Public Cybersecurity Vulnerability Market

Research from the National Institutes of Standards and Technology (NIST) National Vulnerability Database (NVD)

By Tanner Johnson
Senior Research Analyst – IoT Cybersecurity

IHS Markit conducted comprehensive research and analysis surrounding a dozen organizations that disclose information security vulnerabilities. As a component of this research, IHS Markit cross-referenced the data from these vendors against the information publicly disclosed by various government agencies, including:

- The MITRE Corporation
- The National Institute of Standards and Technology (NIST)
- The Computer Emergency Response Team Coordination Center (CERT/CC)
  - While listed with other reporting organizations, the CERT/CC is not a security vendor

Research Scope

The scope of IHS Markit's analysis used the following constraints:

- Vulnerabilities will only be credited to a vendor if they are ultimately responsible for managing the disclosure of the vulnerability
- All vulnerabilities must have been disclosed within the 2018 calendar year
- All vulnerabilities must have been assigned a common vulnerability and exposure (CVE) number.
- Disclosed vulnerabilities with associated CVEs that were not credited to the organizations within our scope were not incorporated or discussed as part of our overall analysis.
- In the instances where credit for a vulnerability was claimed by two or more vendors, we granted credit to each vendor making the claim, as there was no way to independently validate credit.
  - **1,454** vulnerabilities were claimed once, **80** vulnerabilities claimed twice, and **46** vulnerabilities were claimed three times.
  - This resulted in a total of **1,580** unique and verified vulnerabilities.
- As we attributed credit for each vulnerability to all vendors who claimed it, the resulting total number of all verified vulnerabilities claimed by the 12 research organizations for 2018 is ***1,752***.

Analysis Methodology

The data collected for this report stems from multiple sources, including:

- Primary Internal Research
- Individual Vendor Interviews
- Open Source Publications
- Publicly Disclosed Reports

IHS Markit collected all publicly available vulnerability data from each of the organizations listed in the executive summary and assigned credit for each vulnerability. However, in order to be attributed credit for a listed vulnerability an organization had to be responsible for effectively managing its disclosure, meaning that the organization directly orchestrated the release of the vulnerability.

- Credit for managing a vulnerability was not assigned to a vendor simply because it was listed on their publicly facing advisory website.

IHS Markit then collected data on all verified vulnerabilities during 2018 using the NIST NVD data feeds and used this data as the baseline for vendor comparison.

- To be considered verified, all vulnerabilities in our analysis had to have an associated CVE number in order to prevent rejected or duplicated entries from being introduced into the analysis, as well as have a CVSS value assigned by the NVD.

- Vulnerabilities without a CVE, while credited to the vendor listing them, could not be used in our analysis.

The CVSS and CWE metrics assigned by the NVD allowed IHS Markit to conduct a comparative analysis of the performance of all vendors, the severity of the vulnerabilities they disclosed, and the attack methodology of the vulnerabilities credited to each vendor.

Vulnerability Market Analysis

A vulnerability is a weaknesses, error, defect, flaw, or bug that poses a threat to the confidentiality, integrity, and availability of data within a computer system. Hackers seek to take advantage of any vulnerabilities present in hardware, software, and firmware, as they can be exploited in ways that compromise the systems on which they reside. The greater the window of time between the discovery of a vulnerability, its disclosure, and ultimate remediation, the more time a potential hacker to exploit the vulnerability.

Vulnerabilities that exist, but are unknown to the affected vendor, are commonly referred to as zero-day vulnerabilities. Zero-day vulnerabilities simultaneously pose the greatest threats to information security, while being viewed as the greatest prize for hackers to attain and share. As vulnerabilities can only be addressed once they are discovered and shared with the affected vendor, there is an incentive to report a vulnerability as quickly as possible. Even if a vulnerability is mitigated through a patch or an update, the threat remains for every user who hasn’t implemented the security fix.

As more product vendors, security organizations, and individual researchers contribute to the process, the associated threats introduced by vulnerabilities can be mitigated with greater efficacy. The potential impact of these vulnerabilities can vary greatly, as some security flaws may merely be annoying, others are critical enough to have potentially catastrophic consequences for the vulnerable systems and its users.

