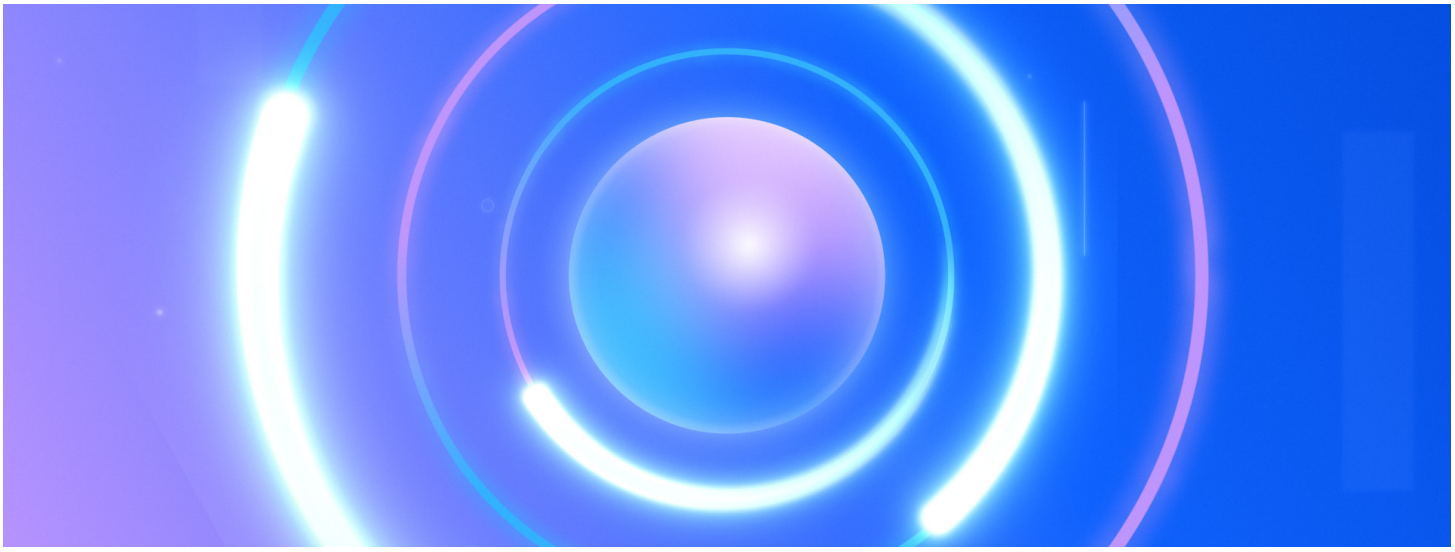
IBM Newsroom

New IBM Study Finds Cybersecurity Incident Responders Have Strong Sense of Service as Threats Cross Over to Physical World

- Sense of duty to protect others cited amongst the top reasons 77% of respondents entered Incident Response (IR)

- Ransomware has exacerbated the psychological demands of IR for 81% of respondents

- Majority of respondents have sought out mental health assistance due to their experiences responding to cyberattacks



CAMBRIDGE, Mass., Oct 3, 2022 /PRNewswire/ -- IBM Security (NYSE:IBM) today announced the results of a global survey that examines the critical role of cybersecurity incident responders at a time when the physical and digital worlds are increasingly converging. The study, released during National Cybersecurity Awareness Month, found that incident responders surveyed – the frontline responders to cyberattacks – are primarily driven by a strong sense of duty to protect others; a responsibility that's increasingly challenged by the surge of disruptive attacks, from the proliferation of ransomware attacks to the recent rise of wiper malware.

Organizations that are essential to the global economy, supply chains and the movement of goods have become prime targets for disruptive attacks. In 2021 IBM Security X-Force observed cyberattacks against energy companies quadrupling from the year prior, while manufacturers saw more ransomware attacks than any other industry – from food manufacturers to medical devices, cars and steel manufacturers. As cyberattacks threaten essential services to our daily needs, incident responders in these industries are faced with more pressure to defend the digital front line. In fact, 81% of respondents stated that the rise of ransomware has exacerbated the psychological demands associated to cybersecurity incidents.

