Threat 360

Cyber security

Advanced Threat Protection Service

Human Centric Innovation

Co-creation for Success
## Recent Damaging Data Breaches

<table>
<thead>
<tr>
<th>COMPANY</th>
<th>COST OF BREACH</th>
<th>WHAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo</td>
<td>$350 million</td>
<td>3B accounts compromised</td>
</tr>
<tr>
<td>Equifax</td>
<td>$114 million</td>
<td>115M accounts stolen</td>
</tr>
<tr>
<td>Far Eastern Int’ Bank</td>
<td>$60 million</td>
<td>Money stolen</td>
</tr>
<tr>
<td>Ethereum</td>
<td>$40 million</td>
<td>Money stolen</td>
</tr>
<tr>
<td>Uber</td>
<td>$?? million</td>
<td>57m personnel details stolen</td>
</tr>
<tr>
<td>Dun &amp; Bradstreet</td>
<td>$?? million</td>
<td>Accounts stolen inc’ personnel details</td>
</tr>
</tbody>
</table>

- 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
Businesses must take action

**UK manufacturers fall victim to cyber attacks, survey reveals**

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.

80 UK manufacturers subjected to cyber attacks but many more may have gone undetected, report finds.
Understand the threats – a dual perspective

**Inside-Out**

**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

**Outside-In**

**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

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

- 180°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.

- 180°view - Passive Threat Assessment looks at both the clear and dark web for information and threats relating to domain and brand.
180° view - Passive Threat Assessment

- 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
180° view - Passive Threat Assessment

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.
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
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
shaping tomorrow with you