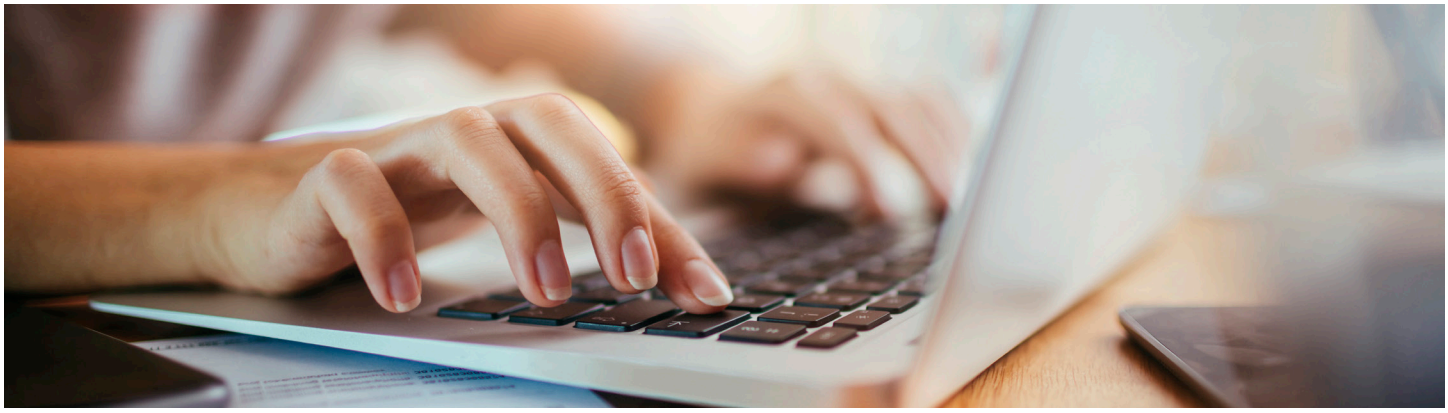

Data Event Detection and Investigation in a Remote World

What Organizations Can Do Now to Ensure Preparedness

While it is a given that cyber criminals, human error, and reliance on data and information systems are here to stay, organizations are facing the unanticipated possibility that remote work will be a long-term or even permanent part of operations. Cybersecurity measures, including efforts related to incident response preparedness, must adapt accordingly.

NetDiligence® interviewed Chris Dilenno from Mullen Coughlin, a mid-size national law firm solely dedicated to data security/privacy incident response management, counseling, and litigation. Mullen Coughlin's team has extensive experience (approximately 20,000 matters over 15 years) counseling organizations on pre-event preparedness, incident response, regulatory investigation defense, and single-plaintiff/class-action defense arising out of data privacy events. Here, Mullen Coughlin provides abbreviated guidance on what businesses can do to better prepare for the investigation of and response to a data privacy event in a remote-work world.

MULLEN COUGHLIN

What Organizations Can Do Now to Prepare for a Cyber Incident

ND: ***What steps can an organization take now to better prepare to respond to an incident with some or all staff working remotely?***

MC: There are four steps that should be taken to respond to a data privacy event. First, ensure your cyber incident response plan is realistic, short, and flexible. Second, understand the risks of remote work and operations. Third, understand challenges the organization will face regarding remote coordination of incident detection and response. And finally, conduct remote tabletop exercises to ensure your incident response plan is flexible enough to handle all types of events.

ND: ***How can an organization ensure its cyber incident response plan is realistic?***

MC: An organization's incident response plan should be short, flexibly responsive to cyber events, updated on at least an annual basis, and contain business and personal contact information for the incident

response team (and their backups), including contact information for your cyber insurance carrier and broker and the toll-free event reporting number that most carriers provide. It should allow for immediate internal alert of suspicious activity to technology, risk, operations, and legal departments. It should NOT direct the engagement of, or reliance on, previously engaged IT providers or the direct engagement of external incident response support vendors (other than counsel). It must be flexible enough to address various and constantly evolving cyber risks, but structured enough to always provide for rapid response, data preservation, and engagement of appropriate incident response support providers at the earliest detection of suspicious activity. Finally, you should be able to access the plan at a moment's notice, even in off hours. One example that we've seen of a robust but flexible plan is Breach Plan Connect®, from NetDiligence. In addition to the features discussed here, it includes a mobile app to facilitate response communications, which is extremely important in a remote-work environment.

ND: ***How can an organization understand its unique risks with regard to remote work and operations?***

MC: Remote operations create unique risks. Some organizations seamlessly transitioned from in-person to remote operations. But we've heard plenty of stories about staff being told to purchase laptops or portable devices as the company wasn't able to provide prior to going remote. The introduction of new devices and new work environments should be red flags for organizations. It is key to: (1) confirm access and audit rights to all devices connecting to the system or housing the organization's data; (2) conduct a review of new technical and legal risks to information and system security, including the heightened risk of phishing attacks, ransomware, and social engineering; and (3) conduct fresh employee training on device, information and system access, use, and security.

ND: ***How can an organization understand challenges it will face regarding remote coordination of incident detection and response?***

MC: If you've not conducted employee training since moving to a remote work environment, you must. In post-COVID operations, detection and reporting of suspicious activity and the ability to monitor system usage while users are connected remotely present new challenges. Historically, incident response plans depended on key staff gathering in a central location or conducting in-person investigations. Today, this "in-person" ability to swiftly detect and immediately respond to suspicious activity is much more difficult.

ND: ***What recommendations do you have for organizations performing remote tabletop exercises?***

MC: Start. Use real experts who don't dabble in the space. Organizations must conduct expert remote tabletop exercises to ensure the incident response plan is flexible enough to handle all types of events from afar. Regular and varied tabletop exercises are important if you want to efficiently execute your response.

The key to successful and swift execution is practice. Employ several fact patterns based upon recent cyber trends and risks unique to the organization. At the conclusion of the tabletop exercise, reflect on opportunities for improvement and effectuate them.

MENTIONED IN THIS ARTICLE

Breach Plan Connect®, powered by NetDiligence®, is a turnkey solution designed to help senior managers oversee and coordinate their organization's response to a cyber incident. Breach Plan Connect (BPC) provides a ready-made incident response plan that can be easily customized for different types of organizations. It comes with a mobile app for 24x7 access and communication, a critical requirement in remote-work environments or when company systems have been compromised. BPC makes it easy for senior managers and legal counsel to: a) monitor the organization's overall response, and b) provide guidance and authorization as needed to tactical teams, such as IT and related third-party experts. For more information, visit us at: https://netdiligence.com/solutions/breach-plan-connect/