To conduct comprehensive analysis on any vulnerability, there are several characteristics and values that need to be identified first in order to cross reference them across reporting organizations:

- Common Vulnerability and Exposure (CVE) values
  - Unique identifier given to each vulnerability by a CVE Numbering Authority (CNA)
- Common Weakness Enumeration (CWE) values
  - Preliminary identifier used to categorize and define common software weaknesses
- Common Vulnerability Scoring System (CVSS) values
  - Numerical score reflecting the severity of the vulnerability

Results

The associated CVSS score attached to each vulnerability by the NVD provides organizations with a visible metric to gauge the severity associated with any vulnerability and help prioritize any threat remediation strategies.

Critical threats are those that can have potentially catastrophic impacts on an organization’s information security. These threats typically surround unauthorized root-level access and can result in the modification or disclosure of data or denial of service (DoS). Threats are often elevated to this level if an attacker can gain access without any special conditions or knowledge.

- Critical scoring vulnerabilities accounted for roughly 9.6% of all disclosed threats.

High-scored threats can also have substantially damaging effects to the information security of an organization. However, these vulnerabilities are traditionally more challenging to exploit, as they require certain conditions be met first. Although, any exploitation can still result in privilege escalation or loss of access to data.

- High scoring vulnerabilities accounted for the majority of those disclosed, accounting for roughly 62.0%.

Medium vulnerabilities can have negative impacts on an organization's data security, but are often more challenging to exploit, as specific requirements must be met to effectively exploit the vulnerability.

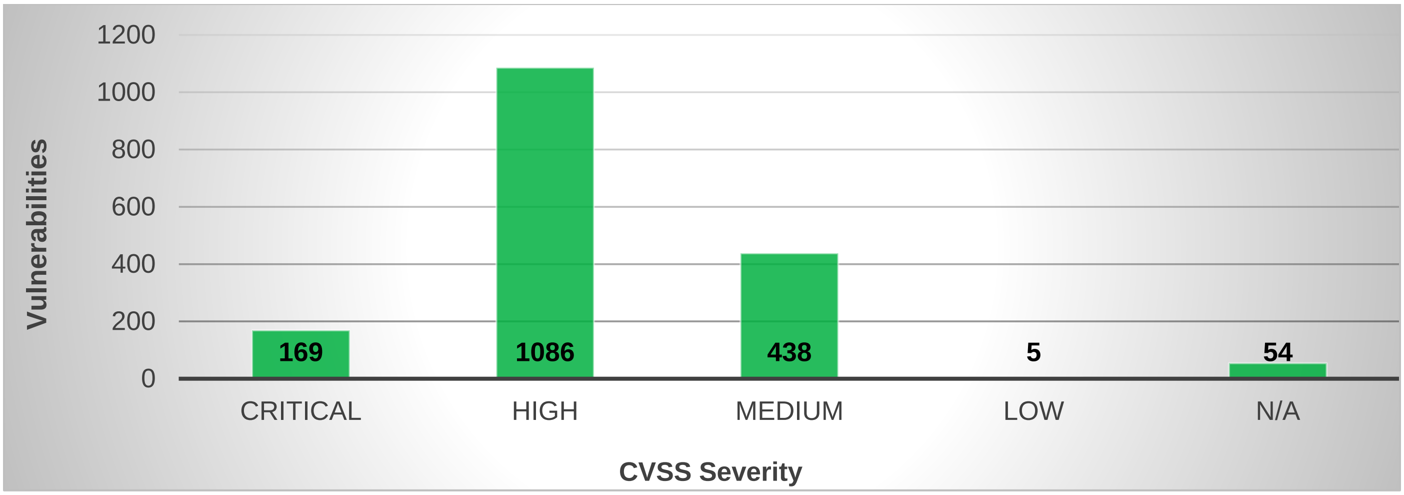
- Medium scoring vulnerabilities were ranked second, comprising roughly 25.0% of those disclosed.

