Crime Fighters

Five awesome cybersecurity jobs you never knew existed

BY MATT ALDERTON

It's perhaps unlikely that any child has ever said, "When I grow up, I want to work in the IT department." However, that might soon change, thanks to the flourishing field of cybersecurity. Not only because cybersecurity professionals are in high demand — there are expected to be more than 1.5 million unfilled positions in the field worldwide by 2020, according to a 2015 study by cybersecurity training nonprofit (ISC)² — but also because cybersecurity careers can be surprisingly exciting.

Not convinced? Here are five positions that might change your mind:

PENETRATION TESTER

Penetration testers, or pen-testers, are hackers with a heart of gold. Also known as ethical or white-hat hackers, it's their job to break into computer systems to help organizations identify — then fix — their weaknesses.

"You get paid to break into customers' networks," says Chris Triolo, vice president of customer success at Respond Software, a provider of automated cybersecurity threat protection. "Whether exploiting a vulnerability on an unpatched web server, sending a malicious file through email enticing a user to click on it or tricking an employee to give you their password, anything goes."

CYBERCRIME INVESTIGATOR

This job could appeal to fans of crime shows and detective novels.

"Cybercrime investigators ... are hired to investigate cybersecurity crimes," explains Jeff Friess, practice leader of the cybersecurity division at Global Executive Solutions Group, an executive search firm. "For example, Equifax, one of the largest credit bureaus, was penetrated in 2017 and personal data for 145 million people was compromised, including Social Security numbers. Cybercrime investigators would work to figure out who did the hack and help bring them to justice — just like the FBI would investigate a homicide."

INCIDENT RESPONDER

After cyberattacks, victims call the authorities, including incident responders, who are digital EMTs.

"When a company is facing a massive cybersecurity attack or realizes there's been a data breach, incident response teams are the 'first responders' who come in to help them shut down the attack, investigate what happened and strengthen their systems against future attacks," says Wendi Whitmore, global lead of incident response and intelligence services at IBM, which she describes as a "cybercrime scene investigation unit."

THREAT RESEARCHER

Threat researchers are the translators of the cybersecurity world. Their job is to take the complicated IT language and decode it for businesspeople.

"If cybersecurity were a football analogy ... threat researchers like me are the coaching staff that breaks down the biggest plays in the game," explains Curtis Jordan, lead security engineer and threat researcher at TruSTAR Technology, which, through its security intelligence platform, allows companies to share information about cyberthreats. "Being a threat researcher gives you a front-row seat to the latest hacks happening on your network and beyond. You observe common exploits, analyze them, identify large-scale patterns and then relay those back to security teams so that they know what malicious behavior to look for."

THREAT HUNTER

Cybersecurity is a game of cat and mouse. As a threat hunter, you're the cat.

"This role is close to that of a field biologist, as the threat hunter observes their prey — third-party attackers — in the wild," says Kayne McGladrey, director of information security services at Integral Partners, a cybersecurity firm whose specialty is identity and access management, and a member of the Institute of Electrical and Electronics Engineers. "Threat hunters set traps and snares that appeal to (cybercriminals) and lead to fake computers where the threat hunter can monitor an attacker's behavior before shutting down the breach." ■

GETTY IMAGES