Logo

NEWS RELEASE

# INTRUSION Research Shows Confidence in Teams and Technologies to Thwart Cyberattacks Yet Cyber Breaches Still Commonplace Suggesting False Sense of Security

8/4/2021

Majority of Respondents Report at Least One Data Breach at Their Organization in the Past

- While IT budget allocations are significant for cybersecurity products, and respondents have confidence in their plans, teams, and products, they still regularly suffer data breaches suggesting a false sense of security
- Concern about cyberattacks threatening an organization abound as remote employees return to the office with their own devices
- 80% reported that security analysts at their organization spend time trying to resolve false-positive alerts with nearly half (47%) stating that it is standard practice to ignore 50% or more of alerts

PLANO, Texas and LAS VEGAS, Aug. 04, 2021 (GLOBE NEWSWIRE) -- INTRUSION, Inc. (Nasdaq: INTZ) today announced findings from a commissioned survey conducted in July about IT security decisionmakers’ false sense of security when it comes to neutralizing threats.

The research suggests that while IT security decisionmakers often consider cyberattacks a serious concern and are allocating a significant share of their IT budget to address their cyber defense challenges, data breaches have still been uncomfortably commonplace. Key takeaways from the survey include:

Budget vs. Breaches
Data breaches are too commonplace despite allocating significant portions of their IT budget to cybersecurity.

- Close to half explicitly dedicate 20% or more of their total IT budget to cybersecurity.

- One-third reported a data breach at their organization within the past 12 months with two-thirds of those cases involving employee personal devices (e.g., laptop, Smartphone). Ultimately, more than half (52%) reported a data breach at their organization at some time in the past.

### Response Plans, IT Staffing, Solutions

Significant cyberattack concerns often remain even with formal response plans and the combination of staff and solutions being considered effective.

- 84% reported having a formal cyberattack response plan. However, among these respondents, a sizable proportion (44%) were still "Very Concerned" about cyberattacks harming their organization.
- Among those who rate both their cybersecurity team and software, services, tools, etc. as "Very Effective," 61% were still "Very Concerned" about cyberattacks threatening their organization. When asked which -- staff or solutions -- was most critical for effective defense against cyberattacks at their organization, 28% favored the cybersecurity team, while 19% favored their product mix. Slightly more than half felt that both were equally important.

### Inside vs. Outside Threats

The survey addresses internal and external threats and reveals a sentiment of false security given the occurrences of data breaches.

- Approximately three-fourths (76%) expressed it is probable that malware has been embedded in computer hardware/equipment manufactured abroad and sold to U.S. organizations.
- When asked if their organization has sufficient protection from outside threats to their networks and from inside threats such as call-homes, respondents answered, "yes, definitely" 47% and 58% of the time, respectively. (A "call-home" is when malware on a device tries to connect with a command-and-control server to get updates or instructions.)

### Data Breaches Continue Despite Heightened Efforts and Investment

INTRUSION believes the survey findings demonstrate that IT decisionmakers are struggling with the current combination of IT staffing/security solutions ability to effectively stop cyberattacks.

"Virtually every day we wake up to a new headline of a successful cyberattack impacting every facet of our lives," said INTRUSION Chief Evangelist Gary Davis. "If you're in charge of IT security at any sized company, getting a good night's sleep may be a problem. With leaders fretting over the effectiveness of their teams and technologies things could get dramatically worse as those asked to work at home during the COVID-19 pandemic make their way back to the office with all their devices."

Continued Davis, “with 52% of IT/Security decision-makers reporting a data breach at their organization sometime in the past, we feel that those at the tip of the spear for their IT security can and should feel confident that they can effectively protect their company from being tomorrow’s headline.”

For additional details, plus a link to the official report please visit: **https://shield.intrusion.com/reports/2021-cybersecurity-confidence-report-pr**

About the Survey

INTRUSION commissioned Amplitude Research, Inc. to conduct a web survey about cybersecurity at organizations in the U.S. To qualify for the survey, respondents had to indicate that they are involved in decisions about IT security / Internet security at their organization. Also, when it comes to decisions about IT security purchases, services, design, set-up, and/or administration for IT security / Internet security at their organization, respondents were required to be a primary / final decisionmaker (76% of respondents), co-decision-maker (15%), or influencer of decisions (9%). The survey was completed by 450 qualified respondents in July of 2021.

About INTRUSION, Inc.

INTRUSION, Inc. (NASDAQ: INTZ) protects any-sized company by leveraging advanced threat intelligence with real-time artificial intelligence to kill cyberattacks as they occur – including zero-days. INTRUSION’s solution families include INTRUSION Shield, an advanced cyber-defense solution that kills cyberattacks in real-time using artificial intelligence (AI) and an advanced threat intelligence cloud; INTRUSION TraceCop™ for threat discovery and disclosure; and INTRUSION Savant™ for network monitoring and advanced persistent threat detection. For more information, please visit **www.intrusion.com**.

About Amplitude Research

Amplitude Research, Inc is a full-service online survey company and market research firm headquartered in Boca Raton, Florida that serves a wide variety of industries and markets throughout the United States and globally. Amplitude specializes in all kinds of consumer, b2b and IT market research studies, customer satisfaction studies, and job satisfaction / employee engagement surveys. Amplitude’s services include study design, survey administration, sampling, data analysis, custom report writing, and a full range of additional reporting and survey administration services. For more information about Amplitude Research, visit the company's website at **http://www.amplituderesearch.com**.

Cautionary Statement Regarding Forward Looking Information

This release may contain certain forward-looking statements, including, without limitations, statements about the performance of protections provided by our INTRUSIONShield product, as well as any other statements which reflect management's expectations regarding future events and operating performance. These forward-looking statements speak only as of the date hereof and involve a number of risks and uncertainties, including, without limitation, the risks that our products and solutions do not perform as anticipated or do not meet with widespread market acceptance. These statements are made under the "safe harbor" provisions of the Private Securities Litigation Reform Act of 1995 and involve risks and uncertainties which could cause actual results to differ materially from those in the forward-looking statements, including, risks that we have detailed in the Company's most recent reports on Form 10-K and Form 10-Q, particularly under the heading “Risk Factors.”

INTRUSION Media Inquiries

Michael Krems, Analyst & Public Relations Manager

Email: Michael.Krems@intrusion.com

Mobile: 805.496.8166

Source: INTRUSION Inc.