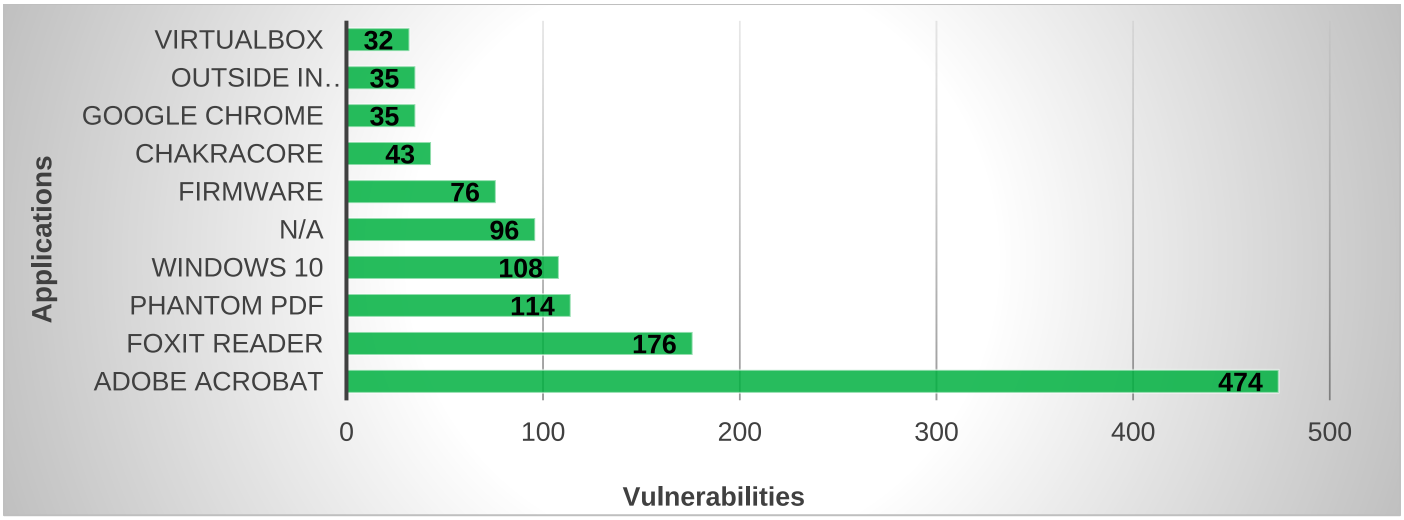
Low-N/A scored vulnerabilities have little to no impact on the data security for an organization and pose more of an annoyance than a legitimate threat.

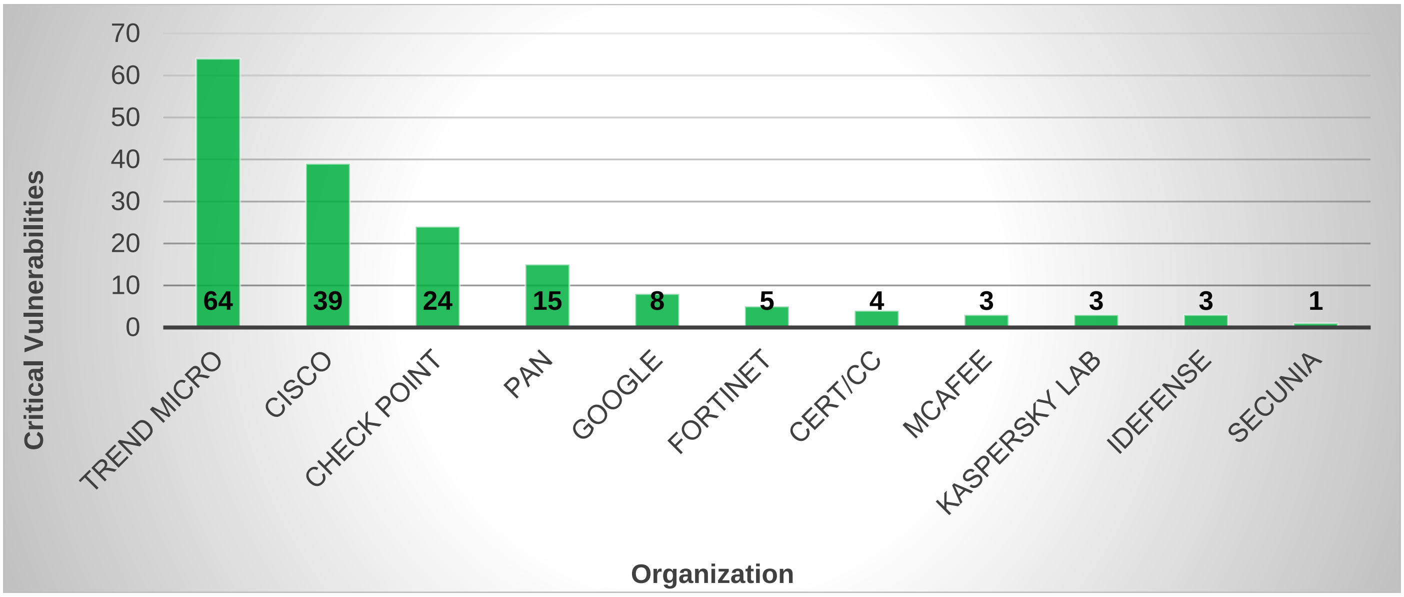
- These low-grade threats accounted for less than 3.3% of all disclosed vulnerabilities.

