Threat 360

Cyber security

Advanced Threat Protection Service

FUJITSU

shaping tomorrow with you

Human Centric Innovation

Co-creation for Success

CYLANCE

© 2018 FUJITSU

Recent Damaging Data Breaches

FUJITSU

COMPANY	COST OF BREACH	WHAT
Yahoo	$350 million ✧	3B accounts compromised
Equifax	$114 million	115M accounts stolen
Far Eastern Int' Bank	$60 million	Money stolen
Ethereum	$40 million	Money stolen
Uber	$?? million	57m personnel details stolen
Dun & Bradstreet	$?? million	Accounts stolen inc' personnel details

Known value of data breaches Data breach announced – actual cost pending legal/ government action

✧ Value of the breach was not known until 2017 when Verizon devalued the sale of Yahoo by $350 million over this one incident

© 2018 Fujitsu

Businesses must take action

UK manufacturers fall victim to cyber attacks, survey reveals

News 23 APRIL 2018

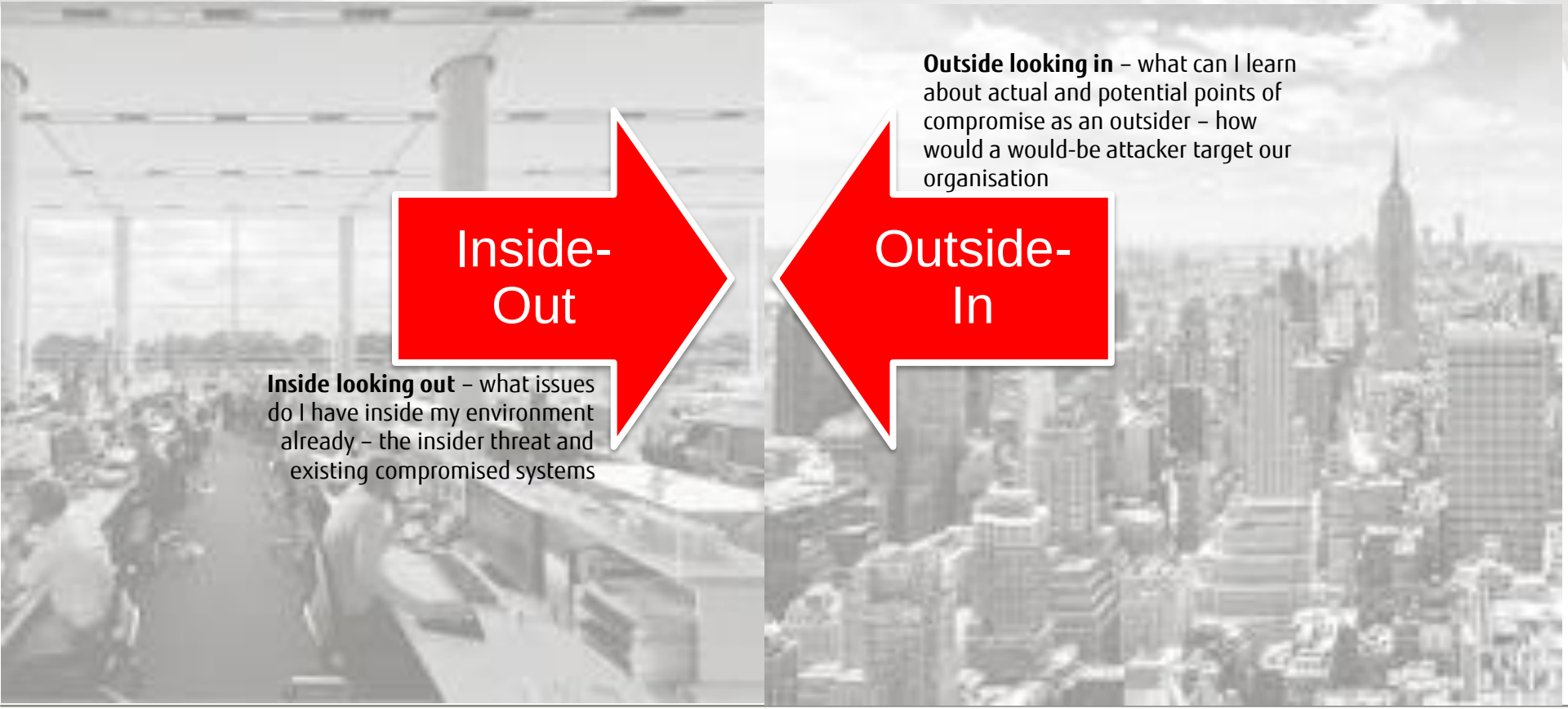
80 UK manufacturers subjected to cyber attacks but many more may have gone undetected, report finds.


The Telegraph HOME NEWS SPO
Technology
News Reviews Opinion Internet security Social media Apple Google
Technology
Verizon to buy Yahoo for $250m less as deal to go ahead despite data breaches

Rob Norris, VP Head of Enterprise & Cyber Security EMEIA at Fujitsu, said manufacturers cannot afford not to take their security seriously: "With events over the past year revealing just how enormous the potential cost – both reputationally and financially – of suffering a major security breach can be, manufactures cannot afford not to take their data protection and cyber security seriously, or indeed make it a number one priority. In fact, with our latest report revealing a fifth of the UK public believe cybercrime and hacking are the biggest challenges facing the UK today, **every single manufacturer has an obligation to make data protection as much of a priority as the public**.

