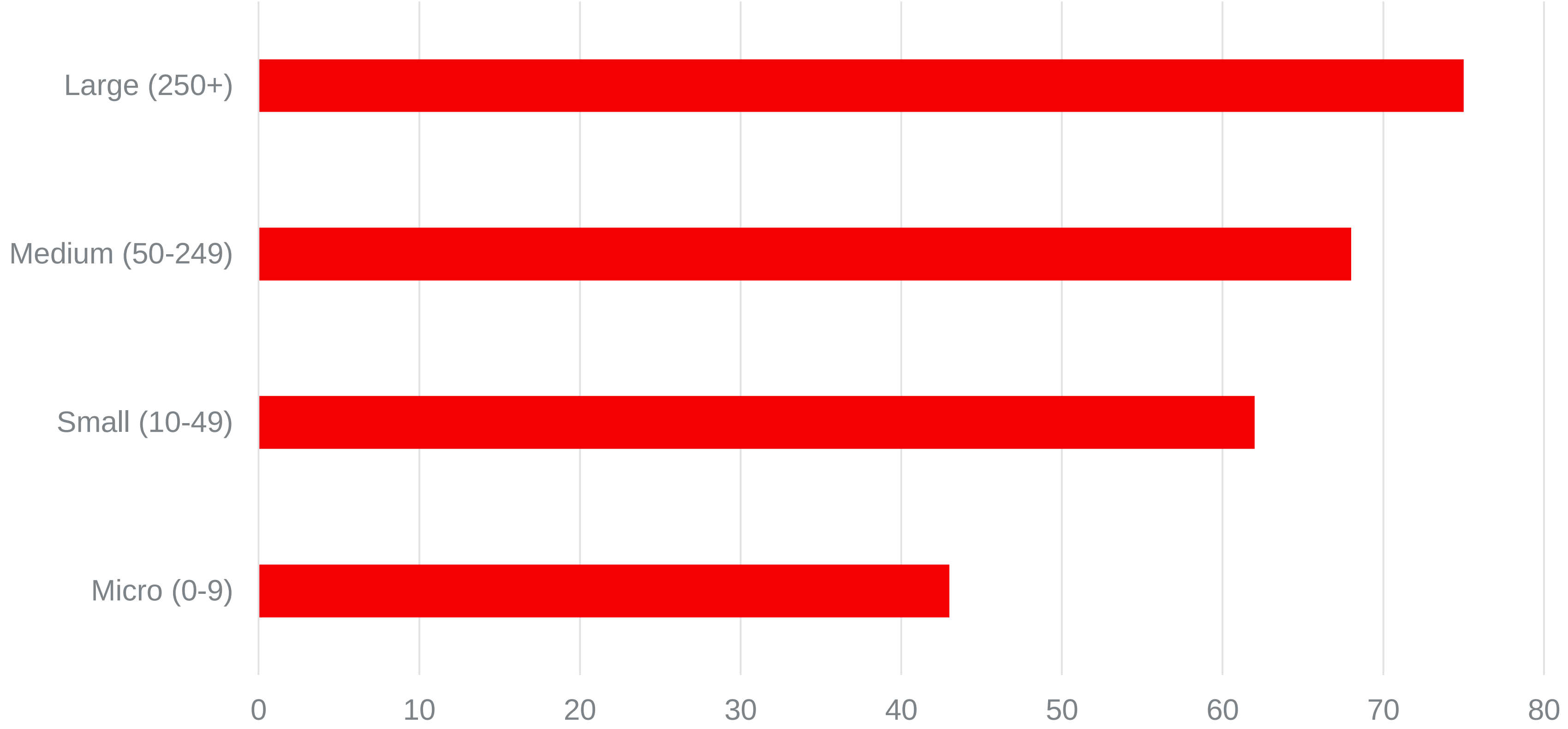
What did we see in 2019?

- Surge in ransomware
  - Highly targeted leading to massive increases in amount demanded
  - Variation of targets
- Managed Service Providers (MSPs) targeted as conduit
- Business email compromise leading to funds transfer fraud
- Data breaches are alive and well
- Surge in post-GDPR data breach reporting



Risk Management Trends

Firms identifying a cyber attack in last 12 months:



Source: Dept. for Digital, Media, Culture, “Cyber Breaches Survey 2020”

