JULY 2021 REPORT

TECH CHECKPOINT

JOB POSTINGS

KC | 5,871 +270 since June '21

US | 627,027 +47,877 since June '21

TOP 10 OCCUPATIONS

Occupation Title	# of Current Postings	Change from Last Month
Software Developer	1,570	+62
Computer User Support Specialist	1,502	+105
Network and Computer Systems Administrator	749	+62
Computer Systems Engineer/Architect	582	+33
Information Security Analyst	356	+32
Infromation Technology Project Manager	259	+28
Computer Systems Analyst	242	+13
Software Quality Assurance Analyst and Tester	208	-41
Database Administrator	99	-6
Web Developer	86	-10

TOP 10 CERTIFICATIONS

Certification Title	# of Current Postings	Change from Last Month
Secret Clearance	121	-19
CISSP	84	+11
PMP	76	-1
CCNA	58	+8
CSM	40	+17
CISM	38	+5
CCNP	35	+7
MCP	32	New
CISA	29	Returning
MTA	28	-1

TOP 10 HARD SKILLS

Skill Title	# of Current Postings	Change from Last Month
Computer Programming/Coding	1,097	+67
Agile	1,010	+58
Structured Query Language	871	+5
Java	752	+37
Amazon Web Services	692	+111
Microsoft Azure	661	+47
Python	612	+46
JavaScript	567	+36
Linux	499	+29
Scrum	439	+42

TOP 10 EMPLOYERS

Employer Title	# of Current Postings	Change from Last Month
Garmin*	284	+62
CTG	231	+4
Humana	211	-19
Cerner*	194	+39
Deloitte	147	+2
Accenture	119	+20
Honeywell	111	+25
WellSky Corporation	80	-14
Netsmart	77	-19
H&R Block	70	Returning

* Numbers for this company include job postings that may have previously been listed under an alternate name, or with an extension (like Corp. or Intl.) in the name. No duplicate listings are counted.

Report produced by the KC Tech Council | kctechcouncil.com

Data source: JobsEQ, a tool produced by Chmura | http://www.chmuraecon.com/jobseq/
This data was collected early August, 2021.

THE TECH CHECKPOINT | JULY 2021

DATA INSIGHT

After a small dip in June hiring, July has made gains back to May levels for Kansas City and nationwide. The Kansas City metro area increased to 5,871 total postings from 5,601 in June, trending upwards as the local hiring market begins to gear up after a summer lull. The United States job postings for the month of July grew to 627,027 total postings, up from 579,150 and perhaps indicative of lessening inflationary fears and a normal growth in hiring as Fall approaches.

The Top 10 Occupations saw increases for most categories, with Computer User Support Specialist leading the way (+105), reflecting strong hiring trends for area service desks. A perennial heavyweight, Software Developer (+62) tied for second with Network and Computer Systems Administrator. Software Quality Assurance Analyst and Tester (-41) suffered the most significant number of losses, followed by Web Developer (-10).

For Certifications, July saw a total of 541 postings, growing by 8%. CSM (+17) led the way for certifications in the category in June, followed by CISSP (+11). By far, the largest decrease was for Secret Clearance (-19), although remaining category leader. PMP (-1) and MTA tied for second-most losses, with all other categories showing growth in July. A returning certification, CISA (+29) and one new certification, MCP (+32), debuted this month with strong posting numbers.

The Top 10 Hard Skills for July showed increases across the board to a total of 7,200 postings, with strong growth of 7% overall. Computer Programming/Coding (+67) again led the category with 1,097 postings but Amazon Web Services (+111) led in terms of growth and again demonstrated the increasing popularity of cloud platforms. Structured Query Language (+5) had the smallest increase in growth and was the only entry to have single-digit growth.

The Top 10 Employers of Tech Talent also reflected growing hiring, with a total of 1,524 postings in July. Employers largely remained the same from last month, although HR Block (+70) returned to the category after an absence of three months. The category leader was Garmin (+62), with Cerner (+39) following in second place. There were two companies with a downward trend, Humana (-19) and WellSky Corporation (-14).

EMERGING IT TRENDS

Recently ransomware attacks have become a fixture in the news. Although they have existed for many years, the Colonial Pipeline attack was one of the first large-scale attacks against an American company to grab the nation's attention thanks to panic buying and long lines at Northeastern gas stations. The rise of cryptocurrency has only facilitated these attacks thanks to the inherent near-untraceable characteristics of this new form of payment.

816.960.3800
ITSolutions@eccoselect.com
www.eccoselect.com

EMERGING IT TRENDS CONTINUED

While ransomware attacks are hard to prevent, there are steps a company can take to reduce the odds of suffering one. A robust cybersecurity team, up-to-date software, and good backup and contingency planning can help reduce the severity and potential of an attack, but there are other methods such as:

- **Educate employees:** A vital part of corporate cybersecurity is educating employees on safe computing practices. Cyber threats often being with something as simple as clicking a link or attachment in an email. It is critical to educate personnel on recognizing signs of ransomware and how to react when they encounter suspicious activity. Provide employees with a point of contact to report unusual or suspicious emails to the appropriate parties. Provide annual training on threats such as ransomware, phishing, and social engineering. With proper guidance and training, a company's employees can become the first line of defense in protecting against ransomware.

- **Limit access:** Understand the sensitivity of the information within your company and limit access accordingly. Companies should review existing access and privilege controls for all users and ensure the level of access is appropriate for their day-to-day duties. Restricting these privileges will decrease a company's overall risk of ransomware attacks and other forms of cybercrime. Multi-factor authentication (MFA) should be required for employees who have access to sensitive files and information. MFA requires users to use two forms of identification to gain access; for example, using an ID and password and then answering a verification challenge texted to their mobile phone.

- **Block known risks:** most organizations protect their server infrastructure, but don't forget one of the primary paths of ransomware is via employee devices. Companies should ensure they have up-to-date and appropriately configured malware detection running on desktops and laptops. Software such as this detects known ransomware and prevents it from going through the malicious file encryption process.

Cybersecurity is not just a technology issue; it is a business issue. Ransomware attacks will continue to escalate in volume and severity. However, a robust cybersecurity team and well-informed employees can help buttress defenses against this type of malware. As in most cases, an old proverb applies equally well to avoiding ransomware attacks as it did to the medical field; An ounce of prevention is worth a pound of cure!

Author: Ted Deel, VP Software Development and Solutions
tdeel@eccoselect.com

Citation: Rosenberg, A. (2017, June 28). Technology is the hidden driver of low inflation: BlackRock's RiederAlex. CNBC. https://www.cnbc.com/2017/06/28/technology-is-the-hidden-driver-of-low-inflation-blackrocks-rieder.html.