IBM Study: Security Response Planning on the Rise, But Containing Attacks Remains an Issue

Tuesday, June 30, 2020 10:00:00 AM (GMT)

- Global Survey Finds Use of More Than 50 Security Tools Leads to Less-Effective Security Response
- Majority of Organizations Don't Have Specific Plans for Common and Emerging Attacks

CAMBRIDGE, Mass., June 30, 2020 /PRNewswire/ -- IBM (NYSE: IBM) Security today announced the results of a global report examining businesses' effectiveness in preparing for and responding to cyberattacks. While organizations surveyed have slowly improved in their ability to plan for, detect and respond to cyberattacks over the past five years, their ability to contain an attack has declined by 13% during this same period. The global survey conducted by Ponemon Institute and sponsored by IBM Security found that respondents' security response efforts were hindered by the use of too many security tools, as well as a lack of specific playbooks for common attack types.

While security response planning is slowly improving, the vast majority of organizations surveyed (74%) are still reporting that their plans are either ad-hoc, applied inconsistently, or that they have no plans at all. This lack of planning can impact the cost of security incidents, as companies that have incident response teams and extensively test their incident response plans spend an average of $1.2 million less on data breaches than those who have both of these cost-saving factors in place.[1]

The key findings of those surveyed from the fifth annual *Cyber Resilient Organization Report* include:

- **Slowly Improving:** More surveyed organizations have adopted formal, enterprise-wide security response plans over the past 5 years of the study; growing from 18% of respondents in 2015, to 26% in this year's report (a 44% improvement).
- **Playbooks Needed:** Even amongst those with a formal security response plan, only one third (representing 17% of total respondents) had also developed specific playbooks for common attack types — and plans for emerging attack methods like ransomware lagged even further behind.
- **Complexity Hinders Response:** The amount of security tools that an organization was using had a negative impact across multiple categories of the threat lifecycle amongst those surveyed. Organizations using 50+ security tools ranked themselves 8% lower in their ability to detect, and 7% lower in their ability to respond to an attack, than those respondents with less tools.
- **Better Planning, Less Disruption:** Companies with formal security response plans applied across the business were less likely to experience significant disruption as the result of a cyberattack. Over the past two years, only 39% of these companies experienced a disruptive security incident, compared to 62% of those with less formal or consistent plans.

"While more organizations are taking incident response planning seriously, preparing for cyberattacks isn't a one and done activity," said Wendi Whitmore, Vice President of IBM X-Force Threat Intelligence. "Organizations must also focus on testing, practicing and reassessing their response plans regularly. Leveraging interoperable technologies and automation can also help overcome complexity challenges and speed the time it takes to contain an incident."

Updating Playbooks for Emerging Threats

The survey found that even amongst organizations with a formal cybersecurity incident response plan (CSIRP), only 33% had playbooks in place for specific types of attacks. Since different breeds of attack require unique response techniques, having pre-defined playbooks provides organizations with consistent and repeatable action plans for the most common attacks they are likely to face.

Amongst the minority of responding organizations who do have attack-specific playbooks, the most common playbooks are for DDoS attacks (64%) and malware (57%). While these methods have historically been top issues for the enterprise, additional attack methods such as ransomware are on the rise. While ransomware attacks have spiked nearly 70% in recent years,[2] only 45% of those in the survey using playbooks had designated plans for ransomware attacks.

Additionally, more than half (52%) of those with security response plans said they have never reviewed or have no set time period for reviewing or testing those plans. With business operations changing rapidly due to an increasingly remote workforce, and new attack techniques constantly being introduced, this data suggests that surveyed businesses may be relying on outdated response plans which don't reflect the current threat and business landscape.

More Tools Led to Worse Response Capabilities

The report also found that complexity is negatively impacting incident response capabilities. Those surveyed estimated their organization was using more than 45 different security tools on average, and that each incident they responded to required coordination across around 19 tools on average. However, the study also found that an over-abundance of tools may actually hinder organizations ability to handle attacks. In the survey, those using more than 50 tools ranked themselves 8% lower in their ability to detect an attack (5.83/10 vs. 6.66/10), and around 7% lower when it comes to responding to an attack (5.95/10 vs. 6.72/10).

These findings suggest that adopting more tools didn't necessarily improve security response efforts — in fact, it may have done the opposite. The use of open, interoperable platforms as well as automation technologies can help reduce the complexity of responding across disconnected tools. Amongst high-performing organizations in the report, 63% said the use of interoperable tools helped them improve their response to cyberattacks.

Better Planning Pays Off

This year's report suggests that surveyed organizations who invested in formal planning were more successful in responding to incidents. Amongst respondents with a CSIRP applied consistently across the business, only 39% experienced an incident that resulted in a significant disruption to the organization within the past two years compared to 62% of those who didn't have a formal plan in place.

Looking at specific reasons that these organizations cited for their ability to respond to attacks, security workforce skills were found to be a top factor. 61% of those surveyed attributed hiring skilled employees as a top reason for becoming more resilient; amongst those who said their resiliency did not improve, 41% cited the lack of skilled employees as the top reason.

Technology was another differentiator that helped organizations in the report become more cyber resilient, especially when it comes to tools that helped them resolve complexity. Looking at organizations with higher levels of cyber resilience, the top two factors cited for improving their level of cyber resilience were visibility into applications and data (57% selecting) and automation tools (55% selecting). Overall, the data suggests that surveyed organizations that were more mature in their response preparedness relied more heavily on technology innovations to become more resilient.

About the Study

Conducted by the Ponemon Institute and sponsored by IBM Security, the *2020 Cyber Resilient Organization Report* is the fifth installment covering organizations' ability to properly prepare for and handle cyberattacks. The survey features insight from more than 3,400 security and IT professionals from around the world, including the United States, India, Germany, United Kingdom, Brazil, Japan, Australia, France, Canada, ASEAN, and the Middle East.

Review the full report here: https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839

Sign up for our correlating webinar taking place July 23 at 11:00 AM ET here:
https://event.on24.com/wcc/r/2448121/9297B87DE7A378D816846835989BD762

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 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 70 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.

Media Contact:
Kim Samra
IBM Security
ksamra@ibm.com

510-468-6406

[1] IBM Security and Ponemon Institute: *2019 Cost of a Data Breach Report*

[2] IBM Security, *2020 X-Force Threat Intelligence Index*, (2020), p. 15

View original content to download multimedia: http://www.prnewswire.com/news-releases/ibm-study-security-response-planning-on-the-rise-but-containing-attacks-remains-an-issue-301085557.html

SOURCE IBM

Countries: United States
Industries: Computer Electronics, Hardware & Software, High Tech Security, Peripherals
Languages: English
Primary Identifiers: IBM-US
Related Identifiers: IBM-US