Ongoing Threats

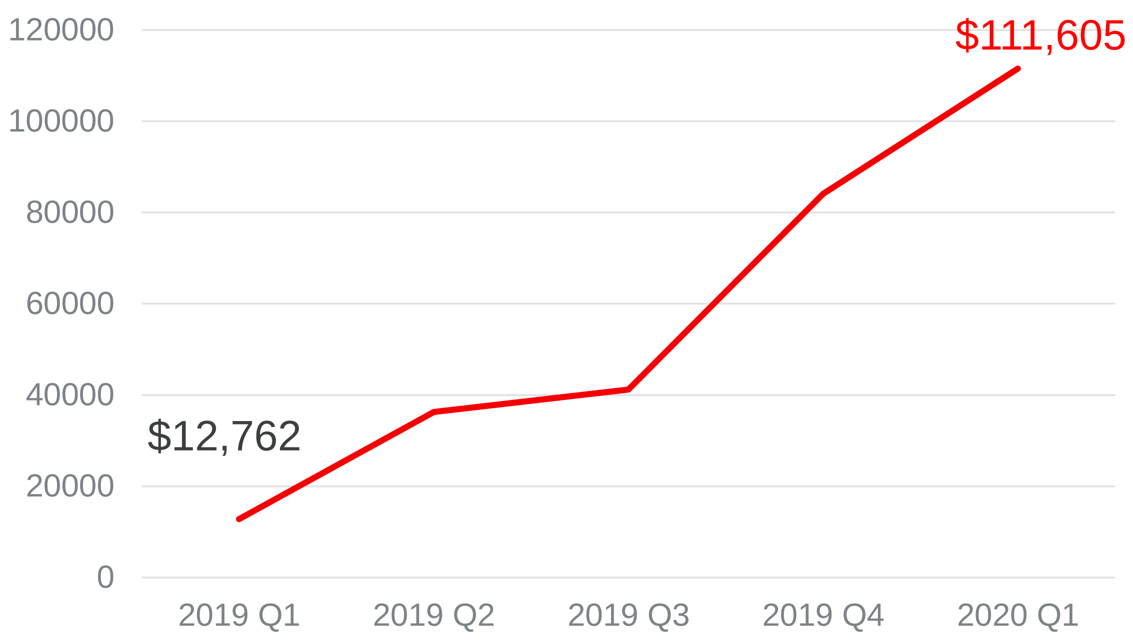
- Ransomware only getting worse
- ‘Doxing’
- Social Engineering Fraud
- Nation-state attacks
- Industrial espionage
- Supply chain concerns

CyberRisk Claim Trends

Ransomware

- A type of malicious software designed to block access to a computer system until a sum of money is paid
- New versions of ransomware are sophisticated, encrypting data and backups, propagating quickly through systems
- Ransom demands are becoming more aggressive

Average Ransom Payment – since Q1 2019



Source: Coveware Q1 2020 Ransomware report

TRAVELERS

CyberRisk Claim Trends

Email Compromise → Social Engineering Fraud

- Web based platforms are becoming more widely used.
- Once a fraudster has access to email, this access is used to perpetrate other crimes:

  - Social Engineering Fraud

  - Invoice Manipulation

  - Computer Fraud

  - Theft of PII

Email Compromise – unfortunate consequence

- In addition to any 1st party loss, Data Privacy laws require individuals whose confidential information was accessed within emails be notified
- Notification Costs, Forensic Investigation, Legal Fees
- Organizations that are vulnerable to these attacks tend to get hit repeatedly until the vulnerability is addressed.