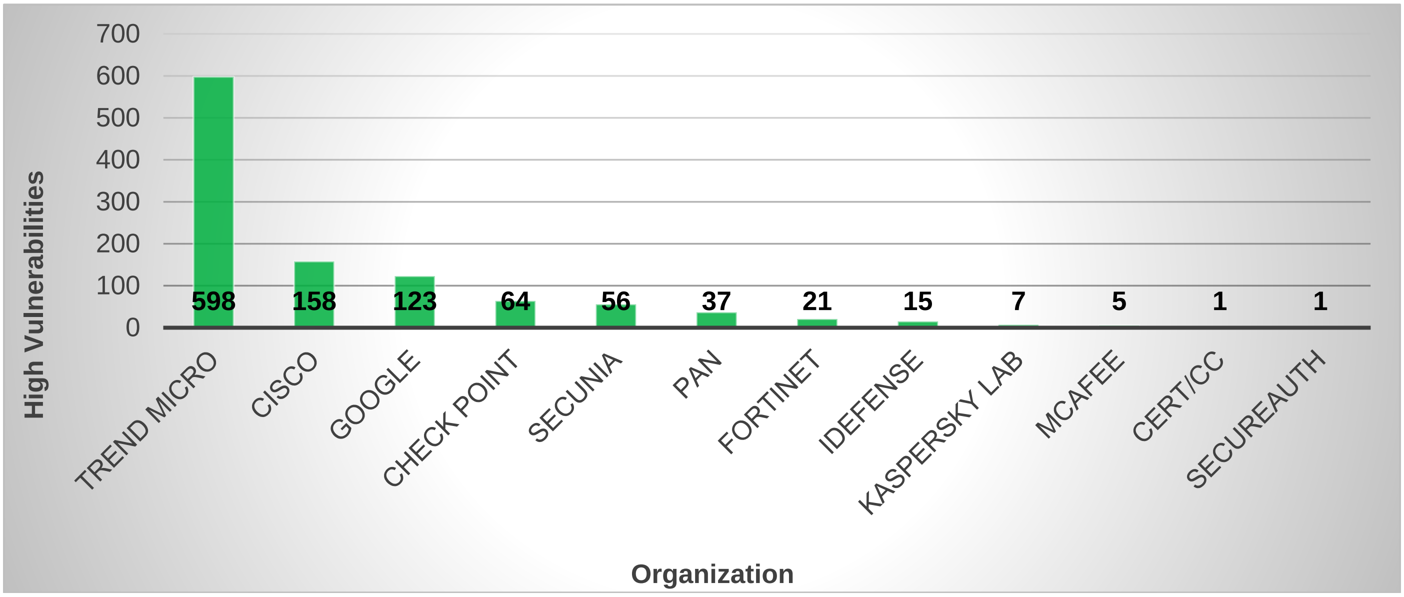
Conclusion

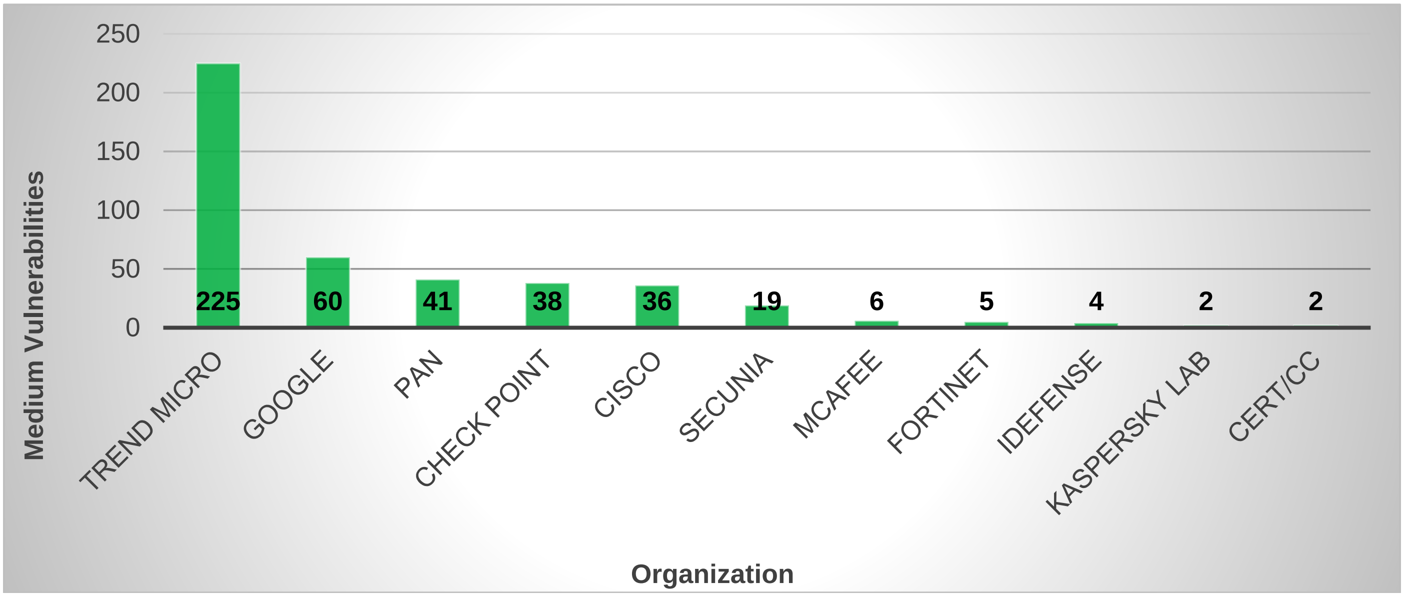
Each of the organizations analyzed in this research is contributing towards the efforts of discovering and disclosing information security vulnerabilities. It is through the diligence of vendors such as these that the security of data can become more robust, as flaws can only begin to be addressed once they are acknowledged. As technology continues to evolve, it is imperative that this work continue if comprehensive security is to be achieved through the responsible management of vulnerabilities.