© 2018 FUJITSU

Understand the threats – a dual perspective



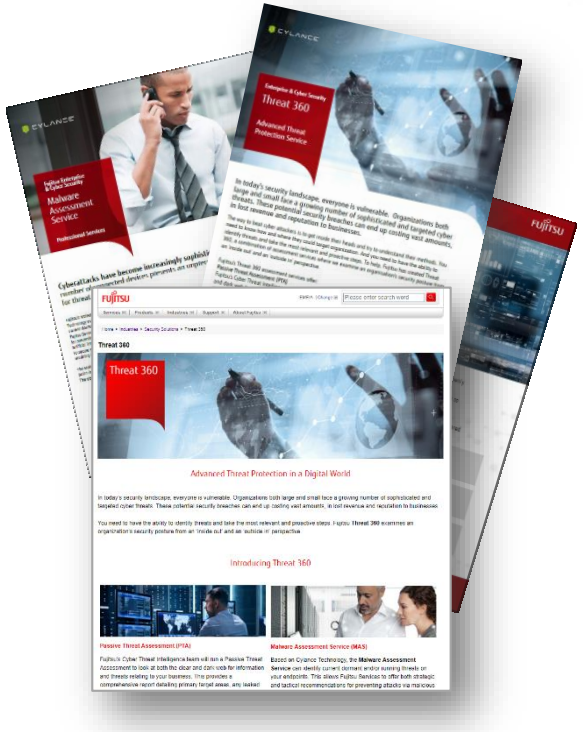
Inside looking out – what issues do I have inside my environment already – the insider threat and existing compromised systems

Outside looking in – what can I learn about actual and potential points of compromise as an outsider – how would a would-be attacker target our organisation

© 2018 Fujitsu

Threat 360 – an holistic approach

- Fujitsu's Threat 360 assessment service is a combination of a Malware and Passive Threat assessment
- Enables the business to identify where it's vulnerable or compromised – and then how to act to limit any exposure.
  - 180º view - Malware Assessment is a lightweight, unobtrusive point-in-time assessment across approx. 20% of the estate to identify malware that has not been identified by other security technologies.
  - 180º view - Passive Threat Assessment looks at both the clear and dark web for information and threats relating to domain and brand.



© 2018 FUJITSU

180º view - Passive Threat Assessment

FUJITSU

- Clear & Dark web analysis
- Employee account credentials
- Website vulnerabilities
- Email address dumps
- Dark web references on underground forums
- Domain spoofing analysis
- Metadata on company docs available online
- Open source intelligence assessments, highlighting any likely phishing attacks

© 2018 FUJITSU

180º view - Passive Threat Assessment

FUJITSU

240+ assessments since 2016

- 100% of assessments have helped, identifying at least one avenue of attack
- Majority of assessments identify email addresses on known malware target lists
- ~50% of reports find exposed customer passwords
- ~98% of companies assessed had at least one variant of their domain registered

Specific examples

- Users in a data dump identified as an undisclosed breach
- Identification of service headers discovered a forgotten development server, with known vulnerabilities
- VIPs commonly identified in mailing lists receiving larger amounts of MalSpam.

© 2018 FUJITSU

180° view - Malware Assessment Service

FUJITSU

Malware Assessment Service (MAS)

- Provides a 'light-weight', unobtrusive point-in-time assessment across defined percentage of endpoints within your estate
- Uses CylanceProtect to identify compromises within the enterprise including dormant/ running threats on laptops, desktops and server estate

Outcomes

- On average, 14 pieces of greyware or malware per machine are detected during each assessment
- Typically Cylance runs alongside an existing AV during each POC but will always identify new threats.
- Fujitsu and Cylance have previously observed an active Advanced Persistent Threat (APT) actor during a recent assessment.
- Average oldest Potentially Unwanted Programme (PUP) discovered is around 11 years old!
- Older software carry higher likelihood of known vulnerabilities/ flaws
- Average number of Remote Access Trojans (RATs) is 10

CYLANCE

© 2018 Fujitsu

Customer benefits

Cost Savings

- Little to no up front cost
- Reduced post breach activities
- Brand and reputation protection

User Satisfaction

- Proactive services
- Tailored to the Customer environments
- Customer references

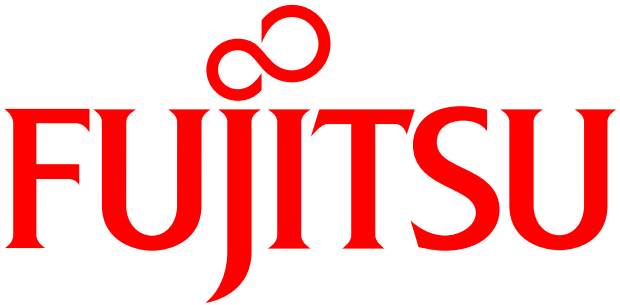
Efficiency

- Early warning | proactive threat advice
- Faster breach/ incident response times
- Shorter planning horizons

Security

- New and historic threat identification
- Breach detection
- Informed risk management decisions

© 2018 Fujitsu



shaping tomorrow with you