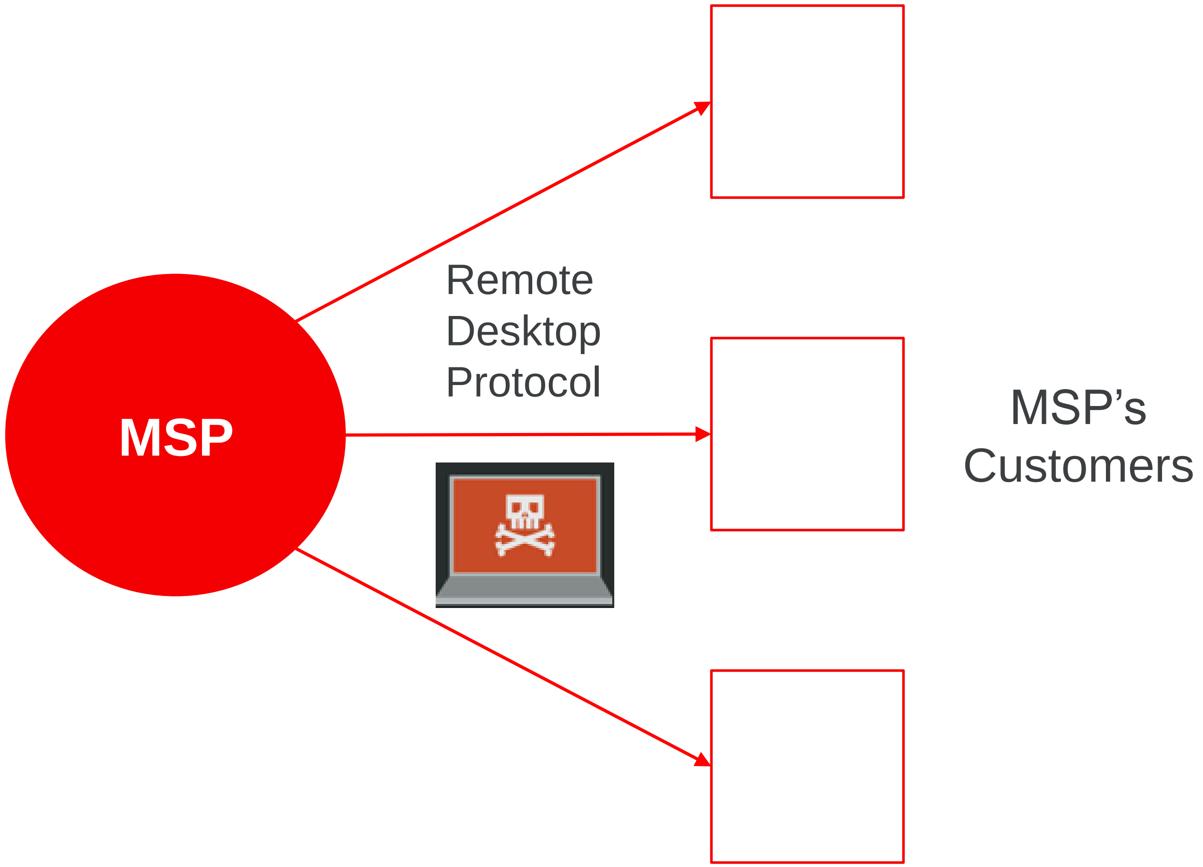
Percentage of reported UK cyber crimes involving fraudulent emails

87%

Aggregation – Managed Service Providers

Use of external cyber security providers:

- Micro firms: 34%
- Small firms: 57%
- Medium firms: 65%
- Large firms: 49%
- Overall: 39%



Source: Dept. for Digital, Media, Culture, "Cyber Breaches Survey 2020"

Aggregation – Data Breaches

59% of companies reported they have experienced a data breach caused by one of their vendors

Only **34%** of companies keep a detailed inventory of what information is shared with others.

Source: Ponemon Institute “Data Risk in the Third-Party Ecosystem”

Regulatory Updates

- The march towards more data privacy regulation goes on
  - California Consumer Privacy Act (CCPA)
  - Brazil - General Protection Law: Feb
  - India – Personal Data Protection Bill (DPB)
  - Australia looking at changes
- Uptick in GDPR fines
  - 150 fines issued in 2019, totaling €103m[1]
  - Massive increase in staff in UK and multiple countries
- Legislation forbidding ransom payment?

Legal Developments

- *Morrisons* – a ‘win’ for employers, but still shows value of cyber security measures (and cyber insurance!)

- *Lloyd v Google* – class action status; inherent value of private information

Windows 7

- 14 Jan 2020 - Windows 7 OS no longer supported by Microsoft
- Globally **19.4%** of computers still use Win7
  - UK: 10.3%
  - US: 12.9%

Source: https://gs.statcounter.com/windows-version-market-share (as of 7 May 2020)

Moving from good to better

What does Risk Good Practice look like?

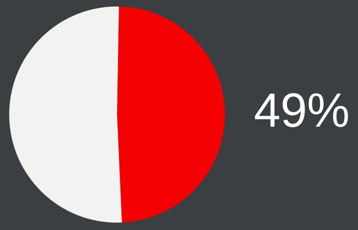
Management Awareness/Involvement

“Good” looks like:

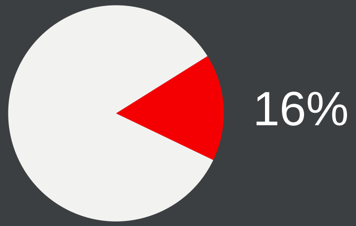
- Awareness/appreciation by the Board
- Senior Management involvement in incident response planning
- Cyber risk assessments (ideally 3rd party)

UK Cyber Survey Results:

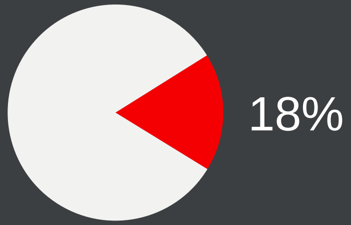
Cyber updates to board at least quarterly:



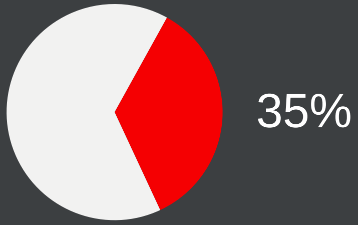
Formal incident management process:



External Audit:



Cyber risk assessments:



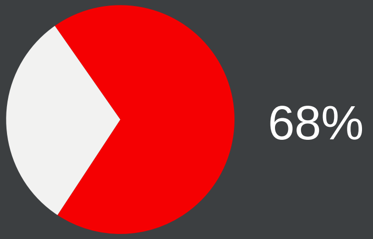
Source: Dept. for Digital, Media, Culture, “Cyber Breaches Survey 2020”

Ransomware – Loss Prevention

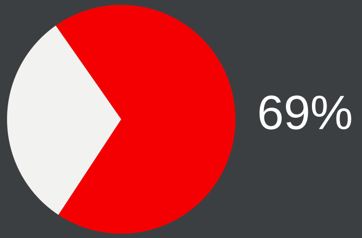
“Good” looks like:

- System Security Controls and Maintenance
  - Multi-Factor (MFA) for Admin Access
- No unnecessary open ports (RDP/SMP)
- Incident Response / Disaster Recovery Planning
- Secure, tested backups
  - Offsite vs. Cloud?
- If Ransom Payment is Necessary:
  - Engage with forensic firms with knowledge of hacker groups
  - Will this particular group be able to deliver functioning encryption keys?
  - Negotiation tactics

Incident Response Plan:



Data backups to cloud:

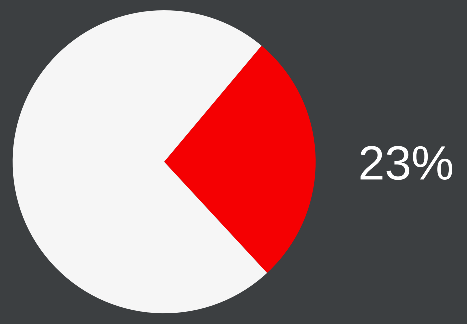


Source: Dept. for Digital, Media, Culture, “Cyber Breaches Survey 2020”

Social Engineering Fraud – Loss Prevention

- Require Multi-Factor authentication for access to email and other web based platforms
- Train staff to look for suspicious emails / conduct Phishing exercises
- Promote culture of security awareness so that employees are willing to question or flag suspicious activity.

Cyber Training:



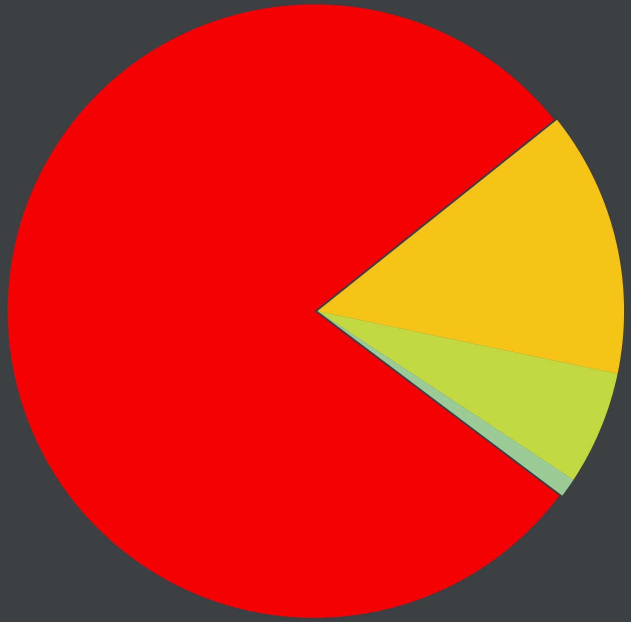
Source: Dept. for Digital, Media, Culture, “Cyber Breaches Survey 2020”

Cyber Insurance – To fully manage your cyber exposure

Reasons for not taking up cyber insurance:

- Think already covered by external service provider: 23%
- Consider themselves not at risk: 22%
- Lack of awareness of cyber insurance: 23%
- ABI Cyber Insurance Claim Payment Rate: **99%**

Purchase Specific Cyber Insurance Policy:



Small – 14%

Medium – 20%

Large – 21%

Source: Dept. for Digital, Media, Culture, “Cyber Breaches Survey 2020”
Source: Association of British Insurers, “Cyber insurance payout rates at 99%, but uptake still far too low,” Aug 2019

Thank you

TRAVELERS