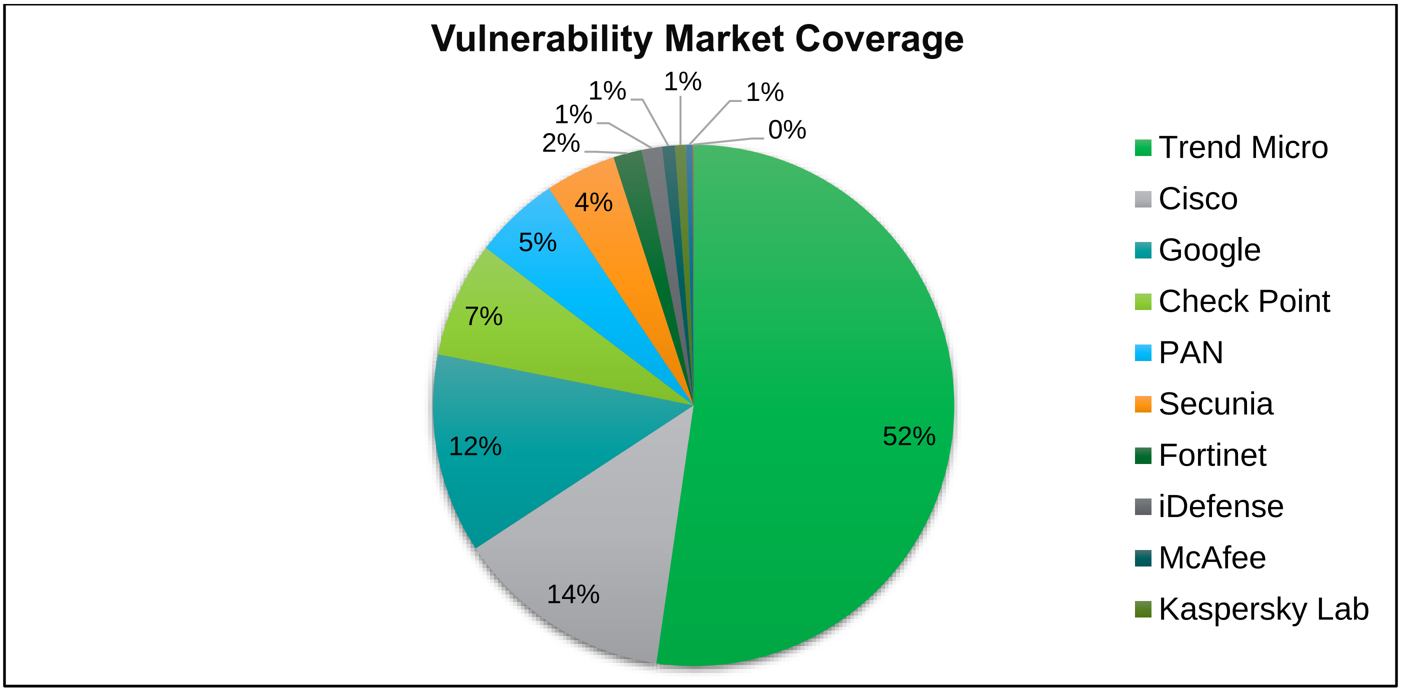





Critical Vulnerabilities
70
60
50
40
30
20
10
0
64
39
24
15
8
5
4
3
3
3
1
TREND MICRO
CISCO
CHECK POINT
PAN
GOOGLE
FORTINET
CERT/CC
MCAFEE
KASPERSKY LAB
IDEFENSE
SECUNIA
Organization


High Vulnerabilities
700
600
500
400
300
200
100
0
598
158
123
64
56
37
21
15
7
5
1
1
TREND MICRO
CISCO
GOOGLE
CHECK POINT
SECUNIA
PAN
FORTINET
IDEFENSE
KASPERSKY LAB
MCAFEE
CERT/CC
SECUREAUTH
Organization


Medium Vulnerabilities
250
200
150
100
50
0
225
60
41
38
36
19
6
5
4
2
2
TREND MICRO
GOOGLE
PAN
CHECK POINT
CISCO
SECUNIA
MCAFEE
FORTINET
IDEFENSE
KASPERSKY LAB
CERT/CC
Organization



	Vulnerabilities Managed	Average of Base Score	Average of Exploitability Score	Average of Impact Score
Trend Micro	916	7.644	2.494	5.040
Cisco	236	7.830	2.344	5.332
Google	217	6.314	1.794	4.432
Check Point	126	7.454	2.606	4.787
PAN	93	7.220	2.484	4.663
Secunia	77	7.100	2.703	4.308
Fortinet	31	7.806	2.187	5.503
iDefense	22	7.700	2.609	5.014
McAfee	14	7.486	2.064	5.257
Kaspersky Lab	12	8.042	2.458	5.517
CERT/CC	7	8.529	3.743	4.757
SecureAuth	1	7.800	1.800	5.900
Total	1752	7.453	2.401	4.946

Lead Analyst

Tanner Johnson
Senior Research Analyst
IoT Cybersecurity
tanner.johnson@ihsmarkit.com
(417) 343-9980

Contributing Analyst

Sean Peterson
Project Manager
IoT and Smart Cities
sean.peterson@ihsmarkit.com
(503) 929-3843

Contributing Analyst

Jeff Wilson
Research Director and Advisor
Cybersecurity Technology
jeff.wilson@ihsmarkit.com
(408) 483-4584

Contributing Analyst

Liz Cruz
Associate Director
IoT and Smart Cities
liz.cruz@ihsmarkit.com
(512) 633-0329

For more information technology.ihs.com

Follow the conversation @IHSMarkitTech

americas
T +1 844 301 7334
E technology_us@ihs.com

emea
T +44 (0) 13 44 32 81 55
E technology_emea@ihs.com

apac
T +60 042913763
E technology_apac@ihs.com

About IHS Markit

IHS Markit (Nasdaq: INFO) is a world leader in critical information, analytics and solutions for the major industries and markets that drive economies worldwide. The company delivers next-generation information, analytics and solutions to customers in business, finance and government, improving their operational efficiency and providing deep insights that lead to well-informed, confident decisions. IHS Markit has more than 50,000 business and government customers, including 80 percent of the Fortune Global 500 and the world's leading financial institutions. Headquartered in London, IHS Markit is committed to sustainable, profitable growth.