The global survey of over 1,100 cybersecurity incident responders in 10 markets, conducted by Morning Consult and sponsored by IBM Security, revealed trends, and challenges that incident responders experience due to the nature of their profession. Some key highlights include:

- **A Sense of Service –** Over a third of incident responders were attracted to the field by a sense of duty to protect and opportunity to help others and businesses. For nearly 80% of respondents, this was one of the top reasons attracting them to IR.
- **Fighting Multiple Battlefronts –** Amid a growing number of cyberattacks in recent years, 68% of incident responders surveyed stated it's common to be assigned to respond to two or more overlapping incidents simultaneously.
- **Impact on Daily Life –** The high demands of cybersecurity engagements also affect incident responders' personal lives, with 67% experiencing stress or anxiety in their daily lives. Insomnia, burnout and impact on social life or relationships followed as effects respondents cited. Despite these challenges, the vast majority acknowledged they have a strong support system in place.

"The real-world repercussions that cyberattacks now have are causing public safety concerns and market-stressing risks to grow," said Laurance Dine, Global Lead, IBM Security X-Force Incident Response. "Incident responders are the frontline defenders standing between cyber adversaries causing disruption and the integrity and continuity of critical services. IBM

salutes all IR teams across the cybersecurity community, and the essential role they play in defending the digital front line."

An Uneven Battlefield

In recent years, not only have cyberattacks become more disruptive, but their sheer volume has increased. X-Force saw a nearly 25% rise in cybersecurity incidents its IR team engaged in from 2020 to 2021. Add to that, Check Point Software Technologies research indicates a 50% increase in overall network attacks per week in 2021 compared to 2020. But as the industry is called to respond to a growing number of cyberattacks, there's only a finite number of security professionals specifically trained and skilled to respond to cybersecurity incidents.

As a result, while many IR teams are forced to take on multiple battlefronts, businesses could be left without the necessary resources to mitigate and recover from cyberattacks. The IBM study found that 68% of incident responders surveyed find it common to simultaneously need to respond to two or more cybersecurity incidents, highlighting a field that is constantly engaged. Amongst U.S. respondents 34% said the average length of an IR engagement was 4-6 weeks, while a quarter cited the first week as often the most stressful or demanding period of the engagement. During this period about a third of respondents work more than 12 hours per day on average.

A Strong Support System in Place

As incident responders take on the pressure and high demands associated with cyber response, the overwhelming majority of respondents acknowledged they have a strong support system in place. Specifically, most respondents feel their leadership has a strong understanding of the activities IR involves, while 95% say it provides the necessary support structure for them to be successful. As well, 84% state they have adequate access to mental health support resources, with many respondents (64%) seeking out mental health assistance due to the demanding nature of responding to cyberattacks.

But businesses can further support incident responders, whether in-house Blue Teams or the external IR teams they engage in the event of a cyber crisis, by prioritizing cyber preparedness and creating plans and playbooks that are customized to their environment and resources. This can help enable a more agile and quick response at the onset of an incident and alleviate an unnecessary layer of pressure across the business.

To that end, situational awareness of their infrastructure is important. Businesses can focus on testing their state of readiness through simulation exercises, not only to get a feel of how their teams will react under attack, but to provide opportunities to correctly integrate multiple teams that are engaged during a cyber incident.

Additional Resources

- Read the complete findings from IBM Security's Incident Responderstudy
- Celebrate and recognize incident responders this Cybersecurity Awareness Monthhere
- Read a Security Intelligence blog on incident responders holding the digital frontline
- To register for IBM Security X-Force's incident response webinar, "Tales from the Digital Frontlines," onWednesday, October 12 at 1:00 pm ET, sign up here
- Schedule a consult with IBM Security X-Force

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development, and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Contact:
Georgia Prassinos
IBM Security Communications
gprassinos@ibm.com

SOURCE IBM

Additional assets available online: Photos

https://stage.mediaroom.com/ibmnewsroom/2022-10-03-New-IBM-Study-Finds-Cybersecurity-Incident-Responders-Have-Strong-Sense-of-Service-as-Threats-Cross-Over-to-Physical-World